



# Becoming the APT

---

Thwarting Advanced Persistent Threats in Your Environment

**CORE Security**

+1 617.399-6980

[info@coresecurity.com](mailto:info@coresecurity.com)

[www.coresecurity.com](http://www.coresecurity.com)

[blog.coresecurity.com](http://blog.coresecurity.com)

## Introduction

---

A sea change is taking place in information technology security. Organizations large and small, across the globe are discovering that two decades of investment in conventional IT security technology such as antivirus software, firewalls and intrusion detection tools can no longer stop hackers armed with sophisticated hacking tools like automated exploit kits, spear phishing attacks and SQL injection. These sophisticated adversaries - some driven by profit, others by political or ideological aims – troll for sensitive information and intellectual property that can be used to game or disrupt world markets. This great and widening imbalance between threats and defenses demands new tools and strategies tailored that will allow organizations of all stripes to adequately protect themselves from the attacks they now face.

This paper was written to help you understand some of these new “advanced persistent” threats and to discuss the kinds of investments you can make today to help prepare your organization to successfully defend itself on the key battlefield of the 21st Century: cyberspace.

## Malware

---

Once a cottage industry, “malware,” or malicious software programs, is now a multi-billion dollar industry characterized by a high degree of automation and diversification. Today, malware production runs at industrial scale. McAfee Labs identified more than six million unique malware samples in the first three months of 2011 – the busiest quarter ever. That kind of output exceeds the ability of antivirus researchers and software firms to stay on top of the threats. Indeed: that’s the point. Attackers, in other words, don’t need to reinvent the wheel to get malicious programs running on a corporate network. Subtle and insignificant modifications to existing malware have proven adequate to bypass antivirus engines and other security products. And good enough is all attackers need to get a toe hold within enterprise networks.

## Advanced Persistent Threats

---

Recent events have shined a light on attacks attributed to so-called “advanced persistent threats” (APTs). A special category of online attacker, the APT refers to agents behind sophisticated, stealthy attacks on U.S. military installations and private firms in the defense industrial base. Though attribution is difficult, many of these attacks have ties to the People’s Republic of China, though other nations and politically aligned hacking groups have also been linked to APT attacks. While APT attacks are generally considered to be state sponsored, APT-style attacks may or may not have ties to state actors. What they do share in common is evidence of considerable advanced planning and reconnaissance on targets, as well as the use of tools and techniques that assure long term, silent compromise of target networks and systems. With detailed foreknowledge of their human targets, APT-style attacks often begin with targeted phishing (or “spear phishing”) attacks on key employees and executives. Often, these use e-mail, social network or even telephone or face to face communications that are highly credible and unlikely to raise suspicion.

Once APT attackers have a foothold on their target network, they’re adept at moving, slowly and deliberately from low value to higher value targets. Weakly protected user accounts, un-patched or poorly configured systems and previously unknown exploits are used to escalate their privileges and take over accounts with

access to key network resources and data. That data is then copied and secreted off site – often using compromised systems on the victim network as initial staging grounds, encryption and back channel communications over uncommon ports to cloud based servers controlled by the attackers.

## More Threats, More Targets

---

Cyber attackers haven't just improved their ability to churn out malicious applications. They've also become savvier about the kinds of targets they choose to compromise. The past few years have been notable for attacks and eye popping thefts from high profile targets – credit card records for 94 million customers of retailer TJX in 2007 and 130 million from Heartland Payment Systems in 2008.

But in recent years, cyber criminals have figured out that that high profile hacks lead to high profile investigations. Besides, trying to fence the stolen financial information of million individuals presents logistical challenges of its own. The result? Online crime groups are moving down stream: targeting smaller businesses and non-profits with fewer assets, smaller budgets and lower profiles. In just one sign of that shift, Verizon reported in their 2011 Data Breach Investigation Report (DBIR) that there were more data breaches in 2010, but less data stolen, as attackers shifted to smaller fry, and smaller bore attacks on point of sale (POS) and Automated Clearing House (ACH) systems that can deliver a steady, if unspectacular, stream of income.

