

**Making Everything Easier!™**

**Seculert Special Edition**

# **Advanced Persistent Threat Protection**

FOR  
**DUMMIES®**  
A Wiley Brand

## **Learn:**

- To protect your information
- How to recognize when a threat is present
- To rid yourself of detected threats
- How APT protection solutions work

Compliments of



**Peter Gregory**



**Seculert is the first cloud-based solution that provides immediate protection from advanced malware and APTs. From the moment of activation, Seculert identifies existing infections and continues to detect unknown malware both inside and outside of your internal network, including remote sites, employees, and even personal mobile devices. By using patented Botnet Interception, Elastic Sandbox technology, and Big Data analytics, Seculert leverages the power of the cloud to combat today's advanced threats. It enables organizations to simply and cost-effectively transform their existing security defenses into a complete solution for detecting, stopping, and remediating malware attacks.**

For more information, scan the QR code below.



# ***Advanced Persistent Threat Protection***

FOR  
**DUMMIES**<sup>®</sup>  
A Wiley Brand

***Seculert Special Edition***

**by Peter Gregory**

FOR  
**DUMMIES**<sup>®</sup>  
A Wiley Brand

## Advanced Persistent Threat Protection For Dummies®, Seculert Special Edition

Published by  
**John Wiley & Sons, Inc.**  
111 River St.  
Hoboken, NJ 07030-5774  
[www.wiley.com](http://www.wiley.com)

Copyright © 2013 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Seculert and the Seculert logo are registered trademarks of Seculert. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.**


For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact [info@dummies.biz](mailto:info@dummies.biz), or visit [www.wiley.com/go/custompub](http://www.wiley.com/go/custompub). For information about licensing the *For Dummies* brand for products or services, contact [BrandedRights&Licenses@Wiley.com](mailto:BrandedRights&Licenses@Wiley.com).

ISBN 978-1-118-76385-8 (pbk); ISBN 978-1-118-76451-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

# Contents at a Glance



Introduction .....	1
Chapter 1: Discovering What Advanced Persistent Threats Are All About.....	3
Chapter 2: Perusing the Methods Used to Stop APTs .....	13
Chapter 3: Looking into Seculert's APT Protection Architecture.....	21
Chapter 4: Enabling Business in the Shadow of APT .....	31
Chapter 5: Ten Ways Seculert Helps Reduce APTs .....	39



# Table of Contents

---

<b>Introduction</b> .....	<b>1</b>
About This Book .....	1
Icons Used in This Book.....	2
<b>Chapter 1: Discovering What Advanced Persistent Threats Are All About.</b> .....	<b>3</b>
What Are Advanced Persistent Threats.....	4
Examining the Modern Methods of APT .....	5
APT Life Cycle .....	9
<b>Chapter 2: Perusing the Methods Used to Stop APTs</b> .....	<b>13</b>
Stepping Back to Traditional Solutions.....	14
Stopping APT Using Modern Methods .....	15
<b>Chapter 3: Looking into Seculert’s APT Protection Architecture</b> .....	<b>21</b>
Traipsing through the Elastic Sandbox Environment .....	22
Performing Big Data Analytics with Automatic Traffic Log Analysis .....	24
Understanding Botnet Interception.....	27
Evaluating the Seculert Dashboard and API.....	28
<b>Chapter 4: Enabling Business in the Shadow of APT.</b> . . .	<b>31</b>
Stopping APT without Stopping Business .....	32
Protecting the Business with Cloud-Based APT Protection .....	32
Enabling BYOD .....	34
Extending Web Filtering.....	35
Protection from Threats from Customers and Partners.....	36
<b>Chapter 5: Ten Ways Seculert Helps Reduce APTs</b> . . .	<b>39</b>
Botnet Perspective .....	39
Cloud-Based.....	39
Big Data Analysis.....	40
Elastic Infrastructure.....	40
Zero IT Footprint.....	40
No Single Points of Failure .....	40
Extend Web Filtering Systems.....	41
Identifies Threats in Customer and Partner Organizations .....	41
Crowdsourcing.....	41
Ridiculously Easy Setup .....	41

## Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact [info@dummies.biz](mailto:info@dummies.biz) or visit [www.wiley.com/go/custompub](http://www.wiley.com/go/custompub). For details on licensing the *For Dummies* brand for products or services, contact [BrandedRights&Licenses@Wiley.com](mailto:BrandedRights&Licenses@Wiley.com). Some of the people who helped bring this book to market include the following:

### ***Acquisitions, Editorial, and Vertical Websites***

**Project Editor:** Carrie A. Burchfield

**Acquisitions Editor:** Amy Fandrei

**Editorial Manager:** Rev Mengle

**Business Development Representative:**  
Melody Layne

**Custom Publishing Project Specialist:**  
Michael Sullivan

### ***Composition Services***

**Senior Project Coordinator:** Kristie Rees

**Layout and Graphics:** Brent Savage,  
Christin Swinford

**Proofreader:** Lindsay Amones

---

### **Publishing and Editorial for Technology Dummies**

**Richard Swadley**, Vice President and Executive Group Publisher

**Andy Cummings**, Vice President and Publisher

**Mary Bednarek**, Executive Director, Acquisitions

**Mary C. Corder**, Editorial Director

### **Publishing and Editorial for Consumer Dummies**

**Kathleen Nebenhaus**, Vice President and Executive Publisher



# Introduction

---

Your information is under attack. Well-funded adversaries have a wealth of tools and techniques available to obtain your information. After they have your information in their possession, they use it to increase their wealth at your expense.

These adversaries are professionals, and they know what they're doing. They believe that, for any given target of information they desire, that it's obtainable if they can discover the technique required to get it. They spend considerable sums in research and development to develop these *advanced* techniques. Your adversaries are patient; they aren't counting on immediate results but instead are *persistent* as they diligently work toward their goal. Unlike the school age hackers and "script kiddies" of the past, these new adversaries represent a real *threat* to the confidentiality and integrity of our information.

These new adversaries and what they represent are known as *advanced persistent threats* (APTs). These techniques and the people who use them represent the greatest menace against the widespread use of electronic information systems today. The operators and owners of information systems have had solutions available to counter APTs, but your adversaries have always been about two steps ahead.

## About This Book

Advancements in information processing are beginning to pay off in the form of better defenses against APTs. Techniques have been developed that use the elasticity, scale, and power of cloud computing together with Big Data analytics to detect APTs in a customer's organization. And, they do this without the presence of hardware or software inside of customers' organizations and without any changes in how customers connect themselves to the Internet.

The ability to detect APTs in a customer's organization without having any equipment in the customer's network seems like magic. In this book, I roll back the shroud of mystery and explain how APT protection solutions work and how they can help an organization gain the upper hand against APTs.

## *Icons Used in This Book*

Icons are used throughout this book to call attention to material worth noting in a special way. Here is a list of the icons along with a description of what each means:



Some points bear repeating, and others bear remembering. When you see this icon, take special note of what you're about to read.



Watch Out! This information tells you to steer clear of things that may leave you vulnerable, cost you big bucks, suck your time, or be bad practices.



