Trend Micro Incorporated
Research Paper
2012

IXESHE
An APT Campaign

By: David Sancho, Jessa dela Torre, Matsukawa Bakuei,
Nart Villeneuve, and Robert McArdle

CONTENTS

INTRODUCTION

The number of targeted attacks is undoubtedly on the rise. These highly targeted attacks focus on individual organizations in an effort to extract valuable information. In many ways, this is a return to the "old hacking days" before more widespread attacks targeting millions of users and the rise of computer worms came about. Sometimes, these targeted attacks are allegedly linked to state-sponsored activities but may also be carried out by individual groups with their own goals.

Trend Micro continues to track and analyze highly targeted attacks, also known as "advanced persistent threats (APTs)." We have, in fact, published two research papers on the Luckycat[1] and Lurid[2] campaigns. This research paper will delve into another prominent group of attackers referred to as "IXESHE" (pronounced "i-sushi"), based on one of the more common detection names security companies use for the malware they utilize. This campaign is notable for targeting East Asian governments, electronics manufacturers, and a German telecommunications company.

The IXESHE campaign makes use of targeted emails with malicious attachments to compromise victims' systems. The emails are often tailored for specific victims and contain malicious attachments that are almost always "weaponized" .PDF files with known exploits that drop malware executables onto targeted systems. In addition, the IXESHE attackers conducted two specific attacks that leveraged zero-day exploits—one in 2009 and another in 2011.

The IXESHE attackers almost always make use of compromised servers as command-and-control (C&C) servers. In some cases, the compromised servers are hosted on target organizations' networks after successful infiltration so the attackers can increase their control of the victims' infrastructure. Using this approach, the attackers amassed at least 60 C&C servers over time. This technique also allows the attackers to cover their tracks, as having the C&C server in the victims' corporate networks means very little C&C traffic leaves them. The attackers' deliberate use of compromised machines and dynamic Domain Name System (DNS) services allows them to hide traces of their presence by confusing their activities with data belonging to legitimate individuals.

Looking at threat intelligence derived from tracking APT campaigns over time primarily based on the network traffic generated by the malware used, we were able to develop indicators of compromise for the IXESHE campaign. The malware samples used in this campaign were not very complicated by nature but do give the attackers almost complete control over their targets' compromised systems.

Victims and Targets

Most of the IP addresses of IXESHE's victims are linked to DSL networks, which made it difficult to determine their identities. Careful research, however, allowed the identification of some of the attackers' victims:

- East Asian governments
- Taiwanese electronics manufacturers
- A German telecommunications company

Campaign victims were identified by using *Whois* records and open source research. Trend Micro generally notifies customers that are believed to have been specifically targeted by APT campaigns.

Context

The IXESHE attackers have been actively launching highly targeted attacks since at least July 2009.

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf
2 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf

TECHNICAL ANALYSIS

Attack Vectors

Available data on the IXESHE campaign indicates that targeted emails with malicious .PDF file attachments were the attackers' vector of choice. In most cases, the attacks involved *Adobe Acrobat, Reader,* and *Flash Player* exploits such as:

- *CVE-2009-4324*[3]
- *CVE-2009-0927*[4]
- *CVE-2011-0609*[5]
- *CVE-2011-0611*[6]

It should also be noted that this campaign used *CVE-2009-4324*[7] and *CVE-2011-0609*[8] exploits when these were still unpatched or considered zero-day vulnerabilities.

The IXESHE attackers also used an exploit that affected *Microsoft Excel–CVE-2009-3129.*[9]

Operations

The IXESHE malware binary allowed the attackers to easily take over and maintain complete control of victims' systems to do the following:

- List all services, processes, and drives
- Terminate processes and services
- Download and upload files
- Start processes and services
- Get victims' user names
- Get a machine's name and domain name
- Download and execute arbitrary files
- Cause a system to pause or sleep for a specified number of minutes
- Spawn a remote shell
- List all current files and directories

3 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324
4 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927
5 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609
6 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611
7 http://contagiodump.blogspot.com/2009/12/dec-18-adobe-0-day-cve-2009-4324-pdf.html
8 http://contagiodump.blogspot.ca/2011/03/cve-2011-0609-adobe-flash-player.html
9 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3129

Initial Delivery Method

Every IXESHE case we examined revealed that the original infection vector was a targeted email with a PDF exploit as attachment. Older versions also used an XLS exploit.

Opening the .PDF file drops and executes a malware in a victim's system. The malware displays a blank .PDF file or a decoy document related to the targeted attack. The emails normally come from compromised personal accounts or are entirely spoofed. Emails from spoofed senders were usually sent via mail servers in the United States and China.

Malware Local System Effects

Once dropped onto target systems by means of a document exploit attached to a tailored email, the malware drops an executable file into one of the following folders:

- *%APPDATA%\Locations*
- *%APPDATA%\Adobe*
- *%TEMP%*

The malware also sets the executable file's attributes to "Hidden." Some of the file names the attackers used include:

- *winhlps.exe*
- *acrotry.exe*
- *AcroRd32.exe*
- *Updater.exe*

In order for the malware to survive rebooting, it normally creates the following registry run key:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run
```

The registry run key, in turn, points to the malware that has been dropped. The value name of this entry varies from sample to sample. Some of the names the attackers used for it include:

- *Adobe Assistant*
- *Migrated*

Some samples, however, do not use a registry run key as load point. Some of the more recent samples we observed create a shortcut (i.e., .LNK file) in the *Startup* folder with names such as *adobe reader speed launch.lnk*.

The malware also checks a system's proxy settings for later use in C&C communications:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Internet Settings
  ProxyEnable
  ProxyServer
```

C&C Communications

Upon installation, the malware starts communicating with one of its C&C servers. Most of the samples appeared to have at least three C&C servers hard coded for redundancy. The C&C communications are easy to identify, as these tended to be coded in the following predetermined format:

```
http://[C&C Server]/[ACD] [EW]S[Some Numbers].
jsp?[Encrypted Base64 Blob]
```

Some samples alternatively use an *FGKD.jsp* or an *FPK.jsp* file.

