INTERNET SECURITY ALLIANCE

THE ADVANCED PERSISTENT THREAT

Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing

ABOUT THE INTERNET SECURITY ALLIANCE (ISA)

Although the Internet Security Alliance (ISA) is structured as a multi-sector trade association, it is actually a unique organization that combines the thought leadership that might be found in a "think tank," with advocacy one would expect from a trade association, and operational security programs that might be found in a professional association. ISA was founded in 2000 in collaboration with Carnegie Mellon University.

ISA'S MISSION

The mission of the ISA is to create a sustainable system of cyber security by combining advanced technology with economics and public policy.

ISA THOUGHT LEADERSHIP SUCCESS

Perhaps the clearest evidence of ISA's thought leadership impact is the fact that its core, incentive-based approach to cyber security is central to the policy development of President Obama's Executive Order, "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity," the Administration's "Cyberspace Policy Review," and Congressional Republicans, as evidenced in the House Republican Cyber Security Task Force Report.

JOINING ISA

ISA membership is open to public and privately held entities and currently has substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries. For information regarding membership, please contact ISA President Larry Clinton (lclinton@isalliance.org).

ISA'S GOALS

The ISA has three programmatic goals:

1. To demonstrate thought leadership in advancing the development of a sustainable system of cyber security;
2. To advocate for public policy that will advance the interests of cyber security; and
3. To create increased awareness and programs that will result in more rapid adoption of cyber security standards, practices and technologies.

ISA SPONSORS RATE ISA VALUE PROPOSTION

Each year, ISA members are polled to determine how well ISA is doing in meeting the organization's goals and how they would rate the ISA value proposition for their company. Below are five year averages for these questions (1= not meeting the goal/value; 5= maximum goal/providing value).

ISA meets goal of Providing Though Leadership ..... 4.6 out of 5
ISA meets goal of successful public policy advocacy ..... 4.8 out of 5
ISA meets goal of stimulating awareness & adoption of good security practices ..... 4.2 out of 5
ISA provides value proposition to its members ..... 4.8 out of 5

ISA is supported entirely by member company annual dues. Regular memberships are $25,000. Sponsorships – which include a seat on the Board & premium service – are $70,000. Smaller firms can become Associate members for $5,000.

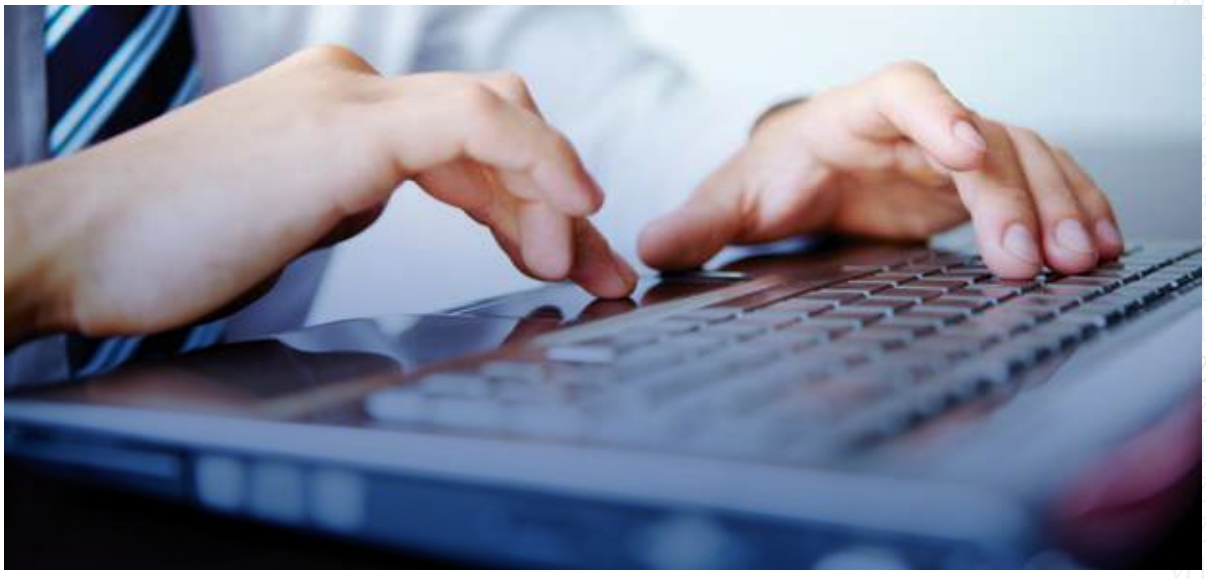
EXECUTIVE SUMMARY

The intellectual property of small and medium-sized businesses (SMB) has never been more at risk from cyber actors known collectively as the "Advanced Persistent Threat" (APT). This threat is intent on gaining and maintaining a long-term presence in a company's network for the purpose of stealing technical and competitive information. The common perception is that this threat has been focused on large companies and governments.

