G00224682

Best Practices for Mitigating Advanced Persistent Threats

Published: 18 January 2012

Analyst(s): Lawrence Pingree, Neil MacDonald

Many security practitioners see the term "advanced persistent threat" (APT) as primarily a marketing term and do not acknowledge that there are advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems. Organizations face an evolving threat scenario that they are ill-prepared to deal with. They must respond to these threats with the proper techniques and technologies. This research will enable security practitioners to understand the new threats they face and the best-practice steps they must take in order to reduce the risk of compromise against the advanced adversaries taking direct aim at their organizations.

Key Findings

- The defining aspect of an APT is that it has advanced beyond existing controls and is not detectable using traditional signature-based security protection mechanisms.
- Because people tend to be easier to target than systems, adversaries are using social engineering and social networks to target sensitive roles or individuals within an organization that either have knowledge, use of or access to the data targeted.
- With APTs, malware delivery is not the only goal; the goal has now changed to establish lasting footholds — persistence — inside the network even after detection and removal, often by obtaining the targeted individual's credentials.
- There is no silver bullet to mitigate APTs. A defense-in-depth strategy must be used across network, edge, endpoint and data security.
- Context-awareness becomes a key next generation capability of all security protection technology platforms to help mitigate the threat from APTs.
- Incident response must be improved to include capabilities such as in-house or third-party forensics and malware analysis.

Recommendations

- Security program managers need to take a strategic approach with tactical best-practice technology configurations in order to properly address the most common advanced targeted attack scenarios to increase both detection and prevention capabilities.

- Start by shutting down the low-hanging vulnerabilities that adversaries will target to deliver the APT.
- To reduce the impact of social engineering attacks, ensure that end users do not have administrative access; and when IT administrator access is required for system administration, perform these functions on isolated systems that are not used for email or Web browsing.
- Focus on unifying security controls through context awareness to consistently enforce security throughout the infrastructure with concerted security responses across multiple security controls.
- Implement security information and event management (SIEM) capabilities. The monitoring and analysis of the output of security controls is as important as the operation of the security controls themselves.
- Acknowledge that not all threats can be prevented and, therefore, the speed to resolution upon detection is also critical. Improve incident response processes.

Table of Contents

List of Figures

Analysis

What Is an Advanced Persistent Threat, and How Has the Term Changed?

The term "advanced persistent threat" is often used by mainstream media and security technology providers and has become a trendy new marketing phrase for selling products and services. The meaning of this new phrase has been elusive to many security practitioners as they often feel this describes the same threats they have faced for many years. Debate continues to rage about how to properly define what's actually new with this terminology and what steps an organization can take to defend against this latest threat. Regardless of whether you agree or disagree with the term APT, there is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it yet.

The term "advanced persistent threat" originated from the United States government as a declassified way to refer to the cybersecurity threats and capabilities posed by specific nation states (specifically the People's Republic of China). In the research titled "Strategies for Dealing With Advanced Targeted Threats," Gartner adjusted its use and definition of the advanced persistent threat to more aptly call the scenario an "advanced targeted threat" to reduce the reliance of the prior terminology that often centered on the country of origin and the persistence of nation states. For the purpose of this research, we will use the term "advanced targeted attack" to more appropriately speak to the real security issues faced by organizations and what best practices they can employ to appropriately address the risks.

When examining the advanced targeted attack, and the new methods being used to breach today's security controls, it can be distilled down to a basic understanding that attackers, especially those who have significant financial motivation, have devised effective attack strategies centered on penetrating some of the most commonly deployed security controls (largely signature-based antivirus and signature-based intrusion prevention), most often by using custom or dynamically generated malware for the initial breach and data-gathering phase.

Advanced attackers are now capable of maintaining footholds inside an organization once they successfully breach security controls by actively looking for ways to remain persistent on the target organization's internal network either through the use of malware or, even if the malware is detected and removed, via postmalware use of user credentials gathered during the period of time the malware was active. They then change their tactics to secondary attack strategies as necessary, looking for other ways around any internal security controls in the event they lose their initial attack foothold.

Organizations must continue to set the security bar higher, reaching beyond many of the existing security and compliance mandates in order to either prevent or detect these newly emergent attacks and persistent penetration strategies.

In Figure 1, we outline the basic high-level attack stages for an advanced targeted attack, and extend the characteristics identified in prior Gartner research to include the aspect of establishing a foothold, postmalware removal. An advanced targeted attack is as an attack that penetrates

