TREND MICRO™

Securing Your Journey to the Cloud

# Trends in Targeted Attacks

By Nart Villeneuve

A Trend Micro White Paper | **October 2011**

## TABLE OF CONTENTS





Trends in Targeted Attacks

## I. ABSTRACT


Targeted attacks constitute a threat category that refers to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. Often leveraging social engineering and malware, these attacks seek to maintain a persistent presence within the victim's network so that the attackers can move laterally throughout the target's network and extract sensitive information. These attacks are most commonly aimed at civil society organizations, business enterprises and government/military networks. Given the targeted nature of these attacks, the distribution is low; however, the impact on compromised institutions remains high. As a result, targeted attacks have become a priority threat.

This paper will examine the stages of a targeted attack from the reconnaissance phase through to the data ex-filtration phase and will explore trends in the tools, tactics and procedures used in such attacks. It will conclude with a high-level examination of mitigation strategies that leverage threat intelligence and data security in order to provide organizations with the information they need to increase their human capacity, to analyze and respond to threats and to customize technical solutions in ways that best fit their own defensive posture.


## II. INTRODUCTION

Targeted attacks that exploit vulnerabilities in popular software in order to compromise specific target sets are becoming increasingly commonplace. These attacks are not automated and indiscriminate nor are they conducted by opportunistic amateurs. These computer intrusions are staged by threat actors that aggressively pursue and compromise specific targets. Such attacks are typically part of broader campaigns, a series of failed and successful compromises, by specific threat actors and not isolated attacks. The objective of the attacks is to obtain sensitive data.

Prior to the highly publicized "Aurora" attack on Google in late 2009, which also affected at least 20 other companies, there was little public awareness regarding targeted malware attacks.[1] However, such attacks have been taking place for years and continue to affect government, military, corporate, educational, and civil society networks today. While such attacks against the U.S. government and related networks are now fairly well-known, other governments and an increasing number of companies are facing similar threats. Earlier this year, the Canadian, South Korean, and French governments have all experienced serious security breaches into sensitive networks.[2] Recently, the European Commission and the External Action Service were also compromised and there was a significant breach at the International Monetary Fund.[3] The security firm RSA was also recently compromised as a result of a targeted malware attack.[4] Following the breach at RSA, the data stolen during that attack may have aided subsequent attacks against L-3 Communications, Northrop

[1] For the attacks on Google, see http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[2] For the compromises in Canada, South Korea and France, see www.cbc.ca/news/technology/story/2011/02/17/cyber-attacks-harper142.html, www.computerworld.com/s/article/9213741/French_gov_t_gives_more_details_of_hack_150_PCs_compromised, http://english.yonhapnews.co.kr/national/2011/03/07/86/0301000000AEN20110307002200315F.html

[3] http://euobserver.com/9/32049, www.bbc.co.uk/news/technology-13748488

[4] www.rsa.com/node.aspx?id=3872010/01/new-approach-to-china.html, www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Grumman and Lockheed Martin.[5] The trend continues in 2011 with compromises at the Oak Ridge National Laboratory and the Pacific Northwest National Laboratory in the United States.[6]

Such targeted attacks leveraging social engineering have been ongoing since at least 2002.[7] The first such campaign to receive significant press coverage occurred in March 2004 and was known as Titan Rain.[8] The attacks were revealed by TIME magazine in 2005 and highlighted the emergence of "cyber-espionage" and threat it poses to government and military networks. In 2006, The Guardian reported on a series of attacks against British MP's which leveraged highly targeted email malware capable of stealing sensitive documents.[9] The following year Der Spiegel reported on attacks against the German government that used malware embedded in popular office files such as Microsoft Word and Excel.[10] In 2007, the New York Times revealed that the Oak Ridge National Laboratory in the Unites States was compromised and that the attackers had used targeted phishing emails.[11]

In 2008, BusinessWeek documented the extension of such threats to defense contractors and other large, private enterprises.[12] This report revealed the social engineering techniques used to lure potential victims into executing malware allowing the attackers to take full control of their computers. Finally, BusinessWeek also revealed that the same attackers had expanded their target set to include the civil society sector as well. In the same year, researchers demonstrated the connection between targeted malware attacks using social engineering and malicious documents.[13] Several presentations at security conferences revealed that attackers were using exploits in popular software packages to send malicious documents (such as PDFs, DOCs, XLSs and PPTs) using contextually-relevant, socially engineered emails to a variety of targets. Moreover, an analysis of the malware as well as the command and control infrastructure revealed that attacks against the corporate sector, the government and military sector as well as civil society could be linked to the same threat actors.[14]

In 2009, the New York Times revealed the existence of GhostNet, a cyber-espionage network that had compromised over 2000 computers in 103 countries.[15] Among the victims, there were high concentrations of compromised computers at Ministries of Foreign Affairs, Embassies and Diplomatic missions around the world. The attackers used socially engineered emails to lure victims into clicking on malicious attachments that allowed the attackers to gain control over these compromised system. After the initial compromise, the attackers would instruct the compromised computers to download a Trojan, known as gh0st or gh0stRAT, which allowed the attackers to take real-time control over the compromised system.

