Realtime publishers

Advanced Persistent Threats and Real-Time Threat Management

The Essentials Series

Beyond the Hype: Advanced Persistent Threats

sponsored by

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Beyond the Hype: Advanced Persistent Threats

Businesses face a constantly evolving threat landscape. One of the greatest challenges is presented by advanced persistent threats (APTs), which are sophisticated, multi-faceted attacks targeting a particular organization. Mitigating the risk of APTs requires advances beyond traditional layered security to include real-time threat management. This Essentials Series describes the nature of APTs, the risks they pose to businesses, and techniques for blocking, detecting, and containing APTs and other emerging threats. We begin with a pragmatic assessment of the nature of APTs, specifically:

- The nature of APTs today
- The continuously evolving threat landscape
- Elements of APTs
- Changing business practices that compound the problem
- Assessment of potential to control and mitigate the risk from APTs

Clearly, the threat landscape continues to become more challenging. The motivation and means for carrying out attacks on information systems is changing. Determined, committed attackers are employing multiple means to breach security controls. Businesses need to respond in kind with multiple security controls, including real-time monitoring and rapid containment measures.

APTs Today

APTs are sophisticated, multi-faceted cyber-attacks targeted at a particular organization. Such attacks are advanced in terms of the techniques that are applied and the insider knowledge the attackers have about their targets. APTs may use multiple vectors, such as malware, vulnerability scanning, targeted hacking, and malicious insiders to compromise security measures. APTs are long-term, multi-phase attacks. Early stages of an APT attack may focus on gathering information about network configuration and server operating system (OS) details; later, efforts may focus on installing rootkits or other malware to gain control or establish communication with a command and control server. Later stages of an attack may focus on stealing intellectual property by copying confidential or sensitive data.

It is important to understand that APTs are not a new means of conducting an attack and are not something that can be blocked or disrupted once and the problem goes away. APTs are better understood to be more like a cyber-attack campaign than a single type of threat; think ongoing processes. An antivirus program may block malware used in an APT attack but that does not mean the attack is stopped. By its very nature, an APT is an ongoing attack. If one tactic does not work, another will be attempted. Realistically, we should not be thinking in terms of a single countermeasure or even adding more layers to a layered security strategy; rather, we should be thinking of processes that together can block when possible and detect and contain breaches in other cases. It's reasonable at this point to ask, How did we get here?

The Evolving Threat Landscape

Businesses and governments face an evolving threat landscape. What began with attempts to gain bragging rights about defacing a major newspaper's Web site or blocking service to a popular site with a Denial of Service (DoS) attack has shifted to attacking for financial gain. Attackers can realize direct financial gains by fraud and intellectual property theft or indirectly by disrupting a competitor's ability to deliver services or conducting a widely publicized data breach that compromises customer private financial information. Besides the changes in motivations, there are changes in the means of implementing attacks.

Changes in application architectures and the decentralization of core operations create opportunities for attackers. In the past, bank tellers and ATM machines were the only ways to conduct transactions with your bank accounts—now you can do it with your phone. It was not that long ago that talk about retailers invoked images of brick-and-mortar stores and malls; now it is just as likely to bring to mind Web sites that sell everything from books to appliances. The Web applications that provide many of the services businesses offer implement workflows that ultimately lead to back-office systems like inventory management and accounts receivables. These can readily become the target for vulnerability scans, injection attacks, and other probes that reveal information about the application architecture and potential vulnerabilities.

Another factor in the evolving threat landscape is the combination of techniques that may be used. Malware can be used to perform a specific task, such as capture keystrokes, or it may include a communications module that works with a command and control server to download instructions allowing attackers to probe, make discoveries, and adapt their tactics to their findings.

Some of the techniques we see in APTs we have seen in the past with blended threats that used a single attack vector to deliver multiple forms of malicious software. We also see attacks will change in response to countermeasures. When antivirus software successfully detected viruses using pattern-matching techniques, malware developers employed encryption and polymorphic techniques to scramble their code enough to avoid detection. Similarly, if one route of entry in a system is blocked, an APT will look for another. The dynamic nature of APTs is a common characteristic of security threats, but there are characteristics that distinguish APTs from other types of attacks.

