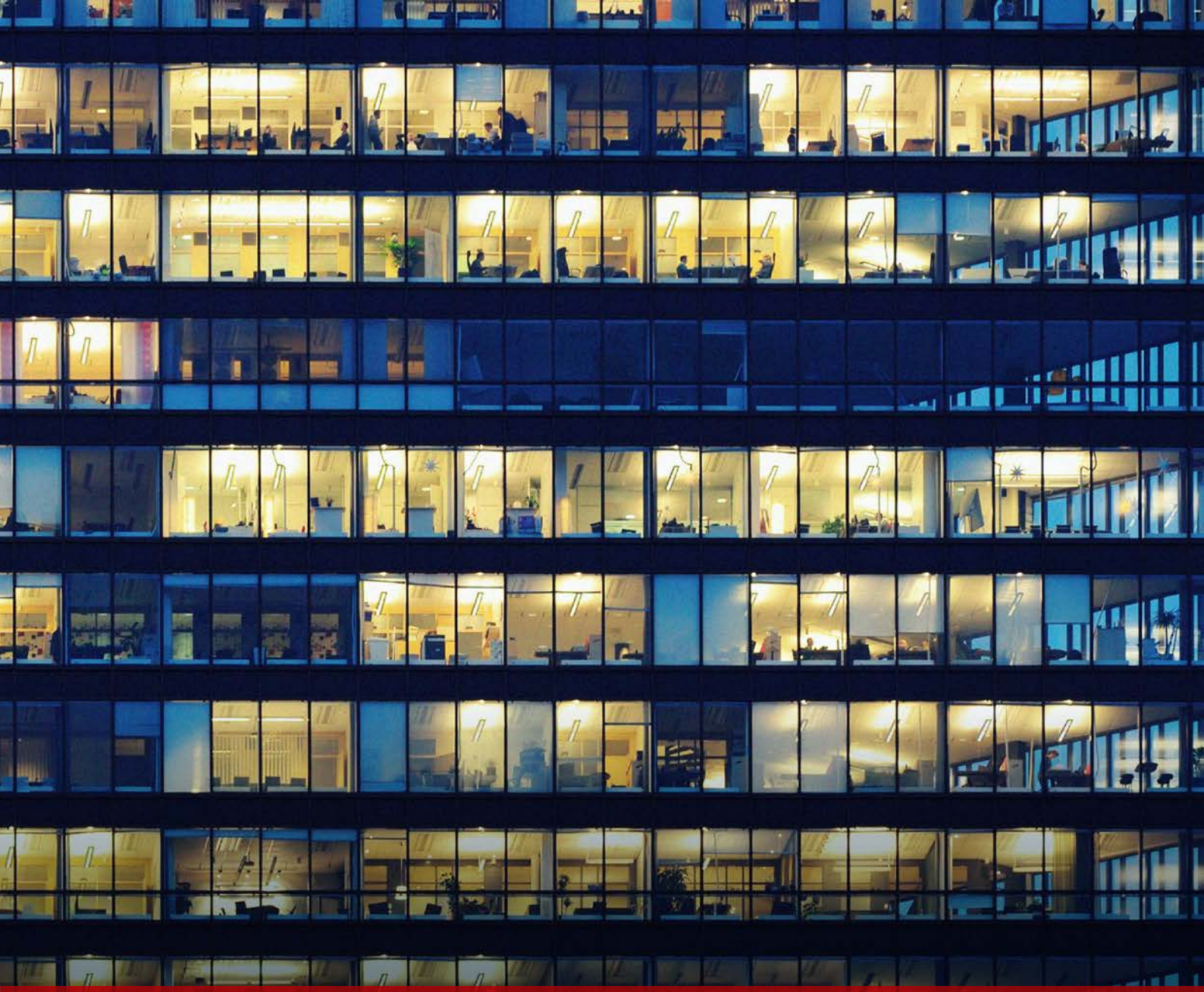


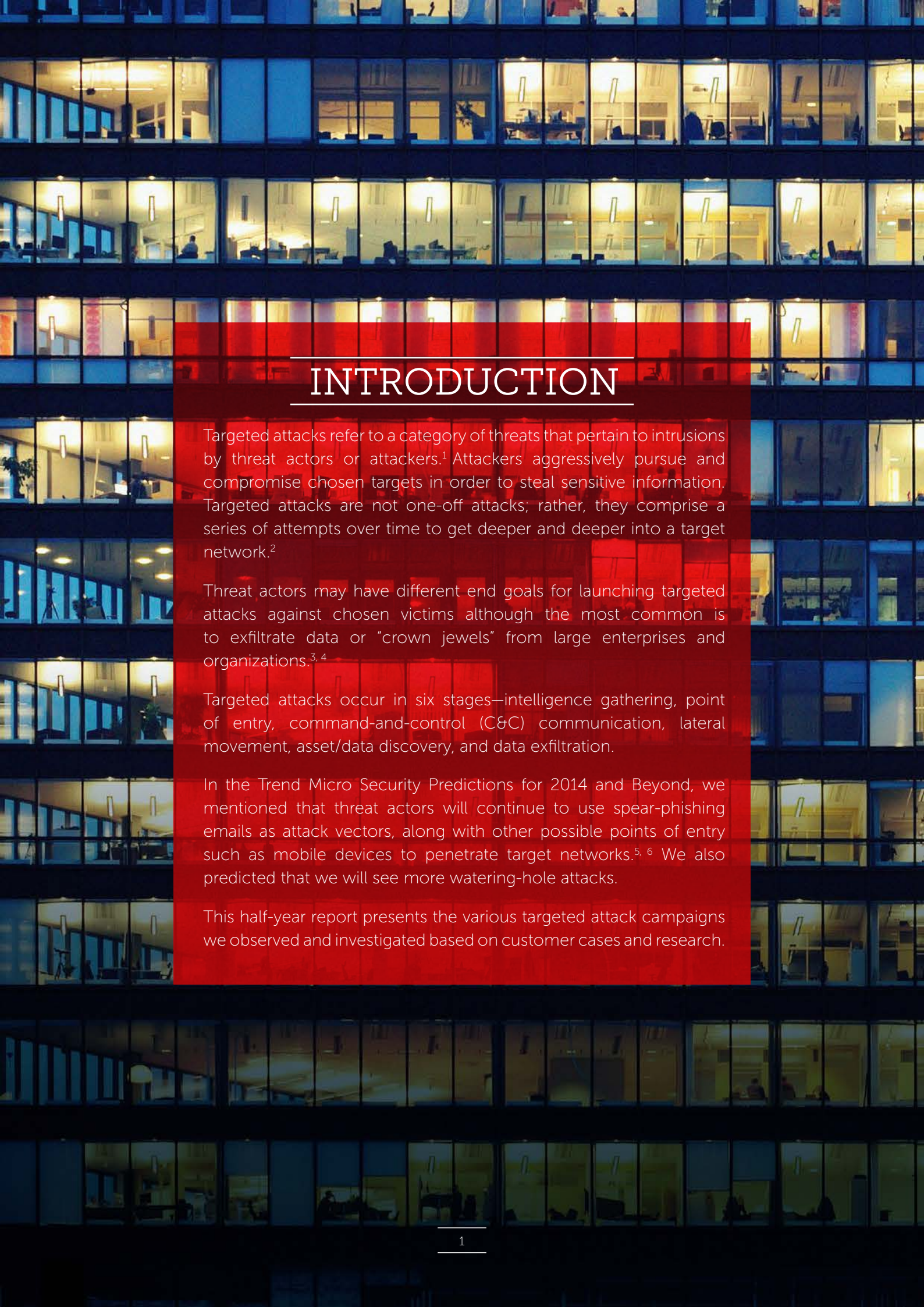
# Targeted Attack Trends

2H 2013 Report

A TrendLabs℠ Report

TREND MICRO™

# CONTENTS



# INTRODUCTION

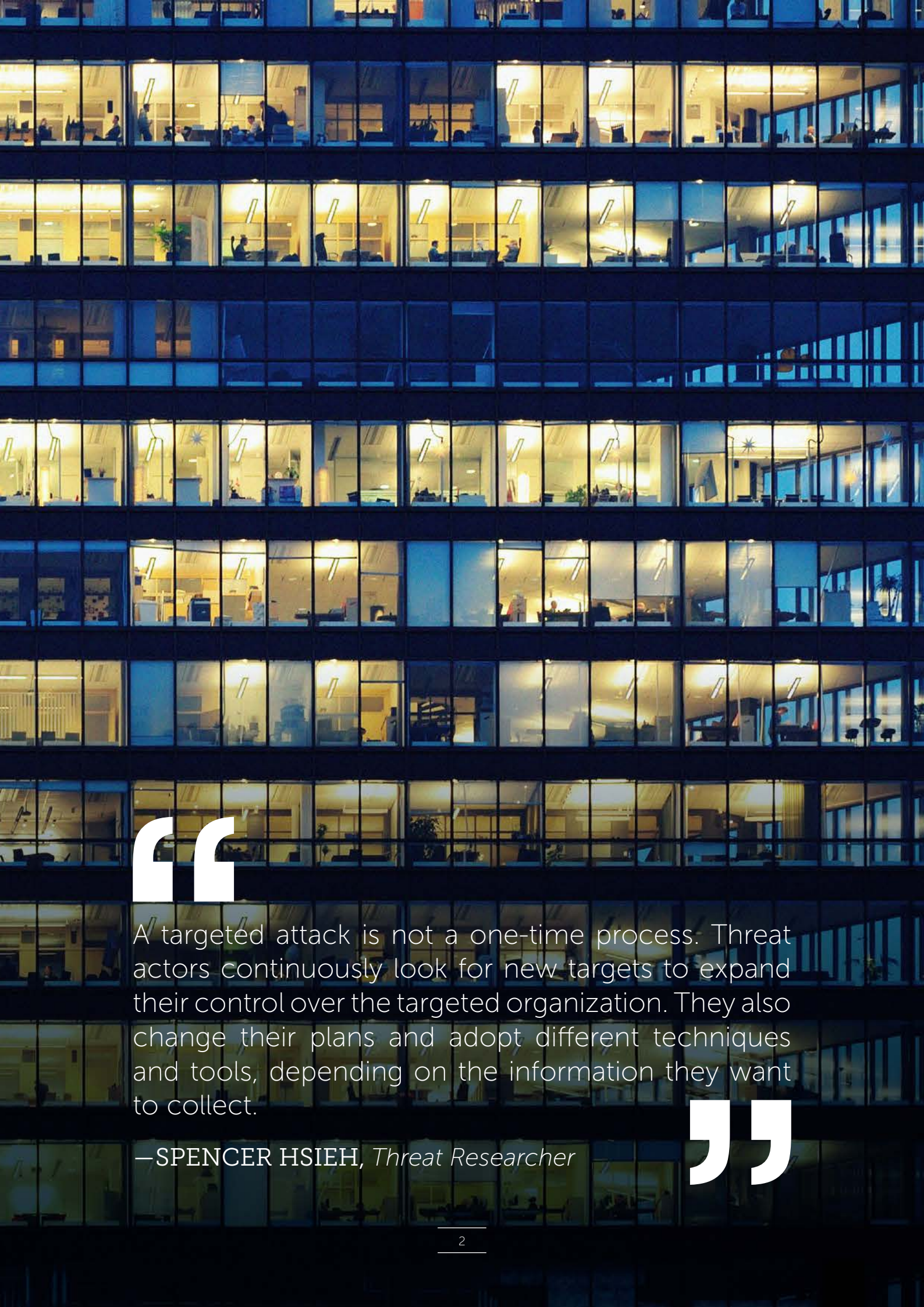
Targeted attacks refer to a category of threats that pertain to intrusions by threat actors or attackers.[1] Attackers aggressively pursue and compromise chosen targets in order to steal sensitive information. Targeted attacks are not one-off attacks; rather, they comprise a series of attempts over time to get deeper and deeper into a target network.[2]

Threat actors may have different end goals for launching targeted attacks against chosen victims although the most common is to exfiltrate data or "crown jewels" from large enterprises and organizations.[3, 4]

Targeted attacks occur in six stages—intelligence gathering, point of entry, command-and-control (C&C) communication, lateral movement, asset/data discovery, and data exfiltration.

In the Trend Micro Security Predictions for 2014 and Beyond, we mentioned that threat actors will continue to use spear-phishing emails as attack vectors, along with other possible points of entry such as mobile devices to penetrate target networks.[5, 6] We also predicted that we will see more watering-hole attacks.

This half-year report presents the various targeted attack campaigns we observed and investigated based on customer cases and research.

