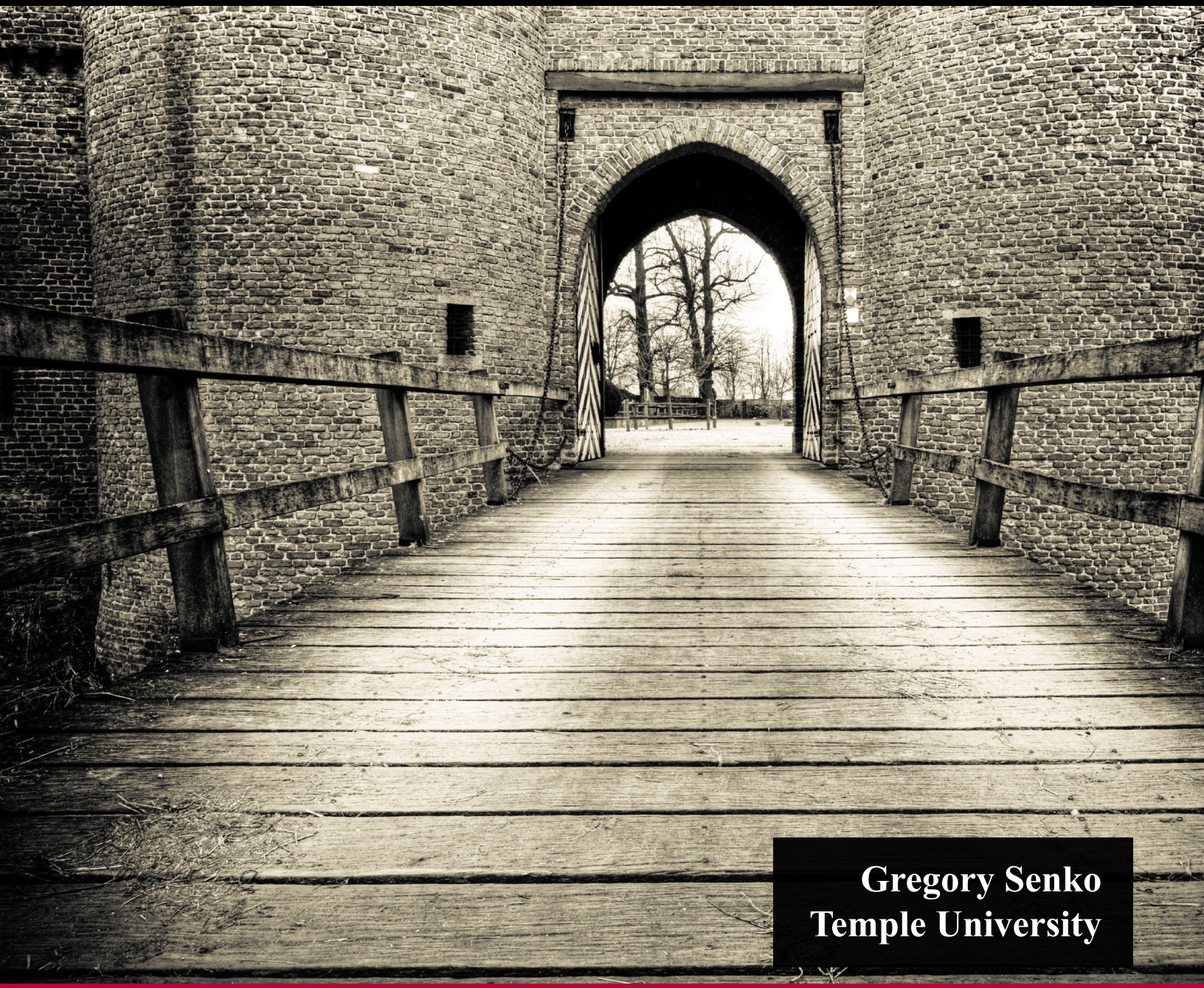
The IBIT Report

A publication of the Institute for Business and Information Technology

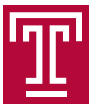
Providing Cutting Edge Knowledge to Industry Leaders **January 2014**

Barbarians Inside the Gate:
Dealing With Advanced Persistent Threats



Gregory Senko
Temple University

Fox School of Business
TEMPLE UNIVERSITY®



Fox School of Business
TEMPLE UNIVERSITY®

The IBIT Report

 ISSN 1938-1271.

The IBIT Report is a publication for the members of the Fox School's Institute for Business and Information Technology. IBIT reports are written for industry and based on rigorous academic research and vendor neutral analysis. For additional reports, please visit our website at http://ibit.temple.edu.

