ADVANCED PERSISTENT THREAT CASE STUDIES

Printed in November 2016

Summary

Kaspersky

Lutech

Trend Micro

Tiger Security

European Electronic Crime Task Force

The European Electronic Crime Task Force (EECTF) is an information sharing initiative, started in 2009 by an agreement between United States Secret Service, Italian Ministry of Internal Affairs and Poste Italiane.

The mission is to support the analysis and the development of best practices against cybercrime in European countries, through the creation of a strategic alliance between public and private sectors, including Financial Sector, Law Enforcement, Academia, International Institutions and ICT security vendors.

EECTF aims to:

- Strengthen relationships between the different players;
- Train and support members through sharing expertise and knowledge:
- Enable an effective communication channel for information exchange;
- Maintaining co-operation on a technical and operational level.

United States Secret Service participates through the Rome Office, the Italian Ministry of Interior participates through the Service of Postal and Telecommunications Police and Poste Italiane participates through the Information Security Department.

Initially restricted to the only Founder Members, the EECTF has been opened thereafter to the main stakeholders in cybercrime, who expressed the will to contribute to a proactive sharing of relevant information and a Permanent Members Group has been started, who gather to analyze emerging trends in cyber-crime and discuss methodologies and techniques to combat them.

The EECTF is run via monthly meetings of a selected group of Permanent Members, quarterly open events extended to a wide Community of selected experts and continuous sharing of information relevant to the cybercrime scenario, also through dedicated specific tools.

Permanent Members are internationally acknowledged organizations, both private and public, with a broad view on prevention, analysis and contrast of electronic crimes at European level, whose competencies might represent instances coming from whole domains of interest.

Permanent Members formally commit to proactively share information with other Members of the Group in a non-competitive environment, according to a non-disclosure agreement, and to actively contribute to the EECTF life, taking part to meetings and supporting the EECTF development.

Additionally, in order to make the most out of the competencies of the whole community of the EECTF, an Expert Group has been started, which gather on a periodic basis and is restricted to only Permanent Members, focusing on technical information sharing about new threats and possible countermeasures.

Executive Summary

In the last years, many public and private organizations have been target of Advanced Persistent Threats (APTs), sophisticated, targeted and persistent threats aimed to steal information like intellectual property, organization or state secrets for economic, technical political, or military reasons. In the future, APTs will probably continue to increase and change their attack patterns.

APTs are very difficult to detect and remove. They can act undetected on network for long time, control the target waiting for the opportunity to leaking out your information. In many cases, skilled and motivated attackers use advanced-intelligence techniques and are able to erase its presence.

Only an early detection and a strong response capability can help organization to face APTs attack. Identification of Threat Indicators and Techniques, Tactics and Procedures (TTP) of attacks as well as information sharing and collaboration can enhance prevention and detection capabilities of organization. In the same time, an effective operative collaboration requires adoption of common methodologies and standards.

The aims of this study are:

- to provide an overview of APTs attack patterns, threat indicators and possible recommendations
- to provide a classification model to facilitate information sharing and enhance defence capabilities

The target group of the publication are the decision makers and security managers of Critical Infrastructure and Institutions. The work is intended to share experts' recommendations in order to correctly prevent, detect and respond to APT attacks.

In order to classify the information gathered in this study and to compare it between the several case studies presented, the publication will use the "Cyber Kill Chain" method.

The Cyber Kill Chain method was adapted from a military concept to information security by Lockheed Martin.

It presents the attack techniques, tactics and procedures in seven steps[1]:

1. Reconnaissance: Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.
2. Weaponization: Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer).
3. Delivery: Transmission of the weapon to the targeted environment.
4. Exploitation: After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.
5. Installation: Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
6. Command and Control (C2): Typically, compromised hosts must

[1] "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill CHains", Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, pag. 4-5

beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.

7. Actions on Objectives: Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration, which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point.

Each chapter presents a case study of attack. The case studies are divided in the 7 phases described above. Moreover, the authors present also a series of recommendations that could be helpful.

Terms and Acronyms

API	Application Programming Interface
APT	Advanced Persisent Threat
ASP	Active Server Pages
AV	Audio Video
AVI	Audio Video Interleave
BACnet	Building Automation and Control networks
BMP	BitMaP
C&C - C2	Command and Control
CMS	Content Management System
DLL	Dynamic-Link Library
DLP	Data Loss Prevention
DNS	Domain Name System
FTP	File Transfer Protocol
GOLANG	Go Programming Language
GSMTP	Google SMTP
HTTP	HyperText Tranfer Protocol
HVAC	heating, ventilating, and air-conditioning control

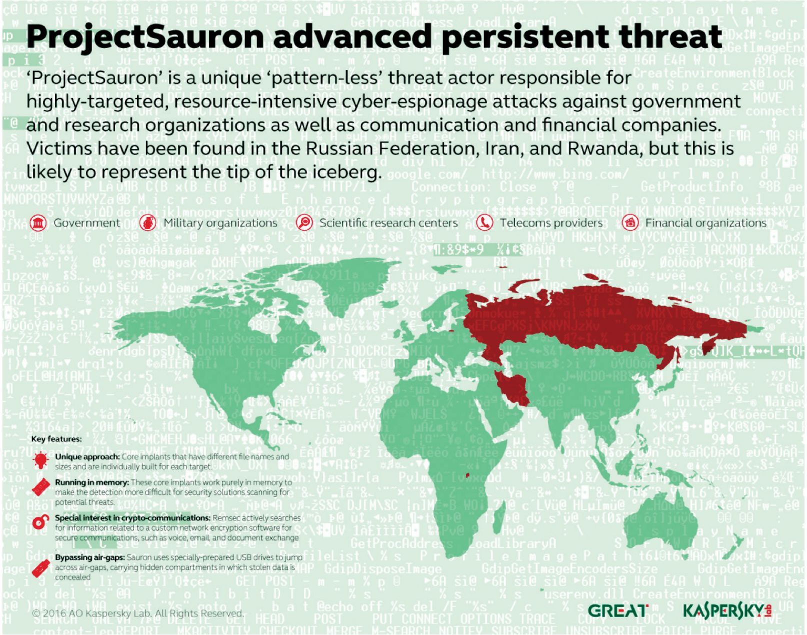
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
ICT	Information & Communication Technology
ID	Device Identification
IDS	Intrusion Detection System
IIS	Internet Information Service
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
KATA	Kaspersky Anti Targeted Attack Platform
LSA	Local Security Authority
L-TMS/CTI	Lutech Threat Management Service for Cyber Threat Intelligence
NAS	Network Attached Storage
OS	Operating System
PE	Portable Executable
PHP	Hypertext Preprocessor
PII	Personally Identifying Information
PNG	Portable Network Graphics
PV	Photovoltaic System
RAT	Remote Access Trojan
RC4	Ron’s Code 4 (RSA Variable-Key-Size Encryption Algorithm by Ron Rivest)
RCE	Remote Code Execution
RTLo	Right to left Override Method

SMTP	Simple Mail Transfer Protocol
STIX	Structured Threat Information eXpression
TA-11	Threat Actor 11
TAXII	Trusted Automated eXchange of Indicator Information
TCP	Transmission Control Protocol
TTP	Techniques, Tactics and Procedures
UDP	User Datagram Protocol
URL	Uniform Resurce Locator
VFS	Virtual File System
VPN	Virtual Private Network
WMI	Windows Management Instrumentation

Kaspersky

1. Case Study

High level summary of the key features of the attack:



ProjectSauron advanced persistent threat

'ProjectSauron' is a unique 'pattern-less' threat actor responsible for highly-targeted, resource-intensive cyber-espionage attacks against government and research organizations as well as communication and financial companies. Victims have been found in the Russian Federation, Iran, and Rwanda, but this is likely to represent the tip of the iceberg.

Government · Military organizations · Scientific research centers · Telecoms providers · Financial organizations

Key features:

Unique approach: Core implants that have different file names and sizes and are individually built for each target.

Running in memory: These core implants work purely in memory to make the detection more difficult for security solutions scanning for potential threats.

Special interest in crypto-communications: Remsec actively searches for information related to a custom network encryption software for secure communications, such as voice, email, and document exchange

Bypassing air-gaps: Sauron uses specially-prepared USB drives to jump across air-gaps, carrying hidden compartments in which stolen data is concealed

Key features:

3. ProjectSauron is a modular platform designed to enable long-term cyber-espionage campaigns.

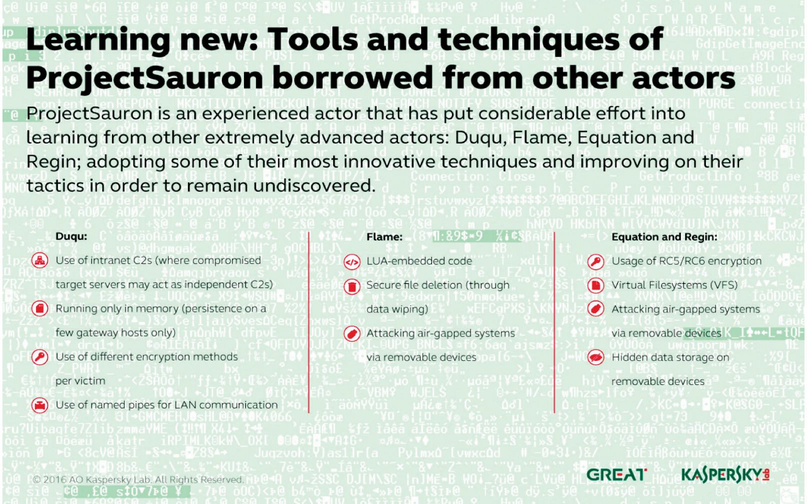
4. All modules and network protocols use strong encryption algorithms such as RC6, RC5, RC4, AES, Salsa20, etc.
5. It uses a modified Lua scripting engine to implement the core platform and its plugins.
6. There are upwards of 50 different plugin types.
7. The actor behind ProjectSauron has a high interest in communication encryption software widely used by targeted governmental organizations. It steals encryption keys, configuration files, and IP addresses of the key infrastructure servers related to the encryption software.
8. It is able to exfiltrate data from air-gapped networks by using specially-prepared USB storage drives where data is stored in an area invisible to the operation system.
9. The platform makes extensive use of the DNS protocol for data exfiltration and real-time status reporting.
10. The APT was operational as early as June 2011 and remained active until April 2016.
11. The initial infection vector used to penetrate victim networks remains unknown.

The attackers utilize legitimate software distribution channels for lateral movement within infected networks.

1.1. CAMPAIGN

ProjectSauron is the name of a top-level modular cyber-espionage platform, designed to enable and manage long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods.

The cost, complexity, persistence and the ultimate goal of the operation (i.e. stealing secret data from state-related organisations) suggest that ProjectSauron is a nation-state sponsored campaign. Technical details indicate that the attackers learned from other highly advanced actors, including Duqu, Flame, Equation and Regin – adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered. All malicious artefacts are customized for each given target, reducing their value as indicators of compromise for any other victim.



Learning new: Tools and techniques of ProjectSauron borrowed from other actors

ProjectSauron is an experienced actor that has put considerable effort into learning from other extremely advanced actors: Duqu, Flame, Equation and Regin; adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered.

Duqu:

- Use of intranet C2s (where compromised target servers may act as independent C2s)
- Running only in memory (persistence on a few gateway hosts only)
- Use of different encryption methods per victim
- Use of named pipes for LAN communication

Flame:

- LUA-embedded code
- Secure file deletion (through data wiping)
- Attacking air-gapped systems via removable devices

Equation and Regin:

- Usage of RC5/RC6 encryption
- Virtual Filesystems (VFS)
- Attacking air-gapped systems via removable devices
- Hidden data storage on removable devices

The name ‘ProjectSauron’ reflects the fact that the code authors refer to ‘Sauron’ in the Lua scripts.

1.2. TARGET OF THE ATTACK AND IMPACT

Usually APT campaigns have a geographical nexus, aimed at extracting information within a specific region or from a given industry. This usually results in several infections in countries within that region, or within a targeted industry around the world. Interestingly, ProjectSauron seems to be dedicated to just a few countries (we have seen attacks in Russia, Iran and Rwanda, although there might be victims elsewhere) and is focused on collecting high value intelligence by compromising almost all key entities that it can possibly reach within the target area.

1.3. PHASE I: RECONAISSANCE

ProjectSauron is highly-focused, stealing confidential data from organisations in Russia, Iran and Rwanda (although there may be other countries too) since June 2011. Not only that, but We have identified more than 30 victims: the target organisations all play a key role in providing state services and come from government, military, scientific research, telecommunications and financial sectors.

1.4. PHASE II: WEAPONIZATION

To-date, the initial infection vector used by ProjectSauron to penetrate victim networks remains unknown.

1.5. PHASE III: DELIVERY

To-date, the initial infection vector used by ProjectSauron to penetrate victim networks remains unknown.

1.6. PHASE IV: EXPLOITATION

ProjectSauron usually registers its persistence module on domain controllers as a Windows LSA (Local Security Authority) password filter. This feature is typically used by system administrators to enforce password policies and validate new passwords to match specific requirements, such as length and complexity. This way, the ProjectSauron passive backdoor module starts every time any network or local user (including an administrator) logs in or changes a password, and promptly harvests the password in plaintext.
In cases where domain controllers lack direct Internet access, the attackers install additional implants on other local servers which have both local network and Internet access and may pass through significant amount of network traffic, i.e. proxy-servers, web-servers,

or software update servers. After that, these intermediary servers are used by ProjectSauron as internal proxy nodes for silent and inconspicuous data exfiltration, blending in with high volumes of legitimate traffic.

Once installed, the main ProjectSauron modules start working as ‘sleeper cells’, displaying no activity of their own and waiting for ‘wake-up’ commands in the incoming network traffic. This method of operation ensures ProjectSauron’s extended persistence on the servers of targeted organizations.

We discovered a few cases where ProjectSauron successfully penetrated air-gapped networks. The ProjectSauron toolkit contains a special module designed to move data from air-gapped networks to Internet-connected systems. To achieve this, removable USB devices are used. Once networked systems are compromised, the attackers wait for a USB drive to be attached to the infected machine.

These USBs are specially formatted to reduce the size of the partition on the USB disk, reserving an amount of hidden data (several hundred megabytes) at the end of the disk for malicious purposes. This reserved space is used to create a new custom-encrypted partition that won’t be recognized by a common OS, such as Windows. The partition has its own semi-file system (or virtual file system, VFS) with two core directories: ‘In’ and ‘Out’.

This method bypasses many DLP products. Software that disables the plugging of unknown USB devices based on device ID wouldn’t prevent an attack or data leakage because a genuine recognized USB drive is used.

To-date, we have not found any zero-day exploits associated with ProjectSauron. However, when penetrating isolated systems, the creation of the encrypted storage area in the USB device does not in itself enable attackers to get control of the air-gapped machines. There has to be another component such as a zero-day exploit placed on the main partition of the USB drive. So far we have not found any zero-day exploit embedded in the body of the malware we have analysed, and we believe it was probably deployed in rare, hard-to-catch instances.

1.7. PHASE V: INSTALLATION

Most of ProjectSauron's core implants are designed to work as backdoors, downloading new modules or running commands from the attacker purely in memory. The only way to capture these modules is by making a full memory dump of the infected systems.

Almost all of ProjectSauron's core implants are unique, have different file names and sizes, and are individually built for each target. Each module's timestamp, both in the file system and in its own headers, is tailored to the environment on which it is installed.

Secondary ProjectSauron modules are designed to perform specific functions like stealing documents, recording keystrokes and stealing encryption keys from both infected computers and attached USB sticks.

ProjectSauron implements a modular architecture using its own virtual file system to store additional modules (plugins) and a modified Lua interpreter to execute internal scripts. There are upwards of 50 different plugin types.

In several cases, ProjectSauron modules were deployed through the modification of scripts used by system administrators to centrally deploy legitimate software updates within the network.

In essence, the attackers injected a command to start the malware by modifying existing software deployment scripts. The injected malware is a tiny module that works as a simple downloader. Once started under a network administrator account, this small downloader connects to a hard-coded internal or external IP address and downloads the bigger ProjectSauron payload from there.

In cases where the ProjectSauron persistence container is stored on disk in EXE file format, it disguises the files with legitimate software file names.

1.8. PHASE VI: COMMAND & CONTROL

For network communication, the ProjectSauron toolkit has extensive abilities, leveraging the stack of the most commonly used protocols: ICMP, UDP, TCP, DNS, SMTP and HTTP.

One of the ProjectSauron plugins is the DNS data exfiltration tool. To avoid generic detection of DNS tunnels at network level, the attackers use it in low-bandwidth mode, which is why it is used solely to exfiltrate target system metadata.

Another interesting feature in the ProjectSauron malware that leverages the DNS protocol is the real-time reporting of the operation progress to a remote server. Once an operational milestone is achieved, ProjectSauron issues a DNS-request to a special subdomain unique to each target.

The ProjectSauron attackers are extremely well-prepared when it comes to operational security. Running an expensive cyber-espionage campaign like ProjectSauron requires vast domain and server infrastructure uniquely assigned to each victim organization and never re-used again. This makes traditional network-based Indicators of Compromise (IOC) almost useless because they won't be re-used in an attack on any other organization.

We collected 28 domains linked to 11 IPs located in the United States and several European countries that might be connected to ProjectSauron campaigns.

IP	ISP
104.131.61.33	Digital Ocean, Inc., US
176.9.242.188	Closco Ltd, Germany
185.78.64.121	MM ONE Group Srl, Italy
192.195.77.59	1&1 Internet Inc., US
216.250.114.149	1&1 Internet Inc., US
217.160.176.157	1&1 Internet AG, Germany
37.252.125.88	Tilaa, The Netherlands
54.209.129.218	Amazon AW, US
66.228.52.133	Linode, US
81.4.108.168	RamNode, The Netherlands
83.125.22.161	AttractSoft GmbH, Germany

Even the diversity of ISPs selected for ProjectSauron operations makes it clear that the attackers did everything possible to avoid creating patterns.

