

Advanced Persistent Threat

Attacker Sophistication Continues to Grow?

By Jason Andress – ISSA member, Colorado Springs, USA Chapter

This paper discusses what exactly APT is, whether or not it is a real threat, measures that can be implemented in order to mitigate these attacks, and why running out to buy the latest, greatest, and most expensive security appliance might not be the best use of resources.

Abstract

Advanced Persistent Threat (APT) is one of the latest buzz phrases in the security and technology industries. This paper discusses what exactly APT is, whether or not it is a real threat, and includes several examples of recent attacks that have been referred to as APT. Also discussed are the measures that can be implemented in order to mitigate these attacks, and why running out to buy the latest, greatest, and most expensive security appliance might not be the best use of resources.

Both the security community and the national media are actively discussing the issue of Advanced Persistent Threat (APT). Some are of the opinion that APT is simply a new buzz word, created by marketing folks to sell more security products and services, and that APT is the new “Cloud.” Others are of the opinion that APT needs to be taken quite seriously because it represents a new stage in the evolution of threats against both military and civilian organizations.

Whether APT is seen as a new method of attack or merely a convenient handle to describe already existing threats, the consequences of such attacks are real, and the damage done is certainly not imaginary. A defense needs to be mustered

against these attacks, some of which may slip past the standard set of defenses used by many organizations. APT attacks often have specific measures in place to avoid detection, or simply pass undetected due to the use of new attack methods or exploits.

This paper will discuss what exactly APT is, including some examples of attacks that have occurred recently and now appear to fit into the overarching paradigm of APT. Also examined will be some of the tools and techniques used to defend against these attacks, as well as several real world examples of where poor defenses led to major breaches that might have long-term impacts on the companies involved and their customers.

What is APT?

The origin of the term *APT* could come from a number of sources, but two in particular stand out as being the most likely.

The first is the security company Mandiant,¹ which provides a variety of security-oriented services, including services that specifically target response to threats that might be classified as APT. Mandiant also publishes quite a bit of research in this

¹ <http://www.mandiant.com>.

particular area of information security, so it might be logical to conclude that the term originated with them.

The second is the U.S. Department of Defense (DoD). The term APT was reportedly used in this setting as early as 2006.² Although no solid evidence exists publicly to prove either theory, the idea of the DoD creating this term does seem sound. In either case, the term is generally agreed to have existed for quite a few years, and its use has been increasingly frequent, both specifically in the security industry and in the technology industry in general.

As with many terms, APT has taken on a number of slightly-differing definitions and meanings as its usage has evolved. To use the most official definition available at present, one can look to the U.S. National Institute of Standards and Technology (NIST), which defines APT as “an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing/extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.”³

The components of APT

The NIST definition can be broken down into three main components:

- **Advanced:** The attacker makes use of a variety of attack tools, including those that might be considered to be beyond the ken of the average attacker. They might have the resources to develop or buy zero-day vulnerabilities and craft malware, attacks, or attack tools in order to avoid the detection or prevention measures many organizations have in place. This speaks to the “adapts to defenders’ efforts to resist it” in the NIST definition.
- **Persistent:** The attack is being executed in the pursuit of a specific goal, not the result of a random discovery of a vulnerability or to demonstrate expertise just for kicks. The attacks will continue to take place until this goal is achieved, and the attacker will maintain access to the environment. This is echoed in the “pursues its objectives repeatedly over an extended period

of time” and “is determined to maintain the level of interaction needed to execute its objectives” statements from NIST. The attacker will also likely take extensive steps to avoid detection, which is atypical of the activities carried out by a hacker merely taking a system for a joyride, or being destructive for the sake of destruction.

- **Threat:** Threats in APT are not those seen in the form of script kiddies performing port scanning on edge devices, or the odd SQL injection attack coming in through a poorly maintained web application. APT attacks represent a more concerted and directed effort. They are not carried out through happenstance or from a piece of malware hammering away at a system through automation. These types of attack imply both organization and the motivation to accomplish the specific goals of the attacker. Attacks with this degree of focus represent both a higher degree of danger and higher level of difficulty to defend against than typical technical defenses, policies, and awareness programs are scoped to handle.

Is APT a real threat?

Whether one likes the term APT or not, whether agreement is reached on how exactly it is used or not: such attacks are definitely a threat. The following are a few examples of what are generally considered to be APT attacks observed over the last couple years.

