A Special TrendLabs Primer on APTs

DETECTING THE ENEMY INSIDE THE NETWORK

How Tough Is It to Deal with APTs?

Human weaknesses include the susceptibility of employees to social engineering ploys—anything from letting in a disguised utility man to opening an email attachment.

What are APTs or targeted attacks?

Advanced persistent threats (APTs) refer to a category of threats that pertain to computer intrusions by threat actors that aggressively pursue and compromise chosen targets. APTs are often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target's network—and are thus not isolated incidents. In addition, while malware are typically used as attack tools, the real threat is the involvement of human operators who will adapt, adjust, and improve their methods based on the victim's defenses.

Enterprises consider targeted attacks a high-priority threat because of the considerable impact past victims sustained. However, the risk of suffering from an attack of this kind remains because human[1] and system weaknesses[2] that allow entry into networks can never be fully resolved.

The very act of doing business these days and interacting with new technologies, platforms, and entities can only further broaden the attack surface. Threat actors have also realized the true value of company data, as can be seen in the notable data breach attacks in 2011. More targeted attacks and cyber espionage will therefore occur in the future.

A better understanding of targeted attacks can give enterprise security groups the correct mindset in dealing with these threats.

How do targeted attacks occur?

Intelligence gathering: Highly similar to a military reconnaissance mission, this initial phase aims to gain strategic information not only on the intended target's IT environment but also on its organizational structure. The information gathered can range from the business applications and software an enterprise utilizes to the roles and relationships that exist within it.

SOME TECHNIQUES SEEN

- **Social engineering*:** Exploits the human element.
    - Email appearing to have come from a target's social network
    - Email coming from a real email account the target knows and trusts (compromised accounts)

*The above are just a few examples of social engineering techniques. Attacks can also utilize recent events, work-related issues or concerns, and other areas of interest for the intended target.

- **"res://" protocol:** Profiles the target's software environment.
    - Able to identify file-sharing programs, web browsers, email clients, download managers, and remote administration tools, among others

Point of entry: As attacks usually target organizations, the delivery mechanism is therefore the most common form of office communication—email. Note, however, that instant-messaging and social networking platforms can also be utilized to entice targets to click a link or download malware. Eventually, establishing a connection with the target is acquired.

System weaknesses include software vulnerabilities or design flaws that can be exploited to gain entry into an enterprise's IT environment.

SOME TECHNIQUES SEEN

- Usage of personal webmail accounts or employing spoofed email addresses of institutions such as the government
    - Email that comes with a PDF, a *Microsoft Word* document, a *Microsoft Excel* spreadsheet, or a *Microsoft PowerPoint* presentation as attachment
- Right-to-left-override (RTLO) Unicode hole
    - Executable files supposed to end in *.exe* are made to appear as simple document files or folder icons
- "Drive-by" exploits
    - Email with links to web pages that exploit vulnerabilities in web browsers or browser plug-ins

[1] http://ctoinsights.trendmicro.com/2011/06/the-human-factor-of-targetted-attacks/
[2] http://ctoinsights.trendmicro.com/2010/11/zero-day-vulnerabilities-risk-overblown/

Real-World Damage to Companies That Suffered from APTs

- Data theft
- Brand damage
- Physical damage

Compromise: Armed with knowledge obtained from the intelligence gathering stage and supplementary insights accumulated from prior attacks to a company's environment, threat actors are able to select and specify the exploits to use on their target. At the end of this stage, a company's network is infiltrated.

SOME TECHNIQUES SEEN

- Exploits
  - Flaws in commonly used business applications such as *Adobe Reader* and *Flash Player* and *Microsoft Office*
  - Zero-day exploits or exploit codes for currently unpatched vulnerabilities
  - Webmail vulnerabilities that affect commonly used webmail services that are accessed from the workplace
  - Exploits for MHTML protocol vulnerabilities wherein the basic act of previewing a message[3] can compromise an account

Command-and-control (C&C) communication: After an organization's perimeter has been breached, continuous communication between the compromised host and the C&C server needs to be preserved. Threat actors use techniques to maintain C&C communication traffic under the radar often either by blending in with legitimate traffic or fully utilizing go-betweens.