Disclaimer: The conclusions and statements of this report are solely the work of the authors. They do not represent the opinion of Temple University or the members of the Fox School's Institute for Business and Informational Technology (IBIT).

Review process: IBIT reports are sourced, reviewed, and produced as follows. The managing editor oversees this process. The editor and editor-in-chief consult on topics and identify new sources of reports. The editor typically works with authors who are interested in writing reports and provides feedback on initial drafts. Completed reports are first screened by the editor-in-chief. After approval the report is sent out for review to two members of the editorial board. The editor-in-chief assesses the completed reviews and provides further guidance to authors. Final reports are then professionally produced and made available to IBIT members.

Foreword

In December 2013 retail giant Target disclosed a security breach that resulted in the theft of 40 million credit and debit card records. This was the latest in a series of well-publicized hacking incidents in the United States, causing individuals and companies to question the security of their electronic information.

This IBIT Report describes how the field of information security has evolved from establishing barriers to prevent unauthorized entry to identifying threats from within a company's own defenses. The ever-increasing sophistication of hackers' use of malicious software (malware) to elude perimeter security and operate over extended periods creates new challenges for the IT organization. These "Advanced Persistent Threats" require new approaches and frameworks. To protect against the barbarians inside the gate, the author recommends four transformative steps to achieve more robust enterprise security. Everyone concerned about the safety of their organization's information assets will want to take note of these recommendations.

Bruce Fadem
Editor-in-Chief
February 10, 2014

Introduction

In July 2013, Bloomberg news reported on what prosecutors called the largest hacking scheme in U.S. history (Voreacos, 2013). They reported that five conspirators had been charged with computer break-ins at corporate retail chains such as 7-Eleven and the large French retailer Carrefour. The hackers are thought to have stolen 160 million credit and debit card numbers. Prosecutors also indicted one of the same five men and another man in a similar scheme that targeted the Nasdaq and 800,000 bank accounts at Citigroup and PNC Financial Services Group, Inc. In another recent case, it was revealed that the retail chain Target lost customer credit and debit card information to hackers on a similar scale.

The start of the 2013 holiday season saw a record number of targeted attacks, according to Symantec (Nahorney, 2013). There were more targeted attacks in November 2013 than that same month in 2012 or 2011 (see Figure 1). It is likely that there will be over 1,000 reported attacks for the second year in a row. Hackers have targeted large-scale virus and denial-of-service cyber-attacks at large corporations and government organizations for years. Besides its scope, this attack proved to be remarkable in another way. The hackers had perpetrated the attack over the course of seven years. The sophisticated attack was a type that has come to be known as an Advanced Persistent Threat (APT).

