Definitive Guide™
to
Advanced Threat Protection

Defeating Your Cyber Enemies With Unified Advanced Threat Protection Defenses

Steve Piper, CISSP

Compliments of:

FireEye™

About FireEye

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise combined with the most aggressive “boots on the ground” helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you’ll detect attacks as they happen. You’ll understand the risk these attacks pose to your most valued assets. And you’ll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,200 customers across more than 60 countries, including more than 130 companies in the Fortune 500.

Definitive Guide™
to
Advanced Threat Protection

Defeating Your Cyber Enemies With Unified Advanced Threat Protection Defenses

Steve Piper, CISSP

CYBEREDGE
PRESS

Definitive Guide™ to Advance Threat Protection

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9888233-6-5 (paperback); ISBN: 978-0-9888233-7-2 (eBook)
Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from FireEye: Michael Evans, Ken Brown, Justin Harvey, Alex Lanstein, David Merkel, Bill Cantrell, Hari Kosaraju

Table of Contents

Introduction vii
- Chapters at a Glance vii
- Helpful Icons viii

Chapter 1: Exploring Cyberthreat Trends and Motives 1
- Reviewing Recent Trends 2
  - Client-side attacks 2
  - Customized attacks 2
  - Socially engineered attacks 2
  - Bring-your-own-device (BYOD) policies 3
- Analyzing Attackers' Motives 3
  - Cybercriminals 3
  - State-sponsored threat actors 4
  - Hacktivists 5
- Making Headlines 5
  - Commercial attacks 6
  - Government attacks 6

Chapter 2: Understanding Advanced Threats 7
- Reviewing Modern Cyberthreat Tactics 8
  - Basic threat tactics 8
  - Advanced threat tactics 10
- Understanding Targeted Attacks 12
- The Life Cycle of a Targeted Attack 13
- Why Traditional Security Is Not Enough 15
  - Bypassing signature-based defenses 15
  - The dissolving network perimeter 16
  - Once compromised, the clock is ticking 16
- Introducing Advanced Threat Protection 17

Chapter 3: Securing the Perimeter from Advanced Threats 19
- What the World Really Needs 20
  - Signature-less malware detection 20
  - Protection — not just detection 20
  - Multi-stage protection architecture 21
  - Response capability 21
  - Dynamic global threat intelligence 22
- How It Works 22
  - Key components 22
  - Detecting web-based threats 26
  - Preventing email threats 27
  - Mitigating mobile threats 27
  - Uncovering threats within files at rest 28
- Exploring Key Features 28
  - Virtual execution of suspicious objects 29
  - Fast-path blocking 29
  - Malicious file quarantine 29
  - Custom rule support 30
  - Malware intelligence sharing 30
  - AV suite integration 31

Dashboard 31
Reports 31
Alerts 32
Role-based access control 32
Third-Party Integration 33
Security information and event management (SIEM) 33
Network forensics 33
Network access control (NAC) 33
Incident management 34

Chapter 4: Strengthening Endpoint Advanced Threat Defenses ... 35

Benefits of Host-based Advanced Threat Protection 36
Eliminating blind spots 36
Validating when attackers are present 36
Investigating and triaging alerts 37
Containing compromised devices 37
How It Works 37
Key components 38
Validating attacks with indicators of compromise 38
Containing compromised endpoints 39
Determining what happened 39
Sharing intelligence with other security platforms 39

Chapter 5: Investigating Advanced Threats with Network Forensics 41

Exploring Network Forensics 42
What is network forensics? 42
Benefits for security analysts 42
Benefits for network operations 44
How It Works 44
Key components 44
Disrupting the attack life cycle 46

Chapter 6: Unifying Advanced Threat Protection Defenses 47

The Case for a Unified Approach 48
The dissolving perimeter 48
New web-based tactics always get through 48
Time is of the essence 49
Not all internal hosts are monitored 49
How It Works 50

Chapter 7: Selecting a Complete Advanced Threat Protection Solution 53

What to Avoid 54
Important Buying Criteria 55
Services Considerations 61
Design and deployment 61
Incident response 61
Managed services 62

Glossary 61

Introduction

Despite billions spent annually on traditional perimeter- and endpoint-based security defenses, advanced threat actors cause enterprises and government agencies to make headlines every day — for all the wrong reasons.

So, why are traditional security defenses so ineffective? And why does it seem like the bad guys always have the upper hand? Isn't there anything else we can do to stop them?

Thankfully, recent innovations in perimeter- and host-based advanced threat protection technology, combined with new network forensics capabilities, are finally giving enterprise IT security teams the edge they need to defeat their cyber adversaries. And this book will show you how.

If you're charged with securing your network from advanced threats, and remediating attacks that eventually get through, then this is one book you simply can't afford to miss.

Chapters at a Glance

Chapter 1, "Exploring Cyberthreat Trends and Motives," reviews major trends over the past half-decade that have dramatically changed the way cyberattackers think and operate. We'll also explore major commercial and government cyberattacks that have made recent headlines.

Chapter 2, "Understanding Advanced Threats," distinguishes between everyday basic threats and sophisticated, highly customized advanced threats. This chapter also describes why traditional security defenses are not enough and how targeted attack campaigns work.

Chapter 3, "Securing the Perimeter Against Advanced Threats," reviews the attributes of an "ideal" perimeter-based advanced threat protection solution and then describes how such a solution detects threats within web traffic, email messages, mobile communications, and files at rest.

Chapter 4, "Strengthening Endpoint Advanced Threat Defenses," describes how host-based advanced threat protection software mitigates attacks on endpoints. We'll review key components and explore how the solution works.

Chapter 5, "Investigating Advanced Threats with Network Forensics," describes how to use high-performance packet capture appliances to investigate and remediate advanced threats.

Chapter 6, "Unifying Advanced Threat Protection Defenses," builds a case for integrating perimeter- and host-based advanced threat protection with network forensics for rapid threat identification and remediation.

Chapter 7, "Selecting a Complete Advanced Threat Protection Solution," describes exactly what to look for — and, more importantly, what to avoid — when evaluating full-featured advanced threat protection solutions. Vendor-delivered service offerings are also explored.

Glossary provides handy definitions to key terminology (appearing in *italics*) used throughout this book.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

Exploring Cyberthreat Trends and Motives

In this chapter

- Understand recent trends that have shifted the way advanced threat actors approach cyberattacks
- Analyze the motives of three primary classes of threat actors who perpetrate advanced attacks
- Review summaries of recent commercial and government data breaches that have made international headlines

Defending cyberthreats has always been a game of cat and mouse. Just when security experts think they've got a particular class of attack licked, the bad guys come out with a new and better way of penetrating enterprise defenses.

Sometimes it seems like today's cyberattackers have the upper hand and there isn't much we can do about it. Well, if that's your perception, I have promising news for you.

Innovations in advanced threat protection defenses are finally giving the good guys the upper hand by equipping them to not only detect and prevent advanced threats, but to contain and remediate them at the endpoint as well.

This book is dedicated to all the devoted IT security professionals on the front line of defending against cyberthreats. This book not only describes the components of modern perimeter- and endpoint-based advanced threat protection solutions, but also tells you how to get started.

In this chapter, I set the stage for how cyberthreats have evolved by describing recent trends that have changed the way attackers operate. Next, we'll dive into the motives of the

three types of threat actors who target enterprise networks. And last, we'll review recent headlines about successful commercial and government data breaches to reinforce how big a problem advanced threats have become.

Reviewing Recent Trends

When it comes to cyberthreats, the only constant is change. Our cyber enemies are continually inventing new and clever ways to penetrate our security defenses. Following are a few recent trends that have influenced modern cyberthreat techniques.

Client-side attacks

Over the past half-decade, the information security industry has witnessed a paradigm shift in the way attackers target enterprise networks. Rather than attempting to infiltrate well-guarded servers of interest directly (by exploiting server-side vulnerabilities), hackers have realized that endpoints are far easier to compromise and can be used as a launching pad for penetrating targets of interest. (See "The Life Cycle of a Targeted Attack" section in Chapter 2.)

Customized attacks

To evade traditional, signature-based network and endpoint defenses — such as next-generation firewalls (NGFW), intrusion detection and prevention systems (IDS/IPS), and antivirus (AV) — attackers customize their attacks for each target. Attackers can easily alter *malware* using off-the-shelf exploit kits such as Blackhole, Phoenix, Kein, Sakura, and others. Once altered, newly created malware can sail past rudimentary signature-based defenses as if they weren't even there.

Socially engineered attacks

Another significant trend among sophisticated attackers is leveraging social media websites — such as LinkedIn and Facebook — to identify workers employed by the same company or government agency. The threat actors then create personalized spear phishing emails that spoof the sender's email address so it appears to the unsuspecting recipient that the email comes from a trusted colleague. A few mouse clicks

to open an infected email attachment or malicious website link are enough to compromise the victim's computer.

Bring-your-own-device (BYOD) policies

An emerging trend in enterprise computing environments is the adoption of internal *BYOD* policies that allow employee- and guest-owned computing devices — such as unmanaged laptops, tablets, and smart phones — to connect to the production network and access confidential applications and data. Although BYOD policies may improve employee productivity and increase morale, they also dramatically increase network security risks by providing fresh targets for advanced threat campaigns.

In the 2014 Cyberthreat Defense Report published by the IT security research firm CyberEdge Group, survey results from more than 750 security practitioners from North America and Europe forecast a rise in BYOD policy adoption from 31 percent in 2014 to 77 percent in 2016. Clearly, BYOD is here to stay.

To download a copy of the 2014 Cyberthreat Defense Report, connect to www.cyber-edge.com/2014-CDR.

Analyzing Attackers' Motives

Now that you've got a handle on some of the trends affecting the cyberthreat landscape, let's shift gears and talk about the three types of threat actors who perpetrate advanced attacks — cybercriminals, state-sponsored threat actors, and hacktivists.

Cybercriminals

Cybercriminals are, by far, the most common type of cyber adversary facing commercial enterprises today. Simply put, cybercriminals are motivated by financial gain. They're looking to penetrate your defenses to compromise endpoints in hopes of gaining a foothold on the network so they can steal confidential data (e.g., credit card numbers and other personally identifiable information).

State-sponsored threat actors

State-sponsored threat actors are individuals or groups employed by nation states to hack into foreign commercial and government networks for espionage. Instead of searching for credit card numbers, they're seeking intellectual property, military plans, software source code, or anything that gives their employers a tactical or economic advantage.

Although not all attacks from state-sponsored threat actors are from China, that nation is most often cited in the news for *advanced persistent threat* (APT) attacks — especially following Mandiant's groundbreaking APT1 report (see "Exposing China's cyber espionage program" sidebar).

Exposing China's cyber espionage program

Mandiant (www.mandiant.com), a FireEye company, is a leader in endpoint-based advanced threat protection solutions and a leading provider of incident response services. In 2013, the company published a groundbreaking report called "APT1: Exposing One of China's Cyber Espionage Units," which provides never-before-seen insight into China's alleged cyber espionage program.

Over the past decade, Mandiant has investigated hundreds of security breaches around the world. The company has tracked more than 20 APT groups with origins in China, but the most active group by far has been dubbed by Mandiant as "APT1."

According to Mandiant's report, APT1 is allegedly tied to the 2nd Bureau of the PLA General Staff Department's 3rd Department, which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. APT1 is situated in a 130,663-square-foot, 12-story facility that is believed to employ hundreds of Chinese cyberattackers. The report suggests that APT1 has established a minimum of 937 *command-and-control (CnC) servers* hosted on 849 distinct IP addresses in 13 countries. The majority of these IP addresses were registered to organizations in China.