SOME TECHNIQUES SEEN

- Cloud-based C&C
  - Threat actors may use webmail as part of their C&C communication. These communications are usually protected by Secure Sockets Layer (SSL) encryption, making it difficult to identify if the traffic directed to sites is malicious.
  - Legitimate sites can also be compromised and turned into C&C servers. This misleads investigators into thinking that though malicious traffic has been detected, deeper investigation will, unfortunately, lead them to a legitimate website.

Lateral movement: Once assured that there is constant access to the breached network, threat actors then laterally move throughout the company's network, seeking valuable hosts that house sensitive information.

SOME TECHNIQUES SEEN

- **"Pass the hash":** Allows escalation of an attacker's privileges to that of an administrator.
- **"Brute-force" attacks:** Allows an attacker's access to database servers, *Microsoft Exchange* email servers, or VPN credentials. The information obtained from these assets reassures subsequent access even if the attacker's tool is uncovered.

Asset/Data discovery: Noteworthy assets are identified within the infrastructure then isolated for future data exfiltration.

SOME TECHNIQUES SEEN

- File lists in different directories are sent back so attackers can identify what are valuable.
- Email servers are identified so attackers can read important email in order to discover valuable information.

Data exfiltration: The attack's ultimate objective is to transmit information from within the target organization's perimeter to a location the threat actor controls. Data transmission can be done either quickly or gradually wherein information is moved to a staging phase then prepared for exfiltration.

SOME TECHNIQUES SEEN

- **Built-in file transfer:** Option offered by some tools such as remote access Trojans (RATs).
- Via FTP or HTTP
- **Via the *Tor* anonymity network:** Able to mask one's location and traffic, providing an attacker a more confidential route.

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

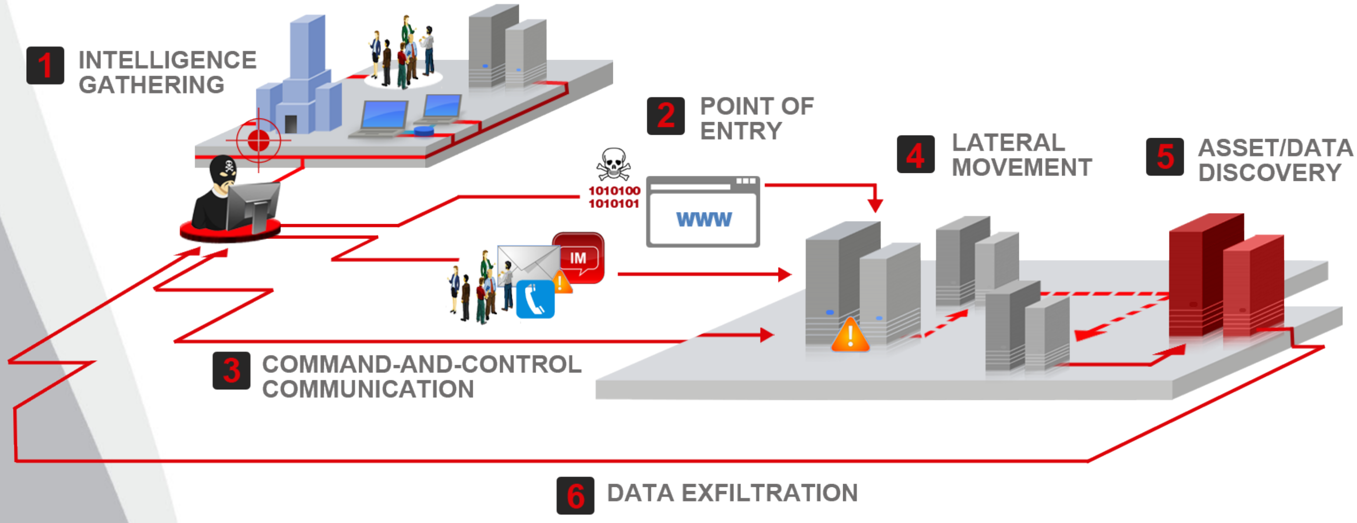


Figure 1. Targeted attack diagram

What Can Enterprises Do Against APTs?

