ADVANCED THREAT PREVENTION

Understanding and defending against zeroday threats, propagating worms, low-and-slow attacks, and more targeted advanced persistent threats (APTs).





Executive Summary

IT organizations have never been as well equipped to deal with sophisticated security threats as they are today. But at the same time, IT organizations have never been at greater risk.

CISOs typically command a substantial set of resources to fight cyberthreats, including well-defined policies, procedures and controls; mature and innovative security technologies; and risk-based implementation approaches. All of these tools help align information security with the needs of the business while protecting mission-critical operations and sensitive information.

Nonetheless, cyber adversaries are in a position of strength. They have substantial funding, human resources, and patience. With their resources, they have overmatched traditional security technologies and routinely create zero-day exploits and conduct low-and-slow or targeted attacks that defy most detection mechanisms. They pick their targets and take advantage of not only ignored exposures but also human trust. They are adept at gathering intelligence, proficient in their approach, and technically skilled at infiltration. Some cyber adversaries have the resources of hacker communities, nations, or powerful criminal enterprises behind them. It is no longer a matter of "if", but "when" your enterprise will face a modern attack.

In this white paper, we will examine the nature of sophisticated threats and the state of defenses against them including:

- » The current threat landscape, particularly in regards to zero-day exploits, blended attacks and more targeted attacks called advanced persistent threats (APT).
- » The nature of zero-day, low-and-slow and targeted attacks and how they are used by attackers to threaten operations, as well as gain entry to networks and obtain the most sensitive data, including government secrets, defense project plans, source code, business plans, intellectual property and personal identifiable information (PII).
- » A brief assessment of various security technologies and their relative strengths and limitations in the face of more sophisticated attacks, and what can be done to improve an organization's security posture.
- » An overview of how ForeScout ActiveResponse™ technology can contribute to a sophisticated defense. A real-world case study illustrates the reasoning, selection and implementation of ForeScout ActiveResponse to address these and other contemporary threats.

Today's Threat Landscape

Despite advancements in security policies, processes, techniques and controls, organizations are are increasingly vulnerable to today's zero-day exploits, low-and-slow attacks, and targeted attacks. Enterprises face a combination of new threats, sophisticated attacks, social engineering, botnet legions, and ingenious self-propagating malware which are hard to detect and more difficult to stop.

The advantage appears to be with attackers who are coordinated and have a wealth of resources to draw from, including hacking communities, organized crime, and nation states. If one of these bad actors decides to target an organization, they hold most of the cards. They can pick not only the victim organization, but use various assessment and penetration methods to take their victim down.

Empirical data shows that the zero-day attack is the most popular and successful tool for the cybercriminal. For example, propagating worms like Conficker have wreaked havoc in networks around the world. Trojans like Zeus have defrauded businesses of millions of dollars. But other surmise that zero-day attacks are just the tip of the iceberg.

Notorious, Sophisticated and Targeted Attacks

Self-propagating malware. From the early days of email worms, this type of threat has reached new levels of sophistication and effectiveness, thwarting traditional antivirus and other anti-malware technologies. Worms and bots currently use a variety of network and other vectors to infect machines without human intervention. Once a large number of machines have been infected, the cyber criminal may take control of the infected machines and form a botnet, which can be used for further malicious activities such as spam distribution, distributed denial-of-service (DDoS) attack, data theft, and fraud.

Early worms such as Nimda, Code Red and Slammer caused massive global disruption. More recently, Conficker, which infected millions of computers in some 200 countries, used a wide variety of advanced techniques to make it difficult to stop and eliminate from networks.

Worms can be used to create botnets, and worm-like techniques employed in targeted attacks under human control to penetrate deeper into the victim network.

Zero-day vulnerabilities. Exploits leveraging zero-day vulnerabilities are regularly going "in the wild", particularly employing customized, stealthy attacks that circumvent traditional security technologies. While attackers can and often do exploit known vulnerabilities that remain unpatched, zero-day exploits minimize the likelihood of detection and maximizes the chances of success.

The so-called Aurora attacks, for example, exploited a zero-day vulnerability in Internet Explorer. A Zeus banking Trojan botnet, which has been responsible for the theft of many millions of dollars from business accounts, leveraged a zero-day exploit of an Adobe PDF flaw. The RSA SecurID attack exploited a zero-day vulnerability in the ubiquitous Adobe Flash plug-in. Stuxnet, which was used to disrupt the centrifuges at Iran's Natanz uranium enrichment plant, used no less than four zero-day exploits. Unfortunately, attackers are able to derive numerous variations of these zero-day mechanisms faster than the anti-malware industry can build, test and distribute signatures to thwart them.

Low-and-slow attacks. In the 1990s, there were numerous "loud and proud" attacks leveraging common scripts to publicly disrupt or defame popular websites, services and companies. But today, many attackers prefer to remain unnoticed. To accomplish this requires the means to fly below the radar of security defenses and conduct malicious activity over longer periods of time – without immediate detection. Attackers are using this method to

remain undetected to achieve bigger net results well before the security breach can be identified or remediated.