[5] www.eweek.com/c/a/Security/Northrop-Grumman-L3-Communications-Hacked-via-Cloned-RSA-SecurID-Tokens-841662/, www.nytimes.com/2011/06/04/technology/04security.html

[6] www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/, www.reuters.com/article/2011/07/06/us-energylab-hackers-idUSTRE7654GA20110706

[7] Diplomatic cables leaked by WikiLeaks reveal that the U.S. government suffered ongoing intrusions by one particular threat actor since 2002. http://cablesearch.org/cable/view.php?id=08STATE116943. The following overview of targeted attacks build off initial research by Richard Stiennon www.threatchaos.com/home-mainmenu-1/16-blog/571-strategic-industries-should-go-on-high-alert

[8] www.time.com/time/printout/0,8816,1098961,00.html

[9] www.guardian.co.uk/politics/2006/jan/19/technology.security

[10] www.spiegel.de/international/world/0,1518,502169,00.html

[11] www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html?ref=technology

[12] www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm

[13] http://events.ccc.de/congress/2007/Fahrplan/attachments/1008_Crouching_Powerpoint_Hidden_Trojan_24C3.pdf, http://isc.sans.org/presentations/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf, http://isc.sans.edu/diary.html?storyid=4177

[14] http://isc.sans.org/presentations/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf

[15] www.nytimes.com/2009/03/29/technology/29spy.html, www.nartv.org/mirror/ghostnet.pdf



Trends in Targeted Attacks

The network was named GhostNet after the attackers' use of gh0stRAT. The attackers were able to maintain persistent control over that compromised computers. In fact, the average length of compromised was 145 days; the longest infection span was 660 days.

This discovery highlighted the fact that attackers do not need to be technically sophisticated or advanced. With some functional but less-than-impressive code along with the publicly available gh0stRAT tool these attackers were able to compromise and maintain persistent control of embassies around the world. This research also showed that attackers can and do make mistakes which allow researchers to uncover the hidden components of their operations.

A year later, the New York Times again reported on the existence of another cyber-espionage network.[16] The report enumerated a complex and tiered command and control infrastructure. The attackers misused a variety of services including Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail in order to maintain persistent control over compromised computers. This top layer directed compromised computers to accounts on free web hosting services, and as the free hosting servers were disabled, to a stable core of command and control servers. While less than 200 computers were compromised, almost all in India, the attackers were able to steal data that included Secret, Confidential and Restricted documents.

In 2010, the Christian Science Monitor reported that there were significant breaches in the networks of three major oil companies: Marathon Oil, ExxonMobil, and ConocoPhillips.[17] The CSM reported that senior executives were targeted with socially engineered emails that contained malware. In 2011, McAfee reported similar attacks against oil companies around the world. Companies in the energy and petrochemical industries were also targeted.[18] McAfee released another report, "Shady RAT" that documented intrusion into at least 70 organizations around the world.[19]

Trend Micro discovered an ongoing series of targeted attacks, known as "LURID," that successfully compromised 1465 computers in 61 different countries. LURID attacks appear to be another separate but related Enfal network with a geographic focus. Although there is clear evidence that the Tibetan community is also a target, interestingly the majority of victims of this attack were concentrated in Russia and other CIS countries. From our analysis, we ascertained that numerous embassies and government ministries, including some in Western Europe, were been compromised as well as research institutions and agencies related to the space industry.[20]

While targeted malware attacks are currently used to steal data, future attacks could aim to modify data. The emergence of Stuxnet in 2010 revealed that targeted malware attacks could be used to interfere with industrial control systems.[21] Stuxnet was designed to modify the behaviors of programmable logic controllers (PLCs) for specific frequency converter drives manufactured by two companies, one in Finland and the other in Iran.[22] The target of the attack is widely believed to be Iran's uranium enrichment capability.[23] Stuxnet demonstrates that future threats could focus on sabotage, not just espionage.

[16] www.nytimes.com/2010/04/06/science/06cyber.html, www.nartv.org/mirror/shadows-in-the-cloud.pdf

[17] www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

[18] www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

[19] www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[20] http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/12802_trend_micro_lurid_whitepaper.pdf

[21] http://threatinfo.trendmicro.com/vinfo/web_attacks/Stuxnet%20Malware%20Targeting%20SCADA%20Systems.html

[22] www.symantec.com/connect/blogs/stuxnet-breakthrough

[23] http://threatpost.com/en_us/blogs/report-iran-resorts-rip-and-replace-kill-stuxnet-072211

