WHITE PAPER:
CUTTING THROUGH THE HYPE

Preparing the Right Defense for the New Threat Landscape

Advanced Persistent Threats: A Symantec Perspective

Who should read this paper

Chief Information Security Officers (CISO or CSO) or Directors of Information Security looking to separate hype from reality to understand how to defend themselves against Advanced Persistent Threats and other targeted attacks.

Confidence in a connected world. Symantec.

WHITE PAPER: CUTTING THROUGH THE HYPE

Advanced Persistent Threats: A Symantec Perspective

Preparing the Right Defense for the New Threat Landscape

Content

Introduction

Today we are seeing targeted cyber attacks on organizations grow progressively more sophisticated, more serious, and more extensive. In the mid-2000s, the “black hat” community evolved from adolescent hackers bent on mayhem to organized crime networks, fueling highly profitable identity theft schemes with massive loads of personal data harvested from corporate and government networks. More recently, changes in IT infrastructure and usage models, including mobility, cloud computing, and virtualization have dissolved traditional enterprise security perimeters, creating a "target-rich" environment for hackers. But perhaps the most significant new element in the threat landscape is the emergence of highly targeted, long-term, international espionage and sabotage campaigns by covert state actors.

These long-term, state-sponsored campaigns are sometimes known as Advanced Persistent Threats (APTs). The term has become a buzzword used and misused by the media, and by some technology vendors. While APTs do represent a real danger in today’s world, it is important to understand how they figure within a larger context. Only by separating reality from hype and seeing how APTs relate to the broader field of targeted attack methods and techniques will organizations be able to safeguard their information and operations in the coming decade.

What is an APT?

An APT is a type of targeted attack. Targeted attacks use a wide variety of techniques, including drive-by downloads, Microsoft SQL® injection, malware, spyware, phishing, and spam, to name just a few. APTs can and often do use many of these same techniques. An APT is *always* a targeted attack, but a targeted attack is *not necessarily* an APT.

APTs are different from other targeted attacks in the following ways:

- **Customized attacks**—In addition to more common attack methods, APTs often use highly customized tools and intrusion techniques, developed specifically for the campaign. These tools include zero-day vulnerability exploits, viruses, worms, and rootkits. In addition, APTs often launch multiple threats or “kill chains” simultaneously to breach their targets and ensure ongoing access to targeted systems, sometimes including a "sacrificial" threat to trick the target into thinking the attack has been successfully repelled.
- **Low and slow**—APT attacks occur over long periods of time during which the attackers move slowly and quietly to avoid detection. In contrast to the “smash and grab” tactics of many targeted attacks launched by more typical cybercriminals, the goal of the APT is to stay undetected by moving “low and slow” with continuous monitoring and interaction until the attackers achieve their defined objectives.
- **Higher aspirations**—Unlike the fast-money schemes typical of more common targeted attacks, APTs are designed to satisfy the requirements of international espionage and/or sabotage, usually involving covert state actors. The objective of an APT may include military, political, or economic intelligence gathering, confidential data or trade secret threat, disruption of operations, or even destruction of equipment.[1] The groups behind APTs are well funded and staffed; they may operate with the support of military or state intelligence.
- **Specific targets**—While nearly any large organization possessing intellectual property or valuable customer information is susceptible to targeted attacks, APTs are aimed at a much smaller range of targets. Widely reported APT attacks have been launched at government agencies and facilities, defense contractors, and manufacturers of products that are highly competitive on global markets. In addition, APTs may attack vendor or partner organizations that do business with their primary targets. But government-related organizations and manufacturers are not the only targets. Ordinary companies with valuable technology or intellectual property are now being targeted by nation-states. With the globalization of world economies, national security and economic security have converged.[2] Moreover, organizations that maintain and operate vital national infrastructure are also likely targets. Symantec.cloud™ security, which allows the

1-Joel Brenner, “The Calm Before the Storm,” Foreign Policy, September 6, 2011
2-Ibid.

