White Paper

McAfee®

Combating Advanced Persistent Threats

How to prevent, detect, and remediate APTs

Table of Contents

Advanced persistent threats (APTs)—sophisticated, covert attacks bent on surreptitiously stealing valuable data from targeted and unsuspecting companies—can inflict serious harm to your business. Their relentless, persistent intrusions typically target key users within organizations to gain access to trade secrets, intellectual property, state and military secrets, computer source code, and any other valuable information available. And no one—from government agencies to start-ups—is immune today. You can, however, take proactive and rigorous steps to detect APT in their early stages and implement asset-protecting remediation.

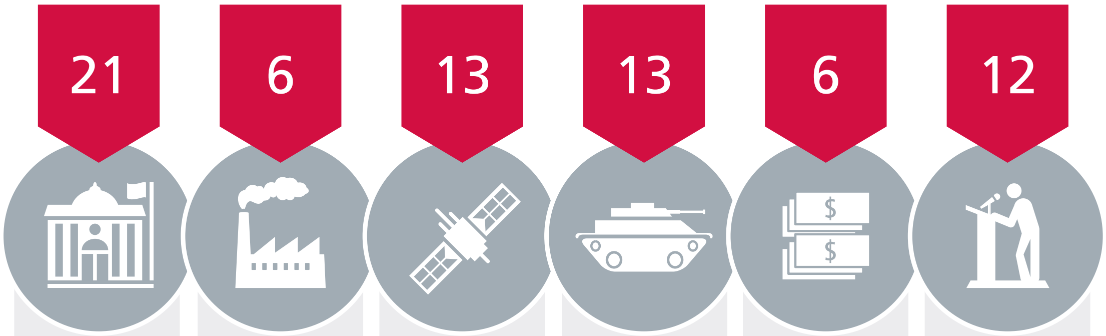
APTs According to Gartner

"Gartner uses a simple definition of APT. 'Advanced' means it gets through your existing defenses. 'Persistent' means it succeeds in hiding from your existing level of detection. 'Threat' means it causes you harm."

—Strategies for Dealing With Advanced Targeted Threats
John Pescatore
August 2011
Gartner

Targeted Attacks Are on the Rise

Until recently, most organizations assumed that they could fly under the radar of targeted attacks, that APTs were mostly a concern of governments, financial services organizations, and large energy and utilities companies. New data suggests that these same targeted attack techniques are being used on an ever-widening range of industries and companies. In Operation Shady RAT, for example, data from of a single command and control server showed evidence that one attack organization successfully hacked 71 companies across 31 industries.



US Federal Government	6	Construction/Heavy Industry	3	Electronics Industry	3	Defense Contractor	13	Real Estate	2	International Sports	5
US State Government	5	Steel Industry	1	Computer Security	2			Accounting Industry	2	Economics/Trade	2
US County Government	3	Energy	1	Information Technology	2			Agriculture	1	Think Tanks	2
Canadian Government	2	Solar Power	1	Satellite Communications	2			Insurance	1	International Government/Economics/Trade	1
Vietnam Government	1			News Media	2					Political Non-Profit	1
Taiwan Government	1			Information Services	1					US National Security Non-Profit	1
US Government Contractor	1			Communications Technology	1						
United Nations	1										
Indian Government	1										

Source: McAfee

Figure 1. In Operation Shady RAT, McAfee identified 71 compromised parties, comprising more than 31 unique organization categories.

What Is an APT?

While APTs use many of the same techniques as traditional attacks, they differ from common botnets and malware because they target strategic users to gain undetected access to key assets. APTs can do insidious damage long before an organization knows that it has been hit.

While blocking attacks before they can infiltrate your network is always the best means of minimizing harm, organizations under APT siege can fight back with intelligently designed incident response plans geared to their unique characteristics.

APT is to intrusion detection what stealth aircraft are to radar. They are targeted attacks designed to evade conventional detection. Once "inside" and disguised as legitimate traffic, they can establish covert, long-term residency to siphon your valuable data with impunity.

While recent headlines have focused on the most sensational examples of highly organized and well-funded attacks—Google, Adobe, RSA, Lockheed Martin, SONY, and PBS—thousands of undisclosed attacks have quietly plagued government agencies and corporations large and small worldwide.

APTs represent a fundamental shift compared to the high-profile hacking events of prior years that commonly targeted networks. Focusing on the weakest links of your defense chain, APTs target specific system vulnerabilities and, more importantly, specific people. While the victimized organizations vary in size, type, and industry, the individuals they target usually fit the same profile: people with the highest-level access to the most valuable assets and resources.