While the distribution of targeted attacks remains low, the impact on high profile institution remains high. Most Internet users will never be victims of targeted attacks and are much more likely to face a variety of common threats such as fake security software (FAKEAV) and banking Trojans (Zeus, SpyEye, Bancos).[24] However, the methods used in targeted attacks being adopted by the criminal actors that have a much larger target set. For example, exploits used in a targeted attack may eventually find their way into exploit packs that are sold in underground forums. Moreover, those in the cybercrime underground may be increasingly interested in and may be profiting from the extraction of sensitive information. In fact, a recent series of attacks, that can be loosely considered as targeted, involved the use of ZeuS and a well known cybercrime infrastructure to extract documents from U.S. government networks.[25] Moreover, there have been some suggestions that threat actors involved in cyber-espionage are directly cooperating with cyber-criminals.[26]

The boundaries between online crime and espionage appear to be blurring, making issues of attribution increasingly more complex. At a minimum, these developments indicate that attacks that are often considered to be criminal in nature, such as the targeting of banking credentials of individuals, also pose a threat to those in the government and military sectors. It is well understood that these attackers aim to maximize their financial gain from malware attacks. Therefore, these developments may indicate that there is an emerging market for sensitive information as criminal networks seek to monetize such information and develop their capabilities in this area.[27]

## Targeted Attacks

Targeted attacks constitute a threat category that refers to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. Often leveraging social engineering and malware, these attacks seek to maintain a persistent presence within the victim's network so that the attackers can move laterally throughout the target's network and extract sensitive information. While information may trickle out in the press about a single victim or a single attack, there are usually many more. Moreover, they are often geographically diverse and most commonly aimed at civil society organizations, business enterprises and government/military networks. Given the targeted nature of the attacks, the distribution is low; however, the impact on compromised institutions remains high. As a result, targeted attacks have become a high priority threat.

In a typical targeted attack, a target receives a socially engineered message—such as an email or instant message—that encourages the target to click on a link or open a file. The links and files sent by the attacker contain malware that exploits vulnerabilities in popular software such as Adobe Reader (e.g. PDFs) and Microsoft Office (e.g. DOCs). The payload of these exploits is malware that is silently executed on the target's computer. This allows the attackers to take control of and obtain data from the compromised computer. The attackers may then move laterally throughout the target's network and are often able to maintain control over compromised computers for extended lengths of time. Ultimately, the attackers locate and ex-filtrate sensitive data from the victim's network.

[24] **Cybercrime:** http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/wp04_cybercrime_1003017us.pdf
**Zeus:** http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf
**FAKEAV:** http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/unmasking_fakeav__june_2010_.pdf

[25] www.nartv.org/mirror/kneber_spearphishing_crimeware.pdf, www.nartv.org/2010/08/27/crime-or-espionage/
www.nartv.org/2010/09/09/crime-or-espionage-part-2/, http://krebsonsecurity.com/2011/01/white-house-ecard-dupes-dot-gov-geeks/

[26] www.theregister.co.uk/2011/09/13/apt_botnet_symbiosis/print.html, http://krebsonsecurity.com/2011/01/ready-for-cyberwar/

[27] www.krebsonsecurity.com/2010/02/zeus-a-virus-known-as-botnet/



Trends in Targeted Attacks

These targeted attacks are rarely isolated events. It is more useful to think of them as campaigns—a series of failed and successful attempts to compromise a target over a period of time. Therefore the specificity of the attacker's prior knowledge of the victim affects the level of targeting associated with a single attack. As a result, some attacks appear to be less precise, or "noisy," and are aimed at acquiring information to be used in a future, more precise attack.[28] Such "spearphishing" attacks are "usually directed toward a group of people with a commonality" as opposed to a specific target but are useful for gaining an initial foothold in a future target of interest.[29] When technical information regarding the target's preferred antivirus products and specific versions of installed software is combined with intelligence acquired from previous attacks and/or harvested from publicly available information and social networking platforms, an advanced combination of social engineering and malicious code can be deployed against the target.[30]

Analyzing the stages of an attack can provide insight into the tools, tactics and procedures of the attackers.[31] This behavior helps indicate whether an attack can be linked to a broader campaign and helps build intelligence that can be used to inform incident response procedures and help mitigate future advances by the attacker. While there is considerable overlap, the anatomy of an attack can be segmented into six components:

- **Reconnaissance/Targeting**—profiling the target in order to acquire information concerning their defensive posture and deployed software as well as a contextual understanding of roles and responsibilities of key personnel and relevant themes to inform social engineering.
- **Delivery Mechanism**—selection of a delivery mechanism, such as Email or IM, in conjunction with social engineering and embedding malicious code into a delivery vehicle (such as exploit code and malware embedded in a PDF document).
- **Compromise/Exploit**—execution of malicious code, usually involving human interaction after successful social engineering, that results in a compromise that delivers control of the target system to the attackers.
- **Command and Control**—communication from the compromised system to a server under the attacker's control. This could be a server component of a remote access Trojan (RAT) or a server that receives "check ins" that notify the attacker of a successful compromise and allows the attackers to issue commands and download additional malware to the compromised system.
- **Persistence/Lateral Movement**—mechanisms that allow malware to survive a reboot, continued remote access (e.g. through legitimate VPN credentials and/or additional backdoors) and lateral movement throughout the network in order to enumerate file systems and locate sensitive information.
- **Data Ex-filtration**—staging and transmitting of sensitive data, often involving encryption and compression, to locations under the attacker's control.