This icon indicates technical information that's probably most interesting to technology planners and architects.



If you see a Tip icon, pay attention — you're about to find out how to save some aggravation and time.

# Chapter 1

---

# Discovering What Advanced Persistent Threats Are All About

.....

## *In This Chapter*

- ▶ Understanding the nature of advanced persistent threats (APT)
  - ▶ Exploring the methods used by APT operations
  - ▶ Pondering the new philosophy of “assumption of breach”
  - ▶ Looking into traditional solutions to the APT
- .....

**T**he weapons of the enemy often can't be seen or detected. Often their weapons are ghostly shadows leaving little trace in systems and networks. Even in cases where malicious activity in a system is confirmed, it's still difficult to identify the actual agent responsible for it.

Your enemies have invested vast resources to find new ways to wage war on you and your organizations. And for the moment, they're winning. Their motivation for profit and anarchy seem to be greater than your motivation for protecting your systems, or so it would seem.

The general term for the tools and techniques used by your adversaries is *advanced persistent threats* (APTs). In this chapter, I describe APTs and why they're such a potent menace to your company.

## What Are Advanced Persistent Threats

An advanced persistent threat is the capability and intent to wage a prolonged campaign against a specific entity in order to obtain information or influence the behavior of the entity. Does this definition scare you? It probably should a little. Being a target of an APT should be sobering, to say the least because a determined adversary, on any battlefield, can be quite a handful to deal with.

So maybe you are wondering what a cyber threat is, then. I should shift gears for a moment and give you more ways to understand the difference between an APT and a non-targeted cyber threat. Try these comparisons on for size:

- ✔ An APT targets a specific organization for a specific purpose, but an ordinary adversary is generally more interested in finding targets of opportunity.
- ✔ An APT is generally slow and methodical — you could say *strategic*. An ordinary adversary is typically opportunistic and performs a quick strike and is done with it.
- ✔ An APT utilizes specially chosen tools and techniques to compromise the entity. An ordinary adversary uses whatever tools he has right now.

Now, examine an analogy of APT in the physical world: stealing cars. An ordinary car prowler canvasses a parking lot or a street, looking for any car that was left unlocked or has valuables visible inside. The prowler uses whatever tools he brought with himself to steal a car — any car will do.

This is contrasted by an APT car thief who wants to steal *your* car. Perhaps the prowler knows that you have some specific valuable object in your car, or maybe the prowler wants to steal or damage your car, depriving you of its use, in order to make a point.

## *Advanced, persistent, threats*

To better understand what you're dealing with when it comes to APTs, check out the breakdown of the term:

- ✔ **Advanced:** It gets through your existing defenses.
- ✔ **Persistent:** It keeps trying until it gets in, and once done, it succeeds in remaining hidden from your current level of detection until it attains its objective.
- ✔ **Threat:** It can cause harm.

APT isn't just about the individual methods, but instead, that they're part of a long-range strategic plan to compromise the specific target.

## *Examining the Modern Methods of APT*

It often feels as though your adversaries are taking a page out of *The Art of War* as their playbook. The tools and methods used against you today are stealthy and difficult to detect, therefore it sometimes seems that they can spring into action on a whim. In this section, you have the opportunity to look at the variety of APT tools that an adversary can use against an organization.

### *Malware*

*Malware* is a general term that encompasses many types of software with a common theme: compromise information or systems for one or more of the following reasons:

- ✔ To disrupt computer or network operations
- ✔ To obtain sensitive and/or valuable information
- ✔ To take over control of a target system

### *Malware capabilities*

Malware uses many techniques to spread itself, infect computers, stay hidden, and fulfill its objectives. These capabilities include the following:

- ✔ **Viruses:** These are code fragments that attach themselves to legitimate computer programs, hard drive boot sectors, and document macros. They're triggered when the objects they're attached to are activated.
- ✔ **Trojan horses:** These are typically standalone programs that pretend to be something they aren't. Usually a victim is tricked into running the Trojan horse, believing that the program will fulfill some other purpose.
- ✔ **Worms:** These programs have the ability to spread from system to system with little or no help from people.
- ✔ **Ransomware:** These programs restrict access to programs or data on a system and demand that the victim pay a ransom in order to restore proper function.
- ✔ **Rootkits:** These malicious programs include mechanisms designed to evade detection — way more so than other types of malware.
- ✔ **Malicious plug-ins:** These malicious software extensions are intended for browsers, word processing programs, spreadsheet programs, and so on. Extensions are a popular way of adding functionality to popular programs, and they've caught the attention of malware producers.
- ✔ **Key loggers:** These programs record a victim's keystrokes and mouse movements and send them to the key logger's owner, who can use captured login credentials to perpetrate fraud.



Regardless of the type, all forms of malware have a common theme: deception, disruption, and/or theft of information.

### *Knowing how malware infiltrates a computer*

In order to perform its function, malware needs to be able to get into the target computer and be executed. This occurs in two main ways:

- ✓ **Attacking a vulnerability:** Malicious software is attempting to exploit a vulnerability in the target system, which could enable the malware to install itself or do whatever task it was designed for.
- ✓ **Tricking the user into executing:** A user is coerced into running a malicious program.

Some types of malware employ a blend of these. For example, a drive-by attack utilizes a website with malicious software that's installed on a victim's computer when the victim visits the website. The malicious software is able to install itself if a specific vulnerability in the victim's computer exists.

## *Phishing and other e-mail attacks*



A *phishing attack* is a form of fraud, where an attacker creates fraudulent e-mail messages designed to appear to originate from legitimate parties. The intention of the phishing message is to trick the recipient into believing that the message did originate from a legitimate party and that some action should be carried out.

The usual objectives of phishing messages include

- ✓ **Credential theft:** The phishing message may attempt to trick the recipient into visiting what appears to be a legitimate website where the user tries to log in. When the user enters login credentials, they are unknowingly giving their login and password to the attacker, who can then use them to defraud the victim.
- ✓ **Malware install:** The phishing message may contain an attachment containing malware, or it may contain a link to a website that attempts to install malware on the victim's computer. The malware is then executed, permitting the malware to begin to carry out its intended purpose.

## Assumption of breach

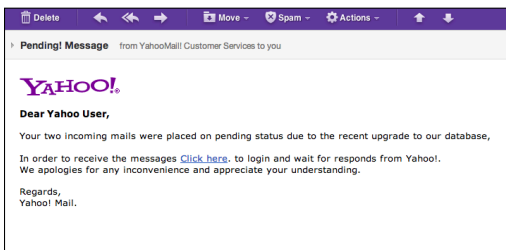
Security professionals dedicate themselves to one or more aspects of protection of their organizations' assets against compromise. Traditionally a security professional's self-talk has been, "We must prevent intrusions into our networks and systems." This thought must give way to a new assumption: Compromise is inevitable — practically a statistical certainty.

Security professionals know that it isn't possible to find and block every security hole in an organization. Not enough resources exist to do so. And besides, when an organization has

done an exemplary job of plugging technical security holes, a would-be intruder needs only to turn to the organization's personnel through phishing and other social engineering techniques. If the organization's networks and systems bar the intruder's entry, it's time to get help from an insider.

