PROFICIO
SECURITY AND NETWORKING SOLUTIONS

Advanced Persistent Threats: Effective Threat Mitigation through Domestic Managed Security Service Providers

Domestic MSSPs as the Best Means of Addressing the Problem of Advanced Persistent Threats

Introduction

Cyberthreats exist in various forms ranging from the mildly annoying viruses developed by misguided teenagers to much more sinister threats such as consistent attacks on private and governmental networks orchestrated by professionals with financial or political motives. The need to differentiate between random, uncoordinated cyberthreats and attacks of a persistent, targeted nature sponsored by foreign governments or rival organizations and carried out by teams of professionals has established a new classification of cyberthreats collectively referred to as **Advanced Persistent Threats (APTs)**.

In a world where private enterprise and governments have become increasingly dependent on networked computer systems to perform critical infrastructure tasks, defending such networks against APTs has become a matter of both private and national security. In private organizations, networked systems play varying yet essential roles which also means they require protection from APTs designed to destabilize their operations and obtain confidential data. Although a large number of APT attacks are not disclosed by the organizations attacked[1], a number of attacks within the last three years have become reference points within the public domains such as the Stuxnet incident which involved a sophisticated computer worm targeting the networks of Iranian nuclear facilities and Operation Aurora, where the systems of well-known organizations such as Google and

[1] Baich, Rich. *Cyber Espionage: The Harsh Reality of Advanced Security Threats*. Publication. Deloitte LLP, 29 July 2011. Web. 12 Nov. 2012. <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_cyber_espionage_07292011.pdf>.

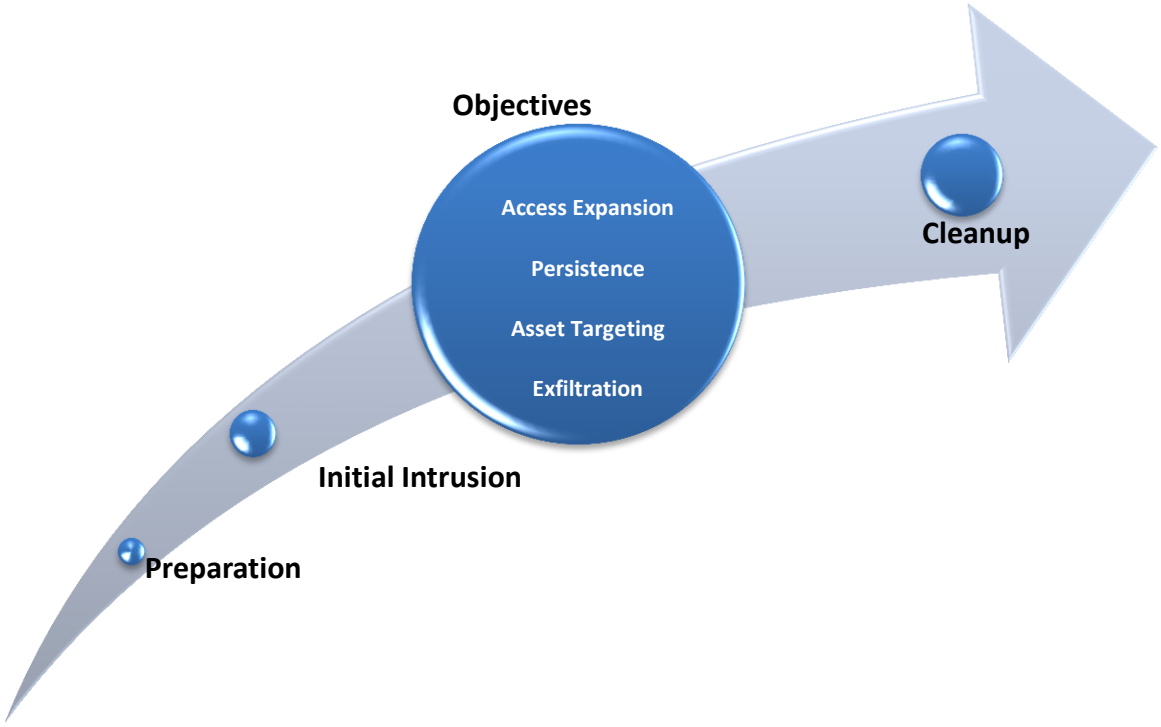
"This analysis of multiple log and event sources through cross-device and functional correlation enables analysts to target the real threats in a sea of noise."

