Making Everything Easier!™

Special Edition

Advanced Evasion Techniques

FOR DUMMIES®

Compliments of

McAfee®
An Intel Company

Klaus Majewski, CISSP, CISA

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

Much of McAfee's advanced evasion technology comes from its acquisition of Stonesoft Corporation in 2013. Commenting on the sophistication of this technology in the 2013 Magic Quadrant for Enterprise Network Firewall, Gartner notes that McAfee has been "very innovative in analyzing threat evasion techniques" and that "its firewall features are innovative against modern and advanced threats." *

* Greg Young, "Magic Quadrant for Enterprise Network Firewalls", Gartner, 7 February 2013.

Advanced Evasion Techniques

FOR

DUMMIES®

SPECIAL EDITION

by Klaus Majewski, CISSP, CISA

WILEY

A John Wiley and Sons, Ltd, Publication

Advanced Evasion Techniques For Dummies®, Special Edition

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom *For Dummies* book for your business or organisation, contact CorporateDevelopment@wiley.com. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

ISBN: 978-1-118-43272-3

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Introduction

Welcome to *Advanced Evasion Techniques For Dummies*, your guide to the security evasion techniques that have become a serious preoccupation of the IT industry. This isn't to say that IT security hasn't been a major source of worry in the past; on the contrary, the last decade has been witness to growing security threats, cybercrime and compliance regulations. However, recent research has shed new light on the business of protection and demonstrated that advanced evasions will break the security protection model that most organizations are using today. Given this changing threat landscape we need to rethink traditional security models. And that's where this book comes in.

About This Book

This book provides an overview of network security in general, and explains how cybercriminals can use hidden or currently undetectable methods to penetrate protected network systems. *Advanced evasion techniques (AETs)* bypass traditional common network security solutions. They can transport any attack or exploit through network security devices and firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS), and even routers doing deep packet inspection.

In this book you'll find out all about AETs, and get useful pointers and advice to help you secure your organization. If you're working in government, the military, banking, industry, e-commerce or with other critical infrastructures, read this book to find out what you're up against and how to better protect against advanced evasions.

Foolish Assumptions

In writing this book, we've made some assumptions about you:

- You're an IT professional, or work closely with specialists, and you possess at least basic knowledge of IT networks.
- You're familiar with network security terminology (for example, you can differentiate between a bug and a new feature).
- You're interested in network security evaluation and/or risk assessment for your organization.
- You have a proactive approach to IT and want to learn where the security model is heading.

How to Use This Book

Advanced Evasion Techniques For Dummies is divided into four concise and information-packed chapters. Here's a glimpse of what you can expect:

- **Chapter 1, Understanding the Security Risk,** is a primer that walks you through the concepts of network attacks, patching and different levels of protection.
- **Chapter 2, Getting the Lowdown on Advanced Evasion Techniques,** starts with some background on evasion research and then explains AETs and why traditional detection fails.
- **Chapter 3, Considering the AET Threat to Industry,** looks at industrial control systems, the regulatory framework, and why AETs are the weapon of choice for attacks on high-value targets.
- **Chapter 4, Protecting Against AETs,** provides practical steps for assessing risk, testing your network and deploying protective measures.

Icons Used in This Book

To make it easy to navigate to the most useful information, we use icons to highlight key text:

The target draws your attention to top-notch advice.

The knotted string highlights important information to bear in mind.

Watch out for these potential pitfalls.

Where to Go from Here

You can take the traditional route and read this book straight through. Or, you can skip between sections or chapters, using the headings as your guide to pinpoint the information you need. Whichever way you read, you can't go wrong. Both paths lead to the same outcome – a better grasp of what AETs are, what kind of risk they represent to your business and how you can protect against them.

Chapter 1

Understanding the Security Risk

In This Chapter

- Knowing the current state of play with cybercriminals
- Seeing how network attacks work
- Linking vulnerability and patching
- Recognizing the limitations of layered security

This chapter gives you a good grounding in the current state of Internet security. We look at the Internet from the point of view of cybercriminals, and see how rosy the picture is from their side. We explore what network attacks are – who carries them out, and how. We consider patching to correct bugs, and show how this creates vulnerabilities. And finally, we take a look at the common approach to fending off attacks – layered security – and how this fails in the face of AETs.

Seeing How Cybercriminals Are Operating

From the cybercriminal's point of view, the Internet is full of targets. Some targets are well protected, but most can be easily hacked. For example, home computers are often easy targets and criminals can use them as platforms to perform attacks against other computers.

Counting the cost of cybercrime

The Ponemon Institute's 2012 Cost of Cyber Crime Study found that the median annualized cost of cybercrime for 56 benchmarked major organizations was $8.9 million per organization. The study found that companies faced crimes caused by malicious code, denial of service, stolen or hijacked devices, malicious insiders and other attacks. The Institute also noted that 'all industries fall victim to cybercrime', including retail, hospitality and consumer, with the sectors of defense, utilities, energy and finance likely to experience the highest associated costs.

With no universal Internet police, and without law enforcement that successfully covers international Internet criminality, criminals perceive the Internet as a low-risk environment. Online crime may be hard to trace; the possibility of getting caught is potentially small – even if caught, jail sentences are short; and the huge scale of potential rewards is attractive.