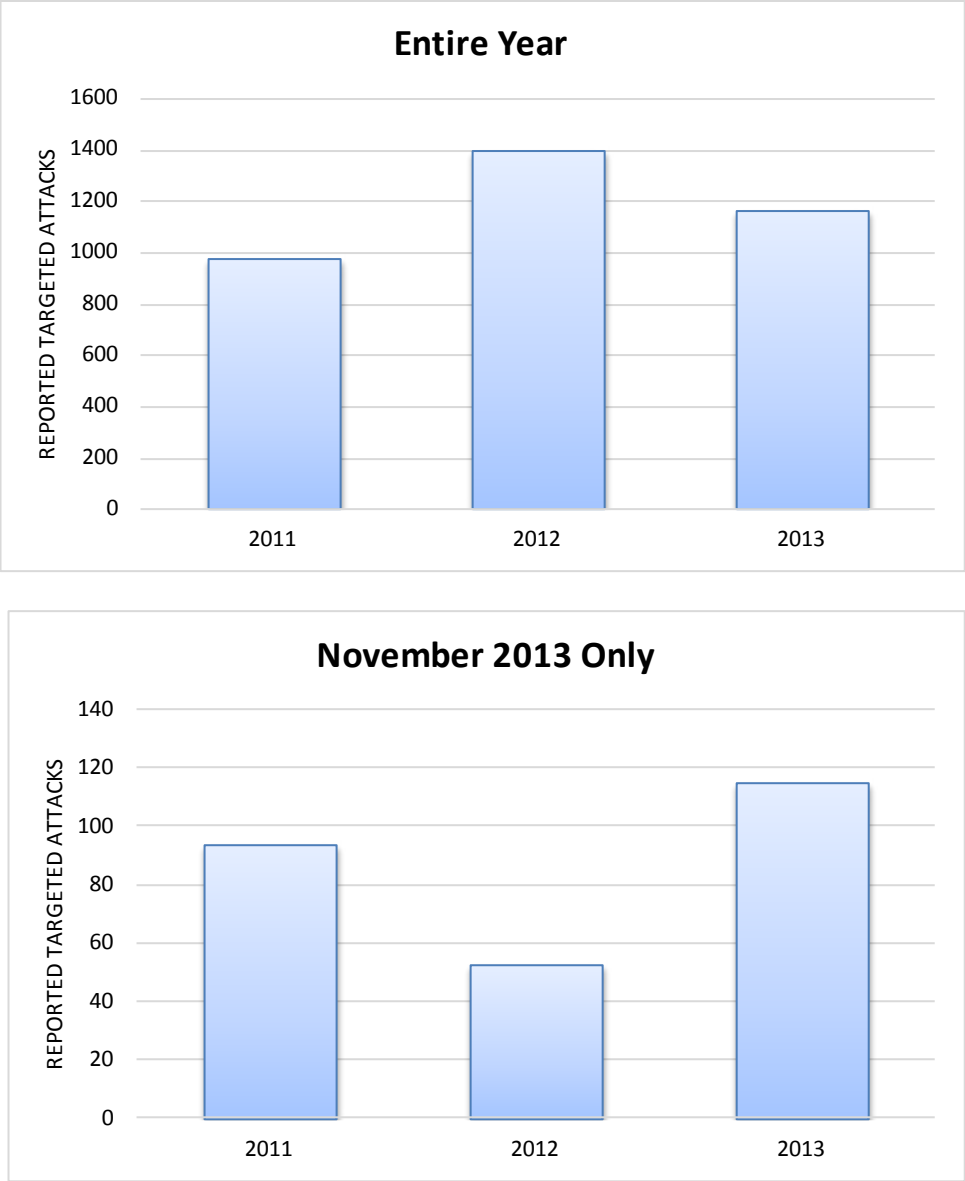


Figure 1: Targeted Attacks in 2013

This report outlines how the historical approach to security of placing emphasis on the strength of barriers to entry has led to the approaches for addressing Malware threats reflected in today's Corporate Information Security Apparatus. Current strategies and techniques for dealing with Advanced Persistent Threats that have proven able to circumvent common "peripheral" security measures are discussed and recommendations made regarding how IT organizations can adapt to face these sophisticated, targeted attacks.

Year-end total for 2013 was estimated based on figures available through November, 2013 from the Symantec's Monthly Intelligence Report (Nahoroney, 2013).

Fortified

It is human nature to protect ourselves and the things we care about by building barriers to keep things out. Castles had high walls and moats that made it difficult to penetrate a fortified city.

Similarly, isolation was the first technique that secured computer systems. While protecting computer equipment from theft and keeping systems from becoming vulnerable to operational disruption was a goal, the isolation strategy was a natural consequence of the "unwired" world. At first, computers were expensive and required special facilities that were easily locked down and protected against unauthorized entry. Physical security was the order of the day and everyone knew how that worked. It had been refined over thousands of years of human innovation and standardization.

In most corporations, perimeter security management still dominates efforts to protect corporate information assets.

However, even ancient peoples developed techniques to overcome the physical barriers erected by their adversaries. And, just as humans in antiquity built ladders to scale castle walls and movable scaffolding to bridge moats, physical break-ins still occur in everything from banks to warehouses to data centers.

Walls within Walls

Ancient fortress builders often constructed concentric walls to isolate more important structures and establish additional lines of defense against intruders. Today, network engineers now rely on multiple layers of logons and passwords to keep separate applications and databases secure from prying eyes and potential tampering.

The walls-within-walls approach added cost and complexity that made it difficult for companies to efficiently use their expensive computer systems. Controlled but ready access to information within a corporation is the lifeblood of commerce; individual application credentials were increasingly seen as complicated and productivity-inhibiting. As a consequence, systems that tracked identities and certified valid users surfaced as a way to open the environment to users "inside the walls" of a corporate network. This enabled access and facilitated optimal responses to business needs while still executing access controls at the individual level. The focus turned to strategies to prevent unauthorized users from accessing the network from outside.

Halt. Who goes there?

In most corporations, perimeter security management still dominates efforts to protect corporate information assets. The goal is to erect sufficient barriers to deter most would-be intruders. Most successful security penetrations prey on the naiveté of users, based on simple social engineering techniques that use "phishing" emails to trick users into allowing malware, software specifically designed to

compromise security or cause damage, to be installed on their systems. The response has been to identify the patterns that typically present through these malicious software agents, and to screen computers and networks for them.

This approach has led to the complicated and sometimes business-inhibiting array of network access passwords, firewalls, virus screening software and hardware, and intrusion detection systems that electronically "guard the gates" of most corporations. The goal is to keep bad people and software from getting into the protected environment. It is very much designed to work as a moat and walls protected a fortified city. The security "forces" are organized to continually re-enforce the barriers (update software and virus rotation signatures), stand guard against attack (monitoring and penetration detection), and respond to attacks (dedicated attack response teams) by isolating infected or compromised devices and interrupting access by malicious users.