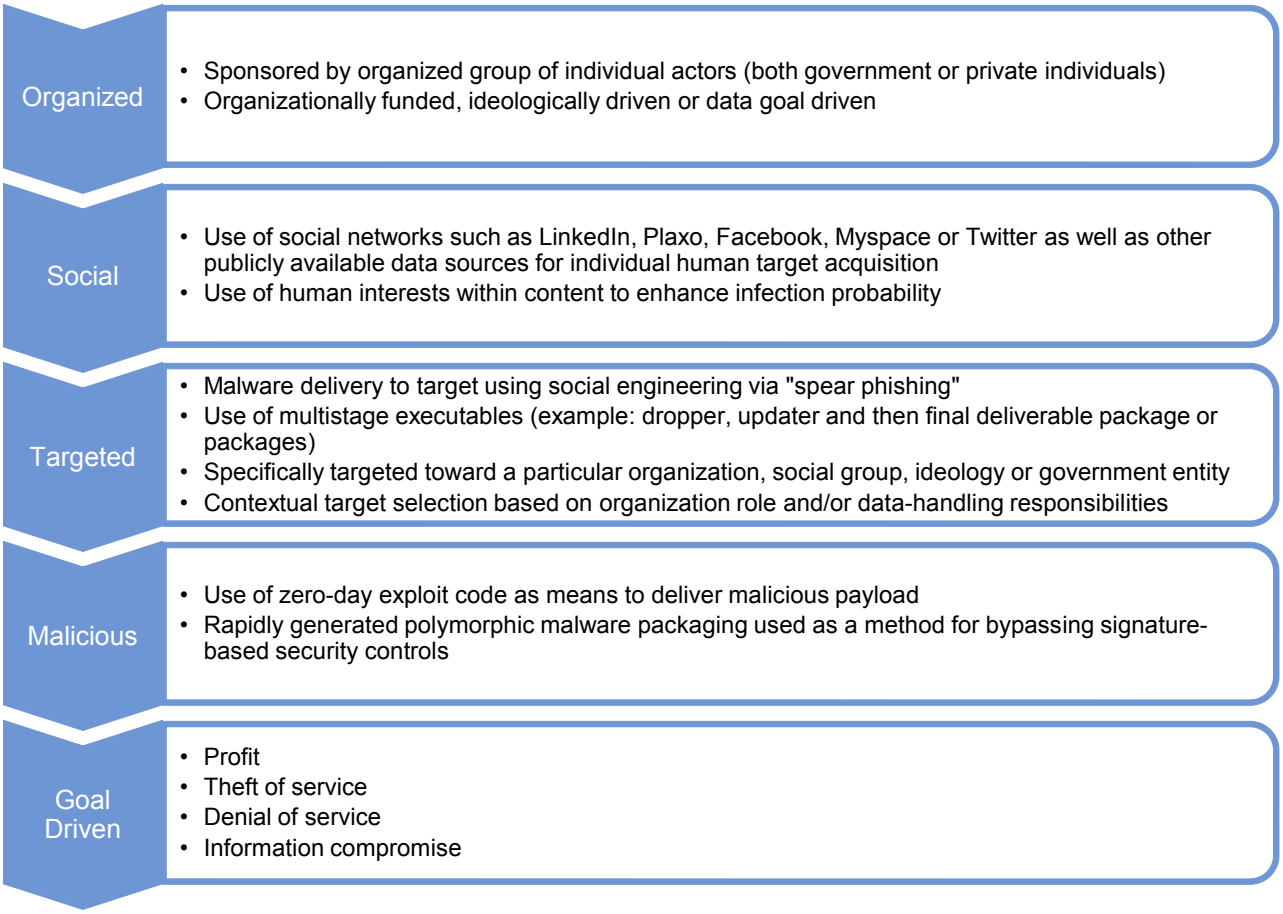
existing security controls using malware, seeks to significantly delay the detection of infection, establish a lasting foothold and then either cause meaningful organizational harm and gather information, then exfiltrate targeted data from an organization's systems. One of the most defining attributes of an advanced targeted attack is that it commonly uses polymorphic and dynamic malware creation techniques combined with rapid deployment to obfuscate the delivery of the malware payload from existing signature-based security controls that rely largely on signature update propagation to enforcement points. Since advanced attacks often target end users as the weakest link, another defining aspect of ATAs is the use of social engineering leveraging social network role intelligence to target sensitive roles or individuals within an organization that either have knowledge, use of or access to the data targeted.

Figure 1. Typical Advanced Targeted Attack Goals

Source: Gartner (January 2012)

While nation states can pose a larger threat than many other types of cyberattackers, the most sophisticated and advanced targeted threats are frequently developed by financially motivated attackers — the funding of ATAs at the nation-state level is not a necessary requirement as many of the latest tools and techniques are freely shared in the hacker underground. In fact, some nation states can develop their own cybersecurity tools that can be accidentally leaked into the underground, and in turn underground hackers can also be engaged by nation states to either perform attacks or develop tools on behalf of the nation state, further clouding the situation and highlighting why we shouldn't focus on the parties involved as much as the technology best practices we must implement for mitigation of the latest risks. In Figure 2, we outline the common characteristics of ATAs.