In addition, cybercriminals can reach millions of targets worldwide, which means that each crime doesn't have to be big. If you steal $100 from one million different targets then you make $100 million profit. If each victim only suffers a $100 loss, it's such a small amount that the police may not even bother to investigate.

Given these conditions, you can see why cybercrime continues to increase and continues to challenge the legal community. As cybercriminality becomes more industrialized, organized, sophisticated and businesslike, it poses a greater threat to enterprises, their business and their bottom line.

Understanding Network Attacks

Two kinds of attacks exist: network-based and host-based. Table 1-1 explains the differences.

Table 1-1 Comparing Network-Based and Host-Based Attacks

Type of Attack	*Where It Attacks*	*Example*	*Type of Protection Used*
Network-based	Over the network	Conficker worm	Network security devices
Host-based	Locally at the target host	Melissa virus	Anti-virus products and host security systems

In this book we concentrate on network-based attacks because AETs work mainly with this type of attack. AETs conceal network-based attacks so that network security devices don't see them as attacks or exploits, enabling criminals to gain access to targets on the network.

Knowing the network-attack players

A typical network attack has three players:

- **Attacker device:** Sends attack network traffic to the target device and tries to break into it and, finally, remotely control it.
- **Network security device:** Normally set somewhere between the attacker and the target device; its mission is to protect the target device against attacks.
- **Target device:** Can be anything from a normal laptop to a specific corporate enterprise resource planning (ERP) server.

Conficker still in the wild

The Conficker worm, first detected in November 2008, exploits vulnerability in the Server Service on Windows computers and uses a specially crafted remote procedure call (RPC) request to force a buffer overflow and execute shellcode on the target computer – enabling a criminal to take remote control of the machine. Some of Conficker's well-known victims include the French army, who had to ground fighter jets in 2009, and the Greater Manchester Police, who were forced to shut down their network for three days in 2010.

Microsoft's Security Intelligence Report from April 2012, which gathered data from over 660 million systems worldwide, found that the Conficker worm had been detected about 220 million times worldwide in the previous two and a half years. Research showed that Conficker infections were mostly a result of weak or stolen passwords and exploitations of vulnerabilities for which security updates exist but hadn't been implemented.

Looking at a typical attack flow

Here are the steps in a typical network attack flow:

1. **Collect information.**

   Attackers try to find as much information as possible about the target device and its environment. They can use different sources of information like the WHOIS database, web pages and the domain name system (DNS). They can also use social engineering and try to get information from people who work in the company where the target device is located. In addition, plenty of different information-gathering programs are available from the Internet that attackers can use to automatically dig up more information about the target device.

2. **Search for vulnerabilities.**

   Many online resources provide in-depth information about vulnerabilities in different operating systems and applications. Attackers can also use specific scanner programs that probe networks for unsecured ports or seek attack susceptibilities in application architecture.

3. **Select the correct attack method.**

   Attackers have to choose an appropriate attack that exploits the vulnerability of the target device.

4. **Attack.**

   Attackers try to execute their own code in the target device or open a command prompt so that they can create a reliable remote control connection to the target device.

5. **Steal the information.**

   Attackers search for the information in the device. Depending on what the attackers are after, they can either steal the information from the device or use the target device as a platform to launch a new attack further into the target's environment.

Understanding Patching

If attackers can't find any vulnerability in the target system then surely they can't find an attack that will compromise the device? Theoretically, this is true. But in practice bugs and patches create additional vulnerability.

Knowing that software will always have bugs

Many argue that the ultimate security solution is totally bug-free software that no one can exploit. Unfortunately, creating such software is a mission impossible. The US military tried once to create a software program that they could mathematically prove to contain no bugs. The project was very costly and the program itself was quite short. They didn't try again.

Studies conducted on software quality have reported that for every thousand lines of code you always have at least three bugs.

Modern software programs contain several million lines of code, and finding all the bugs during the internal quality testing phase is impossible. In 2005 Toyota recalled 160,000 Prius hybrid cars following reports of warning lights illuminating for no reason and

engines stalling unexpectedly, thanks to a bug in the smart car's embedded code. All operating systems and applications contain bugs. Microsoft, for example, uses Service Pack updates to fix thousands of bugs and security holes in its operating systems.

Seeing how patching fixes bugs

Software vendors know that bugs exist in all software. So they're continuously providing bug fixes. They do so through a process called *patching* – a manual or automated process that provides software bug fixes to software users.

Unfortunately, a time window exists between discovering a bug, coming up with a solution and then deploying the fix. It's during this time window that attackers can take advantage.

Some circumstances heighten vulnerability:

- Patches can break production servers instead of fixing them. (An attacker's target system is a collection of the base operating system and business software, all of which contains bugs. For simplicity, we call this kind of computer and its software a *production server*.) Patches fix some process or method in the software, but it is possible that by fixing one problem, it inadvertently changes another process or method in the software, causing something new to break. The tightly integrated relationship of operating system and business software means that a patch for the operating system, fixing a vulnerability there, may introduce a new problem for the business software.

  Security-conscious companies test their patches before they apply them so they can be sure that the fix doesn't break their production server. But this increases the time window during which the production server is vulnerable.

- You can't patch very critical production servers that control processes (industrial machine controllers or nuclear reactor controllers, for example) immediately, because you can't restart or disturb them while they're controlling the process. (See Chapter 3 for more details.) Advanced intrusion prevention systems (IPS) today can temporarily address this problem, virtually patching target devices (blocking network traffic intended to exploit the specific vulnerability the patch would fix) until the actual patch can be applied to the production server.

