Targeted Attack Trends in Asia-Pacific

A TrendLabs℠ Report

TREND MICRO™

CONTENTS

INTRODUCTION

Targeted attacks or threats that compromise specifically chosen targets to steal confidential information can affect organizations in various ways, ranging from brand damage to actual revenue loss. A recent Harvard Business Review study revealed that the top 3 effects of targeted attacks were potential brand damage, damage to professional reputation, and potential loss of intellectual property.[1]

We continued to monitor targeted attack campaigns and trends in the Asia-Pacific region in the first half of 2014. We saw technique enhancements even though threat actors continued to exploit old vulnerabilities in various software and applications. Emails were still the most-used infection vector when instigating targeted attacks. Watering-hole attacks were also seen, just as we predicted would happen this year.[2]

> No one-size-fits-all solution exists when dealing with targeted attacks. Every network is different, which means each is configured differently. IT administrators need to fully understand the networks they manage and implement the necessary defense measures that fit their environments.
>
> —Spencer Hsieh, *Threat Researcher*

THREAT LANDSCAPE

REFINED TARGETED ATTACK TACTICS TO BETTER EVADE DETECTION

One of the primary goals of targeted attacks is to exfiltrate organizations' crown jewels or confidential company data. Based on the previously cited Harvard Business Review study, the most commonly stolen types of data were personally identifiable information (PII) (28%), authentication credentials (21%), intellectual property (20%), and other sensitive corporate/organizational data (16%).

In the first haft of 2014, threat actors continued to refine their tactics to stay under the radar while stealing information. The following are just some of the notable techniques they used:

- **Cloud-based file storage platform abuse:** This June, threat actors used a Type II PlugX remote access tool (RAT) variant to be able to use Dropbox as a download site for a backdoor's command-and-control (C&C) settings.[3] Abusing the cloud-based file storage platform allowed threat actors to better evade detection despite the implementation of network traffic monitoring. Even though this was not the first time attackers abused Dropbox, it was the first time we saw them use the platform as an update download site for their backdoor's C&C settings.[4]

- **Windows® PowerShell framework abuse:** Abusing the Windows PowerShell task automation and configuration management framework is not a commonly seen targeted attack technique.[5] But in a case seen this May, a malicious .LNK file email attachment we detect as LNK_PRESHIN.JTT had Windows PowerShell commands that enabled it to download files and bypass execution policies to execute the files downloaded.[6] It particularly downloaded another malicious PowerShell scripting file that downloaded the final backdoor payload.

  Even though the PowerShell framework is only available on computers running Windows 7 and newer OSs, the malware used in the attack also ran on computers running older OSs such as Windows XP SP2, Windows Server 2003, and Windows Vista, if these had PowerShell installed.

- **Sleep timer feature abuse:** Apart from legitimate platform and framework abuse, we also saw a backdoor take advantage of built-in OS features such as sleep timer in the Siesta Campaign.[7] The said backdoor could accept a sleep command that allowed it to remain dormant for varying periods of time before regaining access to C&C servers, most likely to evade detection.