[28] http://blog.trendmicro.com/how-sophisticated-are-targeted-malware-attacks/

[29] www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

[30] http://blog.trendmicro.com/highly-targeted-attacks-and-the-weakest-links/

[31] http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/,
http://computer-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy and www.rsa.com/innovation/docs/SBIC_RPT_0711.pdf

The threat actors behind targeted malware attacks do not always use zero day vulnerabilities—exploits for vulnerabilities for which there is no patch available. While some might believe that the threat actors behind targeted malware attacks have mythical capabilities, both in terms of their operational security and the exploits and malware tools used, they, in fact, often use older exploits and simple malware.[32] The objective of these attacks is to obtain sensitive data; the malware used in the attacks is just an instrument. They will use whatever is required to gain entry based on reconnaissance. In addition, they will adjust their tactics in reaction to the defenses of the victim.

Therefore, an active defense requires a combination of technical and human capacity with an emphasis on data protection. First, technical solutions for defense, monitoring and remediation must be in place. While organizations typically maintain defenses such as antivirus software, intrusion detection/prevention systems, firewalls and other security products, monitoring, logging and analysis of the outputs of these tools is critically important.[33] The ultimate objective behind targeted attacks is the acquisition of sensitive data. Therefore data loss prevention strategies that focus on identifying and protecting confidential information are critically important.  Enhanced data protection and visibility across the enterprise provides the ability control access to sensitive data and to monitor and log successful and unsuccessful attempts to access it. Enhanced access controls and logging capabilities allow security analysts to locate and investigate anomalies, respond to incidents and initiate remediation strategies and damage assessments.

Building human capacity is an integral component of defense. The threat actors behind targeted attacks make considerable effort to improve their social engineering because they know that exploiting the human factor is a critical component of a successful compromise. As a result, education and training programs are a key. Staff and employees must be aware of targeted attacks and must be expecting them. In addition, the policies and procedures must be in place to both minimize exposure and provide clear and consistent processes that allow staff to report suspected attacks. In order to ensure that reporting and investigation occur, it is important to identify who owns that process and who can trigger the remediation and damage assessment strategy if a compromise should occur.

Information security analysts armed with threat intelligence are a critical component of defense. Threat intelligence provides information on the tools, tactics and procedures of threat actors. Understanding these processes allows information security analysts to customize defensive strategies to counter the specific threats an organization faces. As a result, an organization can integrate threat intelligence, increased human capacity, and technical solutions in a customized way that best fits their own defensive posture.

[32] http://news4geeks.net/2011/08/04/researcher-follows-rsa-hacking-trail-to-china/

[33] http://us.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/datalossprevention/wp02_dlp-compliance-solutions_100225us.pdf



Trends in Targeted Attacks

## III. TRENDS IN TARGETED ATTACKS

### Reconnaissance/Targeting

The use of social engineering in targeted malware attacks is ubiquitous. Social engineering refers to techniques that "exploit the human element" by manipulating trust.[34] The objective of social engineering is to manipulate individuals into revealing sensitive information or executing malicious code. In order to increase the efficacy of social engineering, information gleaned from a variety of public sources including business profiles and social networking sites is often used.

Social engineering attacks typically leverage current events, subject areas of interest and business functions related to the target. Since malware attacks are more likely to be successful if they appear to have originated from someone the target knows, the delivery mechanism, usually an email, is often specifically addressed to the target and appears to have originated from someone within the target's organization or someone in target's social network.[35] In extremely targeted cases, attackers may actually send email directly from a compromised, but real, email account of someone the target knows and trusts.

There are a variety of social engineering techniques that are commonly seen in the wild. In order to masquerade as a real person that is known to the target, attackers will actually register email addresses with popular webmail services such as Gmail, Yahoo! Mail and Hotmail using the names of the target's colleagues. While there are still attacks that spoof legitimate business or governmental email addresses in order to convey legitimacy, these attempts may be more easily detected.[36] The attacker's shift to personal email addresses also reflects the fact that employees often check their personal email accounts from work and sometimes use these accounts for business purposes.[37]

Attackers will often leverage authority relationships, such as boss-employee, in order to communicate a sense of importance so that the target will open a malicious attachment. To increase the authenticity, attackers will also use the classification markings of the government and intelligence services.[38]

In order to help detect social engineering attacks, messages can be assessed for accuracy, language, spelling and grammar as well as relevance to the target. However, attackers are now using techniques such as forwarding legitimate emails, from mailing lists or from emails acquired from previously successful attacks, along with malicious links and attachments. As users grow weary of unknown attachments and scan them with anti-malware products, attackers are also now sending two or more attachments with one socially engineered email with only one of the attacments containing malicious code. If the target manually scans one of the attachments and no malware is detected, the user may open the other attachments, including the malicious one, without having manually scanned them believing that they are all clean.