To download a copy of this report, connect to Mandiant's website at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Also fueling the case against China is the May 2014 indictment of Chinese military officers charged with hacking U.S. companies to steal industry secrets about nuclear and solar power initiatives. It's the first time the U.S. government has formally accused another nation of using the Internet to break into U.S. businesses.

A federal grand jury in Pennsylvania indicted five men — depicted in the "Wanted by the FBI" poster below (see Figure 1-1) — on 31 counts of espionage. These men are reportedly members of a People's Liberation Army entity known as Unit 61398.

Figure 1-1: FBI "Wanted" poster depicting five alleged Chinese hackers

Hacktivists

Hacktivists are attackers who attempt to break into or disrupt computer networks for politically or socially motivated reasons. For example, a hacktivist might leave a conspicuous message on the home page of a website that gets a lot of traffic or embodies a point of view the attacker opposes.

Making Headlines

Hardly a day goes by without news about a commercial or government cyberattack. I could fill this entire book with examples from the past year alone. But the following sections highlight some of the more recent high-profile attacks that have made international headlines.

Commercial attacks

- ☑ **P.F. Chang's** (June 2014): P.F. Chang's CEO, Rick Federico, issued a statement acknowledging a large-scale data breach, discovered on June 10, 2014, which resulted in the theft of an untold amount of credit and debit card data. Reports suggest that the breach began on September 18, 2013 and will likely affect up to 7 million cardholders who visited the company's 211 restaurants during that nine-month span.
- ☑ **AOL** (April 2014): Over 2.4 million email addresses, postal addresses, and address books were compromised. Hackers sent spoofed emails from about 2 percent of AOL email accounts.
- ☑ **Neiman Marcus** (January 2014): Information from over 1.1 million credit cards was stolen as a result of "RAM-scraping malware" installed on point-of-sale terminals.
- ☑ **Adobe** (October 2013): Hackers compromised source code to Acrobat, ColdFusion, and ColdFusion Builder, and stole Adobe IDs and passwords for more than 152 million users — including me!

Government attacks

- ☑ **U.S. Department of Veterans Affairs** (January 2014): Medical and financial records from at least 5,300 U.S. military veterans were exposed after a bungled software update.
- ☑ **Finnish Government** (November 2013): A Finnish Foreign Service Internet network data breach caused by a Red October malware variant targeted classified communications between officials of Finland and the European Union.
- ☑ **U.S. Federal Reserve** (February 2013): A system vulnerability enabled outside exposure to a contact database designed to facilitate communication between banks. Email addresses, phone numbers, and other contact information were stolen and published. The hacktivist collective called "Anonymous" claimed responsibility for the attack.

Chapter 2

Understanding Advanced Threats

In this chapter

- Distinguish between basic and advanced tactics used by attackers
- Understand why traditional security defenses are inadequate for mitigating advanced attacks
- Explore the life cycle of a targeted attack

Over the last decade, threat actors have grown in both number and sophistication. A decade ago, you could count on your perimeter *intrusion prevention system* (IPS) and your host-based antivirus (AV) software to defend your organization against data breaches. These days, malware associated with advanced threat campaigns sails past these traditional security defenses like they aren't even there.

But what makes advanced attacks unique? And why are traditional defenses so inept at detecting them?

This chapter explores the key differences between basic and advanced tactics used by threat actors and describes why traditional security defenses fall short. It also explores the life cycle of targeted attacks so you can better recognize their telltale signs.

This chapter concludes by introducing the key components of modern advanced threat protection solutions. It describes why each of the components is pivotal to mitigating threats at both the perimeter and on endpoints.

Reviewing Modern Cyberthreat Tactics

Attackers use a range of tactics to achieve their objectives. In most cases they will take the path of least resistance. That means using tactics that are good enough to get them in the door. When the target is more heavily fortified, attackers typically employ more-advanced tactics.

Let's dive in and understand the range of tactics used by today's threat actors.

Basic threat tactics

Simply put, *basic threat tactics* are easier for traditional perimeter- and host-based cybersecurity defenses to detect. These threats target known operating system and application vulnerabilities and can often be identified with pattern-matching signatures.

Let's proceed by exploring some of these basic threat tactics that have been a nuisance to IT for many years.

Worms, Trojans, and viruses

A *worm* is a malware program that replicates itself — typically through vulnerabilities in operating systems — over a network in order to propagate. Worms typically harm networks by consuming bandwidth, but also provide a "lateral" attack vector that may infect supposedly protected internal systems or exfiltrate data. Unlike a computer virus, a worm can propagate from host to host on its own.

A *Trojan* (or *Trojan horse*) typically masquerades as a helpful software application, with the ultimate purpose of tricking a user into granting access to a computer. Trojans may self-replicate within the infected system, but cannot propagate to other vulnerable computers on their own; they typically join networks of other infected computers (called *botnets*; see next section) where they wait to receive further instructions, and into which they submit stolen information. Trojans may be delivered by means of spam email or social media, or may be disguised as a pirated installer for a well-known game or application.

A *virus* is malicious code ranging in severity from mildly annoying to completely devastating. By attaching itself to a program or file, it spreads from one computer to another, leaving infections as it travels. However, unlike a worm, a virus can't travel without human action.

Spyware and botnets

Spyware is software that gathers user information through an Internet connection without the user's knowledge, usually for advertising purposes (called adware, which displays pop-up ads), but sometimes to steal confidential information such as usernames, passwords, and credit card numbers. Spyware applications are typically bundled as a hidden component of shareware or freeware programs downloaded from the Internet. Once installed, the spyware monitors user activity and then covertly transmits that information in the background to someone else.

A *botnet* is a collection of compromised Internet-connected computers on which malware is running. Each compromised device is called a *bot* (or zombie), and the human controlling a botnet is called the bot herder (or botmaster). Command and control of a botnet typically involves web servers (called *command-and-control* or *CnC* servers) operated for the specific purpose of controlling bots, though some older botnets are directed by the bot herder using Internet Relay Chat (IRC). Bots are often used to launch *denial-of-service attacks*, relay spam, store stolen data, and/or download additional malware to the infected host computer.

Phishing attacks

Social engineering attacks — such as phishing and baiting — are extremely common. As I discuss in Chapter 3, these attacks, when successful, can lead to much broader, more-sophisticated cyberattacks.

Phishing is an attempt to acquire information (and, indirectly, money) such as usernames, passwords, and credit card information, by masquerading as a trustworthy entity in email communication. After clicking on a (seemingly innocent) hyperlink, the user is directed to enter personal details on a fake website that looks and feels almost identical to the legitimate one.

Unlike *spear phishing*, which is a tactic used for *advanced targeted attacks*, phishing is opportunistic. A single, generic email is sent to hundreds or sometimes thousands of recipients.

Baiting occurs when a criminal casually drops a USB thumb drive or CD-ROM in a public area like a lobby, parking lot, or cyber cafe. This drive or disc is labeled with words such as "executive compensation" or "company confidential" to pique the interest of whoever finds it. When the victim accesses the media, it installs malware on his computer.

Advanced threat tactics

In contrast to some of the basic tactics outlined above, *advanced threat tactics* are difficult – if not impossible – for traditional signature-based defenses to detect. They are often highly customized and designed to compromise specific targets. And although most tactics — basic and advanced — exploit known vulnerabilities, some advanced tactics are crafted to exploit vulnerabilities that are unknown to the general public. (More on that later.)

Let's now explore various types of advanced tactics that are keeping security professionals lying awake at night.

Customized malware

The simplest way to evade traditional security defenses is to customize malware for each attack. This is surprisingly easy. By changing a single parameter using an off-the-shelf exploit kit, attackers can customize malware to exploit a known vulnerability in such a way that makes it virtually undetectable by threat-based signatures.

Drive-by downloads

These days, you don't have to actively download a file from the Internet to become infected with malware. Simply visiting or "driving by" a website without stopping to click on anything can result in a compromised endpoint.

A *drive-by download* usually exploits an unpatched web browser. Sometimes websites designed to deliver drive-by payloads are owned and maintained by a cybercriminal. Other times, attackers compromise perfectly legitimate websites to increase the chances of victimizing a host.

Watering hole attacks

A *watering hole attack* is performed when an attacker compromises a website that is frequently visited by users of an organization that he or she is targeting. The attacker inserts code into the website that results in malware infection. Once infected, the user's host will typically connect to a CnC server to obtain further instructions by the attacker.

Spear phishing attacks

A spear phishing email is just like a phishing email except it is carefully constructed to target an individual person or group of people employed by an organization of interest. Attackers frequently use social media sites, such as LinkedIn and Facebook, to construct carefully crafted emails that appear to be sent from trusted friends or colleagues. Opening a malware-infected email attachment or clicking on a malicious embedded link can cause the victim's computer to become compromised.

Spear phishing is one of the most common tactics attackers use to initiate an advanced targeted attack.

Zero-day attacks

A *zero-day attack* occurs when an attacker exploits an operating system or application vulnerability that is not generally known to the public. This tactic gets its name from the fact that the attack was launched on (or increasingly before) "day zero" of public awareness of the vulnerability — and, in many instances, before the vendor itself was even aware. In some instances, the vendor is already aware of the vulnerability, but hasn't disclosed it publicly because the vulnerability hasn't yet been patched.

Zero-day attacks are extremely effective because they can go undetected for long periods (usually several months but sometimes a couple of years), and when they are finally identified "in the wild," patching the vulnerability can still take days or even weeks.

Understanding Targeted Attacks

Attackers often use a combination of the aforementioned tactics as part of a *targeted attack*. Here, an advanced threat actor, such as a nation-state or a well-resourced cybercriminal group, carefully constructs a multi-pronged campaign with a specific organization and objective in mind. Once executed, the campaign is designed to penetrate an unsuspecting user's host or mobile device in an attempt to gain a foothold on the network so that the attacker can steal the data he is targeting.

For example, a threat actor may target a specific group of users at an organization with spear phishing emails that contain custom malware that exploits a zero-day operating system vulnerability.

Targeted attacks, in particular, have captured headlines in recent years, largely as a result of campaigns by *advanced persistent threat (APT)* actors originating from China. But if you think that all APT attacks originate from the Far East, you're certainly mistaken. (See "Dispelling APT myths" sidebar for more information.)

Dispelling APT myths

APT is one of the most widely used — and frankly, misunderstood — acronyms in the IT security industry. Inaccuracies about APT attacks nearly equal correct information. Let's take this opportunity to dispel some of the more common APT myths.

Myth #1: All targeted attacks are APT attacks. APT is a specific term for targeted attacks committed by state-sponsored threat actors as part of cyber espionage campaigns. APT attacks are never perpetrated to steal credit card numbers, for example.

Myth #2: All APT attacks originate from China. Although China deserves much of the credit for the hype associated with APT attacks, the truth is that more than a dozen countries — including Russia, Israel, Iran and even the United States — have been publicly implicated in initiating APT attacks against other countries.

Myth #3: Only governments are the targets of APT attacks. This couldn't be further from the truth. There are countless examples of governments attacking commercial entities for political gain. Recent examples include China's alleged attacks against *The New York Times* and Westinghouse.

The Life Cycle of a Targeted Attack

To better understand how to protect against advanced threats, let's enter the mind of a cybercriminal to explore the five stages of a typical targeted attack campaign.