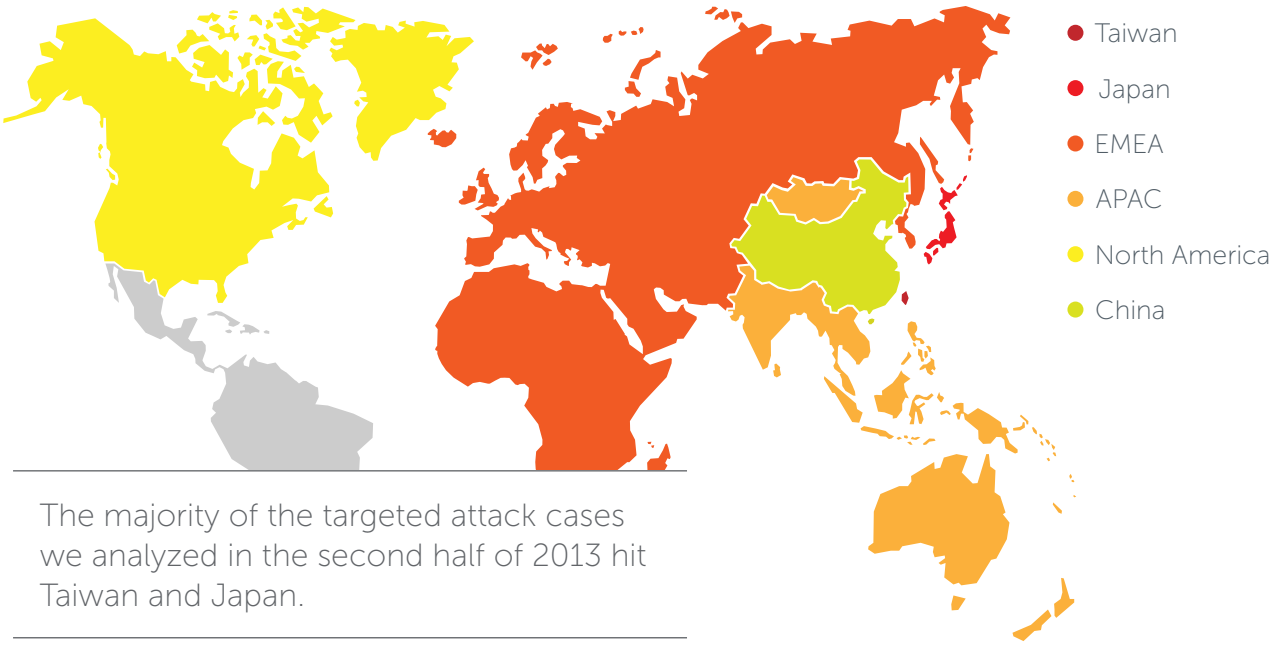


> A targeted attack is not a one-time process. Threat actors continuously look for new targets to expand their control over the targeted organization. They also change their plans and adopt different techniques and tools, depending on the information they want to collect.
>
> —SPENCER HSIEH, *Threat Researcher*

# THREAT LANDSCAPE

## TARGETED ATTACKS HIT TAIWAN AND JAPAN

In the second half of 2013, the majority of the targeted attack cases we analyzed hit Taiwan and Japan. Countries in Europe, the Middle East, and Africa (EMEA) were, however, also targeted.

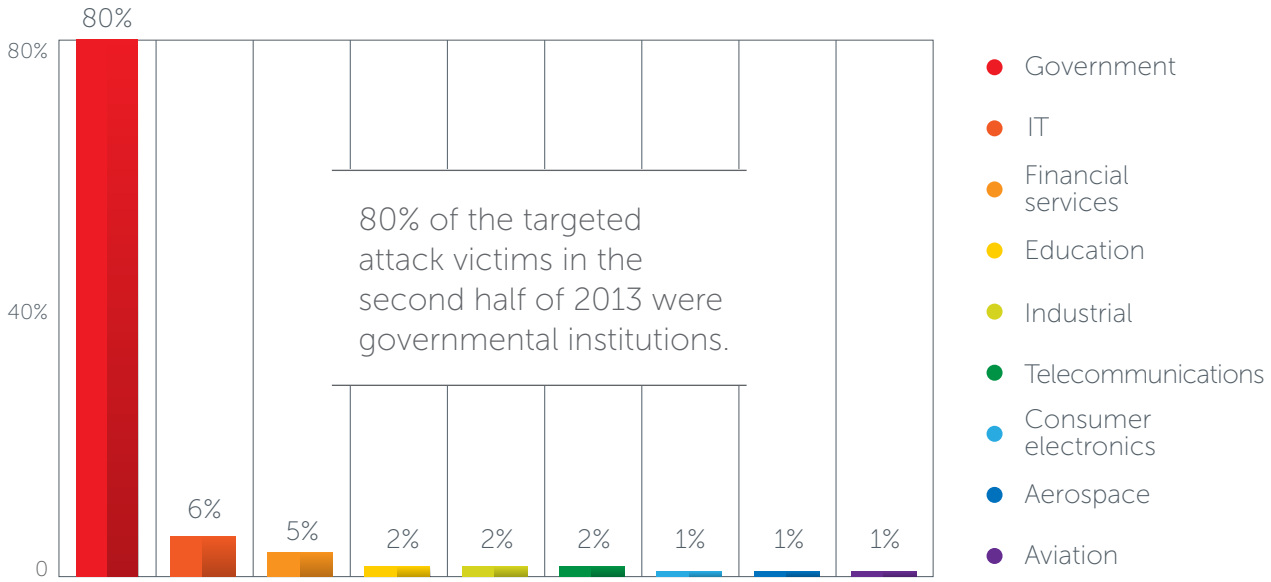



The majority of the targeted attack cases we analyzed in the second half of 2013 hit Taiwan and Japan.

*Countries/Regions most affected by targeted attacks*

# GOVERNMENTAL INSTITUTIONS, STILL THE MOST PREFERRED TARGETS

According to our findings, the majority of the targeted attack victims were governmental institutions. Companies in the IT industry—both software and hardware vendors—were also hit, along with organizations in the financial services (e.g., banks) sector.