A well-publicized example is that of the TJX breach. Albert Gonzalez orchestrated low-and-slow attacks in which the TJX network was penetrated with common exploits and malware. This allowed Gonzalez to breach systems and extract sensitive data, including personal identifiable information (PII) and financial transaction records slowly, over a year. Gonzalez also successfully breached Heartland Payment Systems, Hannaford Brothers, BJ's Wholesale Club and a number of other companies.

Even modern-day botnets constructs employed by "black hats" attempt to ascertain the detection watermarks of common security tools employed by their targets.

Advanced Persistent Threats (APTs). APTs are top of mind, as security events and revelations since early 2010, in particular, show incontrovertibly that government, commercial and political entities are falling prey to APTs. These targeted attacks are being executed by extremely tenacious and highly educated attackers who can draw on the vast resources of nation states and other entities with more than ample means to support them.

At risk is highly sensitive information such as government secrets; military, diplomatic and political intelligence; details on new defense systems; business plans; financial and personal records; business projections, product development plans, and even source code.

There have been countless attacks of this type over the years. The CISO for defense contractor Northrop Grumman said recently that his company has been the target of these types of attacks for years. But, APTs hasve become top of mind in many organizations in light of recent spectacular, very public incidents, starting with the Aurora attacks in early 2010. Other high profile, targeted attacks, such as the theft of SecurID information from security giant RSA and the huge Sony breach, have reinforced the urgent concern over APTs.

There is more evidence to suggest that APTs may be growing more prevalent. In its 2011 Data Breach Investigations Report, Verizon Business says its latest data suggests an increased need for vigilance against APTs and greater incidence of theft of classified information, intellectual property and other highly sensitive organizational data.

In August 2011, McAfee uncovered a series of successful ATP-style attacks, dubbed "Operation Shady RAT," against 72 organizations, mostly in the U.S. McAfee says this is only one of hundreds or perhaps thousands of such servers belonging to these perpetrators.

The ramifications can be enormous. RSA has reportedly spent \$66 million in response to the SecurID theft. Subsequent attacks against defense contractors Lockheed Martin and L-3 were linked to the compromised RSA tokens and were certainly very costly to those firms. The attack against Sony shut down its PlayStation Network, with its tens of millions of account holders, for more than a week and exposed credit card information of about 10 million subscribers.

In summary, when it comes to modern day attacks - what has evolved is the sophistication of the approach and attack tools, the wealth of information-gathering resources at the attackers' disposal, and the growth of attacker communities that coordinate attacks and expedite knowledge transfer. Let's explore advanced threats in more depth.

Advanced Threats and Attacks Exposed

Zero-Day Attacks and Propagating Malware

By definition, there are no patches for zero-day vulnerabilities and no signatures to detect zero-day attacks. So, many attackers are going to use them selectively in attacks aimed at returning big dividends. Given that there is often a considerable delay between the attack and methods to identify the new attack, neither the attacks nor the resulting exploits can be addressed in a timely manner using conventional security methods.

The increasing prevalence of zero-day attacks signifies an increased number of skilled cybercriminals who have the deep expertise and resources to reveal previously unknown vulnerabilities, typically in popular operating systems and applications such as Microsoft Windows, Internet Explorer and Adobe Flash. These entities may be supported by nation states, as strongly indicated in Stuxnet and Aurora, or well-financed criminal enterprises and hacking communities that distribute and sell zero-day kits.

The Aurora attacks used spear-phishing messages to introduce malware that exploited a heretofore-unknown vulnerability in Internet Explorer version 6,7 and 8 on most Windows client and server operating systems. The memory-corruption flaw allowed the hacker to inject a Trojan onto the target computer to steal data and transmit it back via an encrypted channel.

The Stuxnet attack was remarkable in a number of ways, not the least of which was the use of four zero-day exploits. The attack embedded malware via USB drives that were introduced into segregated control networks for Iran's uranium enrichment program, likely using some social engineering ploys. A zero-day Windows shortcut exploit allowed Stuxnet to install from a USB drive without any user action other than inserting the drive into a computer.

Stuxnet used three additional zero-day exploits, including two privilege escalation exploits, and a print spooler exploit used to propagate as a worm through the control systems, and, according to reports, achieved at least some success in destabilizing Iranian centrifuges.

While Stuxnet was a startling example of propagating worm technology as a zero-day threat, it shared common characteristics of all self-propagating malware in that it depended on particular vulnerabilities. It exploited several known vulnerabilities, as well as the four zero-day flaws, to spread to additional devices across a network. It launched port scans to gather information about a target, such as operating system or application version, to determine if the target was vulnerable.