Advanced threat protection technologies have some exciting advances, including some that are the point of this book, that can really help an organization improve the technical aspect of intrusion detection and prevention.

Phishing attacks are a clever form of *social engineering*, which is defined as one of several methods used to trick people into doing something that will aid an attacker. A typical phishing message is shown in Figure 1-1.



**Figure 1-1:** An example of a phishing message.

Other forms of phishing, include

- **Spear phishing:** These are phishing attacks that are directed towards specific people, or (usually) toward people in a specific organization.





✓ **Whaling:** These are phishing attacks that target executives in a specific organization.

Spear phishing and whaling are often used in APT campaigns.

## APT Life Cycle

In order to protect an organization from advanced persistent threats, it is helpful to understand your adversary's tactics. If you hope to prevent at least some of your adversary's attempts to compromise you, you need to know how they operate. In this section, I discuss a typical life cycle methodology used by adversaries planning and executing an APT attack on an organization. The life cycle is depicted in Figure 1-2.



**Figure 1-2:** The APT life cycle.

The typical life cycle methodology used is as follows:

**1. Define the target.**

An adversary chooses a target organization and perhaps a target within an organization. The motivation for target selection may be monetary, political, or ideological in nature. The objective may be to steal money, steal data, disrupt the operations of the target system, or publicly embarrass the organization.

**2. Build the team.**

Loners seldom perform sophisticated attacks against targets; instead, the attacker(s) builds a team of experts with the necessary skills to conduct APT operations. Ever seen the movie *Ocean's Eleven*? If so, think about the team and how it was built.

**3. Build or acquire tools.**

The adversary, knowing something about the nature of the target, draws up a shopping list of the tools required to conduct reconnaissance as well as the actual attack and compromise.

**4. Conduct research and reconnaissance.**

The adversary begins to study the target, becoming intimately familiar with the people, processes, and technologies associated with the actual target. Often, this research involves identifying the actual target. For example, if an adversary wishes to steal gift card numbers from a card issuer, the adversary needs to learn how the card issuer's systems work so he can identify the actual system containing the data he wants.

**5. Response testing.**

Before starting actual attack operations, adversaries often perform initial intrusions to see whether the target organization detects the attack and responds. Based on the results of these early tests, the attack team may alter its techniques and try other types of intrusions. Perhaps the organization's monitoring and response is better in some respects than in others.

**6. Deploy the tools.**

Here, intruders begin to set up their systems, tools, and so forth to begin the attack. Can you sense the anticipation?

### 7. Make the initial intrusion.

The initial intrusion is the very start of the actual attack operation. This may take many forms, including

- Spear phishing attacks
- Whaling attacks
- Stealing a laptop or mobile device
- Compromising a public-facing system that contains one or more exploitable vulnerabilities
- Posing as an office equipment repairperson in order to plug a device into the organization's internal network

### 8. Initiate the outbound connection.

After intruders have successfully compromised a system inside of the organization's network, they initiate a communications channel from the compromised system to a system controlled by the intruders. Intruders know that they can't use a system that they actually own as the other end of their communications channel. Instead, they probably choose another compromised system elsewhere that can't be traced back to them. Otherwise, if a security engineer or law enforcement investigator got lucky and detected this outbound connection, it would lead straight to the intruders.

If the objective of the APT is to disable the target system, this may be a step you can skip. It all depends on the tools and tactics required to fulfill the operation's objective.

### 9. Expand access.

After intruders have established their foothold, they may need to revert back to research and reconnaissance in order to better understand the organization's internal network and systems architecture. This step helps locate the ultimate target system containing the data they wish to steal (or the system they wish to deface or disable).

In order to evade detection, this operation may be iterative and involve testing to determine whether their operation has been detected, as well as the



development or acquisition of other tools that couldn't have been anticipated earlier.

## 10. Collect and exfiltrate data.

After the intruders have identified the system(s) containing the data they wish to steal, they perform whatever steps are necessary to obtain the data and ship it back home through the outbound connection established earlier.

This step is rarely as easy as it sounds. Often, it may be necessary to extract the data slowly so this operation continues unnoticed. Or, if intruders are stealing data by sniffing it in an internal network, they may slowly collect and exfiltrate the data, or they may permit the target data to accumulate over a potentially long period of time (many months or more) and then ship it out in one large data transfer.

## 11. Cover your tracks and remain undetected.

Depending on the nature of the APT operation, the intruders may wish to keep an eye on things for a while. They know that the more time passes before their intrusion is detected, the more likely it is that they won't be apprehended.

An important consideration in an APT operation is the erasure of evidence of their intrusion and subsequent operations. In instances where it's not possible to disable logging, other means may be needed to make sure that log data doesn't betray the operation. Options include injecting meaningless data into the logs in order to fill them up more quickly (which in some cases causes older data to be overwritten).



Rarely will an intrusion operation neatly follow these steps. While the sequence of events in an APT operation resembles these steps, often an adversary will have to go back a step in order to improve the operation. For example, attack tools are built or acquired, and then research is conducted. Often, the results of research may indicate that additional tools are needed. Indeed, in practically every step of the APT life cycle, intruders often find that they need yet another tool to perform a task. Such is real life in a life cycle.

## Chapter 2

---

# Perusing the Methods Used to Stop APTs

---

### *In This Chapter*

- ▶ Looking back at traditional methods
  - ▶ Understanding how Big Data can be used to detect APTs
  - ▶ How cloud-based machine learning helps win the APT fight
- 

**I**magine you're the security manager of a large bank with hundreds of branches. As you review reports, you realize that small amounts of cash are disappearing from dozens of branches. This is occurring despite numerous controls such as end-of-day cash drawer balancing, security cameras, and checklists. You would have to review thousands of hours of video surveillance footage and pour over hundreds of reports to find the patterns that lead you to your thief.

This scenario is totally impractical, but it's not unlike the IT security problem today where you're expected to keep an eye on "every door" of an entire enterprise network.

Cloud-based Big Data analytics brings massive firepower to this problem. But to understand where this solution comes in, in this chapter, I first discuss the traditional methods available for combating Advanced Persistent Threats (APTs). This look is a peek in the rear-view mirror. But to understand where you're going, it's important to know where you've been. Today, adversaries are looking forward and innovating, creating more potent and stealthy threats than ever before. So I also discuss the more modern methods of combating these issues. You've got to fight fire with fire by having tools that can detect today's APTs.

## *Stepping Back to Traditional Solutions*

This book is about innovations in the effort to reduce the APT threat. In order to better understand these innovations and the short-term future, it's smart to look at the journey of the methods used to combat these threats. I'm only going to go back a few years when malware and targeted attacks were becoming commonplace.

### *Antivirus*

Antivirus programs have been around since the 1980s, and with advances in malware, antivirus (also called antimalware) programs have done a decent job of catching up. Signature and heuristic based techniques have been the mainstay of antivirus techniques. But recently the status quo is starting to crumble. For more information on malware, see Chapter 1.