Here is the list of ProjectSauron domains (domains in bold were extracted from malware, the rest were found via Passive DNS and are not validated):

ad-consult.cc	easterncredit.net	**ping.sideways.ru**
art-irisarns.com	**flowershop22.110mb.com**	rapidcomments.com
bikessport.com	gtf.cc	sba-messebau.at
chirotherapie.at	iut.hcmut.edu.vn	utc-wien.at
csrv01.rapidcomments.com	liebstoecklco.at	weingut-haider-malloth.at
dee.hcmut.edu.vn	lydia-leydolf.at	**wildhorses.awardspace.info**
der-wein.at	mail.mbit-web.com	windward-trading.biz
dievinothek.net	mbit-web.com	winnie-andersen.com
display24.at	mycruiseship.net	
dr-rauch.com	**myhomemusic.com**	

1.9. PHASE VII: ACTIONS ON OBJECTIVES

ProjectSauron actively searches for information related to rather uncommon, custom network encryption software. This client-server software is widely adopted by many of the target organizations to secure communications, voice, e-mail and document exchange.

In a number of cases we analysed, ProjectSauron deployed malicious modules inside the custom network encryption's software directory, disguised under similar filenames and accessing the data placed beside its own executable. Some of extracted Lua scripts show that the attackers have a high interest in the software components, keys, configuration files and the location of servers that relay encrypted messages between the nodes.

Also, one of the embedded ProjectSauron configurations contains a special unique identifier for the targeted network encryption software's server within its virtual network. The behaviour of the component that searches for the server IP address is unusual. After getting the IP, the ProjectSauron component tries to communicate with the remote server using its own (ProjectSauron) protocol as if it was yet another C&C server. This suggests that some communication servers running the mentioned network encryption software could also be infected with ProjectSauron.

The fragment of configuration block below, extracted from ProjectSauron, shows the kind of information and file extensions the attackers were looking for:

```
.*account.*|.*acct.*|.*domain.*|.*login.*|.*member.*|.*user.*|.*name|.*emai
l|.*_id|id|uid|mn|mailaddress|.*nick.*|alias|codice|uin|sign-in|strCodUtente|.*pas
s.*|.*pw|pw.*|additional_info|.*secret.*|.*segreto.*

[^\$]$

^.*\.(doc|xls|pdf)$
```

```
*.txt; *.doc; *.docx; *.ppt; *.pptx; *.xls; *.xlsx; *.vsd; *.wab; *.pdf; *.ppk; *.rsa;
*.rar; *.one; *.rtf;~WPL*.tmp; *.FTS; *.rpt; *.conf; *.cfg; *.pk2; *.nct; *.key; *.psw
```

Interestingly, while most of the words and extensions above are in the English language, several of them point to Italian, such as 'codice', 'strCodUtente' and 'segreto'. This suggests that the attackers had prepared to attack Italian-speaking targets as well. However, we are not aware of any Italian victims of ProjectSauron at the moment.

1.10. RECOMMANDATIONS

When talking about long-standing cyber-espionage campaigns, many people wonder why it takes so long to catch them. Perhaps one of the key elements in detecting APTs is having the right tools for the right job. Trying to catch government or military grade malware requires specialized technologies and products.

One such product is the Kaspersky Anti Targeted Attack Platform (KATA). In September 2015, our anti-targeted attack technologies detected a network anomaly in a customer's network. Further investigation led us to a suspicious module – an executable library, loaded in the memory of a Windows domain controller. The library was registered as a Windows password filter and had access to sensitive data in clear text. Further research revealed signs of massive activity from a new threat actor that we codenamed 'ProjectSauron', responsible for large-scale attacks against key governmental entities in several countries.

KATA analyses network traffic (connections to certain hosts, objects in web and e-mail traffic, etc.), processes data and alerts an administrator about potentially suspicious behavior. Such a technological solution is heavily dependent on effective security intelligence – in this case Kaspersky Lab intelligence. Regardless of the sophistication of a threat, there is always an initial infection, lateral movement within the compromised network and data exfiltration. The data produced by these activities is different to normal corporate workflow and can be identified using intelligence-based methods.

1.11. INDICATORS OF COMPROMISE

ProjectSauron's tactics are designed to avoid creating patterns. Implants and infrastructure are customized for each individual target and never re-used – so the standard security approach of publishing and checking for the same basic Indicators of Compromise (IOCs) is of little use.

However, structural code similarities are inevitable, especially for non-compressed and non-encrypted code. This opens up the possibility of recognizing known code in some cases.

That's why, alongside the formal IOCs (see below), we provided relevant YARA rules. While the IOCs have been listed mainly to give examples of what they look like, the YARA rules are likely to be of greater use and could detect real traces of ProjectSauron.

For background: YARA is a tool for uncovering malicious files or patterns of suspicious activity on systems or networks that share similarities. YARA rules—basically search strings—help analysts to find, group, and categorize related malware samples and draw connections between them in order to build malware families and uncover groups of attacks that might otherwise go unnoticed.

We have prepared our YARA rules based on tiny similarities and oddities that stood out in the attackers' techniques. These rules can be used to scan networks and systems for the same patterns of code. If some of these oddities appear during such a scan, there is a chance that the organisations have been hit by the same actor.

C2

185.78.64[.]121
rapidcomments[.]com
81.4.108[.]168
bikessport[.]com
178.211.40[.]117
176.9.242[.]188
www.myhomemusic[.]com
flowershop22[.]110mb[.]com
wildhorses[.]awardspace[.]info
sx4-ws42*.yi[.]org *(mask)*
217.160.176[.]157
asrgd-uz%d.weedns[.]com (*mask)*
we%d.q.tcow[.]eu *(mask)*
5.196.206[.]166

Filenames

Most of the ProjectSauron DLL filenames seem to have been generated automatically by multiplication of several prefixes, roots and suffixes in a random order.

%System%\rpchlpr.exe
%System%\symnet32.dll
%System%\rdiskman.dll
%System%\rseceng.dll
%System%\msprtssp.dll
%System%\ncompc.dll
%System%\rdeskm.dll
%System%\dpsf.dll
%System%\nsecf.dll
%System%\rdesk.dll
%System%\dpsloc.dll
%System%\ddeskm.dll
%System%\rdisksup.dll
%System%\rcompf.dll
%System%\ncompsup.dll
%System%\rdiskf.dll
%System%\iseceng.dll
%System%\msasspc.dll
%System%\wpsloc.dll
%System%\wpackpwf.dll
%System%\rcnfm.dll
%Temp%\kavupdate.exe
%Temp%\kavupd.exe
%Temp%\klnupd.exe
%System%\hptcpprnt.dll
%System%\rdeskf.dll
%System%\ncnfloc.dll
%System%\msaosspc.dll
%System%\ndiskloc.dll
%System%\mperfcl.dll

%System%\polsec.dll
%System%\sxsmgrkbd.dll
%System%\cfgbaseprt.dll
%System%\seccertapi.dll
%System%\krbsec.dll
%System%\prnpapi.dll
%System%\ndisk.dll
%System%\ndisksup.dll
%System%\rdiskloc.dll
%System%\pngmon.dll
%System%\kavsec64.dll
%System%\wlseccomm.dll
%System%\rcnfsys.dll
%System%\wpackshim.dll
%System%\ncnfsys.dll
%System%\sxsapifeed.dll
%System%\wmupdsvc.dll
%System%\dpsf.dll
%System%\compc.dll
%System%\rdiskf.dll
%System%\compman.dll
%System%\cnfsys.dll
%System%\isecf.dll
%System%\klsec.dll
%System%\nagent.exe
%System%\rpsf.dll
%System%\tv_prntx64.dll
%System%\wdesksys.dll
%System%\dsecc.dll
%System%\dcompf.dll
%System%\dsecman.dll
%System%\isecc.dll
%System%\rcompc.dll
%System%\rcnfloc.dll
%System%\rdisk.dll
%System%\dcompman.dll

%System%\npsloc.dll
%System%\nsecc.dll
%System%\wcprts32.dll
%System%\rpsloc.dll
%System%\rsecman.dll
%System%\mstimed.dll
%System%\dcompsup.dll
%System%\compsup.dll
%System%\ncompman.dll
%System%\rsecloc.dll
%System%\rdeskman.dll
%System%\mfc64d.dll
%System%\sceclid.dll
%System%\ddesksys.dll
%System%\isecman.dll
%System%\scsvc32.exe
%System%\polcfg.dll
%System%\cnfloc.dll
%System%\nseci.dll
%System%\eapproxycrypt.dll

In-memory string

EFEB0A9C6ABA4CF5958F41DB6A31929776C643DEDC65CC9B67AB8B0066FF2492

MD5

Pipe backdoor / rpc helper
46a676ab7f179e511e30dd2dc41bd388
9f81f59bc58452127884ce513865ed20
e710f28d59aa529d6792ca6ff0ca1b34

Passive sniffer backdoor
1F7DDB6752461615EBF0D76BDCC6AB1A

227EA8F8281B75C5CD5F10370997D801
2F704CB6C080024624FC3267F9FDF30E
34284B62456995CA0001BC3BA6709A8A
501FE625D15B91899CC9F29FDFC19C40
6296851190E685498955A5B37D277582
6B114168FB117BD870C28C5557F60EFE
7B6FDBD3839642D6AD7786182765D897
7B8A3BF6FD266593DB96EDDAA3FAE6F9
C0DFB68A5DE80B3434B04B38A61DBB61
B6273B3D45F48E9531A65D0F44DFEE13
BB6AEC0CF17839A6BEDFB9DDB05A0A6F
C074710482023CD73DA9F83438C3839F
C3F8F39009C583E2EA0ABE2710316D2A
CF6C049BD7CD9E04CC365B73F3F6098E
40F751F2B22208433A1A363550C73C6B
1D9D7D05AB7C68BDC257AFB1C086FB88

Generic pipe backdoors
181c84e45abf1b03af0322f571848c2d
2e460fd574e4e4cce518f9bc8fc25547
1f6ba85c62d30a69208fe9fb69d601fa

Null session pipes backdoor
F3B9C454B799E2FE6F09B6170C81FF5C
0C12E834187203FBB87D0286DE903DAB
72B03ABB87F25E4D5A5C0E31877A3077
76DB7E3AF9BE2DFAA491EC1142599075
5D41719EB355FDF06277140DA14AF03E
A277F018C2BB7C0051E15A00E214BBF2

Pipe and Internet backdoor
0C4A971E028DC2AE91789E08B424A265
44C2FA487A1C01F7839B4898CC54495E
F01DC49FCE3A2FF22B18457B1BF098F8
F59813AC7E30A1B0630621E865E3538C
CA05D537B46D87EA700860573DD8A093
01AC1CD4064B44CDFA24BF4EB40290E7

1511F3C455128042F1F6DB0C3D13F1AB
57C48B6F6CF410002503A670F1337A4B
EDB9E045B8DC7BB0B549BDF28E55F3B5

Core platform (Lua VFS)
71EB97FF9BF70EA8BB1157D54608F8BB
2F49544325E80437B709C3F10E01CB2D
7261230A43A40BB29227A169C2C8E1BE
FC77B80755F7189DEE1BD74760E62A72
0209541DEAD744715E359B6C6CB069A2
FCA102A0B39E2E3EDDD0FE0A42807417
5373C62D99AFF7135A26B2D38870D277
91BB599CBBA4FB1F72E30C09823E35F7
914C669DBAAA27041A0BE44F88D9A6BD
C58A90ACCC1200A7F1E98F7F7AA1B1AE
63780A1690B922045625EAD794696482
8D02E1EB86B7D1280446628F039C1964
6CA97B89AF29D7EFF94A3A60FA7EFE0A
93C9C50AC339219EE442EC53D31C11A2
F7434B5C52426041CC87AA7045F04EC7
F936B1C068749FE37ED4A92C9B4CFAB6
2054D07AE841FCFF6158C7CCF5F14BF2

1.12. FURTHER INFORMATION

Further information, including a full technical analysis of ProjectSauron, is available on the securelist.com web site.

Lutech

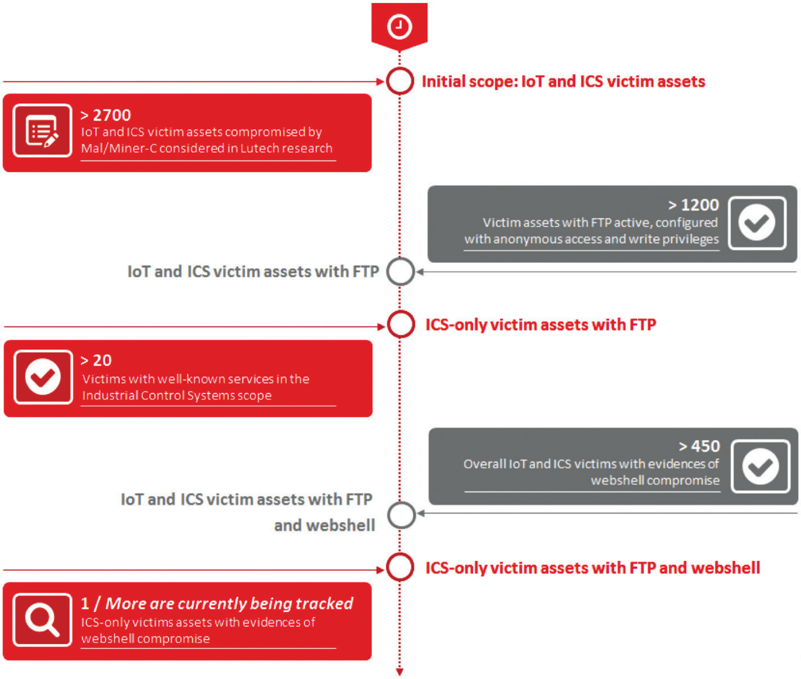
2. Case Study

The Advanced Persistent Threat case study hereby presented is based on information provided by Lutech Threat Management Service for Cyber Threat Intelligence (L-TMS/CTI).
Lutech TMS/CTI is an end-to-end service dedicated to scouting cyberspace (open, closed, private and controlled areas, in Internet, Deep Internet and Darknets), including correlation, contextualization, monitoring, analysis, validation and proactive alerting about cyber threats like hactivism, apt, employee attack, phishing / pharming and malware "in the wild", data breach and leakage, unkown exposed / rogue / vulnerable asset – mobile apps included, ID and PII theft, financial credential and CC theft, domain abuse, resource abuse – such as botnet, spam e command-and-controls. Cyber threats may be both active – though unknown – or being prepared or even completely inactive. Targets of such threats are so called cyber assets, i.e. not only traditional ICT services and systems or data, but also people and intangible assets such as brand.
The starting point of the study performed by the Cyber Threat Intelligence team of L-TMS/CTI is a paper by Sophos: "Cryptomining.......... malware on NAS servers" by Attila Marosi, Senior Threat Researcher, SophosLabs[2]. Based on the analysis of FTP server compromised for cryptomining purposes described in the paper above, Lutech Cyber

[2] https://nakedsecurity.sophos.com/2016/09/08/cryptomining-malware-on-nas-servers-is-one-of-them-yours/

Threat Intelligence team has performed both a drill-down on ICS and IoT victim assets and an assessment of other forms of compromise, trying eventually to track down the threat actors. Campaign evolution and changes are still under monitoring. The chosen name for the campaign is “Winter Is Coming”.

Here follows a timeline diagram of the research performed by Lutech Cyber Threat Intelligence team about the “Winter Is Coming” campaign:



Initial scope: IoT and ICS victim assets
> 2700
IoT and ICS victim assets compromised by Mal/Miner-C considered in Lutech research
> 1200
Victim assets with FTP active, configured with anonymous access and write privileges
IoT and ICS victim assets with FTP
ICS-only victim assets with FTP
> 20
Victims with well-known services in the Industrial Control Systems scope
> 450
Overall IoT and ICS victims with evidences of webshell compromise
IoT and ICS victim assets with FTP and webshell
ICS-only victim assets with FTP and webshell
1 / More are currently being tracked
ICS-only victims assets with evidences of webshell compromise

Lutech Cyber Threat Intelligence team started its research by considering 2753 assets victim of the Mal/Miner-C malware analyzed in Sophos paper (see [1]), which can be related to IoT and Industrial Control Systems (ICS) technologies.

1086 of these assets have been detected providing anonymous FTP access, with write access available, even to the Web Server root directory.
Among the 1086, 16 are strictly related to ICS-only technologies, meanwhile on 463 of them evidences of webshell compromise have been detected.
Current research of Lutech Cyber Threat Intelligence team is addressed at tracking the broadening of the webshell diffusion to ICS targets too: 1 victim in this scope has been identified, but more compromissions could happen eventually.

2.1. CAMPAIGN

Lutech Cyber Threat Intelligence team conclusion about attribution of the threat is that there is not enough information to determine if it’s addressed against specific organizations.
Nevertheless, several conclusions can be drawn:

- Mal/Miner-C remained undetected for quite some time and it’s still largely diffused, being deployed on a few thousands assets with no intention to bring them down and in general with the only goal of staying quiet and keep mining.
- The same actor behind Mal/Miner-C, well aware of the features, misconfigurations and vulnerabilities of the compromised asset he can leverage on, is eventually probing other ways of abuse of this leverage. A possible reason is the actor perceiving the risk of a fall in revenues provided by its current campaign and eventually trying to exploit to revenue streams
- Assuming for a while this is the case, the actor behind Mal/Miner-C is deploying web shells to the same assets, trying to stay unnoticed or just avoid making noise until the moment of changing attack plans come: i.e. the moment when the income generated by crypto mining will fall and he will need to switch to new revenue streams. Consider that due to their simplicity and acting like any other Web page, shells can be very stealthy on a server and be very difficult to detect.

- In that moment remote and webshell access to the victims can be suddenly monetized to ask ransoms, to resell access to the targets, etc.
- Last but not least, even though the actor behind Mal/Miner-C is not the one we should be concerned of, two facts must be considered:
  - The vulnerable and/or misconfigured assets compromised by Mal/Miner-C stay there.

Opportunity for someone to exploit them is real, since a chance to make profit is clear.

2.2. TARGET OF THE ATTACK AND IMPACT

“Winter Is Coming” campaign has no impacts yet that can be considered significant.
This missing piece in the jigsaw is eventually reinforcing the conclusions drawn in the previous section: the campaign is probably in the preparation stage and it’s not yet the right time to act, for instance asking for a ransom or disrupting target assets and related services.
Considerations above apart, these are some examples out of the most significant services provided by a sample of the victims:

- Some targets can be related to SmartHeat Deutschland, a company of the SmartHeat group, a manufacturer of heat pumps, covering heat requirements in the living area, in business or in the industry.
- Some can be related to WEB’logs monitors, cost-effective mini data logger for monitoring on private PV systems, manufactured by Meteocontrol GmbH.
- Others can be related to TwinCAT 2/3 PC-based control software by Beckhoff Automation GmbH & Co. KG, used from Print-, Wood Working-, Plastic- or Window Construction Machines, to Wind Turbines and Test Benches up to buildings like Theatres or Sport Arena.