By design, APTs are able to evade standard perimeter and endpoint defenses. Industry analysts and experts have made a clear case that an expanded and layered definition of security due diligence is now a must for most enterprises and government organizations. Trend Micro provides a range of solutions that allow organizations to meet these new requirements, combating APTs with the best protection and proactive detection technologies.

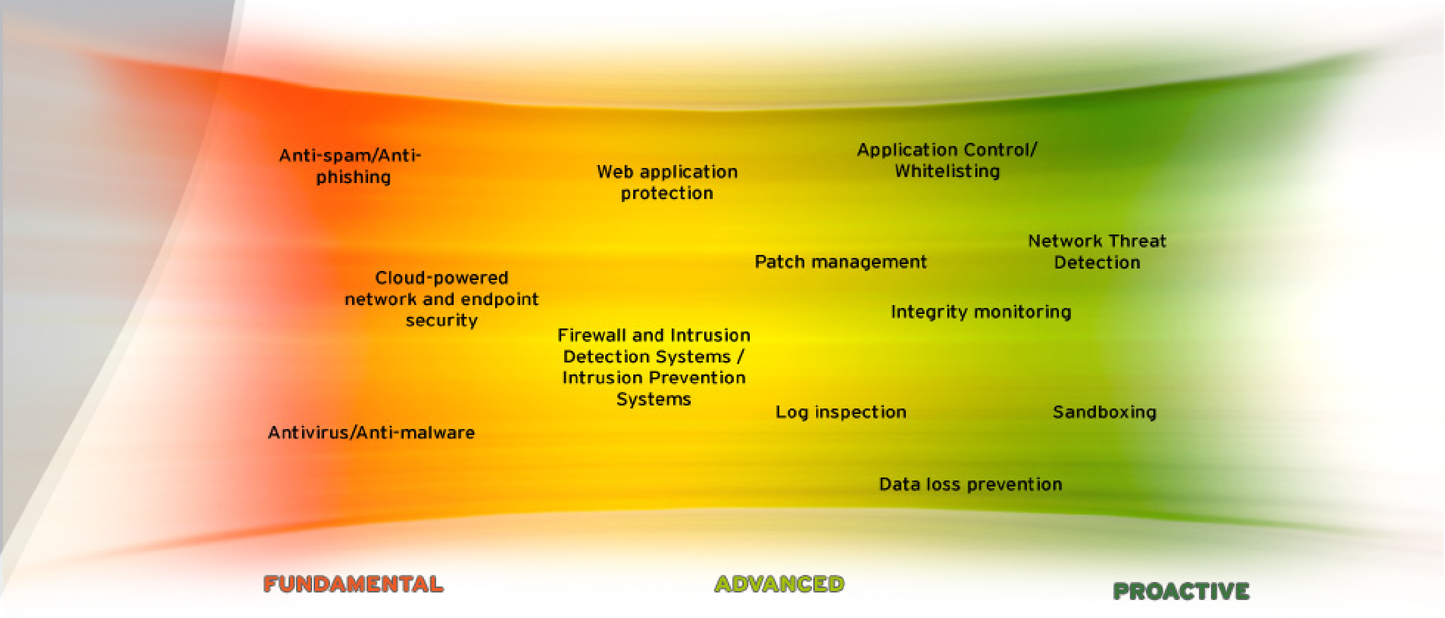


Figure 2. Security risk management diagram

Fundamental Defense

Standard perimeter and endpoint security technologies are essential to prevent most attacks and, at their best, may detect or block certain aspects of an APT or a targeted attack. The key factors behind the effectiveness of these products is the provider's ability to source new threat information and the "time to protect"—how quickly new threat information is made available to the products deployed.