Realizing That Layered Security Isn't Enough

Network security professionals are tackling the problem of vulnerable servers in many ways. One of them is *layered security*. You can have several layers of network security devices, and the devices can perform different tasks. For example, at the perimeter of the organization, firewalls and VPN concentrators restrict traffic that's going to reach the organization. The next layer might contain intrusion prevention systems (IPS) to inspect traffic for any malware or attacks.

Another layered approach is to add network security devices (usually IPS) in front of the vulnerable service to create a so-called virtual patch in which the network security device stops all traffic attempting to access the vulnerability (allowing through traffic bound for the target which is not attempting to access the vulnerability).

If a way exists to bypass layered network security or virtual patching then vulnerable production servers are in danger. As we show in the following chapters, AETs can do exactly that. Patching and layered network security are not always enough to protect organizations from AET attacks.

Think of the situation as being similar to when you've locked up the rest of your house to protect against burglars but have left your backdoor wide open. Cybercriminals can bypass layered security with AETs, giving them easy access to your production servers. In addition, AETs do not often leave traces for forensics analysis as traditional network security devices neither see nor detect AETs, so they will not flag the traffic for later analysis.

Getting Wise to the Invisible Threat

IT decision makers should know about AETs and vulnerabilities in layered security, taking them into account in their risk management decisions. Because few people are aware of AETs, they are very attractive and valuable tools for cybercriminals.

In a 2012 interview (published in *Infosecurity* magazine), Electronic Art's vice-president and chief information security officer, Spencer Mott, had some wise words. He said there are two types of chief information security officers: 'those that have been attacked, and those who don't know they've been attacked'.

Chapter 2

Getting the Lowdown on Advanced Evasion Techniques

In This Chapter

- Knowing what AETs are
- Following the research into advanced evasions
- Understanding the basic principles of AETs
- Taking a look at AETs in action
- Seeing the problems with current network security devices

In this chapter, we tell you all about AETs – what they are, how much of a risk they pose to security, how they work and why they get past traditional network security devices.

Defining AETs

A leading principle in internet protocol design is the robustness principle:

> *The implementation of a protocol must be robust. Each implementation must expect to interoperate with others created by different individuals. While the goal of this specification is to be explicit about the protocol, there is the possibility of differing interpretations. In general, an implementation should be conservative in its sending behavior, and liberal in its receiving behavior. That is, it should be careful to send well-formed datagrams, but should accept any datagram that it can interpret (e.g., not object to technical errors where the meaning is still clear).*

– RFC 760 – Department of Defense Standard Internet Protocol, January 1980

The robustness engineering principle is a leading cornerstone of Internet protocol design. However, Internet protocols are often complicated and allow for various interpretations in implementation.

By making use of rarely used protocol properties in unusual combinations, an attacker can make it difficult for network security to detect an attack. In addition, an attacker may make detection even harder by deliberately crafting network traffic that disregards conventional protocols. If the receiving end of the traffic liberally attempts to interpret the traffic, an attack can reach the destination undetected. Such concealment techniques are collectively known as *evasion techniques*.

An *advanced* evasion technique enables the successful delivery of known malicious code without detection by:

- Combining one or several known evasion methods to create a new technique that's delivered over several layers of the network simultaneously
- Being able to change the combination of evasions during the attack
- Evading inspection through clever design

Researching Evasions

Evasions aren't a new phenomenon. Ptacek and Newsham wrote an academic paper in January 1998 called 'Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection'. They explained how simple evasion techniques work and how attackers use them to bypass network security devices.

McAfee started AET research in 2007. The project began because Research and Development (R&D) could not find good commercial evasion testing tools that they could use to test network security devices. So the R&D Vulnerability Analysis Team decided to build their own automated advanced evasion testing tool to test their network security products.

First, they looked for any research that had been done to describe different kinds of evasions, and how they work. Some theoretical technical papers regarding evasions were available, but none described implementation of ideas.

Then, to see what had already been developed in this field, the team started to look for open source or free tools that implemented evasion techniques. They could find only a couple of tools and their coverage was minimal.

So the team built their own version of an evasion tool, incorporating all they had learned, and continued their research into evasions and preventing them. In doing so, they discovered several hundred new evasions.

The team learned four lessons while implementing the testing tool:

- Evasions exist in every protocol.
- Evasions can be combined together to create new evasions.
- The order of combined evasions is important.
- The number of different evasion combinations is massive.

When the Vulnerability Analysis Team started testing their own products with advanced evasions, they found that some of the advanced evasions bypassed the security devices. They wanted to know whether advanced evasions could also bypass other security products. So they asked independent institutions to test leading next generation firewalls and intrusion prevention systems (IPS) to see how other vendors fared. The team were surprised when they heard the results.

The independent institutions were easily able to bypass all tested network security devices.

Typically, they ran the test environment for two seconds and during that time period several AETs were successful. Even very basic evasions bypassed many devices. Just imagine, what would have happened if they had run the same test environment for a few days?

The Vulnerability Analysis Team was worried. This was a devastating result for the whole security community. Almost all existing network security devices were vulnerable to AETs. It seemed that advanced evasions were a neglected area of security, perhaps because good evasion testing tools did not exist to test the vulnerability.