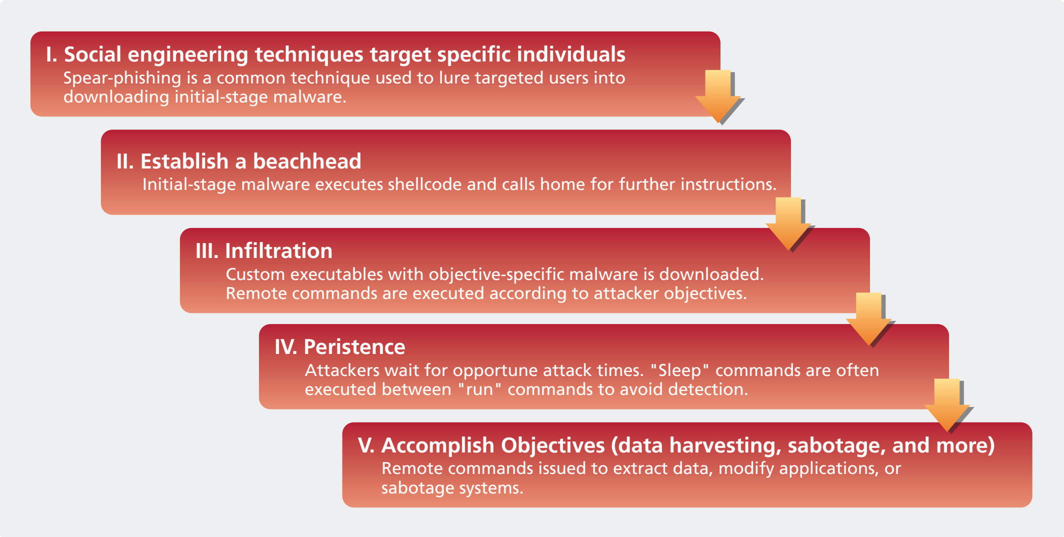
Vulnerabilities Matter

"The reality is that the most important issues are the vulnerabilities and the techniques used to exploit them, not the country that appears to be the source of the attack. The major advance in new threats has been the level of tailoring and targeting—these are not noisy, mass attacks that are easily handled by simple, signature-dependent security approaches."

—*Strategies for Dealing With Advanced Targeted Threats*
John Pescatore
August 2011
Gartner

Stages of a Targeted Attack

For entry, many APTs use spear-phishing techniques. They try to persuade the user to click on seemingly harmless links. For example, attacks seeking access to financial data will often target senior finance officials by sending them a legitimate-looking Microsoft Excel file innocuously named "Recruitment Plan." Initial-stage malware downloads typically happen together with the bait file and executes quietly in the background in order to avoid detection by the user.



I. Social engineering techniques target specific individuals
Spear-phishing is a common technique used to lure targeted users into downloading initial-stage malware.

II. Establish a beachhead
Initial-stage malware executes shellcode and calls home for further instructions.

III. Infiltration
Custom executables with objective-specific malware is downloaded. Remote commands are executed according to attacker objectives.

IV. Persistence
Attackers wait for opportune attack times. "Sleep" commands are often executed between "run" commands to avoid detection.

V. Accomplish Objectives (data harvesting, sabotage, and more)
Remote commands issued to extract data, modify applications, or sabotage systems.

Figure 2. Typical APT attack steps.

Early-Stage APT Detection and Prevention

Because APTs operate covertly and are difficult to detect, months can pass with no visible compromises to the organization quietly under attack. Moreover, single instances may be detected while multiple others inside the same organization go unnoticed. Comparable to combating a life-threatening disease, early detection is vital. Here are some warning signs:

Warning Signs	Detection Methods	Recommendations
Suspicious Emails	Email is the most widely used entry point for targeted attacks. Monitoring email activity for suspicious messages and downloads can help detect APTs early.	• McAfee® Email Security with message, sender reputation and effective spam filtering • Employee education on safe email practices
Anomalous Traffic	Establish a baseline of normal network behavior (protocols, applications, user behavior). Watch for unexpected changes in protocol usage, traffic volume, and user behavior.	• McAfee Network Threat Behavior Analysis tracks network activity and assign host threat factors according to malicious-looking behavior
Look for Shellcode	Malware payloads are typically hidden in common file formats (pdf, html, gif, and other file types). Being able to decrypt, decode, and uncover malware shellcode is one of the most effective methods for discovering APTs.	• McAfee Network Threat Response can detect shellcode in real-time in most common file formats, including pdfs, the most widely used method for delivering exploit code.
Suspicious Connections	Attacks can often use IP addresses, websites, files, and email servers with a history of malicious activity. Use tools with built-in reputation intelligence to scrutinize the reputation of connections with unreliable sources outside of your organization.	• McAfee Global Threat Intelligence™ provides reputation information through the following McAfee products: ◦ Network Security Platform ◦ McAfee Enterprise Firewall ◦ McAfee Web and Email Security

Have the Proper Tools

"One of the key steps to defending against the subtle and quiet attacks that are part of APT is to have the proper tools in place."