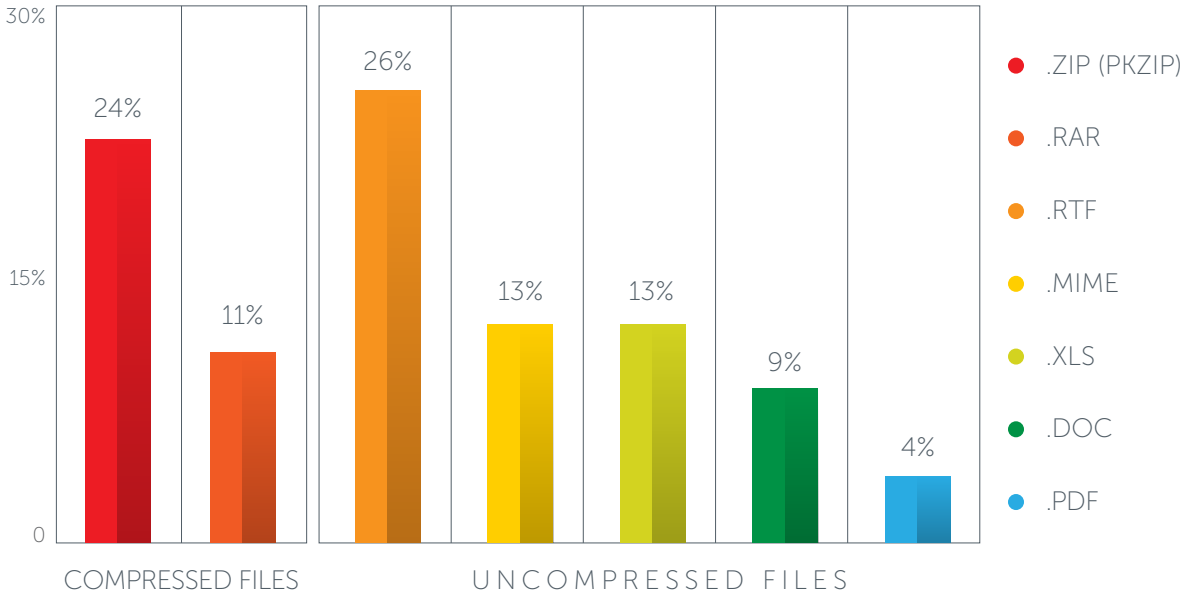

*Targeted attacks seen by industry*

# SPEAR-PHISHING EMAILS REMAINED A PRIMARY MEANS TO GET IN TO TARGET NETWORKS

Email remains the primary business communication means, and as such, also the most typical point of entry that threat actors abuse to penetrate target networks. Threat actors typically send spear-phishing emails with contextually relevant subjects to specific people with different functions in a target organization.

File attachments serve as malware or exploit carriers that trigger the start of the infection chain that eventually leads to the succeeding stages of a targeted attack. Their use fools users into thinking they are opening a legitimate document or file.

In the second half of 2013, data showed that the majority of the targeted attack cases we analyzed used Microsoft™ Rich Text Format (RTF) attachments—a type of document file format. .ZIP, .XLS, and .MIME were also commonly used.

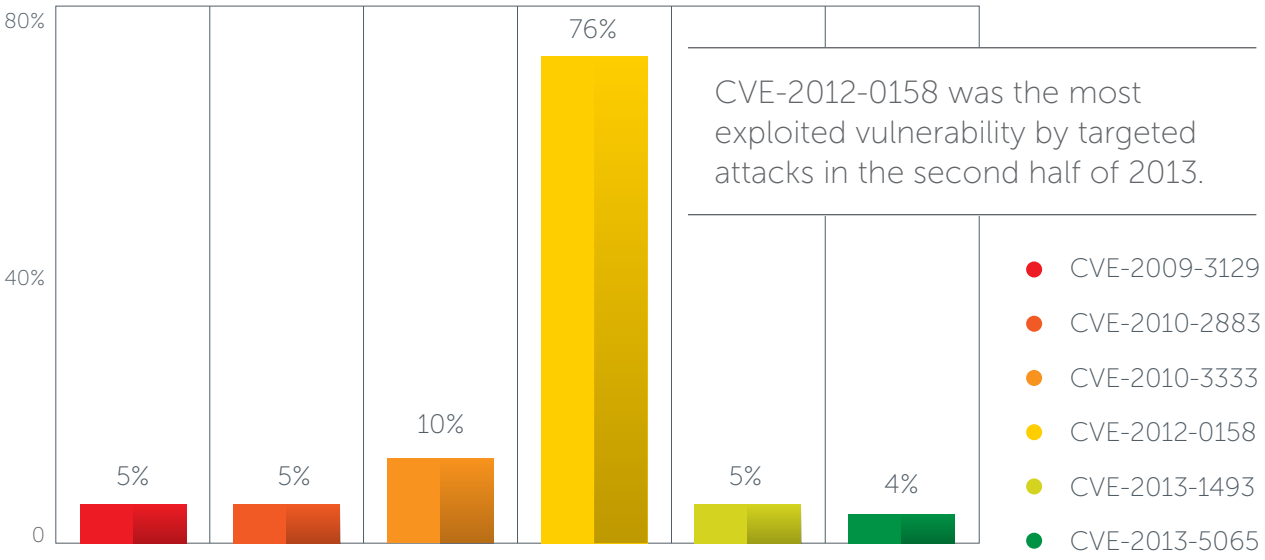



.ZIP (compressed) and .RTF (uncompressed) files were the most commonly used attachment types in emails related to targeted attacks.

*Commonly seen spear-phishing email file attachments used in targeted attacks*

# TRIED-AND-TESTED VULNERABILITIES PROVED USEFUL IN TARGETED ATTACKS

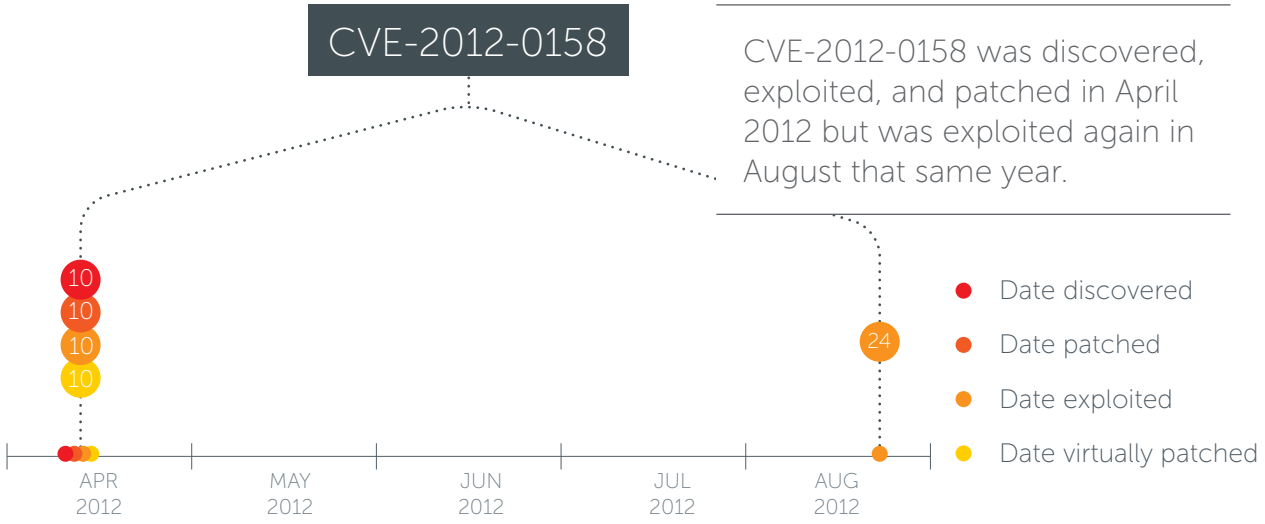
Threat actors continued to exploit old vulnerabilities in various software and systems. They took advantage of the fact that enterprises are often forced to delay patch and update application to maintain critical business operations and test the patches and updates in their environments before deployment. This delay opens up windows of exposure that could result in infection.