So the team contacted CERT-FI in Finland, where the R&D lab was based. (CERT-FI promotes security by disseminating information on threats to information security.) The team provided 23 sample traffic captures of working advanced evasions and asked CERT-FI to give this information to all relevant security vendors.

Amazingly, the response from other network security vendors was poor. They either didn't respond at all, or they said that AETs weren't a problem for their devices. It took almost two years and 287 new sample advanced evasion traffic captures before network security vendors started to understand the scope of the problem.

Realizing the Massive Scope for AETs

The scope for different AETs is vast. The situation is similar to that of the anti-virus industry 15 years ago, where everyone knew that a massive virus problem existed, but no one in the industry could tell how big the problem was. Today, the anti-virus industry has all but stopped counting the number of viruses and virus variations in existence, simply because the number is too large. Similarly, the number of unique advanced evasion possibilities is now so massive that it is difficult to comprehend.

For example, McAfee discovered 147 atomic evasions during 2010. Combining two or more evasions further expands the number of unique evasion possibilities, and the number quickly grows from there as the order of atomic evasions within a combination adds uniqueness as well. In mathematical terms, the number of unique combinations of evasions is a binary number that has 147 digits (2^{147}) – a truly massive variety of potential combinations.

All of these evasion combinations do not work, but too many of them do. From a security perspective, the challenge is to find those combinations that are deadly and create a defense for them. The need for automated advanced evasion testing tools is mandatory for this work.

Working through the Key Principles of AETs

You can identify AETs according to certain underlying principles. AETs

- Are delivered in a highly liberal way (see the 'Defining AETs' section earlier in this chapter)
- Target traditional security devices
- Use rarely used protocol properties
- Use unusual combinations of evasions
- Craft network traffic that disregards strict protocol specifications
- Exploit the technical and inspection limitations of security devices: memory capacity, performance optimization, design flaws and so on

AETs are a means to disguise cyber-attacks in order to avoid detection and blocking by network security systems. AETs enable cybercriminals to deliver malicious content to a vulnerable system without detection, which would normally stop the threat. Traditional network security is ineffective against AETs in the same way that traditional radar is ineffective against a stealth fighter attack.

Relying exclusively on protocol anomalies or protocol violations to block advanced evasion techniques is not sufficient. Although some protocol anomalies and violations occur only when AETs are being used, most protocol irregularities emerge due to a slightly flawed implementation of commonly used Internet applications.

For more accurate detection, you need to analyze and decode network traffic layer by layer. Because an attack may be concealed by evasions in many different layers, you need to carry out network traffic normalization and careful analysis of every appropriate layer.

Looking at an Evasion Example

Evasion techniques often do not need to be that advanced to penetrate traditional network defenses. This is why there is so much concern about them. In fact, the simple fragmentation evasion is a good starting place and will still evade many of the leading network security products.

Consider the infamous Conficker worm (see Chapter 1), first detected in November 2008, which exploits a vulnerability in the Server service of Windows computers. Though devastating at the time, this worm is now easily detected by all legitimate network security devices.

Network traffic in a Transmission Control Protocol/Internet Protocol (TCP/IP) network is based on packets. You can fragment these packets into smaller packets if needed, but common practice is to use as few packets as possible to improve efficiencies. To implement one of the simplest evasions possible, break the Conficker worm into two fragments, then send them through the network security device, waiting ten seconds between fragments. Sadly, when changed this way, many network security devices will not detect the Conficker worm, even with everything up to date.

What happened?

Well, network security devices need to handle millions of connections every second. This leads to the limitation that they can only keep some part of those connections in memory. The normal amount of memory allocated for the inspected traffic is about seven seconds per connection.

In the Conficker example, two fragments are sent ten seconds apart. So for the first seven seconds, the network security device has a partial match, but will do nothing with the traffic until it has a complete match. Only a complete and positive match to the detection fingerprint will elicit any action from the network security device.

But after seven seconds, the network security device times out its held memory, recycling it for other use. This means all investigation on the first part and partial match of Conficker is lost. When the second part of Conficker comes through at the ten second mark, like the first part, the network security

device does not make a complete match, so it takes no action. In this way, both parts of Conficker are allowed through to attack the target device and not even an alert is made.

This simple fragmentation AET is a rudimentary example that demonstrates vulnerabilities of devices that have too little memory compared to the amount of traffic they're inspecting. While memory limitation-based vulnerabilities may be less frequent in the future as network security devices adopt 64-bit architectures and are able to access more memory, it illustrates the point and there are many other vulnerabilities that AETs can exploit.

Considering Weak Points in Traditional Network Security Devices

Organizations face two critical questions:

- Why are traditional network security devices unable to offer effective protection against advanced evasions?
- Why are the fixes for normal exploits ineffective against the advanced evasion problem?

The answer lies in traffic handling, inspection and detection. Each of these capabilities is instrumental in building proper advanced evasion protection in next-generation firewalls or even intrusion prevention systems (IPS).

Are you sacrificing security for speed?

Network security devices should do traffic normalization on each TCP/IP layer. But many network security devices favor speed over network security, and therefore they take short cuts. These devices do not inspect all four layers of the TCP/IP model. This often allows the network security device to operate faster, but leaves the network vulnerable to advanced evasions.

AETs exploit shortcuts and weaknesses in normalization and inspection processes.