- **Operation Aurora** – January 12, 2010 – Google, Adobe, and dozens of other companies came under attack in 2009 and 2010 from sources believed to be in China. The attacks were carried out through spearphishing attacks conducted by sending links over email and Instant Messaging (IM) pointing at a server containing malicious JavaScript. The JavaScript used a zero-day Internet Explorer exploit to download a backdoor and connect the infected machine to a command and control network. The attackers used the compromised systems to mine the environments for intellectual property and to compromise additional systems.⁴
- **RSA** – March 18, 2011 – RSA, a subsidiary of EMC that deals in encryption and security software and devices, was attacked and suffered the loss of information “specifically related to RSA’s SecurID two-factor authentication products.”⁵ These products are used globally to secure access to a wide variety of environments, and RSA has not been forthcoming about what specific data was breached. Attackers initiated the attack by sending RSA’s employees a malicious spreadsheet which contained a zero-day Adobe Flash

2 Cloppert, M. (2009, July 22). Security Intelligence: Introduction (pt 1). Retrieved April 3, 2011, from SANS Computer Forensics and Incident Response with Rob Lee: <http://computer-forensics.sans.org/blog/2009/07/22/security-intelligence-introduction-pt-1>.

3 National Institute of Standards and Technology. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. Gaithersburg, MD: National Institute of Standards and Technology – http://fismapedia.org/index.php?title=NIST_SP_800-39_Appendix_B.

4 McAfee Labs and McAfee Foundstone Professional Services. (2010). Protecting Your Critical Assets: Lessons Learned from “Operation Aurora.” Retrieved April 25, 2011, from McAfee.com: <http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf>.

5 Coviello, A. (2011, March 18). Open Letter to RSA Customers. Retrieved April 25, 2011, from RSA.com: <http://www.rsa.com/node.aspx?id=3872>.

FROM ANALYSIS TO ASSURANCE



With emerging technology and trends creating business risks at an increasingly rapid rate, effective IT audit professionals must be able to move rapidly and accurately when assessing risk. Regis University's online **Master of Science in Information Assurance** degree program will ensure that you have the tools and skills to do so—even as technology continues to change and advance.

The MS in Information Assurance curriculum is modeled on the guidelines and recommendations provided by:

- The Committee on National Security Systems (CNSS) 4000 training standards
- The International Information Systems Security Certification Consortium Ten Domains of Knowledge
- The International Security Audit and Controls Association

Regis University is designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

The program can be taken on campus or completely online



vulnerability, which was subsequently used to install a backdoor on the exploited systems. The attackers were then able to escalate privilege on the systems, use these same credentials to gain access on other systems, and eventually access and exfiltrate the target data.⁶

- **Oak Ridge National Laboratories** – April 21, 2011 – At the Oak Ridge National Laboratories, which conducts research in nuclear energy for national security purposes, attackers sent a spearphishing email to employees about their benefits. The email contained a link to malware that exploited a zero-day Internet Explorer vulnerability. Nearly 60 employees were infected and as much as one gigabyte of specifically targeted technical data was exfiltrated. Several of the other national labs in the U.S. were targeted with the attack at the same time.⁷

The focus of all of these attacks was to retrieve data or intellectual property from the target. In the case of Operation Aurora, some of the companies involved lost portions of the intellectual property on which their businesses are based. In the RSA breach, unspecified data related to the SecurID devices used by thousands of clients was stolen, potentially leading to security issues for many other companies. In the case of the Oak Ridge National Laboratories, the data exfiltrated was not specified, but the focus of the facilities there is on nuclear energy. In any of these cases, the impact of the attacks was grave for the attacked party, and the potential fallout could be much worse.

Moreover, these attacks are only a few of those published recently in the national media. It can be safely assumed that APT attacks are being conducted against considerably more sensitive targets in militaries and governments around the globe. The general public is not privy to the details of such attacks, if they are even aware of their occurrence at all.

Defending against APT

Defending against attacks that are purposefully stealthy and reflect a high level of technical skill can be challenging at best. A great deal of money can be spent buying firewalls, IDS/IPS, monitoring software, and other similar tools, in addition to expending the resources required to implement and manage them, only to have a skilled attacker bypass these measures entirely. This goes double for products advertised to defend against APT specifically. A blog post from the head of the Cisco Computer Security Incident Response Team (CSIRT) sums up the situation nicely: “If anyone attempts to sell your organization on a hardware or software solution for APT, they either don’t understand APT, don’t really understand

how computers work, or are lying – or possibly all three.”⁸ The very definition of APT precludes the easy detection and mitigation of such attacks through the standard measures employed to filter the simpler threats posed by malware and script kiddies. So what can be done to defend against APT?