Stage 1: The initial compromise

Unlike cyberattacks from a decade ago, most targeted attacks begin with the exploitation of an end-user device. These days, most headline-making data breaches begin following receipt of a spear phishing email that tricks an unsuspecting user into clicking on a malware-embedded attachment or a link to a malicious website.

Stage 2: Establishing a foothold

Once a user's endpoint device has been compromised, a *remote administration tool/Trojan*, or RAT, is executed behind the scenes. The RAT "phones home" by initiating an outbound connection between the infected host and a CnC server operated by the cybercriminal. Sometimes the CnC protocol is sent in the clear while other times the command channel is encrypted. Once this is completed, the attacker has established full control over the infected host and a foothold on the network.

Stage 3: Escalating privileges

After establishing a foothold, the cybercriminal waits patiently until a user enters valid administrative credentials into the compromised host. All keystrokes are logged by the RAT using a keylogger function and uploaded to the CnC server for analysis.

In many instances, the stolen credentials are insufficient for compromising servers of interest. Thus, savvy threat actors target Active Directory servers (or other user directories) to exfiltrate usernames and password hashes for all user accounts for offline cracking. Passwords of eight characters or fewer can usually be revealed within a few hours (or sometimes minutes) using modern password cracking applications. Longer passwords are typically less vulnerable.

Stage 4: Moving laterally

With escalated privileges in hand, attackers move laterally across the network until they locate servers of interest. Lateral movement does not necessarily involve the use of tools other than those already supplied by the compromised host operating system, such as command shells, NetBIOS commands, VNC, or Windows Terminal Services used by network administrators to service remote hosts.

A common and easy way an attacker can move laterally in a Microsoft Windows environment is by using stock Windows commands, such as NET.EXE (to map a drive) and AT.EXE (to schedule a command). To move laterally, an attacker can map a drive to another Windows machine with NET.EXE, copy the malware to the drive, and then remote execute it with AT.EXE.

Once the ultimate target has been identified and adequate logon credentials have been acquired, the attacker's patience and determination begin to pay off.

Stage 5: Data theft

Once they have identified target servers, attackers determine the best course to steal data. Veteran cybercriminals typically exfiltrate data in "chunks" — perhaps in increments of 50-100 megabytes. Our attacker may decide to group files or records together into compressed, password-protected RAR files in case they're discovered by IT personnel during transit. Or sometimes the attacker will use an XOR-byte encrypted outbound stream to evade signature based detection (as well as data loss prevention schemes).

Attackers cover their tracks

Both during and after the attack, the most advanced threat actors try to avoid leaving any clues that a data breach ever took place. Thus, they employ a variety of tactics to minimize the risk of post-breach detection, including:

- ☑ Planting malware or launching distributed denial of service (DDOS) attacks to distract the IT security staff and keep them busy doing other things.

- ☑ Accessing network file shares, which are relatively unprotected and completely wiped only in extreme circumstances.
- ☑ Deleting the compressed files after they've been extracted from the staging server.
- ☑ Deleting the staging server if it's hosted in the cloud or taking it offline if under control of the attacker.
- ☑ Uninstalling malware at the initial point of entry.
- ☑ Using command line tools (WEVTUTIL.EXE, for example) to erase log traces.

Why Traditional Security Is Not Enough

As illustrated in this section, there are multiple reasons why traditional security defenses are inadequate for detecting advanced threats.

Bypassing signature-based defenses

Malware associated with targeted attacks is highly customized. Rudimentary IPS, AV, and other traditional, signature-based defenses can't possibly detect newly created malware — because no signature exists to defeat it.

Telltale signs of a targeted attack

Although targeted attacks are extremely difficult to detect at all stages of their life cycle, certain telltale signs may indicate a network compromise:

- Increase in elevated logons late at night
- Large, unexpected flows of data originating from within the network, particularly on non-standard ports
- Large chunks of data appearing in places where they should not exist
- Abnormal event log entries of AV and firewall stop and restart commands

The dissolving network perimeter

The network perimeter has rapidly declined as an entry point for advanced threats for more than a decade — ever since laptops were used to access corporate applications and data. Today, workers are using mobile devices — such as tablets and smartphones — to gain unprecedented access to information, fueled by the adoption of well-intentioned BYOD policies. Unfortunately, mobile devices are now the "Wild West" for cyberattackers. Attackers are bypassing perimeter defenses each time a user carries an exploit right through the office front door.

Once compromised, the clock is ticking

Savvy security professionals know that despite all efforts to mitigate cyberthreats, their networks will ultimately be compromised. IT security teams are no longer judged solely on their ability to prevent threats, but also on their capacity to contain and remediate them. After all, once your network has been compromised, the clock is ticking.

As you'll discover in Chapter 5, network forensics technology has now achieved "must-have" status for every serious enterprise incident response team.

Introducing Advanced Threat Protection

At this point, you should now have a deeper appreciation of the challenges facing IT security professionals. Trying to combat today's advanced threats using traditional security products is like showing up to a gunfight with a pocketknife. You don't stand a chance.

Fortunately, innovations in advanced threat protection technologies are affording IT security professionals new capabilities to detect, mitigate, and remediate advanced threats at all stages of the targeted attack life cycle — before, during, and after the attack.

Specifically, three advanced threat protection technologies are at the heart of this new strategy and are the combined focus of the remainder of this book. These technologies are:

- ☑ Perimeter-based advanced threat protection (see Chapter 3)
- ☑ Host-based advanced threat protection (see Chapter 4)
- ☑ Network forensics (see Chapter 5)

So, turn the page to discover the first of these three technologies and learn how successful IT security organizations are dramatically improving their network security postures.

Chapter 3

Securing the Perimeter from Advanced Threats

In this chapter

- Review the key components of a perimeter-based advanced threat protection solution
- Explore key features for mitigating advanced threats within web traffic, email messages, mobile communications, and files at rest
- Learn use cases for integrating perimeter-based advanced threat protection within your existing IT infrastructure

Up until the last half-decade, securing the perimeter from cyberthreats meant deploying a high-quality standalone IPS or next-generation firewall (NGFW) with integrated IPS protection. But as attackers are increasingly using highly customized exploits, these traditional security solutions simply can't keep up.

You need an additional layer of protection to supplement — not replace — your existing perimeter defenses. Once you have identified and removed known threats from *ingress* (inbound) *traffic*, you must then inspect traffic with a more thorough solution specifically designed to catch threats missed by signature-based defenses.

In this chapter, I review the key components of modern-day advanced threat protection solutions. I then describe how these components function to detect threats within web, email, and mobile communications, as well as files at rest. Finally, I explore key features found within perimeter-based advanced threat protection solutions and describe how these solutions integrate with your existing IT infrastructure.

What the World Really Needs

Before I delve into the inner workings of perimeter-based advanced threat protection, let's step back and look at the "big picture." Let's clearly understand what the world really needs to effectively defend against advanced threats. In other words, let's review the must-have attributes of effective advanced threat protection solutions.

Jump to Chapter 7 for a complete list of buying criteria.

Signature-less malware detection

The first and, perhaps, most obvious attribute of any advanced threat protection solution is its ability to detect unknown malware without relying solely on pattern-matching signatures. You'll discover how this is done later in this chapter (see "How It Works" section), but for now, recognize that reliance on signatures is the biggest differentiator between advanced threat protection solutions and traditional security defenses.

Don't get the wrong idea. Signatures – or MD5 or SHA checksums, to be more precise – definitely play a role with best-of-breed advanced threat protection vendors that share threat intelligence among their global customer base. (See "Dynamic global threat intelligence" section.) Signatures also make *inline* blocking possible, as described next.

Protection — not just detection

Most advanced threat protection offerings today are capable only of being deployed passively, or *out of band*. Such products are designed to detect advanced threats rather than block them. That's practical for unknown, never-before-seen threats, which require time to analyze. But if a threat has been seen by that device before – or perhaps other similar devices around the world (especially those owned by other organizations) – clearly the better approach is to block those known threats outright, saving valuable processing resources on your advanced threat protection devices.

Most organizations that acquire advanced threat protection appliances capable of inline blocking first deploy them in a passive, out-of-band configuration. This buys them time to analyze the results and ensure that no false positives were triggered. After a few weeks of zero false positives, organizations gain confidence that placing their appliances inline will not hamper user experiences.

Multi-stage protection architecture

In a perfect world, IT would maintain full control of every computing device on the network. Then you'd have to worry only about cyberattacks originating from outside the network. But with the explosion of mobile computing, compromised devices are regularly hand-carried right through the office front door on laptops, tablets, and now smartphones.

What the world needs is an advanced threat protection solution that monitors attacks not only from the outside in, but from the inside out as well — across all stages of the targeted attack life cycle. Better advanced threat protection solutions monitor outbound traffic looking for connections to blacklisted IP addresses and URLs, which are likely tied to malware connecting to CnC servers for instructions or – even worse – exfiltrating stolen data.

Response capability

Continuing the theme of what the world really needs, it's important to appreciate that the best security solutions integrate with other security solutions to share intelligence and to respond to threats. Leading advanced threat protection solutions afford their users response capabilities tied to both endpoint security and network forensics solutions. (More on that in the "Third-party Integration" section.)

Dynamic global threat intelligence

Some so-called advanced threat protection vendors do not give their customers the opportunity to share threat intelligence with each other. Leading vendors, on the other hand, enable customers to upload newly created threat signatures to the vendor's cloud in near real time to help "inoculate" others, so to speak. I call this practice "community immunity." As a result, when one customer is "ground zero" for a new advanced threat, other customers are protected from that threat within a matter of minutes.

How It Works

Now that you understand the attributes of a successful advanced threat protection offering, let's roll up our sleeves and delve into how these solutions actually work.

Key components

Let's begin by exploring key components of leading advanced threat protection solutions.

Malware analysis appliances

At the heart of every advanced threat protection solution is a malware analysis appliance. These high-performance, purpose-built appliances (see Figure 3-1) analyze suspicious object types contained in web traffic, email messages, or files at rest. They also block known threats by using highly accurate intelligence to stop inbound threats and unauthorized outbound communications.

Discerning potential malware in web traffic and doing the same in email messages require different approaches. Some vendors market a one-size-fits-all malware analysis appliance (or cloud offering) that attempts to detect threats in all three mediums (or two, if unable to inspect files at rest). Avoid such sub-optimized solutions, as they typically suffer from high *false-positive* and *false-negative* rates.

Figure 3-1: Sample malware analysis appliances

As I mentioned earlier, advanced threat protection products are not meant to replace traditional security defenses. They're meant to augment them. Typically, the malware analysis appliance is placed behind the NGFW (or behind the IPS if a traditional firewall is used) so the NGFW can filter out basic (known) threats prior to content analysis (see Figure 3-2). This helps reserve processing power of the malware analysis appliance toward detecting advanced threats using the virtual execution engine (see next section).