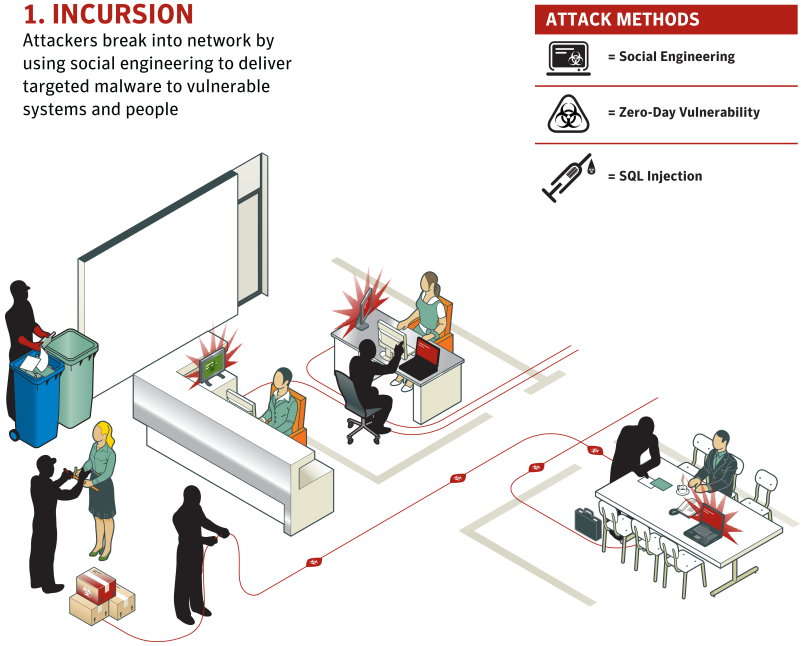
amalgamation of targeted attack data across multiple organizations, reports that only 1 in 25 of its customer organizations has been targeted. The most targeted industries are minerals and fuel (1 in 8), followed by transportation and utilities, telecommunications, and engineering.[3]

How relevant are APTs?

It should now be evident that although not every organization is a likely target of an APT, they are a real and serious threat to some organizations. Additionally, any organization can benefit from better understanding of APTs, because APT techniques are likely to be adopted over time by mainstream hackers and cybercriminals. Finally, since anyone could be the object of a targeted attack—and APTs are examples of highly advanced, long-term, and large-scale targeted attacks—if you have a better understanding of APTs, you can better defend your organization against targeted threats of any kind.

How do APT attacks work?

APT attacks are carefully planned and meticulously executed. They typically break down into four phases: incursion, discovery, capture, and exfiltration. In each phase a variety of techniques may be used, as described below.



Phase 1: Incursion

In targeted attacks, hackers typically break into the organization's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods. These methods are also used in APTs, often in concert. The main difference is that while common targeted attacks use short-term, "smash and grab" methods, APT incursions are designed to establish a beach head from which to launch covert operations over an extended period of time. Other characteristics of APT incursions include the following:

- **Reconnaissance**—APT attacks often employ large numbers of researchers who may spend months studying their targets and making themselves familiar with target systems, processes, and people, including partners and vendors. Information may be gathered both online and using conventional surveillance methods. In the case of the Stuxnet attack on organizations believed to be operating Iranian nuclear

3-Martin Lee, "Repeat Attacks Betray Attackers' Motivations," Symantec, July 13, 2011

facilities, the attack team possessed expertise in the design of the programmable logic controllers (PLCs) used for uranium enrichment that were targeted in the attack.[4]

- **Social engineering**—Incursion is often accomplished through the use of social engineering techniques, such as inducing unsuspecting employees to click on links or open attachments that appear to come from trusted partners or colleagues. Unlike the typical phishing attack, such techniques are often fed by in depth research on the target organization. In one case, a small number of human resource employees were targeted using an apparently innocuous attachment, a spreadsheet on hiring needs that appeared to come from a job listing website. In the case of Hydraq, targeted users were led to a picture-hosting website where they were infected via a drive-by-download.
- **Zero-day vulnerabilities**—Zero-day vulnerabilities are security loopholes that are unknown to the software developer and may therefore be exploited by attackers before the developer can provide a patch or fix. As a result, the target organization has zero days to prepare; it is caught off-guard. Since it takes significant time and effort to discover zero-day vulnerabilities, only the most sophisticated attacker organizations are likely to take advantage of them. APTs often use one zero-day vulnerability to breach the target, switch to a second and then a third as each point of attack is eventually fixed. This was the case with Hydraq. The Stuxnet attack was exceptional in that four separate zero-day vulnerabilities were exploited simultaneously.
- **Manual operations**—Common or massive attacks employ automation to maximize their reach. "Spray and pray" phishing scams use automated spam to hit thousands of users in hopes that a certain percentage will click on a link or attachment and trigger the incursion. On the other hand, while APTs may deploy spam, more often they target distinct individual systems and the incursion process is tightly focused—not the automated process used in non-APT attacks.