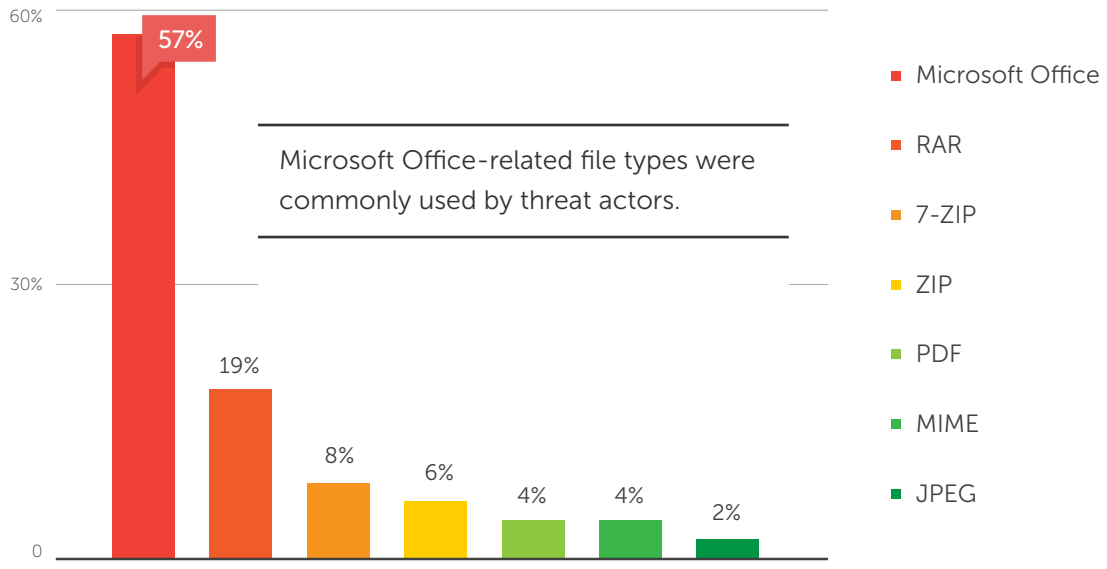
SPEAR-PHISHING EMAILS, STILL MOST FAVORED NETWORK INFILTRATORS

Most of the targeted attacks seen in the region during the first half of 2014 used spear-phishing emails as infection vector. In fact, almost 80% of the targeted attack malware arrived via email. Typically sent to employees in target organizations, spear-phishing emails convince recipients to either click a malicious link or download and execute a malicious file. Contextually relevant subjects are always used. One such attack used news of Lao People's Democratic Republic's Deputy Prime Minister's death as lure.[8] It bore the subject, "BREAKING: Plane Crash in Laos Kills Top Government Officials."

The spear-phishing email used in this attack, as in similar ones, had a file attachment that served as malware carrier. Apart from spear-phishing emails, threat actors also compromise websites via watering-hole techniques to get in to their target networks. A typical watering-hole attack involves three basic steps—guessing what websites targets frequently visit, infecting these with malware, and waiting for targets to visit them and infect their computers—essentially triggering the targeted attack cycle.[9]

MICROSOFT OFFICE FILES USED AS ATTACHMENTS

Data from the first half of 2014 shows that Microsoft Office files are the most commonly used attachments. This is not a surprise, as these are widely used within any type of organization. In addition, many organizations are not able to regularly patch or upgrade their versions of Microsoft Office, leaving many exploitable vulnerabilities for an attacker to target.