*Most commonly exploited vulnerabilities related to targeted attacks*

The majority of the exploits used in targeted attacks in the second half of 2013 took advantage of vulnerabilities that have been patched, some as early as 2009. This proves that exploiting old vulnerabilities remains an efficient way to get into target networks.

CVE-2012-0158 was addressed by the release of MS12-027, which pertains to vulnerabilities existing in Windows common controls.[7] If exploited, the vulnerability could allow an attacker to execute malicious code on an infected system.



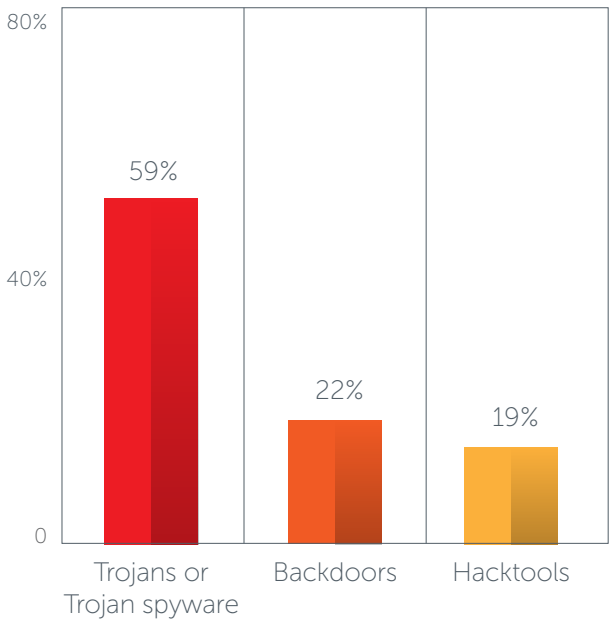

*Vulnerability timeline for CVE-2012-0158*

In the second half of 2013, the CVE-2013-1493 vulnerability was abused by the threat actors behind the BLYPT Campaign.[8, 9] The Java™ exploit downloaded an installer that, in turn, downloaded the main BLYPT component. A zero-day exploit also took advantage of the CVE-2013-5065 vulnerability in Windows® XP and Windows Server 2003, which was addressed by MS14-002.[10, 11]

Microsoft also announced that it would no longer support and provide security updates for Windows XP by April 2014 in 2013.[12] For threat actors and cybercriminals, this could mean launching far more effective attacks via exploits because these would no longer be patched. For users, especially enterprises that would stick to using the unsupported OS, this could mean even more security risks.

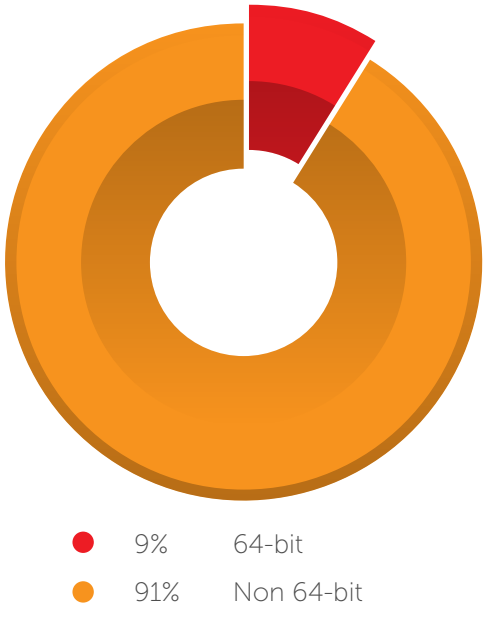
## MALWARE, STILL EFFECTIVE TARGETED ATTACK TOOLS

The top 3 malware types most commonly used in targeted attacks were backdoors, hacktools, and Trojans or Trojan spyware.




*Most common malware types used in targeted attacks*

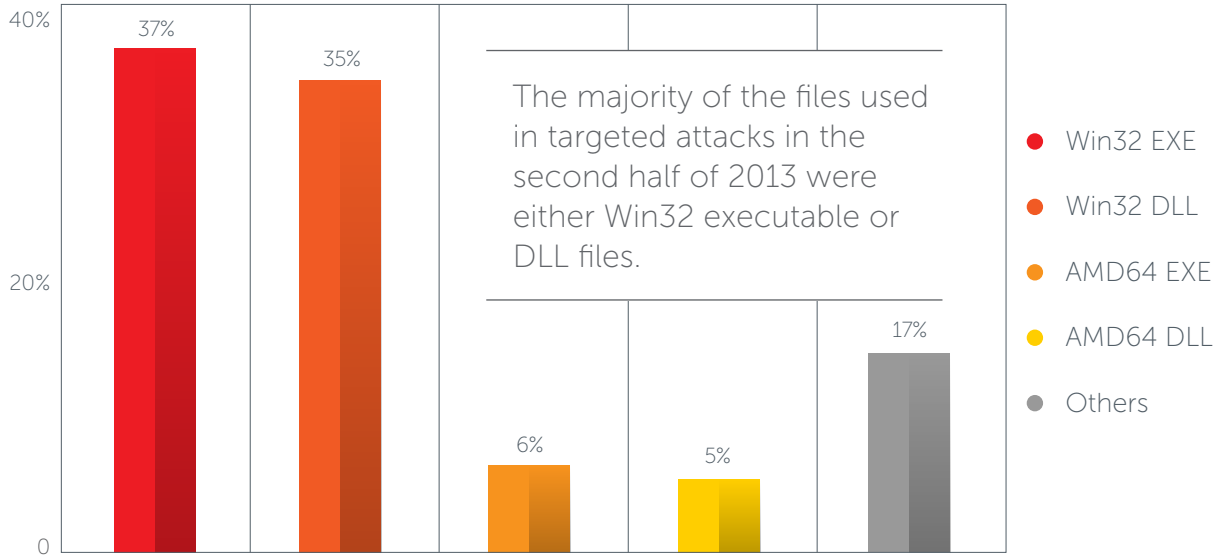
Almost 60% of the malware used in targeted attacks were Trojans or Trojan spyware.




