Realtime publishers

Advanced Persistent Threats and Real-Time Threat Management

The Essentials Series

Planning for Real-time APT Countermeasures

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

Planning for Real-time APT Countermeasures

Advanced persistent threats (APTs) have emerged as a significant threat to businesses, governments, and other organizations. The previous two articles in this series have examined technical aspects of APTs and the challenges to mitigating the risk of an APT attack. APTs are not just malware and they cannot be stopped with just antivirus or perimeter controls. APTs employ social engineering techniques designed to circumvent conventional blocking defenses. Rather than try to outsmart an antivirus program, an attacker gets around the antivirus system. When an employee willingly follows a link in a phishing lure email and downloads what appears to be a legitimate program but is in fact encrypted malware, there is little chance of blocking it. Users have access control rights to download and save applications. Pattern-based detection techniques do not detect encrypted malware. In summary, conventional perimeter and endpoint defenses will not stop an APT.

To be clear, perimeter defenses and endpoint security are necessary to address the risks posed by APTs, but they are not enough. We need real-time threat management. Before deploying such controls, it is advisable to assess the current state of hardware, software, and security controls, prioritize assets, and perform a gap analysis. The results of these efforts will help to plan what proactive controls should be deployed.

This article is organized around basic steps to plan for the deployment of real-time threat management to mitigate the risk of APTs:

- Developing a business case for real-time threat management
- Assessing the current state of readiness for real-time threat management
- Developing a deployment plan

Not surprisingly, some of the recommendations that follow would fit equally well when describing other types of countermeasures. APTs are a collection of well-established techniques used for malicious purposes applied in methodical and comprehensive ways. Countermeasures used in the past can still be useful here. The key distinguishing characteristic of APTs is the speed at which they can progress. This, in turn, drives the need for real-time threat management to complement perimeter and endpoint defenses.

Business Case for Real-Time Threat Management

Executives and IT managers have no shortage of competing demands for resources. Why when a business has invested so much in antivirus, network filtering, identity management, and other security controls should they focus additional resources on real-time threat management? The short answer is because those countermeasures are not enough.

The risk from APTs is well documented. Well-publicized cases, such as Stuxnet, Zeus, and Aurora show that APTs can threaten financial to industrial control systems as well as businesses and governments. The success of these attacks also speaks to the limitations of widely used layered security mechanisms. Again, these mechanisms are essential, but they are not sufficient to mitigate the risk from APTs. APTs are designed to use human and technical resources to collect intelligence, probe for vulnerabilities, and plan multiple-step coordinated actions against a target. The techniques used in APTs are chosen precisely because they can either compromise or avoid such security measures.

The business case justification for real-time threat management is a pragmatic one: APTs exist, organizations with information, financial resources, or intellectual property of sufficient value are potential targets, and commonly used layers security defenses are insufficient to block a sophisticated attack. In addition, once a breach occurs, damaging acts can take place within minutes in many attacks. A well-planned and executed response that requires hours or days to implement may be as effective as no response at all. APTs can operate sufficiently fast enough that automated responses triggered by constant monitoring is required.

Assessing the Current State of Readiness for Real-time Threat Management

Once the business case for deploying real-time threat management has been made, the next step is to assess the current state of readiness. This involves three steps:

- Inventory IT infrastructure
- Prioritize assets
- Perform a gap analysis

The final product of this stage is a description of the potential weak spots in current security controls. Real-time threat management does not replace perimeter or endpoint defenses, it complements them. When endpoint and perimeter defenses are up to date and deployed throughout a network, the attackers have to go to greater lengths to successfully breach the infrastructure.

An inventory of IT infrastructure includes:

- Hardware and network infrastructure
- Software, especially enterprise applications
- Database, content management systems, and other repositories
- Security controls

The purpose of the inventory is to understand what can be a target of an attack or exploited in an attack. Network management and asset management tools are available that can discover assets on a network and produce an inventory of both hardware and software on those systems.

With an inventory in hand, the next step is to prioritize assets. Not all applications, servers, or other infrastructure are created equal. The object is to group assets according to their relative importance so that resources can be allocated to the most important assets first.

We should also understand where there are gaps in the current configuration of layered security controls. In particular, what security controls are missing with respect to blocking, detecting, and containing attacks? Do any of the controls in place support real-time threat management? For example, are log analysis tools capable of operating in a real-time manner? What is the delay between an event being logged and an alert being triggered?

Also consider whether governing policies and procedures are adequate for real-time threat management. They should include specifications for how to respond to a suspicious event as well as who (and what automated controls) should be involved with a response. At the conclusion of these steps, you will be in a position to plan the deployment of a real-time threat management system.

Planning the Deployment of a Real-Time Threat Management System

As you plan your real-time threat management system and evaluate candidate systems, consider three key requirement areas:

- Controls for blocking
- Controls for monitoring
- Containment mechanisms

Controls for Blocking

Blocking network attacks is a complex operation and requires a number of types of controls. Network-level malware detection should be deployed even when antivirus is deployed on endpoints. This type of redundancy is helpful when one of the instances of the control is bypassed or compromised. Vulnerability scanning will help to detect weakness in applications. There are different types of vulnerability scanning. For commercial or open source applications, vulnerability scanning can help to maintain appropriate patch levels and mitigate the risk of attacks using known vulnerabilities. For custom applications, vulnerability scanning can help identify potential points of injection attacks, especially SQL injection attacks. As helpful as vulnerability scanning can be, it does not address the problem of zero-day attacks, which exploit as-yet-publically-unknown vulnerabilities in applications.

Compliance verification procedures should also be implemented. Such procedures can help detect configurations that do not meet minimal security control standards.

Controls for Monitoring

Real-time threat management requires a number of types of monitoring mechanisms:

- Network-level analysis
- Log analysis
- Host intrusion prevention
- Blacklisting of known command and control servers

Network-level analysis demands advanced techniques to adequately identify anomalous patterns without generating too many false alarms. A combination of heuristic rules and statistical pattern recognition techniques may improve overall performance by leveraging the strengths of both while compensating for each technique's weaknesses.

Like network analysis, log analysis must be sufficiently accurate and precise to minimize both false positives and false negatives. It must also scale to meet the volume of logs that are generated in your site, so consider performance and throughput when evaluating this and other analysis tools.

In addition to monitoring network traffic and logs, critical servers should be monitored. By establishing a baseline of activity on a server, host intrusion prevention can help detect anomalous activity on a server, such as unusually high volumes of I/O or changes to application libraries. File integrity checks should also be included in this type of monitoring.

Do not forget to monitor higher levels of network traffic and, in particular, block access to known malicious servers. A real-time threat management application should ideally provide access to up-to-date blacklists on known command and control servers that could be used to direct parts of an advanced attack on your network.

Containment Mechanisms

In the event of a breach, a real-time threat management system should be able to automatically remedy the situation. This can include isolating compromised devices on the network and patching known vulnerabilities. Containment mechanisms should also support risk management procedures, such as generating alerts and escalating notifications according to the severity of events.

Summary

APTs present a new set of challenges from a security perspective. APTs are designed to circumvent commonly deployed security controls. They are also noteworthy for the time that attackers are willing to invest in collecting intelligence and probing for vulnerabilities. Conventional perimeter and endpoint security controls are necessary but not sufficient to prevent the full range of threats posed by APTs. Real-time threat management that entails blocking, detection, and containment can help mitigate the damage that can be done by fast-moving APTs that can progress from breaching controls to compromising systems and data in a matter of minutes.