The *Base64* blob is of particular interest. It makes use of a custom *Base64* alphabet. Once decoded, this blob reveals a standardized structure of the information sent to the registered C&C server, which includes the following details:

- Computer name
- Local IP address
- Proxy server IP and port
- Malware ID

To date, we have seen several custom *Base64* alphabets, including:

- +NO5RZaGHviljhYq8b4ndQ=p012ySTcCDrs/xPgUz67FM3wemKfkJLBo9VtWXIEuA
- HZa4vjliGndQ=p012y+NO5RST/xPgUz67FMhYq8b3wemKfkJLBocCDrs9VtWXIEu
- j4vpGZaHnldQ=i012y+N/zPgUO5RSTx67FMhYb8q3wemKckJLBofCDrs9VtWXIEu
- p12kJLBofCDrs9VtWXIEuainyj4vd+=H0GZIQNO5RST/zPgUx67FMhYb8q3wemKc
- aZHGvilj4ndQ=p012y+NO5RST/xPgUz67FMhYq8b3wemKfkJLBocCDrs9VtWXIEu
- ZvQlajHi4ndG=p012y+NO5RST/xPgUz67FMhYq8b3wemKfkJLBocCDrs9VtWXIEu
- ZaGHvilj4ndQ=p012y+NO5RST/xPgUz67FMhYq8b3wemKfkJLBocCDrs9VtWXIEu
- 4HlvZGjaiQdn=p012y+NO5RST/xPgUz67FMhYq8b3wemKfkJLBocCDrs9VtWXIEu
- pGIaHnZj0vdQ=i421y+NO5RSY/zMgUx67KPhTb8q3wemFckBLJufWErs9VtCXIDo
- QpaZIivj4ndG=H021y+NO5RST/xPgUz67FMhYq8b3wemKfkJLBocCDrs9VtWXIEu
- pGZaHnlj4vdQ=i012y+NO5RST/zPgUx67FMhYb8q3wemKckJLBofCDrs9VtWXIEu

Some similarities exist across different versions of the *Base64* alphabet, which indicates that these are most likely not completely randomly generated. Instead, the attackers manually cut and pasted older versions after altering some parts.

The malware ID seems to be a campaign code with a different IP address for each attack. Some of the campaign codes we have seen include:

- 19
- [0222]
- [0713]
- [0802]
- [CR1008]
- [CR1031]
- [CZ0312]
- [CZ0913]
- [CZ0921]
- [LY]MAIL_20090923
- [LY]MAIL_20091015
- [LY]MAIL_20091208
- [LY0406]
- [LY0420]
- [LY0816]
- [LY1207]
- [TL1109]
- [WH0827]
- [WH1122]
- [WL1013]
- [WZ1011]
- CRML_0505
- CRML_MIL
- Firebox4
- JUST_0525
- JUST_JP_6080
- KA_1016
- KS_0602
- KSX_0520
- LY_ML0430_30m
- ly0610
- MAIL_20091208
- MAIL_JAP_0220
- MAIL_JAP_0304
- MAIL_JAP_0325
- MAIL_JAP_0407
- MAIL0524
- manufact
- ML_20091223
- ML0419._30m
- ML0623.LINK_10m
- ML0628
- ML_20091216
- ML_20091223
- MW0629
- OM222
- sandbox
- sandbox4
- sandbox6
- success
- UNKNOWN
- wl0711
- ZWJP_KS_1222

It appears that the numbers in the given campaign codes refer to dates when the campaigns were launched in "MMDD" format. The letters are possibly related to the target industry or company.

If the malware does not get a response from the C&C server, it will choose another random number after the AWS part of the URL and try again.

Once connected, the malware specifically waits for the remote server to issue the following commands, which may vary from one version to another:

- ***del [parameter]:*** Allows a remote user to delete files.
- ***disk [parameter]:*** Lists all available drives.
- ***dos [parameter]:*** Allows a remote user to execute commands via *cmd.exe*.
- ***get [parameter]:*** Allows a remote user to download a file from the remote server onto a local machine.
- ***list [parameter]:*** Lists files on the victim's machine.
- ***ls [parameter]:*** Allows a remote user to display the contents of a directory.
- ***kill [parameter]:*** Allows a remote user to terminate processes.
- ***put [parameter]:*** Allows a remote user to upload a file from a local machine to a remote server.
- ***rsh [parameter]:*** Similar to the *sh* or *dos [parameter]* except for the fact that this is an already-existing file or shell.
- ***run [parameter]:*** Allows a remote user to execute programs.
- ***sh [parameter]:*** Allows a remote user to execute commands via *cmd.exe*.
- ***sleep [parameter]:*** Causes a system to sleep for a certain amount of time.

Related AES Campaign

We have also been tracking another campaign, which we refer to as the "AES campaign," which appears to be related to IXESHE. The main body of the malware related to the IXESHE campaign can be identified by its connection to a C&C server using a file such as *AWS12345.jsp* and a custom *Base64* blob; the malware associated with the AES campaign operates very similarly. The samples used in the AES campaign slightly differed in terms of C&C communication but had significant similarities with IXESHE malware, which used the format:

```
http://[C&C Server]/[ACD] ES[Some Numbers].jsp
```

Even though the network traffic format of the AES campaign was slightly similar, instead of the more familiar *AWS[random].jsp* format, it used several other formats for certain commands or events such as:

- AES: Initial beacon.
- DES: Send the path of *%systemdir%*.
- PES: Send the result of the "put" command.
- SEU: Send the "error" or "invalid" command.
- SUS: Send the system name, which is not encoded, upon receiving the "exit" command.
- ZES: Send the result of the "dos" command.

Another difference in the traffic is that AWS uses the POST method with the format, *"http://[C&C Server]/FPK [Some Numbers].jsp?[Base64 Blob],"* when the "get" command is invoked. The *Base64* blob contains the file specified in the "get" command.

Analysis of the binaries also revealed similarities between the AES and AWS samples. These included the encoding algorithm and commands used. Even though some commands varied, the format and parameters used essentially remained the same.

C&C INFRASTRUCTURE

The majority of the IXESHE campaign's C&C servers were based in Taiwan and the United States.