[34] http://portal.acm.org/citation.cfm?id=1067721.1067728&coll=ACM&dl=ACM

[35] www.nartv.org/mirror/shadows-in-the-cloud.pdf and http://portal.acm.org/citation.cfm?id=1290958.1290968&coll=GUIDE&dl=GUIDE&CFID=74760848&CFTOKEN=96817982

[36] For example, the information contained in the email headers can be processed for anomalies, and information such as originating IP address and the route an email took to get to its destination can indicate that an email did not originate from the sender it claims to be from.

[37] www.computerworld.com/s/article/print/9015092/White_House_use_of_outside_e_mail_raises_red_flags?taxonomyName=IT+in+Government&taxonomyId=13 and www.computerworld.com/s/article/print/9114934/Update_Hackers_claim_to_break_into_Palin_s_Yahoo_Mail_account?taxonomyName=Networking&taxonomyId=16

[38] www.nartv.org/2010/09/09/crime-or-espionage-part-2/

Attackers engage in reconnaissance not just to improve the level of social engineering used in an attack, but to profile the software used by the target. One of the techniques used, in conjunction with social engineering, leverages the "res://" protocol in order to determine the software present in the target's environment. This information can then be used in future attacks to identify specific applications in order to select an appropriate exploit.[39] The res:// protocol, which was built into Internet Explorer since version 4.0, can be used to remotely detect specific software present on a computer by simply getting a user to visit a Web page from a browser.[40]

We have found attacks that have used the res:// protocol to check a target's environment for file-sharing programs, web browsers, remote administration tools, email clients, download managers, and media players. In addition, attackers are able to detect security software, including major antivirus products and personal firewalls, as well as the PGP encryption software and Microsoft security updates. They also check for virtual machine software, such as VMWare, which may indicate that they are being investigated by the security community.

The information obtained via social engineering, whether or not the attack was a success or a failure, is incorporated by attackers in future attacks.

### Delivery Mechanism

The delivery mechanism in a targeted attack is typically an email. However, attackers may also use instant messaging services to entice the target into clicking a malicious link or downloading malware. The emails are often sent from webmail accounts, especially Gmail, or from spoofed email addresses, such as government email addresses, through compromised mail servers.[41] Often, the email will contain an attached document, such as a PDF a Word Document, Excel spreadsheet or PowerPoint presentation. These attachments contain malicious code designed to exploit vulnerabilities is specific version Adobe's PDF reader or Flash and versions of Microsoft Office.

However, attackers still use executables as attachments, or provide links to download them. Malware has been discovered that uses Unicode characters to disguise the fact that it is an executable. This technique allows the attackers to make executables files that end with an ".exe" suffix, appear to end in ".doc." In order to take advantage of default Windows configurations that do not show file extensions, attackers have attempted to trick users into thinking that executables are simply directories by making their executable's icon an image of a folder.[42]

The attackers still hide executables inside of compressed file formats such as ZIP or RAR. Sometimes, these archive files are encrypted to avoid network-based malware scanning and the attackers provide the password to decrypt the archive within the socially engineered email.

Finally, rather than include an attachment with a socially engineered email, attackers will simply include links to web pages that contain exploit code. Known as "drive by" exploits, these web pages contain code designed to exploit vulnerabilities in popular browsers and browser plug-ins to install malware on the target's computer.

[39] http://blog.trendmicro.com/how-sophisticated-are-targeted-malware-attacks/

[40] http://xs-sniper.com/blog/2007/07/20/more-uri-stuff-ies-resouce-uri/

[41] http://contagiodump.blogspot.com/2011/04/contagio-data-spear-phish-email-senders.html

[42] www.nartv.org/2010/03/07/malware-attacks-on-solid-oak-after-dispute-with-greendam/ and www.f-secure.com/weblog/archives/00001675.html



Trends in Targeted Attacks

Rather than send the target to a completely unknown web page, attackers are now compromising legitimate websites that are contextually relevant to the target and embedding "iframes" that silently load exploits from locations under the attackers control.[43]

While email has been the most common delivery mechanism for targeted attacks, there are increasing reports of attempts made using instant messaging and social networking platforms. There have been reports of Facebook messages being used as delivery mechanisms and the New York Times reported that the "Aurora" attack on Google originated with an instant message.[44]

### Compromise/Exploit

In order to install malware on the target's computer, attackers will use malicious code that is designed to exploit a vulnerability, or "bug," in a particular piece of software. Attackers are most often exploiting flaws in Adobe's PDF reader, Adobe Flash and Microsoft Office. The attack surface among these software packages is being extended by embedding one file format inside another. For example, a recent attack involved embedding a malicious Flash object inside a Microsoft Excel spreadsheet.[45] As the vulnerabilities are fixed, or "patched" attackers seek new exploits known as zero day exploits. The term "zero day" refers to exploits for which there is no patch available from the software vendor.