However, as the larger targets have become aware of the threat and taken significant action to mitigate it, the APT has begun to focus increasingly on small and medium sized-businesses, which are far less likely to have sophisticated cyber defenses or the staff to run them. In its recently released "Internet Security Threat Report 2013," Symantec revealed that the "largest growth area for attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them."[1]

From an attacker's perspective, SMBs represent lucrative targets: they often have less extensive defenses, but maintain significant intellectual property of their own or as part of larger companies' supply chain. The result has been a surge in attacks on companies whose only previous contact with the sophisticated threat had been what they had read in the newspapers.

This Internet Security Alliance (ISA) report is intended to begin to fill that knowledge gap by providing small and medium sized-business leaders with practical recommendations to help protect their organizations from APT. It is not intended to be an all-encompassing description of the APT, nor an all-encompassing formula for protection, nor a compilation of standards-based practices. There are many good references already available for that purpose. Rather, it is a quick guide to easy and/or cost-effective measures that might not otherwise end up on the "radar" of small and medium-sized business leaders.



[1] Symantec. "Internet Security Threat Report: 2013." 16 April 2013. Web. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

ISA Board members collaborated on this research to find low cost, but high impact, tactics, techniques and procedures that would not break the budget and would not overwhelm organizations with few cyber security resources at their disposal (both money and personnel). We have classified SMB organizations by the size of their organic Information Technology (IT) staffs and not on based on the organization's revenue or overall employee count. The classifications are as follows:

- Organization with Independent IT Staffing: No organic IT staff
- Small Organization: Less than 10 IT staff
- Medium Organization: More than 10 IT staff

Within this construct, the ISA collaborators targeted specific actions for the leaders of each sized business to consider:

Organization with Independent IT Staffing- Configure Vendor Security Updates for Automatic Installation

- Train Employees to Recognize Social Engineering Attacks
- Upgrade Your Computers to the Latest Operating System
- Remove Administrative Privileges for the Typical Employee
- Ensure Your E-mail Provider Offers Virus/Phishing Scanning

Small-Sized Organization

- Minimize Your Internet Connections
- Employ Whitelisting for Access to Network Assets
- Restrict Web Surfing

Medium-Sized Organization

- Protect Your Intellectual Property When You Are Traveling
- Require 2-Factor Authentication – Restrict Server Access to the Internet for Non-Customer Facing Servers
- Monitor Remote Accesses from Conflicting Geographic Locations
- Hire a Full-Time Security Professional
- Do Not Allow Remote Administration of Your Domain Controller
- Use Microsoft's EMET Technology
- Seek Outside Sources for Situational Awareness
- Use Non-Networked Computers for Certain Sensitive Data
- Invest in Long-Term Retention of Analytical Data
- For U.S. Companies, Install U.S. Department of Homeland Security SAFETY Act-Approved Software

These recommendations are not meant to be cumulative and not exclusive to that particular classification level. If your organization is an unsupported business by our definition, then you should not exclusively consider the recommendations in that category. The ISA recommends you consider all of these recommendations and implement the ones that directly apply where you have the resources to be successful.

- **Organization with Independent IT Staffing: No organic IT staff**
- **Small Organization: Less than 10 IT staff**
- **Medium Organization: More than 10 IT staff**

THE APT: THE "AVERAGE" PERSISTENT THREAT

THE RISE OF THE THREAT AND WHAT ENTERPRISES NEED TO DO ABOUT FIGHTING IT

Calendar year 2010 consisted of 525,600 minutes.

On average, during every one of these minutes:

- 45 new viruses were created,
- 200 new malicious web sites went up,
- 180 personal identities were stolen,
- 5,000 new examples of malware were created, and
- $2 million dollars of corporate revenue were lost.

And, those were the good old days.

In just the last 2 years, cyber attacks have become far more pernicious. During this time, we have seen a dramatic evolution wherein the ultra sophisticated attacks commonly referred to as the Advanced Persistent Threat (APT), which had heretofore been largely confined to nation states and defense establishments, have now become common throughout industry.

The Advanced Persistent Threat now more closely approximates the "Average" Persistent Threat, and the average enterprise is going to have to learn how to protect itself from this new and different form of cyber threat.

The Internet Security Alliance Board is populated by a number of firms that have been dealing with these more sophisticated attacks for a number of years. While not all firms have the range of resources that larger ones do, it is still necessary that they reorient their approach to dealing with these new threats.

This booklet attempts to outline a series of steps for firms without extensive security budgets that they then can initiate to better protect themselves from these modern cyber attacks.

WHO ARE THESE GUYS AND WHAT ARE THEY DOING TO ME?

A traditional model of cyber defense might be designed to prevent hackers from penetrating the network and therefore to stop breaches from occurring.

Virtually every key word in the above sentence is now outdated.

Modern sophisticated attacks are not carried out by "hackers." We are now dealing with professionals.

The sorts of attacks now broadly used throughout the economy are perpetrated by well-organized, well-funded, highly sophisticated attackers.

These attackers commonly use multi-dimensional attack methods in unique combinations based on the surveillance of the particular system that they have decided to attack.