*64- and non-64-bit malware distribution*

Almost 10% of the malware used in targeted attacks in the second half of 2013 exclusively ran on 64-bit systems.

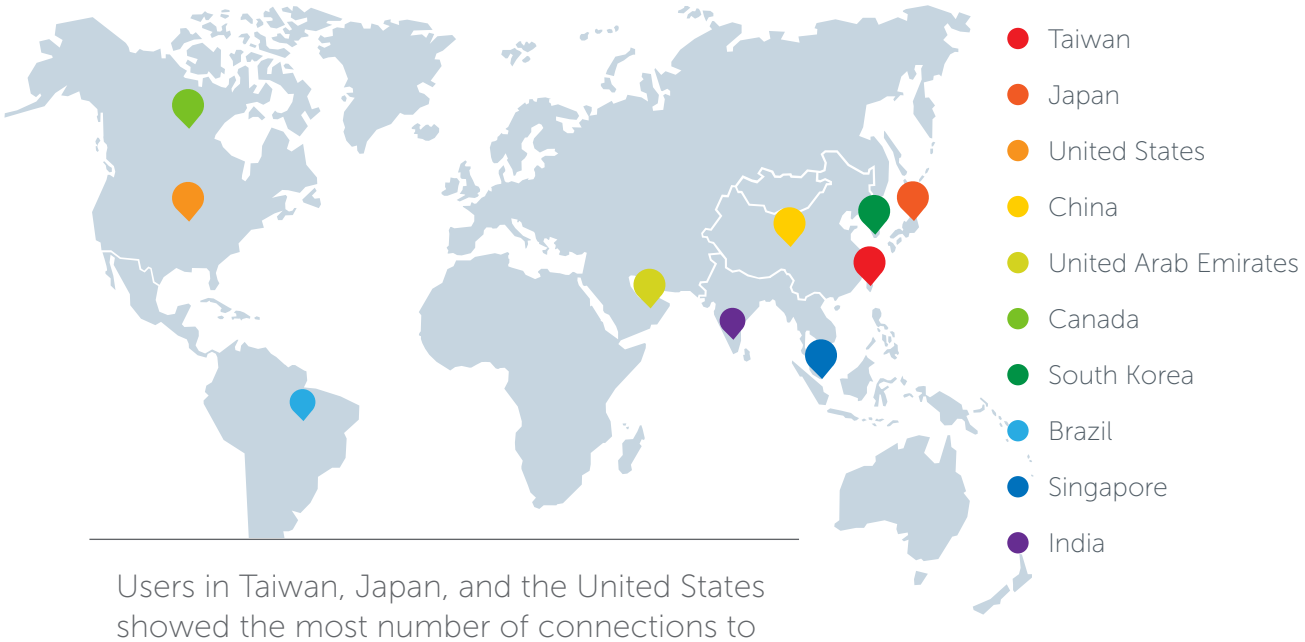
Most of the malware used in targeted attacks in 2013 were executable files that, when unknowingly executed by users, could start an infection chain. Threat actors often used backdoors to establish server communications, which enabled them to send malicious commands to infected systems so they could go deeper into target networks and eventually steal data.[13] Hacktools and Trojans or Trojan spyware, on the other hand, were employed to steal user credentials that allowed threat actors to infiltrate other areas of target networks.




*Most commonly used file types in targeted attacks*

# C&C SERVER COMMUNICATIONS REVEALED DIVERSE VICTIMS

We monitored the C&C server activities related to various targeted attacks in the second half of 2013 as well. Most of the connections to C&C servers related to targeted attacks came from Taiwan, Japan, and the United States.




Users in Taiwan, Japan, and the United States showed the most number of connections to C&C servers related to targeted attacks.

*Countries with the most number of users who accessed C&C servers related to targeted attacks*

# TARGETED ATTACK CAMPAIGN PROFILES

The following were some of the active targeted attack campaigns we observed in the second half of 2013:

- **IXESHE:** This campaign was detected as early as 2009 and became known for its use of compromised servers for C&C in order to hide malicious network activities.[14] It also made use of dynamic Domain Name System (DNS) services to further hide the threat actors' tracks or presence in target networks. Some of its known victims include East Asian governments, Taiwanese electronics manufacturers, and a telecommunications company.

- **ESILE:** We detect the malware related to this campaign, which targeted certain governmental institutions in Asia/Pacific (APAC), as BKDR_ESILE.[15] Note that researchers outside Trend Micro refers to this as the "ELise Campaign."[16]

- **ZEGOST:** This campaign used an exploit in the guise of Vietnamese documents as social engineering lure based on the samples we obtained.

- **TRAVNET:** This campaign got its name from strings found in related data-stealing malware's code, NetTraveler.

- **HOUDINI:** We detect the malware related to this campaign as DUNIHI variants, which targeted users in Latin America.[17, 18] These were capable of executing at least 13 malicious commands on infected systems.

# FEATURED CAMPAIGNS: BLYPT AND ESILE

> An organization can become a target not only for its own products or the information it holds but also because it is somehow connected to an ultimate target.
>
> — JIM GOGOLINSKI, *Senior Threat Researcher*

## MOST OF THE BLYPT CAMPAIGN SERVERS WERE HOSTED IN ROMANIA AND TURKEY

The BLYPT Campaign and the new backdoor family associated with it were named after the binary large objects (blob) found in infected systems' registry when the Java exploit is executed. In one of the samples we analyzed, the exploit used—JAVA_EXPLOYT.HI—targeted the CVE-2013-1493 vulnerability.[19, 20] When the vulnerability is exploited, the backdoor executed arbitrary code on systems.

Upon closer investigation, the exploit served as a delivery mechanism for the actual BLYPT component, as it downloaded the installer—*~tmp{random values}.tmp*. Afterward, it attempted to access three servers every 3 seconds as many as 32 times until it successfully downloads the backdoor.