Figure 2. Typical Characteristics of Advanced Targeted Attacks



Source: Gartner (January 2012)

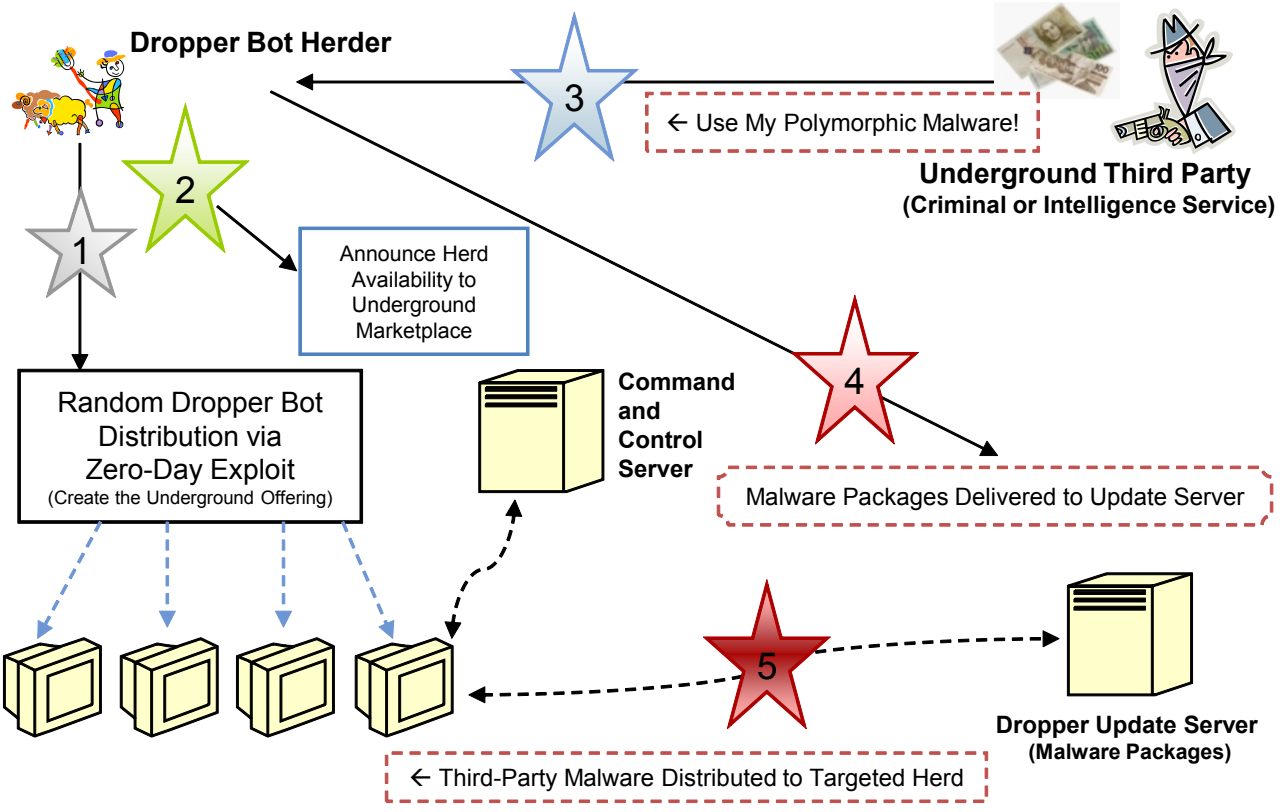
Advanced attackers include other actors such as well-organized individuals, hacktivists and organized crime with fame or financial fraud goals within their scope of desired outcomes. These entities now have the knowledge of how to leverage malware to bypass existing security controls and organizations must now take more meaningful tactical steps and focus less on compliance-related activities to decrease the likelihood of a successful breach.

Stopping Advanced Targeted Attacks Using an Attack Life Cycle Approach

Mitigating the threat from ATAs requires a defense-in-depth strategy across multiple security controls. In order to understand what best practices make sense, we need to first understand the life cycle of an ATA — how ATAs typically penetrate our systems and exfiltrate information. In Figure 3 below, Gartner outlines the common pattern of distribution of custom malware. In Step 1, a bot herder creates, customizes and distributes polymorphic malicious binaries in order to infect random hosts with a dropper (aka a remote installation agent). In Step 2, the herder then announces the availability of their new bot herd to the underground, often including the IP ranges and locations

across the Internet of the infected hosts. This entices other interested underground third parties that are looking to breach a particular IP address space where the dropper has been deployed (for example, financial services, government networks or otherwise). In Step 3, the third party inquires with the bot herder to distribute malware to the herd; sometimes this is a paid-for service, provided for free or exchanged for information or other underground bits (copyrighted software or malicious code the herder does not have). In Step 4, the malware package (often originating from the interested third party) is distributed via the herd's update server via commands sent via the bot herd command and control server. The final stage (not shown in this depiction) is the execution of the malware payload, which can contain any number of final instructions that can commonly do things such as information gathering, user account gathering, data indexing, data copying and uploading, and anything else that a programmer could implement using software code.

Figure 3. Typical Advanced Targeted Attack Malware Distribution Life Cycle



Source: Gartner (January 2011)

We can use the ATA life cycle to devise new protection and detection mechanisms. For example, if we can't stop the ATA from getting on a system initially in Step 1, we may be able to detect its communications back to the botnet command and control nodes in subsequent steps.

Below, Gartner outlines strategic initiatives and best practices that can help reduce the likelihood of success in each phase of the typical advanced targeted attack life cycle. The goal of these best practices is to provide tactical ways to minimize the attack surface through optimizing detection

and prevention capabilities available in both existing and emerging security technologies. One common security threat addressed in this research is the pervasiveness and capabilities present in today's malware. Many of the best practices below are focused on preventing and detecting malware infection as this is the most commonly used mechanism to exfiltrate data from internal networks and is often also used to enhance the persistence of an ongoing data breach whether it is a nation state or another bad actor.