They have at their disposal thousands of custom versions of various malware that are used in tandem with clever social engineering, such as, targeting end-users with spear phishing techniques (a technique called "whaling," wherein they go after the "big fish," i.e., C-Level executives, is often used). People, the real weak link in the cyber defense chain, are often the primary targets, not the networks themselves. This allows attackers to maintain their presence within a system, even if they are initially eradicated via technical means, as they retain access to individuals who they use to reacquire their network targets.

Modern, sophisticated attackers will modify and escalate their attacks as they learn more about the target system. Once they have penetrated their targets, they will typically hide. Unlike an earlier generation of "hackers," who sometimes sought to compromise systems for the bragging rights, these attackers prefer to be stealthy, remaining dormant at times. Indeed, they may turn themselves on and off intermittently to better circumvent defenses and "call home" periodically in order to exfiltrate sensitive corporate data, including intellectual property, business operations information and corporate legal and planning documents.

HOW SUCCESSFUL IS THE "AVERAGE" PERSISTENT THREAT?

Perhaps the single most defining characteristic of the modern attacker is that they will invariably succeed in compromising, or breaching, the systems they target.

The notion of perimeter defense is largely passé. It is only slightly hyperbolic to say that there are only two kinds of companies: those who know

they have been compromised, or breached, and those who don't know yet that they have been compromised.

These sophisticated attacks surfaced and became evident approximately a half-dozen years ago in the defense sector. Initially, the degree of sophistication and the attendant cost in launching these attacks suggested most of them to be state sponsored.

However, as with most technological innovations (including attack methods), the modalities to launch these attacks over time have been disseminated throughout the attack community so that these methods are more generally available to non-state entities, such as, organized crime groups that attack for financial motives, and even some "hacktivist" communities that are interested in using the newer attack methods to pursue a social and/or political agenda.

As the attack methods have become more widely disseminated, a broader community of attack victims has become targets. According to the PricewaterhouseCoopers "Global Information Security Survey: 2012," the so called "APT" has become the major driver of security spending in firms, comprising 45% of the financial services industry spending, 43% for the consumer products industry, 49% for the public utility industry, 49% for the entertainment and media industry and 64% for the industrial and manufacturing sector.[2]

These percentages are sure to continue to rise.

WHAT IS NEEDED TO ADDRESS THESE MODERN ATTACKS?

According to the latest PwC study, companies are countering APT-style attacks largely through signature-based anti-virus protection (51%) and intrusion detection and protection solutions.[3]

Unfortunately, conventional information security defenses don't work against the APT. The attackers successfully evade all signature-based anti-virus solutions, intrusion detection and protection solutions and other best practices, and remain inside their targets even after the target believes that the malware deployed has been successfully removed.[4]

Dealing with an evolved set of cyber attacks will require an evolved notion of cyber defense. The evolved notion of cyber defense needs to begin with an appreciation that cyber security is not just an "IT" issue; it is an enterprise-wide, risk management issue that must be addressed by the operations and technical staff in full accordance with overall business objectives and overseen by an organization-wide risk management team, and not by the CIO or CISO alone.[5]

Senior management must take an active leadership role in understanding and supporting the persistent cyber threat and financing adequate mechanisms to address it. Research has repeatedly shown that the number one problem in enterprises managing their cyber security is not technical, it's economic.[6, 7, 8]

While there are substantial economic liabilities associated with insecure information systems, there are also economic incentives to deploy less secure systems. It can be difficult for enterprises to fully assess the cost-benefits of security, which may be unclear and non-measurable until some future date.

Businesses are regularly tempted to deploy less secure technologies, such as, VoIP and cloud solutions, or adopt business practices, such as, the use of outsourced services or extended supply chains, all of which provide substantial cost and efficiency benefits, but have security liabilities.

[2] PricewaterhouseCoopers. "Global State of Information Security Survey: 2012." Sept. 2011.

[3] PricewaterhouseCoopers. "Global State of Information Security Survey: 2012." Sept. 2011.

[4] Mandiant. "M Trends Report: The Advanced Persistent Threat." 2010.

[5] Internet Security Alliance and the American National Standards Institute. "The Financial Management of Cyber Risk: An Implementation Framework for CFOs." 2010.

[6] PricewaterhouseCoopers. "Global State of Information Security Survey: 2012." Sept. 2011.

[7] McAfee and the Center for International and Strategic Studies. "In the Crossfire: Critical Infrastructure in the Age of Cyber War." 2010

[8] Internet Security Alliance, American National Standards Institute and Santa Fe Group. "The Financial Impact of Breached Protected Health Information; A Business Case for Enhanced PHI Security." March 2012.

Even smaller organizations need to adopt more sophisticated risk management approaches to secure themselves that properly integrate security and business needs and derive cost efficient solutions. In its recently released "Internet Security Threat Report: 2013," Symantec described how targeted attacks against small businesses (that is businesses with between 1 to 250 employees) accounted for 31% of all targeted attacks in 2012, compared with 18% in 2011. This was a threefold increase. As Symantec noted:

> *"While small businesses may assume that they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property, and keep money in the bank. White it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyberdefenses."*[9]

WHAT DOES DEFENSE AGAINST MODERN CYBER ATTACKS MEAN?