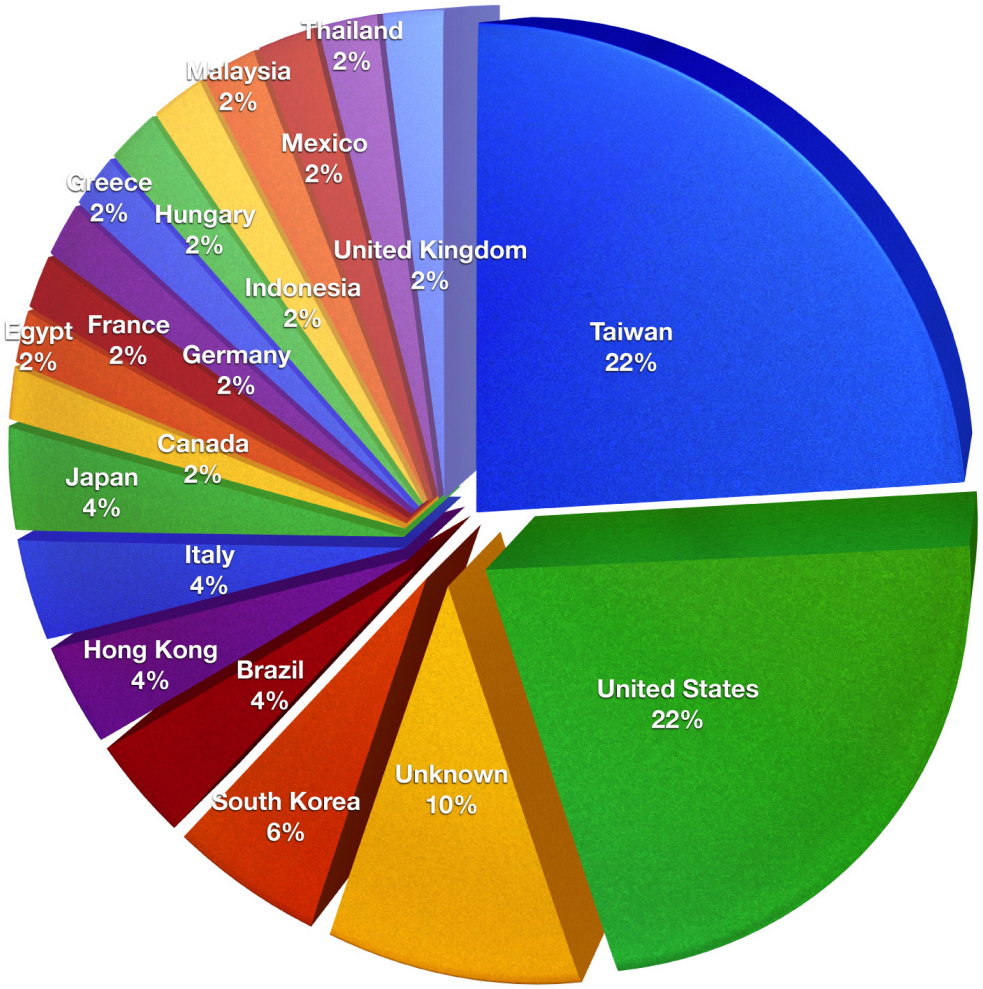

Figure 1. Breakdown of C&C servers by country

This is, however, not an indicator of attribution. It is not possible to determine where the attackers are based solely on where their C&C infrastructures are located. In addition, not all of the C&C servers are currently active. Many, if not all of them, appear to be compromised machines. In fact, at least 11 of the C&C servers were hosted on the compromised machines of an East Asian government, which made these very useful for launching targeted attacks against it.

Most of the malware samples directly accessed an IP address as a C&C server. Connections to domains did exist in some cases. The domains were usually registered using free dynamic DNS service providers or compromised websites.

Overall, this strategy was part of the attackers' modus operandi. By choosing compromised machines to act as C&C servers, fewer clues were left for investigators to follow in an attempt to find out who is behind the attacks compared with those using bulletproof hosting services and registered domain names. To conduct research on these servers, investigators need to differentiate between information related to malicious and legitimate use.

Real C&C Location

One very interesting error revealed more insights into the C&C network's setup. One of the malware samples we tested was designed to access *xxx.xxawan.com* via port 443, which, at that time, resolved to *xx.xxx.114.87:443,* a server located in the United States. The sample, however, received the following error message from the server:

```
[SERVER]connection to xx.xx.x2.202:56413 error
```

This indicated that the front-end servers actually functioned as proxy servers and that the true C&C servers were hidden behind this initial group of C&C servers. This made the network more resistant to takedown and analysis. Due to a server error, however, the attackers revealed the location of one of their back-end servers. We discovered that the IP address, *xx.xx.x2.202,* is located in Guangdong, China.

The particular error returned looked very similar to errors generated by a tool called *"HTran."*[10] *HTran* stands for *"HUC Packet Transmit Tool,"* a connection bouncer that redirects TCP traffic destined for one host to an alternate host, keeping the real host hidden from view. "HUC," in this case, stands for the hacking group, "Honker Union of China." It was coded by a hacker who goes by the handle "lion." This tool's error-checking code, however, is flawed. Assuming that everything properly works, the tool functions very well as a proxy server but if the real server is currently inaccessible, *HTran* will send an error message, revealing its whereabouts.

Running a port scan on this server revealed some open ports shown in the table below.

Port	State	Service
80/tcp	Open	HTTP
8080/tcp	Open	HTTP Alternative

Based on OS fingerprinting, the server appears to be running *Windows 7 Enterprise Server.* With only a few open ports, however, it was very difficult to confirm this. In addition, we did not receive a response when we tried to connect to these ports.

10 http://www.secureworks.com/research/threats/htran/

ATTRIBUTION AND UNIQUE FINGERPRINTS

Previous research on the IXESHE campaign indicated several connections to groups possibly from China. In addition, the IP address hiding behind the *HTran* instance was an IP range assigned to China.

Upon further investigation of the "manufact" campaign, however, it appears that the gang behind it may be English speakers. The name of the campaign, for one, is most likely a shortened form of "manufacturing." The OS the C&C server uses is also an English install of *Microsoft XP*. It is also likely, of course, that the C&C server is a compromised machine so it does not use the attackers' first language.

The malware samples, which appear to have been developed using *C++*, had a number of strings and error codes in English such as "Enter command" and "Receive command error!"

The date format used in the campaign codes (i.e., MMDD) also provided us a clue as to where the attackers may be from. This date format is only commonly used in China, Korea, Iran, Japan, Hungary, Lithuania, and the United States.

Based on the limited amount of information we gathered about the attackers, it was very difficult to pinpoint their exact location.

Unique Fingerprints and Modus Operandi

An attack can be considered associated with the gang behind the IXESHE campaign if it exhibits the following characteristics:

- Uses a specially crafted targeted email with a malicious file attachment
- Uses document exploits, primarily .PDF files, to drop malware into target systems
- Uses malware detected by security vendors as IXESHE variants
- Uses a malware that sends a GET request to the C&C server in the following format:

```
http://[C&C Server]/[ACD] [EW]S[Some
Numbers].jsp?[Encrypted Base64 Blob]
```