Contemporary malware may carry and deliver multiple payloads for different purposes, depending on the target system, network or goal of the attack. It can use obfuscation techniques, such as packing and encryption, to evade detection by signature-based security software and/or change their behavior on the network to evade anomaly-based or heuristic detection.

Worms are frequently used to create botnets, which can be employed for a wide range of malicious purposes and changed/updated through their command and control channels.

The Conficker worm and its variants was a highly successful and disruptive example of a modern worm. Conficker, which infected millions of systems around the world, was not, strictly speaking, a zero-day exploit. It was a glaring example of the damage that can be done if security patches are not applied as quickly as possible. Although Microsoft issued a patch for this vulnerability in Windows' Server Service in October 2008, Conficker was launched with great success about a month later.

Conficker was propagated as a Windows dynamic link library (DLL) as part of the scvhost.exe service and used a second layer of packing for obfuscation. It dynamically generated lists of potential target domains. If Conficker's scans found a vulnerable target, it opened up a backdoor port to propagate to the new victim machine. It checked to see if a computer was connected to the Internet; if not, it rechecked every 60 seconds. The creators of Conficker updated the worm four times, resulting in version A through E. Each new version of Conficker included a new exploit or propagation technique.

Low-and-Slow Attacks

Low-and-slow attacks use the process of conducting analysis and target acquisition, network surveillance, system breach, data extraction and attacks at such a low or intermittent rate as to be undetected by common security provisions.

Low-and-slow attacks can utilize common attack kits and brute force penetration methods, but the difference is that these attacks occur over long periods of time to evade detection. Low-and-slow attacks are typically not detected by log management or intrusion prevention systems as they fly below the incident threshold settings.

The prevalence of low-and-slow attacks is difficult to determine; there is a paucity of data. In some cases, a conventional high-volume attack is used in conjunction with a low-and-slow attack to distract and consume the resources of security operations in order to ensure the success of the low-and-slow attack.

To detect and thwart low-and-slow attacks, IT security managers can use specialty products that are specifically designed for low-and-slow attacks, or they can try tuning conventional security products by lowering their alarm thresholds. In most cases, traditional products can't be tuned by the customer, or the result of such tuning results in a large administrative penalty with many more log files and false positives to sort through. In these cases, tuning efforts and responding to false positives can outweigh the benefits.

Advanced Persistent Threats (APTs)

The blended use of spear-phishing, zero-day exploits, advanced malware obfuscation and the ability to evade detection and continue operating without arousing suspicion are what many information security professionals now call Advanced Persistent Threats or APTs.

The techniques are not unlike those used in successful, targeted attacks aimed at stealing huge amounts of customer information, such as the recent stunning theft of millions of records from SONY. The lesson is that enterprises must assume that they can become a target, whether the attacker's goal is to harm reputation or to obtain intellectual property, credit cards or personally identifiable data.

In some ways, APTs are the epitome of "low-and-slow" attacks as they too are designed to fly under the radar to infiltrate networks. The attacks can be extremely difficult to detect and challenging to remediate before considerable, even irreparable damage has been done. They are designed to evade traditional security tools such as antivirus and intrusion prevention systems. Unfortunately, evidence confirms that they are almost always successful.

APT is a very people-intensive endeavor, from both the attacker and victim perspective. While automated tools may and often do play a part in an attack scenario, the attackers exercise hands-on, personal control over each

stage of the intrusion. Many APT attacks begin with spear-phishing techniques that trick a key employee into giving up authentication credentials. This provides a foothold in the network.

APT Attack Stages

Stage One: Spear-phishing

Social engineering has always been part of the attacker arsenal, but it has become increasingly more sophisticated and effective. Intruders start with intelligence-gathering, gleaning information (business and personal) on key personnel, company structure and even initiatives from corporate websites, online forums, blogs, search engines and, increasingly, social media such as Facebook, Twitter and LinkedIn. Managers and employees comfortably and all-too-openly use these media to share and discuss corporate information with colleagues, partners and clients.

The well-crafted spear-phishing source will appear to be a legitimate communication from, for example, HR or IT. It will appear to be a message or phone call from within the company, about company business. Compared to the laughably crude phishing messages of a few years ago, these messages are entirely credible. The spear-phishing message can include a very legitimate-looking file (a Word or Excel document containing a contact list, for example, or even an image file) that carries an exploit, or perhaps a link to a malicious or compromised website that will download the malware. And the request or "call to action" appears reasonable and legitimate.

The intrusion at RSA, for example, started with a two-day spear-phishing campaign targeting two small groups of relatively low-level employees, using an Excel file entitled "2011 Recruitment Plan.xls" with malware that exploited an Adobe Flash zero-day vulnerability. In the Google attack, employees were directed to a malicious website which downloaded malware to exploit a zero-day Internet Explorer vulnerability. Targeting highly placed employees with a spear-phishing attack is likely to yield quicker results, but it requires more information and attention to detail. A more polished presentation is used to dupe the victim, who is more likely to suspect the validity of the message. On the other hand, sales representatives are not likely to regard themselves as likely targets, and they are likely to trust the source.