Not only do enterprises need to rethink their strategy for cyber defense, the metrics of what constitute cyber defense must also be reassessed. The notion that we are going to keep the attackers completely out of networks may be impractical and even counterproductive if it drains limited resources to an outmoded metric of perimeter defense.

Given the inherently porous nature of cyber systems, it is quite likely that determined attackers will penetrate virtually any system. This does not mean there is no defense. It means there is a need to change the concept of defense from walling off the system to detecting, monitoring and mitigating attacks on the system.

The reality is that enterprises actually have much more control over cyber attackers when attackers are inside their system than when attackers are on the outside selecting access points into it. Moreover, most cyber attacks are not successful when they merely penetrate the system. In most instances, success for the attacker does not occur until they gather valuable information and then exit the system with it. If an enterprise can detect an unwelcome entity within the system, for example, and block its pathway back out, it can successfully mitigate the attack even if the system has been successfully breached.[10]

[9] Symantec. "Internet Security Threat Report: 2013." 16 April 2013. Web. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[10] Brown, Jeffrey. "A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels." Internet Security Alliance. March 2009.

CALIBRATING APT REQUIREMENTS BASED ON THE SIZE OF THE ORGANIZATION'S IT STAFF

This document will attempt to assist organizations in addressing their security needs in two ways: first by identifying the primacy of the needed allocation of resources based on the size of their Information Technology staff.

It must be understood, however, that just as the nature of the attacks will likely continue to change, the degree of intervention and investment required may also change, and, hence, organizations are urged to monitor their IT security needs on a continuing, and enterprise-wide basis.

Over the years, ISA members and other large companies have developed tactics that are not expensive or technically difficult to implement. They are not panaceas and will not make a company as secure as if they had fielded much broader or more expensive advanced capabilities, but they will help at a reasonable cost and level of effort. This document, therefore, offers a series of easy and/or inexpensive measures that small and medium-sized companies can use, not to solve the APT problem, but to make it much more difficult for the APT to succeed.

Not all the recommendations in this document will be appropriate for all organizations. Different defensive measures require different levels of maturity and staff levels. Accordingly, for the purposes of this document, we've divided organizations into categories based on the size of their IT support.

I Organization with Independent IT Staffing

These are companies with no, or minimal, IT staff. Typically, they buy their basic IT services (e-mail, internet connectivity, on-line storage, or business applications) from managed service or cloud providers and might buy their employee computers at a local retailer. This is not intended to say that these companies are unsupported, but rather that they have no organic IT staff that could oversee security functions.

S Small-Sized Organization

These are companies with a small, but full-time, IT staff--typically no more than ten. The staff takes care of desktop support, a few servers, and vendor coordination for other basic services. There is seldom a dedicated IT Security person. More often, one of the technicians that "knows something about security" will be the lead for any security measures. It is likely this individual may have no formal security training or certification. Some companies of this size may vest their physical or facilities security person with the cyber security responsibility. A small company is also unlikely to have any but the most basic security measures such as anti-virus, simply because the buy-in costs for a standards-based security infrastructure have a fixed minimum cost that would be too large a percentage of the IT budget.

M Medium-Sized Organization

A medium-sized organization is one that covers a wide range of enterprises and might have between 11 and 100 IT personnel on the staff. The key distinction between a medium-sized organization and the other two smaller groups is that the medium-sized organization has a critical mass of IT professionals. They are likely to have considerable technical and analytic skill in-house putting them in a position to devote one or more people to IT security. An organization of this size would also be highly likely to maintain much of their own security infrastructure or to work closely with a managed security provider.

EFFECTIVE MEASURES FOR ORGANIZATIONS WITH INDEPENDENT IT STAFFING

CONFIGURE VENDOR SECURITY UPDATES FOR AUTOMATIC INSTALLATION

Rapid patching of security flaws is still the single most effective measure in defending a network from any threat. In fact, it is the most cost-effective security measure when implemented zealously. Automating the process will improve the speed and consistency of the patching process. Most operating systems and common applications today have the capability to reach back to the vendor and automatically receive security and "bug" updates to the software running on the computer. Make use of this service. It will have a positive impact on your security far in excess of any resource expense or inconvenience.

MORE INFORMATION/WEB LINKS

- **Windows Update Information: Windows Update**
  http://windows.microsoft.com/en-us/windows/help/windows-update
- **Linux Update Information: "How to Configure Auto-Updates on Linux Ubuntu Servers"**
  http://www.zartl.info/?p=422
- **Apple Update Information: "OS X: Updating OS X and Mac App Store apps"**
  http://support.apple.com/kb/HT1338

TRAIN EMPLOYEES

Not far behind patching in effectiveness against threats is employee training. The simplest measure any sized company can take to avoid compromise is to train your employees to be wary of unsolicited e-mails and avoid web surfing to risky sites on company computers. It is no coincidence that the majority of compromises today occur during business hours when employees are most active on the internet.

