Advanced Persistent Threats

September 30, 2010

By: Ali Golshan (ali.golshan@us.pwc.com)

PRICEWATERHOUSECOOPERS

Agenda

Section 1

Current Threat Landscape

- Context
- Common Targets for APTs
- Recent Attacks
- Shift in Purpose
- Repercussions

Context

Conventional Cyber Attacks

- Conventional cyber attacks use **known** vulnerabilities to exploit the **un-specific** targets
- Examples include malware (viruses, worms and Trojans), and traditional hacking and cracking methods

Advanced Persistent Threats (APTs)

- There is a new breed of attacks that is being referred to as Advanced Persistent Threats
- APTs are targeted cyber based attacks using **unknown** vulnerabilities, customized to extract a **specific** set of data from a **specific** organization
- APTs have the following characteristics that make them particularly dangerous:
  - **Persistent**: The persistent nature makes them difficult to be extracted
  - **Updatable**: The attacker can update the malware to be able to continuously evade security solutions even as they are upgraded

APTs target specific organizations to obtain specific information

Since these are specialized attacks, they are **customized for their targets**, and are designed to **extract very specific information** based on the target. Most common targets are:

Government agencies

- Government agencies are targeted by Foreign Intelligence Services (FIS)
- APTs can be used for theft of military level secrets and in cyber warfare for destabilization along with conventional warfare
- 2007 McAfee report stated approximately 120 countries are trying to create weaponized internet capabilities
- Example: The Russia-Georgia war of 2008 was the first example of a APT coinciding with conventional warfare. The targets were Georgian government sites, as well as sites of U.S. and British embassies

Financial industry

- The financial industry is targeted by transnational criminal enterprises
- Example: Targeted attacks in December 2009 on Citibank infrastructure initiated by Russian organized crime

Organizations with IP

- Organizations with IP are targeted by FIS & competitors to access confidential intellectual property
- Using APTs organizations can bypass spending years on R&D and billions of dollars by getting access to a competitor's R&D data
- Example: The aurora attacks in late 2009, early 2010 targeted 30+ US organizations and extracted valuable IP relevant to the organization

Availability of launching infrastructure makes APTs more common

- **GhostNet**
  - This was one of the first APTs
  - Infiltrations discovered in embassies belonging to India, South Korea, Portugal, Germany, and over 10 others
  - Due to the infiltrations of GhostNet, USA Government initiated its first serious Cyber Warfare defense program
- **Aurora incidents**
  - Infiltrated over 30 companies, including Google, and Adobe
  - Exposure of confidential IP
- **Conficker A-E**
  - Infiltrated French Navy, UK Military, Germany Army, and more
  - Carried anti-virtualization and anti-debugging armoring, self-defense code, and persistent in design
  - Now variants are commercialized to target specific sectors
  - Government systems experienced significant downtime to cleanse and recover systems

Attacks with Purpose

Cyber attacks have been prevalent since the birth of the internet. However, with APTs, there is a clear shift in the purpose, the mode of operation and the people behind these attacks.

- **Purpose**
  - Attacks are planned by teams of attackers with specific skills (ex. the Zeus Trojan creators)
  - Attacks are tailored towards a particular technology, or company to maximize advantage & financial returns
- **Financing**
  - Cyber crime is well funded, and backed by individuals as it is much lower risk than conventional crime
  - It is the 2nd largest economy on the net
  - High prices are paid for zero-day vulnerabilities
  - The Ponemon institute reported the average cost of an attack grew from $169,000 in 2004 to $350,000 due to advanced attacks
- **Organized**
  - Organizations actively recruit and train skilled individuals to conduct cyber attacks