- Uses dynamic DNS services for or compromised machines as C&C servers

RELATIONSHIPS BETWEEN ATTACK COMPONENTS

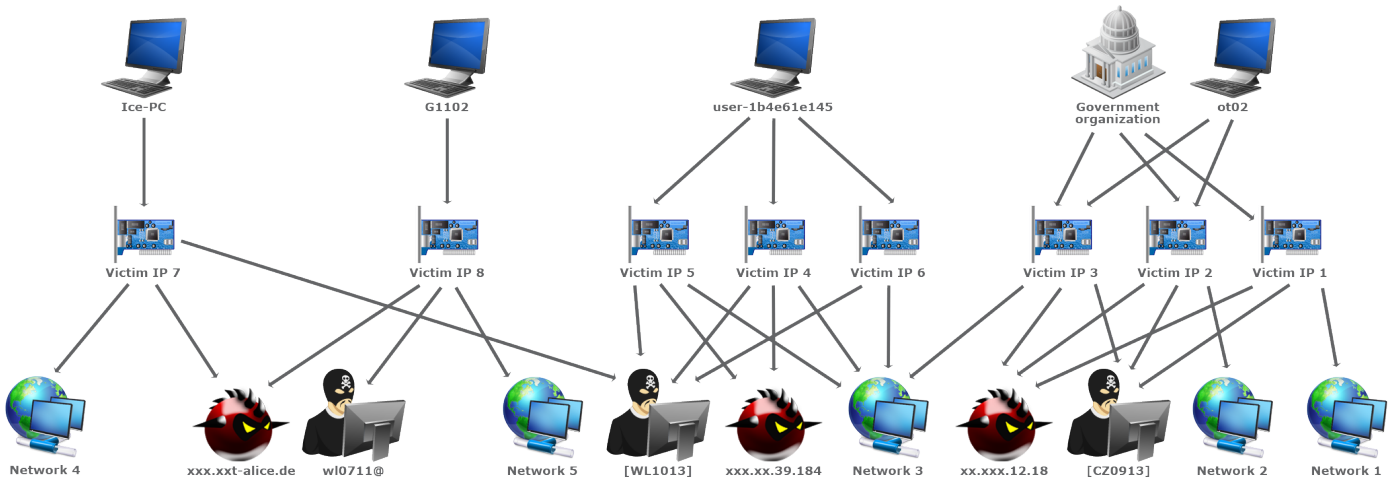

Figure 2. IXESHE targeted campaign #1

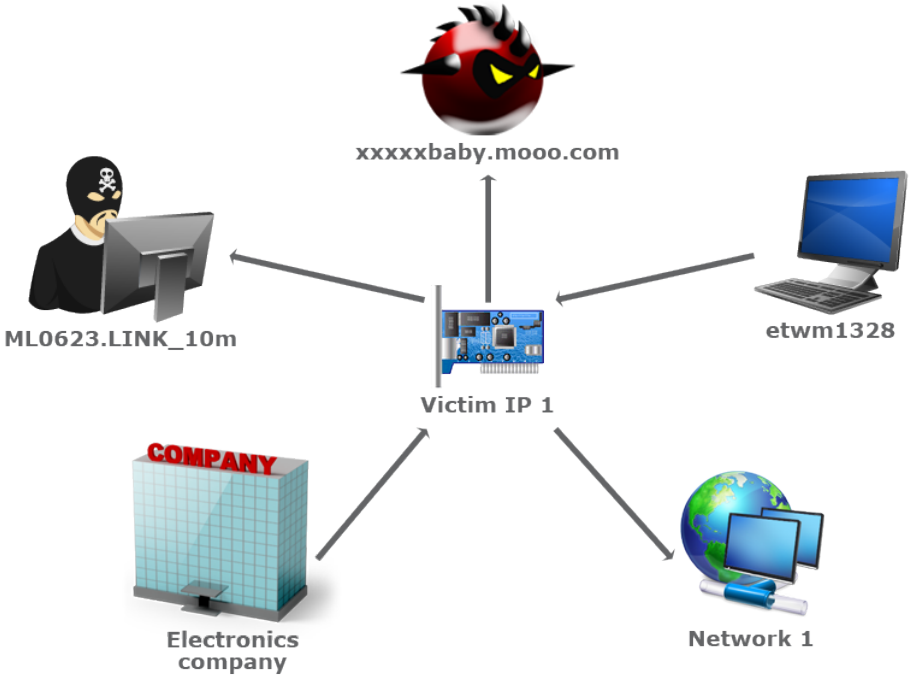

Figure 3. IXESHE targeted campaign #2

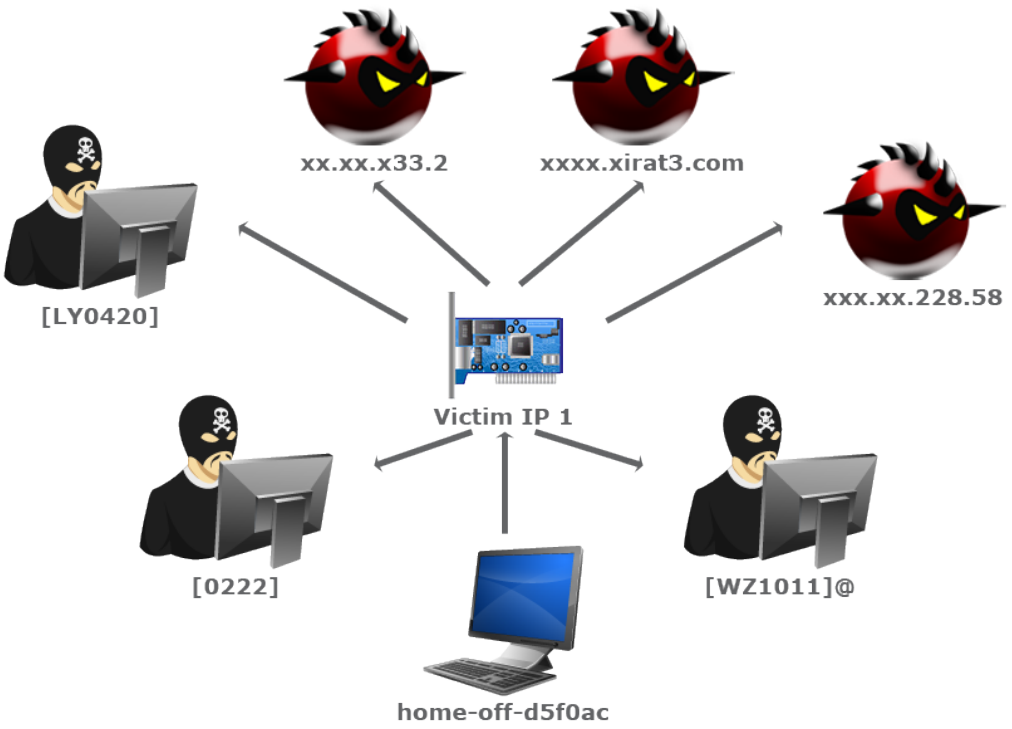

Figure 4. IXESHE targeted campaign #3

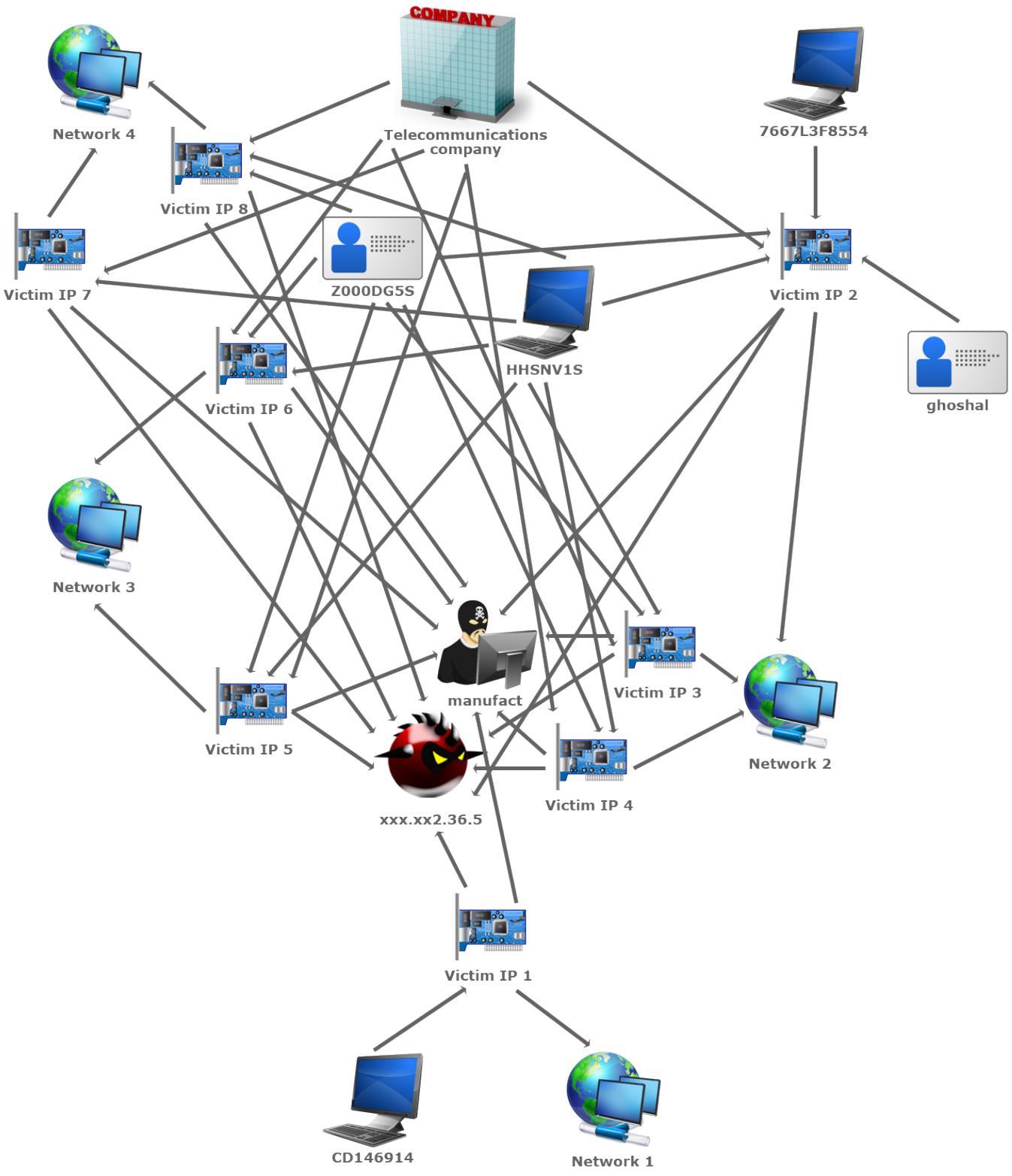

Figure 5. IXESHE targeted campaign #4

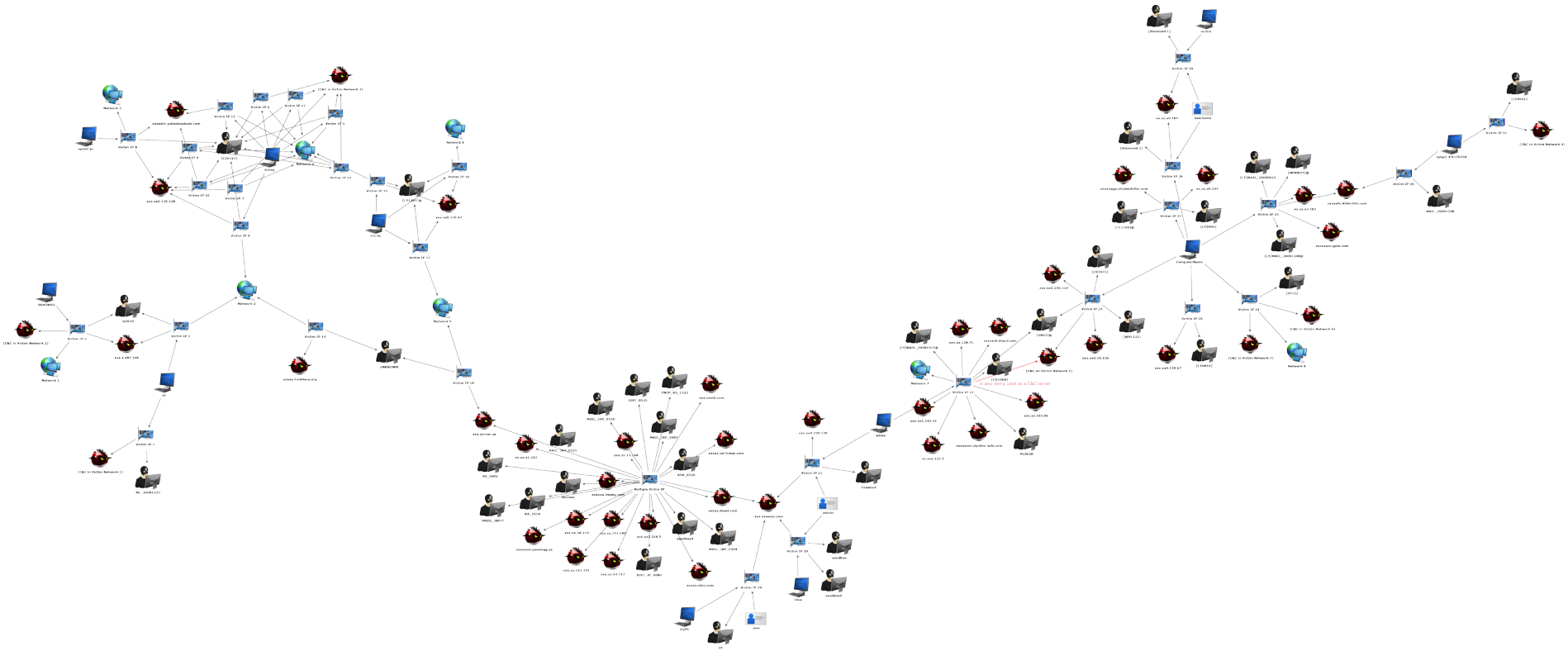

Figure 6. IXESHE targeted campaign #5

TIMELINE

This section lists known incidents exhibiting the same threat actor behaviors and so may be from the same group behind IXESHE dating to as far back as July 2009. With the exception of the samples described in *ContagioDump*, the dates for other samples refer to when the respective sandboxes saw them for the first time. As such, these dates should be considered "at least by" and not the actual date of the attack.