Finally, some of them expose BACnet services. BACnet is communication protocol designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment.

2.3. PHASE I: RECONAISSANCE

2.3.1. Reconaissance

Reconnaissance is the Cyber Kill Chain phase where research, identification and selection of targets are performed, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.
“Winter Is Coming” reconnaissance activities are performed starting from assets already victim of Mal/Miner-C campaign, hence leveraging on reconnaissance patterns used by this malware to identify assets where it can deploy its new instances. This tactic is very effective and efficient, though functionally equivalent to looking for FTP servers, with anonymous access, factory-default authentication parameters or even well-know credentials (eventually available in wordlists populated with data coming from mega-leaks such as Linkedin, Yahoo, etc.), providing write access to the web server root directory.

2.3.2. Indicators (STIX)

In this section the indicators of compromise useful for detecting this kind of activity are provided.
A target victim is an asset providing HTTP and FTP, with files info.zip or Photo.scr listed in one or more levels in the directory or referenced in an iFrame of the homepage. Eventually, the presence of woooooooot.php file is another indicator for the threat actor to look for.

More precise recon activities also look for HTTP server able to execute PHP applications, possibly with PHP versions that can serve specific PHP webshells (see Weaponization).

2.3.3. Recommandations (Course of Action)

Blocking reconnaissance activities filtering out packets containing indicators described above could be a simple and effective strategy. Eventually this can bring to minor service disruption in case the info.zip files are legitimately served via FPT/HTTP. Blocking enquiries about PHP stack presence and its version number raise the cost of starting with the attack.

2.4. PHASE II: WEAPONIZATION

2.4.1. Weaponization

Weaponization is the Cyber Kill Chain phase where happens the coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer).
“Winter Is Coming” weapons are PHP webshells. A webshell or backdoor shell is a malicious piece of code (e.g. PHP, Python, Ruby) that can be uploaded to a site to gain access to files stored on that site. Once it is uploaded, the attacker can use it to edit, delete, or download any files on the site, or upload their own. Shells have many uses. They can be used to edit the webserver directory index page of site, and then attackers can leave their mark or “deface” for visitors to the site to see when they go to the homepage. Attackers may also use it to gain root access to the site and have full control of it.

2.4.2. Indicators (STIX)

A comprehensive list of PHP webshells can be found on https://github.com/JohnTroony/php-webshells and https://devnulls.blogspot.it/2015/09/php-web-shell-list.html.

Indicators can be defined by reverse engineering of the available shells, eventually focusing on c99.php, c100.php, r57.php, locus7shell which seem being used in “Winter Is Coming” campaign.

2.4.3. Recommendations (Course of Action)

To prevent a site from having a shell uploaded onto it, a webmaster must always keep up with the latest security updates and make sure to have a secure admin panel. They must also make sure that if they do have an admin panel they make sure it only permits the user to upload .jpeg, .png, and other image file types only.

2.5. PHASE III: DELIVERY

2.5.1. Delivery

Delivery is the Cyber Kill Chain phase where Transmission of the weapon to the targeted environment happens. The adversaries convey the malware to the target. They have launched their operation.
“Winter Is Coming” delivery mechanism is by logging in to FTP services with anonymous access or embedded credentials (anonymous, root, admin, etc.) with default and frequently used weak passwords.

2.5.2. Indicators (STIX)

A target victim presents FTP service access logs from remote IP addresses, probably characterized by a negative IP reputation scoring. IP reputation score is a metric telling whether an IP addresses is involved in any nefarious activity – mainly, though not exclusively - in spamming activities, in malware and spyware incidents, in a distributed denial of service attack, or if it’s a command and control server or just associated with a botnet.

2.5.3. Recommendations (Course of Action)

To prevent the delivery, a policy denying remote root or admin to the FTP server should be enforced on the perimeter. Anonymous access should be allowed only from selected trusted parties, not the whole Internet. IP reputation score of the enquiring IP addresses should be considered to filter out sources of traffic already marked as bad by the Internet community.

2.6. PHASE IV: EXPLOITATION

2.6.1. Exploitation

After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

"Winter Is Coming" exploitation happens leveraging FTP service built-in feature called anonymous access.

Anonymous FTP is a means by which archive sites allow general access to their archives of information: these sites create a special account called "anonymous". User "anonymous" has – in general - limited access rights to the archive host, as well as some operating restrictions: in fact, the only operations allowed are logging in using FTP, listing the contents of a limited set of directories, and retrieving files; some sites limit the contents of a directory listing an anonymous user can see as well; note that "anonymous" users are not usually allowed to transfer files to the archive site, but can only retrieve files from such a site.

In the case of asset victim of "Winter Is Coming" the restrictions and access rights have been poorly configured: write access even to critical directories such as the Web server root is allowed.

Another exploitation mechanism is accessing the FTP service with embedded credentials related to privileged users (i.e. root, admin, etc.), with the benefit of default or frequently used weak passwords, easily available from online manuals, device or systems support sites, wordlists exchanged in pastebin-like sites or in the cybercrime underground. When access is performed as a privileged user, unlimited write access is fully allowed.

2.6.2. Indicators (STIX)

A target victim has FTP service access logs with evidence of authentication activity with anonymous access or privileged accounts with default credentials or well-known passwords.

2.6.3. Recommandations (Course of Action)

To prevent the exploitation, a policy denying remote root or admin to the FTP server should be enforced on the perimeter. Anonymous access should be allowed only from selected trusted parties, not the whole Internet, furthermore preventing from uploading (i.e. writing) content to the site.

2.7. PHASE V: INSTALLATION

2.7.1. Installation

Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
“Winter Is Coming” installation operations happen browsing via FTP service to the web server root directory and - exploiting write access - uploading there a copy of the selected webshell, compatible with the target PHP platform version (see Reconnaissance). When the shell is installed, it will have the same permissions and abilities as the user who put it on the server.

2.7.2. Indicators (STIX)

A target victim has FTP service access logs with evidence of FTP browsing to the web root directory (i.e. multiple CD commands) and upload commands (i.e. a combination of PUT, MPUT and).

Furthermore, filename indicators can be identified starting from the comprehensive list of PHP webshells found on https://github.com/JohnTroony/php-webshells and https://devnulls.blogspot.it/2015/09/php-web-shell-list.html.
Filename indicators can be defined by reverse engineering of the available shells, eventually focusing on c99.php, c100.php, r57.php, locus7shell which seem being used in "Winter Is Coming" campaign.

2.7.3. Recommendations

To prevent the installation, upload (i.e. write) privileges should be carefully configured and definitely disallowed for anonymous access. Eventually agent or agentless Host IDS software can be deployed onto the asset, checking for FTP upload commands including filenames indicators related to well-known webshells as parameters: in this case the Host IDS software should also switch into prevention mode, disrupting the upload command and making it unsuccessful.
Some of the other things that can indicate the presence of a shell are files that seem out of place or have an unusual timestamp. While some attackers are extremely careful with their file names and timestamps, others do get careless.
A system administrator can also periodically do a search of all files in the web root hierarchy looking for the functions that a shell depends on, such as the eval(), passthru(), exec() and system() if running PHP or the equivalent in the supported languages.
In any case, once the shell is detected, simply delete the file from the server.

2.8. PHASE VI: COMMAND & CONTROL

2.8.1. Command & Control

Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on

the keyboard” access inside the target environment.
In the case of webshells, used in the “Winter Is Coming” campaign, some are self-sufficient and contain all needed functionality while others require external actions or a “Command and Control” (C&C) client for interaction.
One of the PHP webshells seen in “Winter Is Coming” is the c99 shell. It is approximately 1,500 lines long and some of its features include displaying security measures the server may have in place, a file viewer that includes the files’ permissions, an area where the user can run custom PHP code on the server, and the contents of phpinfo(). Phpinfo() is a core PHP function that creates a Web page and outputs valuable information about the OS, Web server and PHP configurations. It also has the ability to search the server for configuration files, password files and other writeable files and directories. It also has tools built in to encode/decode strings from various formats as well as a brute-force password cracker. It has a GUI to directly connect to a database server and if the attacker is concerned about detection, it has a function to self-delete the shell.
We have also seen a hybrid between the simple shell and the full-featured shell. Some shells have a type of command and control (C&C) structure. The attacker has their own local interface where they can simply type in the URL of a compromised machine and insert code similar to the simple shell. The benefit here is the footprint on the infected server is extremely small and doesn’t include code that is being picked up by anti-virus scanners.

2.8.2. Indicators (STIX)

Perimeter defense mechanisms or server access logs should present evidence of connection from remote IP addresses, probably characterized by a negative IP reputation scoring. IP reputation score is a metric telling whether an IP addresses is involved in any nefarious activity – mainly, though not exclusively - in spamming activities, in malware and spyware incidents, in a distributed denial of service attack, or if it’s a command and control server or just associated with a botnet.

2.8.3. Recommendations

To prevent the connection with the Command & Control, IP reputation score of the commanding IP address should be considered to filter out sources of traffic already marked as bad by the Internet community.
In case the shell is self-sufficient, mitigations fall back onto others presented here.

2.9. PHASE VII: ACTIONS ON OBJECTIVES

2.9.1. Actions on Objectives

Action phase in the Cyber Kill Chain is when, after progressing through the first six phases, intruders can take actions to achieve their original objectives. Typically, this objective is data exfiltration, which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point.
"Winter Is Coming" campaign show no evidence of actions yet. Nevertheless, a statement can be made that the campaign is probably in the preparation stage and it can eventually switch to action, for instance asking for a ransom or disrupting target assets and related services. Operationally, the webshells can be activated for one of these two primary purposes.

2.9.2. Indicators (STIX)

Indicators of activity can be identified in commands issued to the shell, provoking an impact on the target asset. Such commands can be reverse engineered starting from the comprehensive list of PHP webshells found on https://github.com/JohnTroony/php-webshells and https://devnulls.blogspot.it/2015/09/php-web-shell-list.html.
More easily, the PHP passthru function, or the similarly functioning

eval(), exec() and system() are functions that will take a string and send the string to the underlying system for processing: these are usually signs of a webshell in action.

Logs can also indicate there is a shell on a server and in use: watch for unusual requests to files when the requests do not correlate or don't make sense by protocol. A PDF or JPG file being called with GET parameters could be an indication the file extension is not accurate and that it is actually a webshell.

2.9.3. Recommendations

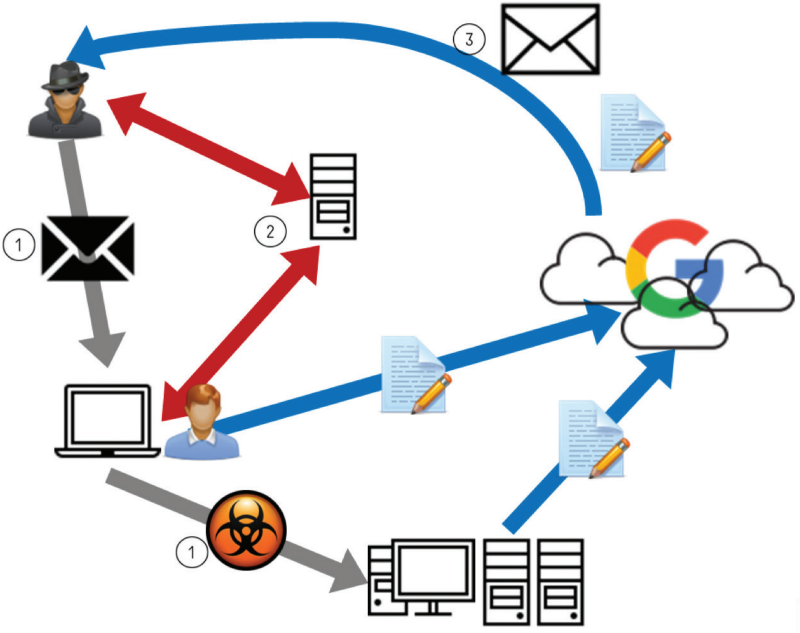
If the server is running PHP and doesn't have a demonstrated need for the passthru, eval, exec or system functions, it would be wise to disable these, making it difficult for these shells to operate.

Agent or agentless Host IDS software can be deployed onto the asset, checking for commands issued to the shell, intercepting and blocking them before they're passed onto the underlying operating system.

Trend Micro

3. Case Study

The PLEAD APT has been observed to target Taiwan for a few years now, which was observed to have started in 2012. It has been known to target companies from Heavy, Technology, Government, and Computer industries. The PLEAD APT has been known to use spear-phishing technique in order to infiltrate target organizations. These spear-phishing emails have improved over time and have made use of different methods in tandem with social engineering. At its core is the main backdoor, which, although vary in their installation methods, have a distinct behavior which may also be used as indicator to help detect their presence. Communication between backdoor and C&C does have distinct pattern in them, although some differences are noticeable across samples over time. Another tool being used by PLEAD APT is a pure information stealing tool with the main purpose of stealing documents. Exfiltration of stolen documents by this tool makes use of a popular cloud service, making its upload traffic look like a regular upload. This campaign is still active to this day and is still being monitored.



1. Exploit targets with spear phishing email and install malware in target network;
2. Command and Control;
3. Exfiltrate documents and information by Google drive and SMTP.

3.1. CAMPAIGN

PLEAD campaign is a targeted attack focusing on Taiwan. The name PLEAD is mainly based on the letters in the backdoor commands of the main backdoor tool of the campaign. This campaign has been ongoing since 2012.They target several industries including government, technology and heavy until today. There are multiple tricks employed in the operation and the tools make use of various installation methods but will typically have identical functionalities.

3.2. TARGET OF THE ATTACK AND IMPACT

PLEAD campaign's main objective is information theft, with primary interest in document file types containing sensitive information. The campaign's primary targets are organizations that belong to government as well as administrative agencies. As espionage operation against its victims, the impact could be critical due to the confidential data were stolen.

3.3. PHASE I: RECONAISSANCE

3.3.1. Reconnaissance

It is currently unknown how PLEAD's reconnaissance stage is conducted. However, seeing the spear-phishing email they have delivered to targets. We can tell that they know their targets in the following perspective: duty and responsibility, on-going project status.

3.3.2. Indicators (STIX)

Not Available.

3.3.3. Recommendations

Not Available.

3.4. PHASE II: WEAPONIZATION

3.4.1. Weaponization

The PLEAD utilize different loading tactics to load the malware. Usually multiple layer encryption are involved, and in some cases the functional malware is resident in memory only.

Here are some different ways we have observed in the wild.

A. Encrypted payload in PE resource section

The malware is embedded into the resource of other executable file. The resource name is usually popular file extension, such as AVI, BMP and so on. The content of resource is binary blob, which includes shellcode, malware binary and encryption key. Once loaded, the blob first decrypted by RC4, and then shellcode would take care of loading and active the malware.

B. 3-Layers Encryption

The malware is encoded into hexadecimal data, and acts as part of the source code of another executable file. The loader would first reconstruct the hexadecimal data into correct order in stack, and then decrypts it into encryption key. Again RC4 is used to perform second decryption to get shellcode. The shellcode would do the third layer decryption and active the malware

C. Separate Malware

The malware is encrypted into a standalone file, another loader executable would load, decrypt and launch the malware

D. Hacking Team Exploit CVE-2015-5119

PLEAD threat actors were also able to get a hold of one of Hacking Team's leaked exploits, CVE-2015-5119 and created a version of PLEAD that will be directly injected into memory, following the successful exploitation using the specially-crafted .docx file.

E. Other exploits

Except CVE-2015-5119, the threat actor also utilizes CVE-2012-0158 and CVE-2014-6352 to compromise the victim.

3.4.2. Indicators (STIX)

Type	File Hash
Encrypted payload in PE resource section	a672b8efe4604237268d7d9f3ddb167e9993b3f2 15cd664fe6241a6183b27ee72d754ad1a63c84ad 2ea45d789da38e063ae077b11608274aa3cd5d50 5ffcfe0c880e1cf9382cb9c7960f09ba73e1dffc 801d2d405a94f45bafcd0fe91d7428a2d9e4fed6 807a0cf2718894db6fc5db0bb1327e8ff64e70a6 8744e49f4d774e96b90caa84ef03f3bb47fffd47 9d5a919bfd43d07667a63faf63e6728a3ec565e9 b26232619bb78b29ae984d925ff747e59e7ed642 b8e13908d04c9e538254595ea5889ba287da04e6 bc3509ee4f56f38060d49498246e1a178477da02 d1289aa419f16a382af06aaf1c81fbf18f712483 e45e927f01e0800dde31c2735da53909a5ff0804
3-Layers Encryption	018efed8fa801fc73ac2fa69875df2df680794be 35dc42e01e14da4d79f439da3a801e2055581cb1 3caa693e55acedc4455b72a7045fffa4a5026526 4b4f4e76af249c753ac805e175f5d477cd0bda42 580200422617365420a4da8d2b2de1ef2b41d7c1 58ffb0c45970f5f74eaad42c0b80f533e95158f1 6633de73d0345001a6a47fb585a70a266792cc72 66359ace48822064f089eee33e0cd761bf8dfe62 79481abe404194119aea584d7709f17e631b4bc3 8f1b3cef05bb59ea466eee55296990ca38f24274 b016d27a0823bda1fdcf297b8f6b280c36f176ef e52caa2020f320e6e277dcdd39bdcd6737b9fa7c e9b83fedaa98d0228683eebba1ca72270cb4b2f2 f3e6408e6c1dc69b9c46dbb9e9284fe3b30ff914
Separate Malware	b5c6fcd164fddbddb37d701fd3335c79f2e8a999
Hacking Team Exploit CVE-2015-5119	ec4cf4d1aa43124247da89618b3fb0be6c9de7c5 3c6e539e0d557bd8e504a3806e50246e88802bd4
CVE-2012-0158	6ade72b0e7407eebd681da39501be181f94a8a5d c4c512c0ba4bb99617b9b1b4420f38cc7b809034
CVE-2014-6352	8379ff4be2ab8f09ba3c357a4683e05f5076e265

3.4.3. Recommendations

Threat actors have adopted multiple methods which are discussed previous to make their tools as stealthy as possible. They compiled those tactics into a piece of malware. Please refer to the recommendation of Exploitation section for comprehensive discussion.

3.5. PHASE III: DELIVERY

3.5.1. Delivery

PLEAD's main method of delivery is by using phishing emails directed towards their target. There are currently two known method of email delivery used by PLEAD.