### *Firewalls*

Firewalls have a long history of blocking or admitting network packets based on originating and destination IP address and port number. They're still good at that, but most threats have moved to the inside of network packets where traditional firewalls don't look. Think of it like a security guard that examines only the persons entering and leaving the building but not looking inside the packages they're carrying.

But there's the next generation firewall that performs deep packet inspection and does examine the contents of each packet, looking for malicious patterns (signature and heuristics based). Another type of firewall, called the Web Application Firewall (WAF), is specifically designed to examine the contents of packets flowing between users' browsers and web servers. WAFs are designed to detect the various types of attacks against web servers, such as SQL injection, cross-site scripting, and buffer overflow attacks.

## *Intrusion prevention systems*

Intrusion prevention systems (IPSs) are the newer generation of intrusion detection systems (IDSs) that got their start in the 1990s. IDSs could only generate alerts when they detected malicious traffic, but an IPS can be configured to permit or block network packets based on their origin, destination, and particulars about their contents.

## *Other APT defenses*

To make sure you have a complete view of all the efforts to combat APTs, there are a few other mentionables worth, um, mentioning. They are

- ✔ **Web filters:** These systems control which websites users in an organization are permitted to visit while on the job. Web filters have the ability to block access to websites based on whether they're relevant to the business at hand, as well as being able to block access to websites that may represent a real threat to the organization (such as those known to host malware).
- ✔ **Spam filters:** We love them and we hate them. Spam filters, when properly tuned and maintained, block over 99 percent of the spam that rockets in from everywhere. While good spam filters block most attacks, spear phishing attacks have a very good chance of bypassing spam filters. Therefore, messages with malicious intent will get through to targeted personnel.

## *Stopping APT Using Modern Methods*

You can employ many methods to stop APTs. This section gives you a better idea of those ways.

## *Stopping APTs with Big Data analytics*

There is strength in numbers. This familiar phrase instructs you about phenomena seen in nature: flocks of birds, herds of sheep, and schools of fish. In the continuing battle against APTs, the advantage that Big Data analytics gives you is a lot more detail regarding the effects of APTs on their target organizations. In other words, collecting and comparing events across numerous organizations, and from one organization over an extended period of time, has a great advantage over just looking at events inside of one organization.

In this section, I discuss the ways in which Big Data analytics contributes to the balance of power in the APT wars.

### *Joining the dark side*

They say that “familiarity breeds contempt,” and this is true when it comes to the analysis of malware and APTs. However, familiarity with APTs also gives the observer additional insight into the workings of APTs and botnets in particular.

By permitting a system to join a botnet, it’s possible to intercept and analyze all interaction between the command and control (C&C) and an infected machine. By understanding both the traffic patterns as well as the specific messages used, it’s then very easy to positively recognize APT traffic when these patterns and messages are seen elsewhere.



Using the time-proven principles of honeypots and honeynets, walking a mile in a compromised system’s shoes gives Seculert a unique perspective on the precise nature of a malware or bot infection. Botnets aren’t just seen from the outside; they’re observed from within. The grappling hook, the infection, the burial deep in the heart of the infected system, and the start of a new bot army recruit are all observed closely. Seculert’s modern methods remember all these details and use them to detect APT infiltrations in its customers’ networks.

### *Event correlation*

By analyzing log data from numerous sources in an organization, the events represented by that log data can be correlated, which helps to better understand those events and their true



extent. This technique has been used by hardware based security information and event management (SIEM) solutions for many years.

Try to imagine a security alerting system with the ability to correlate events across all the entry and exit points in an organization, and you can see that it's possible to detect and understand events that were difficult to detect by using traditional means. Innovative companies are doing this advanced event correlation today to detect APTs that are flying beneath the radar of traditional solutions (see the earlier section "Stepping Back to Traditional Solutions").

### ***Event extrapolation***

By analyzing data from various sources, you can identify other victim machines even without access to log data from their part of the organization. Log data from one part of an organization may reveal botnet-controlled systems that are communicating with other "owned" systems.

### ***Machine learning***

Machine learning isn't new. With techniques like expert systems, neural networks, and artificial intelligence, machine learning can accomplish a lot of useful work provided it's given good data and clear objectives.

By using machine learning in a Big Data environment, it's possible to distinguish network traffic that's associated with botnets and malware, from network traffic that's benign. There are patterns of communication that are unique to botnets and malware that good machine learning can easily distinguish. For instance, malware periodically connects to its command and control server in order to receive instructions. Also, malware related traffic tends to be more periodic than traffic from a random website. Based on these facts, it's possible to apply statistical techniques to detect and measure the periodicity of any such traffic. Alone, this isn't enough to positively determine the presence of malware, but it's still an important clue.

### ***APT's long tail nature***

The interaction of users on the Internet is a good example of a typical "long tail" phenomenon. It's usually not possible to accurately classify the nature of traffic between a user and the Internet by examining a network packet or two. Instead, you

must observe this traffic for a while to understand whether the undercurrents are harmful or benign in nature.

This, together with the fact that there are over a billion Internet users, means that an almost unimaginable volume of data represents the entirety of Internet interaction. This is why it takes Big Data techniques to properly analyze this volume of data.

APT behavior is long tail because an APT present on a user's computer may lie dormant for long periods of time. It may initially communicate with its C&C (command and control) network after installing itself, but then communicate often — or rarely — over a period of days, weeks, or months. It can be a very long time before the APT begins to communicate in tell-tale ways that distinguish it from non-hostile software.

### *Analyzing malware*

Surely an organization in the business of detecting APTs is going to be familiar with malware. They can permit their analysis systems to be compromised and taken over by botnets. But this isn't the only way to gain familiarity with malware.

Customers can also upload known malware directly into a service, which turns the malware loose on a system in order to observe it and understand its interactions over time. This gives the service highly reliable data on a malware behavioral profile. Knowing this gives the service the ability to recognize the same malware behavior in a customer's network.

Here's how it works. Customers can manually upload suspicious files in order for the service to examine them and determine if they're indeed malicious. The service is able to run the malware in a "sandbox," which is a specialized system with safeguards not used on end user systems. The service analyzes the malware and its network interaction and then puts this malware behavioral profile information into its Big Data analytics system, so that it can recognize the presence of this malware on other customers' networks (or even on the same customer's network).



If you're a Seculert customer, you can also automatically upload files through Seculert's API. For example, a customer's e-mail server can upload attachments to Seculert's platform for analysis. Seculert can inform the e-mail server whether the attachment should be removed.

## Upload your own logs to Seculert

Organizations that use Seculert's APT protection platform can go one step further by uploading their own gateway traffic log data to Seculert. The primary benefit here is that Seculert can add a customer's traffic logs to the already-massive database of events from other organizations. This practice helps all Seculert customers by giving Seculert that much more data to analyze.

Another benefit of uploading one's own logs is the ability for Seculert to better identify malware or bots in one's own network. While Seculert has the ability to do this in the absence of an organization's log data, there may be clues in log data that may help identify additional compromised systems.