Northrop Grumman were attacked in order to obtain confidential information on individuals as well as corporate projects.

Considering the increasing sophistication of APT attacks and their perpetrators who are well-aware of the tools organizations use to protect networks and know how to evade implemented security controls and measures, traditional means of cyberthreat containment such as the simple use of antivirus solutions and firewalls remain largely ineffective. The gap in APT protections has created a need for customized solutions to deal with APTs utilizing real time network intelligence. This analysis of multiple log and event sources through cross-device and functional correlation enables analysts to target the real threats in a sea of noise. Several **Managed Security Service Providers (MSSPs)** offer these solutions combined with a suite of techniques, tools, and network security services on an outsourced basis to organizations in need of protection from APTs. MSSP efforts are directed from a **Security Operations Center** or **SOC**, a unit designed to coordinate the monitoring, management and mitigations of threats against client networks and systems.

The APT Lifecycle

Several attempts have been made to deconstruct the ATP lifecycle over the last few years which have produced valuable research and a comprehensive understanding of the phases in the APT Lifecycle: [2]



[2] "Lifecycle of the Advanced Persistent Threat." *Information Security Services, Managed Security Services*. Dell Secureworks, 04 May 2012. Web. 12 Nov. 2012. <http://www.secureworks.com/resources/articles/featured_articles/20120504gen/>.

Preparation: As with all attacks that concern compromising the security infrastructure of a target organization, preparation is necessary in order to determine how best to breach the defenses of that organization and achieve the objectives of the attack. Tools and infrastructure for the attack are developed or purchased, plans are made and information on the target is collected from various sources usually in order to determine the best means of gaining entry. Most of this phase occurs outside the purview of the target. Reconnaissance efforts such as port scans may be detected by Intrusion Detection Systems and serve as a warning that such attacks are about to occur.

Initial Intrusion: Attackers succeed in gaining access to the target's infrastructure through a variety of techniques. The use of phishing emails or linkbait that directs users within an organization to a web location where malware can be installed on their computers is common. This malware typically installs silently without notification by exploiting weaknesses such as unpatched browsers or software and provides access to internal company infrastructure via the infected device. Even with the presence of a firewall, malware can encrypt and route messages and information through allowed routes such as HTTP's Port 80 to those controlling it and responsible for the attack.

Objective: Once intrusion is successful, attackers then set about in achieving the objectives of their attack through a variety of means.

- *Access Expansion* – Sometimes a single device is all the attackers mean to target, however, frequently the attackers intend to compromise as many devices as possible. Several techniques can be used to achieve this such as compromising the domain controller or Active Directory server to obtain credentials for the user accounts of other computers on the network. When such credentials are obtained, expanding access by installing malware on additional systems using administrative privileges is easy.

- *Persistence* - With the substantial amount of effort and time APT perpetrators use to organize and succeed with their attacks, they understand that once access has been gained it must be maintained. Antivirus software may later recognize components of their installed malware or control infrastructure as threats and delete or block them so a variety of means to ensure persistence and backup alternatives for continuous access are employed. Antivirus systems may be disabled or compromised; malware may be installed on devices not likely to be scanned such as routers and printers. Malware may be continuously updated to avoid the chances of detection with new antivirus signatures.

- *Asset Targeting* - The main purpose of the attack may be to obtain information from specific sources which may range from documents, to servers or databases. In other circumstances the purpose of the attack may be to disable computers or cause equipment to malfunction as in the Stuxnet malware case. Regardless of variants, the assets that are critical to achieving this ultimate purpose have to be identified and focused on by the perpetrators.