It's instructive to note that the same people who have learned to be wary of emails that purport to come from their bank will implicitly trust anything that appears to be of internal origin. Banks tell their customers they will never receive an email asking for your password, but organizations rarely have such policies with internal employees. The vast majority of employees would not question an email from an internal IT manager that asks the employee to "click here" to install new software or divulge a password.

APT Attack Stages

Stage Two: Command and Control

The second stage of the APT attack is the actual exploit which triggers when the victim opens an attachment or clicks a link. Typically, a Trojan is installed on the victim's computer. The Trojan establishes a backdoor channel to the command-and-control Web server. The Trojan often exploits a zero-day flaw to avoid detection, but it can also exploit a known flaw if the target system is not patched. In any case, the aim is to avoid detection by traditional security tools such as signature-based antivirus and IPS. To evade detection, targeted attacks often utilize customized malware which has never before been seen by the large security vendors (Symantec, McAfee, etc.). Verizon reports that three-fifths of the malware it encountered in its investigations were either custom-built or the code was modified to be unrecognizable by traditional antivirus programs.

The connection to the command-and-control server (often hijacked servers; the Google attack reportedly utilized a server owned by hosting provider Rackspace) creates a remote shell that allows the attacker to transparently issue commands to the victim's computer. This gives the attacker complete freedom to upload and download files, check the status of its operations against the network, download additional malware for more functionality, or "go quiet" until the victim's computer is needed. The attacker may even change the malware and tools used in reaction to the victim organization's security activity.

The ability to move and change malware and attack attributes, "polymorphing," is critical to avoiding detection, as the means to mutate and relocate makes the attack not only hard to identify but hard to remove. The Verizon report notes that in addition to evading detection for months, almost two-thirds of the attacks required weeks or even months to contain once they were discovered.

The attack on Google, for example, used a number of different pieces of malware and several layers of encryption to hide its activity.

Stage Three: Privilege Escalation and Expansion

The attacker will gather credentials for the target system, then use the system to run tools such as network sniffers to gather information about other systems on the network. The target system is thus a launch point for attacks on additional systems. The attacker's goal is to gain a deeper penetration into the organization, with the eventual goal of gaining strong privileges on key systems. Once that has been achieved, corporate data is readily available for extraction.

In addition to polymorphism techniques to avoid detection, attackers maintain persistence on the network in a variety of ways. For example, attackers may leave tools or malware that have served their purpose or may be merely decoys to deflect attention from the important components, which they can activate at a time of their choosing.

APT Attack Stages

Stage 4: Data Exfiltration

The attacker locates, gathers and passes the data to a remote server – often a compromised server that is used as a way station for storage and obfuscation. Because the attacker is able to maintain persistence, the attack process may remain inactive for a time or take advantage of additional opportunities, such as additional data sources, new or updated documents, databases or source code, or new intelligence the attacker has gathered about the organization and/or its people.

Leveraging Security Technologies

No single tool or class of tools is significantly effective against zero-day attacks, propagating worms, low-and-slow attacks and APTs. The individuals or groups involved in these types of attacks have time, technology and resources on their side. They have malware and subterfuges for evading detection. They are skilled (they are not script kiddies) and they are tenacious.

Technology has its limits in the face of today's sophisticated threats, but different classes of security countermeasures, when combined, offer the means to preempt, identify and reduce the impact. Newer technologies hold some promise to effectively address zero-day exploits, sophisticated self-propagating malware and targeted attacks such as low-and-slow and APTs. Let's briefly examine common defenses employed by network and security operations.

Firewall

Traditional stateful network firewalls are quite limited in their ability to thwart attacks. All manner of applications flow freely through Port 80, and many applications use protocols that actively search for other open ports. Moreover, firewall rule sets become extremely hard to manage over time in complex environments, with out-of-date, misconfigured and even contradictory rules between network tiers. "Next generation" firewalls are better in that they are able to exercise application-layer control to support web application security, acceptable use policy, and malware detection through built-in IPS technologies. (See the subsequent discussion of network intrusion prevention capabilities and limitations.)

Antivirus

Antivirus / antimalware is primarily signature-based and thus largely ineffective against zero-day exploits and the obfuscation techniques used by contemporary malware authors. While they are a necessary defense to capture a large percentage of malware, they are also simply overwhelmed by the crushing number of new malware types and variants that appear daily. Vendors have turned to techniques such as file and source reputation, but these are still techniques designed to try to keep pace with the bad guys. In fact, leading AV vendors are placing heavy emphasis on correlating and analyzing data from their population of deployed security tools to gather intrusion intelligence on the assumption that their customers have been successfully attacked.