The Enemy Within

As the story at the beginning of this report indicates, hacking has not only become a big business with higher and higher stakes, but has also turned into an arms race. The complex attacks now being brought to bear on specific corporate and government targets certainly brings to mind the legendary Trojan Horse the ancient Greeks used to penetrate the fortification of their adversaries. However, these attacks are also instances of espionage-style infiltration and subversion of a key mission of high profile companies: protection of their most valued assets, their customers.

The Emerging Challenge of Advanced Persistent Threats

The Stuxnet virus received a great deal of media attention in 2010 and 2011. One reason was that fears of an Iranian nuclear weapon made any event related to that perceived threat newsworthy. Stuxnet was most significant as the first well-publicized appearance of a successful, and apparently state-sponsored, act of modern Cyber Warfare. To date, it has been found in computers in places as sensitive as a Russian nuclear power plant and as remote as the International Space Station. The media attention given Stuxnet marked the beginning of the public awareness of Advanced Persistent Threats.

People who read about Stuxnet were impressed by its ingenuity, while others saw Stuxnet as an opportunity. Employing analytics, reverse engineering, and code cannibalization, hackers now had a working model for the construction of malware deliberately designed to elude perimeter security by circumventing traditional security arrangements that recognize threats as patterns in digital transmissions. Malicious hackers could now penetrate "secure" networks and continue to stealthily operate over an extended period from the place that companies had not thought to protect themselves: inside the victims' own defenses.

Advanced Persistent Threats (APTs) employ common hacking strategies in combinations that make them difficult to detect (see Figure 2). Many of the techniques are familiar to the general public as well as to security professionals. An IT security organization that relies on the tried-and-true strategy of strongly enforcing perimeter security with Internet firewalls and malware detection software and hardware must be ready to respond when a clever hacker penetrates those boundaries. But what if there is nothing out of the ordinary to detect?

APTs often use a variety of techniques to accomplish their mission. One of those missions is to take up residence within a company's computer systems and networks in a way that allows them to continue to accomplish malicious tasks and improve their compromising position over time. Often, this is an extended amount of time, such as the seven-year hack reported by Bloomberg (Voreacos, 2013).

Advanced Persistent Threats (APTs) employ common hacking strategies in combinations that make them difficult to detect (see Figure 2).