## *Applying cloud-based Big Data analytics to detect malware*

Imagine that you're detecting APTs for hundreds or thousands of customers all at once. Not only are you looking at a truly massive amount of data, but you have to ask yourself, where can machine learning on this scale be implemented?

If you're thinking, the Cloud, you'd be spot on. Combined forces are stronger than individuals. A cloud-based Big Data solution against APTs is going to be stronger than organizations going at it alone with their point solutions.

In this section, I describe some of the reasons why cloud-based analytics beat the other methods hands-down.

### *Scalability and elasticity*

Only the vast computing infrastructures of the largest cloud providers such as Amazon, Google, or SoftLayer are capable of supporting the massively parallel Big Data machine learning systems required for the job.

It's not only the fact that hundreds or thousands of processors can be brought to bear on Big Data problems but also the elasticity of cloud resources that make this economically possible.

Seculert uses the power of Hadoop to accomplish this task. Hadoop is an open source software framework designed to work across thousands of systems on petabytes (millions of gigabytes) of data, on the biggest computational challenges in the world.

### ***Strength in numbers***

There are significant advantages to cloud-based processing APT protection. First, in cloud-based APT protection, data from hundreds of organizations is analyzed in parallel. With this unique “big picture” view, it’s more likely that the APT protection system is going to recognize the presence of threats in any one of them, than in the traditional solutions found today.

Second, APTs are usually custom-tailored and targeted for a specific campaign. Therefore, anti virus software won’t recognize APT malware. This is where cloud-based machine-learning techniques are used to detect APT attacks.

## Chapter 3

---

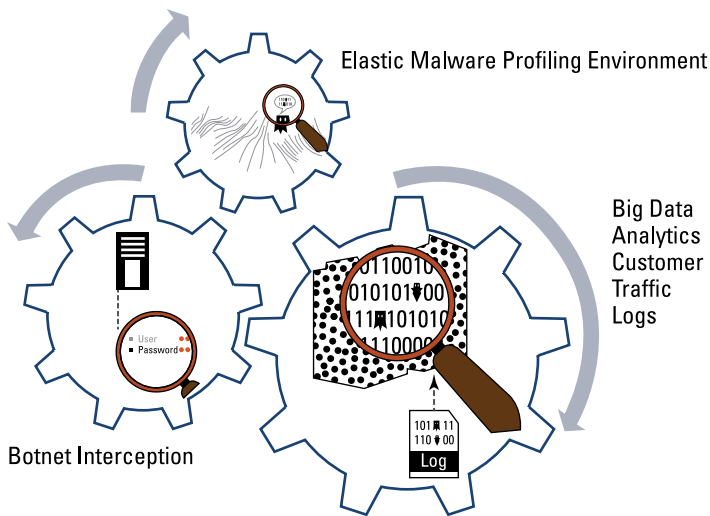
# Looking into Seculert's APT Protection Architecture

.....

### *In This Chapter*

- ▶ Checking out the elastic sandbox environment
  - ▶ Using Big Data analytics with automatic traffic log analysis
  - ▶ Getting a grasp on botnet interception
  - ▶ Looking at the Seculert Dashboard and API
- .....

**I**f you've been reading this book straight through to this point, you may have noticed that I explain concepts about architecture without actually showing you how its solution works. So in this chapter, I give you Seculert's architecture of how the big picture works (see Figure 3-1). The Seculert platform contains three primary components: Botnet interception, automatic traffic log file analysis, and an elastic sandbox environment.



**Figure 3-1:** The overall Seculert APT protection architecture.

## Traipsing through the Elastic Sandbox Environment

The *elastic sandbox* is the part of the Seculert platform where malware is introduced, examined, and profiled. Try thinking of this as an Internet Petri dish where all kinds of nasty things are allowed to grow, all under the microscope. Malware is introduced to the sandbox using three principle methods:

- ✔ **Customer upload:** Seculert customers can upload samples of suspected malware that they find on their own systems. Doing this helps Seculert examine the software to determine whether it is, in fact, malicious.
- ✔ **Botnet interception:** Seculert has many computers on the Internet that resemble computers used by ordinary people. Seculert permits these computers to become infected with APTs; this allows Seculert to examine

the resulting malware traffic over time, which permits Seculert to gather intelligence about the threat. Seculert correlates this activity with customers' web activity logs to help pinpoint infected systems.

✓ **Partner upload:** Seculert business partners routinely share malware that they find in their own labs or in the wild.

The elastic sandbox permits these malware samples to infect systems and do whatever they want to do. Seculert monitors each malware infection closely, including all its network communications. This helps Seculert recognize similar behavior of infections elsewhere.

Seculert carefully simulates many different types of environments, including various geographic regions. This technique helps “tease out” different types of APT behavior. The reason for this is that APTs are sometimes built to infect specific environments based on known criteria. By varying the environment, you can more effectively profile APTs in many different conditions found in the wild.

Seculert receives over 40,000 new malware samples every single day. Seculert's elastic sandbox analyzes this traffic generated by the APTs, and information is sent to the automatic traffic log analysis component in the system (more on the traffic log analysis in the following section “Performing Analysis with Automatic Traffic Log Analysis”). This includes traffic between computers infected with bots and their command and control (C&C) masters.



Seculert's elastic sandbox is responsible for the discovery of new botnets including Ramnit, Kelihos.B, Mahdi, Shamoon, and Dexter. By the time you read this, the sandbox may have already uncovered a few more botnets.

The elastic sandbox is the malware laboratory, which observes malware and APTs for weeks, months, and even years to detect activity. In Figure 3-2, you see the Sandbox image, and in Figure 3-3, you see the Sandbox results.

Home / Elastic Sandbox

Upload suspicious samples directly to the Elastic Sandbox and allow the samples to live in a close to real-world elastic environment, where the malware behavior and evolution will be closely examined over time.

Upload EXE File

1. Analysis Region: Any Region  US  UK  DE

2. Analysis Period:  2 Min  5 Min  10 Min  30 Min  60 Min

3. Choose File:

**Uploaded Files**

File Name	File Size	Region	Period	Upload Date	File Status
sa.exe	761.65 KB	US	10	2013-08-08T12:07:14.61	Malicious
sa.exe	761.65 KB	US	2	2013-08-08T12:07:03.597	Malicious
ze.exe	174.63 KB	DE	2	2013-08-08T12:06:53.66	Malicious
ze.exe	174.63 KB	US	2	2013-08-08T12:06:35.673	Malicious
sa-file	717.65 KB	US	10	2013-08-08T08:00:22.007	Unrecognized
sa-file	717.65 KB	US	2	2013-08-08T08:00:11.257	Unrecognized

**Figure 3-2:** Elastic Sandbox results displayed on the dashboard.

## Performing Big Data Analytics with Automatic Traffic Log Analysis

The *automatic traffic log analysis* is the part of the Seculert system that performs the Big Data multi-layered analysis on APTs. Think of it as the brain that processes data from various sources to come up with its conclusions about APTs in customer environments. The traffic log module is depicted in Figure 3-4.



