Report

McAfee
An Intel Company

The Security Industry's Dirty Little Secret

The debate over advanced evasion techniques (AETs)

Table of Contents

Introduction

Advanced persistent threats (APTs) have been central to network security discussions in the past few years, with many organizations implementing new solutions to protect themselves from this determined type of malware. Yet, cybercriminals continue to be effective in penetrating the network defenses of even the strongest security systems, including some very high-profile enterprises.

One of the dirty little secret weapons hackers use to bypass security systems and penetrate even the most locked-down networks are advanced evasion techniques (AETs). While AETs are not a secret among the hacking community—where they are well known and have been in widespread use for several years—there are misunderstandings, misinterpretation, and ineffective safeguards in use by the security experts charged with blocking AETs.

To assess what IT security professionals understood about AETs, and what measures are being put in place to stop them, McAfee commissioned Vanson Bourne in January 2014 to survey 800 CIOs and security managers from the US, UK, Germany, France, Australia, Brazil, and South Africa. The findings indicated that most respondents do not fully understand AETs and, as a consequence, lack the proper technology to stop them.

Among the top findings were the following:

- More than one in five admits their network was breached (22%), and nearly 40% of those breached believe that AETs played a key role.
- A full 39% of IT decision makers do not believe they have methods to detect and track AETs within their organization.
- Almost two-thirds of respondents (63%) say that the biggest challenge when trying to implement technology against AETs is convincing the board they are a real and serious threat.

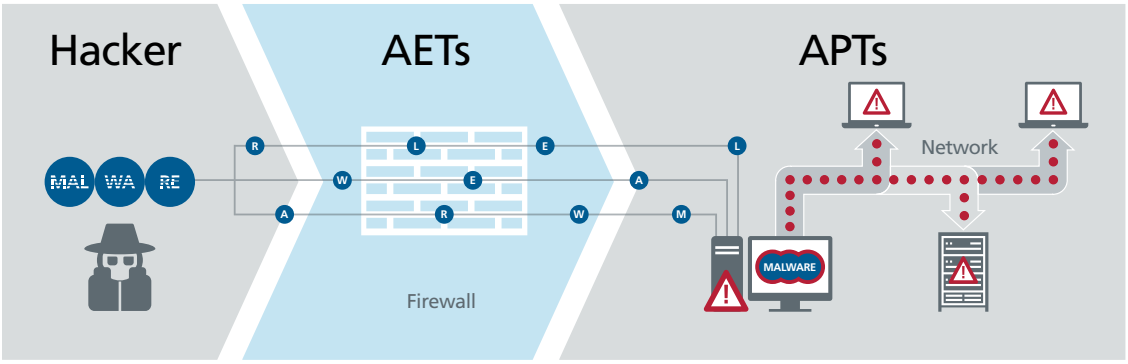
Because of the debate about the very existence of AETs, hackers continue to use these techniques successfully to exfiltrate information. This confusion allows hackers to further invest in increasingly sophisticated attacks, while staying "under the radar" even longer, resulting in damaging and costly data breaches. The longer the industry continues to debate the existence of AETs, the longer businesses will be vulnerable to them.

How Are AETs Different From APTs?

APTs have gained the attention of security staff as real threats since they can go undetected for weeks or months, silently syphoning sensitive data out of the organization. Motivated by profit, hackers use APTs, which include multiple hacking methods, exploits, and malware, to remain in a network and operate as long as needed without being detected.

AETs are used by well-resourced, motivated hackers to execute APT attacks. While the AET is not an attack by itself, as the bits of code in the AET are not necessarily malicious, they are used to disguise an attack. The danger lies in that AETs provide the attacker with undetectable access to the network. By developing a set of dynamic AETs, the hacker creates a "master key" to penetrate any locked-down network to exploit and compromise their vulnerable target victims.

AETs use a combination of evasion techniques, such as fragmentation and obfuscation, to bypass network security controls like firewalls and intrusion prevention systems (IPSs). AETs work by splitting up malicious payloads into smaller pieces, disguising them, and delivering them simultaneously across multiple and rarely used protocols. Once inside, AETs reassemble to unleash malware and continue an APT attack.



Hackers apply **advanced evasion techniques (AETs)** to disguise their attack. This includes splitting up malicious payloads into pieces and sending them across multiple and rarely used protocols.

The AET successfully penetrates the target network undetected. Once inside, AETs reassemble to unleash malware and continue an **advanced persistent threat (APT)** attack.

APTs are precisely targeted attacks on a business or political entity that require a high degree of stealth over a prolonged duration of operation in order to be successful.

Figure 1. The components of an attack.

