Realtime publishers

Advanced Persistent Threats and Real-Time Threat Management

The Essentials Series

Need for Real-time Management and Responding

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

Introduction to Realtime Publishers i
Need for Real-time Management and Responding 1
Limits of Standard Endpoint and Perimeter Security Controls 1
Stages of Response to a Breach 3
Ideal and Realistic Assessment of Preventing a Breach 4
Summary 5

Copyright Statement

Need for Real-time Management and Responding

Ideally, we can deploy security controls that would prevent a successful attack by an advanced persistent threat (APT), but we should be pragmatic in our assessment. APTs are multifaceted and although one countermeasure, such as an antivirus system, may block one part of an APT, there can be other elements of the attack that do not depend on detectable malware. Just consider a malicious insider who uses social engineering to discover the password to an administration account of a document management system in order to copy the contents of the repository and mine them for intellectual property. When planning a response to the threat of APTs, we should assume there will be a breach at some time. The overall goal of risk management in this case is to minimize the impact of threats by blocking when possible and detecting and containing when not—to do that, we need real-time monitoring and remediation mechanisms.

This article considers the need for real-time threat management and response, specifically:

- The limits of conventional endpoint and perimeter security controls
- The stages of a response to a breach by an APT
- Ideal and realistic assessments of preventing a breach

As in the first article in this series, a dominant theme is the assumption that we should take the threat of APTs seriously and plan for a breach. This is not to say all businesses will be the victims of an APT attack or that all APT attacks will be successful. From a purely pragmatic perspective, it is better to be prepared for a breach and not suffer one than being unprepared if a breach does occur.

Limits of Standard Endpoint and Perimeter Security Controls

Standard endpoint and perimeter controls can work well to block opportunistic and unsophisticated attacks, but APTs are designed to circumvent these countermeasures. For example, an attack can begin with the identification of employees with access to key information systems followed by spear-phishing and other social engineering techniques. The goal at this stage of the attack is to lure the victim into installing malicious software under the guise of some legitimate operation, such as clicking on a link in an email to access a form or retrieve content.