For more information about layers of the TCP/IP model, refer to W. Richard Stevens' *TCP/IP Illustrated, Volume 1: The Protocols* (Addison-Wesley, 1994).

Packet-based inspection

Most traditional, signature-focused network security devices only inspect segments or pseudo-packets, and cannot inspect a constant data stream. This fundamental design issue is extremely difficult to change. Especially in the case of hardware-based products, the redesign of security devices would require a significant R&D outlay.

Many packet-based network security devices offload low-level packet handling functions to custom-built hardware components to improve performance and efficiency. This design philosophy focuses on known exploits and locks these vendors into a processing path that assumes signature-based pattern matching of short network traffic segments. The combination of hardware offload and short segment analysis requires less central processing unit (CPU) and memory resources, so over time, these vendors tend to save manufacturing costs, investing less into device CPU and memory.

Data-stream-based inspection requires more memory and CPU capacity to continue to perform effectively in throughput. Converting to data-stream-based inspection from segment-based inspection requires significant changes to low-level functions. Most of the signature matching products do not have the design flexibility to make these changes because they implemented their processing logic in hardware.

For many signature-focused traditional network security vendors, redesigning their hardware-based products or changing to a 64-bit environment to make more memory available is not practical because of hardware production commitments, which compromise their flexibility.

AETs exploit segment-based or pseudo-packet-based inspection by spreading attacks over segments or pseudo packet boundaries.

Exploit-based detection

Effective protocol reassembly and normalization enables proper advanced evasion handling and ensures that a vulnerability-based approach can detect and prevent attacks successfully. On the other hand, exploit-based approaches, relying on packet-oriented pattern matching and short segment analysis, do not consider deep protocol reassembly and stream normalization to be important. As a result, they are often incapable of identifying advanced evasions and pose a serious risk to the overall security posture.

A pure signature-based approach, as is common with exploit-based and packet-oriented defenses, would require a unique signature for every combination of advanced evasions. Because of the massive number of known combinations of advanced evasions, the sheer volume of required signatures for this approach would make the system unmanageable (too many signatures needed).

A typical network security device has between 3,000 and 30,000 signatures active at any given time. If you attempted to protect against some of the advanced evasion techniques using a signature-based approach, you might create 1,000,000 new advanced evasion signatures as a good starting effort. Unfortunately, technology today cannot process traffic against even this many signatures while still maintaining acceptable throughput performance.

Fortunately, there is another way to solve this problem. Read on if you want to know the solution.

Chapter 3

Considering the AET Threat to Industry

In This Chapter

- Knowing about advanced persistent threats
- Protecting industrial control systems

In this chapter, we look at AETs in relation to large, critical systems – industrial control systems – to help you understand the importance of protecting against the threat at all levels of an organization.

Seeing AETs as a Master Key for Cybercriminals

AETs aren't yet well known and they can bypass common network security devices, so they're very powerful tools for cybercriminals.

Cybercriminals aim to use minimum effort against their target. They don't want to use methods that are overkill; after all, they're running their operations like a normal business and so they have to keep costs down.

Advanced evasion testing isn't easy. McAfee took more than four years to create an advanced evasion testing tool, and the developers were network security professionals. So it stands to reason that developing an AET on the cybercriminal side costs a lot of money, time and brainpower.

For this reason, criminals use AETs against targets that are very difficult or where the potential reward value is very high. These are typically targets that have several layers of network security in place and good network surveillance. For example, Professor Andrew Blyth and his team at the University of Glamorgan perform network forensics whenever UK government organizations have been targets of an attack. He has commented that 'AETs pose a serious threat to network security and we have already seen evidence of hackers using them in the wild'.

Protecting Industrial Control Systems

The emergence of Stuxnet in 2010 encouraged many organizations to focus on the security of their supervisory control and data acquisition (SCADA) networks as part of their industrial control systems (ICS).

The vulnerability of industrial networks and the possible consequences for the security of people and the environment mean that people with responsibility for securing industrial networks must work hard to perform advanced risk assessment and find suitable solutions.

However, even with many organizations tightly securing their SCADA networks, another malware attack in the fall of 2011 – the Duqu Trojan – proved that conventional attack methods were still successful and ICS security still had many gaps.

Therefore, security for SCADA and other ICS networks, especially with the emergence of AET attacks, is still a concern.

Limiting exposure

It's not just SCADA networks but rather *all* ICS systems that are faced with security challenges. Figure 3-1 shows that while some organizations are more likely to be attacked than others, every organization is at risk of becoming a victim of cybercrime.

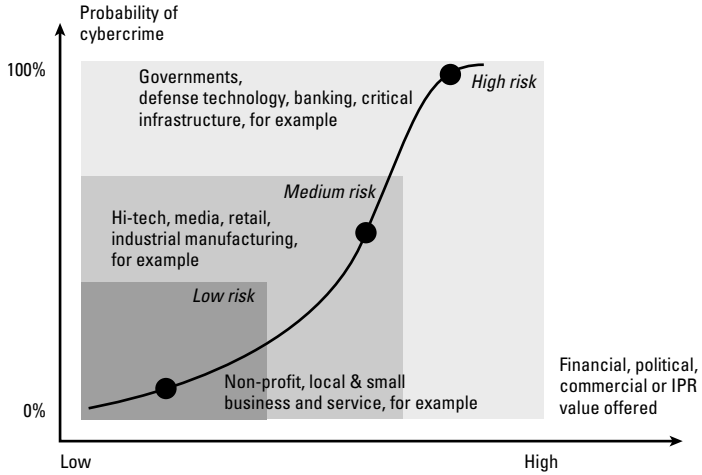

Figure 3-1: How the onslaught of advanced threats affects different industries.