Use a Strategic Security Approach to Implement Tactical Best-Practice Controls

In prior Gartner research titled "Strategies for Dealing With Advanced Targeted Threats," Gartner had defined strategic technologies that should be employed in a defense-in-depth, layered approach model. This layered approach is typical of many enterprise organizations and is often managed in independent ways to accomplish stated security goals, namely, detect, prevent, respond and eliminate. There are tactical steps that must be taken inside each of the layers of the model in order for this strategy to adequately increase the security of most enterprises, and organizations can follow these steps to increase their security enough to at minimum detect and even prevent a large number of these attacks.

Best-Practice Strategies

- Use a defense-in-depth approach; no one single technology will stop advanced targeted attacks.
- Ongoing integration and sharing of security intelligence among your security controls should be a stated security program goal.
- Context-aware security controls (see "The Future of Information Security is Context-Aware and Adaptive") should be a key requirement when evaluating the next generation of security protection platforms (network, endpoint, edge and so on)
- Review all security technologies and existing controls and, if necessary, update or uplift them, and utilize advanced features in the latest products or services to keep up with changes in the threat landscape.
- Acknowledge that technology alone won't stop ATAs. Review the best practices below, but do so with the mind-set of unifying the security processes between each technology so that effective management of threats is possible and reduction of breach events is the more likely result.
- Staff appropriately to ensure you can operate all the latest technologies and, if necessary, engage third parties to manage or operate more commodity security controls while you focus more on the strategic security processes and technologies.

What Best Practices Must Be Adopted to Reduce the Threat of ATAs?

Keep Up to Date With the Threat Landscape

Advanced targeted attacks and their techniques are changing rapidly, making it increasingly difficult for most security practitioners to stay up to speed with the latest threats and appropriate threat mitigation technology and practices. It is more important than ever that both security practitioners and their organizations remain diligent in educating themselves and their employees about these new threats and how to combat these latest techniques.

Best Practices

- Review your IT security department's education budget and ensure you have appropriately allocated continuing education for security-specific education initiatives for both your security team and your organization for dealing with advanced targeted attacks.
- Invest in forensics capabilities. For the security team, ensure appropriate levels of education on malware analysis and incident response are a critical focus area for at least members associated with these functions.
- Create a role-centric security awareness program focusing on educating employees on the sensitive roles they hold so that these employees better understand how attackers are attempting to gain access to company data and how that data is likely to be used (examples are finance, accounts payables, human resources and business operations, etc.).
- Consider extending your involvement with external information and security-related nonprofit organizations to enhance knowledge and collaboration of your security team and organization with others in aligned industries.
- Establish relationships with government-sponsored security threat and information-sharing programs to boost collaboration and enhance the response characteristics of your incident response procedure or process (examples: InfraGuard and CERT/CSIRT).
- Task a member of your security team to regularly review news articles, publications and critical infrastructure protection alerts while comparing and contrasting this information with your current vulnerabilities and known risk profile.
- Subscribe to security intelligence services that provide information on a regular basis to keep abreast of the latest malicious activities and event information as well as how vulnerabilities are being exploited.

Thwart Social Engineering Techniques Through Education

ATAs frequently target end users using social engineering techniques and attacks that are often more effective because they are targeted with knowledge gleaned from social networking sites. Further, it is likely that organized attackers will search for information readily at their disposal on the Internet to find individuals and organizational roles to target. They do this in order to gain insight into an organizational structure, internal operations and eventually to target individuals they believe

will potentially have access to or own the most sensitive information. For example, if an organized group of individuals wants to target individuals handling sensitive credit report information within an organization, they may look up your organization on social business websites such as LinkedIn or Plaxo to determine the finance manager's name. Once the attacker knows the name of a potential victim, they will add this person's name to the list of targeted individuals when they decide to launch the social engineering phase of their attack.

It is important that organizations think like their adversary and understand that it is *any* weakness (aka vulnerability) that can be used against their organizations and that a determined attacker will stop at nothing to find a technical vulnerability to exploit or determine where weaknesses exist in your business processes. It is critical that all organizations take the proper steps to deal with the social engineering aspect of their users.

Best Practices

- Review company policy to ensure that it has taken appropriate steps to prevent the inappropriate posting of internal information onto public social media sites. Your policy should extend the applicability of the data classification framework to data posted to external sites and including punitive language such as a termination clause.
- Ensure that your end-user security awareness programs highlight that disclosure of current or active individual job role information onto the Internet is highly discouraged by the company (keep mindful of freedom of speech issues) and also highlight that this information is often used by attackers to identify employees to attack with targeted malware content and malicious URLs.
- Augment your awareness campaigns to properly describe how attackers are actively using external data repositories to generally target employees through the use of social engineering techniques to gain their trust, and stress the importance of the suspicious mind-set for all communications through email and via the Web.