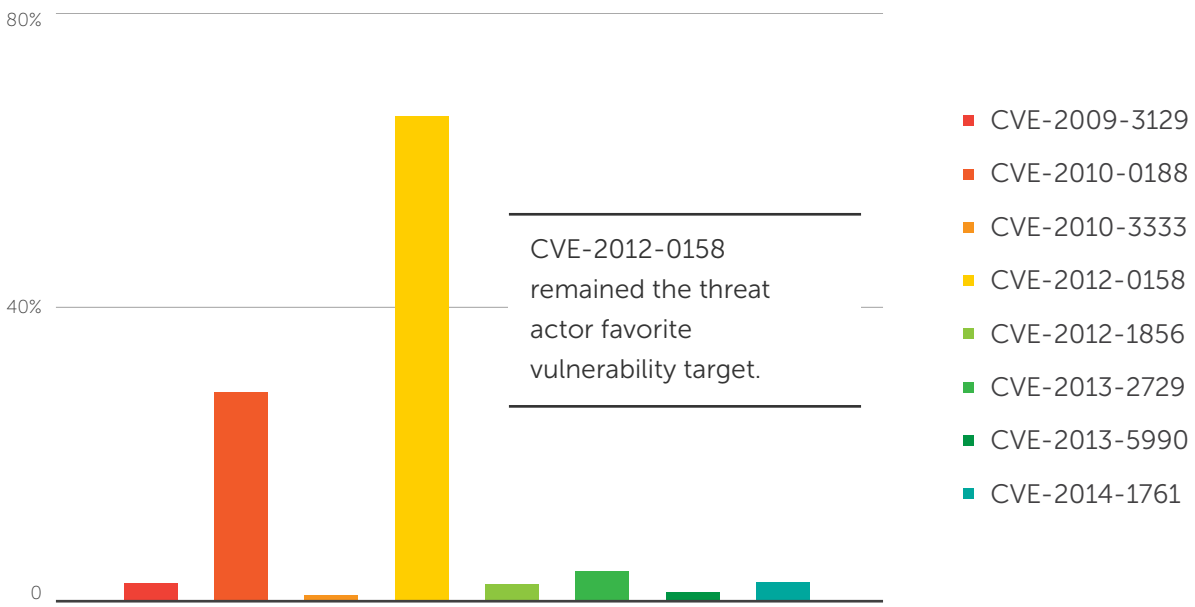


Commonly seen email file attachments used in targeted attacks

NEW AND OLD EXPLOITS FIGURED IN THE THREAT LANDSCAPE

Zero-day and tried-and-tested exploits both figured in the targeted attack landscape. As in the latter half of 2013, threat actors continued to exploit a bug in Windows Common Controls (CVE-2012-0158) and addressed by Microsoft Security Bulletin MS12-027.[10, 11] The PLEAD campaign against Taiwan ministries, in particular, was such an attack.[12]

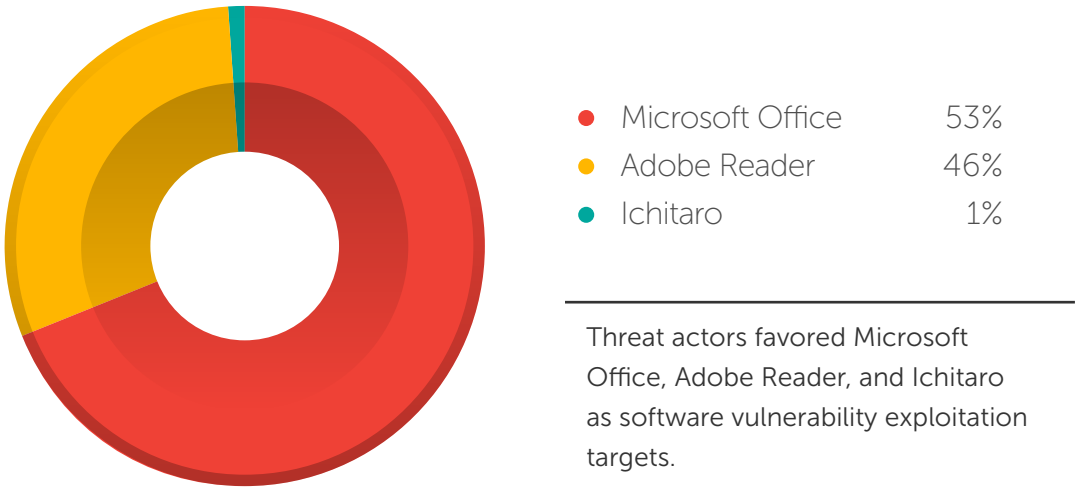
Exploiting old vulnerabilities still worked because some IT administrators sometimes forgo the application of security fixes to avoid disrupting critical business operations. Another reason could be patch testing prior to actual implementation to ensure that fixes would not have adverse effects on corporate environments.