Most attacks rely on a user surfing to a web site, opening a malicious attachment, or clicking on a link in an e-mail (attacks on customer facing web servers being the main exception). APT attacks are especially prone to socially engineered e-mails. Studies involving spam click-through rates vary widely, but the experience of many Internet Security Alliance member companies has validated that about 5% of the targets of attacks will succumb to social engineering techniques (i.e., they will click on anything). Training them to recognize a socially engineered e-mail is the best way to reduce that percentage—even reducing it from 5% to 4% can make a significant difference in your company's risk profile and response costs.

MORE INFORMATION/WEB LINKS

- **"Cyber Security 101 for Small Businesses"**
  http://www.brainshark.com/rsa/cybersecurity101
- **Cybersecurity Best Practices Posters for the Workplace**
  https://www.selinc.com/cybersecurity/posters/

UPGRADE YOUR COMPUTERS TO THE LATEST OPERATING SYSTEM.

On the surface, this sounds like a basic standard practice, but most companies wait years to upgrade just to avoid the disruption or to delay capital expenditures. But whether it's Microsoft, Apple, Linux or Unix, the latest versions of the operating systems and most common applications are usually much more secure than their predecessors. For Windows enterprises especially, Windows 8 and Windows 7 represent a significant improvement in security from previous versions. We recognize that there is a cost to this, but it is well worth the investment.

MORE INFORMATION/WEB LINKS

- **Windows 8 OS Security Features: "What you should know about Windows 8 security features"**
  http://www.techrepublic.com/blog/security/what-you-should-know-about-windows-8-security-features/7900
- **Windows 7 OS Security Features: "10 Windows 7 Security Features You Should Know About"**
  http://www.eweek.com/c/a/Security/10-Windows-7-Security-Features-You-Should-Know-About-694976/
- **Linux Security Distributions**
  http://www.serverwatch.com/server-trends/10-secure-linux-distributions-you-need-know-about.html
- **Apple Product Security**
  https://ssl.apple.com/support/security/

REMOVE ADMINISTRATIVE PRIVILEGES FOR THE TYPICAL EMPLOYEE

Most attacks require malicious code to be remotely installed on a computer, which, in turn, requires the more privileged administrator access to the computer. By ensuring only the lesser privileged "user" accounts are available, you can greatly reduce the ability of attackers to install malicious code. While this will be inconvenient for power users, the cost of additional support for those users will be more than offset by the reduced expenses in incident response.

MORE INFORMATION/WEB LINKS

- **Microsoft OS: "Why you should not run your computer as an administrator"**
  http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows_security_whynot_admin.mspx?mfr=true
- **Linux OS: "HTG Explains: What's the Difference Between Sudo & Su?"**
  http://www.howtogeek.com/111479/htg-explains-whats-the-difference-between-sudo-su/
- **Apple OS: "Enabling and using the 'root' user in Mac OS X"**
  http://support.apple.com/kb/ht1528

ENSURE YOUR E-MAIL PROVIDER OFFERS VIRUS/PHISHING SCANNING

Obtaining e-mail services from domain providers is relatively simple; however, not all such providers offer the same level of filtering and scanning of inbound e-mail. By leveraging providers that do scanning for virus or phishing, you are able to cut the noise of attacks (mostly bad) to your employees. This reduces the white noise that they have to be on the lookout from your user awareness training. The time you spend shopping around for an e-mail service that does a good job scanning will pay for itself quickly.

Different defensive measures require different levels of maturity and staff levels.

EFFECTIVE MEASURES FOR SMALL-SIZED ORGANIZATIONS

MINIMIZE YOUR INTERNET CONNECTIONS

Your company should maintain as few internet connections as possible. More importantly, they should be maintained by a single group. Consistency in the configuration and monitoring of your Internet gateways is a critical prerequisite for stopping or detecting any malicious cyber activity. The more gateways you have, the more difficult it is to configure them properly, even for a single group. If they are operated by independent groups, it is nearly impossible.

EMPLOY WHITELISTING FOR ACCESS TO NETWORKED ASSETS

A common tactic by the APT is to compromise an individual's desktop computer and then remotely log into key servers using the compromised desktop as a jumping off point. Against that tactic you can protect your key assets by only allowing administrative access to them by specifically identified computers. This "White List" method, which can be easily implemented with common firewall access lists, helps to mitigate the risk of unauthorized access from compromised employee computers.

RESTRICT WEB SURFING

Unrestricted web surfing is one of the fastest ways to guarantee your network will be compromised. There are literally hundreds of thousands of malicious sites around the world, many of which are corrupted advertising sites or other sites that appear as links on perfectly legitimate sites. While most of these malicious sites support botnets or financial crime, they nonetheless pose a threat to your network. If your company culture and business model allows it, greatly restricting web surfing on company assets is a huge security plus.

A middle ground for restricting web surfing is to prohibit access to "uncategorized" sites. Many businesses use web proxies to funnel all company web traffic through a set of filters that can block specific web addresses either individually or by categories. In many cases, this is done at the behest of the Organization's General Counsel or HR Department so that access to pornography, gambling, or other sites that could put the company at legal risk is restricted. One category all of these services have in common is called "uncategorized."

