Cyber kill usage for Advanced Persistent Threat (APT)

Industry-wide, cyber security defenders are struggling to keep pace with increasingly advanced (and well-funded) criminal campaigns. These campaigns have substantial, bottom-line impacts and require rapid response with advanced counter-measures. These criminal campaigns are called Advanced Persistent Threats and can be summarized as:

- **Advanced** – Sophisticated attackers behind the threat utilize the full spectrum of computer intrusion technologies and techniques customized to match their target.
- **Persistent** – These advanced operators are patiently focused on their target, rather than opportunistically seeking immediate financial gain. The attack is conducted through continuous monitoring and establishing prolonged footholds in order to achieve their objectives.
- **Threat** – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The advanced and persistent operators have a specific objective and are skilled, organized and well-funded.

Many organizations have sound fundamental cyber security capabilities. However, advanced persistent threat (APT) tactics require more agile and advanced defenses. Organizations must continue the fundamentals while adding more advanced and complimentary capabilities. New technologies and methodologies are needed to detect, prevent and respond to threats in near real-time.

APT: Common Tactics

All attacks follow the same set of fundamental steps:

1. Infiltrate the Network
2. Establish a Foothold
3. Elevate Privilege
4. Internal Reconnaissance
5. Move Laterally
6. Maintain Persistence
7. Exfiltration Data

These seven steps can be accomplished in many ways, but progress methodically in order to circumvent layered security controls. These steps can be seen in recent, high-profile breaches.

Step 1: Infiltrate the Network

Criminals will infiltrate a network by various means, e.g.:

1. Use stolen credentials to remotely logon
2. Exploit a vulnerable computer
3. Phish for a user's credentials
4. Install malware on a system
5. Social engineer a user to provide access
6. Many other ways

In the Major US based retail store breach, the attackers compromised a vulnerable computer used by a third party HVAC vendor.

These threats and vulnerabilities can be protected through layered defenses, such as (but not limited to):

1. Secure password policies

2. Patching known vulnerabilities
3. End user awareness and education
4. Web content filtering
5. Vendor security reviews

Step 2: Establish a Foothold

Criminals will establish a foothold to ensure that they can log in again and again. To accomplish this they will:

1. Download remote access tools
2. Create network backdoors and tunnels allowing stealth access that goes undetected

These threats and vulnerabilities can be protected through layered defenses, such as (but not limited to):

1. Privileged account management
2. Removal of local admin rights
3. Application whitelisting
4. Network firewalls
5. Intrusion Detection/Prevention Systems

In the Major US based Entertainment company breach attackers used tools created from code used in previous attacks. This code reuse allowed the attack to be attributed to North Korea.

Step 3: Elevate Privilege

Criminals then attempt to gain access to other compromised systems by granting their account Admin level access. To do this they use:

1. System vulnerabilities
2. Improperly configured accounts or settings
3. Exploit tools

One of the US based Home appliance store stated "The hackers… acquired elevated rights that allowed them to navigate portions of Home Depot's network."

These threats and vulnerabilities can be protected through layered defenses, such as (but not limited to):

1. Patching known vulnerabilities
2. Removal of local admin rights
3. Application whitelisting
4. Configuration scanning
5. Intrusion Detection/Prevention Systems

Step 4: Internal Reconnaissance

The attackers have access and a privileged account, now they will explore the network and collect information on:

1. How the network works
2. What security devices are present
3. What other users accounts are of value
4. Where else on the network they can go

Retail store breach involved searching the network for POS terminals and their configurations. This allowed customized tools to be developed by the hacker.

These threats and vulnerabilities can be protected through layered defenses,

1. Secure configuration standards
2. Privileged account management
3. Log file analysis

4. Intrusion Detection/Prevention Systems

Step 5: Move Laterally

Once an environment has been investigated, criminals then move to compromise systems discovered in the internal Reconnaissance step repeating steps 2 and 3 on each new system.

These threats and vulnerabilities can be protected through layered defenses, such as (but not limited to):

1. Network segmentation
2. Log file analysis
3. Intrusion Detection/Prevention Systems

In Home appliance store the attackers utilized lateral movement from internal systems to the POS terminals to install the RAM scraping malware to steal account information.

Step 6: Maintain Presence

After each compromised system criminals work to ensure the systems they've compromised remain under their control. After all they wouldn't want all their hard work to be lost.

These threats and vulnerabilities can be protected through layered defenses, such as

1. Patching known vulnerabilities
2. Removal of local admin rights
3. Application whitelisting
4. Configuration scanning
5. Intrusion Detection/Prevention Systems

The attackers maintained their presence in the retail store breach by compromising an internal server used to aggregate account Information from the POS systems.

Step 7: Data Exfiltration

Once the criminals locate data they are interested in they will copy that data out of the network through various means, such as:

1. Email
2. File transfers
3. USB storage

These threats and vulnerabilities can be protected through layered defenses, such as

4. Data Loss Prevention (DLP) controls
5. Firewalls
6. Port control (USB, SD, etc.)
7. Email filters
8. Web content filtering

For a Major US Bank, An employee stole customer information on 350,000 clients, including partial account numbers. This information was caught by DLP filters.

