COMODO
Creating Trust Online®

WHITE PAPER

Endpoint Security and Advanced Persistent Threats

The Invisible Threat

They're out there waiting. Sitting at their computers hoping for you to make a mistake.

And you will. Because no one is immune to their advances. It might be an email from your bank. Or a solicitation from a local charity. Or a message from the college you attended updating you on friends and alumni. Their tricks are unending and eventually you will succumb by clicking on an email, opening an attachment, downloading a file. When you do, they've got you. And the worst part is that you'll probably never know. That's the malicious nature of an Advanced Persistent Threat (APT).

"A key APT strategy is the vulnerability of email systems to phishing where users are tricked into opening seemingly innocuous emails and downloading malware"

The 2013 Verizon Report on Data Breaches makes clear that we all need to be on guard. According to Verizon, "We see victims of espionage campaigns ranging from large multinational corporations all the way down to organizations that have no IT staff at all."

The Report defines APTs as originating from three discrete types of perpetrators. These include: (1) Organized Crime (2) State-Affiliated Agents (3) Political & Social Activists.

Verizon notes that, "More than 95% of all attacks tied to state-affiliated espionage employ phishing as a means of establishing a foothold in their intended victims' systems." The report then concludes that most organizations – from small firms to Fortune 1000 companies and Federal Agencies -- do a less than optimal job of protecting their email systems from phishing.

One reason is that while we tend to focus on the advanced nature of APT attacks, most do not rely on sophisticated solutions such as the Stutznet virus used to cripple Iranian nuclear enrichment facilities. APTs instead use widely understood and available techniques such as Brute Force hacking, Phishing and SQL Injection to obtain access to networks and confidential data. A key APT strategy is to exploit the vulnerability of most email systems to phishing, where users are tricked into opening seemingly innocuous emails and downloading malware.

Spammers also leverage phishing, but cast a wide net. They obtain emails from a variety of sources and send out their spam with little or no thought about the number of recipients. A common technique is to make the message appear to originate from a major bank. The spammers send the

email to every address they have, knowing that some percentage of the people who receive it will be customers of the bank and susceptible to their message.

How APTs Differ From Standard Hacking

Rather than target a mass audience, APTs zero-in on specific individuals in an organization who, if compromised, can be used to advance the goals of the attack. This requires more patience and, as the name implies, more persistence than an undifferentiated email blast.

When sending out an APT, hackers go to great lengths to make the subject line and message appear plausible. They analyze address book information and use any other data they can obtain about either an individual or an organization. For example: if salesperson receives a message inviting them to sign up for a tradeshow that their company is actually participating in, he or she could be easily fooled into clicking on a dangerous link.

"Stealth is the key. By having the breach remain unknown, the hacker can return again and again to exploit the same individual or company."

Equally important, an APT is not a one shot attempt. If the tradeshow ruse doesn't work, the hacker might next identify the college the salesperson attended and use that in a subsequent email. Over time, they will come back again and again to the same person as well as other people in the organization until one of them makes a mistake and clicks on the link.

A "watering hole" is a technique used to infect the target without direct email contact. How it works: the hacker identifies a website they know the individual visits and injects it with malicious code that the victim will then download. This is similar to a "drive by attack" with a third-party website employed as the point of infection. In this way, many small and medium size companies are unwitting participants in the APT because their websites provide a weak link to reach the intended target.

APTs do not look for a home run at the outset. The first objective is to gain access into low priority areas that companies fail to protect adequately: the weakest links. By being patient, the hackers can gradually work their way into higher-value segments of the network where important data resides.

Once a hacker gains access to the desired data, they benefit from the fact that intrusion detection systems focuses primarily on the traffic coming into the network – not the traffic going out. By encrypting, compressing and transferring the stolen data without detection there is no reason for the hacker to close shop.

Stealth is the key. Most hackers want you to know you've been infected and compromised. APTs don't. By having the breach remain unknown, they can return again and again to exploit the same individual and company.

The most high profile example of an APT is the compromise of a White House email system by Chinese hackers in 2012. While the public was assured that nothing important was stolen, many have their doubts. After all, the emails were for the White House Military Office which is responsible not only for the President's schedule but also the codes used to order a nuclear attack.

"Every user that communicates on the network is a potential weak link that needs to be addressed."

We don't know what exactly the Chinese hackers were looking for, but the lesson for all of us is that if the White House can be hacked then we are all vulnerable. You may not think your enterprise is significant target, but every organization has financial and personal data that is attractive to hackers. Payroll records are just one example.