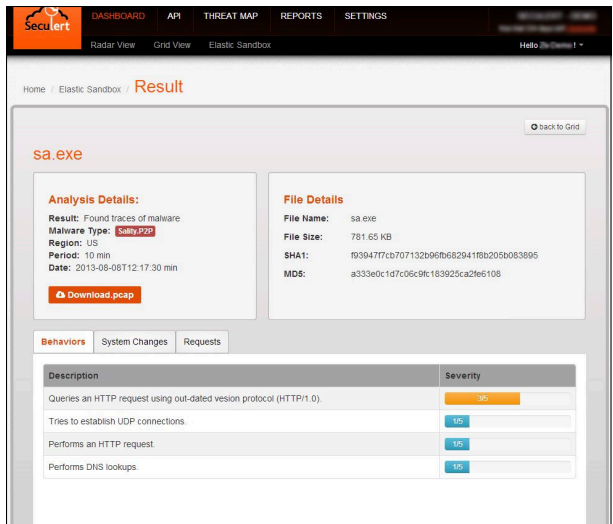


Figure 3-3: Malware details are available by clicking one of the results.

Two major data sources exist for traffic log analysis:

✔ **The elastic sandbox that creates a malware behavioral profile:** This component is where malware is grown and observed. The profile generated in the sandbox is sent to the log analysis module for processing. For more information on the sandbox, see the preceding section, “Traipsing through the Elastic Sandbox Environment.”

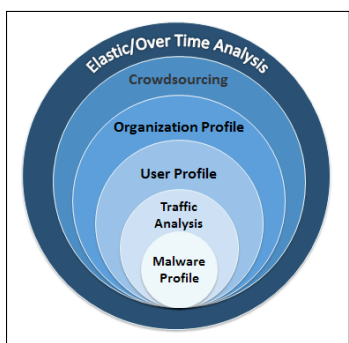


Figure 3-4: The six main layers to Seculert's log analysis.

- ✔ **Customer uploads:** Customers can upload their logs from several brands of web filter systems, such as BlueCoat ProxySG, Websense, Cisco IronPort Web Security Appliance, and all common web proxy or secure web gateway solutions that support access logs.

You can use several techniques for processing traffic logs:

- ✔ **Malware profile data layer:** Seculert receives and analyzes tens of thousands of unique malware samples each day from different sources (Seculert's internal systems, public sources, partners, and other security companies). It analyzes and profiles the malware communication patterns in an elastic cloud-based environment.
- ✔ **Traffic analysis data layer:** Seculert applies different methodologies in order to analyze Internet traffic logs and to detect suspicious and malicious activity, including domain and IP reputation, Domain Generation Algorithm detection, and botnet traffic correlation.
- ✔ **User profile and organization profile data layers:** Seculert automatically profiles each user machine's traffic logs — as well as overall organization traffic logs — in order to find abnormal activity and detect unknown and malicious communications. For instance, if a user usually browses to U.S. websites between 9:00 a.m. and 5:00 p.m., an abnormal activity will be HTTP POST data being sent to a server in China at 2:00 a.m.
- ✔ **Crowdsourced data layer:** Whenever Seculert identifies malicious activity in logs from one customer, it automatically detects similar malicious activities in other customers' logs, even if the logs are from different types of security solutions or vendors.
- ✔ **Elastic/over time analysis of cross-correlated data layers:** APT attacks reside undetected within the corporate network for a long period of time (hence they are *persistent*). Seculert uses elastic cloud facilities (Infrastructure-as-a-Service, or IaaS) for the Big Data analytics. This process allows Seculert to instantly analyze logs that extend over a long period of time (for example, months or even years of traffic logs).

## *Understanding Botnet Interception*

*Botnet interception* is the part of the platform where Seculert permits APTs and other malware to run while being closely observed. It works like this:

1. Malware that customers and partners upload (and those that Seculert acquires by other means) automatically runs in the Seculert elastic sandbox environment.
2. Seculert observes the malware and identifies the ways that the malware communicates with its C&C servers.
3. Seculert checks if there is a list of domains that may be used in the future in the APT’s C&C servers.
4. Seculert can automatically identify the domains that aren’t yet registered.
5. Seculert automatically registers future malware domains and points them to Seculert’s “Sinkhole” server.

Whenever the current C&C server’s domain gets suspended or blocked by the ISP (which is part of the traditional tactic for fighting the botnet), the malware will start communicating with Seculert’s “Sinkhole” server.

6. Seculert’s “Sinkhole” automatically logs the initial communication and immediately ends the session, so that the malware won’t consider Seculert’s “Sinkhole” server as the C&C server, and move on to the next domain.
7. Seculert knows that the information in the “Sinkhole” system is enough to identify the IP address and often even the actual name of the infected machine, as well as the web-interface domains and identities used by the victim on the infected machine.

This is how Seculert is able to identify infected systems inside of a customer’s environment, even without using information provided by the customer.

## *Evaluating the Seculert Dashboard and API*

After you register, you get a free evaluation of Seculert, and where existing customers (and customers evaluating the system) can perform several functions to configure the system:

- ✔ **Define core networks:** Organizations define the external IP networks or address ranges used in their groups.
- ✔ **Define internal portal domains:** Organizations define the URLs of internal portals used in their groups. One URL example is `https://portal.mycorp.com`.
- ✔ **Define internal service domains:** Organizations specify portals, such as `https://owa.mycorp.com`.
- ✔ **Define e-mail domains:** Organizations specify e-mail domains used, such as `user@mycorp.com`.
- ✔ **Define partner domains:** Organizations specify the domains used by their partners, such as `https://partners.mycorp.com`.
- ✔ **Define customer domains:** Organizations specify the portals where their customers log in, such as `https://customers.mycorp.com`.

After customers are up and running with Seculert, they can upload data:

- ✔ **Upload malware:** Customers can upload malware found in their environments. The dashboard sends these to the elastic sandbox. See the earlier section in this chapter entitled “Traipsing through the Elastic Sandbox Environment” for more info on the sandbox.
- ✔ **Upload logs:** Customers can upload their logs from their web filter access logs, which are sent to the elastic sandbox.

The really cool features are the views available in the dashboard that indicate the machines that are compromised with APT malware. These views appear in Figures 3-5 and 3-6. Customers can also upload malware using Seculert's RESTful API, otherwise known as a *Web service*. A powerful feature is the ability to loop sophisticated malware intelligence back into existing systems. For example, Seculert's platform integrates with firewalls, secure web gateways, and SIEM devices.



Figure 3-5: Seculert's dashboard displays devices infected with malware.