## Employees: Your Biggest Vulnerability

---

Employees, rather than network or application weaknesses, represent the single largest threat facing organizations in nearly every industry. So-called “social engineering” tactics are often the first stage of most advanced attacks. This type of soft attack might include e-mail or instant messages via social networks that are targeted at key employees. Their goal is often to push malicious code onto a target's computer, gaining access to a sensitive corporate network. In other cases, e-mail and instant messages, phone calls or even face to face encounters can be used to harvest information that might be used at a later stage of the attack, such as names and titles of personnel, information on applications that are running internally, behind the corporate firewall, or even credentials for key IT assets. Many firms have increased training and awareness of these kinds of attacks, but financial services organizations are only as strong as their most vulnerable employee, so achieving uniform protection is hard.

### **Morgan Stanley: Victim of Aurora Attack**

Banking giant Morgan Stanley was a victim of a stealthy attack that is believed to be part western of a wide-scale hack of leading firms dubbed “Aurora.”

The attack, which was first made public by Google, has been linked to China and is believed to have been carried out by groups linked to the Chinese People's Liberation Army.

Originally associated with technology and defense firms including Google, Adobe, Juniper Networks and Rackspace, the attack was actually much broader, involving leading firms in industries such as petrochemicals, entertainment and finance.

According to internal e-mail stolen from the security firm HBGary and published online by the group Anonymous, Morgan Stanley was one firm targeted by the Aurora attackers. The hackers placed malware on Morgan Stanley's network that was tailored to stealing and transmitting sensitive documents. Morgan Stanley declined to comment and the exact length or nature of the attack isn't known, but the company was looking into help from firms to increase its defensive posture and plug holes in its network defenses that were exploited by the Aurora attackers.

The increasing use of social networking applications like LinkedIn and Facebook makes social engineering attacks easier than ever to conduct. Social networks put reams of personal- and organizational information online and create implicit trust relationships between employees and a vast network of “friends” and business associates. Attackers can leverage a detailed understanding of each employee’s social graph and use that information to concoct targeted phishing e-mails or other social engineering attacks that have a high likelihood of success. Furthermore, social networking platforms have become a leading vector for attack using malicious links and attachments.

## **Legacy Controls Fight the “Last War”**

---

Finally, many of the tools and technologies that are mainstays of IT security today were developed to fight the ‘last war’ against worms, viruses and e-mail spam. These tools are necessary – especially in light of regulatory requirements – but insufficient to counter the threat posed by advanced, persistent threats that use tools such as spear phishing attacks, custom data stealing malware and zero day exploits to gain control over critical IT assets. Legacy IT security products like network and Web vulnerability scanners, intrusion detection and endpoint protection suites are still often siloed with their own management and reporting systems IT staff have to struggle to make sense of their security posture and correlate information in ways that is necessary to spot stealthy attacks. The rapid growth of Web infrastructure and the adoption of Web-based applications within financial services firms – from social networking platforms to software as a service –leaves financial services organizations exposed to sophisticated Web based attacks launched via search engine optimized Web pages or social networks.

## **Thwarting Advanced Threats and Attacks**

---

It’s important to remember that advanced persistent threats are a “who” and not a “what.” That is: the characteristic that most defines them is that they’re human opponents with a clear objective in mind. No single security technology is likely to thwart them because, by definition, attacks that are unsuccessful will be followed by further attacks until their objective is achieved. (That’s the “persistent” part.)

If APTs can’t be stopped, how can they be defeated? By putting in place technologies and processes to proactively identify and mitigate the key vulnerabilities that are common to most all APT attacks, while also instituting a program of continuous security monitoring that incorporates new threat intelligence and ongoing posture assessments. Will taking these steps prevent an APT attack? Possibly not. Will they raise the bar considerably for advanced persistent adversaries, while protecting critical IT assets? Yes.