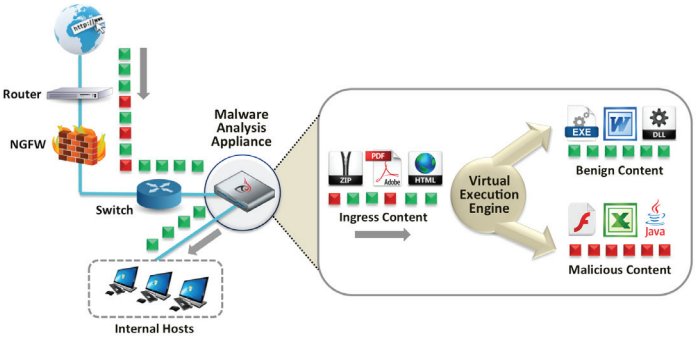

Figure 3-2: Typical advanced threat protection deployment

Virtual execution engine

The *virtual execution engine* is the "secret sauce" of every advanced threat protection platform. It inspects traffic and files, looking for thousands of suspicious characteristics including obfuscation techniques like XOR encoding and other disguising behavior. Sessions are replayed in a (safe) virtual execution environment (think virtual machines, but using a

custom-built virtualization engine specifically designed for security analysis) to determine whether the suspicious traffic actually contains malware. (View the "Call the bomb squad!" sidebar for an interesting, real-world analogy.)

Better advanced threat protection offerings contain virtual execution engines capable of inspecting dozens of file types (rather than just .exe and .dll files), including: asf, com, doc, docx, dll, exe, gif, ico, jpeg, jpg, mov, mp3, mp4, pdf, png, ppsx, ppt, pptx, qt, rtf, swf, tiff, unk, vcf, xls, xlsx, zip… and the list goes on.

Once a suspected threat has been classified as malware by the virtual execution engine, new threat intelligence is automatically created and distributed to your other appliances (if you have a central management system; see next section) and possibly to other organizations around the world (see "Cloud threat intelligence network" section just ahead).

The quality of the virtual execution engine is paramount to the success of your advanced threat protection platform. Unlike rudimentary *sandbox* offerings, a high-quality virtual execution engine is not susceptible to common sandbox-evasion techniques, such as:

- ☑ Malware designed to detect the presence of sandbox environments
- ☑ Malware designed to suppress its payload until a computer mouse has been clicked (indicating that it's running in a live PC operated by a real person)
- ☑ Malware designed to suppress its payload until a certain user action has been taken, such as scrolling down to page three of an Adobe PDF file (again, a sign that it's running in a real PC)

Call the bomb squad!

I've always been a big fan of using real-world analogies — and, in some instances, clichés — to describe how a given technology functions or the benefits it provides. When it comes to advanced threat protection, I think I've found a good one.

At first, I considered the "finding a needle in a haystack" analogy, but these days large enterprises and government agencies are targeted with advanced cyberattacks several times each day. So instead of looking for one needle in a haystack of cyberattacks, they're really searching for dozens.

Then I considered a crash test dummy analogy, where the suspicious traffic component (suspected malware) is the dummy and the Microsoft Windows session running in the virtual execution engine (replicating the target environment) is the car. This analogy also isn't bad, but it breaks because the car is going to crash every time regardless of what's inside. Sometimes files examined are simply benign.

After searching long and hard for a better analogy, I finally found one. Ever hear accounts in the news of bomb squads being called to examine a suspicious bag left at the airport or in a busy area like Times Square in New York City? In these instances, the bomb squad sends in a robot to examine the suspicious bag and, if necessary, pick it up and place it in a bomb disposal truck capable of withstanding massive explosions without affecting its surrounding area.

Comparing this scenario to an advanced threat protection solution, the person who called the bomb squad is like the malware detection algorithm. The robot is analogous to the subsystem responsible for redirecting the suspected malware into the bomb disposal truck. And the truck is like the virtual execution session used to "prod" the suspected malware (the suspicious bag) to determine any potential damaging effects (an explosion), but in a safe and secure environment.

I hope this analogy helps you understand how advanced threat protection technology works and provides an easy way for you to explain it to less-technical colleagues.

Central management system

Although most advanced threat protection appliances provide a web-based graphical user interface (GUI) for local administration, better advanced threat protection vendors offer a central management system console for multi-appliance administration, consolidated threat monitoring, reporting, alerting, and malware intelligence distribution.

Cloud threat intelligence network

Earlier in this chapter, I described the importance of sharing threat intelligence. This is accomplished through a *threat intelligence network* facilitated by the vendor.

All malware analysis appliances receive intelligence updates throughout the day. Vendors that offer intelligence networks typically give their customers two options — (1) the ability to receive the threat intelligence or (2) the ability to share and receive threat intelligence. Most organizations choose the latter.

Because these intelligence networks require only metadata from infectious objects to create threat intelligence, organizations need not worry about the potential for sensitive data to leave their network.

Okay, so now that you have a handle on the key components of advanced threat protection solutions, let's explore four use cases for detecting advanced threats – web, email, mobile, and files at rest.

Detecting web-based threats

Leveraging advanced threat protection technology to detect web-based attacks is the most common use case for deploying this technology. Experience has shown that cybercriminals use the web as a primary threat vector to deliver zero-day exploits, infect endpoints through drive-by downloads, and distribute malware associated with spear phishing attacks.

Leading advanced threat protection vendors offer high-end, multi-gigabit appliances that can be deployed both passively and inline. Even if you decide not to deploy your appliances inline on day one, be sure to select models that are designed for inline deployment for when you're ready.

If you're also thinking about refreshing your IPS technology, be advised that some advanced threat protection vendors offer appliances with IPS built in.

Preventing email threats

The second of four use cases is preventing threats attached to spear phishing emails that bypass traditional anti-spam and reputation-based technologies. In this instance, suspicious email attachments are analyzed by the virtual execution engine contained within the advanced threat protection appliance. If the attachment is determined to be malicious, the file is quarantined and an alert is sent to the central management system console.

Leading advanced threat protection vendors offer email-inspection solutions as both physical appliances and cloud-based services. Unlike web-inspection solutions that must contend with latency (when appliances are placed inline), users won't notice if an email arrives seconds later than it should. Thus, I suggest talking with your advanced threat protection provider to determine whether an appliance- or cloud-based email-inspection solution is right for you.

Mitigating mobile threats

The third use case — and certainly the newest— is detecting threats targeting mobile devices, such as smartphones and tablets. Research indicates that more than a million malicious or high-risk apps exist in the wild at any given time. Many of these apps can be help attackers conduct targeted attacks through a variety of threat vectors. Knowing what an app does with the information it accesses is critical to securing your network and intellectual property.

Leading security vendors are now complementing their web and email threat-prevention offerings with cloud-based mobile security solutions to extend the reach of advanced threat protection to mobile devices. By installing a lightweight agent on (typically Android-based) managed mobile devices, IT security professionals can now mitigate threats targeting those devices by assessing app behavior.

Some mobile advanced threat protection products offer APIs to interface with mobile device management (MDM) and mobile application management (MAM) platforms to facilitate the distribution of agent software.

Uncovering threats within files at rest

The final use case for advanced threat protection is uncovering threats within files at rest. Remember, sometimes malware-infected files are hand-carried into the organization on laptops and mobile devices, bypassing your perimeter defenses.

To accomplish this task, a special advanced threat protection appliance is needed. This appliance connects to available NFS-, CIFS- and Samba-compatible file shares. (APIs may be made available to connect to SharePoint, Dropbox.com, and Box.net data repositories.)

The process of assessing stored files for threats is essentially the same as for web and email advanced threat protection solutions. Files are evaluated within the safety of virtual machines using the virtual execution engine. If a file is deemed malicious, an alert to the central management system is triggered and the file can be quarantined.

When evaluating advanced threat protection vendors, avoid those that support just one or two of these four use cases. Although you may not have budget for all four solutions on day one, it's good to know that when you acquire additional components in the future, they'll integrate with your current platform.

Exploring Key Features

Let's now explore key features found in leading advanced threat protection products and discuss how these products integrate with your existing IT infrastructure.

No two advanced threat protection products are alike. Product functionality varies widely. As you review the features in this section, take note of which ones are particularly applicable to your organization. Then refer to Chapter 7 for additional considerations for buying advanced threat protection solutions.

Virtual execution of suspicious objects

Signature-less analysis to detect unknown threats is critical. Look for the ability to replay traffic containing suspicious objects — such as web pages, binaries, and files — in the safety of a virtual execution environment. This is different from forwarding a suspicious file or executable to a sandbox. Replay is the byte-by-byte capture and reconstruction of the traffic flow within a virtual execution environment. A single web page, for example, is made up of 20 to over 200 different objects served from dozens of different web locations. Replay technology is the only way to analyze complex web-based attacks, such as drive-by download attacks.

Don't get trapped into thinking that today's advanced threats can appear only in exe or dll files. Malware can be embedded in web pages and dozens of file types.

Fast-path blocking

Blocking outbound callbacks and known inbound threats goes hand-in-hand with signature-less analysis. Although I've spent a fair amount of time describing the limitations of traditional signature-based defenses, I've also acknowledged how important they are in stopping known attacks in a *defense-in-depth* strategy. Look for advanced threat protection solutions that incorporate both signature-based and signature-less techniques to defend efficiently against known and unknown attacks, respectively.

Malicious file quarantine

Malicious files, emails, and related attachments detected by the virtual execution engine can be quarantined and stored on the malware analysis appliance (or the central management console, if available) for further forensic analysis. The files may also be collected as digital evidence by computer crime investigators from the FBI or other authorities.

Custom rule support

Leading advanced threat protection systems enable advanced users to import custom malware-detection rules created using the YARA rules language. (YARA is a tool designed to help malware researchers identify and classify malware samples.) When the malware analysis appliance triggers an imported YARA rule, the virtual execution engine immediately analyzes associated objects for potential cyberattacks. This is helpful for organizations that are frequently targeted by a specific class of cyberattack.

For more information on YARA, connect to http://plusvic.github.io/yara/.

Malware intelligence sharing

Part of the beauty of an advanced threat protection solution is that organizations are protected by their locally generated threat intelligence and can choose to share this with other organizations. With a cloud threat intelligence network (owned and operated by the vendor), once one organization has detected a brand new threat ("ground zero" for the attack), all other organizations are protected within minutes.

While organizations can certainly defuse advanced threats with a standalone malware analysis appliance, collective immunity makes their appliances run more efficiently by focusing resources on analyzing truly unknown cyberattacks. Plus, organizations commonly receive a vendor discount on their annual cloud threat intelligence network subscriptions for their willingness to share anonymous threat intelligence.

As I mentioned earlier, it's important to understand that at no time will any of your files, or even content contained within those files, ever be sent to the cloud threat intelligence network. Threat protection profiles, for example, include only anonymized data, such as a checksum of the file.

AV suite integration

Preferred solutions can integrate with popular AV suites, such as McAfee, Symantec, Sophos, and more. Integrating with an AV suite allows each malicious object to be further analyzed to determine if the AV platform detected the malware stopped by the malware analysis appliance. This enables organizations to more efficiently prioritize incident response follow-ups.

Dashboard

The dashboard (see Figure 3-3) is the primary interface used by security analysts to monitor the security state of the network and the workload of the organization's malware analysis appliances. Dashboards are accessed via web browsers and are easy to interpret. Better dashboards offer the ability to drill down within event data to reveal details of attacks and help the security analyst determine next steps.