The Big Picture

Above and beyond the tools normally in place, a major concern should be the other components of the security program, i.e., the “big picture.” Although tools are important and definitely have a place, they can be subverted by a skilled attacker in a variety of ways. Assessments are needed to discover these areas and mitigate them before they are found by an attacker. Ultimately, there are a number of areas in which steps need to be taken in order to defend against APT. These include new tools, methodologies for detecting baseline changes, and increased testing efforts.

Defending against APT: Tools

One of the key steps to defending against the subtle and quiet attacks that are part of APT is to have the proper tools in place. The standard firewalls, IDS, etc., may not be enough to reveal the presence of a highly skilled attacker, let alone enable a response to the attack. Worse yet, many such measures are purchased, plugged in, and perhaps only occasionally updated. All the security in the world can be in place, but if these tools are not actually monitored, they may as well be disposed of to save on the utilities. Attackers count on these tools being simply plugged in and ignored, or not even being capable of detecting the social engineering or zero-day attacks they are using.

The key tools needed, from an APT perspective, are those that enable logging and monitoring to be carried out, and to examine the results of such efforts. Being able to assess the present situation of the hosts, networks, border devices, and the traffic flowing through and to them at any given time is critical, as well as having access to the historical data.

If the capability does not exist to examine the records of what has happened in the environments that are being protected, it becomes very difficult to detect how the attacker gained entry, what attacks were being used, how long the systems had been compromised, and generally what the scope of the incident actually was. With the standard high-level log files found in most organizations, it might not be possible to find some traces of an attack in the firewall, IDS, or host logs. The salient information they contain, if present at all, will be bur-

The key tools needed are those that enable logging and monitoring to be carried out, and to examine the results of such efforts.

6 Rivner, U. (2011, April 1). Anatomy of an Attack. Retrieved April 25, 2011, from RSA.com: <http://blogs.rsa.com/rivner/anatomy-of-an-attack>.

7 Department of Energy-funded lab silenced by APT attack. (2011, April 21). Retrieved April 25, 2011, from SC Magazine – <http://www.scmagazineus.com/departments-of-energy-funded-lab-silenced-by-apt-attack/article/201144>.

8 Reid, G. (2011, March 23). Cisco CSIRT on Advanced Persistent Threat. Retrieved April 3, 2011, from Cisco Blog: <http://blogs.cisco.com/security/cisco-csirt-on-advanced-persistent-threat>.

ied among many irrelevant entries. If proper alerts are not in place, the first indication of the incident may be in the news, and then there will be a scramble to quickly find the specifics of the attack in the relevant systems. Even after an investigation, if the historical information does not exist to track the attack to its beginning, there may be little or no indication of what actually happened.

Defending against APT: Baselines

Developing a baseline of the normal network and host activities can be critical in detecting APT attacks. Such baselines may represent network traffic, host activity, process logs, or a combination of many such measures. When in environments

that are the subject of an attack that is taking great pains to be stealthy, these attacks will not necessarily ring all of the bells and whistles on the firewalls and IDSs that are relied on for protection. A good baseline of normal activity in the environment can enable the detection of activity that is anomalous in the specific environments, where matching against the signature of a specific attack might not. On the negative side of such efforts, poorly tuned detection systems can be equally harmful due to the difficulty of making a de-

termination regarding the legitimacy of the issues discovered.

If what an environment should look like under normal conditions is unknown, then there is little hope of being able to discover anomalous activity until it begins to impact productivity sufficiently as to draw attention.

Baselines also provide a good starting place to mitigate the A in APT. Unfortunately, in the case of dealing with a genuine zero-day attack, by definition, it will be very difficult to defend against. One of the slim threads of hope that does exist is to catch the attack through the use of heuristic detection or by looking for anomalous activity in the environment. These capabilities may enable us to react to the unusual network traffic generated by a Trojan exfiltrating information out through the firewall, a rootkit modifying critical system files, or other such activity. Many vendors, both in the network and in the security appliance areas, are providing products with these sets of features, but it is important to be aware that they are not magic bullets.