Solution

Earlier Detection of Advanced Threats

- Detect APT tactics by analyzing multiple stages of the attack lifecycle
- Inspect content before it reaches systems (email attachments, web links, etc.)
- Use threat intelligence to help identify indicators of compromise (security community)
- Extend detection beyond and within the network perimeter

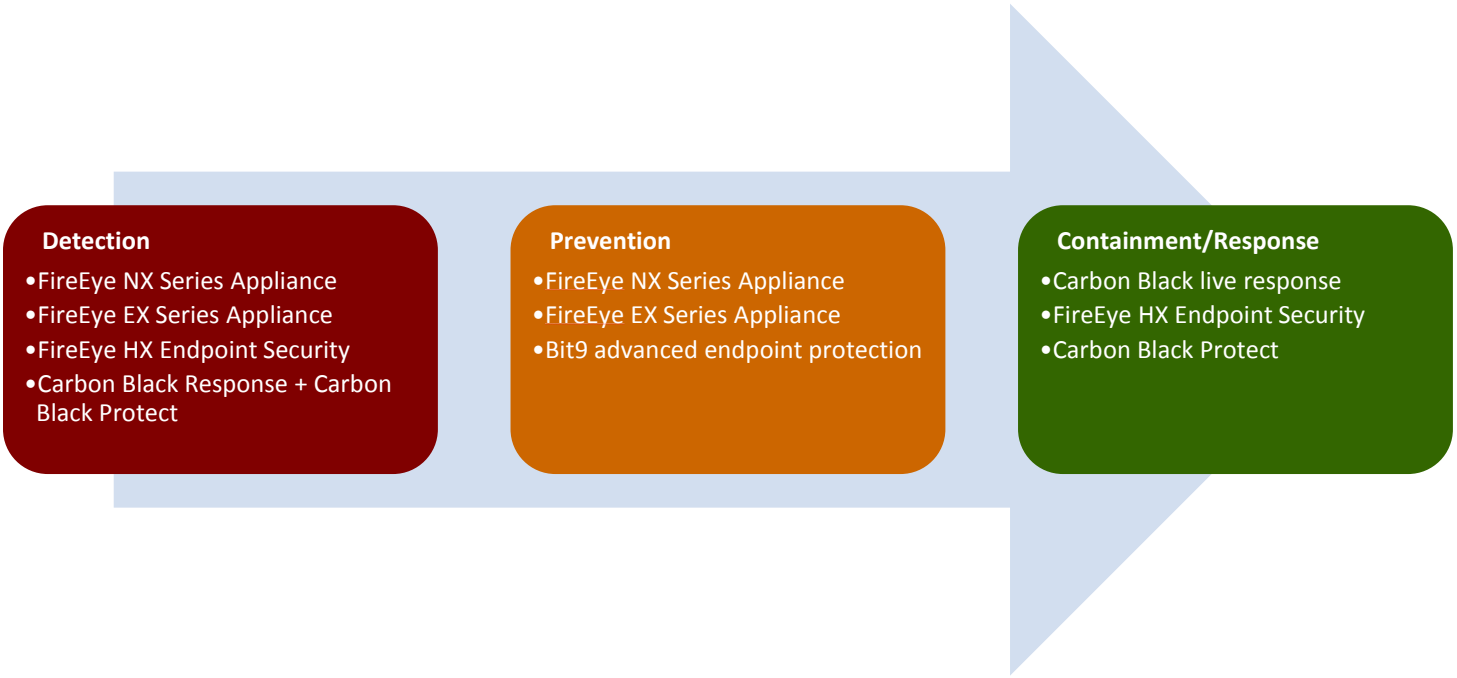
Prevention of continued compromise and callback

- Block malicious files from running
- Block malicious web links
- Prevent communication to known ‘bad actors’
- Stop attacks from spreading across our systems and networks (Quarantine)

Advanced containment and live response

- Respond to and triage of compromised endpoints
- Advanced forensic analysis of ‘realized’ security incidents
- Rapid impact evaluation, to promptly develop appropriate countermeasures

Solution Component



Cyber Attack and Advance Control

FireEye NX and EX watch for attempts to infiltrate the network through behavioral analysis in secure virtual machines

FireEye HX alerts on attempts to compromise workstations and servers

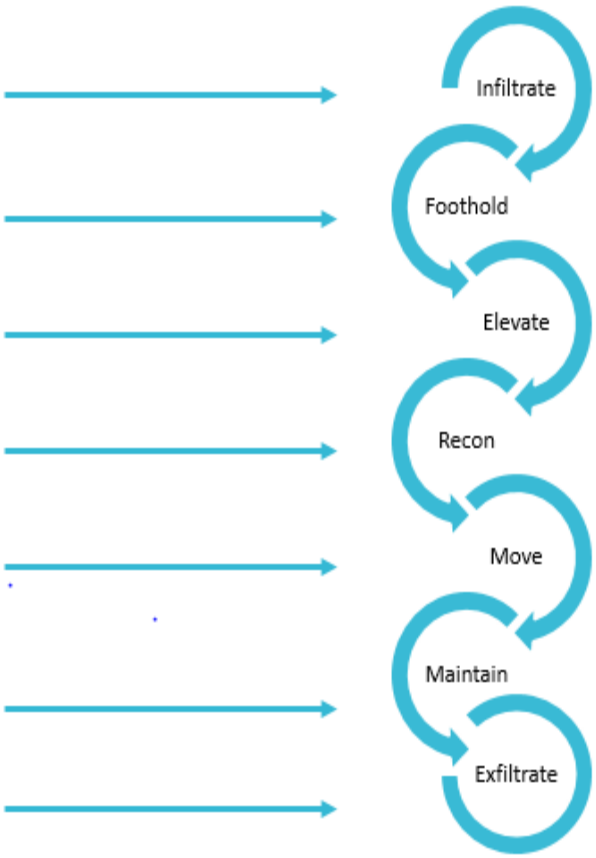
FireEye HX identifies attempts to increase permissions and shares that information with other security devices

Security Professionals are trained to watch for anomalous, reconnaissance activities

FireEye NX detects attempts to move throughout the network and infect other machines

Carbon Black Protect enforces control on workstations and servers to ensure only approved applications are installed

Carbon Black Response quickly identifies the scope of compromise and aids in investigation



Authored by Vikas Kumar
TCS Enterprise Security and Risk Management