Best Practices That Apply to All Layers

There are best practices that should be evaluated at all layers using a defense-in-depth approach to reduce vulnerabilities in each — network, email, Web and endpoint. Common elements of best practices appropriate to all layers include:

- Ensure you are using the latest offering and engine from your security platform protection provider. Most platforms have evolved well beyond purely signature-based approaches for malware detection to include behavioral and anomaly detection capabilities.
- Evaluate the context-aware security capabilities of your security platform provider. Security platforms must become context-aware — identity, application, content, location and so on — in order to make better information security decisions regarding ATAs (see "The Future of Information Security is Context Aware and Adaptive"). If your provider doesn't have this or have it on its road map, consider switching vendors.

- Linkage into IP reputation services. Like content, pure blacklisting-based approaches for IP address filtering, URL filtering and email sender filtering no longer work. Next-generation security platforms incorporate cloud-based community context for determining the relative goodness or badness of a specific IP address or URL. At a minimum, communications with IP addresses and URLs with low reputations should be logged, and some organizations will choose to block these entirely.
- Activation of data loss prevention (DLP) capabilities. Most security policy enforcement points have embedded DLP capabilities to detect when sensitive data is being handled by each layer. Alternatively, these security platforms may integrate with enterprise content-aware DLP offerings for their patterns. Review and implement DLP capabilities of the platform to ensure it is configured to detect and use a workflow to provide approvals of or block the release of sensitive data types such as credit card numbers, intellectual property and personally identifiable information as needed.
- Integration into SIEM. All of the security platforms in this research document create logs of activity and events. Consolidating this vital data into broader security information and event management platforms increases the ability to correlate events, enabling more effective incident response prioritization.

Upgrade Your Perimeter and Network-Based Security

Advanced targeted attacks often exploit the fact that many organizations allow essentially unlimited Internet access or utilize only outbound URL-based filtering technologies as their predominant outbound access control mechanism. Targeted attacks take specific advantage of porous egress filtering policies that many enterprises use, and leverage the commonly allowed sets of ports and protocols to exfiltrate data to the outside world. If outbound filtering is enabled, many attackers know they can sometimes use common ports and protocols to go around existing defenses by using standard ports such as TCP port 80 (HTTP) and TCP port 443 (HTTPS), or UDP through port 53 (DNS), and leverage these small outbound holes in our perimeter defenses to send command and control communications or to send data outside the enterprise. Encrypted communications such as HTTPS and VPN access is being increasingly used as a way to bypass the inspection controls that exist in more traditional security inspection technologies, so organizations must respond by ensuring this data is properly terminated and inspected.

Enterprises should consider reviewing their perimeter defenses and capabilities to ensure they have implemented appropriate levels of inspection of *all* (especially outbound) network traffic at the edge of their networks. Advanced targeted attacks will likely perform reconnaissance of the network in order to identify potential opportunities for exploitation and then use varying techniques to "jump the fences" we have in place. For example, if your users have no essential business need to send traffic toward other countries, you should consider whether blocking this network traffic is warranted. The latest generation of Web security gateways, firewalls and IPSs provide additional features that can be leveraged for detecting and disrupting advanced targeted attacks.

Below, Gartner reviews the common techniques that can be used to improve on defense-in-depth goals to either thwart attackers or enhance our detection capabilities at the network layer.

IPsec & SSL VPN Remote Access Connections

Organizations commonly allow remote access to enhance remote employee productivity; however, remote endpoints, especially if they are not owned or controlled by the enterprise, have a relatively higher likelihood of being compromised. All forms of remote enterprise access, and especially those from poorly controlled PCs, must be treated as potential threat vectors, with relatively higher levels of access control, authorization and threat prevention technologies as well as the use of monitoring and detective security controls.

Once a user is authorized to connect to the internal network using a virtual private network connection or SSL VPN, they often obtain unfettered access to the internal networks or systems within the organization's environment. Although a VPN connection may be authenticated with a strong two-factor authentication mechanism and access controls may be in place, threats still exist with these connections. Mobile devices such as laptops, home desktops and other mobile devices such as tablets and smartphones still represent risks that remain beyond just identifying the user and encrypting the connection in transit across the Internet.

Best Practices

- Review your VPN devices and ensure all users are required to utilize a risk-appropriate authentication method prior to authorization (see Gartner research titled "Good Authentication Choices for Workforce Remote Access").
- Review your VPN device policy and ensure that users are only permitted to the internal environment that they specifically need to access and not to the entire organization.
- Implement internal inspection devices, such as IPS, between your VPN termination device and your internal network environment so that attacks can be prevented within your infrastructure.
- Consider technologies that allow for the termination and security inspection of SSL traffic so that attacks cannot be perpetrated in the encrypted tunnel back to your internal applications or systems obfuscated from your security inspection technologies.
- Validate that monitoring controls are in place and appropriate levels of logging are performed off-device in centralized log servers and deploy security information management systems so that attacks can be detected or analyzed through additional analysis or correlation of incoming events.
- Regularly review VPN events identified and ensure these are correlated in your SIEM technology and look for anomalous patterns of activity. Leverage vendor-supplied anomaly detection and alerting capabilities when technically feasible.
- Where possible, reduce the use of direct network-level VPN access and alternatives such as Web and application portals.
- For mobile devices, consider implementing a mobile device management technology to ensure for basic consistency of security controls extended out to mobile devices.