While several high profile campaigns, such as the "Aurora" attacks against Google and the recent breach of RSA, have leveraged zero day exploits in order to compromise their targets, many targeted attacks do not employ the use of zero day exploits.[46] In fact, some older, reliable exploits such as CVE-2009-3129, CVE-2010-3333, CVE-2010-2883 for Adobe PDF Readers and Microsoft Office are still in use. In addition, attackers may use "drive-by exploits," such as the zero day exploit for Internet Explorer that was used in "Aurora" (as described in MS10-002), not just malicious documents.

Vulnerabilities in popular webmail services have been exploited to compromise email accounts. Personal email is increasingly becoming a target as users who check their personal email accounts at work may provide attackers with sensitive information that may be related to their company.[47] Moreover, their personal email account can be used to stage future targeted attacks. While there was considerable media attention regarding a recent phishing attack on Gmail users, there has been a variety of recent attacks on popular Webmail platforms.[48] In addition to attacks that exploited Gmail, Hotmail and Yahoo! Mail users have also been targeted. While the attacks appear to have been separately conducted, these have some significant similarities.

Google also previously revealed that attackers are exploiting a vulnerability in the MHTML protocol in order to target political activists who use Google's services.[49] Trend Micro researchers in Taiwan revealed a phishing attack that exploited a vulnerability in Microsoft's Hotmail service. In fact, rather than clicking a malicious link,

[43] www.nartv.org/2010/07/29/human-rights-and-malware-attacks/

[44] www.nytimes.com/2010/04/20/technology/20google.html and http://blogs.aljazeera.net/asia/2011/03/23/china-and-google-detailed-look

[45] http://contagiodump.blogspot.com/2011/03/cve-2011-0609-adobe-flash-player.html

[46] For example, of the 251 targeted malware attacks received by contagiodump.blogspot.com, only 10 were zeroday.

[47] http://blog.trendmicro.com/targeted-attack-exposes-risk-of-checking-personal-webmail-at-work/

[48] http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html and http://blog.trendmicro.com/targeted-attacks-on-popular-web-mail-services-signal-future-attacks/ http://contagiodump.blogspot.com/2011/08/targeted-attacks-against-personal-gmail.html

[49] http://googleonlinesecurity.blogspot.com/2011/03/mhtml-vulnerability-under-active.html

[50] http://blog.trendmicro.com/trend-micro-researchers-identify-vulnerability-in-hotmail

even simply previewing the malicious email message could compromise a user's Hotmail account.[50] Trend Micro researchers also alerted Yahoo! of an attempt to exploit Yahoo! Mail by stealing users' cookies in order to gain access to their email accounts.[51]

Attackers are able to successfully exploit their targets because their reconnaissance, along with knowledge gained from previous attacks, allows them to determine what exploits to deploy. If certain attack vectors are well secured, attackers will locate areas of vulnerability elsewhere.

### Command and Control

When malware is executed on the target's system, it "checks in" with one or more servers under the control of the attackers. Command and control mechanisms allow the threat actors to confirm that an attack has succeed, typically supplies them with some information about the target's computer and network and allows the attackers to issue commands to the compromised target. The initial malware is often a simple, small "dropper," so the attackers will often instruct the compromised computer to download components that have additional functionality. The attackers will commonly instruct the compromised computer to download second stage malware, such as a remote access tool/Trojan (RAT) which allows the attackers to take real time control of the system.

Keeping the communication channel between the compromised machine and the command and control server open is important to the threat actors behind targeted malware attacks. As network monitoring software improves and is able to identify malicious and even anomalous traffic, an increasing amount of obfuscation and stealth is being used to conceal command and control network traffic. Increasingly, malware is making use of cloud-based command and control in an attempt to blend in to normal network traffic.[52] These services can be used as update mechanisms that inform the compromised host of new command and control servers, or they can be used as command and control exclusively.

For example, there are malware samples that use webmail accounts as elements of command and control. When malware connects to well known services such as Gmail or Yahoo! Mail the session is protected by SSL encryption and therefore network monitoring software will be unable to determine if the subsequent traffic is malicious or not. The attackers use such webmail accounts to send commands to compromised hosts, update compromised hosts with additional malware tools or components, and ex-filtrate data from compromised hosts. In addition to webmail services, could-based storage services are being used to host additional malware components. The use of such services provides the attackers with command and control infrastructure that cannot be easily detected as malicious.