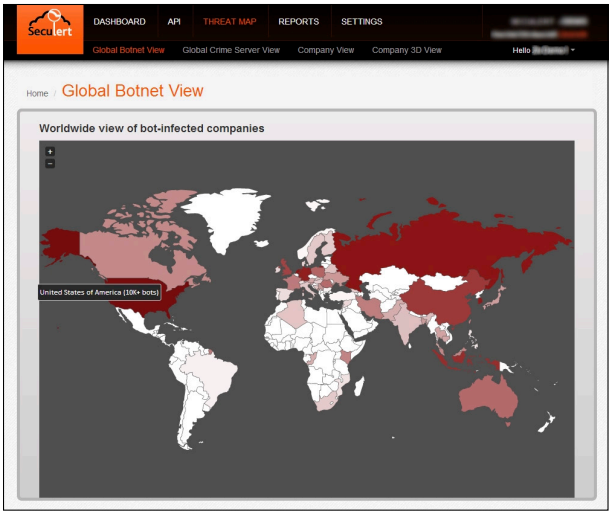


Figure 3-6: The dashboard shows APT threats based on geography.



## Chapter 4

# Enabling Business in the Shadow of APT

---

### *In This Chapter*

- ▶ Understanding the advantages of cloud-based APT protection
  - ▶ Making BYOD work
  - ▶ Extending the reach of threat intelligence into customer and partner infrastructures
- 

**R**eally good security is supposed to be a business enabler, but lately it seems that malware, spear-phishing, spam, botnets, and advanced persistent threats (APTs) have IT organizations on the ropes. IT security departments were just beginning to feel like they had the whole endpoint security problem under control with anti-malware, application whitelisting, USB control, and endpoint malware filtering, and now people start showing up to work with their personal iPads, Android tablets, and ultrabooks that they want to connect to the corporate network.

Bring Your Own Device (BYOD) has been an unwelcome disruption from IT departments and IT security departments. The prospect of supporting and managing security in a heterogeneous environment in a season of “doing more with less” is giving everyone heartburn. But cloud-based APT protection is helping to re-center the balance of power and permit IT security to once again be a business enabler.

In this chapter, I discuss some of the ways that cloud-based solutions are giving back where it’s needed the most.

## *Stopping APT without Stopping Business*

IT is a business enabler because it permits the business to carry out its operations more efficiently than by humans alone. And in many cases, information technology creates new business activities that are just not possible any other way. Big Data is a great example of this.

There is no question that the security threats have never been more potent than they are now. As organizations pour more of their wealth into their IT systems, adversaries are getting more creative with new and innovative ways to access and obtain that wealth for themselves.

Unless you've been living under a rock for the past decade, it's easy to see how computer hacking attacks have grown ever more sophisticated. How are you supposed to fight back and continue doing business without enacting so many security controls that the department of IT security doesn't turn into the department of business prevention?

## *Protecting the Business with Cloud-Based APT Protection*

Organizations can use cloud-based APT protection systems to augment their processes. In this section I describe the components of a typical management program and tell you how a service complements those processes.

Here's the breakdown:

- ✓ **Gather information.** Subscribe to alerts regarding all in-scope hardware and software components. Also, subscribe to bulletins that announce information about real-world threats.
- ✓ **Develop an incident response capability.** Write procedures to be used when a security incident occurs.
- ✓ **Develop a perimeter defense capability.** Obtain defenses to block known external threats:



- Firewalls to block all unnecessary network traffic while permitting only network traffic specifically required for the business
  - Web filtering system for blocking access to non-business sites as well as sites that are known to host malware
  - Spam blocking capabilities for preventing unwanted e-mail, such as phishing from reaching users' e-mails
  - Data leakage prevention (DLP), which comes in many flavors and includes many different capabilities ranging from USB storage device control to e-mail content inspection
  - Web application firewall (WAF) if the organization has web-based applications
- ✔ **Develop an intrusion detection and prevention capability.** Obtain an IPS that detects and/or prevents attacks on the enterprise network.
- ✔ **Develop a malware protection and removal capability.** Install and actively manage anti-malware software on all systems that are commonly affected by malware. Write procedures and obtain tools to be used when malware is discovered on a system or device in the organization.
- ✔ **Develop a patch management capability.** Implement tools and procedures to quickly deploy security patches and configuration changes to at-risk systems.
- ✔ **Develop an APT protection capability.** Use tools such as cloud-based APT protection systems to become informed about compromised internal systems. This enables the organization to detect systems that have already been compromised.

Unlike the other controls listed in this section, adding a cloud-based APT protection system doesn't involve the addition of any on-premises hardware or software, and doesn't introduce additional failure points to the organization's infrastructure. Because they are cloud-based, services continuously improve their APT protection capabilities with no changes or updates required to customers' networks.



Seculert innovates at this same pace. An organization using Seculert's platform doesn't need to incorporate additional processes. Instead, you just view the Seculert dashboard one or more times each day to see if there are any new active APTs in the network, or integrate the results automatically by using Seculert's API. After a threat is identified, existing malware removal procedures should be sufficient.

## Enabling BYOD

BYOD is all about the phenomenon where employees are bringing their personally owned devices to work, namely tablet computers, such as iPads, and smartphones, such as iPhones and Androids. And, employees cite greater productivity and job satisfaction, so they want to use these devices for both personal and work purposes.

Who can blame them? Having company e-mail on my smartphone means I can stay in touch with my peers, superiors, and customers without having to be tethered to a laptop-at-a-hotspot (which is almost as constraining as being at work).

The reason why CIOs and IT Managers are upset about BYOD, though, is all about the cost of support. Lawyers and corporate risk managers are often concerned about data leakage. But the reason why CISOs and security and risk managers are concerned about BYOD is the plethora of security risks that are introduced, including the following:

- ✓ **Firewall — lack of visibility and control:** The ability for the organization to enforce firewall configuration is impaired or removed altogether. Also, it's difficult or impossible to prevent the user from tampering with firewall settings.
- ✓ **Anti-malware — lack of visibility and control:** The organization's ability to monitor, update, and prevent tampering with anti-malware is weakened.
- ✓ **Patching — lack of visibility and control.** It may be difficult for organizations to include personally-owned devices in its patch management system.
- ✓ **Security configuration — lack of visibility and control.** IT may have less control over the security configuration

of BYOD devices. It's more of an honor system than an enforceable mechanism.

- ✓ **Local authentication — lack of visibility and control.** Often it's more difficult to manage local access to personally owned devices in the same way that IT can control access to company owned assets.

Are you getting the idea here? With the lack of direct control over devices not owned by the organization, it's often more difficult to enforce security policies around authentication and security controls such as firewalls, patching, and security configurations.

But take a step back and look at the big picture. Are you wondering why these matters are of concern for the CISO? Well, data security in an organization is typically there to protect the organization's most sensitive information, whatever it might be. The ability to protect this information is significantly compromised if endpoints (laptops, desktops, tablets, and smartphones — whoever owns them) can't be centrally managed and monitored.



The core of information security is usually concerned with the protection of key information. Security measures directed elsewhere are usually in support of this key objective.

Cloud-based APT protection systems mitigate the BYOD concern in an indirect but powerful way. Instead of adding more devices or programs inside of a customer's infrastructure, they detect APTs by gathering intelligence directly from within botnets and analyzing their network traffic logs over time. This is a powerful alternative to signature-based malware detection systems or data leakage prevention systems.



Seculert's platform enables BYOD and provides visibility to all devices connecting to an organization's network, not just those that are owned, managed, and monitored by the organization (the primary angst of BYOD).