It is impossible for a proxy vendor to assign a category to every website in the world. What they haven't categorized yet ends up in a catch-all category called "uncategorized." Most uncategorized sites are perfectly legitimate. However, a fair portion of attacker command and control addresses also fall into this category simply because they are created just for an attack, and are, if nothing else, too new to have been categorized. By blocking access to uncategorized sites, a company can often prevent malware from communicating back to the attacker even after a computer is technically compromised.

This might create an inconvenience for employees who need to access local businesses, which are commonly uncategorized, but with the prevalence today of smart phones and tablets operating on a separate cellular network, rather than the organization's network, this inconvenience is far less than it was just a few years ago.

EFFECTIVE MEASURES FOR MEDIUM-SIZED ORGANIZATIONS

HIRE A FULL-TIME SECURITY PROFESSIONAL

Advising companies to hire full-time security professionals is not a novel recommendation, nor is it focused necessarily on the APT. However, our experience is that it is often difficult for a company to know when it has crossed the size threshold. Many companies end up hiring a security staff in the aftermath of a cyber attack that has come to the attention of the FBI or other law enforcement agency. It is far better to build a security staff before there is a problem.

In general, if your company is big enough to have its own network and IT shop, you need a full-time security professional. This is not a part-time job for a system administrator or your facility security lead. Even if the bulk of your cyber security functions are provided by a managed service provider, you need someone on staff with the training to evaluate the supplier's performance. There is simply too much specialized knowledge required for a facility security lead to understand the threats, mitigation, and risk assessment processes.

PROTECT YOUR INTELLECTUAL PROPERTY WHEN YOU ARE TRAVELING

When traveling abroad, some countries will take the opportunity to search your hard drive and mobile devices. Why make this easy? Take freshly installed laptops with no data on them. Only take the files that are absolutely necessary and encrypt them. Only take burner mobile devices and not the ones you use day-to-day.

Follow all local laws, but do not make it easy for a foreign government to review your intellectual property.

REQUIRE 2-FACTOR AUTHENTICATION

Simple passwords and userIDs are no longer sufficient to protect a business's high risks assets. All system administrators should use 2-factor authentication, which combines the userID/password (something you know) with either a physical token or one-time password system (something you have) or a biometric method like fingerprints (something you are). This ensures a compromised password will not provide access to the most critical resources on your servers.

By the same logic, all remote access should also require 2-factor authentication. A favored tactic of the APT once they get a foothold in your network is to quickly capture as many login IDs and passwords as possible. Once they have those, they simply log in remotely as if they were the legitimate user. Demanding a second factor makes this risk negligible except under the most extraordinary circumstances.

MORE INFORMATION/WEB LINKS

Two Factor Authentication: The Pros and Cons of Two-Factor Authentication
http://blog.softlayer.com/2011/the-pros-and-cons-of-two-factor-authentication/

RESTRICT SERVER ACCESS TO THE INTERNET FOR NON-CUSTOMER FACING SERVERS

Attackers prefer servers over user desktops or laptops. Servers generally contain the most critical data. Perhaps more importantly, they are typically on 24 hours a day, thereby allowing attackers to operate at their own convenience. An easy way to help protect servers is to use simple firewalls to limit a server's access to the internet to predetermined, or white listed, web sites, such as, the software update sites of your applications or operating system. This accomplishes two key goals.

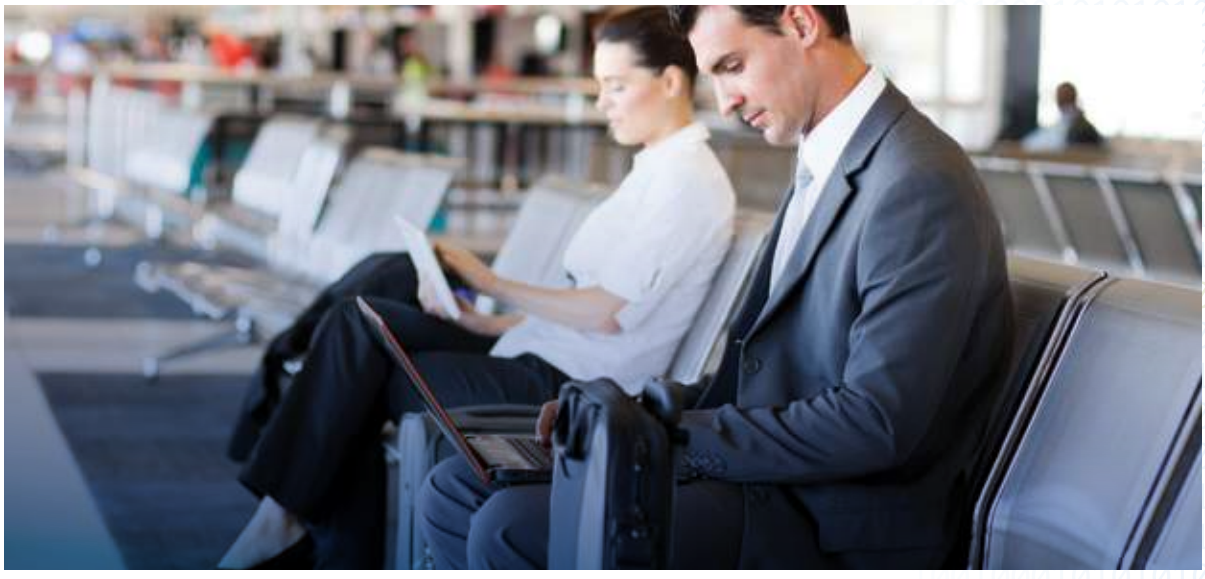
First, it prevents administrators from checking e-mail and surfing the web from the server using their administrative accounts. This eliminates the primary way in which attackers get malware directly onto servers.