Defending against APT: Testing

Testing security footing and defensive measures is one of the primary methods for ensuring that an APT attack can actually be repelled. When looking at APT attacks, the low hanging fruit does need to be taken care of, such as patching, vulnerability assessment, and poor programming practices on websites and applications. A greater effort also needs to be made to find and mitigate the issues that a skilled attacker will use.

Many organizations will say they carry out penetration testing against their systems and environments. Such efforts often comprise little more than running scanning tools such as Nmap and Nessus, and some variety of web scanner, and compiling the reports that result from them into a document. Scanning and report generation are simple, tangible, “hold up the report” methods of demonstrating that “security is important to us.” Sadly, against APT such efforts are not very effective.

In the case of APT, attackers are going to greater lengths to access critical assets than these tools can detect. These attackers will make use of zero-day exploits, social engineering attacks, client-side attacks, and perhaps even physical attacks such as dumpster diving or theft in order to achieve their goals. It is a very rare penetration test indeed that will go to such lengths to find security holes.

Depending on the value of what is being protected, it may be worthwhile to go through the effort, expense, and potential pain required to conduct a very extensive penetration test. In many cases, external testers can better demonstrate what weaknesses an attacker might be able to make use of, as they may not have the blind spots or ideas of how things should look that an internal tester might. Additionally, this is something that needs to be repeated at some regular interval, as most environments are generally not static, and new weaknesses will open up over time, no matter how vigilantly they are maintained.

In order to really defend against attackers that possess the skills to carry out an APT attack, security measures need to be tested from the attacker’s perspective. Half measures here are not enough.

Defending against APT: Security awareness

Many recent attacks, whether they are specifically classified as APT or otherwise, had components to them that were not, and could not have been, mitigated through technical security measures. In both the attacks on RSA and on the Oak Ridge National Labs discussed earlier, spearphishing attacks were used as part of the attack efforts. In combination with the zero-day vulnerabilities used in the attack, these efforts proved highly successful.

Looking at the attacks against Google, RSA, and Oak Ridge National Labs, they all have a common theme: the use of simple phishing and social engineering attacks. These attacks might have been lessened, or potentially even foiled entirely, by a higher level of security awareness on the part of the employees and administrators of these companies. Derailing an APT attack at this early phase through training and security awareness efforts is considerably less expensive and less painful than handling the attack after it has resulted in a breach.

Developing a sense of paranoia regarding social engineering attempts in personnel can go a long way toward defending against such attacks. This may cause some issues internally when attempts are made to carry out administrative activities, ask users for personal information, and other similar ef-

A greater effort also needs to be made to find and mitigate the issues that a skilled attacker will use.

If these efforts can make it possible to repel an APT attack for a very low cost, how can it make sense not to implement them?

forts, but this is an area in which it might be better to have people fail on the side of excessive caution.

While it is very easy to scoff at security awareness and training and apply very limited funding to these efforts from our security budget, its importance is greatly underestimated. If these efforts can make it possible to repel an APT attack for a very low cost, how can it make sense not to implement them? Fostering a strong security mindset in our environments will only help in the long run.

Defending against APT: Defense-in-depth

Lastly, we come to the old saw of defense-in-depth. Although old news, this is still one of the keys to protecting against APT. When one normally examines defense-in-depth, one might think of a simple layering of technical controls that will catch issues if a failure occurs in any particular one area, as shown in Figure 1.

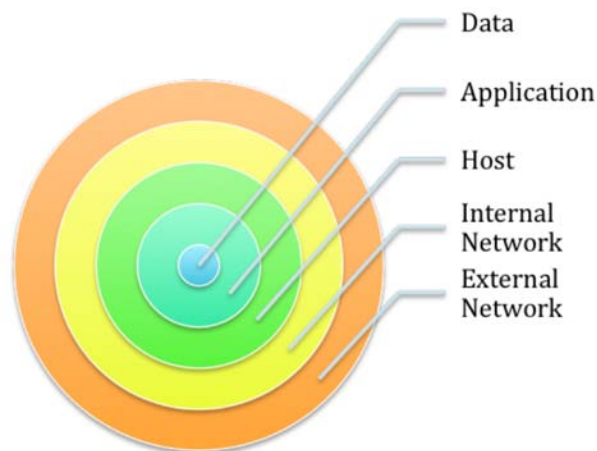


Figure 1 – Defense-in-Depth

In a typical defense-in-depth implementation, these layers might be put in place:

- Firewalls and DMZs on the externally-facing portions of networks
- Additional firewalls and IDS/IPS on the internal portions of networks
- Software firewalls, HIDS/HIPS, and anti-malware tools on hosts
- Access controls and logging on applications
- Encryption on data

These efforts in isolation are not enough to protect critical assets in the face of APT. Attackers read the same books and articles, and attend the same conferences as security professionals; they are able to compensate for many of the measures that might be in place as a defense.