Steps that are most critical to thwart APTs include:

### **Identifying critical assets**

Even sophisticated organizations fall to APTs and other sophisticated attacks because they fail to pay proper attention to securing and monitoring critical assets. Stopping a receptionist or support desk employee from clicking on a malicious Web link is a difficult task and, in a large organization with thousands of employees, it may be impossible to prevent. However, hardening application servers, databases that store critical customer account information or transaction processing systems is a more defined and achievable task. And, when

critical systems are properly secured against attack, APT attacks will be less likely to spread from less sensitive to more sensitive systems, limiting the scope of compromises.

## Testing exploitable network, endpoint and Web-based systems

Of course, just knowing where your critical IT assets are located isn't enough. In order to prevent APT attacks, financial services firms need to learn to think and act like hackers, themselves. This means identifying the exploitable vulnerabilities on their network and likely paths of attack that sophisticated hackers might use to gain access to sensitive systems and data. Accounts of recent APT- and hacktivist attacks against firms like EMC/RSA, Google, the International Monetary Fund and The NASDAQ and HB Gary Federal make clear that advanced, persistent adversaries are adept at exploiting vulnerabilities on low-value assets then using those to move laterally within networks to the high value IT assets that are their target. SQL injection vulnerabilities on publicly accessible Web applications, for example, often provide the foothold that sophisticated attackers need to begin their exploitation of an entire network. Unfortunately, financial services firms lack the human resources to assess the security of hundreds, thousands or tens of thousands of IT assets, let alone study the possible connections between such systems that could be used by attackers. If APT attacks are to be stopped, however, organizations need to find a way to thoroughly and continuously vet public facing applications, internal network assets and endpoints for vulnerability to known exploits and common attacks.

## Optimizing existing security investments

In recent years, various tools have emerged to help with the problem of security information overload. Log management and security information and event management (SIEM) software have helped to make order out of the chaos of siloed security tools such as intrusion detection sensors (IDS), vulnerability scanners, network and application firewalls and endpoint protection suites. Governance, Risk and Compliance (GRC) tools can help connect the dots between mandated protections and processes and a firm's current security deployments and posture.

However, firms facing advanced persistent adversaries need more than a means of correlating information from their security infrastructure or producing reports for auditors. Penetration testing of corporate environments allows your staff to "see" networks in the way that likely adversaries will see them – with a focus on critical exposures and at risk data and systems. In addition, penetration testing enhances the value of

## Bank of America's Long, Strange Trip

Bank of America, one of the largest financial institutions in the world, found itself at the center of a maelstrom of negative news reports in 2011, after internal documents from the company were leaked to the Web site Wikileaks.

The leaked e-mails, which the whistle blower site said showed malfeasance on the part of BoA executives, led the group Anonymous to launch distributed denial of service (DDoS) attacks against BofA Web site. But that was just the beginning of the problem. After Anonymous hacked security firm HBGary in February, 2011, Bank of America again found itself in the headlines, this time over internal HBGary e-mail that suggested the bank sought help from HBGary and other firms to strike back at Wikileaks, Anonymous and other individuals it found hostile.

Bank of America denied any responsibility for the e-mails, which we sent by HBGary, Palantir and others in the hope of winning BoA business. But the bank's image was tarnished, while retaliatory DDoS attacks and other online actions followed the release of the HBGary e-mail.

tools like vulnerability scanners and intrusion detection sensors – identifying systems that are most at risk so that the capabilities of those products can be focused in areas where there is the greatest need. Similarly, the high level views provided by SIEMs and risk management tools can be informed by the results of penetration testing; providing ongoing monitoring and measurement so that they no longer represent the snapshot of an organization’s posture at a point in time, but a real-time picture of an organization’s security posture that highlights those areas that represent the highest risk of compromise.