The installer also provided feedback on its installation status by accessing the URL, *http://{malicious server}/index.aspx?info=<status keyword>*. The status keyword can be any of the following:

- *startupkey_%d where %d = RegCreateKeyW return*
- *reuse*
- *configkey_%d where %d = RegCreateKeyA return*
- *configkeyvalue_%d where %d = RegSetValueExA return*
- *tserror_4_%d where %d = GetLastError from call to connect*
- *createproc_%d where %d = GetLastError from call to CreateProcessW*
- *reusereboot_%d_%d_%d*

The following malware are related to the BLYPT Campaign:

- BKDR_BLYPT.A[21]
- BKDR_BLYPT.B[22]
- BKDR64_BLYPT.B[23]

Two of the BLYPT variants above—BKDR_BLYPT.A and BKDR_BLYPT.B—run on 32-bit systems. BKDR64_BLYPT.B, on the other hand, runs on 64-bit systems. BKDR_BLYPT.A is saved as *NTCRYPT{random values}.TPL* while BKDR_BLYPT.B and BKDR64_BLYPT.B are saved as *CERTV{random values}.TPL* in the *%App Data%\Microsoft\Crypto\RSA* directory. While they had the same general routines, their C&C-related routines differed. BKDR_BLYPT.A used its installer to save C&C information in the system registry while BKDR_BLYPT.B and BKDR64_BLYPT.B embedded C&C information in a file. All three variants also stored C&C information in the following registry despite varying formats:

```
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\
Certificates\5A82739996ED9EBA18F1BBCDCCA62D2C1D670C\Blob key
```

BKDR_BLYPT.A is formatted in plain text:

```
<ip1>#:<port1>#:#:<server page1>#;<ip2>#:<port2>#:#:<server
page2 >#;<ipN>#:<portN>#:#:<server pageN>#;
```

BKDR_BLYPT.B and BKDR64_BLYPT.B, on the other hand, are formatted in binary text:

```
struct
{
DWORD ip;
WORD port;
} cncServer;
cncServer cncList[];
```

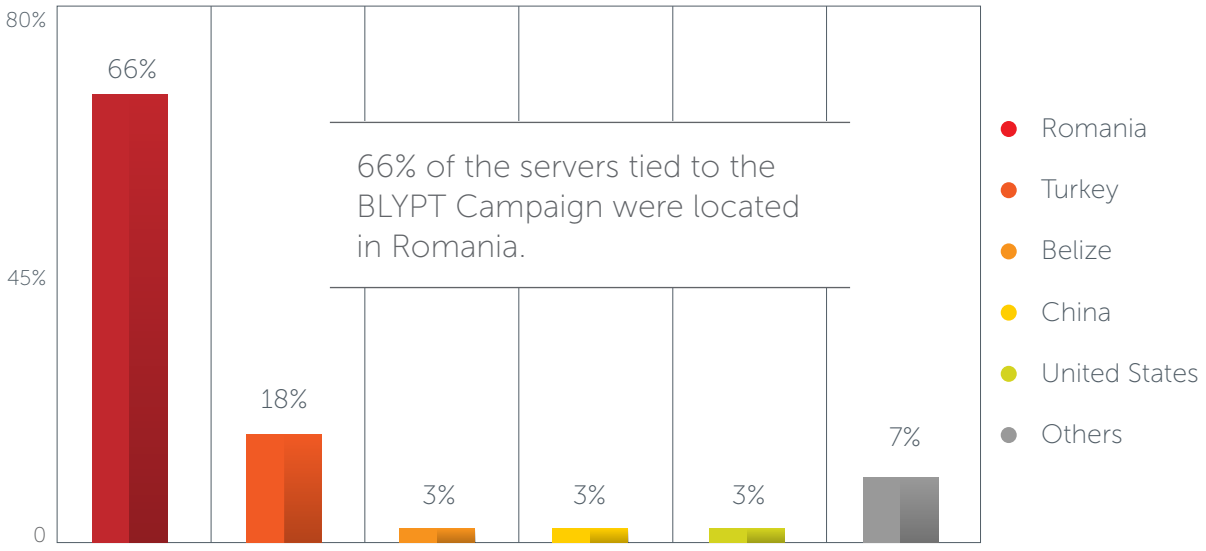
The following is a sample raw data format:

```
<(DWORD)ip1><(WORD)port1><(DWORD)ip2><(WORD)port2><(DWORD)
ipN><(WORD)portN>
```

To encrypt information, the threat actors behind the campaign used alleged RC4 (arc4) and used "http://microsoft.com" as decryption key.

When executed, the backdoors executed the following commands on infected systems:

- Receive updated DLL binary
- Receive updated configuration
- Receive HTTP request commands such as GET request to *http://103.31.186.19:1000/FetchIP.aspx* to retrieve the public IP address of the infected system




*BLYPT C&C server locations*

# THE ESILE CAMPAIGN HIT GOVERNMENTAL INSTITUTIONS IN APAC

The ESILE Campaign reportedly targeted various governmental institutions in APAC. This campaign got its name from the project path based on the debug stub of the malware used, an example of which is *C:\LStudio\Project\Lotus\Elise\Release\SetElise.pdb*. All of the malware related to this campaign are detected as BKDR_ESILE variants. The backdoors allowed threat actors to remotely open a command-line console to issue several commands such as:

- *net user*
- *net localgroup administrators*
- *net view*
- *netstat -ano*
- *tasklist /v*
- *net start*
- *systeminfo*

To gather threat intelligence, IT administrators could look for the following network and file indicators:

### Network traffic indicator:

- C&C HTTP requests that should match the following RegEX:

```
(POST|GET)\s /[a-f0-9]{10}/page_[0-9]{10}.html
```

### Malicious file indicator:

- BKDR_ESILE has the following strings in the unpacked malware body:
  - *EliseDLL.pdb*
  - *EliseDLL*

Note that the ESILE Campaign is part of a larger campaign that is also dubbed by other reasearchers as "APT0LSTU." We are currently monitoring and conducting further research into this campaign.