- *Exfiltration* - In the case of information, once the documents or information sought after has been located and collected, the next important thing is to successfully transfer such information from the organization or company's internal borders to an external location such as a FTP server from which it can be retrieved. If the purpose of asset targeting was not to obtain information but to cause damage, this objective stage is unnecessary.

Cleanup: The hallmark of the best APTs and regular hack attacks is that the targets usually do not know the breach occurred or how it was achieved. This phase requires the erasure of all signs of an attack and its origins, this is akin to the burglary of a home, where specific objects have gone missing but there is no sign of forced entry into the home or the fact that the burglars were even there in the first place. With the theft of information, the objects in the burglary analogy remain in place as information is typically copied and not deleted, so the cleanup phase makes it hard to detect that there was even an intrusion in the first place.

When the objective is to damage or disable infrastructure, the cleanup phase is mostly about obfuscating the attack vectors, mode of intrusion and origins of attack not the fact that an attack has occurred as that fact is easily noted after the damage occurs.

How do You Know When You're Attacked?

Anti-virus Configuration and Monitoring: Traditional anti-virus monitoring can often detect an initial infection. Anti-virus may or may not be able to contain the malicious code but can prevent the majority of Trojans and other infections from spreading to other devices.

Analyze Intelligent Event Security Technologies: Implement appropriate configurations and monitor of event logs from all hardware. Anomalous event logs from devices, even those that are not designed to detect malware, such as firewalls, can identify the existence of malware.

Monitor DNS Logs: Monitoring DNS logs can also provide potential evidence of APT/malware infection. When malware is introduced it must connect back to a command and control systems. Often, these command and control systems are reached by via preconfigured domain names and DNS servers can detect multiple failed query attempts.

Monitoring of Host-Based IPS Logs: Configure your host-based IPS to report alerts to the enterprise security console and configure to block potentially malicious activity. Put processes in place to alert security staff to critical alerts issued by the IPS.

Content Filter Log Monitoring: Content filtering systems in the customer environment should be setup to prioritize security alerts and events characteristic of APT threats.

Windows Event Log Monitoring: Windows Event logs should be correlated and automated so that priority events are promptly sent to security operations staff.

Use System Image Backups or Rescue Disks for Validation: Most advanced malware has the ability to defend or disguise itself from detection by traditional anti-virus. Malware can hide in locations not scanned by anti-virus software. Therefore potentially infected devices can be effectively treated with standard "rescue disks." Alternatively, in situations where there is any doubt as to whether an infection has been effectively removed from a system, rebuild the system from a corporate image to ensure removal of malicious software.

Outbound Traffic Monitoring: Outbound firewall logs often show the characteristic patterns of APT-infected systems. Infected systems generate significantly increased network activity often attempting to obtain outbound internet access to command and control systems. This activity was

APTs: Past, Present and Future

To understand APTs better it is important to understand the past history of APTs, the current situation and what will possibly happen in future.

The origins of the Advanced Persistent Threat phrase came from the United States Air Force in 2006 when it describe the role of nations in attacking the networks and computer infrastructure of targets as an element of cyberwarfare[3]. However it was not until 2010 when Google publicly acknowledged that it had been the victim of cyberattacks purportedly emanating from China in what was deemed as Operation Aurora or the Aurora attacks, that the term became more widespread. Currently it is used to describe several other cyberthreats of a similar nature which have occurred in recent times such as the Stuxnet worm in Iran in 2010, the Nitro Attacks of 2011 against a range of companies involved in advanced materials research and the Shamoon malware attack of Saudi oil and gas producer Saudi Aramco in 2012.[4]

As cyber capabilities develop and the world becomes more dependent on networked systems for critical infrastructure it is only plausible that the possibility and frequency of these attacks will increase. Due to the stealthy nature of such attacks and secrecy within government and corporate organizations, a large portion of such incidents are typically undetected or unreported. However, as of 2011, Cisco's 2Q2011 Global Threat Report established that the number of unique instances of malware had doubled from 105,536 to 287, 298 between March to June 2011, the average encounter rate in that period was 335

---

[3] Bejtlich, Richard. "Understanding the Advanced Persistent Threat." *Information Security Magazine*. N.p., 1 July 2010. Web. 14 Nov. 2012. <http://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat>.