A. E-mail Attachments
PLEAD is delivered through phishing email as an attachment. The RTLO method is used to attract the target into executing the attachment. In some cases they also send document with exploitation to the victim, but the number is relative less compare to RTLO.

B. E-mail with Link
PLEAD will still utilize phishing emails to deliver their payload. However, instead of an attachment, they will include a download link (using Google drive link) and use social engineering to lure targets into downloading the malicious payload from the link. This method of delivery has been seen from more recent PLEAD attacks.

3.5.2. Indicators (STIX)

Type	File Hash
E-mail containing attachments	8379ff4be2ab8f09ba3c357a4683e05f5076e265 cec9fff426d3d334bf49d25e7792fcce62f613a3 b50909eba0e24b2604ef11a05d3c8f869b45c414 cc82b8649db3edfd1e6ac592adcad69e906cb549 b0801d7333867e4842c41e0e9230ebd8e20d28ab a1df1e7ccddadfc947295b13bb19231266be316d
E-mail with gdrive link	cd22ce02420845b3b9b0ec4432fe4157b1270e96 f93d9eb5936b5126bc05af5dafc80c107105fe78

3.5.3. Recommendations

Not like Cybercriminal SPAM, APT spear-phishing E-mail looks nothing different to the other E-mail sent by normal users. The traditional detection rules may not able to detect APT delivery easily. Here we recommend applying dynamic solution on organization's mail servers. Especially some security solution featured with sandbox processing.

3.6. PHASE IV: EXPLOITATION

3.6.1. Exploitation

A. Right-To-Left-Orientation

PLEAD uses RTLO in order to disguise its file extension as a document file. This is paired with a suitable icon related to its fake extension, as well as using suitable file names to lure targets into clicking them. In some of the phishing emails used to deliver PLEAD backdoors, decoy documents are also included to increase "legitimacy", while in later emails, and they no longer attach the backdoor but instead let the target download them from legitimate cloud storage providers (google drive).

In one situation, the downloaded file is a valid PNG image. However, appended below is a block of encrypted binary. It is decrypted using RC4, and the output is an executable file that will inject codes to a legitimate process.

B. Use of exploits

PLEAD has mainly been seen making use of RTLO trick but there have been several incidents were PLEAD did use actual vulnerabilities in their attacks. One of these is CVE-2012-0158, which has already been patched log ago but is quite a popular choice for exploitation. Another vulnerability used is CVE-2014-6352, it's for Power Point documents which they also used to deliver PLEAD.

C. “Fileless” PLEAD

PLEAD also made use of one of Hacking Team’s leaked exploits, CVE-2015-5119, and made a “file-less” infection version of PLEAD. This version makes use of a specially-crafted .docx file which will trigger the exploit. Once the exploit is triggered, an instance of iexplore.exe process will be launched, where the PLEAD backdoor will be directly injected and executed in iexplore’s memory space, without creating an actual physical copy of the file to disk.

3.6.2. Indicators (STIX)

For the exploits indicators, please refer to the Weaponization section of Indicators.

Type	File Hash
RTLO PLEAD	6448cd86c7954ebc52fad629d026075e7b5426f8 aa5d613f95d0fbaf5fbd192c2445f068012705db 0fb1081ee56b7db5e70e8027400e1d38ffffee69 49c3c256f304bc15767791f56ba3ac146de8d7c2 02674d058c66ff1941ff3ff39ff50bbd32e8e99c cc97b05e1f5645a76cabb3cbd1cd4f5cdf84b7b4 3caa693e55acedc4455b72a7045fffa4a5026526 d1289aa419f16a382af06aaf1c81fbf18f712483 5ffcfe0c880e1cf9382cb9c7960f09ba73e1dffc

3.6.3. Recommendations

Parent-child process relationship – PLEAD’s specially-crafted document file will be launched by a normal process (WORD.exe, EXCEL.exe, etc.), as are all document files. These document-related processes launching iexplore.exe or other processes should be seen as a possible indicator of compromise, most likely something related to exploitation.

Exploit patches – Patching known vulnerabilities is always a good protection from specific vulnerabilities. Applying patches on time is also advised as to acquire the protection as soon as possible.

Exploit Hardening Applications – Exploit hardening applications can help defend against vulnerability exploitation. Having such application is a good way of increasing security especially systems that are more exposed to such threats.

True file type indicator – As the more common method used by PLEAD, RTLO is not really a software exploit but rather a trick to exploit the user's trust in seeing the "file extension" of the malware and "trusting" that it is a document file. A true file type identifier can help users know that what they are trying to execute is actually an executable file and not a document file that it pretends to be.

3.7. PHASE V: INSTALLATION

3.7.1. Installation

PLEAD and DRIGO backdoors primarily makes use of the run registry for their autostart mechanism. After launching successfully, they tried to copy itself to specific location, mostly under %appdata%, and create a new registry pretend to be certain normal applications.

Sometimes PLEAD also installs itself as a service, in such case it likes to pretend to be WMI (Windows Management Instrumentation) related service.

3.7.2. Indicators (STIX)

Create RunKey in registry

SHA1	02674d058c66ff1941ff3ff39ff50bbd32e8e99c
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\NVIDIA Corporation
Data	%APPDATA%\Microsoft\Protect\nvidia.exe

SHA1	07f27380978b75ec7990ee3b134ecc0221e4f8ee
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Intel Corporation
Data	%APPDATA%\Microsoft\Windows\Themes\Intel.exe

SHA1	519c09cfc4314f2d92f7f8879f97ccacb06114b2
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Adobe Update
Data	%APPDATA%\Microsoft\Windows\AdobeARM.exe

SHA1	5ffcfe0c880e1cf9382cb9c7960f09ba73e1dffc
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\NVIDIA Corporation
Data	%APPDATA%\Microsoft\Protect\ime.exe

SHA1	801d2d405a94f45bafcd0fe91d7428a2d9e4fed6
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\NVIDIA GeForce Service
Data	%APPDATA%\Identities\nvidia.exe

SHA1	8744e49f4d774e96b90caa84ef03f3bb47fffd47
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Power Manager
Data	%APPDATA%\Microsoft\Protect\powercfg.exe

SHA1	e45e927f01e0800dde31c2735da53909a5ff0804
Key	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Power Manager
Data	%APPDATA%\Identities\powercfg.exe

SHA1	15cd664fe6241a6183b27ee72d754ad1a63c84ad
Path	%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\onenote.exe

Create Auto-Start File

SHA1	2ea45d789da38e063ae077b11608274aa3cd5d50 807a0cf2718894db6fc5db0bb1327e8ff64e70a6 9d5a919bfd43d07667a63faf63e6728a3ec565e9 b26232619bb78b29ae984d925ff747e59e7ed642 bc3509ee4f56f38060d49498246e1a178477da02
Path	%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\sched.exe

SHA1	b8e13908d04c9e538254595ea5889ba287da04e6
Path	%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\search.exe

SHA1	d1289aa419f16a382af06aaf1c81fbf18f712483
Path	%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\lsm.exe

Service

SHA1	88ef7d51484924e9f28df9eff52c07cf3356e3e3
Service	WmicSvc
DisplayName	Windows Management Instrumentation Helper
Service DLL	C:\Program Files\Internet Explorer\wmic.dll

SHA1	545a9f65623846813f01489c3c3772317c7b4de7 b8d20f94bd1c6226f76f3b353372053017adbdf9
Service	WmiSvc
DisplayName	Windows Management Instrumentation Helper
Service DLL	C:\Program Files\Internet Explorer\wmic.dll

SHA1	b2aa41bf79bd2cf5d1c68d4552a9ead4a21ba0be
Service	WmiSvc
DisplayName	Windows Management Instrumentation Helper
Service DLL	C:\WINDOWS\system32\wmic.dll

SHA1	d71447bf6240245bf8463b97c446aa83c3418efa
Service	WmiSvc
DisplayName	Windows Management Instrumentation Helper
Service DLL	C:\Documents and Settings\Administrator\Application Data\wmic.dll

Type	
Common Filenames	applicatios.exe, applications.exe, nvidia.exe, IMSCMIG.exe, wuaclt.exe, wuaclts.exe, wuaclt32.exe, intel.exe, imea.exe, jucheck.exe, juched.exe, ctfmon.exe, imemg.exe, adobereader.exe, sched.exe, lsm.exe, search.exe, onenote.exe, powercfg.exe, ime.exe, wmic.dll
Common Regrun names	NVIDIA Corporation, Microsoft IME Migration, ctfmon, Adobe Corporation, MSUPD32, hkcmds, AVIREIST, inetingo, Power Manager
Common service names	WmiSvc, WmicSvc

3.7.3. Recommendations

Create a run key in registry or register a service on target compromised host is not a new technique nowadays. Autoruns is a sysinternals utility which provides comprehensive knowledge of auto-starting locations of any startup entry. Especially the entries marked in pink do not contain publisher information or the digital signature either doesn't exist or doesn't match.

3.8. PHASE VI: COMMAND & CONTROL

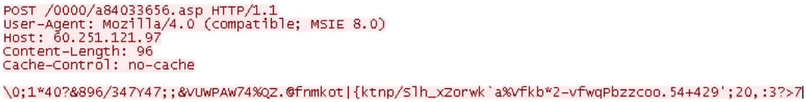
3.8.1. Command & Control

A. PLEAD

A remote access control tool provides the following functionality: sleep, listdir, upload, delete and exec with corresponding command: C, A, L, E, P, G, D.

The C&C protocol of PLEAD can be easily described as below,

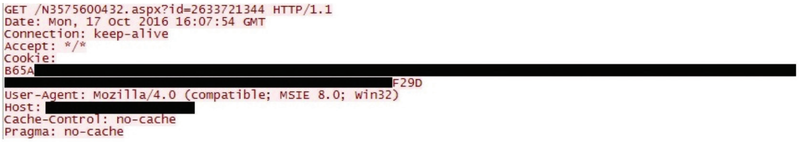
(GET|POST)\s\/\d{4}\/\w\d+\.(js|asp|jpg|css)\sHTTP/\d\.\d
d{4}: beacon sequence
And the content of network packet is encoded by XOR.
C&C Traffic Example,



```
POST /0000/a84033656.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: 60.251.121.97
Content-Length: 96
Cache-Control: no-cache

\0;1*40?&896/347Y47;;&VUWPAW74%QZ.@fnmkot|{ktnp/Slh_xZorwk`a%Vfkb*2-vfwqPbzzcoo.54+429';20,:3?>7
```

Here is another PLEAD protocol. The request template is "/N%u.aspx?id=%u", two "%u" are random number



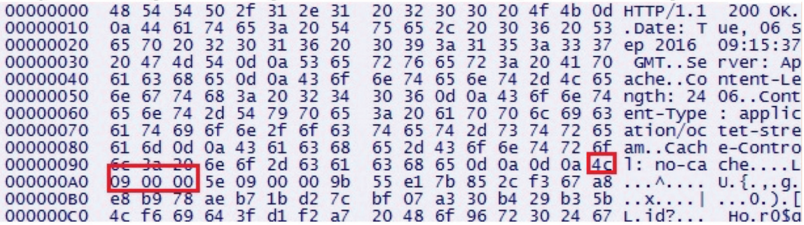
```
GET /N3575600432.aspx?id=2633721344 HTTP/1.1
Date: Mon, 17 Oct 2016 16:07:54 GMT
Connection: keep-alive
Accept: */*
Cookie:
B65A[redacted]F29D
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: [redacted]
Cache-Control: no-cache
Pragma: no-cache
```

Some PLEAD samples do not have backdoor routines. Instead, they would download extra backdoor routines when they connect to C&C server. In such way they could adopt the new backdoor capability easily without re-deploy backdoor. The PLEAD backdoor capability of PLEAD could be calssified into following functions roughly:

- Machine or network information gathering;
- Process and file manipulation;
- Shell;
- Password stealing.

The downloading attemption could be summerized into three steps:

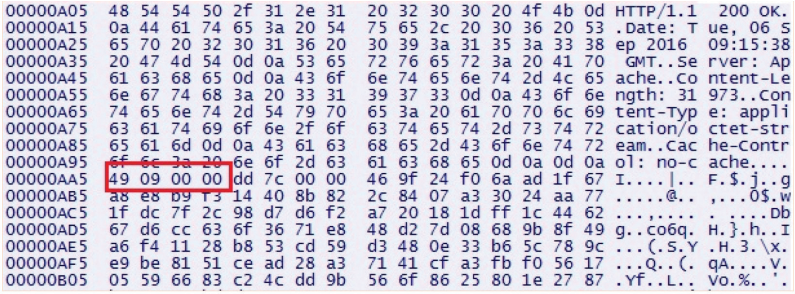
1 Initial response: the first response from C&C site
The HTTP response start with "4c 09 00 00", following with a 4-bytes unsigned integer which indicates (content length – 8)



```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d HTTP/1.1  200 OK.
00000010  0a 44 61 74 65 3a 20 54  75 65 2c 20 30 36 20 53 .Date: T ue, 06 S
00000020  65 70 20 32 30 31 36 20  30 39 3a 31 35 3a 33 37 ep 2016  09:15:37
00000030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70  GMT..Se rver: Ap
00000040  61 63 68 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65 ache..Co ntent-Le
00000050  6e 67 74 68 3a 20 32 34  30 36 0d 0a 43 6f 6e 74 ngth: 24 06..Cont
00000060  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63 ent-Type : applic
00000070  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65 ation/oc tet-stre
00000080  61 6d 0d 0a 43 61 63 68  65 2d 43 6f 6e 74 72 6f am..Cach e-Contro
00000090  6c 3a 20 6e 6f 2d 63 61  63 68 65 0d 0a 0d 0a 4c l: no-ca che....L
000000A0  09 00 00 5e 09 00 00 9b  55 e1 7b 85 2c f3 67 a8 ...^.... U.{.,.g.
000000B0  e8 b9 78 ae b7 1b d2 7c  bf 07 a3 30 b4 29 b3 5b ..x....| ...0.).[
000000C0  4c f6 69 64 3f d1 f2 a7  20 48 6f 96 72 30 24 67 L.id?...  Ho.r0$g
```

2 Continue response: C&C site sends more data to backdoor beside the initial response

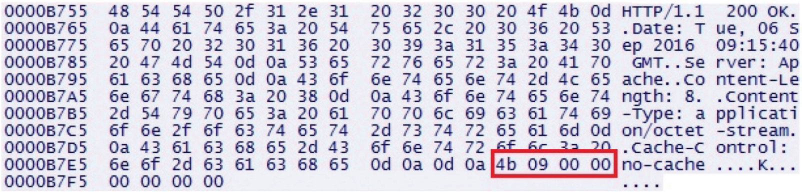
The HTTP response start with “49 09 00 00”, following with a 4-bytes unsigned integer which indicates (content length – 8)



```
00000A05  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d HTTP/1.1  200 OK.
00000A15  0a 44 61 74 65 3a 20 54  75 65 2c 20 30 36 20 53 .Date: T ue, 06 S
00000A25  65 70 20 32 30 31 36 20  30 39 3a 31 35 3a 33 38 ep 2016  09:15:38
00000A35  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70  GMT..Se rver: Ap
00000A45  61 63 68 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65 ache..Co ntent-Le
00000A55  6e 67 74 68 3a 20 33 31  39 37 33 0d 0a 43 6f 6e ngth: 31 973..Con
00000A65  74 65 6e 74 2d 54 79 70  65 3a 20 61 70 70 6c 69 tent-Typ e: appli
00000A75  63 61 74 69 6f 6e 2f 6f  63 74 65 74 2d 73 74 72 cation/o ctet-str
00000A85  65 61 6d 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72 eam..Cac he-Contr
00000A95  6f 6c 3a 20 6e 6f 2d 63  61 63 68 65 0d 0a 0d 0a ol: no-c ache....
00000AA5  49 09 00 00 dd 7c 00 00  46 9f 24 f0 6a ad 1f 67 I....|.. F.$.j..g
00000AB5  a8 e8 b9 f3 14 40 8b 82  2c 84 07 a3 30 24 aa 77 .....@.. ,...0$.w
00000AC5  1f dc 7f 2c 98 d7 d6 f2  a7 20 18 1d ff 1c 44 62 ...,.... . ....Db
00000AD5  67 d6 cc 63 6f 36 71 e8  48 d2 7d 08 68 9b 8f 49 g..co6q. H.}.h..I
00000AE5  a6 f4 11 28 b8 53 cd 59  d3 48 0e 33 b6 5c 78 9c ...(.S.Y .H.3.\x.
00000AF5  e9 be 81 51 ce ad 28 a3  71 41 cf a3 fb f0 56 17 ...Q..(. qA....V.
00000B05  05 59 66 83 c2 4c dd 9b  56 6f 86 25 80 1e 27 87 .Yf..L.. Vo.%..'.
```

3 End response: C&C site use this to indicate there is no more data

The HTTP response start with “4b 09 00 00”, follow with “00 00 00 00”



```
0000B755  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d HTTP/1.1  200 OK.
0000B765  0a 44 61 74 65 3a 20 54  75 65 2c 20 30 36 20 53 .Date: T ue, 06 S
0000B775  65 70 20 32 30 31 36 20  30 39 3a 31 35 3a 34 30 ep 2016  09:15:40
0000B785  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70  GMT..Se rver: Ap
0000B795  61 63 68 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65 ache..Co ntent-Le
0000B7A5  6e 67 74 68 3a 20 38 0d  0a 43 6f 6e 74 65 6e 74 ngth: 8. .Content
0000B7B5  2d 54 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69 -Type: a pplicati
0000B7C5  6f 6e 2f 6f 63 74 65 74  2d 73 74 72 65 61 6d 0d on/octet -stream.
0000B7D5  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20 .Cache-C ontrol: 
0000B7E5  6e 6f 2d 63 61 63 68 65  0d 0a 0d 0a 4b 09 00 00 no-cache ....K...
0000B7F5  00 00 00 00                                      ....
```

The response sequence is

1 Initial response
2 1~many continue response
3 End response

3.8.2. Indicators (STIX)

Type	Server List
C2 Servers	ioffice.xpresit.net iavrias.playop.net idropx.serverpit.com twnic.ignorelist.com foodinfo.serverpit.com pixtail.serverpit.com iebay.serverpit.com icst.ygto.com dcns.soniceducation.com conderpay.etowns.net ipaddress.suroot.com movieonline.redirectme.net beersale.serveme.com csbc.itaiwans.com ipcheck.ignorelist.com carsails.allowed.org opensslv3.csproject.org appinfo.xpresit.ne babystats.dnset.com appinfo.fairuse.org longdays.csproject.org iphone7.pwnz.org opensslv971.ssl443.org imusic.getce.com fatgirls.fatdiary.org inewdays.csproject.org spotify.effers.com

3.8.3. Recommendations

C&C sites

PLEAD group likes to use compromised router in TW as first level C&C site, keeping eyes on those suspicious domains which are resolved to TW router.