Authentication Technology Sample Vendors: RSA, ActivIdentity, CryptoCard, SafeNet, Symantec, Vasco, Nexus Technologies, PhoneFactor, SMS Passcode and SecurEnvoy

SSL VPN Sample Vendors: Juniper Networks, Cisco Systems and Citrix

Mobile Device Management Sample Vendors: Sybase, Good Technology, AirWatch and MobileIron

Firewalls

Firewalls represent an import layer of security control for network layer connectivity. Since ATAs must communicate out in order to be useful, network-based security approaches must be improved to incorporate more context about the network flows taking place — geolocation awareness, application awareness and identity awareness. Next-generation firewalls (NGFWs) have added extensive capabilities to help mitigate ATAs by expanding their defense-in-depth approach to include more network layers in their inspection capabilities.

Best Practices

- Review and if necessary adjust your egress network firewall rules in order to ensure only business-critical services are permitted to both enter and leave the network; this includes the consideration of geographical filtering at the country level (GEO IP filtering).
- Review and if necessary adjust your ingress network firewall rules in order to ensure only critical inbound services are permitted to enter the network; this also includes geographical blocking or filtering at the country level based on business need.
- Consider the use of application awareness (a form of context awareness) provided in NGFW functionality that leverages deep packet inspection techniques to permit valid (authorized) applications and deny everything else. To enable the NGFW functionality, you may need to perform a firewall refresh if you are using first- generation firewalls that only provide filtering based on IP protocols, source and destination IP address and port numbers.
- Review and (if available) regularly implement new capabilities provided by the latest firewall technologies to incorporate new concepts that emerge such as today's dynamic threat feeds that are provided via hosted or cloud-based services to deliver malicious threat lists for instant blocking at the firewall (don't allow your firewall technology to stagnate).
- Ensure proper zoning and segmentation is performed in your internal network environment and that proper firewall logging and inspection is performed between high- and low-security segments.

NGFW Sample Vendors: Check Point, Palo Alto Networks, Fortinet and SonicWALL

Intrusion Prevention Devices

Like firewalls, network-based intrusion prevention system (IPS) solutions provide an important layer in an ATA mitigation strategy. For best results, use signatures with proven low false-positive rates.

While some organizations are concerned about IPS, consider that a widespread data breach will likely result in a larger financial loss than the amount of time a service becomes unavailable because of a false-positive detection or a related configuration problem for in-line deployment modes. For in-line IPS deployments, limit system failure risks by architecting for resilience.

Best Practices

- Review and if necessary adjust intrusion prevention security enforcement policies to block rather than just detect known attacks and attack signatures.
- Review your IPS and ensure that the technology you are using has the latest botnet prevention technology to prevent botnet command and control network activity. Likewise, see if communications to other types of low-reputation IP addresses can be blocked or allowed and logged for further investigation.
- Review your IPS's features and ensure it provides host and traffic anomaly detection (for example, using processing netflow data) and has capabilities to prevent or at minimum detect and alert on the anomalous (statistically deviant) traffic exiting through your perimeter devices.
- Review your current intrusion prevention implementation and, if available, implement blocking capabilities that include reputation-based or real-time block list threat feeds provided by your technology vendor.
- Review and if necessary adjust protocol anomaly detection and prevention capabilities to ensure nonstandard communications are blocked while expected and authorized protocol communications are allowed through known standard ports such as HTTP (TCP port 80), for example, not permitting an FTP session through the standard HTTP port.
- Review and ensure all internal segments are inspected with IPSs that are configured to block known high- and medium-high-fidelity signatures with low false positives as directed by your technology provider.
- Make sure that network visibility extends into virtualized environments either by tapping internal virtual switch traffic out for external inspection or by virtualizing IPS capabilities and running directly within the virtualized environment.

IPS Sample Vendors: McAfee (Intel), Sourcefire, Cisco, IBM, Juniper, HP TippingPoint and Check Point

Advanced Threat Detection/Prevention

Network-based advanced threat detection and prevention technologies have emerged adjacent to IPSs in order to combat the problem of the zero-day polymorphic malware that is often used to deliver the targeted attack payload. Advanced malware often uses file multipacking, layered encoding, dynamic malware creation and other more advanced techniques to bypass many of today's existing signature-based security controls and deliver their malicious payloads onto the targeted individuals' computing systems. Some of these products also include features such as behavioral detection, heuristics, anomaly detection, virtual execution environments and other policy

rules around content to enable the rapid evaluation and blocking of potentially malicious content. They often enhance their detection and prevention capabilities to block network callbacks using a variety of techniques, including reputation-based threat feeds, traffic anomaly detection, malware execution observation and various real-time block lists to enhance prevention capabilities. These technologies offer a valuable second opinion to augment and complement existing protection mechanisms.

Best Practices

- Evaluate and deploy a network-based advanced threat detection/prevention technology to reduce the potential success of zero-day malware and other targeted attacks.
- If already deployed, review your existing advanced threat detection/prevention technology and ensure that you take appropriate steps to employ any prevention capabilities it provides as directed by your technology vendor.
- Review your advanced threat detection/prevention deployment and ensure that all network connections to the Internet are inspected.
- If network topology prohibits full network visibility, evaluate and prioritize placement of these types of capabilities to the public Internet connections and critical systems within the data center.
- Properly employ your incident response process around this new technology and execute the process when appropriate indications exist for a potential malware infection or command and control callback is detected.