White-listing

Complementary to AV, leading white-listing products are no longer simple static tools, but can respond and be adjusted dynamically to respond to changing conditions. These are still most effective in limited settings, such as ATMs and kiosk computers, which can effectively be locked down, or highly restrictive environments where enforcement of locked system images is mandatory. White-listing (or black-listing) can be resource intensive outside of strictly controlled and less dynamic environments – but they do offer another layered defense mechanism.

Email Security

Email security products and hosted services are quite effective against spam and routine AV checks. Email filtering uses a broad set of assessment techniques including the use of reputation lists to identify, flag and remove spam and emails containing malicious payloads. They often block obvious phishing messages, such as a poorly worded request from a foreign bank or messages containing illicit or pornographic content. But they are often typically ineffective against more advanced phishing and of no help against spear-phishing and targeted attacks. Once a disreputable source is identified, email security products and services can be updated to filter out a good amount of malicious activity.

Web Security Gateways

Web security gateways are an extremely beneficial layer of security against unwanted Internet use and preventing access to known malicious sites and web malware. They apply reputational and behavioral analysis to Web transactions and employ AV and anti-spyware either at the perimeter or in the cloud. They have narrow means to protect against more advanced attack techniques and targeted attacks. Here too, they can be employed to support layered defenses.

Data Loss Prevention

Data loss prevention (DLP) solutions are most effective at spotting common patterns of the use of specific data, such as credit card and Social Security numbers, customer and partner information, and patient health record IDs. They can be configured to identify specific information that would be deemed inappropriate for general distribution. DLP solutions can be difficult to manage and tune when dealing with more complex data, especially using keywords, phrases and contextual algorithms to spot intellectual property, sensitive business intelligence, etc. DLP, in conjunction with email filtering as part of a layered defense model, can be employed to identify ATP exfiltration of standard data – albeit less effective against non-standard data, such as designs, source code, formulas, business plans, etc.

SIEM

Invaluable tools for centrally correlating and analyzing log data from a wide range of security and network devices, and applications, SIEM can be a powerful, even essential weapon in the detection of APTs, but not in real time.

SIEMs are vital as an investigation and reporting tool, but the systems do not offer response other than alerting and are often too late to mitigate APTs. They are best for forensics and to create reporting and alerting rules to identify subsequent attacks. Advanced algorithms for sophisticated rule creation / query capabilities can enable security personnel to identify and investigate more advanced threats and fraud. This level of SIEM use usually requires considerable expertise and material investment of dedicated, experienced staff.

Deep Packet Inspection and Analysis

Information security specialists are adopting a variety of network traffic inspection products, once used for network performance troubleshooting, for attack forensics. The deep packet inspection (DPI) solutions are also becoming more security focused. DPI solutions perform packet inspection as a means to analyze all activity on the network, in some cases logging every packet. They can help detect and analyze malware and suspicious network activity. This too requires considerable expertise and investment of dedicated staff in order to conduct forensics that can identify threat patterns used to identify future attacks. Given the "polymorphic" nature of APTs and advanced threats, DPI is not an immediate advanced threat countermeasure, but can be an integral part of security analysis processes.

Network Intrusion Prevention

Network intrusion prevention systems (IPS) are effective shields against many forms of known attacks, such as DDOS attacks and other known exploits. However, most IPS systems are primarily based on signatures, and therefore they are useless against zero-day attacks. Furthermore, most IPS systems are designed with traffic intensity thresholds, which makes them miss the low-and-slow attacks.

Most IPS systems are quite prone to false positives, in which legitimate business traffic is mistaken for an attack. This fault wastes valuable IT management time, as the devices need to be tuned and logs need to be constantly analyzed. Many organizations never put their IPS systems into blocking mode out of fear that legitimate business traffic will be blocked; the devices simply serve as after-the-fact logs of the malicious activity that occurred on your network. IPS systems also require extensive maintenance time to update signatures, etc.

In an attempt to detect zero-day attacks, many IPS devices incorporate network behavioral analysis in addition to signatures. Network behavioral analysis identifies anomalous network activity and has some ability to identify zero-day attacks, especially if they are high-volume attacks. This technique analyzes network flow data for anomalies and can be valuable for identifying suspicious activity and network performance issues - but less so for dealing with threats in real time. However, anomaly-based analysis is also prone to false positives that it is not often used in blocking mode (see NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems" for additional IPS details).

Network Access Control

Network Access Control (NAC) is an effective tool to enforce network access policy and automate endpoint security before network access is granted. NAC assesses the type of device, who owns the device, and whether the device is "healthy" in terms of security controls, configuration, patches and approved software. Then, NAC grants the device an appropriate level of network access. Network access policies can be quite granular and can provide different levels of access by type of user (e.g. employees, contractors, guests), role (sales, finance, manufacturing, HR), location, and time. Advanced NAC products can also continuously monitor the behavior of devices after they have joined the network, which is known as post-connection monitoring.