Most commonly exploited vulnerabilities related to targeted attacks

A zero-day vulnerability in Windows XP and Windows Server® 2003 was also exploited in a targeted attack this April prior to the end of support for the OSs.[13] The said zero-day bug was patched via MS14-002 a couple of days after.[14]

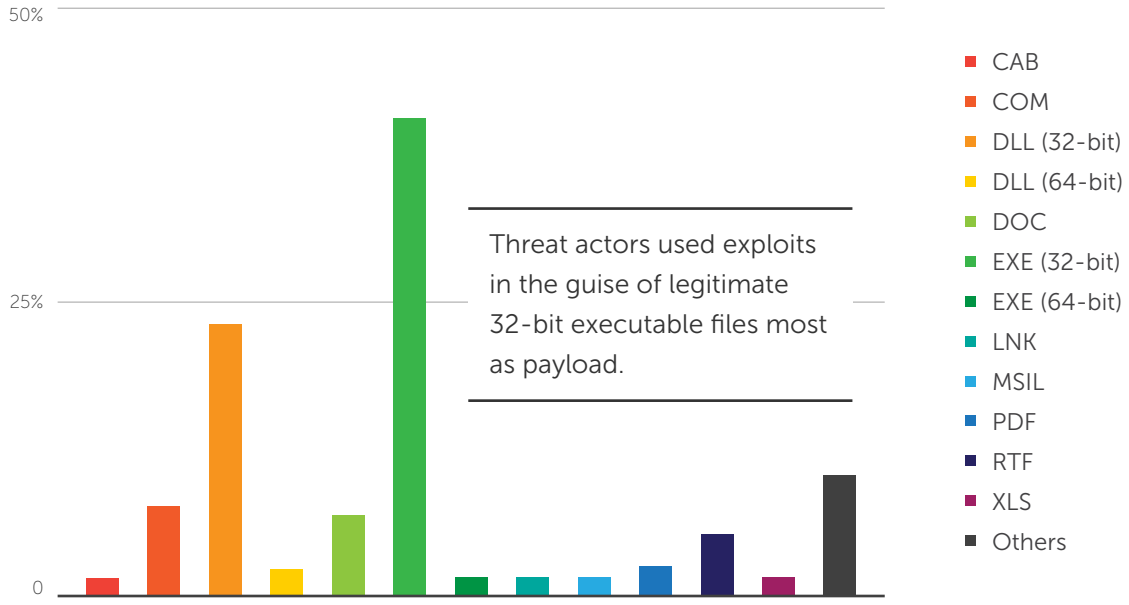
The threat actors behind the Taidoor Campaign, active since 2008, took advantage of a Microsoft™ Office vulnerability this May.[15] Likewise, a vulnerability in Ichitaro (CVE-2013-5990), a popular word processor in Japan, was also exploited in the ANTIFULAI Campaign.[16]



Most commonly exploited software related to targeted attacks

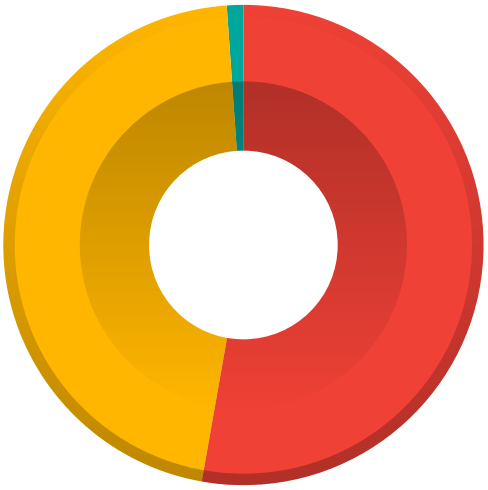
DOCUMENTS AS ATTACHMENT TO TARGETED ATTACK EMAILS

Documents (.DOC and .RTF files) unsurprisingly work as targeted attack payload carriers, as these commonly changed hands in any kind of organization. Unsuspecting recipients often execute attacks' final payloads because they believe they are opening legitimate files from trusted senders.



Most commonly used file types in targeted attacks

Most of the malware used in targeted attacks were Trojans or Trojan spyware (53%), followed by backdoors (46%). Backdoors typically aid in establishing C&C communications and executing remote commands while Trojans and Trojan spyware aid in downloading the final payload and exfiltrating data.



- Trojan/Trojan spyware 53%
- Backdoor 46%
- Hacktool 1%

Backdoors and Trojans or Trojan spyware were the most-used malware types in targeted attacks.