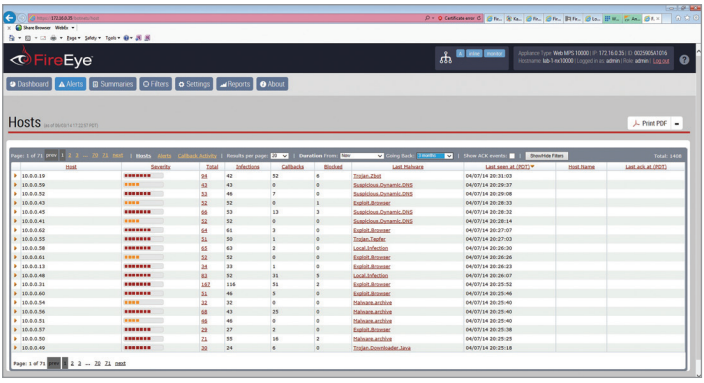

Figure 3-3: Sample advanced threat protection dashboard

Reports

Today's advanced threat protection solutions provide powerful and convenient ways to search for and report on specific types of cyberattacks by name or type. Organizations can view event summaries such as the most severely infected hosts and the most common malware and callback events, including geolocation details. Some solutions even provide the capability to map event data in Google Earth!

Reports can be generated by users on the fly or automatically created at specified time intervals (daily, weekly, monthly) by the central management console.

Trending reports, in particular, can help demonstrate progress in reducing the number of compromised systems.

Alerts

Alerts help keep security analysts abreast of potential cyber breaches. Typically, alert notifications can be sent via SMTP, SNMP, syslog, and HTTP POST. Alerts are also displayed within the web-based interface of the centralized management system appliance.

Upon detection of a new cyberattack with an associated call-back, the malware analysis appliance registers one or more high-severity alerts. While the appliance (if configured for inline operation) is capable of severing callback communications to defuse the attack, it's important to follow up and remediate the host compromised by that attack.

Role-based access control

Most advanced threat protection systems provide multiple user roles to ensure that administrative privileges are granted only to IT personnel who require them for their jobs. Common user roles include:

- ☑ **System administrator** – full administrative control over the entire deployment.
- ☑ **Regional administrator** – administrative control over one or more malware analysis appliances.
- ☑ **Security analyst** – access to dashboards and reports only; no ability to modify or delete event data or modify system settings.

Third-Party Integration

No information security system should ever operate in a vacuum. Security products should work in concert with one another to provide IT with greater context about the environment it's protecting and, ultimately, reduce the risk of successful cyberattacks.

This section describes how advanced threat protection systems integrate with other IT platforms, starting with SIEM.

Security information and event management (SIEM)

A SIEM is one of the most commonly requested platforms for integration with advanced threat protection systems. And it's no surprise, since the entire purpose of a SIEM is to aggregate security events from across the organization and correlate them (using dozens of pre-built and custom correlation rules) to uncover hidden cyberattacks.

Security events can be exported in real-time streams to SIEM platforms in syslog, common event format (CEF), and vendor-proprietary formats that offer more attack details for deeper analysis.

Network forensics

Network forensics appliances capture every single packet that traverses the network. Once a malware analysis appliance has classified a new form of malware, the analyst can query the network forensics database to determine the context in which the host was compromised and to identify other hosts potentially compromised by the same attack.

Network access control (NAC)

Today's NAC solutions can complement advanced threat protection solutions by automatically quarantining hosts (by using vendor-supplied APIs) identified as either the source (if located within the network) or target of an attack. By rapidly removing infected hosts from the network, you minimize the chances that additional malware will propagate and exfiltrate data.

Incident management

Incident management (or ticketing) platforms have been around for years. They are commonly used by internal IT and help desk staff to track and manage IT incidents. An incident could be as simple as resolving a help desk call or as complex as terminating an APT attack.

Organizations often request the ability to feed advanced threat protection alerts into their existing incident management platform. This is accomplished by forwarding specially formatted SMTP alerts from the central management system to the incident management system or by parsing the XML format alerts to conform to existing incident alert templates.

Grocery chain hungers for advanced threat protection

After seeing headline after headline about major retailers being victimized by cyberattacks, it didn't take much prodding for the chief security officer (CSO) of a major U.S. grocery retailer to realize that his company could be next. With more than 10,000 servers and 120,000 endpoints to defend, the company couldn't afford to rely on traditional security defenses alone.

After reading promising things about a new category of security technology called advanced threat protection, the company's CSO realized it was time to put this technology to the test in their live environment. So he asked his staff to evaluate products from three leading vendors. After a series of onsite evaluations, the decision became clear. The company selected NX Series appliances from FireEye (www.fireeye.com).

The first FireEye NX appliance took about 15 minutes to install and configure. Within hours, it detected threats that were completely missed by the company's existing IPS. To make sure the results weren't a fluke, the security team tried re-tuning its IPS to detect threats similar to those it previously missed. It couldn't.

The FireEye platform "was the only product — out of dozens and dozens that I've deployed — that truly worked out of the box," said a company security manager. "We have a small team with limited resources. We were looking for something that was easy to set up and administer. That's exactly what the FireEye platform delivered."

Chapter 4

Strengthening Endpoint Advanced Threat Defenses

In this chapter

- Review the benefits of host-based advanced threat protection
- Discover ways to mitigate advanced threats that bypass your perimeter defenses
- Learn how to validate the presence of advanced threats through "indicators of compromise"

Chapter 3 describes how to mitigate advanced threats at the perimeter. This chapter describes how to do the same at the host level — because no matter what any security vendor tells you, there is no single "silver bullet" solution for mitigating advanced threats.

Relying solely on perimeter-based advanced threat protection presents two primary risks. First, mobile endpoints operating outside your network are not protected by your perimeter defenses. Your users' devices may become compromised when off the network and then be carried through your front door and connect to the network. And second, advanced threats that are detected (but not blocked) by your perimeter-based defenses can still hit your network if they're not quickly remediated.

In this chapter, you'll learn the role of host-based advanced threat protection and understand how it integrates with your existing perimeter-based defenses.

Benefits of Host-based Advanced Threat Protection

There are many reasons to use host-based advanced threat protection — especially to augment your perimeter-based defenses. This section highlights some of the key benefits.

Gartner, the IT research firm, recently adopted a new term for host-based advanced threat protection: "endpoint threat detection and response." For the purposes of this book, these terms mean the same thing.

Eliminating blind spots

The only thing worse than knowing you've been victimized by an advanced attacker is not knowing that you've been victimized by an advanced attacker. Unfortunately, today's network perimeter is dissolving rapidly. When operating outside your network, mobile devices are simply blind spots. And once they reconnect to your network, they present formidable security risks.

Host-based advanced threat protection solutions eliminate these blind spots by monitoring mobile devices for advanced threats when operating both inside and outside the network.

Remember that the same advanced threats that bypass traditional network security solutions also bypass traditional endpoint security solutions, such as host-based AV and anti-malware offerings.

Validating when attackers are present

A network security alert from any network security device doesn't necessarily mean that an attack has succeeded. Each piece of malware is designed to exploit a specific vulnerability within a specific operating system or application. Thus, it's difficult to know when an attack has actually succeeded and when it has failed.

Host-based advanced threat protection solutions help security analysts filter through the noise of network security alerts by identifying the alerts that really matter — saving you and your colleagues significant time and effort.

Investigating and triaging alerts

Once you've identified the security alerts that really matter, you must triage them by prioritizing alerts based on asset and network security risk. Then you must investigate the root cause and material impact of each suspected attack — activities that are streamlined using modern host-based advanced threat protection solutions. This can be a time-consuming process – especially if you have hundreds or thousands of endpoints and need to track down the physical device across a large area.

Containing compromised devices

Remember that when investigating security alerts, every second that ticks away could mean the attacker is moving laterally throughout your network or even stealing proprietary information. Once a security alert has been validated, you must contain affected endpoint devices immediately before matters get worse.

Leading host-based advanced threat protection solutions enable you to effectively disconnect infected endpoints remotely — whether connected to the network or a Wi-Fi hot spot on an airplane — while maintaining the ability to remotely investigate the threat. Containing compromised devices buys security analysts valuable time to contact the user and remediate the threat.

How It Works

So, now that you've gained insight into why host-based advanced threat protection is must-have technology for enterprise networks, let's explore how these solutions actually work.

Key components

Life for IT security professionals would be wonderful if the devices they must secure were always connected to their internal networks — defended by layers of both traditional security devices and advanced threat protection appliances.

Unfortunately, we live in the real world. We must keep our endpoint devices safe no matter where they go. Host-based advanced threat protection solutions use lightweight agents that are installed on every monitored endpoint device. These agents maintain constant contact with an endpoint monitoring appliance (see Figure 4-1) which, in turn, remains connected to your existing malware analysis appliances (see Chapter 3 for a refresher).

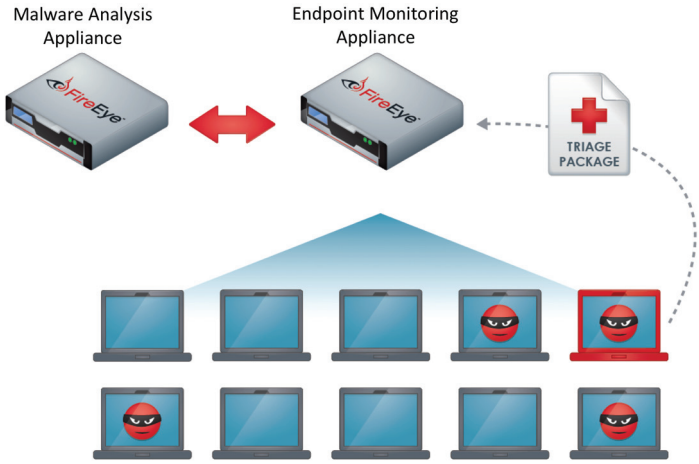

Figure 4-1: Host-based advanced threat protection conceptual diagram

Validating attacks with indicators of compromise

Every alert sent from your malware analysis appliances to your endpoint monitoring appliance should create an *indicator of compromise* (IOC). The IOC may be a checksum yielded from a just-validated sample of advanced malware or the IP address or URL of a CnC server detected through the monitoring of outbound host communications.

The agents installed on your managed devices are constantly generating checksums for files received and continuously logging source and destination IP addresses, ports, and URLs associated with network and Internet communications. The endpoint monitoring appliance validates attacks by comparing IOCs against records from tens or even hundreds of thousands of hosts – all in the blink of an eye.

Containing compromised endpoints

Once an attack has been validated and the victimized host has been identified, the security team can send a request to the endpoint agent to block the host from communicating with all other hosts except the endpoint monitoring appliance. This ensures that the attack can cause no further damage while the team investigates the incident.

Determining what happened

With the compromised host effectively quarantined, the security analyst must leverage all available network and endpoint intelligence (including network forensic intelligence, if available, as described in Chapter 5) to answer the following key questions:

- ☑ How did the attack occur?
- ☑ Did the attacker access other hosts?
- ☑ What, if any, data was exfiltrated?
- ☑ Is the attacker still on the network?
- ☑ How can we ensure this attack won't happen again?

The last question is the focus of the next section.

Sharing intelligence with other security platforms

Host-based advanced threat protection platforms generate a treasure trove of threat intelligence. This intelligence — such as checksums from newly identified malware and IP and URL reputation data — can and should be shared with your other security platforms.

A key benefit of obtaining perimeter- and host-based advanced threat protection solutions from the same vendor is that threat intelligence generated by both solutions is pooled together – and typically shared with all other customers around the world.

Federal research center discovers a better way to combat advanced threats

A large U.S. federally funded research and development center with more than 1,200 employees nationwide consistently found itself in the crosshairs of politically motivated APT attacks. The organization regularly conducts long-term technical research projects pertaining to energy, space exploration, and national defense. Naturally, sensitive data originating from these high-profile projects is frequently targeted by nation state-sponsored cyber spies.