Because of this, efforts are underway to find generally applicable solutions. For example, the NERC-CIP standard (North American Electric Reliability Corporation-Critical Infrastructure Protection) is mandatory for large power grids in the United States. However, no uniform global regulation exists for the protection of ICS networks, so various standards of various levels of effectiveness are used today, such as Achilles by Wurldtech Security Technology and ISA Secure.

Similarly, research into possible security gaps is in its infancy. For example, in 2011 NSS Labs uncovered security gaps in programmable logic controllers (PLC) that are used to monitor and control industrial processes. If hackers were to exploit this gap, they'd gain complete control over the system and could control the main processor.

Virtual patching

One way to limit the risk of SCADA systems is to remove them from the network. You reduce lines of attack considerably if no connection exists to the outside. But a full removal from the network is frequently impossible. For this reason, organizations and companies with SCADA systems often use security solutions such as intrusion prevention systems (IPS).

Intrusion prevention system (IPS) devices monitor the entire data traffic and only allow it into the network if there's no indication of a threat. If malware tries to gain access to the network, they automatically disrupt the data connection and thus prevent the malware from penetrating into the network. This security method also allows for the virtual patching of servers and services by protecting vulnerable servers that will only be patched during the next maintenance window: an important requirement of industrial networks.

But AETs disguise or modify cyber-attacks to the extent that they're not identified and blocked by security systems, resulting in the undetected infiltration of malicious content into the unprotected systems. In contrast to simple evasion techniques, AETs:

- Vary the methods used to disguise an attack
- Can be combined to a virtually unlimited degree
- Use different levels in network traffic

And hence they weaken conventional security mechanisms.

The devices that inspect data traffic, such as next-generation firewalls and IPS, use different techniques, but most of them work with protocol analysis and pattern-matching signature detection. This approach detects certain attack patterns displayed by malware in data traffic, which exploits weak spots in a communication system.

But if threat patterns are constantly changing, most next generation firewalls and IPSs struggle to detect the hidden attack through a pattern match within the data packet. Sometimes all that's needed is a small change, such as a segment offset, and they no longer resemble any of the attack patterns filed in the signature set. The result: the security system doesn't detect the hidden malicious code and lets it enter the network. Since no alarm would advise of a possible threat, cybercriminals can then freely move around the system to find a possible weak spot or a non-patched server.

Looking at a simple example

Cybercriminals seem to have better understanding of AETs than network security testing manufacturers.

Think about a paper machine or a nuclear power plant or an electric grid. All are controlled by some kind of computer or system of computers. Normally, the control computers have operating systems developed five to ten years ago, and they're probably still controlled using Windows NT. The life span of an industrial control system is easily 15 years.

The problem is that the control computer can't be updated regularly, because many of the updates require rebooting of the machine. These industrial control environment machines are rebooted only once or twice a year during maintenance windows.

So when a new patch becomes available for the control machine, network security staff can't apply it immediately. It might be six months before the staff applies the patch. Meanwhile, members of staff protect the control computer with network security devices like next generation firewalls or IPSs. But the control computer is vulnerable while the patch isn't applied. Cybercriminals have a window of opportunity.

Previously, industrial control systems were in a totally separate network, but lately system administrators have connected these to office networks and some even directly to the Internet because business requires connections to outside systems. This means that cybercriminals can have network access to these systems.

Cybercriminals will use known exploits against the unpatched control computer (Windows NT in the example) and use AETs to hide the exploit from the network security devices. Now they can take control of the paper machine, nuclear reactor or electric grid.

The lesson here is to make sure that you're protected against AETs if you're running an ICS environment where you can't apply patches immediately.

Chapter 4

Protecting Against AETs

In This Chapter

- Seeing how your network fares in an AET test
- Working out the risks
- Inspecting traffic
- Opting for centralized management
- Testing solutions in a real-life environment

When it comes to AETs, no network security device on the market today can guarantee 100 per cent protection (though some come very close). Unlike traditional threats (like Stuxnet or Conficker, for example) where a signature update seemed to fix the problem, a simple device update does not fix the AET problem. How AETs operate and the sheer number of possible evasion combinations mean that protection against AETs is an uphill battle – and we're just starting the fight.

Still, organizations should take steps to increase their protection against the threat. In fact, any organization that fails to understand and reduce the risk of AETs is opening its network to known and unknown vulnerabilities. In an age of sophisticated cybercrime, many organizations – including government agencies and enterprises – risk serious repercussions for failing to ready their networks in the fight against AETs.

This chapter provides practical guidance that organizations can apply to increase their level of protection against AETs.

Testing Your Own Network

Arm yourself with knowledge – know the holes in your network.

McAfee started to talk publicly about AETs in late 2010. Many people saw AET demonstrations, but they weren't convinced because those demonstrated network security devices weren't theirs. They were also certain that they could tweak their security devices so that no AETs would be able to bypass them.

So McAfee provided a portable version of an advanced evasion testing tool, called the Antievasion Readiness Test (AERT).