Second, if malicious code does get on the server, it ensures the attacker will not be able to communicate directly with the malicious code.

Most covert communications use web sites activated just for that malicious purpose. If the servers can only go to predefined legitimate web sites (such as patching download sites), any traffic destined for other malicious sites will be blocked.

MONITOR REMOTE ACCESSES FROM CONFLICTING GEOGRAPHIC LOCATIONS

If an attacker gains the userID and password of an employee, they will often attempt to log in as the user to access your network rather than using a more exotic covert method. One good way to detect this is to correlate the geographic locations of remote accesses. If an employee logs in from an IP address in one geographic area (for example, New York) and then logs in from another area (for example, Korea) in less time that it would take to travel to the new area, it is a good indication that something is wrong. Such a check can usually be accomplished by running an automated script against remote access logs.



DO NOT ALLOW REMOTE ADMINISTRATION OF YOUR DOMAIN CONTROLLER

The domain controller is one of the most critical servers in any network, large or small. Among other things, it contains the password of every user on your Windows environment. If your company runs its own domain controller, one way to protect it is to only permit the controller to be administered via a direct physical connection. This would prevent an attacker from outside or even from another computer inside the network from accessing the domain controller. This tactic is often easier for smaller enterprises than larger ones. With a smaller user population or geographic spread, the need for an administrator to get into the system from home or another location may be less pressing.

You are not in this alone. There are many organizations that exist solely to provide threat information to the commerical sector.

USE MICROSOFT'S EMET TECHNOLOGY

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) allows administrators to apply security mitigation technologies to arbitrary applications. Modern versions of Windows include technologies such as Data Execution Prevention and Address Space Layout Randomization. These two techniques, combined in EMET, make it very difficult for many malicious attacks to succeed.

EMET is implemented on an application-by-application basis. Not all of EMET's defensive technologies are appropriate for all applications because they may interfere with "creative" programming techniques that legitimate software developers sometimes use. But where it is available, we strongly recommend it for Windows environments, especially for the most commonly exploited applications, such as, Microsoft Office and Adobe products.

SEEK OUTSIDE SOURCES FOR SITUATIONAL AWARENESS

You are not in this alone. There are many organizations that exist solely to provide threat information to the commercial sector. Some are from the government, some are industry associations and some are commercial offerings. Find something that you are comfortable with and increase your situational awareness so that you can better protect your company's business interests.

MORE INFORMATION/WEB LINKS

Situational Awareness: "Intelligence-driven Information Security is Key to Combating APTs…"
http://www.countertack.com/blog/bid/97894/Intelligence-driven-Information-Security-is-Key-to-Combating-APTs-Says-Report

USE NON-NETWORKED COMPUTERS FOR CERTAIN SENSITIVE DATA

Certain electronic assets should be stored, accessed, and manipulated on computers that are not physically connected to the Internet (or even other corporate networks). A small business may wish to commit one or more computers that are not connected to any network. These computers can be used to store, access, and manipulate data assets that are highly sensitive. By not connecting these computers to networks, the only avenue open for malware is through removable media that is used to transfer data between other computers. This greatly reduces the likelihood of malicious attacks.

INVEST IN LONG-TERM RETENTION OF ANALYTICAL DATA

When a compromise occurs, network logs, server logs and netflow data are the primary mechanisms by which an investigator can determine what happened and where on the network the attackers went. This data is essential for the investigation and recovery from an APT, or any other cyber event. Without it, there is little an investigator can do short of physically looking at every device on your network. Network device and server logs will tell you what activity occurred on any given device. Netflow is the metadata about network traffic that includes sending and receiving addresses and times, the protocol used and volume of data. Having this information is often the only way to track the movements of an attacker as they move from device to device across your network. If you can't track their movement, you can never be sure you identified all the compromised devices. It is also the best way to characterize the volume of data that might have been removed from your network.

Unlike most of the measures we recommend here, this one will require investment, but is one of the highest returns on investment a company can make. You should try to retain this data for as long as possible, but six months is a good place to start. APT events are often discovered well after the fact. Having the historical data to see what happened 5 or 6 months previously is invaluable.