Advanced Threat Detection/Prevention Sample Vendors: FireEye, Fidelis Security Systems, Damballa, NetWitness and Trend Micro

Focus Your Strategy Toward Malicious Content

Attackers are increasingly focused on delivering malicious content inside of email and Web transactions in order to breach your security and pass through your existing security controls. In the past, signature-based technologies such as antivirus were adequate to protect against a majority of threats. However, the emergence of newer attack and payload delivery techniques that bypass these traditional signature-based approaches must be addressed by new emerging security technologies as well as augmentation of our old paradigm of thinking about traditional security technologies.

Email Content Security

As most ATAs are delivered either via email or the Web, email content security is more important than ever. Content inspection technologies often take the form of email security gateways or software installed on email systems. Email gateways are appliances that are designed to be hardened email relays that are exposed directly to the Internet in order to provide content inspection, email archival, anti-spam and other various anti-malware detection and prevention capabilities as email content enters and leaves an organization's environment.

Best Practices

- Deploy a secure email gateway or equivalent capability from a service provider within your mail delivery architecture.
- To increase detection and prevention rates, Gartner suggests customers broaden the number of antivirus engines that will scan email content; for example, using one antivirus engine at the email gateway and an alternative antivirus engine for your endpoint systems.
- Review and validate that you are actively using email reputation feeds (if available) from your secure mail gateway solution provider.
- Review and ensure your mobile device security includes monitoring of all email going to and from mobile devices.
- Review your email security gateway or software and ensure you are actively blocking phishing attempts.
- Review and ensure you are actively blocking viruses and other malware types.
- Review and consider secure email gateways that implement content sandboxing (virtual environment emulation code execution), also called virtual sandbox technology. This technology allows code traversing through the infrastructure to be tested within a virtualized simulated environment that allows malware to be evaluated for common malicious behavior prior to delivery and subsequent execution on the end system.
- Review and ensure you are actively blocking any hosts or URLs that are listed on real-time URL reputation feed services.

Secure Email Gateway Sample Vendors: Cisco**,** Google, McAfee (Intel), Proofpoint, Symantec and Trend Micro

Secure Email Services Sample Vendors: Barracuda Networks, Cisco, McAfee (Intel), Symantec.cloud, Trend Micro and Zscaler

Web Content Security

As most ATAs are delivered either via email or the Web, secure Web gateway technology should be used. Secure Web gateway capabilities exist in several types of security technology products and services including stand-alone secure Web gateways, unified threat management products, cloud security services and multifunction firewalls. This technology specifically looks at Web content to determine if users are browsing to malicious URLs or downloading content packages that contain malicious executable payloads or other embedded malicious objects and scripts from Web pages and attempts to thwart the delivery of that malicious content to internal systems.

Best Practices

- Deploy a secure Web gateway or equivalent technology to filter and monitor inbound and outbound Web communications and content.

- Implement real-time block lists to block hosts that have already been determined to pose an existing threat.
- Review and utilize reputation feeds and behavioral context security capabilities provided the secure Web content technology to ensure it provides reputation-based threat feeds beyond the capabilities of simple real-time block lists, which take into account additional security context such as whether or not a URL was part of a spam message, hosting site and the longevity of the domain from the date of issuance.
- Review your URL filtering configuration and ensure that known proxy sites, hacking sites and other malicious site categories within your Web filtering product or service are blocked.
- Review and ensure your secure Web gateway product or service is providing active blocking through quarantine or virus content removal.
- Review and ensure your appliance is providing active blocking through quarantine or spyware content removal.
- Review and implement where possible content sandboxing (virtual environment emulation code execution) virtual sandbox technology allows code traversing through the infrastructure to be tested within a virtualized simulated environment that allows malware to be evaluated for common malicious behavior prior to delivery and subsequent execution on the end system.
- If technically feasible, ensure that mobile devices such as smartphones and tablets are also inspected by your secure Web gateway solution by mandating proxy settings (available in iOS 5) or implementing nonsplit tunnel VPN implementations.

Secure Web Gateway Sample Vendors: Cisco, Bluecoat Systems, Websense, McAfee (Intel), Zscaler, Symantec and Trend Micro

Uplift Your Endpoint Security Controls and Detection Stance

The latest malware threats have largely thwarted signature-based detection and prevention capabilities as attackers have become well-aware that endpoint security technology is largely based on the distribution of signatures. One significant factor involved in malware distribution is the wide use of administrative privileges by end users, making it much easier for infection to go beyond the user protection ring and embed itself deeper into the target host operating system or into kernel-level drivers that enable the further obfuscation capabilities. These factors make it necessary to monitor the health and status of endpoint systems whether they are servers, desktops or other devices and look for possible signs of compromise. Technologies now exist that utilize system integrity assessments techniques to baseline systems and report possible compromise. There are two classes of technology that are used to perform this function: one is file and folder integrity monitoring; the other is the systematic assessment of the system integrity to identify suspicious behavior patterns, drivers, etc., that may indicate compromise. Some of these systems can also be combined with network-based sniffing technology to further validate a potential compromised system through network-based behavioral analysis.