- 15 October 2009
  - PDF name/Subject hook: 中共二炮部隊導彈之發展
  - MD5: 16a9f340c0d353332ba6f525376c93e1
  - C&C: xxxxxupsenter.byinter.net
  - Info: http://contagiodump.blogspot.com/2009/12/oct-15-2009-attack-of-day-development.html
  - Campaign code: [LY]MAIL_20091015

- 18 December 2009
  - PDF name/Subject hook: 女兵脫衣比中指 拍照PO上網
  - MD5: 8950bbedf4a7f1d518e859f9800f9347
  - C&C: xxxxxfo.athersite.com
  - Info: http://contagiodump.blogspot.com/2009/12/dec-18-adobe-0-day-cve-2009-4324-pdf.html
  - Campaign code: ML_20091216

- 28 December 2009
  - PDF name/Subject hook: Consumer Welfare Table
  - MD5: c61c231d93d3bd690dd04b6de7350abb
  - C&C: xxx.xx6.148.42 or xxx.xx6.202.49
  - Info: http://contagiodump.blogspot.com/2009/12/dec-29-cve-2009-4324-adobe-0-day.html
  - Campaign code: ML_20091223

- 26 April 2010
  - **PDF name/Subject hook:** [研討會]開南大學公共事務管理學系第五屆「全球化與行政治理」國際學術研討會
  - **MD5:** 58de08c1155a775b760049dff3f5abe4
  - **C&C:** xxx.x.x5.26
  - **Info:** http://contagiodump.blogspot.com/2010/04/apr-26-cve-2009-4324-w-low-detection.html
  - **Campaign code:** ML0419._30m

- 6 May 2010
  - **PDF name/Subject hook:** 蔡政文教授七十華誕系列活動簡報
  - **MD5:** d80eb21cfe8ad1a710c8652b13f8b7ac
  - **C&C:** xxx.xx9.124.13
  - **Info:** http://contagiodump.blogspot.com/2010/05/may-6-cve-2010-0188-pdf-birthday.html
  - **Campaign code:** LY_ML0430_30m

- 10 May 2010
  - **XLS name/Subject hook:** 99下半年國防工業評鑑日期表
  - **MD5:** d4b98bda9c3ae0810a61f95863f4f81e
  - **C&C:** xxxxx.compreautos.com.br
  - **Info:** http://contagiodump.blogspot.com/2010/06/may-10-cve-2009-3129-xls-schedule-of.html
  - **Campaign code:** CRML_0505

- 8 June 2010
  - **XLS name/Subject hook:** 天安艦後的朝鮮半島新局勢
  - **MD5:** 100cf902ac31766f7d8a521eeb6f8d68
  - **C&C:** xxx.xx.187.130
  - **Info:** http://contagiodump.blogspot.com/2010/06/jun-8-cve-2009-4324-korean-peninsula.html
  - **Campaign code:** MAIL0524

- 27 June 2010
  - **PDF name/Subject hook:** Discussion on Cross-Strait Maritime Cooperation
  - **MD5:** 6e14c7a424c2eef7f37810ff65650837
  - **C&C:** xxx.xx.128.71
  - **Info:** http://contagiodump.blogspot.com/2010/07/jun-27-cve-2009-0927-pdf-discussion-on.html
  - **Campaign code:** ML0628

- 1 July 2010
  - **PDF name/Subject hook:** 第五次江陳會談成果記者會本會賴主委講話稿
  - **MD5:** 949265ee1d3e587152a23311a85b3be9
  - **C&C:** xxx.xx.128.71
  - **Info:** http://contagiodump.blogspot.com/2010/07/jul-01-cve-2009-4324-results-of-press.html
  - **Campaign code:** ML0628

- 28 July 2010
  - **PDF name/Subject hook:** Summary of Network Intelligence
  - **MD5:** 738af108a6edd46536492b1782589a04
  - **C&C:** xxx.xx6.54.189
  - **Info:** http://contagiodump.blogspot.com/2010/08/jul-28-cve-2009-4324-pdf-990729-romance.html
  - **Campaign code:** [0713]

- 16 August 2010
  - **PDF name/Subject hook:** Communist China Removes Missiles
  - **MD5:** 6227e1594775773a182e1b631db5f6bb
  - **C&C:** xxxxxck.dnsrd.com or xxx.xx6.34.94 (appears to be a compromised computer of an East Asian university)
  - **Info:** http://contagiodump.blogspot.com/2010/08/cve-2009-4324-cve-2010-1297-communist.html
  - **Campaign code:** [0802]

- 17 August 2010
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 36ee61663fc41496642850c4293fed01
  - **C&C:** xxxxxck.dnsrd.com or xxx.xx6.34.94 (appears to be a compromised computer of an East Asian university)
  - **Info:** http://www.threatexpert.com/report.aspx?md5=36ee61663fc41496642850c4293fed01
  - **Campaign code:** [0802]

- 27 September 2010
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 313158192d4442013f7bedeb9def01ec
  - **C&C:** xx.xx.x3.102
  - **Info:** http://www.threatexpert.com/report.aspx?md5=313158192d4442013f7bedeb9def01ec
  - **Campaign code:** [WH0827]

- 22 February 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** cd0eb6634ea684313389ddce553a6130
  - **C&C:** xxx.xx.228.58
  - **Info:** http://xml.ssdsandbox.net/view/cd0eb6634ea684313389ddce553a6130
  - **Campaign code:** [0222]

- 17 March 2011
  - **XLS name/Subject hook:** Japan Nuclear Radiation Leakage and Vulnerability Analysis
  - **MD5:** 7ca4ab177f480503653702b33366111f
  - **C&C:** xx.xxx.114.44
  - **Info:** http://contagiodump.blogspot.com/2011/03/cve-2011-0609-adobe-flash-player.html
  - **Campaign code:** OM222

- 10 April 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 711542d883f8fca4aeac62ee1b7df6ca
  - **C&C:** xx.xx.x0.244
  - **Info:** http://www.threatexpert.com/report.aspx?md5=711542d883f8fca4aeac62ee1b7df6ca
  - **Campaign code:** [LY0406]

- 20 April 2011
  - **PDF name/Subject hook:** China's Charm Diplomacy in BRICS Summit
  - **MD5:** ae39b747e4fe72dce6e5cdc6d0314c02
  - **C&C:** xx.xx.x9.165
  - **Info:** http://contagiodump.blogspot.com/2011/04/apr-20-cve-2011-0611-pdf-swf-chinas.html
  - **Campaign code:** [Removed due to privacy concerns]