Network

The backdoor downloads the major backdoor routines from the network first; monitor the network traffic, which matches the format we mentioned before.

3.9. PHASE VII: ACTIONS ON OBJECTIVES

3.9.1. Actions on Objectives

A. PLEAD Backdoor

PLEAD backdoor contains capabilities that the attackers can utilize for data exfiltration and information gathering. Among the backdoor capabilities are as follows:

- Harvest saved credentials from Browsers and Outlook
- List Drives, Processes, Open Windows, Files
- Open remote Shell
- Upload target file
- Execute applications via ShellExecute API
- Delete Target file

PLEAD's main targets are documents containing sensitive information. One particular directory of interest that they target is the "Recent" directory. Exfiltration of these documents are done via POST http requests. The same is done with other information that PLEAD backdoor gathers from its victim. During Exfiltration of information, PLEAD will use RC4 to encrypt the information being sent back to the attackers.

B. DRIGO

Another tool used by PLEAD threat actors is the exfiltration tool DRIGO. This is mainly an exfiltration tool which also targets documents. DRIGO is coded using GOLANG and mainly searches the infected target's machine for documents and upload them to Google Drive. Each copy of DRIGO contains a refresh token tied to a specific Gmail account used by the attackers and tied to a Google Drive. The stolen files are uploaded to these Google drives which can then be harvested by the attackers.

There are two types of DRIGO malware used by PLEAD:

GDrive Uploader – This type of DRIGO malware is used to exfiltrate document files by uploading them to attacker-owned google drives. In order to do this, DRIGO will use a refresh token, almost an equivalent of a user credential, and request an access token in order to gain access to its google drive and upload files.

GSMTP Mailer – This type of DRIGO malware makes use of Gmail SMTP services in order to exfiltrate information. It contains a pre-constructed MIME header. The sender and recipient email addresses are hardcoded in the malware. Instead of a password, which is needed to log on to the SMTP server, it instead uses an access token.

Both types of DRIGO malwares are compiled using GOLANG which is designed to easily interact with Google services. This part also presents several challenges in defending against DRIGO.

3.9.2. Indicators (STIX)

Type	List
DRIGO Hashes	f6ac39c9eee840ae3d818e2652497b9dba012a64 ee380b93e771c559070ebf0b4148ba5621fcd502 5ecdc9345fa35007f0b8e7d10190452d1f83979a 1df87fa4126b436d7adfbbf3720df17ca84e3e48 3eaaad2a9746a2b9916437a6c5968401c9dfc263 3fa02b21c74c5271eb5d919baa71b5f4d5284bda
DRIGO Tokens	1%2FRb3HQPOywy4KuTyrihejaUN8duxc3oq89fuKfGSciul 1%2FzT_i6fNmPAp2dRAMf5gd9m4pTaUpOBorXIqt3QJfRfY 1%2FPd2GWZeJuKjb1Lg_uoAPoEqlYbqdH2ueuCcB9I3SST4 1%2FeftUFk_CZG42e5vAL5en4g9WZLQoeIoHDpppMxPZcgg 1%2FKbnxSx4oNaVV-AwJ4dnBNPAbUK_ir63NI1FKKGHoiPw 1%2FeftUFk_CZG42e5vAL5en4g9WZLQoeIoHDpppMxPZcgg
DRIGO GSMTP Mailer	16f721d334b091ce2ed4b0c3a062f34fb418c180

3.9.3. Recommendations

Backdoor Activity – PLEAD exfiltrates most of the information via backdoor communication channel. The exfiltration of information is encrypted but the backdoor communication is not. In addition, backdoor commands can be seen in plain text most of the time. Therefore, it would be recommended that backdoor communication be detected to prevent further exfiltration of information. You may refer to the Command and Control Section of the paper for network protocols used by PLEAD backdoors.

Saved Credentials – Another notable information being stolen by PLEAD are saved credentials in commonly used softwares such as browsers and email softwares. Although very convenient, it is recommended not to automatically save passwords when accessing accounts using these softwares, or at all, as these can be retrieved by malwares. In cases of an incident discovery, it is advised to update your passwords immediately in case there have been credentials that have been exfiltrated.

DRIGO

Persistence - As part of its persistence, DRIGO will have an autostart entry in the "Run" registry, which can be used to check for possible DRIGO infection.

Packed Binary – Majority of the later versions of DRIGO are packed using UPX in order to give them a certain measure of protection against static scanners. However, this can also be used as an indicator of possible infection.

Traffic – DRIGO mainly interacts with Google services and is seen to have used HTTPS traffic identical to the normal Google API generated traffic. However, if in your organization this kind of transaction is not part of your normal routine (your organization does not use automated Google Drive uploads, or does not utilize Google Drive at all), the traffic's distinct structure may be flagged as an indicator of possible infection.

Below is an example of the refresh token traffic that is generated by DRIGO:

Requesting for Access Token:

```
POST /o/oauth2/token HTTP/1.1
Host: accounts.google.com
User-Agent: Go 1.1 package http
Content-Length: 208
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

client_id={REMOVED}apps.googleusercontent.com&client_secret=
{REMOVED}&grant_type=refresh_token&refresh_token={REMOVED}
```

Access token reply:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Thu, 14 Oct 2014 08:08:32 GMT
Content-Disposition: attachment; filename=”sample.txt”;
filename*=UTF-8”sample.txt
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Server: GSE
Alternate-Protocol: 443:quic
Transfer-Encoding: chunked

{
“access_token” : “{REMOVED}”,
“token_type” : “Bearer”,
“expires_in” : 3600
}
```

Tokens, IDs, Secrets – If your organization is using Google APIs to automatically interact with Google services, then you may be able to build a whitelist of tokens, IDs, and/or client secrets that should interact with the services, and seeing tokens, IDs, and client secrets not on the list being used to interact with such services may be an indicator of possible compromise.

Tiger Security

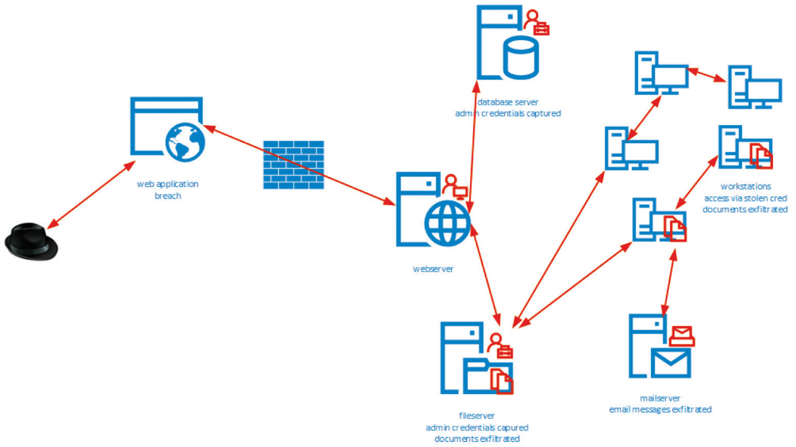
4. Case Study

The group of Chinese origin, known as Threat Actor 11 (TA-11), is known for its government-sponsored high-level cyber-espionage campaigns. Its favourite targets are infrastructure companies, especially telecommunications firms and Internet Services Providers.

A unique feature of the group is the use of free DNS services, in particular those run by Hurricane Electric, in order to redirect popular domains with a good reputation to its C2 servers and remain unnoticed at the eyes of analysts and automated security systems.

In many cases, TA-11 adopts zero-day exploits to hit its targets. Some of them, especially those aiming at the Windows operating systems, where kept secret for as long as six months.

Example of illustration of the attack (High level)



4.1. CAMPAIGN

This illustration shows, from left to right, the different stages of the attack: the TA compromises a frontier web application, then gains access to a low-importance server and starts gathering credentials. Using these and sometimes with the help of privilege escalation exploits, the attacker gains access to the more delicate systems and, once he collects some admin credentials, he moves laterally across the whole network, exfiltrating data and taking advantage of the controlled system in order to attack new targets or getting more and more entrenched.

4.2. TARGET OF THE ATTACK AND IMPACT

The TA has been known for being particularly interested in stealing corporate information, blueprints, IP and financial information.
The attack usually begins with the breach of a web-exposed service and then spreads through the internal network.

4.3. PHASE I: RECONAISSANCE

4.3.1. Reconnaissance

The TA uses different tools and techniques in order to pinpoint a soft spot in the target perimeter. The scans usually last for a few days, and are often associated with manual testing.
There is also evidence of the reuse of previously gathered information and good information storage and classification: in at least one case, a victim organization has been hit again after almost two years and the attackers clearly took advantage of the intelligence gathered during the first hack.
Documented tools and techniques:

- NetSparker
- Acunetix, used usually against general public web applications
- Manual recon: the TA usually employs multiple pentesters, in order to attack different endpoint at the same time

Our hypothesis is that TA-11 adopts all this different automatic scanning tools against secondary targets in order to create big amount of abnormal traffic. All this noise is used to mask the real attacks that take place against their primary target and are carried on manually.
Also during this phase the TA sets up the C2 infrastructure needed to collect the information exfiltrated from the victim's network.

4.3.2. Recommendations

A strong and centralised log collection and analysis process is the only way to detect these activities in the early stages. An anomaly-based intrusion detection system could also help to stop malicious activity before the attackers dig too deep inside the web applications.
A good CMS maintenance and update routine also helps to reduce the vulnerable perimeter.

4.4. PHASE II: WEAPONIZATION

4.4.1. Weaponization

This phase is very target-dependant. We've directly observed more custom techniques, such as coupling a very specific webshell to a jpeg file, in order to trigger a RCE in one of the victim organization web applications.
In other cases, especially when a viable vulnerable service is not available, the attacker uses personalized spear phishing emails that contain a malicious file or link.
Attachments are usually ZIP files. The usage of malicious Microsoft Office files is also well documented.
In this second scenario, the payload consists usually in a customized RAT, such as the 4H RAT or the 3PARA RAT or a backdoor, such as WEB2C, BISCUIT or HttpBrowser.

4.4.2. Recommendations

Preventing this kind of activities might be tricky. The detection of the injected webshell can be especially challenging, given its very small size.

Social engineering attacks like spear-phishing emails are also difficult to counteract. A good level of protection is given by an adequate configuration of the Microsoft Office suite, disabling macros and third party plugins (e.g. Adobe Flash) via group policies has proven a very effective course of action.

4.5. PHASE III: DELIVERY

4.5.1. Delivery

The infection vector and at the same the persistence mechanism used by TA-11 is a Web shell called ChinaChopper.

Developed by the TA itself, it is used to remotely access the compromised Linux and Windows systems. The tool consists of a client GUI interface and a small script file uploaded on the breached server.

Versions for virtually any server-side language (aspx, jsp, cfm, asp, ASPC, php, node) have been documented.

The main feature of this tool is given by the extreme flexibility of the “eval” instruction it contains. ChinaChopper makes it possible to manage the compromised systems in every aspect (file system browsing, editing and creation of directories and files, download of remote files, execution of SQL queries and access to a command prompt). Even more sophisticated modules allow the loading of whole agents directly into memory.

ChinaChopper requires a special client application to show its full potential.

Its small size and the use of a single legitimate function make it practically invisible to common antivirus solutions.

Nonetheless, ChinaChopper cannot provide the interactivity needed during the exploration of an unknown system. To overcome this limitation or to perform more complex operations, the attackers often make great use of scripts, which usually redirect the output to a file. These documents are later retrieved in order to read the results of the scripts.

4.5.2. Recommendations

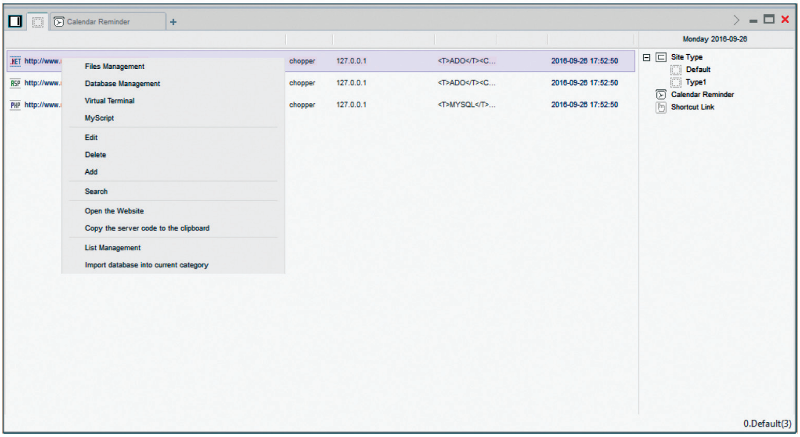
In order to prevent the injection of the web shell on non-UGC websites, a Tripwire-like control system that detects new or modified files could be useful.

Against workstation-side threats, especially if delivered by email, a good AV can be considered the only line of defence, even if this strategy has proven partially ineffective against the last encryption and obfuscation techniques.

4.6. PHASE IV: EXPLOITATION

4.6.1. Exploitation

After the webshell is delivered to the victim server, the TA takes advantage of the GUI client in order to exploit its full potential.



.NET	http://www.	chopper	127.0.0.1	<T>ADO</T><C...	2016-09-26 17:52:50
ASP	http://www.	chopper	127.0.0.1	<T>ADO</T><C...	2016-09-26 17:52:50
PHP	http://www.	chopper	127.0.0.1	<T>MYSQL</T>...	2016-09-26 17:52:50

ChinaChopper allows the attacker to manage files, databases, open a virtual terminal on the server or execute a script.
Multiple custom scripts can be uploaded in order to execute more elaborate commands.

4.6.2. Recommendations

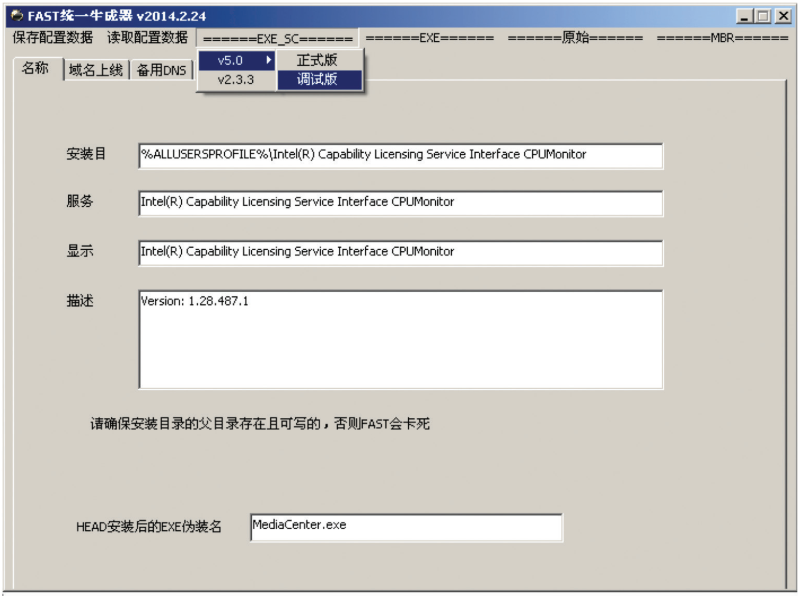
Once the shell is executed, there is not much that can be done to prevent it from being used.
A good least privilege policy, especially for the user in which the server processes run (for example, the IIS/ASP process or the PHP demon process) can be the best barrier in order to mitigate the attackers actions in this step.

4.7. PHASE V: INSTALLATION

4.7.1. Installation

In order to maintain persistence inside the environment, The TA often takes advantage of PLUGX, which is TA-11 RAT of choice.
PlugX is designed and fitted with several backdoor modules, with each module organized to perform tasks unique from the other modules:

- XPlugDisk – allows the malware to copy, move, rename, execute and even delete files.
- XPlugKeyLogger – allows the malware to log keystrokes made on current active windows.
- XPlugRegedit – allows the malware to enumerate, create, delete and modify registry entries and values.
- XPlugProcess – enumerates processes, gets process information and terminates processes.
- XPlugNethood – allows the malware to enumerate network resources and set TCP connection states.
- XPlugService – allows the malware to delete, enumerate, modify and start services.
- XPlugShell – allows the malware to perform remote shell on the affected system.



安装目 %ALLUSERSPROFILE%\Intel(R) Capability Licensing Service Interface CPUMonitor

服务 Intel(R) Capability Licensing Service Interface CPUMonitor

显示 Intel(R) Capability Licensing Service Interface CPUMonitor

描述 Version: 1.28.487.1

请确保安装目录的父目录存在且可写的，否则FAST会卡死

HEAD安装后的EXE伪装名 MediaCenter.exe

These modules should be considered the most dangerous, as they allow the attacker to gain complete control of the infected systems.

PlugX can sometimes be dropped directly on a victim workstation through a carefully crafted spear-phishing email.

Other tools often used by TA-11 are:

MIMIKATZ

This tool allows retrieving cached credentials and hashes. It is employed in preparation of lateral movement and for pass-the-hash or pass-the-ticket attacks. It is often recompiled, encrypted or obfuscated in order to minimize the chance of being detected by AVs.

PSEXEC

This legitimate Microsoft tool is often used by sysadmins in order to maintain batch of systems in a local network. Associated with the right credentials, it can become a powerful weapon and with a very low profile.

PROCDUMP
Another legitimate Microsoft tool and usually whitelisted by AVs, ProcDump can dump portions of memory associated with specific processes.
An exfiltrated lsass.exe memdump might allow an attacker to recover all the cached credentials and hashes, without even have to deploy the less-than-undetectable mimikatz on the target system.
This technique has been documented of specific target system and it's a sign that the attacker is paying lots of attention in order to go unnoticed.

4.7.2. Recommendations

A good AV solution can help prevent or at least lessen the damages caused by the PlugX RAT. However, specially crafted or customized version of this threat is known to evade AV detection with ease.
The power of Sysinternals tools, such as ProcDump and PsExec, can be easily stopped thanks to a good privilege policy, especially regarding administrator/debug rights.
Specific countermeasures can be implemented against Mimikatz. The deployment of KB2871997 in conjunction with the adoption the "Protected Users" group on Windows Vista/Server 2008 is the most useful of these techniques and is supported directly by Microsoft, even if its documentation is somewhat lacking.

4.8. PHASE VI: COMMAND & CONTROL

4.8.1. Command & Control

Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel is established, intruders have "hands on the keyboard" access inside the target environment.
TA-11 has a very distinctive modus operandi: high-precision attacks in

association with daily-set goals. The activity is spread across a 9-hours window that closely recalls a "daily shift". It has also been documented an almost complete stop of the malicious activities consistent with certain Chinese-specific holydays.

They are also particularly careful not to leave artefacts on disk unless absolutely necessary.

The TA also adopts a specific VPN service, which can be purchased from Chinese language only vendors.

The attacker also has considerable experience in lateral movement activities and ability to build custom tools that evade the detection of anti-malware solutions. The installation of persistent implants is carefully evaluated, in order to minimize the chance of exposure.

Often the most traffic-bound activities are synchronized with the working hours of the targeted organization, in order to obfuscate malicious activity in the general "noise" of an actively used network.

4.8.2. Recommendations

A good AV solution, a very disciplined software patching policy and a good and a centralised Windows system logs management can help mitigate and isolate the anomalies produced by the usage of the attackers' tools.

It is also useful to analyse the network logs searching for anomalous bandwidth-consuming outbound HTTP traffic, with payload ranging between 200k and a few megabytes, which might indicate an active exfiltration.

4.9. PHASE VII: ACTIONS ON OBJECTIVES

4.9.1. Actions on Objectives

Once the attacker is well rooted in a couple of systems, the next objective is to try to reach to more sensible systems inside the network. In the case of TA-11, this is accomplished with the tools already listed in section 4.7.1: credentials captured via mimikatz or memory dumps are abused in order to move from system to system using OS provided tools or PsExec based scripts. This allows the attacker to get more and more entrenched inside the network and to get access to progressively more sensible information, that can be quietly exfiltrated via a web-shell or one of the PlugX modules.

4.9.2. Recommendations

Given most of the attackers' lateral movement is indistinguishable from legitimate one, Windows access logs should be collected and routinely scrutinized in order to pinpoint "unusual" or "unscheduled" administrative access.
Network fragmentation, user groups separation and the adoption advanced password management solutions, ideally integrated with two factor authentication devices such smart card or OTP tokens, are the best weapons against lateral movement.

4.10. APPENDIX: STIX IOCS