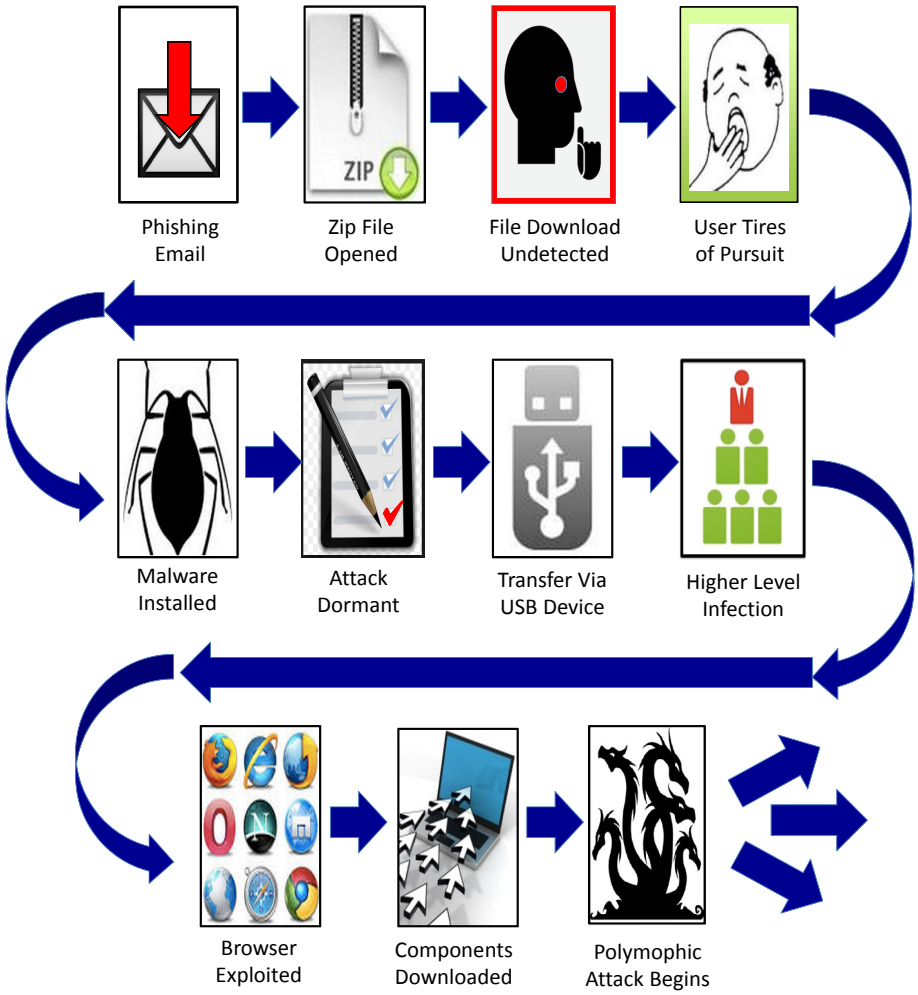


Figure 2: Genesis of an Advanced Persistent Threat

Organized for Incident Response

There are many ways to initiate an Advanced Persistent Threat attack. In the most common example, a company's perimeter security is breached in a phishing attack. It starts in an uneventful way (see Figure 3): an alarmed employee is determined to get to the bottom of the credit card security violation of which he was just notified via email. After a mouse click and a minute wait, nothing happens. Well, nothing visible.

Such an attack becomes invisible to the perimeter defenses. Incident response techniques are not engaged simply because no pre-identified "incident" has occurred. The email server is not churning out virus replicas. No unusual web sites are being visited. No extraordinary network traffic levels are detected. No pre-defined thresholds are being violated.

There are, of course, a number of ways for the initial instance of an APT to be put into place. Hackers are known for their creativity. A more elaborate penetration scheme, for example, might involve the innocent installation of a hardware upgrade by an engineer or technician who has been given a compromised piece of equipment.

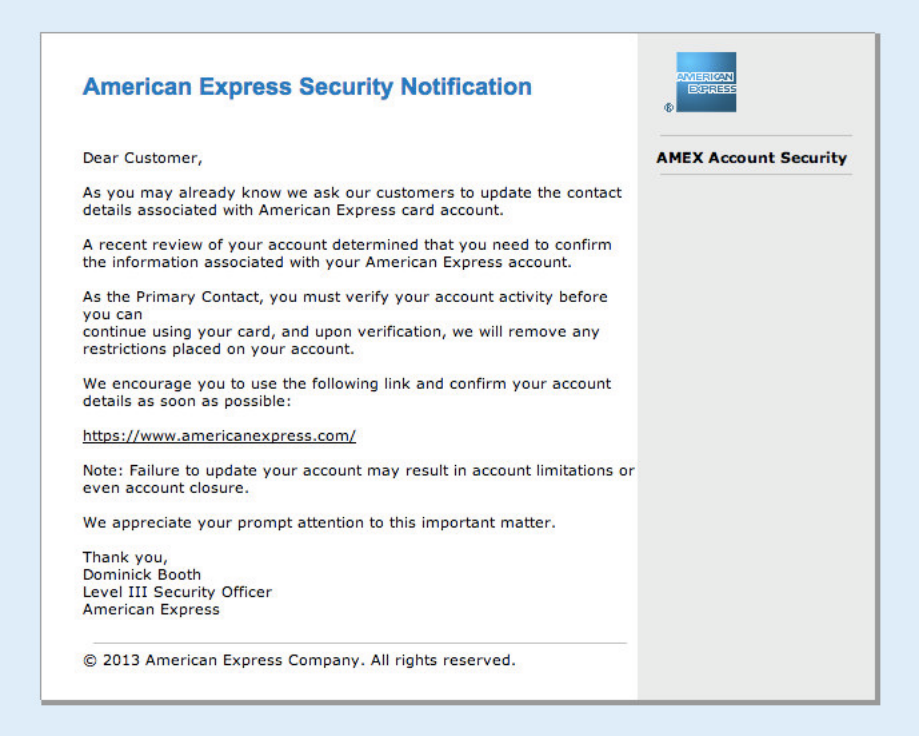


Figure 3: American Express Notification After a Phishing Attack

But, the characteristics of initial dormancy, opportunistic misappropriation of System Administrator rights, and a multi-component, multi-attack potential strategy that is called Polymorphism, are all essential ingredients of the elaborate and targeted attack.

In some cases, the malware is constructed in a purposeful and sophisticated way that goes after specific targets using well-known exploits. Still, the malware can accomplish this without detection by taking advantage of the "window" between the exploit and the opportunistic monitoring used to discover this sort of event. It alters the system's records to disguise its actions.

Assumptions about the safety of the network create a rich target environment for malware.

The reason this type of attack is possible is that the trusted network on which the exploit is running is designed to be secure from outside attack. But, because it is trusted, not all patches and protective techniques are deemed necessary or even cost-effective. Because the perimeter is hardened, the expectation is that attacks will be recognized and thwarted on their way in. Applications are not expected to have to be protected from each other on their own trusted network.