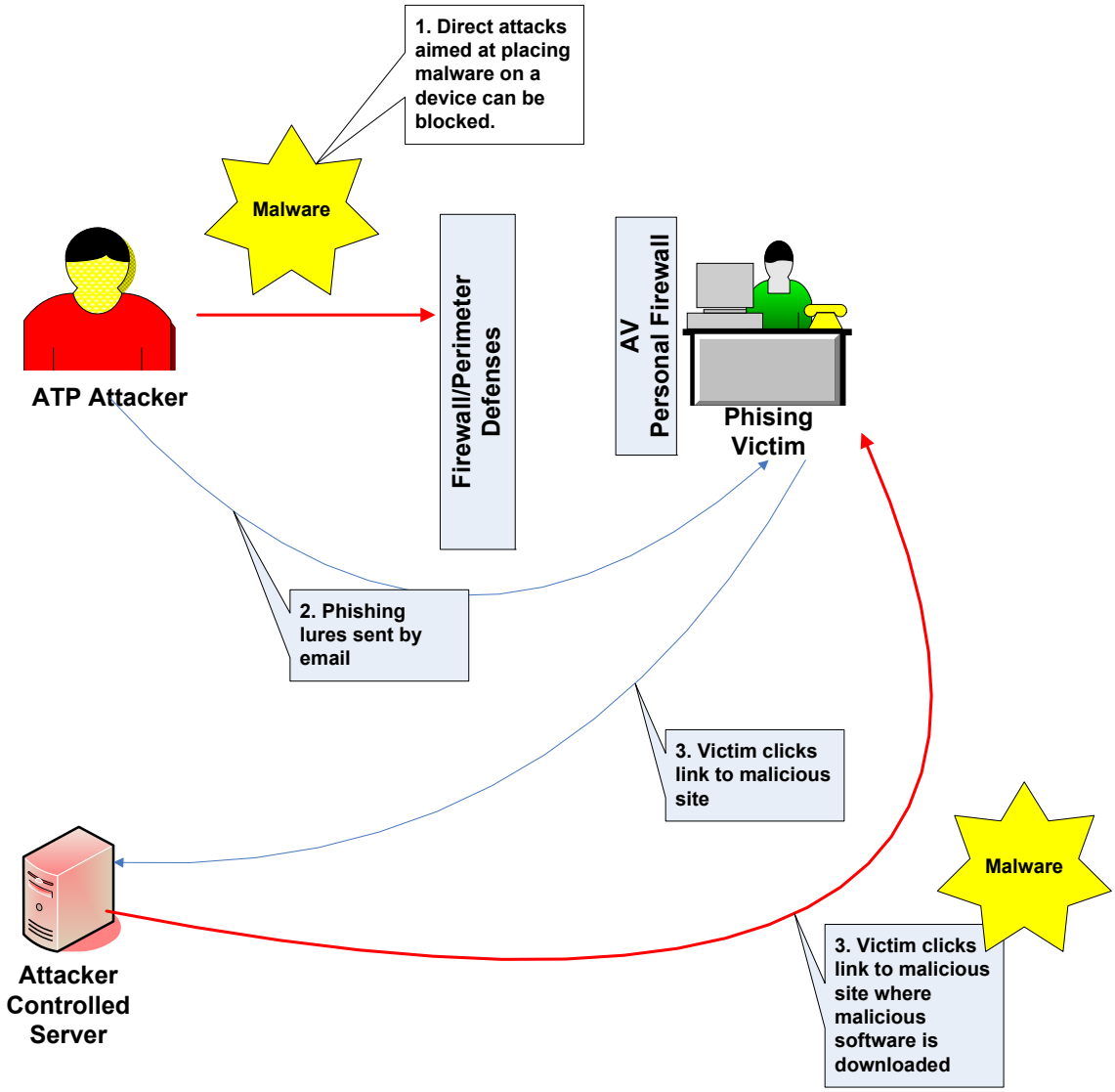

Figure 1: APT attacks use phishing to circumvent perimeter and local device security measures.

Once an attacker has a victim using an attacker-controlled server, the attacker can download malware. Attackers can use encryption and other techniques to avoid detection by pattern-matching–based systems, making it difficult to determine whether the content a user is downloading contains malicious software.

Getting malware into a victim's device is just the first step in an APT attack. The sooner such a breach is detected, the better the chance of containing the damage. This is why we need real-time threat management.

Stages of Response to a Breach

There are four stages to responding to a breach by an APT:

- The initial point of entry
- Compromise of systems and information
- Discovery of a breach
- Containment of a breach

The key stage from a risk management perspective is discovery. Assuming an APT attack has successfully avoided or bypassed perimeter, network, and local defenses, it is then a question of how long the attack continues before it is detected.