Elements of APTs

At the most basic level, there are three characteristics of an attack that make it an APT:

- Motivated by financial gain or competitive advantage
- A long-term, sustained attack
- Targeted at a specific company, organization, or platform

Businesses and governments are the targets of APTs for obvious reasons. Businesses have both financial assets and intellectual property that are highly valued. Governments have faced outside aggression probably for as long as there have been governments—thus, the concept of APTs is in many ways nothing new. What is new is that the means of executing such threats have moved into the realm of networks and applications.

Long-term attacks may continue for days, weeks, months, or even longer. APT attacks can begin with intelligence gathering, which may continue for some time. It may involve both technical and human intelligence gathering. The intelligence gathering efforts can shape later stages of attack, which can be either quick or prolonged. For example, an attempt to steal trade secrets may take months of intelligence gathering about security protocols, application vulnerabilities, and file locations but take only minutes to execute once a plan has been established. In other cases, attacks may continue over longer periods of time. For example, after successfully deploying a rootkit on a server, an attacker may regularly send copies of potentially valuable files to a command and control server for review.

A number of widely publicized APT attacks demonstrate the breadth of means and motivations driving the deployment of APTs:

- The Zeus botnet, for example, started as a platform for attacking financial institutions but was changed to become a framework for other types of APTs.
- The Aurora APT attacked Google and other technology companies seemingly in an attempt to gain access to and possibly modify application code.
- Stuxnet is highly specialized industrial malware that includes a rootkit for a programmable logic controller used in industrial equipment. There has been speculation in the press that Stuxnet was developed by one or more governments.

APTs such as these can take advantage of changes in the way we deliver services.

Changing Business Practices that Compound the Problem

Changes in technology and motivations for attack are only part of the reason APTs have become such a significant threat. The way we architect systems and allow access to business applications is also part of the puzzle.

Consider de-perimeterization. In the past, firewalls would have blocked traffic that was not specifically allowed. As applications advanced, there was more need for more flexible movement of network traffic. Outsiders needed access to internal resources. Developers wrote applications to tunnel blocked traffic over protocols that were allowed through (that is, HTTP). Rather than having a single boundary around all network assets, businesses opened access to more servers and depended on device-based controls and network traffic monitoring.

Another factor that can be exploited by APTs is the increased use of mobile and other unmanaged devices. IT departments do not always dictate the kinds of anti-malware software or access controls that must be in place before a device can be used with internal services. These devices can be used by APTs to stage part of an attack on a business or government network.

Similarly, the increased use of publically available Web applications provides another potential method of attack. For example, an injection attack on a Web application could be used to collect intelligence about the contents of databases as well as the structure of the application.

By expanding employee access to critical information infrastructure, businesses can make it easier and more efficient for employees to perform necessary tasks. However, doing so also increases the potential points of entry for attackers.

Technical and organizational factors are at work with regards to the potential for executing an APT attack. Many of these factors, such as empowering employees and accessing applications from mobile devices, are so beneficial that it is difficult to imagine curtailing them. We can mitigate the risk of APTs without necessarily sacrificing these and other advances.

Pragmatic Assessment of the Potential to Control APTs

From a pragmatic perspective, it is reasonable to assume that APTs will be with us for the foreseeable future. The history of cyber-security is filled with examples of new forms of attacks emerging in response to new types of controls. APTs are long-term process-oriented attacks that are a product of changes in the motivations of attackers and the means available to them to conduct their attacks. Given that APTs are here to stay, what is the appropriate strategy to mitigate the risks associated with them?

We should continue to deploy blocking countermeasures. Anti-malware, encryption, vulnerability scanning, and patching are all good practices. They are not enough, though, to counter APTs, so we should assume there will be a breach. This is not to say there are problems with those countermeasures; this perspective only recognizes the fact that a determined, persistent attacker may find a way to bypass blocking measures.

Working with the assumption that there will be a breach at some point, we must monitor network traffic and host activities in real time. Once a breach occurs, it is imperative to detect that breach as soon as possible and to contain the impact. Containment can include isolating compromised devices, shutting down services, and collecting data for forensic analysis.

Summary

APTs are a class of security threats that pose particular challenges to IT and security professionals. Motivated by financial or other long-term gain and armed with a wide array of malware and hacking techniques, these attackers are willing to spend the time and effort required to breach an organization's defenses. Many of the best practices used in the past are still required today, but as we shall see in the next article, we need to add real-time monitoring and containment techniques to our set of countermeasures.