Read the Headlines...



Don't BE the Headlines!

Security Awareness Incorporated delivers a full line of security awareness training tools to help make your employees a front line of defense. Call us today to discuss an effective and affordable program for your organization.

PCI DSS training courses also available!



www.securityawareness.com

1-888-807-0888

sales@securityawareness.com

AWARENESS IS THE KEY TO SECURITY®

ISSA member discounts

A determined attacker will always be able to find a hole that was missed, a new vulnerability opened when patches were last applied, a misconfiguration in a security appliance or a software tools, or will have access to exploits not known to common defenses.

Taking all of this into account, these layers still need to be in place to help protect critical assets against APT. When faced with a skilled attacker, they will not bring out the highly complex attacks and zero-day exploits first thing. This would not only be unneeded effort, but would be exposing “the good stuff” to those that might build defenses against later attacks. This is why attacks such as phishing and social engineering are so common to APT: no greater level of effort is generally needed. Defense-in-depth serves to close up any gaps in defensive measures.

Conclusion

To sum up our defensive efforts:

- **Tools** – Focus on logging and monitoring efforts
- **Baselines** – Be aware of what the environment should look like
- **Testing** – Test security measures like an attacker
- **Security Awareness** – Foster the security mindset
- **Defense-in-Depth** – Close up the gaps

Yes, it is possible to look at APT attacks and assume that highly sophisticated defensive measures will be necessary to fend them off. In some cases, this may even be true. Unfortunately, many of the attacks that have been publicly reported

recently did not begin with this level of sophistication. Attackers are commonly gaining entry through low-level attacks that are easily prevented, and taking the “low and slow” approach once they are in, in order to avoid detection. These efforts are often enough to defeat the defensive and detective measures that are in place in many environments.

The focus on APT defense does not need to be fancy new technologies or high-priced security appliances. It needs to be on doing a better job of implementing the basic security measures and on knowing what the environment should look like, and when conditions deviate from that. As security measures are improved to stop the current generation of APT attacks, new techniques will be developed and may grow to match the hype, but this is not the current state of affairs.

About the Author

Jason Andress, ISSAP, CISSP, GPEN, CEH, is a seasoned security professional with a depth of experience in both the academic and business worlds. In his present position, he carries out global information security oversight duties, performing penetration testing, risk assessment, and compliance functions. Jason has taught undergraduate and graduate security courses since 2005 and holds a Doctorate in Computer Science, researching in the area of data protection. He has authored several publications and books, writing on topics including data security, network security, penetration testing, and digital forensics. He may be contacted at jason.andress@gmail.com.



APT on Connect!

Take a look at what HBGary CEO Greg Hoglund had to say about APT at the February 2010 ISSA Sacramento Chapter meeting!

Join the Discussion
Connect



Kevin
Spease

Advanced Persistent Threat Video

In February, ISSA-Sacramento Valley had a presentation we'd like to share. Our presenter was Greg Hoglund, CEO of HBGary.



accelerated learning • total immersion • immediate results • locations nationwide



All industries need a trained and effective IT workforce to combat hackers, attackers and security threats.

Maintain the integrity of your organization's communications, infrastructure and operations with certifications in Information Security.

As an authorized training partner of (ISC)², Training Camp is the only approved accelerated training provider for CISSP certification on a global scale.

Through our Certified Ethical Hacker and Forensics programs, Training Camp equips information security professionals with the knowledge to identify and correct exploits that make information systems vulnerable to attack.



IT & Management Training

Corporate & Government
Solutions Available



CompTIA A+
CompTIA Network+
CompTIA Security+
CompTIA Linux+
CompTIA Project+



www.trainingcamp.com

CALL 800.698.5501

We have successfully certified over 25,000 industry professionals in the last 10 years and look forward to adding you and your organization to our list of success stories.