> The overall goal is to quickly detect the problem, analyze all the variables related to the event, adapt, and respond with the appropriate processes and countermeasures to contain the event and mitigate future risks using a similar attack vector no matter where your infrastructure resides.
>
> — J.D. SHERRY,
>
> *Vice President, Technology and Solutions*

# DEFENDING NETWORKS AGAINST TARGETED ATTACKS

Traditional antivirus signature-based solutions and blacklisting are not enough to mitigate the risks targeted attacks pose. Large enterprises and organizations need to implement Custom Defense—a security solution that uses advanced threat detection technology and shared indicator of compromise (IoC) intelligence to unite the security infrastructure to detect, analyze, and respond to attacks that are invisible to standard security products. [24, 25, 26, 27]

Trend Micro™ Deep Discovery is the advanced threat protection platform at the heart of Custom Defense.[28] Using specialized detection engines, custom sandbox simulation, and Trend Micro Smart Protection Network™ intelligence, Deep Discovery identifies malware, C&C communications, and attacker activities signaling an attempted attack. It then delivers in-depth threat intelligence to drive rapid response and automated IoC updates to allow other security solutions to block further attacks.

To get the latest updates on targeted attacks, visit Threat Intelligence Resources - Targeted Attacks.

For more information on the different stages of targeted attacks, read the following reports:

- Data Exfiltration: How Do Threat Actors Steal Your Data?
- Lateral Movement: How Do Threat Actors Move Deeper into Your Network?
- Malicious Network Communications: What Are You Overlooking?
- Targeted Attack Entry Points: Are Your Business Communications Secure?

To learn more on safeguarding or defending enterprise networks from targeted attacks, read the following reports in the "The Enterprise Fights Back" series:

- Securing Your Network Infrastructure Against Targeted Attacks
- Protecting Sensitive Data from Targeted Attacks
- Building an Incident Response Team
- Building Threat Intelligence

# REFERENCES


1. Nart Villeneuve. (October 2011). "Trends in Targeted Attacks." Last accessed May 2, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf.

2. Trend Micro Incorporated. (2013). "Lateral Movement: How Do Threat Actors Move Deeper into Your Network?" Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#how-do-threat-actors-move-deeper-into-your-network.

3. Trend Micro Incorporated. (2013). "Data Exfiltration: How Do Threat Actors Steal Your Data?" Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#how-do-threat-actors-steal-your-data.

4. Trend Micro Incorporated. (2013). "The Enterprise Fights Back (Part II): Protecting Sensitive Data from Targeted Attacks." Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#protecting-sensitive-data-from-targeted-attacks.

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

6. Trend Micro Incorporated. (2013). "Targeted Attack Entry Points: Are Your Business Communications Secure?" Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#are-your-business-communications-secure.

7. Microsoft. (2014). *Security TechCenter.* "Microsoft Security Bulletin MS12-027 – Critical." Last accessed May 7, 2014, https://technet.microsoft.com/en-us/library/security/ms12-027.aspx.

8. Maharlito Aquino. (September 20, 2013). *TrendLabs Security Intelligence Blog.* "BLYPT: A New Backdoor Family Installed via Java Exploit." Last accessed May 2, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/blypt-a-new-backdoor-family-installed-via-java-exploit/.

9. The MITRE Corporation. (2013). *CVE.* "CVE-2013-1493." Last accessed May 2, 2014, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1493.

10. The MITRE Corporation. (2013). *CVE.* "CVE-2013-5065." Last accessed May 2, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5065.

11. Microsoft. (2014). *Security TechCenter.* "Microsoft Security Bulletin MS14-002 – Important." Last accessed May 8, 2014, https://technet.microsoft.com/en-us/library/security/ms14-002.aspx.

12. Trend Micro Incorporated. (2014). "Managing Your Legacy Operating Systems: What Will Life Be Like After Windows XP?" Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#managing_your_legacy_systems.

13. Trend Micro Incorporated. (2013). "Malicious Network Communications: What Are You Overlooking?" Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#malicious-network-communications.

14. David Sancho, Jessa dela Torre, Matsukawa Bakuei, Nart Villeneuve, and Robert McArdle. (2012). "IXESHE: An APT Campaign." Last accessed May 2, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf.

15. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_ESILE.SMEX." Last accessed May 2, 2014, http://about-threats.trendmicro.com/uk/malware/BKDR_ESILE.SMEX.

16. Tsung Pei Kan, Chiu Ming-Chang, Wu Ming-Wei Benson, and Fyodor Yarochkin. "Hunting the Shadows: In Depth Analysis of Escalated APT Attacks." Last accessed May 13, 2014, https://media.blackhat.com/us-13/US-13-Yarochkin-In-Depth-Analysis-of-Escalated-APT-Attacks-WP.pdf.

17. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "DUNIHI Worms Its Way into Removable Drives." Last accessed May 2, 2014, http://about-threats.trendmicro.com/us/webattack/3138/DUNIHI+Worms+Its+Way+Into+Removable+Drives.

18. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "DUNIHI." Last accessed May 2, 2014, http://about-threats.trendmicro.com/us/malware/DUNIHI.

19. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "JAVA_EXPLOYT.HI." Last accessed May 2, 2014, http://about-threats.trendmicro.com/us/malware/JAVA_EXPLOYT.HI.

20. NIST. (2014). *National Vulnerability Database.* "Vulnerability Summary for CVE-2013-1493." Last accessed May 2, 2014, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1493.

21. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_BLYPT.A." Last accessed May 2, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_BLYPT.A.

22. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_BLYPT.B." Last accessed May 2, 2014, http://about-threats.trendmicro.com/apac/malware/BKDR_BLYPT.B.

23. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR64_BLYPT.B." Last accessed May 2, 2014, http://about-threats.trendmicro.com/us/malware/BKDR64_BLYPT.B.

24. Trend Micro Incorporated. (2013). "The Enterprise Fights Back (Part I): Securing Your Network Infrastructure Against Targeted Attacks." Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#securing-your-network-infrastructure-against-targeted-attacks.

25. Trend Micro Incorporated. (2014). "The Enterprise Fights Back (Part IV): Building Threat Intelligence." Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#building_threat_intelligence.

26. Trend Micro Incorporated. (2014). "The Enterprise Fights Back (Part III): Building an Incident Response Team." Last accessed May 2, 2014, http://about-threats.trendmicro.com/ent-primers/#building_an_incident_response_team.

27. Jim Gogolinski. (2013). "Suggestions to Help Companies with the Fight Against Targeted Attacks." Last accessed May 2, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-suggestions-to-help-companies-with-the-fight-against-targeted-attacks.pdf.

28. Trend Micro Incorporated. (2014). "Deep Discovery Advanced Network Security." Last accessed May 2, 2014, http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/.

Created by:

**TrendLabs**

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

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.




Securing Your Journey to the Cloud