## *Extending Web Filtering*

Web filtering products from companies provide excellent protection against a variety of threats related to websites that an

organization's employees are likely to visit. But sometimes an APT-compromised computer will visit websites without triggering alarms. By sending copies of activity logs from web filtering systems, it's possible to detect other compromised systems.

## *Protection from Threats from Customers and Partners*

Numerous APT campaigns infiltrate the target organization via customers and partners. Customers and partners are often trusted more than the general public, and this level of trust may provide an APT with an easier path of entry. In addition to detecting APTs in an organization's own systems, it's possible to detect compromised systems in an organization's partner and customer base.

When setting up the Seculert platform, an organization can simply provide Seculert with the URLs that customers and partners access inside the organization (for instance, <http://partner.company.com>, or <http://customers.company.com>). As Seculert gathers intelligence from botnets, Seculert can identify compromised systems in customer and partner organizations that may pose a threat to the organization. This is a capability that surpasses traditional security controls that are limited to the organization's own network infrastructure (and in some cases even to just the systems it owns and controls).

### **Seculert synergy**

Could other such synergies be developed in the future? Perhaps. One idea might be for an e-mail server to automatically upload attachments to Seculert for analysis. Seculert can examine the malware and inform the

e-mail server whether the attachment should be removed before sending the message to the recipient. This would effectively stop spear-phishing attacks even when using unique malware not seen in the wild.

## Seculert's cloud-based APT protection

The secret sauce in Seculert's business solution is that they can find threats in an organization that's 100 percent cloud based. The implications of Seculert's platform are significant for several reasons:

- ✔ **No server or network hardware:** When an organization uses a cloud-based service, it doesn't have to manage a server or network hardware.
- ✔ **No software to install and maintain:** With Seculert's platform, you don't have on-premises software to install, configure, and manage. Seculert's software resides entirely in the cloud, so its customers don't have to devote any resources to this activity.

- ✔ **No single points of failure:** Unlike firewalls, intrusion prevention systems (IPSs), and other network based security solutions, there are no additional components in the customer's environment that add to the list of failure points.
- ✔ **No rackspace:** Seculert's platform is 100 percent cloud based, which means its solution occupies no rackspace at all.

If you're like me, you've got to be thinking, how can Seculert detect malware in my environment without the presence of any system or device in my network, and without being "in the loop" in any of my network communications? Well, check out Chapter 3 for more information on Seculert.



## Chapter 5

---

# Ten Ways Seculert Helps Reduce APTs

---

### *In This Chapter*

- ▶ Finding more ways to counter the danger of APTs
- 

**S**eculert's cloud-based APT protection platform has many advantages. While I've covered many of them throughout the book, I placed them here in one convenient place for you to cherry-pick as needed.

### *Botnet Perspective*

By permitting (even encouraging) its special cloud-based elastic systems to join actual botnets, Seculert systems act as double agents to gather intelligence about the botnet from within the botnet. This permits Seculert to gather actual samples of botnet communications, examine botnet malware, and discover the IP addresses, and other forensic-enabled data of systems compromised in a customer's environment.

### *Cloud-Based*

By being a cloud-based software-as-a-service (SaaS) platform, Seculert brings immensely powerful tools to an organization without the need to manage yet another complex on-premises device.

The advantage that cloud-based services bring to an organization is this: The organization doesn't need to invest in IT equipment and undertake the usual set of upkeep activities such as hardware maintenance, version upgrades, and compatibility with other systems. Because it's cloud based, Seculert's platform is updated frequently, so you don't have to worry about it.

## *Big Data Analysis*

Seculert examines terabytes of log data daily using Hadoop and other Big Data analysis tools. More than just a big log cruncher, Seculert has expertise in the area of APT protection using machine learning, among millions of activity log entries.

## *Elastic Infrastructure*

Seculert uses the Amazon MapReduce elastic infrastructure to analyze log data from botnets, customer logs, and other sources. This can, at times, require vast amounts of massively parallel computing power that most IT organizations can't undertake on their own.

## *Zero IT Footprint*

Using Seculert means having no additional systems, appliances, or programs in the organization. It also means no re-routing of any traffic through Seculert for analysis. You don't even have to open firewall holes.

## *No Single Points of Failure*

Seculert doesn't "get in the middle" of your internal or external communications. This means that your entire IT infrastructure, including all components, servers, devices, and providers operates as usual. Using Seculert means no new single points of failure.



## ***Extend Web Filtering Systems***

Organizations can extend the value of their web filtering systems such as BlueCoat ProxySG, Websense, and Cisco IronPort Web Security Appliances by uploading HTTP files to Seculert's platform. This helps Seculert identify more compromised systems in your organization than you could otherwise have known about.

## ***Identifies Threats in Customer and Partner Organizations***

Seculert's APT protection can automatically detect compromised machines not only in your own infrastructure but also within the customer and partner organizations who connect to your systems, even if just through a web browser. With Seculert, you're automatically getting intelligence about compromised systems that communicate with you.

Imagine the surprise when one of your partner organizations gets an e-mail from you saying that one of its systems has been compromised. Until you explain how you did it, the partner organization might wonder how you came to know this.

## ***Crowdsourcing***

Customers who use Seculert benefit from crowdsourcing. Seculert is vendor agnostic, which allows customers to upload their HTTP traffic log files and malware samples. The more data that Seculert has to work with, the more its customers benefit. This is a win-win-win for Seculert, you, and Seculert's other customers.

## ***Ridiculously Easy Setup***

At the very beginning of the Seculert Setup Guide is the following warning:

*Warning! Reading this guide will take MUCH longer than the actual setup. Setup takes up to 3 minutes.*

From my own experience this is completely true. All you do is enter your IP blocks, internal and external domains, and e-mail domains, and you're done.

Ongoing management of the Seculert platform can be just as easy. Log in to Seculert and examine the dashboard. Any newly compromised systems will appear before your eyes. Seculert sends e-mail alerts if you want to know about these incidents right now.

## Get a handle on APTs today

Your information very well may be under attack right now. People pay handsomely and have a wealth of tools and techniques available to obtain your information. Stop them in their tracks. With this book, you discover how APTs can be detected and how to stop them and further protect your vital information.

- **Understand the nature of APTs** — *learn what they are all about*
- **Explore the methods used by APT operations** — *get a jump-start at protecting your data*
- **Look into the solutions to the APT** — *study both the traditional and modern approaches*
- **Find out more about Seculert's solution** — *help the service work for you*



**Open the book and find:**

- **The features and benefits APT protection**
- **How to protect your data and assets**
- **Solutions that work for you**
- **How to enable your business in spite of APTs**
- **Ten ways Seculert helps reduce APTs**

**Go to [Dummies.com](https://www.dummies.com)**

for videos, step-by-step examples,  
how-to articles, or to shop!

FOR  
**DUMMIES**<sup>®</sup>  
A Wiley Brand

ISBN: 978-1-118-76385-8  
Not for resale

These materials are the copyright of John Wiley & Sons, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.