4-Nicolas Falliere, "Exploring Stuxnet's PLC Infection Process," Symantec, September 22, 2010

Phase 2: Discovery

Once inside, the attacker maps out the organization's systems and automatically scans for confidential data or, in the case of some APTs, operational instructions and functionality. Discovery may include unprotected data and networks as well as software and hardware vulnerabilities, exposed credentials, and pathways to additional resources or access points. Here again, where most targeted attacks are opportunistic, APT attacks are more methodical and go to extraordinary lengths to avoid detection.

- **Multiple vectors**—As with incursion, APTs tend to use multiple discovery techniques in combination. Once malware is present on host systems, additional tools can be downloaded as needed for the purpose of exploring software, hardware, and network vulnerabilities.
- **Run silent, run deep**—Since the goal of the APT is to remain inside the organization and harvest information over the long-term, discovery processes are designed to avoid detection at all cost. Hydraq (also known as the Aurora or Google attacks) used a number of obfuscation techniques to keep itself hidden inside victim organizations. Specifically, it used spaghetti code, a technique used to make analysis and detection of the malware more difficult.
- **Research and analysis**—Discovery efforts are accompanied by research and analysis on found systems and data, including network topology, user IDs, passwords, and so on.

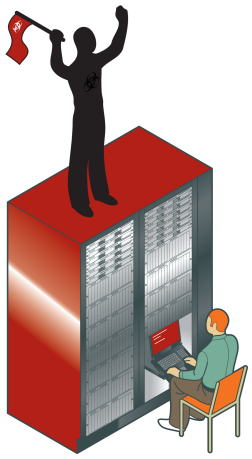
When an APT is detected, the first question asked is: How long has it been there? Not so with the typical targeted attack; if account numbers have been stolen it is not difficult to date the breach and assess the damage. With APTs, however, it may be next to impossible to determine just when the attack took place. Victims may need to comb through log files or even dispose of equipment because the incursion and discovery phases have been so well hidden.

In some cases, the APT kill-chain may be quite easy to find. But appearances can be deceptive. The obvious kill-chain may be intentionally launched to distract the victim while the perpetrators proceed undetected to their actual objectives.

3. CAPTURE

Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.



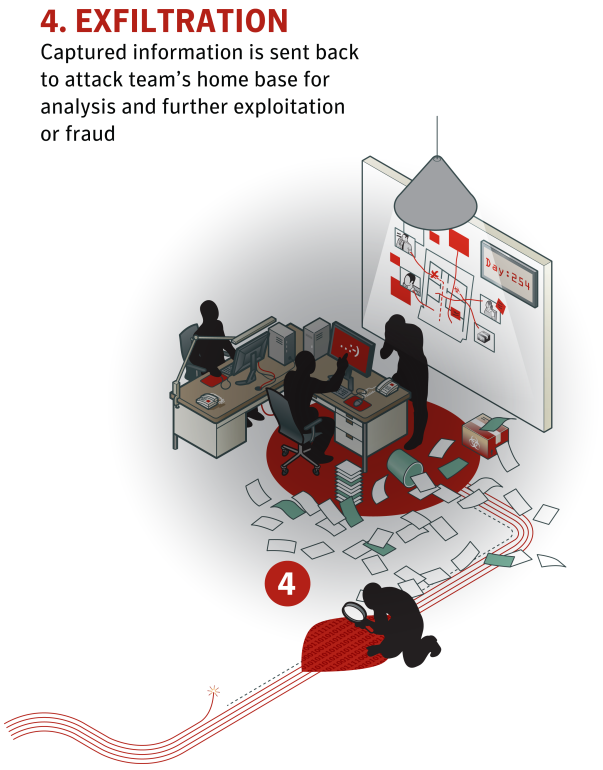
Phase 3: Capture

In the capture phase, exposed data stored on unprotected systems is immediately accessed. In addition, rootkits may be surreptitiously installed on targeted systems and network access points to capture data and instructions as they flow through the organization. In the case of Duqu, which seems to be the precursor to a future, Stuxnet-like attack, its sole purpose was to gather intelligence, which could be used to give attackers the insight they need to mount future attacks. While Duqu was not widespread, it is highly targeted, and its targets include suppliers to industrial facilities.