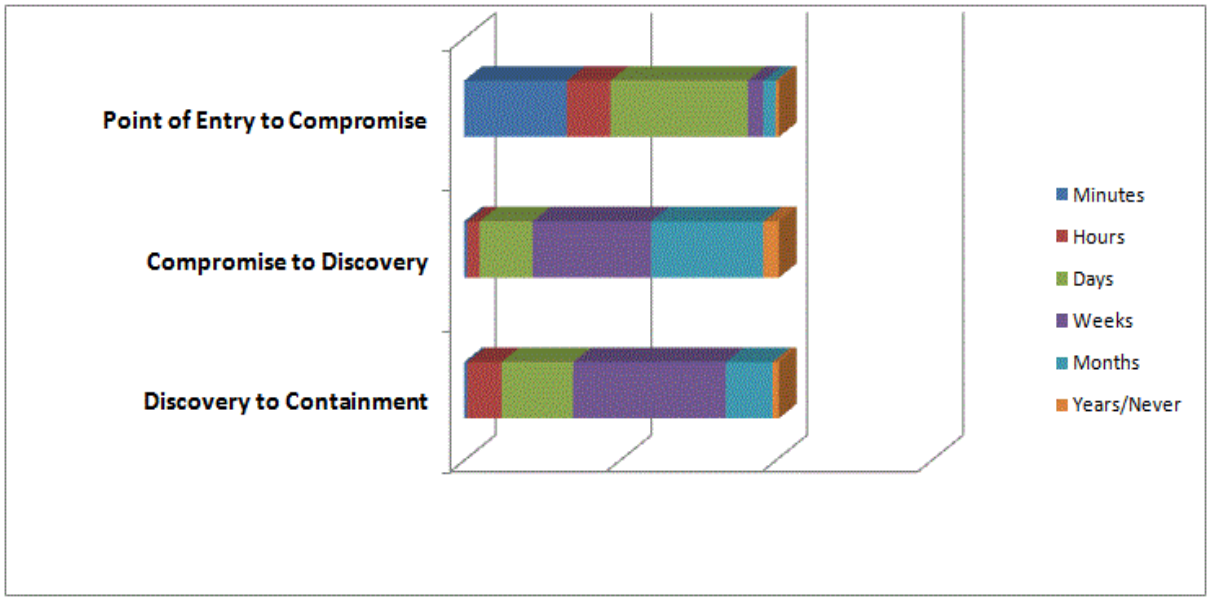

Figure 2: Within minutes, a significant proportion of attacks move from breaching security controls to compromising systems or information. Many of these attacks are not discovered for weeks or months (Source: Verizon 2011 Data Breach Investigations Report).

Two facts about the Verizon data breach study statistics are worth highlighting. First, a significant percentage of attacks lead to a compromise within minutes of a breach. The speed at which APTs operate means that responses that require manual intervention will be too late in many cases. This is why real-time management is required. Often there is no time to waste in initiating a response.

The second fact that we should pay particular attention to is the significant number of attacks that require weeks or months to discover. Until an attack is discovered, it cannot be contained. Some attacks may be point-in-time attacks in which data is stolen or some other malicious act is performed and then the attack terminates. Other attacks could go on as long as they are not detected, for example, streaming customer credit card data to a command and control server 24 hours a day. Active, constant monitoring and analysis is required to discover breaches as soon as possible.

Ideal and Realistic Assessment of Preventing a Breach

As noted earlier, ideally, security controls such as antivirus and perimeter controls would be sufficient to mitigate the risk of a security breach, but it is simply not the case. Attackers understand how perimeter controls and antivirus systems work; and they work well in many cases. The proof of this is the fact that attackers choose to avoid confronting antivirus and perimeter controls by going around them. After all, why bother trying to devise sophisticated malware that can avoid detection when you can use social engineering to trick a legitimate user. Phishing attacks exploit the fact that some users have sufficient access privileges to targeted systems and data. With a sufficiently well-crafted phishing lure, attackers can get these users to unintentionally act as a conduit to reach their target. As humans are sometimes the weakest link in a security strategy, we have to develop strategies that accommodate those weaknesses and mitigate the risks they pose.

A pragmatic approach seeks to prevent a breach and reduce the impact of a breach should one occur. This requires a three-part approach.

First, keep security controls in place and up to date. These include antivirus, encryption, access controls, and vulnerability scanning. Zero-day threats will not be detected by vulnerability scanners, so advanced network monitoring is required to detect and block intrusions. This leads to the second requirement.

Networks and servers should be continuously monitored for signs of a breach. This should include:

- Network traffic analysis
- Server log analysis
- Host intrusion prevention
- File integrity monitoring

Comprehensive monitoring can help detect footprints of an attack, such as an unusual amount of traffic between a server and an external IP address in the middle of the night or the creation of a server account with elevated privileges.

The third requirement is to contain the impact of a breach. Techniques such as virtual patching and automated remediation can disrupt an attack and prevent the vulnerability that enabled the attack from being exploited again. The specific steps that should be executed in order to contain a breach should be defined in a set of risk management procedures.

The overall objective here is to reduce the time between the point of entry of an attack and the point of containment. Real-time threat management, which includes both monitoring and response mechanisms, is required to address the threats posed by APTs. The value of real-time threat management lies in the value of data *not* lost or compromised because containment occurs faster than it would have if manual procedures were required to discover and contain the attack.

Summary

Commonly used endpoint and perimeter security controls are insufficient to block APT attacks. Phishing and other forms of social engineering allow attackers to circumvent those controls by luring users with sufficient access controls into inadvertently being used in the attack. APTs can rapidly move from the point of breach to the point of compromise, often within minutes. Manual intervention to detect and contain APT attacks is often too slow to be effective. Real-time threat management is needed to respond as rapidly as the APT attack progresses.