- 20 April 2011
  - **PDF name/Subject hook:** The Obama Administration and the Middle East
  - **MD5:** 2368a8f55ee78d844896f05f94866b07
  - **C&C:** xx.xx.x9.165
  - **Info:** http://contagiodump.blogspot.com/2011/04/apr-20-cve-2011-0611-pdf-swf-chinas.html
  - **Campaign code:** {Removed due to privacy concerns]

- 20 April 2011
  - **PDF name/Subject hook:** Russia's profit from general NATO disunity
  - **MD5:** 4065b98fdcb17a081759061306239c8b
  - **C&C:** xx.xx.x9.165
  - **Info:** http://contagiodump.blogspot.com/2011/04/apr-20-cve-2011-0611-pdf-swf-chinas.html
  - **Campaign code:** [Removed due to privacy concerns]

- 22 April 2011
  - **PDF name/Subject hook:** Marshall Plan for the North Africa
  - **MD5:** 6d5fb801b890bfa7cc737c018e87e456
  - **C&C:** xx.xx.x9.165
  - **Info:** http://contagiodump.blogspot.com/2011/04/apr-22-cve-2011-0611-pdf-swf-marshall.html
  - **Campaign code:** [Removed due to privacy concerns]

- 28 April 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 14bf72167b4e801da205ecf9c0c55f9b
  - **C&C:** xx.xx.x33.2
  - **Info:** http://xml.ssdsandbox.net/view/14bf72167b4e801da205ecf9c0c55f9b
  - **Campaign code:** [LY0420]

- 1 June 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 6ee4e08e6ab51208757fdc41d0e72846
  - **C&C:** xxxxxain.qpoe.com
  - **Info:** http://www.threatexpert.com/report.aspx?md5=6ee4e08e6ab51208757fdc41d0e72846
  - **Campaign code:** [LY]MAIL_20090923

- 9 June 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 10f193f825ada183fcfd067434ca269e
  - **C&C:** xxxxxfo.AtHerSite.com
  - **Info:** http://www.threatexpert.com/report.aspx?md5=10f193f825ada183fcfd067434ca269e
  - **Campaign code:** [LY]MAIL_20091208
- 21 September 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 32522cdc17a145486e26f35bdd524e7e
  - **C&C:** xxx.xx0.139.67
  - **Info:** http://www.threatexpert.com/report.aspx?md5=32522cdc17a145486e26f35bdd524e7e
  - **Campaign code:** [LY0816]

- 12 October 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 8718ab5c1683a69c4e6092fdcb32cfa2
  - **C&C:** xxx.xx0.63.1
  - **Info:** http://www.malware-control.com/statics-pages/8718ab5c1683a69c4e6092fdcb32cfa2.php
  - **Campaign code:** [CZ0921]

- 19 October 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 80dad66d6224d18babd9ada4a26aee75
  - **C&C:** xx.xxx.21.41 or king.pirat3.com
  - **Info:** http://xml.ssdsandbox.net/view/80dad66d6224d18babd9ada4a26aee75
  - **Campaign code:** [WZ1011]

- 26 October 2011
  - **PDF name/Subject hook:** The Future Redefined 2011 AOEC CEO Summit
  - **MD5:** 3d91d9df315ffeb9bb1c774452b3114b
  - **C&C:** xxx.xxawan.com or xxx.xx4.230.120
  - **Info:** http://www.kahusecurity.com/2011/apec-spearphish-2/
  - **Campaign code:** 19

- 3 November 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** E25DBA0556124D7874D8416DE291CFE2
  - **C&C:** xxxxxfo.sdti.tw or xxx.xx2.246.110
  - **Info:** http://www.threatexpert.com/report.aspx?md5=e25dba0556124d7874d8416de291cfe2
  - **Campaign code:** [CR1031]

- 15 November 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** 829b78f1d1e74c2c5343a0aebb51f519
  - **C&C:** xxxxxaga.chickenkiller.com
  - **Info:** http://www.threatexpert.com/report.aspx?md5=829b78f1d1e74c2c5343a0aebb51f519
  - **Campaign code:** [TL1109]

- 22 November 2011
  - **PDF name/Subject hook:** [Unknown]
  - **MD5:** c4a05230a898d91b30c88d52b3f069b3
  - **C&C:** xxx.xx6.54.150 or xxxxx.ItemDB.com
  - **Info:** http://www.threatexpert.com/report.aspx?md5=c4a05230a898d91b30c88d52b3f069b3
  - **Campaign code:** [WH1122]

CONCLUSION

The IXESHE campaign has been successfully executing targeted attacks since 2009. The attackers primarily use malicious .PDF files that exploit vulnerabilities in *Adobe Reader, Acrobat,* and *Flash Player,* including the use of two zero-day exploits—one in 2009 and another in 2011. While the attackers primarily targeted East Asian governments in the past, they have also started targeting a telecommunications company and electronics manufacturers. They kept track of their targeted attacks by embedding a "campaign tag" in the malware that appears to describe when each attack was launched and, in some cases, the nature of its target. We found more than 40 of these campaign tags.

The IXESHE attackers are notable for their use of compromised machines within a target's internal network as C&C servers. This helped disguise their activities. In addition, the attackers' use of the proxy tool, *HTran,* also helped mask their true location. While their identities remain unknown, the attackers behind the IXESHE campaign demonstrated that they were both determined and capable. While the malware used in the attacks were not very complicated by nature, these proved very effective. This campaign remains an active threat.

DEFENDING AGAINST APTS

Sufficiently motivated threat actors can penetrate even networks that use moderately advanced security measures. As such, apart from standard and relevant attack prevention measures and mechanisms such as solid patch management; endpoint and network security; firewall use; and the like, enterprises should also focus on detecting and mitigating attacks. Moreover, data loss prevention (DLP) strategies that identify the data an organization is protecting and take into account the context of data use should be employed.

Local and External Threat Intelligence

Threat intelligence refers to indicators that can be used to identify the tools, tactics, and procedures threat actors engaging in targeted attacks utilize. Both external and local threat intelligence is crucial for developing the ability to detect attacks early. The following are the core components of this defense strategy:

- **Enhanced visibility:** Logs from endpoint, server, and network monitoring are an important and often underused resource that can be aggregated to provide a view of the activities within an organization that can be processed for anomalous behaviors that can indicate a targeted attack.

- **Integrity checks:** In order to maintain persistence, malware will make modifications to the file system and registry. Monitoring such changes can indicate the presence of malware.

- **Empowering the human analyst:** Humans are best positioned to identify anomalous behaviors when presented with a view of aggregated logs from across a network. This information is used in conjunction with custom alerts based on the local and external threat intelligence available.