Most common malware types used in targeted attacks

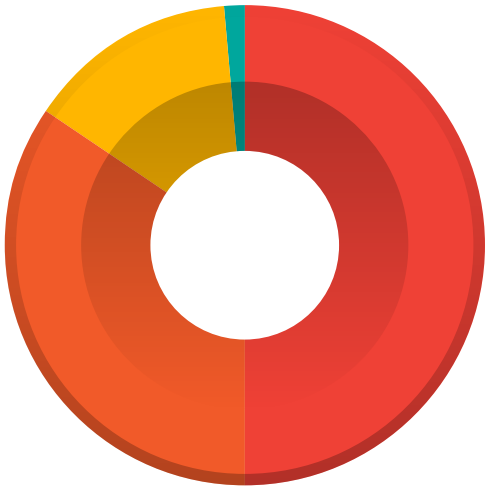
The most-used malware in targeted attacks in the first half of 2014 include PASSVIEW, RIMAGE, XTREME, DarkComet, and HCOREPWSTL.[17, 18, 19] The DarkComet RAT was used in targeted attacks back in 2012.[20] It spread through Skype chats. The Xtreme RAT was also used in targeted attacks against the U.S., Israeli, and other governments that same year.[21]

The following charts show the PASSVIEW- and DarkComet-related victim locations based on the malware used. For both malware, most victims are concentrated in the Asia-Pacific region.

Japan	16%
India	16%
United States	12%
China	9%
Italy	6%
Others	41%

Japan and India were most affected by PASSVIEW

Countries most affected by PASSVIEW



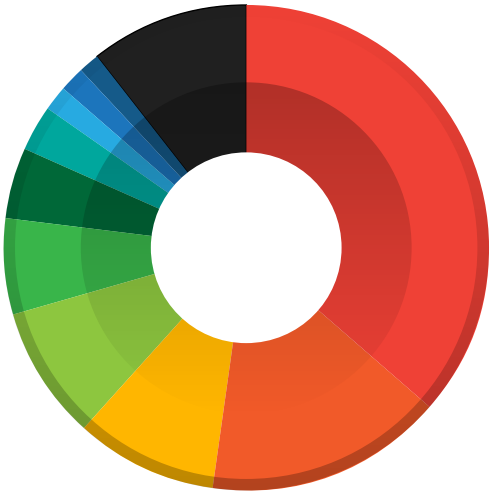
Taiwan	50%
Japan	35%
United States	14%
Vietnam	1%

Half of DarkComet's victims were from Taiwan.

Countries most affected by DarkComet

THREAT ACTORS CHOSE THE RIGHT ATTACK TOOLS FOR UNINIHIBITED COMMUNICATION

As part of our continued monitoring of targeted attacks, we also took a look at certain campaigns. We identified endpoints that communicated with C&C servers that were managed by threat actors.



Taiwan	46%
Japan	20%
United States	12%
Indonesia	11%
China	8%
India	6%
Malaysia	4%
Bangladesh	2%
Philippines	2%
Canada	2%
Others	13%

Targeted attack victim locations

Almost half of the endpoints that accessed C&C servers were located in Taiwan.

United States	48%
Taiwan	13%
China	12%
Hong Kong	9%
Germany	5%
Others	34%

Targeted-attack-related C&C server locations

Almost half of the C&C servers we monitored were located in the United States (top C&C server location). Note, however, that this does not mean that the threat actors were from there. It is, after all, possibe for them to remotely access and manage their servers.

TARGETED ATTACK CAMPAIGN PROFILES

The following were some of the active targeted attack campaigns we observed targeting Asia-Pacific countries in the first half of 2014:

- **IXESHE:** Active since at least 2009, this campaign targeted East Asian governments, Taiwanese electronics manufacturers, and a telecommunications company.[22] It is notable for its use of compromised servers for command and control to evade detection.

- **PLEAD:** This campaign has become well-known for its use of the right-to-left override (RTLO) technique to make targets think they were opening a PowerPoint® file instead of a malicious .SCR file.