The Trend Micro™ Smart Protection Network™, for instance, provides Trend Micro products with the broadest and most up-to-date threat detection capabilities.[4] The Smart Protection Network processes over 4TB of data daily, including daily analyses of over 8 billion URLs, 50 million email samples, 430,000 file samples, and 200,000 IP addresses.

- *InterScan Messaging Security* combines the privacy and control of a powerful on-premise gateway software virtual appliance with the proactive protection of an optional cloud-based prefilter that stops the majority of threats and spam in the cloud.

- *InterScan Web Security* combines award-winning malware scanning with real-time web reputation, flexible URL filtering, and integrated caching for streamlined administration and lower total cost of ownership (TCO).

- *OfficeScan* maximizes security and performance on physical and virtual desktops, providing the industry's strongest threat and data protection, built into a single endpoint agent, and deployed and managed together from a single console.

Advanced Protection

Moving beyond fundamental defense is about providing additional security safeguards for sensitive resources and data, whether physical or virtual and whether these reside in the corporate network, the datacenter, or the cloud. Trend Micro can provide a hardened level of protection for the servers and data that are targets of an attack.

- *Deep Security* provides a single platform for server security to protect physical, virtual, and cloud servers as well as virtual desktops. Tightly integrated modules easily expand to offer in-depth defenses, including anti-malware, integrity monitoring, intrusion detection and prevention, web application control, firewall, and log inspection.

- *SecureCloud* is designed to encrypt and protect data in public, private, and hybrid clouds while also securing data stored in physical and virtual servers. Easy-to-use, policy-based key management authenticates the identity and integrity of servers requesting encryption keys and controls when and where your secure data can be accessed.

Real-Time Threat Management

Moving beyond protection to embrace proactive detection capability is the ultimate step in combating APTs and targeted attacks. Specialized threat detection technology can detect "invisible" malware and human attacker activity by examining the content, communications, and behavior of all network traffic then providing actionable insights to aid in immediate containment and remediation.

Vulnerability exploits are a key tool of attackers and a proactive stance to vulnerability detection and timely patching is critical. A systematic approach to vulnerability management and a proactive virtual patching or vulnerability shielding strategy will minimize the window of opportunity for attackers.

"Most of the targeted attacks that work are indeed persistent yet still build upon the usual weak link—the social engineering ploy where a human gets duped."