Insider Threats

- Insider threats are the 2nd highest danger to organizations, targeted Malware being 1st (IT Business Edge)
- Due to the economic downturn, desperate, disgruntled, or financially pressured employees have resorted to exploiting company information from within and criminal organizations are much more active in recruiting employees to increase their chances of an attack
- Employees are able to purchase Trojan kits such as Zeus and install for theft of financial data
- In 2009, a telecom employee stole customer records and sold them to a data broker who in turn sold the data to competitors. It included millions of records that contained information such as account expiration date so competitors could target those customers at the time they may look for a new provider.
- After a series of disputes with executives and investors, the former YouSendIt co-founder and CEO left the company and later launched a denial-of-service attack against YouSendIt systems
- A former engineer at Fannie May planted a logic bomb that (had it not been discovered) would have shut down the company for at least a week by decimating all of their 4,000 servers

Lasting repercussions can result from APTs

- Governments can lose their position of power if national security information is compromised
- Damage to reputation can lead to loss of customers or partners
- Loss of shareholder value can be caused by panic or data loss
- Organizations can lose competitive advantage due to loss of IP
- Fines & Penalties may be imposed by partners or agencies
  - In case of Heartland, costs of attack have reached $139 million, with over $40 million in settlements
- Theft of sensitive data without the knowledge of the organization can create critical infrastructural weaknesses such as compromised energy grids. Several high profile examples exist.

Section 2

The Disconnect

- Current traditional solutions
- Heuristics and behavior analyzers
- How modern malware operates
- The ‘gap’

Traditional security solutions

Anti Virus

- Reactive solution
- Matches signatures and patterns
- Requires update to signature database
- Captures only known malware

Firewalls

- Relevant when attacks target specific network vulnerabilities
- Malware tunnels through standard HTTP to bypass other required active services
- Next-gen firewalls perform deep packet analysis, however they still require knowledge of vulnerabilities

Web Gateways

- Lists “known-bad” URLs
- In case of Conficker, random, newly generated sites were created for distribution of malicious payload

IDS and IPS

- Monitor network traffic to understand data transmission
- Shift from IDS to IPS, based on attack patterns in traffic streams
- Require knowledge and forms of exploits against discovered vulnerabilities
- Very limited protection against zero-day vulnerabilities

Heuristics and behavior analyzers are a step in the right direction

Essentially “statistical guesses”, based on correlations of various statistics, they try to detect malware based on a certain set of behaviors. However, they are not entirely effective in fighting against APTs because:

- Modern malware shares a large set of behaviors with everyday business applications, and heuristics analyzer create large volumes of false-positives if their rules are too aggressively set
- If rules and heuristics are set too aggressively they will cause excessive false positives
- If not customized and fine-tuned, heuristic and behavior analyzers will allow targeted attacks to pass right through

Modern malware is fundamentally different

The way modern malware operates is fundamentally different from the traditional cyber attacks. The following characteristics of APTs make traditional cyber security solutions ineffective in fighting them:

- Designed and built by highly-skilled developer teams
- Attackers understand target systems, and use zero-day vulnerabilities within payloads
- Gains access without creating “noise”
- Maintains access over a period of time and displays as “normal” traffic
- Communicates with outside resources to download further instructions and payloads
- Dynamically adapts to new security measures that might have been put in place

The ‘Gap’ for conventional solutions

Based on the characteristics of modern malware, here is what is missing from conventional solutions, and needs to be addressed in modern malware solutions:

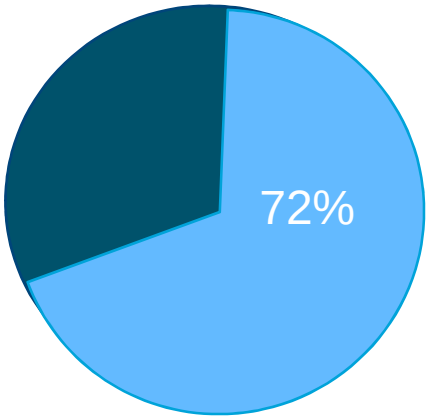
- A solution to provide security across all threat vectors
- A dynamic solution to guard against dynamic attacks
- Protecting against zero-day vulnerabilities across all layers
  - Network layer
  - Application
  - Operating systems
- Accurate against targeted attacks
  - Aggressive heuristics to ensure capture of all suspicious data
  - Low false-positives rate