Before 2011, the organization relied exclusively on signature-based perimeter and host defenses for detecting cyberthreats. Unfortunately, a noticeable rise in spear phishing and watering hole attacks led to multiple system breaches. Fortunately, the breaches were contained before targeted data was exfiltrated.

Knowing it was only a matter of time before its luck ran out, the company invested in web- (NX) and email-based (EX) advanced threat protection appliances from FireEye (www.fireeye.com). It selected FireEye because of the vendor's innovative multi-vector virtual execution (MVX) engine, which detects never-before-seen malware and URLs without relying on signatures.

However, the company was still vulnerable to advanced threats on mobile devices operating outside the safety of its perimeter defenses. So in 2013, the organization added FireEye (formerly Mandiant) HX endpoint threat protection technology to protect vulnerable mobile devices.

With FireEye HX, the security team can continuously monitor these mobile devices looking for indicators of compromise received from FireEye and other perimeter security defenses. And when a compromised device has been identified, the FireEye HX appliance quickly contains the infected device — whether on or off the organization's network — buying valuable time to remotely remediate the threat before damage is done.

With FireEye NX, EX, and HX solutions, this research and development organization finally has the tools necessary to combat APT attacks and ensure that data pertaining to sensitive government research projects remains secure.

Chapter 5

Investigating Advanced Threats with Network Forensics

In this chapter

- Define network forensics and review common use cases
- Learn how organizations use network forensics to validate and remediate advanced threats

As I've stated more than once, no matter how many layers of network and endpoint defenses you have in place, your network will still become compromised. But it doesn't mean that your company has to make headlines. How quickly and effectively you respond to advanced threats can mean the difference between doing a good job and finding a new job.

Fortunately, a new category of technology has emerged in the past decade that dramatically reduces the time and effort to investigate attacks: *network forensics*.

In this chapter, I define network forensics and describe various ways enterprise use this multifaceted technology to improve security, reduce risk, and comply with industry mandates. I also explain how network forensics solutions work and, specifically, how security analysts use this technology to investigate and resolve advanced threats.

Exploring Network Forensics

Let's begin by defining network forensics and exploring how enterprises use this technology to its full potential.

What is network forensics?

Network forensics refers to software packaged in high-performance, rack-mounted appliances designed to capture every packet, flow, and file that traverses your network. These appliances, which are built for the enterprise, capture and index data at wire speed, providing a forensically sound record of all network activity.

Some compare network forensics appliances to television DVRs. But instead of recording your favorite TV shows, they record every show on every channel during every minute of the day – and store them for months at a time.

It's important to remember that the same advanced attackers who bypass traditional network security defenses also elude traditional endpoint security measures, such as host-based AV and anti-malware offerings. Thus, implementing a network forensics solution to investigate successful attacks is critical to any advanced threat protection strategy. But as you'll learn in the next two sections, mitigating threats isn't the only reason for acquiring network forensics.

Benefits for security analysts

Clearly, the primary reason why enterprises deploy network forensics is to mitigate cyberthreats. Here are some of the specific use cases for security analysts:

- ☑ Detecting the presence of cyberthreats
- ☑ Confirming whether an attack actually succeeded
- ☑ Investigating the root cause of successful attacks
- ☑ Tracking attacker movement across the network
- ☑ Determining what, if any, data has been stolen
- ☑ Verifying an attack has been successfully terminated

According to the "2013 Cost of Cyber Crime Report" published by the IT research firm Ponemon Institute, the average time to resolve a cyberattack is 32 days at an average cost of $32,469 per day. This is a 55 percent increase over the 2012 average cost over a 24-day period.

Obviously, remediating cyberattacks as quickly as possible by decreasing the *mean time to resolution* (MTTR) is in all organizations' best interest. Network forensics certainly reduces your MTTR for resolving security incidents, but it also ensures that you don't "over-respond" to successful attacks. (See the "Rightsizing your incident response" sidebar for more insight.)

Right-sizing your incident response

Assessing the impact of a successful cyberattack is never easy. And without network forensics, it's even harder — if not impossible — to determine the full extent of an attack, including what data, if any, was stolen.

Let's say that you're a security analyst at a large retail chain and you've uncovered evidence that a database housing customer credit card data may have been compromised by cybercriminals. But you can't determine whether one credit card number has been stolen or one million — or any! So, what does your company do? Do you warn all of your customers and advise them that their credit card numbers may have been compromised? Or do you roll the dice and hope you caught the attack before data was stolen?

Obviously, unnecessarily alarming millions of consumers can be enormously costly. When responding to a successful cyberattack, the best approach is to "right-size" your incident response. And network forensics helps makes this possible.

By capturing every packet that traverses your network, you can "roll back" the data breach much like a police investigator rolls back video taken from a surveillance system after a bank robbery. With network forensics, you can visualize with 100 percent accuracy exactly what data was exfiltrated. So you know exactly which of your customers were affected — if any at all!

As the saying goes, "Knowledge is power." With network forensics, you have the power of knowing exactly what happened so you can accurately assess the impact of a cyberattack and right-size your response.

Benefits for network operations

An ancillary benefit of network forensics technology is helping network operations staff troubleshoot degraded network performance and detect violations of internal IT compliance policies. Let's explore a hypothetical scenario that pertains to both objectives.

Say your help desk has received calls every day for the past week from users in a branch office who are complaining that the network has slowed to a crawl. You find no evidence that available bandwidth from your Internet service provider has decreased, and all of your systems management consoles appear to be nominal.

But querying your network forensics system reveals that multiple users have connected to Slingbox devices to stream live HDTV from their cable boxes at home to their PCs in the office. These users just couldn't wait to watch their favorite teams competing in World Cup soccer matches.

Streaming a single, live, high-definition TV broadcast from a Slingbox device consumes a minimum of 1.5 megabits per second (Mbps) of bandwidth per user (or up to 9 Mbps using the "Best HD" setting). Just one stream can cause an already populated Internet connection to reach its capacity, thus inhibiting users from doing their jobs.

At some organizations with internal IT acceptable use policies, or AUPs, streaming entertainment video is an internal policy compliance violation. With network forensics, you know exactly which users to contact to help ensure that future policy violations won't happen again.

How It Works

Now that you understand how network forensics systems benefit both security and network operations professionals, let's explore how these solutions actually work — starting with key components.

Key components

The following subsections describe key components of leading network forensics solutions:

Capture probe appliance

The capture probe is the only required component of a network forensics deployment. It is an extremely sophisticated, high-performance, purpose-built appliance designed to capture and store packets (without latent buffering) at speeds up to 20 gigabits per second (Gbps). These appliances come standard with either two 10 Gbps fiber interfaces or multiple 1 Gbps fiber or copper interfaces, along with dozens of terabytes (TB) of disk space to store captured data for weeks at a time.

Leading network forensics vendors typically offer "storage shelves," which are special appliances designed to increase your storage capacity to 300 TB or more.

The more network segments you connect to your capture probes, the more visibility you gain into the security and performance of your network. With aggregation *TAPs*, you can aggregate feeds from dozens of switch *SPAN* ports into a single capture probe appliance.

Avoid so-called network forensics offerings that merely sample network packets. Although less storage is required, you may miss packets that are critical to uncovering the root cause and material impact of a data breach.

Data inspection appliance

Data inspection appliances are optional but highly recommended components. Although most capture probes incorporate basic data querying capabilities, including Wireshark for decoding PCAPs, a data inspection appliance gives security analysts advanced capabilities, including:

- ☑ Indexing packets and flows at wire speed
- ☑ Searching data using Layer 7 attributes
- ☑ Performing top-level DNS queries
- ☑ Querying data stored on multiple capture probes
- ☑ Reconstructing emails and chat messages

Disrupting the attack life cycle

The sequence of steps taken to perpetrate a targeted attack is known as the *attack life cycle*. The attack life cycle begins when the attacker selects a target and initiates his reconnaissance by identifying workers employed by the targeted organization. It ends when targeted data is exfiltrated. (For information on the steps in between, see "The Life Cycle of a Targeted Attack" section in Chapter 2.)

With instant access to raw network packets pertaining to a security alert, security analysts can identify and disrupt attacks throughout the kill chain — from the point of initial compromise, to escalation of privileges and lateral movement, and finally to the act of stealing data.

Financial institution banks on network forensics

With more than 15,000 employees spread across 150+ locations, the CSO of a major U.S. financial services company often wondered if his organization would be the next victim of an advanced targeted attack. Although his company had invested heavily in the latest perimeter-based malware defenses, he knew his network was still vulnerable to malware hand-carried in on mobile devices.

At that point, the company had been lucky. Although several dozen user devices had been infected with malware – usually by way of spear phishing attacks – the CSO's team of expert security analysts were able to contain the devices before the attackers expanded their foothold or stole data.

Knowing that his luck could run out at any time, the CSO directed his team to evaluate leading network forensics solutions to more rapidly investigate threats. After careful consideration, the company selected network forensics appliances from nPulse — now part of FireEye (www.fireeye.com).

As a result, the company's mean time to resolution (MTTR) dropped dramatically within the first month of deployment. Once security analysts were trained to locate data of interest and analyze PCAPs, MTTR dropped from one week to less than a day. Plus, the solution's RESTful API enabled the team to integrate network forensic intelligence into their ArcSight SIEM, allowing security analysts to query data of interest quickly and easily.

Although there's no guarantee that the company will avoid every data breach, the CSO is comforted to know his team now has the tools necessary to minimize the impact of advanced attacks.

Chapter 6

Unifying Advanced Threat Protection Defenses

In this chapter

- Build a case for unifying three key advanced threat protection defenses
- Follow the steps security analysts take to contain infected endpoints and remediate threats

By now, you should have a deeper understanding of how each of the following three technologies helps mitigate advanced threats:

- ☑ Perimeter-based advanced threat protection (Ch. 3)
- ☑ Host-based advanced threat protection (Ch. 4)
- ☑ Network forensics (Ch. 5)

If you've skipped ahead to this chapter and you're not familiar with all three of these technologies, I recommend you flip back to the appropriate chapter(s) before proceeding further.

Let's now tie these three technologies together and build a case for a unified approach. In this chapter, I summarize why perimeter-based advanced threat protection alone is insufficient to mitigate advanced threats. And I detail the steps security analysts follow to mitigate attacks using all three technologies.

The Case for a Unified Approach

The following five sections provide ammunition that you can use when justifying additional investment in advanced threat defenses.

The dissolving perimeter

There's no doubt that your network's perimeter is dissolving. Although your perimeter defenses are essential to protecting your network's assets, you can't rely on them alone to stop all advanced threats.

It's important to remember that not all attacks pass through your firewall. Many of them are hand-carried into the office on laptops, tablets, and now smartphones. Equipping these devices with host-based advanced threat protection software is critical not only for detecting threats, but also for identifying and quarantining hosts that are later found to be compromised.

New web-based tactics always get through

Let's quickly recap how perimeter-based advanced threat protection appliances function. Email-based versions always prevent malware (within email attachments) from reaching their destination. Web-based versions do so only if both of the following are true:

- ☑ The appliance is configured for inline blocking
- ☑ The appliance contains a checksum signature for the malware detected

Of course, the malware used by advanced attackers is highly customized and very short-lived. If a user downloads a file with newly constructed malware, a malware analysis appliance will certainly analyze the suspicious file in the safety of a virtual execution environment. But the verdict on the file — whether benign or malicious — won't be rendered for several seconds. In the meantime, the file is delivered to its final destination without delay — so as to not hinder the user experience. After all, most files accessed via the web are free from malware.