[4] Keefe, Mari. "Timeline: Critical Infrastructure Attacks Increase Steadily in past Decade."*Computerworld*. ComputerWorld, 05 Nov. 2012. Web. 14 Nov. 2012.
<http://www.computerworld.com/s/article/9233173/Timeline_Critical_infrastructure_attacks_increase_steadily_in_past_decade>.

encounters per enterprise per month, and the situation clearly shows that APTs are on the rise not only in the United States but globally. [5]

APT Trends

Monitoring data from several APT incidents which have occurred against various organizations over the years has led to the observance of common trends in most APT attacks.

Targets

Targets of APT attacks are typically private corporate organizations in certain cases other non-governmental organizations such as non-profits and think tanks have equally been attacked. Individuals have also been targeted but in most cases such individuals are targeted due to their work in certain organizations.

Attackers

The attackers behind most APTs depend on several factors but they are professionals who are either funded by governments or corporate organizations. Most of the time the involvement of state actors is suspected and rarely confirmed due to the anonymity afforded by the Internet. Simply because the Stuxnet attack was focused on Iran and Israel and the United States stood the most to benefit from the worm's destruction of Iranian computer systems does not prove that the Israeli or United States government was behind the attack. Although they are the most vocal state actors in trying to get Iran to halt its nuclear program, other state actors or private interests could even have orchestrated the attack to derive benefits.

Goals

The goals of an APT are either political, financial or both. When conducted by state actors, politics is usually the overwhelming motive. Information might be wanted on dissidents or in order to find out the policy aims of defense-related organizations or even to penetrate sensitive governmental communication networks. When driven by privately sponsored entities, corporate espionage is usually driven by financial objectives. The theft of critical research and development intellectual property by foreign pharmaceutical companies would be very damaging to domestic firms who have invested heavily in research. As cited in the Cisco Second Quarter 2011 Global Threat Report, the Pharmaceutical and Chemical sectors were twice at risk of malware threats than even those in the Energy and Oil sectors. The economic motive of such APTs is enormous and well documented.

Risks and Dangers

APTs pose a significant risk to organizations that have invested heavily in IP or other proprietary research. Federal defense contractors and organizations are highly targeted for confidential military secrets on advanced weapon systems. The pharmaceutical industry is also at high risk as it is common to invest hundreds of millions of dollars in R&D for more advanced therapies like HIV antiretroviral

---

[5] *Cisco 2Q11 Global Threat Report*. Rep. Cisco Systems, 2 Aug. 2011. Web. 12 Nov. 2012. <http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_global_threat_report_2q2011.pdf>.

research. The loss of revenue and reputation for many organizations can only be imagined. The chaos that could result from interfering with nationwide systems such as ATM networks of financial institutions, electricity grids, nuclear facilities or even the traffic system in a city like New York further underlines the risks and dangers of APTs.

Ancillary Issues

When dealing with the problem of APTs, several ancillary issues come to mind that equally affect the choice of solution used to secure some form of protection against such threats and how the effectiveness of the protective measures of such solutions are determined.

1. *Organizational Needs* – Security is an intimate aspect of an organizations operational structure. Any measures implemented will have to trustworthy and easily deployed without affecting the functionality or processes of the organization.

2. *Challenges* – Different organizations will experience challenges that affect their response to the APT problem. Such challenges may include factors such as the geographical distribution of network assets. An organization may have components of its networks situated across different areas of the United States and not in one particular building. Other challenges may include issues such as compatibility of solutions employed with existing software and hardware already present on the client's network among other problems.