```
‹stix:STIX_Package
                xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
                xmlns:cybox="http://cybox.mitre.org/cybox-2"
                xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
                xmlns:ASObj="http://cybox.mitre.org/objects#ASObject-1"
                xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"
                xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
                xmlns:EmailMessageObj="http://cybox.mitre.org/objects#EmailMessageObject-2"
                xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
                xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-2"
                xmlns:HostnameObj="http://cybox.mitre.org/objects#HostnameObject-1"
                xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
                xmlns:PipeObj="http://cybox. mitre.org/objects#PipeObject-2"
                xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
                xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2"
                xmlns:marking="http://data-marking.mitre.org/Marking-1"
                xmlns:tlpMarking="http://data-
marking.mitre.org/extensions/MarkingStructure#TLP-1"
                xmlns:et="http://stix.mitre.org/ExploitTarget-1"
                xmlns:incident="http://stix.mitre.org/Incident-1"
```

```
          xmlns:indicator=”http://stix.mitre.org/Indicator-2”
          xmlns:ttp=”http://stix.mitre.org/TTP-1”
          xmlns:ta=”http://stix.mitre.org/ThreatActor-1”
          xmlns:stixCommon=”http://stix.mitre.org/common-1”
          xmlns:stixVocabs=”http://stix.mitre.org/default_vocabularies-1”
          xmlns:ciqIdentity=”http://stix.mitre.org/extensions/Identity#CIQIdentity3.0-1”
          xmlns:snortTM=”http://stix.mitre.org/extensions/TestMechanism#Snort-1”
          xmlns:stix=”http://stix.mitre.org/stix-1”
          xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
          xmlns:TS=”https://misp.tigersecurity.pro”
          xmlns:xal=”urn:oasis:names:tc:ciq:xal:3”
          xmlns:xnl=”urn:oasis:names:tc:ciq:xnl:3”
          xmlns:xpil=”urn:oasis:names:tc:ciq:xpil:3”
          xsi:schemaLocation=”
          http://cybox.mitre.org/common-2
http://cybox.mitre.org/XMLSchema/common/2.1/cybox_common.xsd
          http://cybox.mitre.org/cybox-2
http://cybox.mitre.org/XMLSchema/core/2.1/cybox_core.xsd
          http://cybox.mitre.org/default_vocabularies-2
http://cybox.mitre.org/XMLSchema/default_vocabularies/2.1/cybox_default_vocabularies.xsd
          http://cybox.mitre.org/objects#ASObject-1
http://cybox.mitre.org/XMLSchema/objects/AS/1.0/AS_Object.xsd
          http://cybox.mitre.org/objects#AddressObject-2
http://cybox.mitre.org/XMLSchema/objects/Address/2.1/Address_Object.xsd
          http://cybox.mitre.org/objects#DomainNameObject-1
http://cybox.mitre.org/XMLSchema/objects/Domain_Name/1.0/Domain_Name_Object.xsd
          http://cybox.mitre.org/objects#EmailMessageObject-2
http://cybox.mitre.org/XMLSchema/objects/Email_Message/2.1/Email_Message_Object.xsd
          http://cybox.mitre.org/objects#FileObject-2
http://cybox.mitre.org/XMLSchema/objects/File/2.1/File_Object.xsd
          http://cybox.mitre.org/objects#HTTPSessionObject-2
http://cybox.mitre.org/XMLSchema/objects/HTTP_Session/2.1/HTTP_Session_Object.xsd
          http://cybox.mitre.org/objects#HostnameObject-1
http://cybox.mitre.org/XMLSchema/objects/Hostname/1.0/Hostname_Object.xsd
          http://cybox.mitre.org/objects#MutexObject-2
http://cybox.mitre.org/XMLSchema/objects/Mutex/2.1/Mutex_Object.xsd
          http://cybox.mitre.org/objects#PipeObject-2
http://cybox.mitre.org/XMLSchema/objects/Pipe/2.1/Pipe_Object.xsd
          http://cybox.mitre.org/objects#URIObject-2
http://cybox.mitre.org/XMLSchema/objects/URI/2.1/URI_Object.xsd
          http://cybox.mitre.org/objects#WinRegistryKeyObject-2
http://cybox.mitre.org/XMLSchema/objects/Win_Registry_Key/2.1/Win_Registry_Key_Object.xsd
          http://data-marking.mitre.org/Marking-1
http://stix.mitre.org/XMLSchema/data_marking/1.1.1/data_marking.xsd
```

```
                 http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1
http://stix.mitre.org/XMLSchema/extensions/marking/tlp/1.1.1/tlp_marking.xsd
                 http://stix.mitre.org/ExploitTarget-1
http://stix.mitre.org/XMLSchema/exploit_target/1.1.1/exploit_target.xsd
                 http://stix.mitre.org/Incident-1
http://stix.mitre.org/XMLSchema/incident/1.1.1/incident.xsd
                 http://stix.mitre.org/Indicator-2
http://stix.mitre.org/XMLSchema/indicator/2.1.1/indicator.xsd
                 http://stix.mitre.org/TTP-1
http://stix.mitre.org/XMLSchema/ttp/1.1.1/ttp.xsd
                 http://stix.mitre.org/ThreatActor-1
http://stix.mitre.org/XMLSchema/threat_actor/1.1.1/threat_actor.xsd
                 http://stix.mitre.org/common-1
http://stix.mitre.org/XMLSchema/common/1.1.1/stix_common.xsd
                 http://stix.mitre.org/default_vocabularies-1
http://stix.mitre.org/XMLSchema/default_vocabularies/1.1.1/stix_default_vocabularies.xsd
                 http://stix.mitre.org/extensions/Identity#CIQIdentity3.0-1
http://stix.mitre.org/XMLSchema/extensions/identity/ciq_3.0/1.1.1/ciq_3.0_identity.xsd
                 http://stix.mitre.org/extensions/TestMechanism#Snort-1
http://stix.mitre.org/XMLSchema/extensions/test_mechanism/snort/1.1.1/snort_test_mechanism.xsd
                 http://stix.mitre.org/stix-1
http://stix.mitre.org/XMLSchema/core/1.1.1/stix_core.xsd
                 urn:oasis:names:tc:ciq:xal:3
http://stix.mitre.org/XMLSchema/external/oasis_ciq_3.0/xAL.xsd
                 urn:oasis:names:tc:ciq:xnl:3
http://stix.mitre.org/XMLSchema/external/oasis_ciq_3.0/xNL.xsd
                 urn:oasis:names:tc:ciq:xpil:3
http://stix.mitre.org/XMLSchema/external/oasis_ciq_3.0/xPIL.xsd” id=”TS:Package-
445f046a-5a3b-4a8b-a874-aef6f029665b” version=”1.1.1” timestamp=”2016-10-
19T07:41:52.961307+00:00”>
    <stix:STIX_Header>
        <stix:Title>Export from TS MISP</stix:Title>
        <stix:Package_Intent xsi:type=”stixVocabs:PackageIntentVocab-1.0”>Threat
Report</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Related_Packages>
        <stix:Related_Package>
            <stix:Package id=”TS:STIXPackage-57a45659-6e38-447a-ad5b-201b5b86d7e5”
version=”1.1.1” timestamp=”2016-08-18T13:50:18+00:00”>
                <stix:STIX_Header>
                    <stix:Title>PLA Unit 61398 - cyber attack on top italian ISP
(MISP Event #2786)</stix:Title>
                    <stix:Package_Intent xsi:type=”stixVocabs:PackageIntentVocab-
1.0”>Threat Report</stix:Package_Intent>
```

```
        ‹/stix:STIX_Header›
        ‹stix:Incidents›
          ‹stix:Incident id=”TS:incident-57a45659-6e38-447a-ad5b-
201b5b86d7e5” timestamp=”2016-08-18T13:50:33+00:00”
xsi:type=’incident:IncidentType’›
            ‹incident:Title›PLA Unit 61398 - cyber attack on top italian
ISP‹/incident:Title›
            ‹incident:External_ID source=”MISP
Event”›2786‹/incident:External_ID›
            ‹incident:Time›
              ‹incident:Incident_Discovery precision=”second”›2016-08-
05T00:00:00+00:00‹/incident:Incident_Discovery›
              ‹incident:Incident_Reported precision=”second”›2016-08-
18T13:50:33+00:00‹/incident:Incident_Reported›
            ‹/incident:Time›
            ‹incident:Status xsi:type=”stixVocabs:IncidentStatusVocab-
1.0”›New‹/incident:Status›
            ‹incident:Related_Indicators›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
cfb4-448d-b468-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity: 180.178.34.11
(MISP Attribute #335619)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
180.178.34.11 (MISP Attribute #335619)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-cfb4-448d-b468-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-cfb4-
448d-b468-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›180.178.34.11‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
```

```
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
4120-496d-8553-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 180.178.34.12
(MISP Attribute #335620)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
180.178.34.12 (MISP Attribute #335620)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-4120-496d-8553-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-4120-
496d-8553-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›180.178.34.12‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
7dcc-4dcf-a477-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 43.250.49.161
(MISP Attribute #335621)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
43.250.49.161 (MISP Attribute #335621)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-7dcc-4dcf-a477-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-7dcc-
4dcf-a477-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›43.250.49.161‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
a990-404f-8bbe-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
```

```
                  ‹indicator:Title›Network activity: 180.178.34.14
(MISP Attribute #335622)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
180.178.34.14 (MISP Attribute #335622)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-a990-404f-8bbe-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-a990-
404f-8bbe-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›180.178.34.14‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
45f8-4e2a-9b36-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity:
106.187.53.112 (MISP Attribute #335623)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
106.187.53.112 (MISP Attribute #335623)‹/indicator:Description›
```

```
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-45f8-4e2a-9b36-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-45f8-
4e2a-9b36-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›106.187.53.112‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
7b80-430f-99d8-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity:
106.187.35.120 (MISP Attribute #335624)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
106.187.35.120 (MISP Attribute #335624)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-7b80-430f-99d8-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-7b80-
430f-99d8-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
```

```
condition=”Equals”›106.187.35.120‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
8cb4-4e7f-94ae-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity: 106.184.2.109
(MISP Attribute #335625)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
106.184.2.109 (MISP Attribute #335625)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-8cb4-4e7f-94ae-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-8cb4-
4e7f-94ae-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›106.184.2.109‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
```

```
                                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                ‹/indicator:Confidence›
                            ‹/stixCommon:Indicator›
                        ‹/incident:Related_Indicator›
                        ‹incident:Related_Indicator›
                            ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                            ‹stixCommon:Indicator id=”TS:indicator-57a45970-
7480-40a1-b68d-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                ‹indicator:Title›Network activity:
101.226.179.94 (MISP Attribute #335626)‹/indicator:Title›
                                ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                ‹indicator:Description›Network activity:
101.226.179.94 (MISP Attribute #335626)‹/indicator:Description›
                                ‹indicator:Valid_Time_Position/›
                                ‹indicator:Observable id=”TS:observable-
57a45970-7480-40a1-b68d-3baf5b86d7e5”›
                                    ‹cybox:Object id=”TS:Address-57a45970-7480-
40a1-b68d-3baf5b86d7e5”›
                                        ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                            ‹AddressObj:Address_Value
condition=”Equals”›101.226.179.94‹/AddressObj:Address_Value›
                                        ‹/cybox:Properties›
                                    ‹/cybox:Object›
                                ‹/indicator:Observable›
                                ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                ‹/indicator:Confidence›
                            ‹/stixCommon:Indicator›
                        ‹/incident:Related_Indicator›
                        ‹incident:Related_Indicator›
                            ‹stixCommon:Relationship›Network
```

```
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
8098-49d9-938a-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 219.235.1.153
(MISP Attribute #335627)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
219.235.1.153 (MISP Attribute #335627)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-8098-49d9-938a-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-8098-
49d9-938a-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›219.235.1.153‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
a700-4155-87c9-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 117.174.59.4
(MISP Attribute #335628)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
```

```
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
117.174.59.4 (MISP Attribute #335628)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-a700-4155-87c9-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-a700-
4155-87c9-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›117.174.59.4‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
4538-4f38-892a-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 96.44.186.252
(MISP Attribute #335629)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
96.44.186.252 (MISP Attribute #335629)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-4538-4f38-892a-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-4538-
```

```
4f38-892a-3baf5b86d7e5”>
                      <cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”>
                        <AddressObj:Address_Value
condition=”Equals”>96.44.186.252</AddressObj:Address_Value>
                      </cybox:Properties>
                    </cybox:Object>
                  </indicator:Observable>
                  <indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”>
                    <stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”>High</stixCommon:Value>
                    <stixCommon:Description>Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none</stixCommon:Description>
                  </indicator:Confidence>
                </stixCommon:Indicator>
              </incident:Related_Indicator>
              <incident:Related_Indicator>
                <stixCommon:Relationship>Network
activity</stixCommon:Relationship>
                <stixCommon:Indicator id=”TS:indicator-57a45970-
7e20-4272-a003-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’>
                  <indicator:Title>Network activity:
209.73.152.243 (MISP Attribute #335630)</indicator:Title>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>Malware Artifacts</indicator:Type>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>IP Watchlist</indicator:Type>
                  <indicator:Description>Network activity:
209.73.152.243 (MISP Attribute #335630)</indicator:Description>
                  <indicator:Valid_Time_Position/>
                  <indicator:Observable id=”TS:observable-
57a45970-7e20-4272-a003-3baf5b86d7e5”>
                    <cybox:Object id=”TS:Address-57a45970-7e20-
4272-a003-3baf5b86d7e5”>
                      <cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”>
                        <AddressObj:Address_Value
condition=”Equals”>209.73.152.243</AddressObj:Address_Value>
                      </cybox:Properties>
                    </cybox:Object>
                  </indicator:Observable>
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
6a94-4441-83e5-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity:
67.198.141.162 (MISP Attribute #335631)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
67.198.141.162 (MISP Attribute #335631)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-6a94-4441-83e5-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-6a94-
4441-83e5-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›67.198.141.162‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
ca28-4c2c-8e90-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity:
104.171.165.21 (MISP Attribute #335632)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
104.171.165.21 (MISP Attribute #335632)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-ca28-4c2c-8e90-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-ca28-
4c2c-8e90-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›104.171.165.21‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
52c0-474b-8787-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
```

```
                                    ‹indicator:Title›Network activity:
67.198.141.163 (MISP Attribute #335633)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
67.198.141.163 (MISP Attribute #335633)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-52c0-474b-8787-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-52c0-
474b-8787-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›67.198.141.163‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
7478-4bd2-82e0-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity:
209.73.152.244 (MISP Attribute #335634)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
209.73.152.244 (MISP Attribute #335634)‹/indicator:Description›
```

```
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-7478-4bd2-82e0-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-7478-
4bd2-82e0-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›209.73.152.244‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
12a0-43ce-8d33-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity:
104.247.216.27 (MISP Attribute #335635)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
104.247.216.27 (MISP Attribute #335635)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-12a0-43ce-8d33-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-12a0-
43ce-8d33-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
```

```
condition=”Equals”›104.247.216.27‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
b884-4c3a-ac13-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity:
104.250.137.91 (MISP Attribute #335636)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
104.250.137.91 (MISP Attribute #335636)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-b884-4c3a-ac13-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-b884-
4c3a-ac13-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›104.250.137.91‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
```

```
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
8dac-4283-9d1a-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity: 50.117.40.18
(MISP Attribute #335637)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
50.117.40.18 (MISP Attribute #335637)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45970-8dac-4283-9d1a-3baf5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a45970-8dac-
4283-9d1a-3baf5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›50.117.40.18‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
```