Such assumptions about the safety of the network create a rich target environment for malware. The desire to facilitate user convenience creates the key vulnerability APTs are designed to exploit. The benefits of a robust perimeter cyber defense and a quick incident response become a liability by fostering a false sense of invulnerability and minimizing the perceived need to "look within" for threats.

Defense, the Next Generation

What decisions are leaders of companies, even at the board level, being asked to make in order to secure their operations and make their shareholders comfortable with their cyber defense measures? In response to and anticipation of business concerns over Advanced Persistent Threats, many leading companies, as well as new or emerging ones, are expanding their offerings in this area. There are many variations in the range and type of offerings. In fact, these differences are sometimes exaggerated in an effort to promote their means of identifying, avoiding and addressing the risks associated with APTs. At a high level, vendors can be seen as providing offerings in three areas of approach to networked data security:

1. **Access Management**, or Cyber security devices and techniques aimed at protecting computer networks and Systems from outside attack. Examples include firewalls, intrusion detection systems (IDS), and proxy servers.

2. **Identity Managemen**t, the device and user characterization that establishes a profile and invokes a policy associated with permitted activities.

Examples include identity service engines, directory services such as LDAP, tokens, and smart cards.

3. **Cyber Analytics**, the acquisition, retention, and analysis of both aggregate and detailed cyber activity for use in trend and pattern analysis and predictive modeling. This includes logs and journaling, deep packet inspection, and big data analytics.

The Barbarians at the Gate

Perimeter security is the core of most security policies. The task of identifying malware on the way into the corporate network from the Internet is supported by an array of hardware and software-based strategies.

Intrusion detection systems of various capabilities also abound. In general, these systems share the approach of scanning system and network activity for signatures that represent suspect or policy-violating activities. These systems are limited by the quality and currency of their database of attack signatures.

A third, non-signature based protection scheme employs encryption to further protect systems at the individual device level. Called Endpoint Security, this technique incorporates rules-based Firewall-type restrictions as well as local anti-Malware protection approaches. The goal is to make the individual systems on the network, not just the overall environment, less vulnerable to intrusion. For example, Symantec's Endpoint Security product is popular on Windows-based enterprise systems.

Deep Dive

Google, with its advanced spanning data architecture and "Big Data" analytics, has inspired a relatively new and advanced approach to detecting activity "outliers" that may represent the kind of subtle activity associated with Advanced Persistent Threats. This truly proactive approach can be thought of as a kind of monitoring and analytics "on steroids."

Vast amounts of data from network devices, and even the content of packet traffic on an IP network, can be scanned for anomalies. The basis for comparison is an enormous set of historical data and metadata stored in big data architectures like Hadoop. Hadoop is now offered in a number of commercial security products. They bring the kind of analytic power previously used by the NSA and by lifestyle marketers to the world of every day network security.

Cloud-based Big Data Analytics vendors that gather data histories from their multiple client-base have an advantage over individual companies employing advanced analytics. The broad range of network activity and "deep packet inspection" data they gather enable them to

> The kind of information being transported, not just the type of message traffic and where it is going, provides a new level of analytic possibilities.

see emerging patterns early and recognize threats sooner than their enterprise data-restricted counterparts. So called "Deep Packet Inspection" involves looking not only at the identifying and routing information in a message stream, but also its content. The kind of information being transported, not just the type of message traffic and where it is going, provides a new level of analytic possibilities.

Next Steps for Business Leaders: Four Transformative Steps Toward More Robust Enterprise Security

Information security is often considered a "no win" game. If everything runs well, there is nothing to cheer about. But, when things go wrong, as they are bound to do in the threat-rich environment companies face today, the fingers point up … to the Chief Information Officer.

The successful CIO responds with leadership and vision to inspire and sound strategies to create an organization that knows the criticality of the protection of their company's information assets and is empowered to protect them. There are several key components of the modern information security strategy that every CIO should consider:

Step 1: Strengthen the Fundamentals

Advanced technologies will not buy much advantage without strong security underpinnings. The creation of reliable, fundamental security processes that support solid, up-to-date perimeter security, well-educated security engineers, and well-informed employees and customers should not be overlooked. The value of educating and reminding employees that they are an essential part of the security equation cannot be underestimated. The dollars spent to do this can pay ongoing dividends and are the principal way to deter would-be attackers who rely on inter-personal and technology-enabled versions of social engineering (like phishing emails) to gain a foothold. Also, consider endpoint security if it is not already in place. Don't reject the idea of whitelisting (i.e., locking down the range of operations permitted on a computer or server through software) out of hand; in some critical but vulnerable processes, it can be the most cost-effective solution.