- **Taidoor:** Active since March 2009, the threat actors behind this campaign used a seemingly harmless document that when opened actually executed a malicious file in the background.[23] It also used malicious .DOC files to exploit CVE-2012-0158, one of the most commonly exploited bugs up to this day.[24]

- **ANTIFULAI:** This campaign targets government agencies and privately owned companies in Japan by exploiting a bug in Ichitaro, which allowed the execution of malicious arbitrary code. The malware related to this campaign successfully hid its C&C server URLs to evade detection.

FEATURED CAMPAIGNS: SIESTA AND ESILE

ACTORS BEHIND THE SIESTA CAMPAIGN, NOT SLEEPY AT ALL

The Siesta (Spanish term for "short nap") Campaign was so named due to its final payload's ability to receive sleep commands, which allowed it to stay dormant for various periods of time and in turn evade detection. It reportedly targeted organizations from the following industries:

- Consumer goods and services
- Energy
- Finance
- Health care
- Media and telecommunications
- Public administration
- Security and defense
- Transport and traffic

Like most targeted attacks, the threat actors behind the Siesta Campaign sent emails to chosen executives in specific organizations using fake email addresses of supposed colleagues. They did not, like so many attacks, use an attachment. They instead used a legitimate-looking download link *(http://{malicious domain}/{organization name}/{legitimate archive name}.zip)* to compromise their chosen network targets.

The .ZIP file downloaded contains an executable file we detect as TROJ_SLOTH, a supposed .PDF file.[25] When executed, SLOTH opens or drops a valid .PDF file to hide malicious activity running in the background. It has a backdoor component we detect as BKDR_SLOTH.B, which accesses the C&C server link, *http://www.micro{BLOCKED}.com/index.html*.[26]

The said backdoor waits for the following commands:

- **sleep:** Tells the malware to sleep for a certain period of time. The sample we analyzed had the command, "sleep:120." This told the malware to wait two hours before accessing the C&C server.
- **download:** Tells the malware to download and execute a file from a certain URL. This takes the format, *<download_url>*.

Another SLOTH variant we detect as BKDR_SLOTH.A was used in the Siesta Campaign.[27] This variant, however, accessed a different C&C server, *skys{BLOCKED}com*.

The following table lists the commands the two backdoor variants were programmed to receive and follow.

BKDR_SLOTH.A	BKDR_SLOTH.B
run 1 - Open a remote shell	**sleep:** - Sleep for specified number of minutes
run 2 - Pipe shell commands from URL 1	**download:** - Download and execute another executable file from the C&C server
run3 - Pipe shell commands from URL 2	
http - Pipe shell commands from the C&C server	
x - Sleep for a specified number of minutes	

Digging deeper revealed that the threat actors behind the Siesta Campaign used the name "Li Ning" to register the C&C server, *sky{BLOCKED}.com*. Li Ning supposedly used the email address, *xiaoma{BLOCKED}@163.com*. And that apart from the C&C server link, the same actor had around 79 more registered domains. It is safe to assume that "Li Ning" is a fake name.

THE ESILE CAMPAIGN CONTINUED TO TARGET ASIA/PACIFIC GOVERNMENTS

The threat actors behind the ESILE Campaign continued to set their sights on governmental institutions in the Asia/Pacific region. They used backdoors we detect as BKDR_ESILE variants to remotely execute malicious commands on compromised networks.[28]

Further investigation revealed that ESILE variants exploited the same bug that Taidoor malware did, CVE-2012-0158. Note that Microsoft has patched this vulnerability in 2012. Unlike the Taidoor malware, however, ESILE variants could modify the document template to have varying payloads. This targeted attack technique has been used by other malware such as FARFLI and HORSMY. As in most targeted attack cases, ESILE arrived via spear-phishing emails sporting varying social engineering lures that had to do with health care and taxes, among others. Vague filenames such as "Attachment" have also been used.