```
activity‹/stixCommon:Relationship›
                        ‹stixCommon:Indicator id=”TS:indicator-57a45970-
3458-4658-897f-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                            ‹indicator:Title›Network activity: 50.117.40.19
(MISP Attribute #335638)‹/indicator:Title›
                            ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                            ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                            ‹indicator:Description›Network activity:
50.117.40.19 (MISP Attribute #335638)‹/indicator:Description›
                            ‹indicator:Valid_Time_Position/›
                            ‹indicator:Observable id=”TS:observable-
57a45970-3458-4658-897f-3baf5b86d7e5”›
                                ‹cybox:Object id=”TS:Address-57a45970-3458-
4658-897f-3baf5b86d7e5”›
                                    ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                        ‹AddressObj:Address_Value
condition=”Equals”›50.117.40.19‹/AddressObj:Address_Value›
                                    ‹/cybox:Properties›
                                ‹/cybox:Object›
                            ‹/indicator:Observable›
                            ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                            ‹/indicator:Confidence›
                        ‹/stixCommon:Indicator›
                    ‹/incident:Related_Indicator›
                    ‹incident:Related_Indicator›
                        ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                        ‹stixCommon:Indicator id=”TS:indicator-57a45970-
9d4c-4f1d-a211-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                            ‹indicator:Title›Network activity: 23.89.85.2
(MISP Attribute #335639)‹/indicator:Title›
                            ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
```

```
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
23.89.85.2 (MISP Attribute #335639)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-9d4c-4f1d-a211-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-9d4c-
4f1d-a211-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›23.89.85.2‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
f534-4743-b995-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 50.117.40.20
(MISP Attribute #335640)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
50.117.40.20 (MISP Attribute #335640)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-f534-4743-b995-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-f534-
```

```
4743-b995-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›50.117.40.20‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45970-
648c-4540-810c-3baf5b86d7e5” timestamp=”2016-08-05T09:16:32+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity: 23.104.158.3
(MISP Attribute #335641)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
23.104.158.3 (MISP Attribute #335641)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45970-648c-4540-810c-3baf5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a45970-648c-
4540-810c-3baf5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›23.104.158.3‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
```

```
                  <indicator:Confidence timestamp=”2016-08-
05T09:16:32+00:00”>
                    <stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”>High</stixCommon:Value>
                    <stixCommon:Description>Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none</stixCommon:Description>
                  </indicator:Confidence>
                </stixCommon:Indicator>
              </incident:Related_Indicator>
              <incident:Related_Indicator>
                <stixCommon:Relationship>Network
activity</stixCommon:Relationship>
                <stixCommon:Indicator id=”TS:indicator-57a4569c-
1b2c-416f-97f1-200f5b86d7e5” timestamp=”2016-08-05T09:04:28+00:00”
xsi:type=’indicator:IndicatorType’>
                  <indicator:Title>Network activity: 60.251.33.226
(MISP Attribute #335600)</indicator:Title>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>Malware Artifacts</indicator:Type>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>IP Watchlist</indicator:Type>
                  <indicator:Description>Network activity:
60.251.33.226 (MISP Attribute #335600)</indicator:Description>
                  <indicator:Valid_Time_Position/>
                  <indicator:Observable id=”TS:observable-
57a4569c-1b2c-416f-97f1-200f5b86d7e5”>
                    <cybox:Object id=”TS:Address-57a4569c-1b2c-
416f-97f1-200f5b86d7e5”>
                      <cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”>
                        <AddressObj:Address_Value
condition=”Equals”>60.251.33.226</AddressObj:Address_Value>
                      </cybox:Properties>
                    </cybox:Object>
                  </indicator:Observable>
                  <indicator:Confidence timestamp=”2016-08-
05T09:04:28+00:00”>
                    <stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”>High</stixCommon:Value>
                    <stixCommon:Description>Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none</stixCommon:Description>
                  </indicator:Confidence>
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a4569c-
bb40-4831-a8bb-200f5b86d7e5” timestamp=”2016-08-05T09:04:28+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Network activity: 60.251.33.225
(MISP Attribute #335601)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                  ‹indicator:Description›Network activity:
60.251.33.225 (MISP Attribute #335601)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a4569c-bb40-4831-a8bb-200f5b86d7e5”›
                    ‹cybox:Object id=”TS:Address-57a4569c-bb40-
4831-a8bb-200f5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                        ‹AddressObj:Address_Value
condition=”Equals”›60.251.33.225‹/AddressObj:Address_Value›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:04:28+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a4569c-
cb00-4cb0-86fe-200f5b86d7e5” timestamp=”2016-08-05T09:04:28+00:00”
xsi:type=’indicator:IndicatorType’›
```

```
                                    ‹indicator:Title›Network activity:
61.220.191.197 (MISP Attribute #335602)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
61.220.191.197 (MISP Attribute #335602)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a4569c-cb00-4cb0-86fe-200f5b86d7e5”›
                                        ‹cybox:Object id=”TS:Address-57a4569c-cb00-
4cb0-86fe-200f5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                                ‹AddressObj:Address_Value
condition=”Equals”›61.220.191.197‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:04:28+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a4569c-
2c88-4f9e-8f04-200f5b86d7e5” timestamp=”2016-08-05T09:04:28+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Network activity:
61.220.191.198 (MISP Attribute #335603)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Network activity:
61.220.191.198 (MISP Attribute #335603)‹/indicator:Description›
```

```
                            ‹indicator:Valid_Time_Position/›
                            ‹indicator:Observable id=”TS:observable-
57a4569c-2c88-4f9e-8f04-200f5b86d7e5”›
                                ‹cybox:Object id=”TS:Address-57a4569c-2c88-
4f9e-8f04-200f5b86d7e5”›
                                    ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                        ‹AddressObj:Address_Value
condition=”Equals”›61.220.191.198‹/AddressObj:Address_Value›
                                    ‹/cybox:Properties›
                                ‹/cybox:Object›
                            ‹/indicator:Observable›
                            ‹indicator:Confidence timestamp=”2016-08-
05T09:04:28+00:00”›
                                ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                            ‹/indicator:Confidence›
                        ‹/stixCommon:Indicator›
                    ‹/incident:Related_Indicator›
                    ‹incident:Related_Indicator›
                        ‹stixCommon:Relationship›Network
activity‹/stixCommon:Relationship›
                        ‹stixCommon:Indicator id=”TS:indicator-57a4569c-
5c98-4488-b8a2-200f5b86d7e5” timestamp=”2016-08-05T09:04:28+00:00”
xsi:type=’indicator:IndicatorType’›
                            ‹indicator:Title›Network activity: 23.89.85.11
(MISP Attribute #335604)‹/indicator:Title›
                            ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                            ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›IP Watchlist‹/indicator:Type›
                            ‹indicator:Description›Network activity:
23.89.85.11 (MISP Attribute #335604)‹/indicator:Description›
                            ‹indicator:Valid_Time_Position/›
                            ‹indicator:Observable id=”TS:observable-
57a4569c-5c98-4488-b8a2-200f5b86d7e5”›
                                ‹cybox:Object id=”TS:Address-57a4569c-5c98-
4488-b8a2-200f5b86d7e5”›
                                    ‹cybox:Properties
xsi:type=”AddressObj:AddressObjectType” category=”ipv4-addr” is_source=”false”›
                                        ‹AddressObj:Address_Value
```

```
condition=”Equals”›23.89.85.11‹/AddressObj:Address_Value›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:04:28+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45811-
88b0-422a-a3d3-20135b86d7e5” timestamp=”2016-08-05T09:10:41+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Payload delivery:
edit.aspx|3f2611bf1d1b67799e033bc84363614377eeec05 (MISP Attribute
#335606)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Payload delivery:
edit.aspx|3f2611bf1d1b67799e033bc84363614377eeec05 (MISP Attribute
#335606)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45811-88b0-422a-a3d3-20135b86d7e5”›
                                        ‹cybox:Object id=”TS:File-57a45811-88b0-
422a-a3d3-20135b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                                                ‹FileObj:File_Name
condition=”Equals”›edit.aspx‹/FileObj:File_Name›
                                                ‹FileObj:Hashes›
                                                    ‹cyboxCommon:Hash›
                                                        ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›SHA1‹/cyboxCommon:Type›
                                                        ‹cyboxCommon:Simple_Hash_Value
```

```
condition="Equals">3f2611bf1d1b67799e033bc84363614377eeec05</cyboxCommon:Simple_Hash_Value>
                          </cyboxCommon:Hash>
                        </FileObj:Hashes>
                      </cybox:Properties>
                    </cybox:Object>
                  </indicator:Observable>
                  <indicator:Confidence timestamp="2016-08-
05T09:10:41+00:00">
                    <stixCommon:Value
xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</stixCommon:Value>
                    <stixCommon:Description>Derived from MISP's
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none</stixCommon:Description>
                  </indicator:Confidence>
                </stixCommon:Indicator>
              </incident:Related_Indicator>
              <incident:Related_Indicator>
                <stixCommon:Relationship>Payload
delivery</stixCommon:Relationship>
                <stixCommon:Indicator id="TS:indicator-57a45811-
3a38-4c53-9b69-20135b86d7e5" timestamp="2016-08-05T09:10:41+00:00"
xsi:type='indicator:IndicatorType'>
                  <indicator:Title>Payload delivery:
jquery.aspx|99993445b43084ca2c219f88922853a332c17755 (MISP Attribute
#335609)</indicator:Title>
                  <indicator:Type
xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Malware Artifacts</indicator:Type>
                  <indicator:Type
xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash Watchlist</indicator:Type>
                  <indicator:Description>Payload delivery:
jquery.aspx|99993445b43084ca2c219f88922853a332c17755 (MISP Attribute
#335609)</indicator:Description>
                  <indicator:Valid_Time_Position/>
                  <indicator:Observable id="TS:observable-
57a45811-3a38-4c53-9b69-20135b86d7e5">
                    <cybox:Object id="TS:File-57a45811-3a38-
4c53-9b69-20135b86d7e5">
                      <cybox:Properties
xsi:type="FileObj:FileObjectType">
                        <FileObj:File_Name
condition="Equals">jquery.aspx</FileObj:File_Name>
                        <FileObj:Hashes>
                          <cyboxCommon:Hash>
                            <cyboxCommon:Type
```

```
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›SHA1‹/cyboxCommon:Type›
                            ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›99993445b43084ca2c219f88922853a332c17755‹/cyboxCommon:Simple_Hash_Value›
                          ‹/cyboxCommon:Hash›
                        ‹/FileObj:Hashes›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:10:41+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45837-
7e54-4634-9c29-201c5b86d7e5” timestamp=”2016-08-05T09:11:19+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Payload delivery:
javascript.ashx|1c6dcbaac7c779b6450143308b8d759291342 65a (MISP Attribute
#335612)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                  ‹indicator:Description›Payload delivery:
javascript.ashx|1c6dcbaac7c779b6450143308b8d759291342 65a (MISP Attribute
#335612)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45837-7e54-4634-9c29-201c5b86d7e5”›
                    ‹cybox:Object id=”TS:File-57a45837-7e54-
4634-9c29-201c5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                        ‹FileObj:File_Name
condition=”Equals”›javascript.ashx‹/FileObj:File_Name›
                        ‹FileObj:Hashes›
```

```
                                                    ‹cyboxCommon:Hash›
                                                        ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›SHA1‹/cyboxCommon:Type›
                                                        ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›1c6dcbaac7c779b6450143308b8d75929134265a‹/cyboxCommon:Simple_Hash_Value›
                                                    ‹/cyboxCommon:Hash›
                                                ‹/FileObj:Hashes›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:11:19+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45838-
7318-47ed-b989-201c5b86d7e5” timestamp=”2016-08-05T09:11:20+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Payload delivery:
javascript.js|411837ccc1478cce8f97cfeb5104d04e94f3407b (MISP Attribute
#335615)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Payload delivery:
javascript.js|411837ccc1478cce8f97cfeb5104d04e94f3407b (MISP Attribute
#335615)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45838-7318-47ed-b989-201c5b86d7e5”›
                                        ‹cybox:Object id=”TS:File-57a45838-7318-
47ed-b989-201c5b86d7e5”›
                                            ‹cybox:Properties xsi:type=”FileObj:FileObjectType”›
                                                ‹FileObj:File_Name
condition=”Equals”›javascript.js‹/FileObj:File_Name›
```

```
                        ‹FileObj:Hashes›
                          ‹cyboxCommon:Hash›
                            ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›SHA1‹/cyboxCommon:Type›
                            ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›411837ccc1478cce8f97cfeb5104d04e94f3407b‹/cyboxCommon:Simple_Hash_Value›
                          ‹/cyboxCommon:Hash›
                        ‹/FileObj:Hashes›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:11:20+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45838-
2158-4de1-bdf7-201c5b86d7e5” timestamp=”2016-08-05T09:11:20+00:00” xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Payload delivery:
javascript.jsl730d112cf4ed9a08d1b80cb2fd3c3ce943febbdf2f43b0c69e24b74d298e2d1e (MISP
Attribute #335616)‹/indicator:Title›
                    ‹indicator:Type xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/
indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                  ‹indicator:Description›Payload delivery:
javascript.jsl730d112cf4ed9a08d1b80cb2fd3c3ce943febbdf2f43b0c69e24b74d298e2d1e (MISP
Attribute #335616)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45838-2158-4de1-bdf7-201c5b86d7e5”›
                    ‹cybox:Object id=”TS:File-57a45838-2158-
4de1-bdf7-201c5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                        ‹FileObj:File_Name
```

```
condition=”Equals”›javascript.js‹/FileObj:File_Name›
                        ‹FileObj:Hashes›
                          ‹cyboxCommon:Hash›
                            ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-
1.0”›SHA256‹/cyboxCommon:Type›
                            ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›730d112cf4ed9a08d1b80cb2fd3c3ce943febbdf2f43b0c69e24b74d298e2d1e‹
/cyboxCommon:Simple_Hash_Value›
                          ‹/cyboxCommon:Hash›
                        ‹/FileObj:Hashes›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:11:20+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45811-
0d18-4e00-a820-20135b86d7e5” timestamp=”2016-08-05T09:10:41+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Payload delivery:
edit.aspx|2899cf603c341c9603043c5e35aa24ab6d3eacdd12f1cd850eacdcb9b0716692 (MISP
Attribute #335607)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                  ‹indicator:Description›Payload delivery:
edit.aspx|2899cf603c341c9603043c5e35aa24ab6d3eacdd12f1cd850eacdcb9b0716692 (MISP
Attribute #335607)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45811-0d18-4e00-a820-20135b86d7e5”›
                    ‹cybox:Object id=”TS:File-57a45811-0d18-
```

```
4e00-a820-20135b86d7e5”>
                      <cybox:Properties
xsi:type=”FileObj:FileObjectType”>
                        <FileObj:File_Name
condition=”Equals”>edit.aspx</FileObj:File_Name>
                        <FileObj:Hashes>
                          <cyboxCommon:Hash>
                            <cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-
1.0”>SHA256</cyboxCommon:Type>
                            <cyboxCommon:Simple_Hash_Value
condition=”Equals”>2899cf603c341c9603043c5e35aa24ab6d3eacdd12f1cd850eacdcb9b0716692</
cyboxCommon:Simple_Hash_Value>
                          </cyboxCommon:Hash>
                        </FileObj:Hashes>
                      </cybox:Properties>
                    </cybox:Object>
                  </indicator:Observable>
                  <indicator:Confidence timestamp=”2016-08-
05T09:10:41+00:00”>
                    <stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”>High</stixCommon:Value>
                    <stixCommon:Description>Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none</stixCommon:Description>
                  </indicator:Confidence>
                </stixCommon:Indicator>
              </incident:Related_Indicator>
              <incident:Related_Indicator>
                <stixCommon:Relationship>Payload
delivery</stixCommon:Relationship>
                <stixCommon:Indicator id=”TS:indicator-57a45811-
84ac-4578-8017-20135b86d7e5” timestamp=”2016-08-05T09:10:41+00:00”
xsi:type=’indicator:IndicatorType’>
                  <indicator:Title>Payload delivery:
jquery.aspx|2f988ad83fa60a8030bd3626e0a9bccb4c32d7779284b0033b202b60b57ffa57 (MISP
Attribute #335610)</indicator:Title>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>Malware Artifacts</indicator:Type>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>File Hash Watchlist</indicator:Type>
                  <indicator:Description>Payload delivery:
jquery.aspx|2f988ad83fa60a8030bd3626e0a9bccb4c32d7779284b0033b202b60b57ffa57 (MISP
Attribute #335610)</indicator:Description>
```

```
                  <indicator:Valid_Time_Position/>
                  <indicator:Observable id=”TS:observable-
57a45811-84ac-4578-8017-20135b86d7e5”>
                    <cybox:Object id=”TS:File-57a45811-84ac-
4578-8017-20135b86d7e5”>
                      <cybox:Properties
xsi:type=”FileObj:FileObjectType”>
                        <FileObj:File_Name
condition=”Equals”>jquery.aspx</FileObj:File_Name>
                        <FileObj:Hashes>
                          <cyboxCommon:Hash>
                            <cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-
1.0”>SHA256</cyboxCommon:Type>
                            <cyboxCommon:Simple_Hash_Value
condition=”Equals”>2f988ad83fa60a8030bd3626e0a9bccb4c32d7779284b0033b202b60b57ffa57</
cyboxCommon:Simple_Hash_Value>
                          </cyboxCommon:Hash>
                        </FileObj:Hashes>
                      </cybox:Properties>
                    </cybox:Object>
                  </indicator:Observable>
                  <indicator:Confidence timestamp=”2016-08-
05T09:10:41+00:00”>
                    <stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”>High</stixCommon:Value>
                    <stixCommon:Description>Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none</stixCommon:Description>
                  </indicator:Confidence>
                </stixCommon:Indicator>
              </incident:Related_Indicator>
              <incident:Related_Indicator>
                <stixCommon:Relationship>Payload
delivery</stixCommon:Relationship>
                <stixCommon:Indicator id=”TS:indicator-57a45838-
e1b0-40b9-b054-201c5b86d7e5” timestamp=”2016-08-05T09:11:20+00:00”
xsi:type=’indicator:IndicatorType’>
                  <indicator:Title>Payload delivery:
javascript.ashxla47c58701316f8989a41a5e0c65387baa28bfb2ea908fcc902b25b329c7583ad
(MISP Attribute #335613)</indicator:Title>
                  <indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”>Malware Artifacts</indicator:Type>
                  <indicator:Type
```