Some threat actors use compromised legitimate sites as command and control servers. This allows the attackers some element of deception because even if the network communication is detected as anomalous, upon further inspection the website will be determined to be legitimate. One threat actor simply embeds commands within HTML comment tags in web pages on compromised, legitimate web sites. The malware simply visits these pages and extracts and decodes the commands. The use of custom base64 alphabets and XOR makes decoding the command and the network traffic increasingly difficult. In addition, attackers are making use of stolen or forged SSL certificates in an attempt to make their network traffic appear to be legitimate.

[51] http://blog.trendmicro.com/targeted-attacks-on-popular-web-mail-services-signal-future-attacks/

[52] www.nartv.org/2010/10/22/command-and-control-in-the-cloud/ and http://blog.zeltser.com/post/7010401548/bots-command-and-control-via-social-media



Trends in Targeted Attacks

Some threat actors continue to register domains names for their own exclusive use while others rely on dynamic DNS services for free sub-domains. The free sub-domains provided by dynamic DNS services are often used in conjunction with often off-the-shelf RAT's such as gh0st and poisonivy. While the threat actors are offline, the domain names will often resolve to localhost or invalid IP addresses, and when they come online the domains will resolve to the IPs of the threat actors. Third-party locations can be used to update these RATs as needed.

Trend Micro uncovered a campaign of targeted attacks that successfully compromised defense industry companies in Japan, Israel, India and the USA. The second stage of the attacks involved two components one of which contained custom DLLs created for specific targets and the other a RAT known as "MFC Hunter." This RAT contains three components, the malware that is installed on the victim's computer, the client through which the attacker controls the victim's computer and a "hub" which acts as an intermediary disguising the true location of the attacker.[53] A report by Dell SecureWorks detailed the use of a similar hub known as "htran" through error messages that disclosed the attackers' true locations.[54]

In addition to redundancy, the attackers also seek to obfuscate their malicious network traffic by using intermediaries and in an attempt to blend in with legitimate traffic. As a result, threat actors are able to leverage a variety of strategies to maintain communications between compromised hosts and their command and control infrastructure.

### Persistence/Lateral Movement

Once inside the target's network, the threat actors engaging in targeted malware attacks seek to accomplish two objectives. First, they seek to maintain persistent access to the targets network and second they seek to move laterally throughout the network locating data of interest for ex-filtration. In order to maintain persistence, the initial malware payload will have some method to ensure that it is restarted after a reboot of the compromised computer. In many cases, the persistence mechanism will consist of simple methods such as adding the malware executable to the windows "startup" folder, modifying the Run keys in the Windows Registry or installing an application as a Windows Service. The security firm Mandiant found that 97% of the targeted malware they analyzed used these simple mechanisms.[55] However, there are other methods used to maintain persistence that are less well known. One method known as "DLL search order hijacking" involves placing malicious DLL's in specific locations with specific names so that they are loaded by legitimate applications leaving no forensic traces.[56]

Once inside the system, attackers will move laterally throughout the network. They typically download remote-access-Trojans (RATs) or tools that allow them to execute shell commands in real time on the compromised host. In addition, they may seek to escalate their privileges to that of an administrator using techniques such as "pass the hash" and seek out key targets such as mail servers.[57] The attackers often download and use tools to "bruteforce" attack database servers, extract email from Exchange servers and attempt to acquire legitimate access, such as VPN credentials, so that they may maintain access to the network even if their malware is discovered. As the attackers move throughout the target's network they explore and collect information that can be used in future attacks or information that can be prepared for ex-filtration.

[53] http://blog.trendmicro.com/japan-us-defense-industries-among-targeted-entities-in-latest-attack/

[54] www.secureworks.com/research/threats/htran/

[55] www.mandiant.com/products/services/m-trends/

[56] http://blog.mandiant.com/archives/1207

[57] www.mandiant.com/products/services/m-trends/

### Data Ex-filtration

The primary objective of the threat actors behind targeted attacks is the transmission of sensitive data to locations under the attacker's control. In order to accomplish this objective, the attackers will collect the desired data and compress it and then split the compressed file into chuncks that can be transmitted to locations under the attacker's control. A variety of transmission methods are used such as FTP and HTTP, however, attackers are now making use of more secure methods such as ex-filtrating data using the Tor anonymity network.[58]

With some attacks, data ex-filtration will occur quite quickly. Often, the malware will send directory and file listings to the command and control server. The attacker may then request specific files or directories to be uploaded. Threat actors that rely on RATs may use the built-in file transfer functionality that typically comes with these tools.

In cases where the attackers have an established presence, data, such as the contents of mail servers, will be collected and moved to a staging area for ex-filtration.[59] The attackers will typically use compression tools, such as Rar, to package the data for ex-filtration. The attacker will then return from time to time and ex-filtrate new data.