## **Hardening endpoints and users to attack**

Finally, organizations have to find a way to harden their soft underbelly: the employees, contractors and business partners who can provide easy access to sensitive data and resources. Experience has shown that even low level employees can prove to be critical chinks in the armor of sophisticated IT defenses. Similarly, malware can spread from infected home computers over VPN tunnels to corporate networks, while mobile workers might unwittingly compromise corporate networks with infected laptops and mobile devices, providing a vantage point from which attackers can scan networks, identify other assets and move laterally.

To protect their critical assets, firms need to assess the susceptibility of their employees, contractors and partners to social engineering attacks. Mock attacks as part of a comprehensive penetration testing program can pinpoint vulnerable employees and areas that demand greater user education. Solid employee education about social engineering, phishing and unsafe computing practices based on the findings of such assessments can lower the likelihood that such attacks will be successful – if not prevent them outright. That’s especially true if training is followed by assessments that present employees with real world social engineering attacks and tricks, and then measures their level of awareness and their response to them.

## **CORE Insight: Thwarting APTs with Scalable, Enterprise Testing**

---

CORE Insight® Enterprise from CORE Security® is an automated security testing and measurement solution that helps companies thwart advanced persistent adversaries by continuously and proactively assessing the security of critical information assets. CORE Insight allows companies to emulate advanced attacks - traversing exploitable web application, network and client-side weaknesses throughout a complex, enterprise IT environment.

CORE Insight pinpoints and traces key exposures within large, changing IT environments, scaling up to support 10,000 systems, web applications and end users. Customers define critical IT assets that are important to their organization, including systems handling sensitive data, transactions, operations controls, and so on. INSIGHT users can also identify types of data that advanced persistent adversaries seek, including credit card and Social Security numbers, or account identifiers.

INSIGHT works by replicating real-world attacks that seek to compromise those specific assets. Then the solution’s dashboards and reports distill the results of those tests for IT staff using terminology that is relevant to your business.

CORE Insight can spot key vulnerabilities and attack paths used by advanced persistent adversaries. These include:

- **Network systems:** INSIGHT can test for exploitable vulnerabilities in operating systems, services and applications.
- **Web applications:** INSIGHT analyzes Web applications and dynamically generates and launches SQL injection and blind SQL injection attacks.
- **End users:** INSIGHT can replicate and automatically launch phishing and spear phishing attacks against employees and test end user systems for exploitable vulnerabilities.

CORE Insight Enterprise is unique in its ability to replicate actual attacks against our systems and data – in a safe and controlled manner. Unlike other solutions, it does not scan for potential vulnerabilities, monitor for incidents, or model threats; it proactively uses the same offensive techniques that criminals employ to find and exploit weaknesses that expose our critical assets to data breaches.

INSIGHT follows a seven-step process that replicates attacks in your environment and identifies threats to critical assets.

## What CORE Insight Can Tell Us about Advanced Persistent Attacks

---

CORE Insight continuously tests your network's resistance to attack: identifying, proving and tracing exposures to critical assets. Advanced, persistent adversaries will always require the time and attention of your top IT staff. But even the most talented and knowledgeable security experts can struggle to stay on top of a large and ever-changing IT environment and anticipate every type of attack. CORE Insight allows organizations to automate testing against critical IT assets, find vulnerabilities in a wide range of systems and enumerate connections and potential attack paths. Security test results are centralized in the solution's CSO Dashboard and aggregated in Campaign, Trend and Executive Summary reports; allowing top tier managers and executives easily assess their organization's security posture.



41 Farnsworth Street | Boston, MA 02210 | USA | Ph: +1 617.399.6980 | [www.coresecurity.com](http://www.coresecurity.com)  
Blog: [blog.coresecurity.com](http://blog.coresecurity.com) | Twitter: @coresecurity | Facebook: Core Security | LinkedIn: Core Security

© 2012 CORE Security, the CORE Security logo, and CORE Insight are trademarks or registered trademarks of CORE SDI, Inc. All other brands & products are trademarks of their respective holders.