Section 3

The Risk

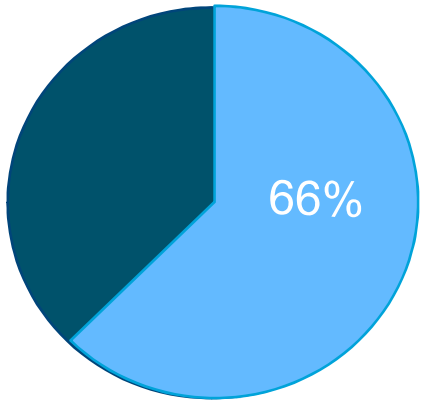
- Statistics
- Factors contributing to the rise in APTs
- What makes APTs even more dangerous?
- Financial Impact
- Other impact

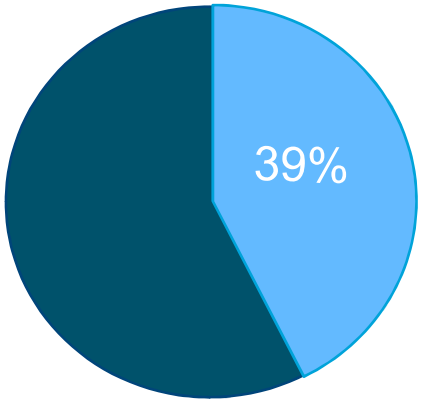
Statistics



72% of corporate networks with 100+ users are compromised

66% of new Trojans are built for theft of banking information





Purchase of zero-day vulnerabilities has grown 39% from 2009 to 2010

Factors contributing to rise in APTs

Financial

- More financial rewards to become black hats in developing countries
- Entrepreneurs have angels, black hats now have devils
- Low risk & high rewards have resulted in a fertile attack landscape, with massive R&D resources
- Zero-day vulnerabilities can be sold on the “black-market” for targeted attacks

New breed of attackers

- Attackers with specialized skills are available for hire
  - Highly educated
  - In depth understanding of networks, applications, OS, and at times, internal knowledge

Attacker’s Advantage

- Attackers have the luxury of being flexible and adjusting to security movements
- Attackers build their exploits to take advantage of our weaknesses
- They only need to succeed once, we need to succeed every time
- They only need to find 1 vulnerability, we need to protect against every known & unknown vulnerability
- Most security professionals overwhelmed with containing damages, rather than building preventative security solutions

Other

- Lack of international cyber laws, and very difficult to prove

What makes APTs even more dangerous?

- Advanced attacks are only starting to mature and most current attacks are ‘proof of concept’
- They are a new methodology, not a new type of attack
- Attackers are willing to change constantly to exploit security solutions
- There is much better information sharing amongst cyber criminals than security companies
- More resources are being provided to cyber criminals and the skills and technology for attacks are already available, ready for someone to pull the trigger
- The security industry is slow to move towards new solutions, considering the investment in the current solutions infrastructure
- Cyber crime is currently costing roughly $250 billion globally per year and the average cost of a sophisticated attack has increased from roughly $4.5 million to $6.6 million per incident year over year
- In 2009, the pentagon spent over $100 million in 6 months responding to and recovering from cyber attacks and forced the defense department to take 1,500 machines off-line

Section 4

What Now?

- An intervention for the security industry
- Paradigm shift

An intervention for the security industry

The current security architecture cannot take us forward for the next 3 to 5 years. A major change needs to be brought about in the way we approach cyber security. To begin with, we will need to change the way we think about cyber security. Specifically:

- Acknowledging the need for truly new and unique technology
- Accepting that “reducing the damage” is not the answer
- Moving away from the ‘detect first, respond later’ approach
- Transitioning from a reactive approach to a proactive approach
- Dynamically discover new vulnerabilities
- Use the R&D going into attacks for a good cause

Paradigm shift

Once we have accepted the need for a new way to approach cyber security, we will have to adopt a few core guiding principles to bring about that change.