NAC with post-connection monitoring capabilities can play an important role in detection of worms, low-and-slow attacks and ATP activity. First, post-connection monitoring can detect if an endpoint has fallen out of compliance after it has been admitted to the network, either by the user (for example, downloaded and is using a P2P application while on the corporate network) or by a malicious party. ForeScout CounterACT, as expanded later in this paper, provides detailed visibility into all user and device activity on the network; including suspicious actions such as network sniffing, unusual port use, and attempts to access unauthorized assets that may be characteristic of malicious activity by a compromised endpoint.

ForeScout Advanced Threat Prevention

Rather than chase the latest threats and develop new signatures to address them, ForeScout Technologies offers an effective threat prevention technology, called ForeScout ActiveResponse™. ActiveResponse does not rely on signatures to detect zero-day threats. Strictly speaking, ForeScout ActiveResponse analyzes network behavior, but it is quite unlike other behavior-based approaches in that it does not produce false positives, nor does it require any tuning period or maintenance. The technology is patented, and it is incorporated within ForeScout CounterACT Edge and CounterACT solutions.

ForeScout CounterACT Edge provides a perimeter-based defense against worms, zero-day, low-and–slow, and targeted attacks. ForeScout CounterACT for Network Access Control provides protection against these threats from within the network. For example, if a laptop computer has become infected with a worm or Trojan while on the road, then the laptop connects to the corporate network, ForeScout CounterACT for Network Access Control will prevent this computer from spreading the infection to other computers on the network.

In the section below, we will describe ForeScout's overall approach to tackling the challenge of zero day attacks, low-and-slow attacks, propagating malware and advanced persistent threats.

ForeScout Integrated Defenses

Authentication. Only authorized users should be allowed to access sensitive network resources. ForeScout CounterACT for Network Access Control automatically enforces this policy in a non-intrusive manner. If desired, it can also apply role-based controls to limit users to just the resources they need to do their jobs. It can also enforce access policies based on time, location, device and device configuration attributes. CounterACT includes an integrated guest registration application which allows contractors and guests to access the network for Internet usage, while ensuring that their computers can't introduce malware or conduct unwanted activity on the network.

Endpoint Compliance. Endpoints on your network should comply with your internal security policies. ForeScout CounterACT for Endpoint Compliance allows administrators to define and enforce endpoint security policy. Compliance can include many factors such as:

- » Operating system patch level
- » Application patch level
- » Required applications (whitelist) or disallowed applications (blacklist)
- » Security agents such as antivirus, patch management, encryption, DLP

Many organizations that deploy ForeScout CounterACT for Endpoint Compliance immediately find 20% to 30% of their endpoints are not compliant. This revelation is a result of the fact that they had been relying on agent-based systems to report system health, but these agent-based systems have blind spots. ForeScout uses a patented, agent-less technology to inspect all computers on the network. No software to deploy, and no blind spots.

CounterACT supports both white-list and black-list endpoint compliance. White-list is comprise d of applications that must be installed and/or running on all endpoints, where as black-list are applications, such as peer-to-peer and or certain instant messaging, that are not allowed to be used. Keeping the network "clean" or in compliance is an important step in making sure advanced threats including APTs either cannot find their way into the network at all, or at least take much longer to find a security breach to exploit - therefore are more likely to be detected before the network is compromised.

Auto-remediation. Maintaining endpoint security and patching known vulnerabilities are critical security processes. Unfortunately, the security systems that are typically deployed onto endpoints (antivirus, patch management, etc.) can't be completely trusted to self-remediate because these systems are often the first target for malware which disables them. These products are often less accurate to dynamically identify and remedy disabled security agents or out-of-date software. A third-party product further assures complete endpoint security and optimizes endpoint protection product investment. ForeScout CounterACT for Endpoint Compliance provides automated identification and remediation of endpoint security issues, and is able to fix a broad array of endpoint compliance issues with little or no human intervention.

ForeScout ActiveResponse™

ForeScout's patented ActiveResponse™ technology has proven extremely effective in blocking human attackers, zero-day attacks, low-and-low and targeted attacks, as well as self-propagating malware. ActiveResponse remains unsusceptible to the majority of new attack technologies because both human attackers and self-propagating threats must perform some reconnaissance in the first stage of an intrusion, i.e. scanning the network for configuration information and vulnerabilities, and then utilizing the information to perform subsequent malicious activity.

ActiveResponse intelligently detects malicious behavior and reconnaissance attempts by an attacker. Reconnaissance might be a standard port scan or a ping-sweep scan, and can also be brute-force login attempts, attempts to collect data via SNMP, NetBIOS and other protocols, etc. – regardless of the interval of the attack.

ActiveResponse is capable of detecting reconnaissance attempts at network layers 2-4 as well as the application layer. What makes ActiveResponse so advanced is that it sends fake replies to the attacker, called marks. Those marks could be a non-existing service, such as fake HTTP server, or higher entities such as fake usernames fake shares, etc. When an attacker tries to use a mark, the attacker's malicious intent is confirmed and he is blocked from the network.