As you'll learn in this chapter, a host-based advanced threat protection solution is useful in this regard because it not only confirms when a malware-infected file has reached its destination, but also tells you which, if any, additional (monitored) hosts may have been infected.

Time is of the essence

Once a malware-infected file reaches a host, the countdown begins until the malware connects outbound to its CnC server or replicates itself on other machines. In either case, speed is critical. You can quickly quarantine malware-infected devices – and prevent attackers from exfiltrating data – by equipping endpoints with advanced threat protection software.

Not all internal hosts are monitored

BYOD is a blessing for employee productivity but a curse for security. Unmanaged devices not equipped with host-based advanced threat protection software are particularly vulnerable to advanced threats.

If, for example, a contractor uses her own laptop to inadvertently download a malware-infected file, there's no way to quarantine that laptop when a security alert has been triggered. The potential exposure to the organization hinges on the user's level of administrative access.

This is where network forensics plays a valuable role. Upon receiving a perimeter security alert, and after determining that the targeted host is unmanaged, a security analyst can query the network forensics system using the destination IP referenced in the alert. Then, the analyst can both verify that the malware reached its destination and determine what, if any, ill effects have transpired, such as CnC callbacks, malware propagation, and data exfiltration.

How It Works

The preceding three chapters described how each advanced threat protection component functions. Now let's explore how security analysts can leverage all three components simultaneously to detect and remediate advanced attacks.

Step 1: Perimeter alert is triggered

Let's begin with an example. Say an employee with a Windows-based laptop has just visited a website and downloaded a file containing newly constructed malware. Once the file (easily) passes through legacy security perimeter devices, such as the firewall and IPS, the malware analysis appliance instantly begins to analyze the file using its virtual execution engine.

Within seconds, the malware analysis appliance detects the malicious malware and generates an MD5 checksum signature so that reoccurrences of that malware will be blocked automatically — not only by the company's internal advanced threat protection appliances, but also appliances owned by other customers around the world.

Additionally, the malware analysis appliance creates an operating system change report that details unauthorized configuration changes caused by the malware. The appliance then sends an alert to its central management system, which, in turn, forwards the alert to the endpoint monitoring appliance associated with the company's host-based advanced threat protection deployment.

Step 2: IOC is generated

The endpoint monitoring appliance processes the alert from the central management system, which includes a copy of the MD5 checksum signature and the operating system change report. Within seconds, the endpoint monitoring appliance generates an IOC (see Chapter 4 for a refresher on indicators of compromise) for this malware and sweeps through its aggregated endpoint intelligence to identify all devices that may have been compromised.

Remember, IOCs are not always signatures. They can also be registry changes, process names, IP addresses, URLs, DNS names, or other attributes associated with a security alert. IOCs can be both network- and endpoint-centric.

Step 3: Compromised endpoints are quarantined

Once all (managed) endpoints that have received the malware-infected file have been identified, it's important to take them offline as quickly as possible. This is where the endpoint monitoring appliance comes into play.

With just a few clicks of the mouse, all infected hosts associated with the aforementioned IOC can be effectively quarantined. The endpoint monitoring appliance submits a command to temporarily terminate network connectivity of infected hosts while retaining communication with the endpoint monitoring appliance so that the device can be investigated. Users may also receive a (customizable) pop-up message or browser notification window advising that their devices have been temporarily quarantined.

Endpoints equipped with host-based advanced threat protection software can be remotely quarantined by the endpoint monitoring appliance even if they're operating outside the network. An infected endpoint could be connected to the Wi-Fi network of a coffee shop and still receive instructions from the endpoint monitoring appliance to isolate it.

Quarantining infected endpoints buys security analysts valuable time to investigate the threat without letting the attacker continue using the device and possibly steal data.

Step 4: Threat is investigated

Over the past decade, enterprises and government agencies have implemented network forensics appliances far and wide. Many security analysts spend more time investigating threats through network forensics than any other security system.

The methods available for investigating cyberthreats vary by network forensics platform. But at a minimum, the following capabilities should exist:

- ☑ Ability to query recorded ingress and *egress traffic* associated with the target IP address (and sometimes the source IP address, if internal) of an attack
- ☑ Ability to query all recorded traffic by port, protocol, IP address, DNS name, URL, and more to identify other potential security exposures that are similar to a known attack
- ☑ Ability to reconstruct and play back content in its original form, such as a web page, email message, and instant (chat) message
- ☑ Ability to reconstruct files in their entirety
- ☑ Ability to analyze PCAPs (packets) using a built-in packet analysis utility such as Wireshark

Network forensics appliances aren't your only source for investigating advanced threats. Better host-based advanced threat protection solutions enable incident responders to query *triage packages* from hosts that summarize endpoint activities and configuration changes in a timeline view.

Step 5: Hosts are remediated

With all of the information about the attack at your fingertips, courtesy of your network forensics appliances, your team can follow their standard operating procedures for remediating infected hosts. This may include scanning hosts for malware, vulnerabilities, and security misconfigurations, or in many cases, wiping the hard drive clean and restoring the host to an approved gold image.

I hope by now I've convinced you that perimeter-based advanced threat protection alone is insufficient for mitigating advanced threats. Host-based advanced threat protection software and network forensics appliances provide critical features to help keep your network safe.

But what should you look for when evaluating these components? The next chapter will help.

Chapter 7

Selecting a Complete Advanced Threat Protection Solution

In this chapter

- Understand what to look for — and what to avoid — when evaluating advanced threat protection solutions
- Explore service offerings made available by preferred advanced threat protection vendors

Once your organization has committed to acquiring a full-featured advanced threat protection solution — equipped with perimeter, endpoint, and network forensics components — you'll need to compile a list of the product capabilities and attributes you need. This chapter will help you get started.

Here I detail important criteria for most enterprises and government agencies looking to buy advanced threat protection solutions. I then describe professional services offered by leading advanced threat protection vendors that you may find useful on day one or beyond.

But first, I want to tell you about product attributes you should clearly avoid when evaluating advanced threat protection offerings.

What to Avoid

Take note of these warnings. Otherwise, you may end up acquiring a solution that provides only part of the advanced threat protection functionality you need.

Avoid partial solutions

Some vendors offer perimeter-based advanced threat protection solutions. Others provide solutions for detecting advanced threats on endpoints. And still others offer network forensics appliances. Very few offer all three.

I recommend avoiding vendors that offer only one or two of these solutions. To maximize your ability to find and stop advanced attackers, it's best to acquire an integrated advanced threat protection platform from one vendor. That way, your perimeter-based solution can forward alerts to your endpoint-based solution, and your network forensics solution can receive commands from your perimeter-based solution.

Avoid detection-only platforms

The best web-based advanced threat protection offerings support both inline and out-of-band modes of operation. Many organizations start with an out-of-band deployment to gain an initial level of comfort. Then they graduate to an inline configuration to block known threats, malware callbacks, and recurrences of newly discovered malware.

Avoid legacy sandbox-based offerings

So-called advanced threat protection solutions that incorporate legacy sandbox technology are easily outsmarted by sophisticated threat actors. They design malware that detects the presence of sandbox environments and, when the sandbox is detected, suppresses its malicious payload to avoid detection.

Avoid all-in-one malware analysis appliances

To best detect today's new breed of cyber attacks, acquire separate, purpose-built malware analysis appliances for email, web, and file-share protection — but be sure they are integrated to share intelligence.

Avoid products without shared intelligence

Most advanced threat protection vendors fail to take advantage of customer-shared threat intelligence. Leading vendors enable customers to opt in to share new threat signatures so others may benefit. This helps optimize the resources of your advanced threat protection appliances: previously seen malware can be blocked instantly rather than having to be evaluated each time it is encountered.

Important Buying Criteria

Now that you know what to avoid, let's review the attributes that most organizations find important when evaluating advanced threat protection solutions.

Integration between network and endpoint defenses

I can't emphasize strongly enough the importance of integration between your perimeter- and host-based advanced threat protection components for detecting and remediating advanced threats. Without tight integration, your perimeter solution can't forward alerts to, and share threat intelligence with, your endpoint solution to effectively discover and quarantine infected hosts.

Support for quarantining infected hosts

When shopping for host-based advanced threat protection, you will find several offerings that can detect threats without relying on signatures alone. But once a compromised host has been identified, it's critical to quarantine that host — while maintaining the ability to administer it remotely – even when that host is connected outside the office.

High-performance network forensics appliances

Network forensics appliances should capture network data at the speed it is transmitted. Unfortunately, some appliances simply can't keep up, so they sample packets for capture rather than recording all packets.

Be sure to select a network forensics appliance with high-speed 10G fiber interfaces that are capable of storing up to 20Gbps of data in real time. Also, be sure it includes ample hard disk space (see Figure 7-1) to store data for weeks at a time. Better network forensics appliances can be expanded by connecting to additional storage modules, so your data can be stored for at least 30 days, with indexed flow data available for at least 90 days.

Figure 7-1: Sample network forensics appliance

Other attributes that are important to consider when evaluating network forensics appliances include:

- ☑ High-speed searching with support for NetFlow v9 and IPFIX flow standards
- ☑ Ability to reconstruct sessions from asymmetrically routed traffic
- ☑ Ability to store data on storage area networks (SANs) for expanded capacity
- ☑ Availability of a RESTful API to support cross-platform integration
- ☑ Ability to timestamp packets in nanoseconds rather than microseconds (to support financial transaction applications)

Integrated platform for all attack vectors

To thwart advanced threats, it's critical to have integrated protections across the common entry points for malware: web, email, and files. The best advanced threat protection platforms incorporate purpose-built appliances (with uniquely different heuristics and algorithms) for detecting malware embedded within email messages, web traffic, and files at rest.

Although you may save a few bucks in the short run by purchasing an appliance from a vendor that claims coverage for two or three of these mediums, in the long run, it's just not worth the risk to invest in a partial solution.

Ability to monitor ingress and egress traffic

Typical perimeter-based advanced threat protection systems monitor ingress (inbound) traffic from websites and email messages to identify suspicious binaries that may contain advanced malware. Unfortunately, most offerings do not monitor egress (outbound) traffic. By monitoring both ingress and egress traffic, your perimeter appliance can detect both inbound malware and corresponding outbound callback attempts.

Monitoring both ingress and egress traffic is an important capability found only in leading advanced threat protection solutions. It provides an additional layer of defense — especially for potentially infected mobile devices hand-carried through the office front door.

Inspection of a broad range of file types

You might be shocked to learn that some rudimentary advanced threat protection solutions are capable of uncovering malware only in unencrypted exe and dll files. The fact is, malware can be embedded in dozens of object types. This includes something as simple as an XOR-encoded binary, in the case of Operation Aurora, or a Microsoft Excel file, which triggered a zero-day Flash exploit in the infamous attack against RSA Security.

Hybrid document exploits highlight the need for broad network security coverage. In the case of the RSA Security breach, the Excel spreadsheet did not attack Microsoft Excel, but rather triggered an exploit against a separate application altogether.

A good advanced threat protection solution applies sophisticated heuristics and malware-detection algorithms to uncover advanced malware in web pages as well as across dozens of file types, including 7z, com, doc, docx, gif, jpg, mov, mp3, mp4, pdf, png, ppt, pptx, rar, swf, tiff, xls, xlsx, zip, and many more.