FOR U.S. COMPANIES, INSTALL U.S. DEPARTMENT OF HOMELAND SECURITY SAFETY ACT-APPROVED SOFTWARE

Beyond simple encryption, there are several forms of data masking and information obfuscation that are available and are DHS SAFETY Act-approved to ensure the confidentiality and integrity of vital enterprise information. In addition to exploitations from outsiders who do penetrate perimeter security measures, these safeguards prevent loss from accidental or intentional misuse of information, particularly during times of transitions, such as application testing, M&A system integration or cloud adoption.

There are many other best practices and innovations that require additional investment or skills, but the ISA board feels this action item list will go a long way to making most companies better protected against the Advanced Persistent Threat without unsupportable cost or effort. It should be noted that we've focused our attention on the APT, whose tactics are driven by the motivation of a long-term presence in your network. We have not addressed measures against cyber criminals or the hacktivist threat. While much of what we propose here are good ideas for any threat, we've chosen not to include any measures that might be tailored to these other threats.

CONCLUSION

The measures we've recommended here are all in addition to basic network hygiene functions, such as, using anti-virus, patching, firewalls, incident response and policy processes. These basics have been discussed at length in numerous standard documents and cyber security primers. Unfortunately, the APT has proven itself able to bypass these basic defenses. Yet the basic defense measures are a prerequisite to our recommendation. They serve as the foundation upon which to build the more APT specific measure.

It should be noted that we've focused our attention on the APT whose tactics are driven by the motivation of a long term presence in your network. We have not addressed measures against cyber criminals or the hacktivist threat. While much of what we propose here are good ideas for any threat, we've chosen not to include any measures that might be tailored to these other threats.

There are many other best practices and innovations that require additional investment or skills, but the ISA board feels this action item list will go a long way to making most companies better protected against the Advanced Persistent Threat without unsupportable cost or effort.

ISA HISTORY OF THOUGHT LEADERSHIP SUCCESS

For a more than a decade, the ISA has been engaged in thought leadership by creating and operating programs designed to enhance our nation's cyber security. ISA accomplishes this by extensively leveraging the wisdom and experience of the security professionals in its membership.

ISA has regularly initiated programs to advance the state of cyber security well before the subjects become generally recognized in the field. Some examples of these groundbreaking programs are listed below.

HISTORIC EXAMPLES OF ISA THOUGHT LEADERSHIP IN CYBER SECURITY

- 2001, ISA becomes the exclusive provider of threats and vulnerability information to the private sector from CERT/cc at Carnegie Mellon University.
- 2002, ISA published its first set of best practices targeted to senior corporate managers.
- 2002, ISA published its first set of best practices for mobile executives.
- 2003, ISA created its first of 3 sets of best practices to combat insider threats.
- 2004, ISA published its first set of best practices for cyber security for small businesses.
- 2005, ISA chaired the Congressionally appointed Cross Sector Cyber Security Working Group on the use of market incentives, rather than regulation, as a means to improve cyber security.
- 2006, ISA in collaboration with Carnegie Mellon University launched its first effort to secure the IT supply chain. The U.S. Cyber Consequences Unit joined the leadership team in 2007.
- 2007, ISA launched its first effort with ANSI to provide an action guide for enterprises to better understand and correct their financial risk of cyber events.
- 2007, ISA launched its efforts with NIST to take the SCAP automated security system designed for the federal desktop and begin to apply it to unified communication platforms such as VoIP.
- 2008, ISA published the "Social Contract" for Cyber Security, describing how market based economic incentives can be more effective tool for cyber security than government regulation.
- 2009, President Obama releases the "Cyberspace Policy Review", more than a dozen ISA white papers are cited in the report—4x more than any other source.
- 2009, U.S. State Dept. sends ISA President Larry Clinton to brief the NATO Cyber Excellence Center on the Social Contract approach, and from there, to Brussels to do the same with the EU.
- 2010, ISA published the "The Financial Management of Cyber Risk" describing a full enterprise-wide model to assess the economics of cyber events.
- 2010, in a meeting with President Obama, U.S. Commerce Department Secretary Locke cites the ISA security checklist for smart phones as one of the major accomplishments in cyber security that year.
- In 2011, the House Cyber Security Task Force released a report of legislative recommendations—which closely follows ISA recommendations.
- ISA has become one of the clearest voices for enhanced cyber security, having been featured in C-SPAN, USA Today, National Public Radio's (NPR's) "Morning Edition," The "News Hour" on PBS, CBS "Early Show," Fox Business News, MSNBC "Squawk Box" and "Power Lunch," CNN & CNN International, Federal News Radio and in many publications.

ACKNOWLEDGEMENTS

The following professionals comprise the Internet Security Alliance's (ISA's) Board of Directors, without which, the work of ISA would not be possible. We would also like to personally thank Jeff Brown of Raytheon, Tom Kelly of Boeing and Rick Howard of VERISIGN, who co-chaired and led this project, as well as Brian Raymond of the National Association of Manufacturers, who fielded the APT focus groups. Their contributions were essential to this project's success.

INTERNET SECURITY ALLIANCE BOARD OF DIRECTORS