Best Practices

- Remove administrative privileges on desktops to reduce the ability of malware infections to cause low-level system damage (see "Best Practices for Removing End-User Administrator Rights on Windows").
- Where privileged access is needed, use privileged account activity management (PAAM) technologies to properly manage the on-demand escalation of privileges.
- Patch more than just Windows and Office. Extend your patch management processes to all common desktop elements (for example, Adobe, Java, alternative browsers and so on).
- Review your existing endpoint antivirus products to ensure they are up to date with anti-malware technology capabilities and uplift if necessary to include complete anti-malware protection, potentially unwanted program detection, and other malware detection and prevention capabilities.
- Add host and server intrusion prevention capabilities to your endpoint systems handling sensitive data types and enable blocking of high-fidelity critical, high and medium attack signatures with low false-positive rates as suggested by your security technology provider.
- Deploy endpoint compromise assessment technology and file integrity monitoring technologies onto endpoint systems handling sensitive data to detect potentially malicious changes or irregular endpoint activities and user behaviors.
- Consider systematically resetting desktop and server workloads to high-assurance states as a way to proactively remove ATA footholds (see "Systematic Workload Reprovisioning as a Strategy to Counter Advanced Persistent Threats: Considerations" and "Systematic Workload Reprovisioning as a Strategy to Counter Advanced Persistent Threats: Concepts").
- Implement a vulnerability assessment and remediation process with service-level agreements for the remediation of all endpoints. Review the effectiveness of remediation efforts across IT support teams on a quarterly basis with responsible parties and/or their management teams.
- Implement network and system behavior analysis capabilities on your endpoint systems to detect potentially irregular or suspicious user and system behaviors.
- Review and consider implementing application sandboxing or application control/whitelisting technology on endpoint systems.
- Review and consider implementing next-generation endpoint infection assessment products to validate the security status of your endpoints.

File Integrity Monitoring Products: Tripwire, IBM Tivoli, Qualys, McAfee (Intel), LogRhythm, nCircle and NetIQ

Endpoint Compromise Assessment Sample Vendors: HBGary and Mandiant

Network Behavior Analysis Sample Vendors: McAfee, Tenable and Radware

Improve Your Automated Monitoring, Correlation and Analysis

The logging of security-related events is a foundation security control, ideally supporting both event detection and analysis. However, many security practitioners begin to be overloaded by the sheer number of logs generated by the security controls. It is important for security practitioners to remember that advanced persistent threats will likely bump into one or two security controls in the course of its life cycle and therefore the likelihood of detection is increased by correlating individual anomalous behaviors within all of the logs in the security control environment so the full pattern of an exploit or attack becomes apparent.

Best Practices

- Ensure you have implemented off device in centralized logging facilities for all your security controls to prevent potential tampering through data breach.
- Form a security operations center or designate specific individuals to operate as a security operations center in order to properly monitor and respond as well as perform initial triage status for security events.
- Implement a SIEM solution to enable centralized log analysis and complex correlation as well as automated anomaly alerting.
- Review anomaly reports and alerts generated by your SIEM system to identify irregular behaviors in the environment.
- When suspicious anomalies or alerts are received by the security operations center, invoke the incident response process.

Improve Your Incident Response Capabilities

Organizations must acknowledge that ATAs will compromise (and likely already have compromised) their organizations. Thus, organizations must have the capability to perform rapid incident response to malware infection in the unfortunate case that their security controls fail. Rapid incident response and remediation efforts enable organizations to substantially limit the damage caused by a malware infection by potentially reducing the amount of time an attacker has to search for and exfiltrate sensitive data, explore adjacent networked systems, perform keystroke logging for user application credentials and other nefarious behavior.

Best Practices

- Define an incident response procedure that defines the roles of appropriate business and IT contacts throughout the organization and other departments needed to respond to security incidents, including human resources, public relations, legal and executive management.
- Retain either internal or external resources for executing an incident response plan; specifically target resources with digital forensics and malware analysis knowledge.
- Consider implementing a secure case management or incident response ticketing system so that security incidents will remain confidential within the incident response process and proper

workflows as well as collaboration can exist between involved parties during execution of the incident response procedure.

- Consider deploying incident response forensics tools that specialize in cybersecurity incident response, including investigation assessment templates for identifying and analyzing suspicious common infection assessment capabilities such as service startup locations, driver hooks, kernel driver analysis, running process exploration, memory snapshot and other various malware analysis technologies.
- When possible, consider automating your incident response investigation triage efforts with integration between forensic analysis tools and other security monitoring software to more rapidly respond to potential suspicious security events when they occur.

Incident Response Forensic Analysis Sample Vendors: Guidance Software, AccessData and Mandiant

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Network Security Monitoring for Lean Forward Organizations"

"Systematic Workload Reprovisioning as a Strategy to Counter Advanced Persistent Threats"

"Strategies for Dealing With Advance Targeted Threats"

"Defining Next-Generation Network Intrusion Prevention"

"Malware, APTs, and the Challenges of Defense"

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600