3. *Legal Issues* – APT incidents can be considered as a criminal activity which may violate a number of laws in several jurisdictions. How does an organization effectively determine what legal violations have occurred with an APT incident and what should be reported the necessary authorities? Is the organization's security provider aware of the legal requirements in the client's jurisdiction and can they comply with such requirements? Are there any challenges that might impede compliance such as the geographical location of the client's security provider? Compliance requirements, regulations, industry mandates and control frameworks such as PCI DSS, HIPAA, Sarbanes-Oxley etc. may also be an issue.

4. *Options* – Several recommended solutions exist for dealing with APT containment but these solutions will usually fall into one of two categories:

    - *In-House* – The in-house option for APT containment means that the organization concerned will have to make use of internal human resources and other tools to deal with the problem of APTs. A variety of techniques, tools and strategies may be employed but the core feature of this option is that everything is handled internally by the organization concerned.

    - *External* – The external means of APT containment requires an organization to outsource its network security requirements to a third-party Managed Security Service Provider that can provide a means to combat the recurring threat of APTs and provide an effective containment solution for the organization concerned.

Advantages of the MSS/SOC Approach to Containing APTs

Knowledge is Power: Once an intrusion has taken place, how do you know you are being attacked? ATPs can be very difficult to detect and advanced event correlation is one of the most effective ways to identify an ongoing attack. Additionally, many routine procedures and precautions can be implemented to prevent, detect and sometimes contain an attack including:

- **Mandatory IT and Internet Security Training for All Employees**
- **Routine Network and System Patching to Minimize Risk From Vulnerabilities**
- **Credential and Account Dissemination Policies and Compliance**
- **Desktop AntiVirus and Anti-Spyware as well as**
- **Network Ingress/Egress Defense**

When compared to the in-house option for detecting, preventing and containing APTs, the external option of using an MSS with a well-equipped SOC is much preferable for a variety of reasons, including:

Cost: An in-house option exists to support a single organization while an MSSP is a dedicated provider of network security services to several organizations. As a result the cost per organization is significantly cheaper when using an outsourced SOC because the costs of acquisition, staffing, tools and training are divided among the MSSPs multiple clients, versus an in-house option that bears the costs alone. As of 2008 it was said that the average MSSP would spend $25 million to $40 million to launch their operations[6]. Few private organizations can justify this investment for an in-house SOC option?

[6] *Can Managing Enterprise Security Be Made Easier?* Rep. Symantec Global Services, 04 Apr. 2008. Web. 13 Nov. 2012.

Skilled Staff Strength: An organization hires in-house staff based on its needs and a budget that is often hampered by constraints; the costs spent hiring such staff may often be viewed as unnecessary especially if an APT is not an imminent threat. An MSSP hires staff as an investment and the cost of hiring such staff to provide solutions and services is an existing part of its strategy not an inconvenience. In addition, an MSSP also spends money to hire more skilled staff to deal with divergent requirements as its business prospects depend on an adequate response to the various security problems of its clients.

Knowledge Sharing and Acquisition: Because of the range of customers and variety of situations they deal with and the solutions they provide, MSSPs are typically more up-to-date than in-house security teams. MSSPs are also regularly approached by vendors of security solutions as a target market for their products and are thus kept informed about latest solutions and practices. In-house SOCs rarely publicize what they do and are unlikely to be marketed to by as many vendors as MSSPs. Acquiring knowledge is also an integral part of an MSSP's business strategy as they need to be competitive at all times while an in-house SOC may view the knowledge acquisition exercise as an expense with no immediate benefits.

Security and Reliability: An in-house SOC is a department within an organization, in the event of an APT intrusion, what stops that department's systems from being equally breached and compromised as well? The bulk of an MSSP's infrastructure is external, providing the necessary isolation from being easily compromised while at the same time efficiently handling the tasks of providing security for client infrastructure. MSSP's have no need to share client resources such as printers or even electrical power; making it a more robust and reliable security option should problems arise. An in-house SOC located at a company headquarters may be compromised or rendered ineffective through its reliance on company resources which can be targeted by attackers who have already breached internal systems.