Advanced technologies will not buy much advantage without strong security underpinnings.

Step 2: Broaden the Focus: Look Within

Many metrics are available and most likely are already being collected about activity on a company's network. They are principally used for performance management, issue identification, and problem mitigation. However, a security-oriented perspective on this same data may yield opportunities to identify subtle changes in activity that underlie a persistent attack. Advances in vendor offerings for aggregating network data and performing advanced analytics should also be considered.

Step 3: More Detection, More Anticipation, Less Remediation

Creating the discipline that encourages the information security organization to act proactively rather than just "put out fires" is a tall order. This is especially true because the resources that have the most sophistication as analysts are also the key personnel in dealing with emergency remediation activities. While these people are dedicated, talented, and capable, it is not in their best interest to design systems that make their day-to-day contributions less valuable or perceived as less essential. For some, it is just simply exciting and rewarding to successfully deal with emergency situations. For that reason, developing procedural and structural approaches that will help insulate the organization from threats can take a back seat to the "firefighting" that currently dominates the IT security function.

However, it is time for organizations to take up the challenge and design a set of thresholds and alerts that are clearly useful and valuable to the company in detecting attacks. Staff need to be given the responsibility to audit the metrics in near-real time, not when there is nothing more exciting to do.

Step 4: Tool Up

As perimeter security vendors enhance their products to become more sensitive to targeted, sophisticated attacks, not all organizations will be able to justify the costs of subscribing to cloud-based, Big Data-driven offerings (such as Splunk). Cisco's commitment to developing a community of analytics vendors that use its recently announced PxGrid standard to aggregate all network security information and enable advanced analytics has the potential to change the way cyber security is managed. At the same time, these technologies provide value in a place appreciated by the majority of network managers: enhanced network performance management and improved network management. We can expect a variety of offerings targeted at multiple price points to emerge as this product ecosystem evolves.

Organize, Re-Organize: Five Essential Cyber Security Functions

Not every enterprise will be able to immediately justify the expense of implementing the most advanced solutions. In that light, the following section describes five essential functions that should be present in the security organization to foster a progressively adaptive and responsive approach to changing Cyber Security threats (see Figure 4 for a summary).

Figure 4: Cyber Security Operations

IT Security Governance

IT Security Policy is a strategic concern that is often, in practice, treated as an afterthought. How is the Project Control Board, System Change Control apparatus, and system development security standards enforcement tied together from a strategic security perspective? Deep integration of security policy that looks ahead to auditability, monitoring, and resiliency concerns is required as a framework, regardless of the security technologies that are put into place.

Security Architecture

The highest level of security certification in the CIA's internal security standards requires that security be "baked in," from the top-down, in all systems and processes. That means that requirements, architecture, design and even testing must always be approached with Cyber Security in mind. What is the level of awareness within the IT organization of the overall approach to security architecture? How about outside the IT organization? Information security personnel need to put forward the best effort possible to support organizational security goals. A proactive, design-centric approach that is well-expressed, easily accessible, available to all those involved, when they need to refer to it, and reinforced through educational reviews and revision is essential to this part of the mission.

Application Development Security Standards and Enforcement

People often do not recognize the importance of an initiative unless it has a high level of sponsorship and they clearly see the rewards for compliance and the penalties for non-conformance.

How are urgent projects that, at pre- implementation review time, are found to have skirted key security considerations, handled? Clearly stated, understood, and uniformly enforced security standards are the only way to proactively reduce vulnerabilities in this case. The post-mortem review that arises from negative audit findings not only represents preventable vulnerabilities to the business, but more critically the specter of expensive remediation work.

Security Operations

Because security overall is often seen as an extension of the governance function and not part of IT, the IT security functions are sometimes minimized and take the form of incident response from an IT service perspective. This practice can be traced back to the origins of IT security in the processes developed for physical security. What is the range of responsibility of the IT Security Operations group? Strong perimeter security and effective incident response is still the basis of IT security. IT Security Operations deserves the same level of formal commitment as Physical Security Operations does, with parallel responsibilities, processes, and enforcement capabilities.

Security Auditing, Monitoring, and Analytics

As a means to accomplish an effective separation of duties, IT auditing is often attached to the Accounting and Financial Internal Audit groups. While the advances in the skill sets and the sophistication of tools available to internal security auditors continues to expand, it is still essentially a retroactive activity. Does the organization have a dedicated internal IT security auditing, monitoring and analytics group? As indicated earlier, the escalation in sophistication of advanced targeted security threats will demand that enterprises make the commitment to proactive and technically-enabled security audit, monitoring and advanced analytics capability in addition to their traditional audit capabilities.