The Antievasion Readiness Test provides:

- Objective, real-life data on your current and planned network security devices' anti-evasion capabilities
- An Evasion Risk Assessment for management in the form of a test report, accompanying test data, and an advisory and risk mitigation plan

The tool uses the organization's own devices and configurations – exactly as they're running in real life. In that way, organizations get a fully realistic and accurate testing situation. The test itself is also run by a vendor-independent, third-party service provider to ensure objectivity and independence from manufacturers and technologies.

Table 4-1 outlines when to take the evasion test.

Table 4-1 Coming to Terms with Cyber-Risk Intelligence: Knowing When to Take the Evasion Test

Situations	*Challenges*
Security Level Evaluation/ audits of existing security devices	Identifying whether or not evasions pose a direct threat
	Evaluating and managing security risks correctly
New Product Evaluation for investment decisions	Assessing which product offers the highest protection against evasions
	Verifying vendor claims
Redesigning network security	Investigating whether your security level is high enough
	Identifying where to place or relocate next generation firewalls, IPSs or other deep-packet inspection devices, and knowing what kind to use

Go online and check out `mcaf.ee/aet` for more information about the Antievasion Readiness Test.

Analyzing the Risks

Audit your critical infrastructure and analyze the most significant assets of your organization:

- How you store them
- Where you store them
- Whether you back up the information

Prioritize your assets by relative importance for your business, and make sure your critical assets and public services have the best possible protection against AETs.

Using Traffic Inspection Methods

Employ traffic inspection methods to solve the advanced evasion problem.

When you identify the assets that you're protecting, you can then map out all the different ways to access those assets. Cybercriminals have to use those same access paths to reach your information if they're going to attack through the network.

As a clever network security specialist, you can secure those access paths using advanced network security solutions. Unfortunately, traditional network security technology is not flexible enough to effectively deal with the AET threat. However, a technology called *traffic normalization* is able to remove advanced evasions from the network traffic travelling down those access paths, and reveal hidden attacks.

Getting to grips with traffic normalization

Using an analogy to the English language is a helpful way of understanding traffic normalization.

Advanced evasions are like using different dialects to hide the actual meaning of the spoken word. Let's assume, for example, that two cybercriminals who would like to rob a bank intend to discuss their plans in a crowded room in a way that nobody else understands what they're trying to do. If the cybercriminals speak normally, the other people in the room can hear what the cybercriminals are saying and stop them if they understand that they're going to rob a bank. To get around this problem, the cybercriminals can use not just one, but several different English dialects and mix them with very specific slang words (as an AET), just to make sure that they're the only people in the room who actually understand what they're saying.

Now just imagine that all those other people in the room are police officers (or traditional network security, if you will). They try to scan all the discussions around them in order

to find those cybercriminals by listening for specific keywords like 'bank', 'robbery', 'money', 'gold' and 'keys'. If they hear any of these words in a specific discussion, they arrest the participants in that discussion and halt their actions. However, these cybercriminals are dedicated and they have strong motivation to break into that bank. They've spent time and effort in learning specific English dialects and slang in order to discuss their bank robbery so that no other people can understand them, so they use very advanced evasion techniques to mask their intentions and do their job. This kind of cybercriminal group is an advanced persistent threat (APT).

In this example, the solution is to understand the same dialects and slang that the cybercriminals are using, so you can translate their discussion back to standard textbook English. This process of translating different dialects back to textbook English – of removing dialects and slang words and replacing them with common words that are part of standard English – is called *normalization*. Now, when the language is understandable, you can scan it and look for specific words, like 'bank', 'robbery' and so on, that indicate to you that the cybercriminals are planning to rob a bank.

You can do the same thing in network traffic. If cybercriminals are using AETs to hide their attacks, you can undertake network traffic normalization to remove evasions and reveal the actual traffic that was hidden beneath them. You can then use standard signature matching processes to detect attacks from the normalized network traffic. In real life, this process is much more complicated than we describe here, but this explanation gives you the essentials.

If you're really interested and would like more details, check out the *Multilayer Traffic Normalization and Data Stream Based Inspection: Essential Design Principles of the Stonesoft IPS* whitepaper from `mcaf.ee/aet`.

Implementing traffic normalization

Advanced evasions work so well against most network security devices because they only inspect part of the data stream.

They don't inspect the complete data stream, so they can't fully normalize the network traffic. As a result, advanced evasions are able to hide attacks from them.

For the traffic normalization process to work against AETs, you have to implement it completely. Doing only part of the process doesn't work. In other words, you have to be able to perform traffic normalization on a complete stream of data, not just for some parts of it.

Changing from packet-based inspection to full stream-based inspection isn't easy. Doing so requires big changes for low-level packet handling and a fundamentally different architecture for the network security device itself. Full-stream inspection uses more memory on the device and affects the performance of the network security device.

For these reasons, it may take some time before network security devices that can fully protect against AETs are available. For example, McAfee took about five years of researching to create protection against AETs. Nobody's protection against AETs is perfect yet, but vendors that are actively researching AETs have a huge advantage against those who aren't researching the area at all.

The evasions themselves have been out there since 1998 and are still very effective against network security devices. But don't despair – know that full traffic normalization and stream-based inspection can solve the problem. Check out the McAfee website at `mcaf.ee/aet` to find out more about these solutions.