—Jason Andress
ISSA Journal
June 2011

Late-Stage APT Detection and Prevention

Most APTs are discovered after security is compromised and damage is well underway. Here are late-stage warning signs:

Warning Signs	Detection Methods	Recommendations
Application Changes	Once inside the network, hackers will often try to issue commands to key applications. Use application whitelisting techniques detect and prevent unauthorized change attempts on key applications.	• McAfee Application Control uses whitelisting capabilities to monitor and manage application change requests.
Data Access Attempts	Unauthorized attempts to access critical data and database structures are a tell-tale sign your network may be compromised. Use database activity monitoring tools to detect unauthorized access attempts.	• McAfee Database Monitoring uses real-time monitoring to detect and terminate suspicious sessions and quarantine malicious users
Data Transfer	*Type of data*—Keep a close watch on sensitive data types using data loss prevention tools. Actively monitor data structures matching intellectual property.	• McAfee Data Loss Prevention monitors servers, clients, and network traffic for the transfer if confidential information
	Quantity of data—Monitor for unusual quantities of data movement, encrypted traffic, or atypical file transfers within or outside your organization.	• McAfee Network Threat Behavior Analysis establishes a baseline of normal activity and alerts users to suspicious anomalies in traffic, including data movement
	Destination of data—Use reputation intelligence to track the destination of out-bound data. Connections with suspicious IP addresses using non-standard protocols or atypical ports are all red flags for APTs.	• McAfee Network Security Platform and McAfee Firewall Enterprise can alert or block suspicious network connections based on McAfee Global Threat Intelligence and behavior heuristics

APT Incident Response Plan

It's vital that every IT organization has an APT incident response plan at the ready. And planning should start with identification and education of individuals and systems most likely to be targeted because of their access to important assets.

The initial response phase is critical because it requires all actions taken once an incident has been detected to prepare for the investigation phase. It can also prevent knee-jerk reactions that could compromise evidence, create redundancy of work, and lead to ineffective remediation steps. Rushing to "fix" compromised systems without performing due diligence on the attack can alert hackers that they've been discovered, further compromising containment.

Furthermore, APTs are like cancers. Remediating only a subset of the infected systems will likely lead to recurring exposure. Before rushing headlong into response mode, notify the appropriate security administrators, gather as much data as possible, and construct a strategic response and remediation plan consistent with your business objectives. The key is to ensure that all evidence is preserved and the process is documented.

Post-mortem analysis of the incident's root cause and recommendations of changes in the process are crucial. Without them, the same mistakes are likely to be repeated the next time an incident occurs.

The following is a framework for creating a custom incident response plan for your organization:

Focus on High-Priority Security Controls

"Gartner recommends focusing on high-priority security controls (for example, the SANS Institute's Consensus Audit Guidelines or the PCI Security Standards Council's Prioritized Approach) and emphasizing improving the effectiveness of change control/configuration management, vulnerability management, intrusion prevention, and privilege management processes."

—Strategies for Dealing With Advanced Targeted Threats
John Pescatore
August 2011
Gartner

Plan Phases	Phase Categories	Detail
Preparation	Risk Assessment	• Identify and classify business assets and data stores • Conduct vulnerability assessment across critical infrastructure • Quantify risk with highest value assets and highest vulnerabilities atop the list • Recommended solutions: ◦ McAfee Risk and Compliance
	Security Assessment	• Review security measures protecting critical business assets • Recommended solutions for APT prevention: ◦ McAfee Email Security with message and sender reputation ◦ McAfee Web Security with URL reputation ◦ McAfee Firewall Enterprise with application awareness ◦ McAfee Network Security Platform for intrusion prevention with file, IP reputation, and behavior heuristics ◦ McAfee Application Control with whitelisting ◦ McAfee Data Loss Prevention
	Organizational Preparedness	• Identify key individuals most likely to be the target of social engineering attacks (due to high levels of access) • Implement aggressive access control by restricting network access of key individuals to 'business need to know' • Employee training: ◦ Prioritize high-risk individuals and work groups ◦ Examples: safe surfing practices, what to do with suspicious emails, social networking dos and don'ts
	Operational Preparedness	• Identify incident response team (including legal and business owners) • Communication plan, including law enforcement if necessary • Schedule/conduct incident response dry run

(continued)

Plan Phases	Phase Categories	Detail
Investigation and Initial Response	Detection	• Recommended detection technologies: ◦ McAfee Network Threat Response for malware detection, root cause analysis ◦ McAfee Network Threat Behavior Analysis to identify attack propagation, scope of attack ◦ Third-party network forensics to assist with log analysis, historical context ◦ McAfee Network Security Platform to detect unusual connection patterns and malware downloads ◦ McAfee Data Loss Prevention to identify data breaches
	Internal Stakeholder Notification	• Business owners • IT management • CEO, CTO • Board of directors (if necessary)
	External Response Strategy Notification	• Corporate/public relations • Law enforcement (if necessary) • Compromised users (if necessary) • Regulatory bodies (if necessary)
Containment	Countermeasures	• Custom intrusion prevention system signatures • Quarantine and clean infected devices • Update firewall rules, policies to block command and control channels

Conclusion

Today's organizations can't assume that they will fly under the radar of APTs. As APT methods propagate within the hacker community, more organizations will fall victim to targeted attacks and suffer potentially irrecoverable losses.

The key to effective APT protection, detection, and response is rigorous implementation of security best practices and ongoing education with your most highly targeted users. Advance incident response planning can significantly improve your chances of early detection and more effective remediation.

To find out more about McAfee solutions and services for Advance Persistent Threats visit these sites:

McAfee Network Security
McAfee Risk and Compliance
McAfee Consulting

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com