Collaborate

- Building new adaptive technology, using combination of practices from various fields of science and mathematics
- Developing better information sharing platforms
- Increased international cooperation is required on all fronts

Anticipate

- Designing solutions based on anticipated shifts in technology over the next 3 to 5 years
- Driving innovative shift in security technology through cutting edge R&D
- Viewing enterprise security spending as a long-term investment

Adapt

- Attackers won't wait for the security industry to catch up
- Need to develop more adaptive security solutions, hardening networks based on types of attacks launched against them
- Rather than gradual improvements to solutions and renaming heuristics to behavior, there is need for new design and architecture in security solutions
- Need to address security concerns first for technologies such as cloud, and virtualization to become fully adopted

Appendix 1–
Case Study

The “Operation Aurora” incident

- Aurora utilized:
  - Social engineering
  - Zero-day vulnerabilities
  - Gaps created by conventional security
- Aurora targeted:
  - Theft of email archives
  - Confidential data
  - A well-defined list of enterprises

The “Operation Aurora” incident

- How Aurora operated:
  - Attacks began in 2009 using a zero-day IE 6.0 vulnerability
  - Lured users to click a link, directing them to a malicious Web site
  - Once the system was compromised, a Trojan was installed
  - Once installed, the Trojan would communicate with the command & control for a variety of commands
  - New payloads would allow for further compromise of the companies systems

The “Operation Aurora” incident

- How Aurora operated:

FW & IPS Failed →

- Attacks began in 2009 using a zero-day IE 6.0 vulnerability
- Lured users to click a link, directing them to a malicious Web site
- Once system was compromised, a Trojan was installed
- Once installed, the Trojan would communicate with the command & control for variety of commands
- New payloads would allow for further compromise of the companies systems

The “Operation Aurora” incident

- How Aurora operated:

FW & IPS Failed →

- Attacks began in 2009 using a zero-day IE 6.0 vulnerability

Web Gateway Failed →

- Lured users to click a link, directing them to a malicious Web site
- Once system was compromised, a Trojan was installed
- Once installed, the Trojan would communicate with the command & control for variety of commands
- New payloads would allow for further compromise of the companies systems

The “Operation Aurora” incident

- How Aurora operated:

FW & IPS Failed →
- Attacks began in 2009 using a zero-day IE 6.0 vulnerability

Web Gateway Failed →
- Lured users to click a link, directing them to a malicious Web site

Antivirus Failed →
- Once system was compromised, a Trojan was installed
- Once installed, the Trojan would communicate with the command & control for variety of commands
- New payloads would allow for further compromise of the companies systems

The “Operation Aurora” incident

- How Aurora operated:

FW & IPS Failed →
- Attacks began in 2009 using a zero-day IE 6.0 vulnerability

Web Gateway Failed →
- Lured users to click a link, directing them to a malicious Web site

Antivirus Failed →
- Once system was compromised, a Trojan was installed

FW & IDS Failed →
- Once installed, the Trojan would communicate with the command & control for variety of commands
- New payloads would allow for further compromise of the companies systems

The “Operation Aurora” incident

- How Aurora operated:

FW & IPS Failed →
- Attacks began in 2009 using a zero-day IE 6.0 vulnerability

Web Gateway Failed →
- Lured users to click a link, directing them to a malicious Web site

Antivirus Failed →
- Once system was compromised, a Trojan was installed

FW & IDS Failed →
- Once installed, the Trojan would communicate with the command & control for variety of commands

Antivirus Failed →
- New payloads would allow for further compromise of the companies systems

PRICEWATERHOUSECOOPERS