```
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                  ‹indicator:Description›Payload delivery:
javascript.ashx|a47c58701316f8989a41a5e0c65387baa28bfb2ea908fcc902b25b329c7583ad
(MISP Attribute #335613)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45838-e1b0-40b9-b054-201c5b86d7e5”›
                    ‹cybox:Object id=”TS:File-57a45838-e1b0-
40b9-b054-201c5b86d7e5”›
                      ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                        ‹FileObj:File_Name
condition=”Equals”›javascript.ashx‹/FileObj:File_Name›
                        ‹FileObj:Hashes›
                          ‹cyboxCommon:Hash›
                            ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-
1.0”›SHA256‹/cyboxCommon:Type›
                            ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›a47c58701316f8989a41a5e0c65387baa28bfb2ea908fcc902b25b329c7583ad‹/
cyboxCommon:Simple_Hash_Value›
                          ‹/cyboxCommon:Hash›
                        ‹/FileObj:Hashes›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:11:20+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45811-
2460-4994-9bd2-20135b86d7e5” timestamp=”2016-08-05T09:10:41+00:00”
xsi:type=’indicator:IndicatorType’›
                  ‹indicator:Title›Payload delivery:
edit.aspx|213e30382a423a88712126ebf5ff38ba8 (MISP Attribute
#335605)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                  ‹indicator:Description›Payload delivery:
edit.aspx|213e30382a423a8871212ebf5ff38ba8 (MISP Attribute
#335605)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45811-2460-4994-9bd2-20135b86d7e5”›
                    ‹cybox:Object id=”TS:File-57a45811-2460-
4994-9bd2-20135b86d7e5”›
                      ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                        ‹FileObj:File_Name
condition=”Equals”›edit.aspx‹/FileObj:File_Name›
                        ‹FileObj:Hashes›
                          ‹cyboxCommon:Hash›
                            ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›MD5‹/cyboxCommon:Type›
                            ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›213e30382a423a8871212ebf5ff38ba8‹/cyboxCommon:Simple_Hash_Value›
                          ‹/cyboxCommon:Hash›
                        ‹/FileObj:Hashes›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:10:41+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45811-
796c-4693-b2ec-20135b86d7e5” timestamp=”2016-08-05T09:10:41+00:00”
xsi:type=’indicator:IndicatorType’›
```

```
                  ‹indicator:Title›Payload delivery:
jquery.aspx|8c1ff8654ddece41452a99cb4a96c508 (MISP Attribute
#335608)‹/indicator:Title›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                  ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                  ‹indicator:Description›Payload delivery:
jquery.aspx|8c1ff8654ddece41452a99cb4a96c508 (MISP Attribute
#335608)‹/indicator:Description›
                  ‹indicator:Valid_Time_Position/›
                  ‹indicator:Observable id=”TS:observable-
57a45811-796c-4693-b2ec-20135b86d7e5”›
                    ‹cybox:Object id=”TS:File-57a45811-796c-
4693-b2ec-20135b86d7e5”›
                      ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                        ‹FileObj:File_Name
condition=”Equals”›jquery.aspx‹/FileObj:File_Name›
                        ‹FileObj:Hashes›
                          ‹cyboxCommon:Hash›
                            ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›MD5‹/cyboxCommon:Type›
                            ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›8c1ff8654ddece41452a99cb4a96c508‹/cyboxCommon:Simple_Hash_Value›
                          ‹/cyboxCommon:Hash›
                        ‹/FileObj:Hashes›
                      ‹/cybox:Properties›
                    ‹/cybox:Object›
                  ‹/indicator:Observable›
                  ‹indicator:Confidence timestamp=”2016-08-
05T09:10:41+00:00”›
                    ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                    ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                  ‹/indicator:Confidence›
                ‹/stixCommon:Indicator›
              ‹/incident:Related_Indicator›
              ‹incident:Related_Indicator›
                ‹stixCommon:Relationship›Payload
delivery‹/stixCommon:Relationship›
                ‹stixCommon:Indicator id=”TS:indicator-57a45837-
```

```
d2f4-4f87-8b58-201c5b86d7e5” timestamp=”2016-08-05T09:11:19+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Payload delivery:
javascript.ashx|8d01d604794d3494cbb31570b1e54182 (MISP Attribute
#335611)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Payload delivery:
javascript.ashx|8d01d604794d3494cbb31570b1e54182 (MISP Attribute
#335611)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45837-d2f4-4f87-8b58-201c5b86d7e5”›
                                        ‹cybox:Object id=”TS:File-57a45837-d2f4-
4f87-8b58-201c5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                                                ‹FileObj:File_Name
condition=”Equals”›javascript.ashx‹/FileObj:File_Name›
                                                ‹FileObj:Hashes›
                                                    ‹cyboxCommon:Hash›
                                                        ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›MD5‹/cyboxCommon:Type›
                                                        ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›8d01d604794d3494cbb31570b1e54182‹/cyboxCommon:Simple_Hash_Value›
                                                    ‹/cyboxCommon:Hash›
                                                ‹/FileObj:Hashes›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:11:19+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
                            ‹incident:Related_Indicator›
                                ‹stixCommon:Relationship›Payload
```

```
delivery‹/stixCommon:Relationship›
                                ‹stixCommon:Indicator id=”TS:indicator-57a45838-
f254-4f28-bf11-201c5b86d7e5” timestamp=”2016-08-05T09:11:20+00:00”
xsi:type=’indicator:IndicatorType’›
                                    ‹indicator:Title›Payload delivery:
javascript.jslbf30f428575d4f02bc1194d28aa42ef5 (MISP Attribute
#335614)‹/indicator:Title›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›Malware Artifacts‹/indicator:Type›
                                    ‹indicator:Type
xsi:type=”stixVocabs:IndicatorTypeVocab-1.1”›File Hash Watchlist‹/indicator:Type›
                                    ‹indicator:Description›Payload delivery:
javascript.jslbf30f428575d4f02bc1194d28aa42ef5 (MISP Attribute
#335614)‹/indicator:Description›
                                    ‹indicator:Valid_Time_Position/›
                                    ‹indicator:Observable id=”TS:observable-
57a45838-f254-4f28-bf11-201c5b86d7e5”›
                                        ‹cybox:Object id=”TS:File-57a45838-f254-
4f28-bf11-201c5b86d7e5”›
                                            ‹cybox:Properties
xsi:type=”FileObj:FileObjectType”›
                                                ‹FileObj:File_Name
condition=”Equals”›javascript.js‹/FileObj:File_Name›
                                                ‹FileObj:Hashes›
                                                    ‹cyboxCommon:Hash›
                                                        ‹cyboxCommon:Type
condition=”Equals” xsi:type=”cyboxVocabs:HashNameVocab-1.0”›MD5‹/cyboxCommon:Type›
                                                        ‹cyboxCommon:Simple_Hash_Value
condition=”Equals”›bf30f428575d4f02bc1194d28aa42ef5‹/cyboxCommon:Simple_Hash_Value›
                                                    ‹/cyboxCommon:Hash›
                                                ‹/FileObj:Hashes›
                                            ‹/cybox:Properties›
                                        ‹/cybox:Object›
                                    ‹/indicator:Observable›
                                    ‹indicator:Confidence timestamp=”2016-08-
05T09:11:20+00:00”›
                                        ‹stixCommon:Value
xsi:type=”stixVocabs:HighMediumLowVocab-1.0”›High‹/stixCommon:Value›
                                        ‹stixCommon:Description›Derived from MISP’s
IDS flag. If an attribute is marked for IDS exports, the confidence will be high,
otherwise none‹/stixCommon:Description›
                                    ‹/indicator:Confidence›
                                ‹/stixCommon:Indicator›
                            ‹/incident:Related_Indicator›
```

```
            ‹/incident:Related_Indicators›
            ‹incident:History›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›Event Threat Level: High‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry time_precision=”second”›MISP
Tag: tlp:red‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›attribute[Internal reference][text]:
Acunetix‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›attribute[Internal reference][text]:
Netsparker‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›attribute[Internal reference][text]: China
Chopper‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›attribute[Internal reference][text]:
reGeorg‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›attribute[Internal reference][text]:
procdump.exe‹/incident:Journal_Entry›
              ‹/incident:History_Item›
              ‹incident:History_Item›
                ‹incident:Journal_Entry
time_precision=”second”›attribute[Internal reference][text]:
PsExec.exe‹/incident:Journal_Entry›
              ‹/incident:History_Item›
            ‹/incident:History›
            ‹incident:Information_Source›
              ‹stixCommon:Identity›
                ‹stixCommon:Name›TS‹/stixCommon:Name›
```

```
                            ‹/stixCommon:Identity›
                            ‹stixCommon:References›
‹stixCommon:Reference›https://github.com/sensepost/reGeorg‹/stixCommon:Reference›
‹stixCommon:Reference›https://github.com/Chora10/Cknife/blob/master/ReadMe.txt‹/stix
Common:Reference›
                            ‹/stixCommon:References›
                        ‹/incident:Information_Source›
                        ‹incident:Handling›
                            ‹marking:Marking›
                                ‹marking:Controlled_Structure›../../../descendant-
or-self::node()‹/marking:Controlled_Structure›
                                ‹marking:Marking_Structure
xsi:type=’tlpMarking:TLPMarkingStructureType’ color=”AMBER”/›
                            ‹/marking:Marking›
                        ‹/incident:Handling›
                    ‹/stix:Incident›
                ‹/stix:Incidents›
            ‹/stix:Package›
        ‹/stix:Related_Package›
    ‹/stix:Related_Packages›
‹/stix:STIX_Package›
```

Conclusions

5.1. CONCLUSIONS

Attacks such as Advanced Persistent Threat are becoming even more sophisticated. There is a growth of these phenomena in terms also of quality. If, at the beginning, the same attack was perpetrated against several targets, nowadays, as showed in ProjectSauron, the attackers avoid creating patterns that could be used to contrast the attack itself by targeted organizations.

Also the geographical areas of a single campaign are often limited to certain countries, implying specific intentions of attackers to collect information on regions or nations. The PLEAD APT has been observed to target Taiwan and has started since 2012.

The use of vast domain, server infrastructures dedicated to the targeted victim and ability to build custom tools evading anti-malware solutions are evidences that the attackers are well prepared and probably in some cases also sponsored by Nation-States.
The main objectives seem to be still espionage and this is also due to the growth of targeted attack market where organized crime units sell tool or complete attack services/packages. This doesn't imply that we could also see in the future a recrudescence of attacks that undermine the integrity of data.

The stealthy way in which APTs operate and the way in which they can bypass controls and anti-malware solutions, make a tough challenge for cyber security teams.
A study of Ponemon Institute shows how is difficult for Information Security departments to manage all the alerts they receive from their systems. In the interviewed organizations, 16.937 are the average alerts received from one organization during a week. Only the 19% were reliable and only the 4% investigated.
Private companies have to change their posture. They could not limit themselves to defend the perimeters. They have to strengthen their intelligence capabilities and their know-how, approaching also "grey

and dark internet areas", where attackers exchange information, tool and know-how.

This new posture should be ruled also by national policies. Nowadays, the private cyber intelligence departments that find databases, outcome from data-breach on the dark web, could not manage it or exfiltrate it because of the law restrictions, even if the databases could contain sensitive information on their organizations.
Law Enforcement Agencies could not monitor the entire web and a support in that terms could come from the private sector.

Even if, the attackers are smarter and they have started to avoid using the same tools, shells and so on, defenders could learn from previous modus operandi. They could assimilate techniques, tactics and procedures of attack to understand also how the attack could be modified, updated or improved. A lot of APTs have been built inspired from their predecessors.

Information sharing should be tailored in a way that is useful for operators. The time spent in order to acquire and analyze information should be faster than now. Standard like STIX, TAXII, YARA Rules should be learnt and understood from each operator.
Operators should know each other and start to trust each other too. The main pillar of information sharing is the trust. Without it, we can sign agreement, memorandum of understanding but that signature will remain written on water.

The Information Security Department should study from defense sector, building Cyber Defense Situational Awareness capabilities inside their organizations.
For that reason is vital also the collaboration with the Defense.

Also Awareness plays a relevant role in the information protection. Spear-phishing, use of cracked software, use of USBs out of policies, dissemination of information on social networks are common practices for employees and managers. These activities enlarge the attack surface and usually are the first entry point.

The efforts that should be put in place are still a lot. Internet of Things is augmenting the means for the attacks and also the target that could be attacked. The cyberspace is the battle domain in which the private public partnership should be stronger because the first line of defense will be even more the private sphere.

This publication aims to disseminate knowledge through high competencies, expressed by information security experts worldwide. The companies involved in this study have presented concrete cases they face during their daily activity.
We know that this study represents just a pebble, but putting together a multitude of pebbles we can build a dyke to defend our networks.

Authors

6.1. GCSEC

GCSEC
The Global Cyber Security Center (GCSEC) is a newly established not-for-profit organization created to advance cyber security in Italy, the region, and around the world. The Center, funded by Poste Italiane, is based in Rome with a strong collaboration with Italian and International government institutions, private bodies, research institutions and international bodies. The mission of the center is to develop and disseminate knowledge and awareness on Cyber Security, creating the conditions for improving capabilities, skills, cooperation and communication between the different stakeholders involved in the use and protection of Internet. In order to achieve these objectives, the Global Cyber Security Center will be a hub of cooperation and innovation where people of every country could meet and work together, sharing their knowledge and experience.

Elena Mena Agresti
Elena is a senior expert in information security and international standards and employed in the Information Security Department of Poste Italiane. She participated in technical committee responsible for reviewing and developing standards or guidelines for ISO and OECD. Elena was the Scientific Direct of Master in Cyber Security organized under the Cyber Security District of Poste Italiane and is Professor in several university masters dedicated to cyber security. She worked in Booz & Company in the Global Resilience practice and has competences in security governance, training and awareness, critical infrastructure protection, risk management, security auditing, policy development, privacy, process analysis and compliance.

Massimo Cappelli
Massimo is Planning Operations Manager in GCSEC and employed in the Information Security Department of Poste Italiane. He coordinates, as PMO, research and education activities of the foundation. In the previous experience, he assumed the role of Associate Expert in Risk Resilience and Assurance in Booz & Company (previous Booz Al-

len Hamilton). He participated as Advisor in NATO Industrial Advisory Group 179. He is PMO of several GCSEC projects.

Nicola Sotira
Nicola is the Director General of GCSEC and Information Security Manager in Poste Italiane. He works in the field of information security for over 20 years with experience in different international companies. Professor at the Master in Network Security of La Sapienza University of Rome, is Member of the Association for Computing Machinery. He is a promoter of technological innovation and was member of several startups in Italy and abroad.

6.2. KASPERSKY

Kaspersky Lab is a global cyber security company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Jose Selvi
Senior Security Researcher, Global Research & Analysis Team.
Jose joined Kaspersky Lab's Global Research & Analysis Team in 2016, where He focuses on Threat Intelligence, Research and Hacking Techniques analysis. Previously He has worked with several important security consultancies, running Penetration Testing services and Security Research projects around the world.
He has been working in the security industry for the last 13 years. During this period of time, He had the opportunity to work in different fields such as Intrusion Detection, Incident Response, Computer

Forensics and Penetration Testing. He is also a regular speaker in security conferences, including several tier-1 international conferences. Jose holds a BSc and MSc in Computer Engineering and a BSc in Telecommunications Engineering. He is a PhD candidate, focusing on Machine Learning techniques, and one of the few individuals that have earned the GSE certification from the SANS Institute / GIAC.

6.3. LUTECH

Lutech is the leader in the Italian market of Consulting, System Integration and Outsourcing, which designs, implements and manages innovative solutions in the ICT, supporting the Digital Transformation and the new business solutions for its Clients. Lutech works as a partner for innovation, providing its Customers with experience and expertise through an offer consisting of three business lines: Consulting, Solutions and Products, Services Among the ICT companies, Lutech is able to deliver services from the strategy definition until the operational management, with specific skills in the following domains: Customer Engagement, Enterprise Applications, Cloud, eHealth, Credit and Card Management, Cybersecurity, Datacenter, Networking, Internet of Things & Big Data, Cognitive Computing. Lutech works on national and international scale for more than 800 Customers on different business sectors: Financial Services, Telco & Media, Public Sector, eHealth, Energy & Utilities, Industry 4.0, Intelligence Solutions.

Francesco Faenzi
Head of Lutech Cybersecurity Business Platform, CISSP / GCIH / CISA / ITIL certified, Security Advisor since 1995, speaker in national events with GCSEC, CLUSIT, AbiLab, The Innovation Group, ANIMP, ANIPLA, founder of Lutech Threat Management Services for Cyber Threat Intelligence and Managed Detection & Response.

Alberto Pasotti
Lutech Cyber Threat Intelligence Team Leader, Cyber Threat Intelli-

gence Researcher & Developer, Incident Response Specialist, Cyber Security Senior Analyst, SCADA Cyber Security Practitioner, GCIH and ITIL certified.

Roberto Romano
Lutech Cyber Threat Intelligence Hactive-CTI™ Team Leader, Cyber Threat Intelligence Researcher & Developer, OSINT e HUMINT Specialist, Cyber Security Senior Analyst, Incident Response Specialist

6.4. TREND MICRO

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints.
Optimized for leading environments, including Amazon Web Services, Microsoft®, VMware®, and more, our solutions enable organizations to automate the protection of valuable information from today's threats. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection.
Trend Micro customers include 45 of the top 50 Fortune® Global 500 companies, and 100% of the top 10 global automotive, banking, telecommunications, and petroleum companies.
With over 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com

Razor Huang
Razor Huang mainly focuses on targeted attack research, malware analysis and cyber threat correlation. He has delivered presentations at AVAR and AVTOKYO and he has been responsible for virus scan engine development.

CH Lei
Malware analyst of TrendMicro, his job is investigating APT instance for TrendMicro customers.

Lenart Bermejo
Currently, Lenart does APT investigation as well as cyber threat reverse engineering. His research focuses both on targeted attack intelligence and threat solutions.

Benson Sy
Benson focuses on APT investigation and malware analysis. Currently, he creates pattern for malware hunting and monitors campaigns particularly in Asia region.

6.5. TIGER SECURITY

Tiger Security is an Italian company, leader in Cyber Intelligence and Unconventional Information Security. Our clients come from both Italy and abroad, and include those in the public sector (Government Organisations, Military and the Law Enforcement Agency) and the private sector (Enterprises in the critical infrastructure field). Tiger Security's mission is to identify, monitor and track cyber threats. We use an unconventional and innovative preventative approach, which guarantees a timely and strategic information framework for our clients, and elite support to contextualise cybernetic threats. In an environment where Cyber Intelligence and information security are of increasing importance, in terms of complexity, danger and the evolution of digital threats, Tiger Security's approach and value proposition stands as an extension of our client's risk management policy.

Authors
Tiger Security CIOC is an elite unit that works on the prediction, analysis and attribution of complex cyber threats, focusing especially on the technical and geopolitical details. The team's goal is to provide the customer organization with a detailed landscape about the

threats, the criticalities and the risks undermining its security, both on the technical and the executive side. Great care is taken on the analysis and correlation of different information sources in order to create a context for the threat, predict potential problems or mitigate their impact.