Protecting networks against targeted attacks strongly calls for building threat intelligence. This can include lists of known indicators of compromise (IoCs) and C&C servers that can serve as reference to determine if an organization's network has already been compromised, thus breaking the targeted attack chain.

IT administrators would do well to check for the following known ESILE Campaign components to protect their networks:

- Strings:
  - *EliseDLL.pdb*
  - *EliseDLL*
- BLOB file component that is typically dropped as *{random}.CAB*
- C&C HTTP requests that match the regular expression (regex), *(POST|GET)\s /[a-f0-9]{10}/page_[0-9]{10}.html*

Part of a bigger campaign known as "APTOLSTU," the ESILE and EVORA Campaigns used RATs to establish command and control. Our findings showed that the group behind these (LStudio) had 71 C&C servers in 10 countries. The ESILE and EVORA malware had the following PDB reference strings inside the malicious binaries:

- *d:\lstudio\projects\lotus\evora\Release\EvoraDLL\i386\EvoraDLL.pdb*
- *D:\work\nbkkkk\Lotus\Elise\EliseDLL\Release\EliseDLL.pdb*

DEFENDING NETWORKS AGAINST TARGETED ATTACKS

Protecting networks against targeted attacks means busting common misconceptions about them. One such misconception is that targeted attacks are one-time efforts. The truth: Targeted attacks are well-planned and can be launched several times until they successfully compromise intended network targets.

IT administrators are strongly advised to look for the following signs of targeted attacks as countermeasure:[29]

- Search for injected Domain Name System (DNS) records as attackers alter DNS settings to make sure their malicious activity is not yet being detected by already-installed solutions.
- Check accounts for failed or irregular log-in attempts because these could indicate lateral movement in target networks, given the fact that threat actors often brute-force their way into administrator accounts.
- Check for unknown large files as these may hold stolen data ready for exfiltration.
- Monitor network logs and protocols to check for abnormal connections made.
- Check abnormal increases in individual employees' email activity logs.

Keep in mind that a one-size-fits-all solution to protect against targeted attacks does not exist. Organizations need to implement what we call a "Custom Defense Strategy," which uses advanced threat detection technologies and shared IoCs and intelligence to detect, analyze, and respond to attacks that are invisible to standard security products.[30]

REFERENCES

1. Harvard Business School Publishing. (2014). "Aggressive and Persistent: Using Frameworks to Defend Against Cyber Attacks." Last accessed September 16, 2014, http://campaign.trendmicro.com/forms/Harvard_Business_Review_Report_1687.

2. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed September 16, 2014, http://about-threats.trendmicro.com/us/security-predictions/2014/blurring-boundaries/.

3. Maersk Menrige. (June 25, 2014). *TrendLabs Security Intelligence Blog*. "PlugX RAT with 'Time Bomb' Abuses Dropbox for Command-and-Control Settings." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/.

4. Softpedia. (July 12, 2013). *Softpedia*. "Experts Reveal How Chinese APT Hackers Abuse Dropbox and WordPress." Last accessed September 17, 2014, http://news.softpedia.com/news/Experts-Reveal-How-Chinese-APT-Hackers-Abuse-Dropbox-and-WordPress-367652.shtml.

5. Maersk Menrige. (May 29, 2014). *TrendLabs Security Intelligence Blog*. "Black Magic: Windows PowerShell Used Again in New Attack." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/black-magic-windows-powershell-used-again-in-new-attack/.

6. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "LNK_PRESHIN.JTT." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/LNK_PRESHIN.JTT.

7. Maharlito Aquino. (March 6, 2014). *TrendLabs Security Intelligence Blog*. "The Siesta Campaign: A New Targeted Attack Awakens." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/.

8. Maersk Menrige. (June 17, 2014). *TrendLabs Security Intelligence Blog*. "Template Document Exploit Found in Several Targeted Attacks." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/template-document-exploit-found-in-several-targeted-attacks/.