Technologies available today such as *Deep Discovery* provide visibility, insight, and control over networks to defend against targeted threats.[11] *Deep Discovery* uniquely detects and identifies evasive threats in real time and provides in-depth analysis and actionable intelligence to prevent, discover, and reduce risks.

11 http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/index.html

Mitigation and Cleanup Strategy

Once an attack is identified, the cleanup strategy should focus on the following objectives:

- Determine the attack vector and cut off communications with the C&C server.
- Determine the scope of the compromise.
- Assess the damage by analyzing the data and forensic artifacts available on compromised machines.

Remediation should be applied soon afterward, which includes steps to fortify affected servers, machines, or devices into secure states, informed in part by how the compromised machines were infiltrated.

Educating Employees Against Social Engineering

Security-related policies and procedures combined with education and training programs are essential components of defense. Traditional training methods can be fortified by simulations and exercises using real spear-phishing attempts sent to test employees. Employees trained to expect targeted attacks are better positioned to report potential threats and constitute an important source of threat intelligence.

Data-Centric Protection Strategy

The ultimate objective of targeted attacks is to acquire sensitive data. As such, DLP strategies that focus on identifying and protecting confidential information are critical. Enhanced data protection and visibility across an enterprise provides the ability to control access to sensitive data as well as monitor and log successful and unsuccessful attempts to access it. Enhanced access control and logging capabilities allow security analysts to locate and investigate anomalies, respond to incidents, and initiate remediation strategies and damage assessment.

TREND MICRO THREAT PROTECTION AGAINST IXESHE CAMPAIGN COMPONENTS

The following table summarizes the Trend Micro solutions for the components of the IXESHE campaign. Trend Micro recommends a comprehensive security risk management strategy that goes further than advanced protection to meet the real-time threat management requirements of dealing with targeted attacks.

Attack Component	Protection Technology	Trend Micro Solution
Predetermined C&C communication format: `http://[C&C Server]/[ACD] [EW]S[Some Numbers].jsp?[Encrypted Base64 Blob]`	Web Reputation	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*
TROJ_PIDIEF, BKDR_PROXY, TROJ_DROPR, and TROJ_DEMTRANC variants	File Reputation (Antivirus/Anti-malware)	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*
CVE-2009-4324 *CVE-2009-0927* *CVE-2011-0609* *CVE-2011-0611* *CVE-2009-3129*	Vulnerability Shielding/Virtual Patching	Server *(Deep Security)* Endpoint *(OfficeScan with Intrusion Defense Firewall Plug-In)* For *CVE-2009-4324:* • Rule #1004008 *(Adobe Reader* and *Acrobat* 'newplayer()' JavaScript Method Code Execution) For *CVE-2009-0927:* • Rule # 1003405 *(Adobe Acrobat* JavaScript getIcon Method Buffer Overflow) For *CVE-2011-0609:* • Rule #1004615 *(Adobe Flash Player* XLS Remote Code Execution) For *CVE-2011-0611:* • Rule # 1004647 (Restrict *Microsoft Office* File with Embedded SWF) For *CVE-2009-3129:* • Rule #1003817 *(Excel* Featheader Record Memory Corruption Vulnerability)

Attack Component	Protection Technology	Trend Micro Solution
xxx.x.x87.206 *xxx.xx2.36.5* *xxx.xx6.129.228* *xxx.xx0.139.67* *xxx.xx.39.184* *xx.xxx.12.18* *xxx.xxrver.us* *xxx.xxt-alice.de* *xxxxxbaby.mooo.com* *xxxxxlic.yahoobigdeals.com* *xx.xx.x1.252* *xxx.xx.228.58* *xxx.xx.183.86* *xxx.xx.128.71* *xxx.xx.13.148* *xxx.xx5.243.44* *xxx.xx2.216.5* *xxx.xx.151.190* *xxx.xx.63.113* *xxx.xx.58.110* *xxx.xx.111.151* *xxx.xx6.54.150* *xxx.xx4.230.120* *xxx.xx0.139.67* *xxx.xx2.246.110* *xx.xxx.223.3* *xx.xx.x3.102* *xx.xx.x9.165* *xx.xx.x0.244* *xx.xx.x33.2* *xxxxxa.2waky.com* *xxx.xxawan.com* *xxxxxmic.dyndns-wiki.com* *xxxxxain.qpoe.com* *xxx.xxrver.us* *xxxxxfo.AtHerSite.com* *xxxxxem.passingg.as* *xxx.xxset.com* *xxxxx.dnset.com* *xxxx.xirat3.com* *xxxxxaga.chickenkiller.com* *xxxxx.otzo.com* *xxxxxck.dnsrd.com* *xxxxx.portrelay.com* *xxxxx.FindHere.org*	Web, Domain, and IP Reputation	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*

Advanced persistent threats (APTs) refer to a category of threats that aggressively pursue and compromise specific targets to maintain persistent presence within the victim's network so they can move laterally and exfiltrate data. Unlike indiscriminate cybercrime attacks, spam, web threats, and the like, APTs are much harder to detect because of the targeted nature of related components and techniques. Also, while cybercrime focuses on stealing credit card and banking information to gain profit, APTs are better thought of as cyber espionage.

IXESHE

First Seen

Individual targeted attacks are not one-off attempts. Attackers continually try to get inside the target's network.

The IXESHE campaign has been actively staging targeted attacks since at least July of 2009.

Victims and Targets

APT campaigns target specific industries or communities of interest in specific regions.

IXESHE has been found to target electronics manufacturers, a German telecommunications company, and East Asian governments.

Operations

First-stage computer intrusions often use social engineering. Attackers custom-fit attacks to their targets.

IXESHE attacks used custom-fit targeted emails with PDF exploits for *CVE-2009-4324*, *CVE-2009-0927*, *CVE-2011-0609*, and *CVE-2011-0611*. These were used to drop malicious executable files that gave the attackers complete control of their targets' systems.

The attackers used either dynamic Domain Name System (DNS) or compromised servers hosted on networks that they previously successfully infiltrated.

Possible Indicators of Compromise

Attackers want to remain undetected as long as possible. A key characteristic of these attacks is stealth.

» Enters networks via a specially crafted, targeted email with a malicious file attachment

» Uses document exploits (primarily PDF exploits) to drop malware onto target systems

» Uses malware detected as IXESHE by security companies

» Sends a GET request to the command-and-control (C&C) server with the format:

```
http://[C&C Server]/[ACD] [EW]S[Some Numbers].jsp?[Encrypted Base64 Blob]
```

* The campaign codes we have seen so far are detailed in the Trend Micro research paper, "IXESHE: An APT Campaign." The characteristics highlighted in this APT campaign quick profile reflect the results of our investigation as of May 2012.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

Securing Your Journey to the Cloud