Conclusion: The Adaptive Security Organization

A "more of the same" security approach is no longer an answer that will satisfy Chief Executives and Boards of Directors. To succeed, CIOs need to be the sponsor as well as the agent of change. The mission: change the organization in response to the changes in the Cyber Security Threat landscape. First, raise awareness of the significance of Advanced Persistent Threats. Encourage communications about this matter within the organization. Involve the security team from the inception of the change process. Foster a sense of urgency and effectively communicate the business risk to create a sense of desire to make the required changes. The rationale should be based on an improved understanding of the origins, evolution, and ultimately, the gaps in standard enterprise security approaches. Share information about recent advances in technical approaches to recognition and avoidance of sophisticated targeted attacks, to illustrate how the required changes may be attained. Provide examples of vendors and security capabilities for your organization to acquire. The new tactics may require investment in cultivating new skills and behaviors. Finally, reinforce these changes in the organization in a way that will sustain a work culture that is sensitive and conducive to a comprehensive approach to Cyber Security. Don't wait to get started.

References

Nahorney, B. (2013). Symantec Intelligence Report: November 2013, Symantec Corporation, retrieved January 1, 2013 from http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_11-2013.en-us.pdf

Voreacos, D. (2013). 5 Hackers Charged in Largest Data-Breach Scheme in U.S. Bloomberg Technology, retrieved January 1, 2014 from http://www.bloomberg.com/news/2013-07-25/5-hackers-charged-in-largest-data-breach-scheme-in-u-s-.html

About the Author

Greg Senko is an IT Strategist, Management Consultant, and former KPMG Partner. He is the Associate Director of the IT Auditing and Cyber Security Program at the Fox School of Business at Temple University. He holds CISSP, PMP, CSM and Prosci Organizational Change Management Certifications. Greg consults with clients in the Finance, Pharmaceuticals, Manufacturing and Communications industries in the Philadelphia area.

Fox School of Business and Management

Established in 1918, the Fox School of Business is the largest, most comprehensive business school in the Greater Philadelphia region, and among the largest in the world with over 6,500 students, 180 full-time faculty and more than 59,000 alumni.

The Fox Bachelor of Business Administration (BBA) in MIS is ranked in the top 15 and the MBA in Information Technology Management in the top 25 by U.S. News & World Report. The Association for Information Systems (AIS) ranked Fox School's MIS faculty number 1 worldwide for research 2009- 2012. The MIS student organization was recently named 'chapter of the year' by AIS.

Institute for Business and Information Technology

The Institute for Business and Information Technology (IBIT) provides cutting-edge knowledge and valuable connections to sustain excellence in IT. IBIT integrates industry perspectives with academic research expertise to create forums that generate best practices. IBIT membership offers firms the opportunity to leverage our knowledge, human capital, relationships, and established network.

CONFERENCES AND COMPETITIONS
IBIT conferences are exclusive interactive forums of practitioners and academics addressing current topics such as analytics, digital business innovation, and cyber-security. The Temple Analytics challenge provides practical experience to students in making sense of big data.

THE IBIT REPORT
Rigorous vendor neutral research that provides actionable knowledge to industry. Recent topics include big data, online labor markets, crowd funding, open innovation, video gaming, and social media.

PROJECTS
IBIT faculty and students work with member firms on joint research projects. Recent examples include a job index for information systems workers, and a grant program on big data.

IT AWARDS
The IT Innovator, Leader, and Distinguished Alumni awards are presented to industry leaders at the annual IT Awards Reception.

INDUSTRY INTERNSHIPS
Project-based internship model provides firms and students with a structured light weight opportunity to work on projects.

EXECUTIVE-IN-RESIDENCE
The program facilitates interaction between students, faculty and industry leaders.

CORPORATE TRAINING
IBIT offers customized on-site training to corporations on specific topics including analytics, cyber-security, and social media.

ADVISORY BOARD
The Fox IT advisory board includes senior executives from Lockheed Martin, Merck, LiquidHub, Walmart, Deloitte, ZDNet, Pfizer, Campbell Soup, Electronic Ink, and others.

The IBIT Report

The Fox School's Institute for Business and Information Technology (IBIT) regularly publishes The IBIT Report for its members. IBIT reports are based on rigorous vendor neutral academic research and are written to provide actionable knowledge to industry. Each report focuses on an important cutting edge topic that is of interest to our members.

For additional information, contact:
Institute for Busines and Information Technology
Fox School of Business
Temple University
210 Speakman Hall (006-00)
1810 N. 13th Street
Philadelphia, PA 19122

ibit@temple.edu
ibit.temple.edu
215.204.5642

Fox School of Business
TEMPLE UNIVERSITY®