## IV. DETECTION AND MITIGATION

The precise nature of targeted attacks increases the difficulty of defense. With significant reconnaissance, and information gained from previously successful incursions into the target's network, the threat actors behind targeted attacks are able to customize their attacks to increase the probability of success. For example, they can ensure that the malware they send to their targets exploits specific software on the targets computer and they can modify the malware so that it is not detected by the security solutions deployed in the target's environment. Therefore, defenses against targeted attacks need to focus on detection and mitigation and not simply on prevention. Moreover, it is important to recognize that the ultimate objective of targeted attacks is the acquisition of sensitive data. Therefore, defensive strategies need to include the discovery and classification of sensitive data and take into account the context in which the data is being used. Once identified, appropriate access controls can be placed on such data.[60]

The ability to develop and act on threat intelligence underpins any defensive strategy. Threat intelligence refers to indicators that can be used to identify the tools, tactics and procedures of threat actors engaging in targeted attacks. This information can include the domain names and IP addresses used by attackers to send spear phishing emails or to host their command and control servers. It can refer to the presence of certain files or registry modifications on compromised computers. Threat intelligence not only refers to such malware artifacts, but also to behavioral characteristics such as the preferred tools and movement patterns of threat actors after the network has been compromised.

[58] www.nartv.org/mirror/shadows-in-the-cloud.pdf
[59] www.mandiant.com/products/services/m-trends/
[60] http://us.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/datalossprevention/esg_outside-in_approach.pdf



Trends in Targeted Attacks

While organizations will benefit significantly from threat intelligence derived from external sources, it is important that an organization begin to develop local threat intelligence based on its own unique circumstances. The ability to detect suspicious behaviors indicative of targeted attacks will depend on how effectively this threat intelligence is leveraged. The core components of a defensive strategy based on leveraging local and external threat intelligence include:

- **Enhanced Visibility**—Logs from endpoints, servers and network monitoring tools are an important and often underused resource that can be aggregated to provide a view of activity within an organization that can be processed for anomalous behaviors that could indicate a targeted malware attack.
- **Integrity Checks**—In order to maintain persistence, malware will make modifications to the file system and registry. Monitoring such changes can indicate the presence of malware.
- **Empowering the human analyst**—Humans are best positioned to identify anomalous behaviors when presented with a view of aggregated logs from across the network. This information is used in conjunction with custom alerts based on the local and external threat intelligence available.

Security solutions that protect at the endpoint and network levels are important, but the technical solutions deployed against targeted malware attacks need to empower analysts with both the tools and the threat intelligence required to identify and mitigate targeted attacks. Security analysts with access to "real-time" views of the security posture of their organization are better positioned to detect, analyze and remediate targeted attacks. In order to do so, they require visibility across the network through the use of monitoring and logging tools. Most of the hosts within a network, whether they are workstations, servers or appliances, create logs and event data that, once aggregated, can be used to detect anomalous behavior indicative of a targeted attack.

Education and training programs combined with explicit policies and procedures that provide avenues for reporting and a clear understanding of roles and responsibilities is an essential component of defense. While traditional training methods are important, simulations and exercises using real spear phishing attempts can be used to engage and educate.[61] Those that are trained to expect targeted malware attacks are better positioned to report potential threats and constitute an important source of threat intelligence. Ultimately, education can generate a more security conscious culture within an organization.

Finally, the primary objective of targeted attacks is access to sensitive data. Today, sensitive information is not only stored in databases but in the cloud and is accessible through a variety of methods including mobile devices. While securing the network layer remains an important component of any defensive strategy, it is also critically important to specifically protect data as well. Identifying and classifying sensitive data allows the introduction of access controls and enhanced monitoring and logging technologies that can alert defenders of attempts to access or transport sensitive data.[62]

[61] www.rsa.com/innovation/docs/SBIC_RPT_0711.pdf
[62] http://us.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/leakproof/wp01_leakproof_dlp_100105us.pdf

## V. CONCLUSION

Targeted attacks remain a high priority threat that is difficult to defend. These attacks leverage social engineering and malware that exploits vulnerabilities in popular software to slip past traditional defenses. While such attacks are often seen as isolated events, they are better conceptualized as campaigns, or a series of failed and successful intrusions. Once inside the network, the attackers are able to move laterally in order to target sensitive information for ex-filtration. The impact of successful attacks can be severe and any data obtained by the attackers can be used in future, more precise attacks.

However, defensive strategies can be dramatically improved by understanding how targeted attacks work as well as trends in the tools, tactics and procedures of the perpetrators. Since such attacks focus on the acquisition of sensitive data, strategies that focus on protecting the data itself, wherever it resides, are extremely important components of defense. By effectively using threat intelligence derived from external and internal sources combined with context-aware data protection and security tools that empower and inform human analysts, organizations are better positioned to detect and mitigate targeted attacks.



**TREND MICRO INC.**

10101 N. De Anza Blvd.
Cupertino, CA 95014

**U.S. toll free:** +1 800.228.5651
**phone:** +1 408.257.1500
**fax:** +1 408.257.2003

**www.trendmicro.com**