Comodo Endpoint Security Management – Featuring the Industry's Only Antivirus Warranty

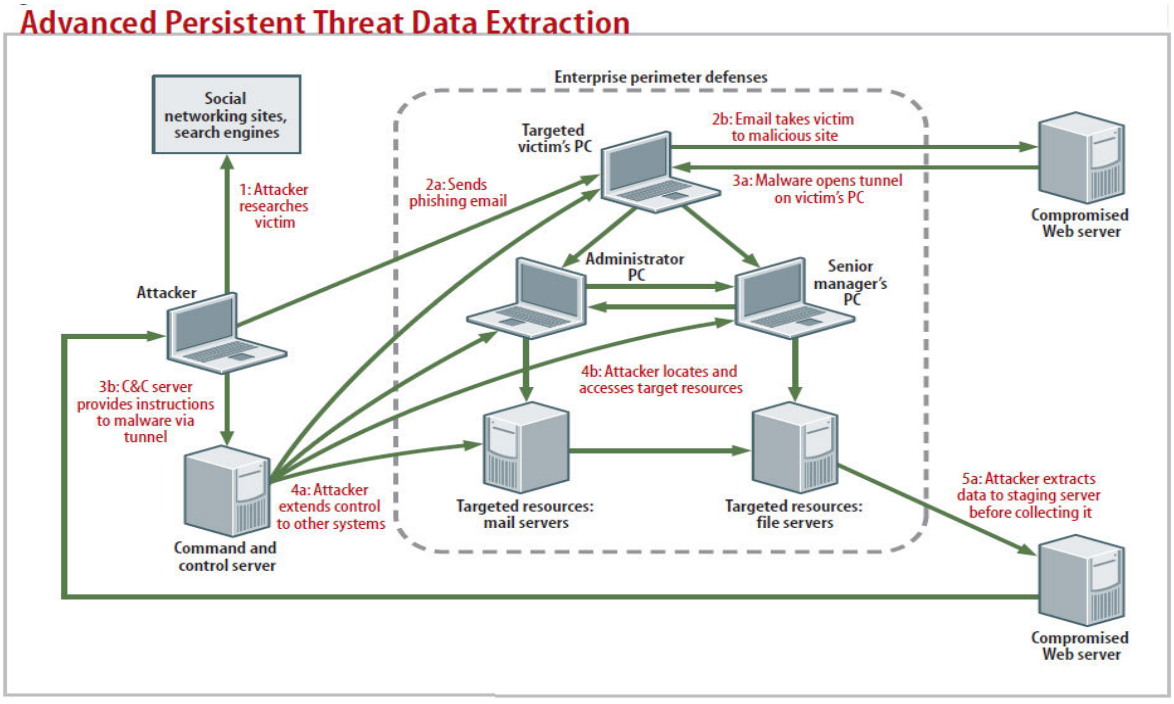
Every device that connects to your network represents a potential entry point for malware. Every user represents a target that can be quickly fooled. Comodo's Endpoint Security Management system makes it easy to ensure that all network devices are configured with the latest security software … enforce strict security policies … and identify problems before they spread.

Key Endpoint Security Management features include:

- Provides the industry's only antivirus warranty
- Features Comodo's patent-pending auto-sandboxing technology to deny access to unknown files
- One centralized management console combines management of LAN and WAN endpoint security and system status
- Unique panoramic view of the endpoint estate with "first-glance" view of 11 critical endpoint metrics
- Automatically uninstalls legacy/existing antivirus products
- Manages Endpoint Security Manager configurations
- Manages CPU, RAM and hard disk usage
- Manages services, processes and applications
- Manages endpoint power consumption
- Manages USB devices

- Set-and-forget policies ensure that endpoint configurations are automatically re-applied if they cease being compliant
- Deploys endpoint policies with pre-configured firewall and application whitelisting rules
- Lowest resource overhead anti-malware suite available on the market
- Allows updating of definition database from the Internet and/or caching proxy

Advanced Persistent Threat Life Cycle	
Phase 1: Reconnaissance	Determine whom to target and how
Phase 2: Spear-phishing attack	Send crafted email and malicious attachment to target victim
Phase 3: Establish presence	Install network back door to allow undetected access, obtain user credentials, install range of attack tools such as packet sniffers, keyboard loggers and scanners
Phase 4: Exploration and pivoting	Perform network exploration and process mapping, extend infection and control to other systems
Phase 5: Data extraction	Encrypt, compress and transfer data out of the network
Phase 6: Maintaining persistence	Analyze data, update and develop attack tools, infect additional machines Return to phase 4 and repeat.



APT Terminology	
Backdoor	Malware that allows remote administration of an infected system.
Compromised/Rogue digital certificate	A digital certificate whose private key and certificate file have been illegitimately accessed and copied
Cyber-something	Internet-related version of an existing activity or thing.
Drive-by download	Method of compromising computers by tricking the victim into unintentionally or unwittingly downloading malware when visiting a website, viewing an email message or clicking on a pop-up window.
Exploit code	Code used to enter a target system by taking advantage of one of its vulnerabilities.
Payload	Once exploit code accesses a target system, the payload is executed (usually to install a backdoor).
Sandbox	A mechanism for executing untrusted code within a tightly controlled set of resources.
Trojan	Malware hidden in a program or file that appears useful, interesting or harmless.
Vulnerability	Typically a flaw in operating system or application software, but a vulnerability can also be a lack of protection, a poor security practice or an incorrect system configuration.
Weaponized document	Document or file containing malicious code.
Zero-day exploit	Exploits that take advantage of vulnerabilities for which there are no patches available from the software vendor.

ABOUT COMODO

Comodo is a leading provider of trust-based, Internet security products for organizations of every size. Comodo's offerings range from SSL certificates and antivirus software to endpoint security, mobile device management and PCI compliance. Clients utilizing Comodo security products include Morgan Stanley, Comcast, Sears, Time Warner, and Merck among others. Comodo is headquartered in Clifton, New Jersey with additional offices in the UK, China, India, Ukraine, and Romania. To learn more, visit www.comodo.com