9. Wikimedia Foundation Inc. (August 22, 2014). *Wikipedia*. "Watering Hole." Last accessed September 17, 2014, http://en.wikipedia.org/wiki/Watering_Hole.

10. The MITRE Corporation. (2014). *CVE*. "CVE-2012-0158." Last accessed September 17, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158.

11. Microsoft. (2014). *Security TechCenter*. "Microsoft Security Bulletin MS12-027 – Critical." Last accessed September 17, 2014, https://technet.microsoft.com/en-us/library/security/ms12-027.aspx.

12. Kervin Alintanahin. (May 23, 2014). *TrendLabs Security Intelligence Blog*. "PLEAD Targeted Attacks Against Taiwanese Government Agencies." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/.

13. Trend Micro Incorporated. (January 6, 2014). *TrendLabs Security Intelligence Blog*. "Recent Windows Zero-Day Targeted Embassies, Used Syria-Related Email." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/recent-windows-zero-day-targeted-embassies-used-syria-related-email/.

14. Microsoft. (2014). *Security TechCenter*. "Microsoft Security Bulletin MS14-002 – Important." Last accessed September 17, 2014, https://technet.microsoft.com/en-us/library/security/ms14-002.aspx.

15. Trend Micro Incorporated. (May 12, 2014). *TrendLabs Security Intelligence Blog*. "Targeted Attack Against Taiwanese Agencies Used Recent Microsoft Word Zero-Day." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-against-taiwanese-agencies-used-recent-microsoft-word-zero-day/.

16. Maersk Menrige. (June 4, 2014). *TrendLabs Security Intelligence Blog*. "ANTIFULAI Targeted Attack Exploits Ichitaro Vulnerability." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/antifulai-targeted-attack-exploits-ichitaro-vulnerability/.

17. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "HKTL_PASSVIEW." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/HKTL_PASSVIEW.

18. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "BKDR_XTREME.SMUM." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_XTREME.SMUM.

19. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "DARKCOMET." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/DARKCOMET.

20. Kevin Stevens and Nart Villeneuve. (February 23, 2014). *TrendLabs Security Intelligence Blog*. "DarkComet Surfaced in the Targeted Attacks in Syrian Conflict." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/darkcomet-surfaced-in-the-targeted-attacks-in-syrian-conflict/.

21. Nart Villeneuve. (November 14, 2012). *TrendLabs Security Intelligence Blog*. "New Xtreme RAT Attacks U.S., Israel, and Other Foreign Governments." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/.

22. David Sancho, Jessa dela Torre, Matsukawa Bakuei, Nart Villeneuve, and Robert McArdle. (2012). *Trend Micro Security Intelligence*. "IXESHE: An APT Campaign." Last accessed September 17, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf.

23. Trend Micro Threat Research Team. (2012). *Trend Micro Security Intelligence*. "The Taidoor Campaign: An In-Depth Analysis." Last accessed September 17, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf.

24. The MITRE Corporation. (2014). *CVE*. "CVE-2012-0158." Last accessed September 17, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158.

25. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "TROJ_SLOTH.A." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/TROJ_SLOTH.A.

26. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "BKDR_SLOTH.B." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_SLOTH.B.

27. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "BKDR_SLOTH.A." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_SLOTH.A.

28. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "BKDR_ESILE.SMEX." Last accessed September 17, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_ESILE.SMEX.

29. Ziv Chang. (August 14, 2014). *TrendLabs Security Intelligence Blog*. "7 Places to Check for Signs of a Targeted Attack in Your Network." Last accessed September 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/7-places-to-check-for-signs-of-a-targeted-attack-in-your-network/.

30. Trend Micro Incorporated. (2014). *Trend Micro*. "Trend Micro Custom Defense: Proven Protection Against Targeted Attacks and Advanced Persistent Threats." Last accessed September 17, 2014, http://www.trendmicro.com/us/business/cyber-security/index.html.

Created by:

TrendLabs

Global Technical Support & R&D Center of **TREND MICRO**

TREND MICRO™

Securing Your Journey to the Cloud