MSSPs with Domestic SOCs as the Best MSS Option

MSSPs vary in terms of characteristics and one of the most important to consider when selecting which MSSP best suits your company's requirements is whether an MSSP has a domestic SOC or not. There are several reasons why MSSPs with domestic SOCs make the best option for network security:

- ✓ **Legal Compliance**
  An MSSP with a domestic SOC will have an adequate understanding of legal issues and compliance requirements in the jurisdiction the client is located. MSSPs with non-local SOCs may be unaware of such issues and requirements leading to problems for the client. MSSPs with domestic SOCs will typically ensure that legal issues and compliance are not a problem in the services they render to their clients because failure to do this will result in problems for them as well.

- ✓ **On-Site Support**
  Certain problems will require on-site support and personnel to handle incidents which have occurred. If an APT incident such as an attempted intrusion of client's servers containing critical financial data, an MSSP with a domestic SOC that can deploy personnel to physically assess the situation is always preferred to one which tells their client: "Send us your logs" or only works on

checking those logs remotely from installed software on the client's network systems in order to make an analysis.

- ✓ **Cost Effectiveness**

  When it comes to matching costs with other benefits, MSSPs with domestic SOCs will be the most cost effective 99% of the time. Hiring MSSPs in Singapore or India may seem cheaper initially until you factor the need for on-site support and the bills that come with footing transatlantic flights and hotel bills. Your clients aren't going to wait for days or weeks, while your MSSP with a non-local SOC tries to find visas and arrange the logistics of getting personnel down to your location to solve an ATP problem.

- ✓ **Convenience**

  Imagine a Texas-based IT company using an MSSP with an SOC in Sydney, Australia. MSSPs with domestic SOCs are simply convenient in all ramifications compared to non-local options. Communication costs between such MSSPs and their clients are minimal. Both parties work in the same or similar time zones and language barriers do not exist.

- ✓ **Security**

  Political dynamics play a role in security. Is your data and network traffic really secure when your MSSP operates SOC facilities in a foreign country? Shouldn't a business in United States be concerned with the security of their network assets if their security provider is an Australian company that makes use of Chinese network engineers? With local SOCs, companies remain better assured of their security and the fact that providers will be subject to local laws in case of any problems.

Conclusion

APTs are a growing problem with evolving dynamics and organizations have to plan for such threats and their effective mitigation by adopting relevant security solutions. Failure to do so may result in anything from loss of reputation to legal repercussions and even organizational collapse. In-house solutions to dealing with such threats are fraught with limitations to their effectiveness such as cost limitations in setting up their SOCs to deal with APTs. As such MSSPs with domestic SOCs provide the best means of mitigating such threats with a suite of security solutions, practices and methodologies that provide several benefits including an increased level of security, cost effectiveness, convenience, compliance with legal issues, frameworks and local regulations among other advantages. As a result of the improved protection offered by MSSPs, organizations can remain rest assured that their network security requirements and functions have been taken care of, while they focus their efforts on the core aspects of their business or organizational responsibilities.

About Proficio and ProSOC

Proficio is a leading provider of networking and security solutions. Enterprises benefit from Proficio's real world experience in delivering large successful projects and rely on our team for security assessments, consulting, project management, implementation, and support.

ProSOC is our security monitoring and analysis service. Using leading SIEM technology, security experts monitor and respond to your security alerts 24x7. Our experts have managed some of the largest and most respected Security Operation Centers in America. Instead of being overwhelmed by alerts, we will identify the short list that matter and then work with you to respond.

For more information see www.proficio.com.

While every effort has been made to ensure the accuracy of the information presented in this publication, Proficio Inc. does not warrant or assume any liability or responsibility for the accuracy, completeness, or usefulness of the information or processes disclosed in its publications or those of its partners. All information is subject to change without notice. Pro**SOC** is a trademark of Proficio Inc. Other product and company names may be trademarks or registered trademarks of their respective owners.

Copyright 2012, Proficio Inc. All Rights Reserved.