– Paul Ferguson,
Trend Micro senior
threat researcher

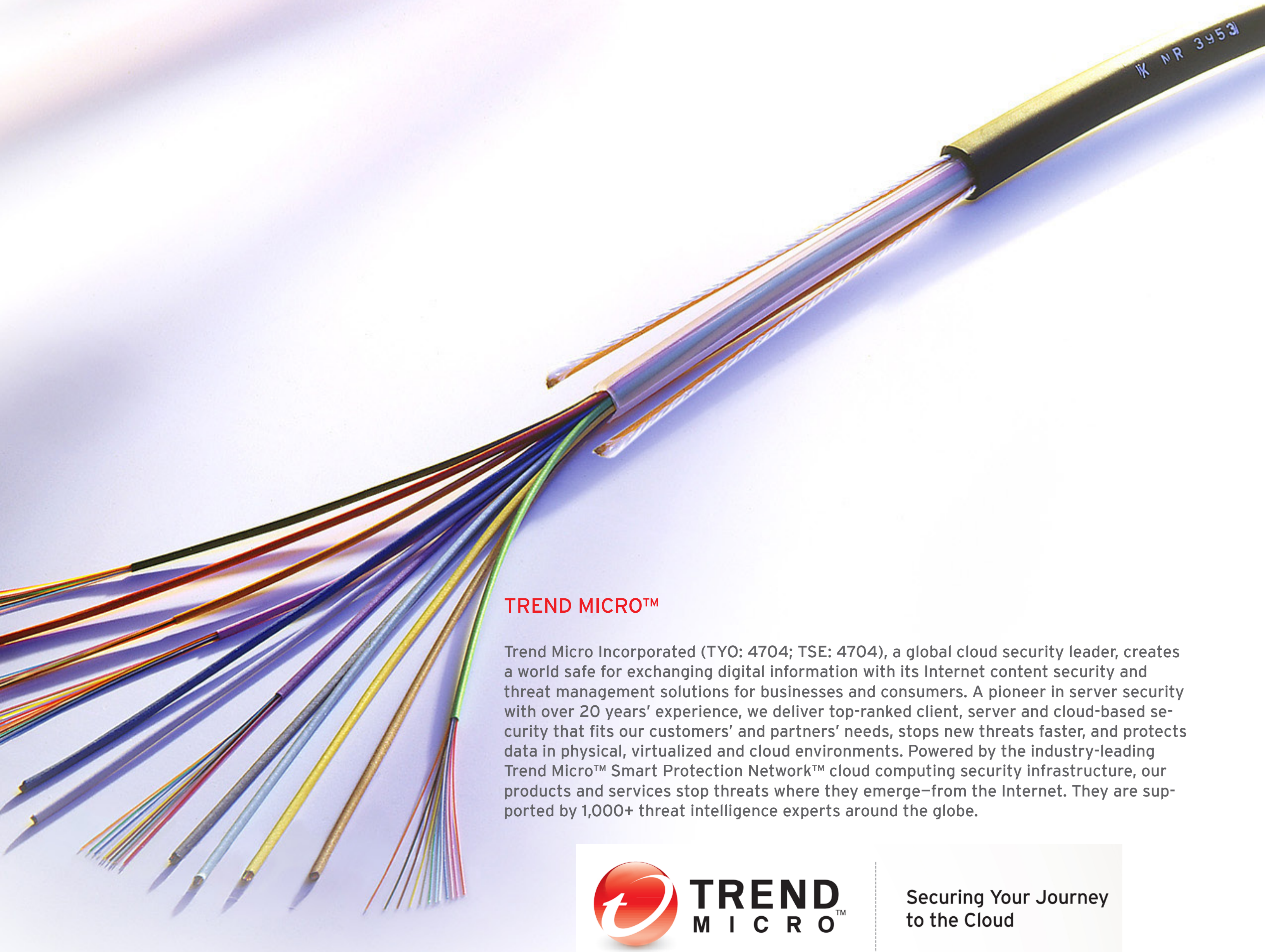
[4] http://www.trendmicro.com/us/technology-innovation/our-technology/smart-protection-network/index.html

These Trend Micro solutions enable you to take the ultimate proactive stance against APTs and targeted attacks:

- *Deep Discovery* provides customers with the networkwide visibility, insight, and control needed to reduce the risk of APTs and targeted attacks. *Deep Discovery* uniquely detects and identifies evasive threats in real time and provides the in-depth analysis and actionable intelligence needed to prevent, discover, and contain attacks against corporate data.

- *Vulnerability Management Services* provides on-demand network discovery, asset prioritization, application and system vulnerability assessment, and remediation tracking in a single software-as-a-service (SaaS) offering.

- *Deep Security* deep packet inspection and intrusion prevention system (IPS) capabilities close the window on vulnerabilities and reduce patching costs by providing virtual patching to rapidly shield vulnerabilities without the need to wait for vendor patches or disrupt your standard patch cycles.



TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO™

Securing Your Journey
to the Cloud

TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

TrendLabs
Global Technical Support & R&D Center of TREND MICRO