The limitation in blocking based on reconnaissance alone is that many tools do scan the network for legitimate reasons. The mark, a patented process, sets ActiveResponse apart from other systems that simply block all reconnaissance activity. If a system or person uses a fake resource, such as the use of a username that does not exist in the organization, it definitively indicates malicious intent.

ForeScout ActiveResponse is not a honeypot. The ActiveResponse goal is not to 'play' with the attacker in order to learn the nature of the attack, but to continue replying until malicious intent is proven and then block the attacker. Honeypots by nature require setting up and maintaining an environment that can be used to analyze attack patterns and objectives. As such, it is materially more labor intensive and requires significant operator expertise. In contrast, ActiveResponse technology, within the CounterACT platform, is easily configured, requiring almost no administration and nominal expertise – they are "set and forget".

Unlike honey pot technology, ActiveResponse generates the virtual responses within the same IP range of the real network, either as a virtual host or a virtual port on a real host. This makes it much harder to differentiate fake responses from the real network. To make the distinction between real and fake resources, ForeScout's CounterACT also learns the real banners used by the real servers (e.g. the exact banner of the IIS server) and generates similar banners in its replies.

Another method employed by ActiveResponse is utilizing the TCP window size. Some of the replies are sent with TCP window size of 0, causing the client-side (the attacker) to send an ACK once a minute in an attempt to open the window for sending data. This method had proved to effectively slowdown malware propagation. Each such reply keeps one attacker's thread constantly occupied and therefore prevents it from continuing to scan the network. Most attacks scan the network from multiple threads in parallel and sooner or later all threads are hit by a virtual resource that replies with TCP window size 0, and the attack is neutralized. This method chokes the worm and eliminates both the malware propagation, as well as the massive traffic generation that could potentially slow the network or even cause an outage. Using this unique detection method, ActiveResponse is effective against "low and slow" attacks either from automated or human sources.

Whether an attacker is physically connected to the network or through a compromised endpoint, attackers are much less likely to successfully complete an attack before being detected and blocked by ForeScout ActiveResponse. ActiveResponse technology is so effective that ForeScout's customers report that when a penetration test team is hired to conduct a vulnerability check against their network, a preliminary condition is to turn off ActiveResponse because otherwise they would not be able to conduct an effective assessment.

ForeScout ActiveResponse™ technology is integrated into ForeScout CounterACT Edge, which blocks intrusions at the perimeter of your network, and ForeScout CounterACT for Network Access Control, which protects your internal network from attack.

CASE STUDY: A Blended Approach to Threat Prevention

A global commercial enterprise with sites in the North America, Europe and Asia recognized it needed stronger network protection to protect their customers' sensitive financial transaction data and personal identifiable information. The organization had mature policies and processes, and all of the common security tools, but the security team determined that they wanted a more automated and advanced approach to address sophisticated, targeted threats.

"It is in the nature of our business to collect sensitive data and personal information about our customers," said the company's information security director. "As such, the highest level of information security is critical and the core of our business practice. Our charge was to figure out how to add significant protection to secure customer data, while at the same time recognizing that we, like other companies, have limited operational resources."

Layered perimeter and intranet protection was deemed essential to combat sophisticated threats. In addition, the IT organization wanted to improve endpoint security.

"The threats we are seeing today comprise both new, zero-day threats as well as low-and-slow attacks; both of which are a lot more difficult and dangerous," said the director, "because either we would normally not be able to defend against perimeter attacks without IPS signatures or the attacks would normally not be identified until too late – and we would have less timely recourse to fix what is compromised."

The company focused on selecting a threat prevention system that would reliably block advanced attacks without disrupting operations or requiring excessive management overhead.

The company selected ForeScout CounterACT
Edge, preferring its signature-less ActiveResponse™
technology to traditional IPS. The director was very

familiar with traditional IPS, having managed three different IPS systems himself over the years. He knew that traditional IPS systems require regular updates, produce false positives, and require tuning. He was impressed by how ForeScout ActiveResponse™ technology keys on the reconnaissance scanning used by all attackers, human and automated. And as a result, CounterACT Edge could detect and block a majority of attacks, zero-day or not, targeted or not.

"We honed in on products that demonstrated a more definite approach to stop intrusions and worms with less administrative effort to maintain and without sacrificing quality," the director added. "ForeScout is more set and forget – once configured, it does not require real tuning or signatures, unlike traditional IPS. There have been no false positives, which can lower confidence in an IPS and disrupt our production traffic. What's more interesting is how strong the technology is. When we hire external service providers to conduct penetration testing, we need to temporarily apply exceptions in CounterACT Edge to let them do their jobs. The network security appliance simply does its job."

Beyond the perimeter, the organization also sought to control network access, implement a guest registration system, and implement self-remediation services. The team selected ForeScout CounterACT to supply all of these needs.