Ability to overcome evasion techniques

Advanced threat protection solutions that incorporate typical sandboxing technology — as opposed to a next-generation virtual execution engine — are often vulnerable to sandbox evasion. As I described in Chapter 3 (see the "Virtual execution engine" section), advanced malware can often detect the presence of sandboxes and suppress its malicious payload, thus evading detection.

When evaluating advanced threat protection platforms, don't be shy about asking vendors how they overcome common sandbox evasion techniques.

Ongoing threat intelligence updates

All advanced threat protection vendors offer the delivery of ongoing threat intelligence updates via the cloud. These updates contain new threat signatures (checksums) for new malware discovered in the wild. However, assuming that the quality of threat intelligence is equivalent across all vendors would be a costly mistake.

Specific attributes of high-quality threat intelligence include:

- ☑ Threat intelligence updates received every 30 minutes around the clock, rather than once daily
- ☑ Inclusion of malicious IP addresses, URLs, and DNS names for egress traffic monitoring
- ☑ The ability for the vendor's customers to share threat intelligence with each other

Remember that when you opt in to sharing threat intelligence, there is absolutely no risk that your files will be shared with other companies. Your malware analysis appliances are merely sharing malware signatures (checksums) rather than the files themselves.

No false positives or negatives

False positives and false negatives resulting from poor advanced threat detection can prove costly for any organization. A *false positive* (good file classified as bad) could mean blocking an important file from reaching its destination, resulting in lost time and revenue. A *false negative* (bad file classified as good) is even worse — a file infected with malware is allowed to proceed to its final destination without further analysis. At this point, I don't think I need to explain what this could mean.

To say that even the best advanced threat protection system on the market will never render a false positive or a false negative is, perhaps, a bit of a stretch. But such occurrences should be rare.

To assess the detection quality of competing advanced threat protection products, put them through their paces with onsite evaluations. Test both products at the same time using the same production traffic (in passive, out-of-band mode) and compare their results.

Support for custom rules

Advanced threat protection administrators sometimes find it helpful to import custom byte-level rules created using the YARA rules language to trigger analysis of all matched objects for threats specific to an organization. (This is akin to creating custom signatures for a network IPS.)

When evaluating competing advanced threat protection offerings, consider the extensibility of each solution and its ability to support custom malware detection rules.

Intuitive user interface

It makes no difference how powerful or feature-rich a security application is. If it's too difficult to use, an IT organization is unlikely to embrace it — at least on a large scale. Advanced threat protection solutions are no exception.

Unlike security solutions that require security teams to tune or create policy rule sets, such as a traditional firewall or IPS appliance, an advanced threat protection system is far more automated. However, it's important that the dashboard be simple and easy to use. Constructing reports and alerts should not require a PhD in astrophysics!

Responsive customer support

Selecting an advanced threat protection vendor is just as important as selecting the product — if not more so. Enterprises and government agencies frequently cite high-quality technical support as a top decision criterion for selecting any IT system.

Be sure to assess the quality of a vendor's customer support service before purchasing a solution. Reach out to the vendor's technical support department at least twice during the evaluation phase, rather than the SE assigned to your account. Perhaps ask a general question about the product's functionality. When doing so, gauge the expertise and responsiveness of the tech support representative and note how long it took you to reach a human being.

Services Considerations

Some advanced threat protection vendors offer a portfolio of services to help get your product investment off the ground and running full tilt. Some vendors can even assist you in the event of a breach.

The following are brief descriptions of services offered by select advanced threat protection vendors.

Design and deployment

Most security vendors have professional services consultants on staff to assist their customers with all phases of product rollout, including:

- ☑ Sizing perimeter malware analysis appliances and network forensics appliances and determining where best to locate them
- ☑ Installing and configuring endpoint software and the endpoint monitoring appliance
- ☑ Configuring your advanced threat protection components to work together and with key components of your existing infrastructure
- ☑ Training IT admins and security analysts on how to manage and monitor the system

In lieu of employing professional services consultants, some vendors invest heavily in channel partner training so their reselling partners can assist customers with deploying their products.

Incident response

Leading advanced threat protection vendors have expert consultants on staff who can assist you with data breach investigations. They offer proven methodologies to validate the breach, determine the root cause, confirm whether attackers are still present, and assist in re-securing your network and recovering from the incident.

They can also help you collect, analyze, and preserve forensic evidence to provide to law enforcement officials in hopes

of finding, stopping, and convicting the perpetrator. Or, conversely, the forensic evidence may be required to defend against potential lawsuits.

Finally, if your organization doesn't have a formal incident response team or processes, your vendor's consultants may be able to help you construct one based on industry best practices and time-proven methods.

Managed services

These days, more enterprises are turning to their security vendors to not only supply best-of-breed security products, but to manage them as well. This is certainly the case with leading advanced threat protection vendors.

Your vendor may offer a subscription-based service to continuously monitor your advanced threat protection system 24 hours per day, alert you to high-priority attacks, and even help you remediate threats before damage is done.

Glossary

advanced persistent threat (APT): A cyberattack conducted by a group of sophisticated, determined, and coordinated state-sponsored threat actors who systematically compromise commercial and government computer networks for political gain.

advanced targeted attack (ATA): A cyberattack conducted by group of sophisticated, determined, and coordinated threat actors who systematically compromise commercial computer networks for financial gain.

advanced threat protection: Category of security products specifically designed to mitigate advanced cyberthreats without relying upon threat signatures.

advanced threat tactics: Methods for breaching a computer network that are difficult to detect using traditional signature-based security defenses. Examples include custom malware, drive-by downloads, watering hole attacks, spear phishing attacks, and zero-day attacks.

attack life cycle: All stages of a cyberattack targeting a computer network, from the initial point of compromise through data theft and all steps in between.

baiting: A social-engineering attack in which physical media (such as a USB flash drive or CD-ROM) containing malware is deliberately left in proximity to a targeted organization to entice the finder to access it.

basic threat tactics: Methods for breaching a computer network that are easy to detect using traditional signature-based security defenses. Examples include worms, Trojans, viruses, spyware, botnets, and phishing attacks.

bot: A compromised computer centrally controlled by a command-and-control (CnC) server for malicious purposes.

botnet: A collection of compromised computers centrally controlled by a command-and-control (CnC) server for malicious purposes.

bring your own device (BYOD): An organizational policy for allowing employees to bring personally owned laptops and mobile devices to their place of work to access the organization's data.

central management system (CMS): A rackmount appliance responsible for monitoring and managing malware analysis appliances within a perimeter-based advanced threat protection solution.

command-and-control (CnC) server: A server operated by a cybercriminal to provide instructions to individual bots and botnets for malicious purposes.

cybercriminal: An attacker who illegally steals data from another computer for personal financial gain.

defense-in-depth strategy: Installing a series of cybersecurity defenses so that a threat missed by one layer of security may be caught by another.

denial-of-service (DoS) attack: A cyberattack intended to disrupt or disable a targeted host by flooding it with benign communication requests from a single host.

drive-by download: Malware downloaded to your computer without your consent or knowledge by simply visiting a web page.

egress traffic: Computer network traffic flowing from inside the network to hosts outside the network.

false negative: Misclassifying a file containing malware as benign.

false positive: Misclassifying a benign file as containing malware.

hacktivism: The use of computers and computer networks as a means to protest and/or promote political ends.

indicator of compromise (IOC): A forensic artifact or remnant of an intrusion that can be used to identify attacker activity. Examples include malware signatures (checksums), IP addresses, and DNS names.

ingress traffic: Computer network traffic flowing from outside the network to hosts within the network.

inline mode: Placement of a network appliance directly in the line of network traffic, enabling it to block cyberattacks.

intrusion prevention system (IPS): An inline (active) signature-based security device that monitors network traffic and blocks known cyberattacks upon detection.

malware: Malicious software (such as a computer virus, worm, or Trojan) created to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

mean time to resolution (MTTR): The average time it takes to resolve a security incident, from start to finish.

network forensics: Technology in the form of rackmount appliances designed to capture every packet that traverses the network for potential post-breach forensic analysis.

out-of-band mode: The mode of operation of a network appliance that enables it to analyze traffic copied from a network TAP or switch SPAN port.

phishing: The act of sending an email to a user falsely claiming to be a legitimate entity in an attempt to scam the user into surrendering private information, such as credit card and Social Security numbers.

remote administration tool/Trojan (RAT): Software that provides the hacker with a backdoor into the infected system to snoop or take control of the host.

sandbox: A software application designed to analyze suspicious binaries in the safety of a virtual machine, although often evaded by sophisticated cyberattackers.

spear phishing: A phishing attempt directed toward a specific organization or person(s) within that organization.

spyware: A type of malware that collects information about users, with or without their knowledge.

state-sponsored threat actor: A cybercriminal employed by a nation-state to conduct cyberattacks against enemies of the state for politically motivated purposes.

TAP: A hardware device used to access data flowing across a computer network. In the context of advanced threat protection, TAPs are used to direct network traffic aggregated from multiple network segments to individual malware analysis and network forensics appliances.

threat intelligence network: An Internet-based service managed by an advanced threat protection vendor to distribute (and receive) cyberattack intelligence to (and from) its customers' malware analysis appliances.

triage package: A host-based advanced threat protection feature that provides incident responders with a timeline view of endpoint activities and configuration changes. Used to investigate (triage) a compromised host.

Trojan: Malware that masquerades as a legitimate file or helpful application with the ultimate purpose of granting a threat actor unauthorized access to a computer.

virtual execution engine: A component on a malware analysis appliance that is responsible for signature-less analysis of suspicious objects in the safety of a virtual machine. Unlike a sandbox, a virtual execution engine is extremely difficult for threat actors to evade.

watering hole attack: A method of targeting websites that are likely to be visited by targets of interest. The attacker compromises the site and injects JavaScript or HTML to redirect victims to additional malicious code.

whaling: A cyberattack directed specifically at senior executives and other high-profile targets within businesses.

worm: A form of malware that exploits network vulnerabilities to propagate itself to other computers.

zero-day threat: A cyberattack against an unknown (or unreported) operating system or application vulnerability.

Don’t rely on legacy signature-based defenses to detect advanced attackers. Stop them in their tracks with advanced threat protection.

Despite billions spent annually on security, high-profile data breaches occur almost daily. Traditional signature-based defenses simply can’t keep up with modern threats. Thankfully, innovations in perimeter- and host-based advanced threat protection, combined with powerful network forensics, are finally giving IT security professionals the upper hand. This book will show you how.

- Understanding cyberthreat trends and motives — review recent trends shaping the cyberthreat landscape and classify types of attackers
- Exploring advanced threat tactics — distinguish between basic and advanced tactics and learn the advanced threat life cycle
- Securing the perimeter — eliminate advanced threats from web, email, and mobile traffic
- Strengthening endpoint defenses — detect, contain, and remediate advanced threats on endpoints
- Leveraging network forensics — investigate and remediate advanced threats with full-packet capture appliances
- Unifying advanced threat protection — combine perimeter- and host-based protections with powerful network forensics

About the Author

Steve Piper is an information security veteran with over 20 years of high-tech experience. A freelance writer and consultant, Steve has authored numerous books on information security, network infrastructure, and Big Data. He holds a CISSP security certification from ISC^2 and bachelor of science and MBA degrees from George Mason University. Learn more at www.stevepiper.com.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9888233-7-2