What's still needed is pressure on the other vendors to implement this protection into their products. McAfee has been working actively with network device testing laboratories, ICSA Labs and NSS Labs, to include AET testing into their network security device certification and testing programs. Currently, these laboratories are only testing very simple evasions, but we sincerely hope that they'll move to more

realistic AET testing in the future. Such a move would force other network security vendors to research AETs and provide protection against them in order to pass ICSA Labs or NSS Labs testing.

Deploying a Centralized Approach

Signature-based network security devices (especially exploit-based) only detect and block predefined and well-known AETs. If the evasions change slightly or combine together in a more complex way, these devices fail the test.

The dynamic and constantly evolving nature of evasions means that centralized management is a must-have defense for networks and critical digital assets.

Organizations must continuously update network security protection to keep up with the threats. Situation awareness, detailed analysis of attack methods and understanding about how the exploits were conducted play a key role. Knowing which attacks were made isn't enough; you need to know how cybercriminals attacked.

The difference in the level of evasion detection and protection provided by different network security vendors is enormous. Because network administrators may not be able to proactively protect against AETs, their only option is to be prepared for immediate and effective reaction. That means they need to

- Centrally monitor all network devices – regardless of vendor or types – for suspicious activity
- Pinpoint attacks and remediate, quickly updating and reconfiguring network devices, as necessary, to minimize damage

A single, centralized management console enables administrators to monitor from a single location, and to create configurations only once before deploying to all devices on the network.

Re-evaluating Patch Management

When possible, patching vulnerable systems provides ultimate protection against network attacks, regardless of whether they've been delivered by AETs. Evasions may help attackers bypass network security devices, but they cannot actually attack a patched system.

Because patch testing and deployment takes time under even the best circumstances, you should have network security devices with virtual patching and other security measures.

Checking Your Existing Intrusion Prevention Solution

Evaluate the capabilities of your existing network security devices to protect your network against AETs.

- How effective are they against evasions today?
- Do they enable you to react quickly to attacks or easily update against newly-discovered threats?

Be critical and proactive: look for alternative options. Table 4-2 outlines how McAfee compares with other network security devices available.

Table 4-2 Comparing Evasion Protections

McAfee	*Other Network Security Devices*
Full-stack visibility McAfee decodes and normalizes traffic on all protocol layers	Analysis of limited selection of layers
Normalization-based evasion removal The normalization process removes the evasions before the data stream inspection	Inspection of individual segments or pseudo packets
Application data stream-based detection Vulnerability based fingerprints detect exploits in the normalized application level data streams	Vulnerability-based, exploit-based, shell code detection; banner matching only
In-house research and tools Evasion-proof product quality assured with automated evasion fuzzing tests	Publicly available information and third-party tools
Updates and upgrades Anti-evasion technology automatically updated	Limited evasion coverage and delayed updates

AETs have changed the security landscape permanently. If a security device isn't capable of handling evasions, your network is vulnerable.

Conducting Field Testing

Many security vendors know how to survive simulated and recorded evasions when these are predefined in stable lab environments. However, when facing live and dynamic evasion disguised exploits, these systems are blind and incapable of protecting your data assets.

If you really want to know the level of your current protection against AETs, test the anti-evasion capabilities of your network security devices in your own environment with your own policies and configurations.

Is your seat belt fastened?

Game-changing threat

In 2010, McAfee discovered that there are millions and millions of ways to bypass even the most advanced network security solution without being detected, blocked or traced. This new breed of cyber threat was called Advanced Evasion Techniques or AETs.

Today the risk of your network being compromised by AETs is growing faster than your security vendor is willing to admit. Why? Because the security industry was also taken by surprise: AETs are a real threat that can do serious damage to your business.

No stone unturned

McAfee network security is the most effective protection available against AETs. Combining full stack inspection and data normalization on all protocol layers, McAfee leave no stone unturned. It focuses on the actual content being transmitted in data streams and detects evasion techniques even when they are applied on multiple protocol levels.

McAfee network security can be adapted to any network environment – physical, virtual or hybrid – and is backed by the industry's best AETs testing tools and environment

Find out if you are protected against AETS at:
mcaf.ee/aet

McAfee, An Intel Company
2821 Mission College Boulevard
Santa Clara, CA, 95054
USA
sales@mcafee.com

McAfee®
An Intel Company

Your indispensable guide to maintaining the security of your network against AETs

The threat posed by advanced evasion techniques (AETs) is growing, and research shows that organizations need to rethink their security models. AETs are able to bypass any security device and ultimately cause significant damage to corporate networks. The bad news is that AETs are a furtive, undetectable procedure. The good news is that solutions are evolving to combat the danger. Read all about it in this book.

- ***Brush up on your network knowledge* – *stay abreast of stealthy techniques***
- ***Adapt your policies* – *maximize your knowledge to protect your systems***
- ***Prepare for the future* – *fortify your operations against future threats***

Open the book and find:

- **What you should know about network security**
- **The full story on advanced evasion techniques**
- **A look at how to evade evasions**
- **Best practices for your network protection**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles or to shop!

Klaus Majewski and McAfee deliver software-based, dynamic, and customer-driven network security solutions that secure information flows and simplify security management. McAfee is a recognized researcher of advanced evasion techniques used in cyber attacks targeted to bypass security systems.

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-43272-3
Book not for resale