The security director likes the combination of CounterACT Edge supporting perimeter defenses and CounterACT capabilities for network access and internal threat monitoring. He calls it a "hybrid approach, whereby NAC sits on top of IPS functions" - delivering comprehensive visibility and security enforcement for all device activity on the network.

Technology Considerations and Coordinated Processes

How should enterprises protect their networks and computers against today's sophisticated threats? There is no single answer.

IT organizations should consider the aforementioned security tool portfolio based on risk profile, budget and personnel constraints. New advanced technologies, including ForeScout ActiveResponse™ technology as incorporated into ForeScout CounterACT Edge threat prevention and CounterACT Network Access Control (NAC) solutions, can augment a security arsenal that contains traditional solutions such as antivirus, patch management, firewall and intrusion prevention.

In addition, organizations should incorporate these top 10 best-practice guidelines:

- 1. Identify your business critical / sensitive information and map respective infrastructure and data stores. Assess your defense architecture. Eliminate non-essential access to resources. Eliminate unnecessary copies of data. Reduce the attack surface. And determine gaps in your defense portfolio.
- 2. Establish clear security policies. Build a security awareness program to alleviate the likelihood of successful spear-phishing attacks. Create and enforce policies regarding corporate information on social media and Web sites.
- 3. Review configuration, change, and patch management policies and procedures. Employ respective tools and controls to monitor and ensure that configurations remain stable and operating platforms are secure / in compliance. Self-propagating malware and human attackers alike will exploit unpatched systems.
- 4. Invest in web filtering, email filtering and anti-malware technologies, which are instrumental in reducing the threat of advanced attacks such as propagating worms, the use of malicious and suspicious websites or IPs, or the distribution of personal identifiable information in clear text.
- 5. Assess if DLP (Data Leakage Prevention) approaches can further reduce inappropriate transmission of sensitive information.
- 6. Define log management policies and ensure the consistent activation, aggregation and review of event logs. Invest in SIEM tools that provide high levels of visibility and cross-correlation across the entire network and security infrastructure with the means to define rules that support identifying policy violations and suspicious behavior.
- 7. Supplement your investment in conventional perimeter security (e.g. firewall, IPS and web filtering) with more advanced threat prevention. ForeScout CounterACT Edge provides unique, real-time threat protection, including protection against zero-day attacks and low-and-slow attacks.
- 8. If you have not already implemented NAC, examine ForeScout CounterACT for Network Access Control. This integrated NAC solution provides complete visibility and control to: keep unauthorized people and systems off your network, enforce endpoint compliance, automate endpoint remediation, and provide post-connection monitoring to detect internal malicious activity.

- 9. Assume that your company can and will become the victim of a zero-day attack. Keep up to date on new threats and their operating attributes. Utilize your SIEM to help identify such threats by assessing network and security infrastructure event logs. Identify the resources and expertise needed to analyze respective security information, as skilled personnel are essential to identify advanced threats, determine the risk to the enterprise, and understand the impact with regards to remediation and resumption. Be prepared for forensics personnel, procedures and tools to investigate the cause and nature of the breach, and how best to initiate mitigation and/ or eradication procedures that maintain the integrity of evidence for both internal and possible law enforcement action. SIEMs and deep packet inspection (DPI) tools can support forensic endeavors.
- 10. Consider that your enterprise will be breached at some point, and have incident response capabilities in place for dealing with the intrusion quickly and effectively. Ensure that incident response policies and procedures are in place and tested to assure adequate response to breaches including communication, assessment, remediation and resumption. Effective incident response should include a written plan with complete guidelines for assessing different risk associated with certain security breach scanarios, and clearly designated personnel and notification procedures. Assess interdepartmental response procedures which, in addition to IT and security personnel, may enlist management, legal, HR, public relations. Define escalation guidelines with criteria, approvals, responsibilities and actions for extreme cases that may require shut down of production systems and involve disaster recovery procedures.

About the Authors

William "Bill" Sieglein is an expert advisor in information security, risk management, privacy and governance to large clients in the financial services, healthcare and non-profit sectors. Bill has directed security and privacy programs for numerous companies and has overseen professional services for security consulting firms. He served as CSO for the Public Company Accounting Oversight Board (PCAOB). An accomplished writer and speaker, Bill is the founder and CEO of the CSO Breakfast Clut, a peer-to-peer network of security and compliance executives from large US organizations. See http://www.cisoexecnet.com.

Scott Gordon (CISSP-ISSMP) is a seasoned enterprise systems and information security industry executive having worked with the best and brightest innovators over the past 20 years. He is the vice president of worldwide marketing at ForeScout Technologies. Scott has advocated and contributed to the advancement of leading-edge products spanning NAC, service management, event correlation, security information management, network security, endpoint security, penetration testing, encryption and risk management. Scott is avid speaker and author of "Operationalizing Security".

© 2011 ForeScout Technologies, Inc. All rights reserved.