- **Long-term occupancy**—The APT is designed to capture information over an extended period. For example, a large-scale cyber spying operation called GhostNet, discovered in March 2009, was able to infiltrate computer systems in 103 countries, including embassies, foreign ministries, and other government offices, and the Dalai Lama's Tibetan exile centers in India, London, and New York City.[5] According to a report by the Information Warfare Monitor, GhostNet began capturing data on May 22, 2007, and continued at least through March 12, 2009.[6] On average, the amount of time that a host was actively infected by an APT was 145 days, with the longest infection span being 660 days.[7]
- **Control**—In some cases, APTs entail the remote ignition or shutdown of automated software and hardware systems. As more and more physical devices are controlled by embedded microprocessors, the potential for mayhem is high. In fact, Stuxnet went well beyond stealing information. Its purpose was to reprogram industrial control systems—computer programs used to manage industrial environments such as power plants, oil refineries, and gas pipelines. Specifically, its goal was to manipulate the physical equipment attached to specific industrial control systems so the equipment acted in a manner programmed by the attacker, contrary to its intended

5-Harvey, Mike (March 29, 2009). "Chinese hackers 'using ghost network to control embassy computers'". The Times (London). Retrieved March 29, 2009.
6-Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," March 29, 2009
7-Ibid.

purpose. Command-and-control servers may covertly seize control of target systems and even destroy them depending on the APT game plan.



Phase 4: Exfiltration

Once the intruders have seized control of target systems, they may proceed with the theft of intellectual property or other confidential data.

- **Data transmission**—Following command-and-control signals, harvested data may be sent back to the attack team home base either in the clear (by Web mail, for example) or wrapped in encrypted packets or zipped files with password protection. Hydraq used a number of novel techniques for sending the stolen information back to home base. One of these was the use of Port 443 as a primary channel for upload of stolen data. It also established connections that resembled an SSL key exchange dialogue, but did not result in a fully negotiated SSL channel. Lastly, it used private ciphers to encrypt content as it left the victim organizations.
- **Ongoing analysis**—Whereas stolen credit card numbers from a targeted attack are quickly packaged for sale, information captured by APTs is often studied at length for clues to strategic opportunities. Such data may be subject to manual analysis by field experts to extract trade secrets, anticipate competitive moves, and plan counter maneuvers.

What to do?

The hype surrounding APTs masks an underlying reality—these threats are, in fact, a special case within the much broader category of attacks targeted at specific organizations of all kinds. As APTs continue to appear on the threat landscape—and there is no reason to think that they will not—we expect to see the same techniques deployed by other cybercriminals. Moreover, the fact that APTs are often aimed at stealing intellectual property suggests new roles for cybercriminals as information brokers in industrial espionage schemes.

The best way to prepare for an APT is to ensure you are well defended against targeted attacks in general. In fact, while the odds of an APT affecting your organization may be relatively low, the chances that you may be the victim of a targeted attack are, unfortunately, quite high.

Symantec offers rigorous security assessments that can help uncover potential risks from targeted attacks.

Targeted Attack Assessment

- Are you concerned that your key employees and executives might be a target of IP theft?
- Do you wonder if any of your key systems have been compromised by malware?

Malicious Activity Assessment

- Are you concerned about hidden infections?
- What are you currently doing to ensure that your organization is not infected?
- Do you want to better utilize your ongoing monitoring?

Data Loss Risk Assessment

- Are you concerned that sensitive data is exiting your network via corporate and personal email accounts?
- Would you like to know which sensitive files are vulnerable because they are accessible to everyone?
- Do you have a compliance initiative that mandates protecting sensitive payment card or personal data?

Vulnerability Assessment

- Do you know which databases, servers, and network devices are vulnerable to hacker attacks?
- Do you know which unmanaged devices pose a security risk to your critical systems?
- Do you know which vulnerabilities should receive highest priority for remediation efforts?

To find out which type of assessment makes the most sense for you, talk to a Symantec representative. To learn more about APTs from Symantec, visit: http://go.symantec.com/apt

Research methodology

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. More than 240,000 sensors in more than 200 countries and territories monitor attack activity through a combination of Symantec products and services, such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and additional third-party data sources. Symantec gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its security products.[8]

Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks that provide valuable insight into attacker methods. In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 vendors.[9] Symantec also facilitates the BugTraq mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 24,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

8-http://www.symantec.com/business/threatreport/topic.jsp?id=emea
9-Ibid.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com