A well-publicized example of network penetration involving AETs is the Operation Troy cyberespionage campaign in South Korea. This APT campaign, which spanned four years, remained hidden by using a variety of custom tools. Experts believe that a Trojan, cloaked by evasion techniques, entered the network undetected and quickly spread throughout the organization. This successful attack indicates that hackers are well aware of AETs and how to use them.

Confusion in the Market

From our findings, it appears that security personnel may be confusing APTs with AETs and, therefore, may not be deploying complete security solutions to thwart the latter. For example, from the surveyed organizations that indicated they were breached within the past 12 months, 17% claimed to have put an AET solution in place prior to the hack. However, we also uncovered that a majority of our respondents are confused about what an AET actually is, which has led to this false sense of protection. A clear indicator of the confusion is that while 70% of those surveyed believe they know what an AET is (in the UK, this percentage falls to 50%), 37% of those incorrectly define the term "Advanced Evasion Technique (AET)." This means fewer than half of all surveyed respondents can properly define an AET.

Fewer than half of all surveyed respondents could properly define an AET.

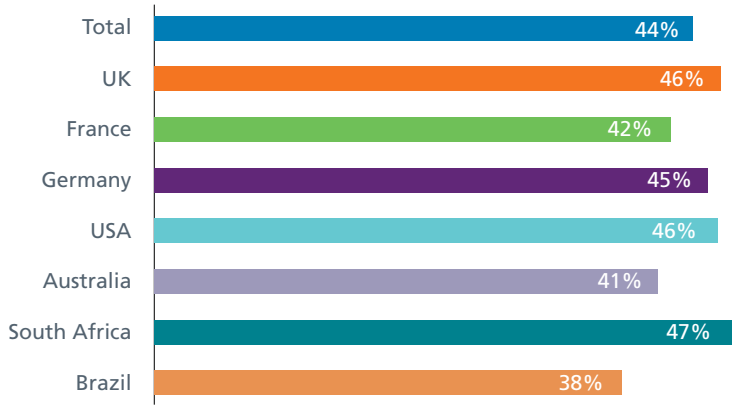


Figure 2. Analysis of a total of 800 respondents who know what an AET is by country.

Millions of combinations and modifications of network-based AETs have been identified to date and are capable of changing dynamically even during an attack. Survey respondents incorrectly estimated that 329,246 AETs have been discovered and studied so far, when in fact the current actual number of tested AETs is **over 800 million**—yet another indicator of the misunderstanding of this threat by security personnel.

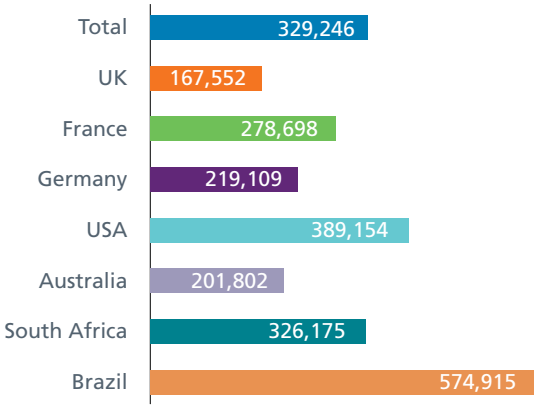


Figure 3. Responses to the question: "*How many different AETs do you believe have been discovered and studied so far?*" This was asked of 800 total respondents. The actual reported number of AETs is currently approximately 800 million.

Our survey indicates that cybersecurity standards may have also furthered the confusion. Well over half of survey respondents (63%) indicated that the plethora of cybersecurity standards has led to confusion over the real risks to business. This percentage is even higher in the UK (70%) and Australia (71%). However, 80% of the security professionals we surveyed would welcome more industry standardization for AETs and how to protect their business, indicating their need for clarity on AETs and their prevention.

"Many organizations are so intent on identifying new malware that they are falling asleep at the wheel toward advanced evasion techniques that can enable malware to circumvent their security defenses. AETs pose a great threat because most security solutions can't detect or stop them. Security professionals and executive managers need to wake up, as this is a real and growing threat."

John Oltsik,
Senior Principal Analyst,
Enterprise Strategy Group

False Sense of Security

AETs are typically referred to as network-based attacks. They are a means of disguise, allowing an intruder to bypass security detection during attack. Most network security systems on the market—IPS, intrusion detection system (IDS), unified threat management (UTM), and even next-generation firewalls—do not have the technology built-in to stop evasions, since they only analyze single-protocol layers and inspect individual segments. Finding a known exploit is easy—but finding AETs requires full-stack traffic analysis and normalization, protocol by protocol. This deep inspection requires a great deal of processing power, which can create a hit to throughput performance of some network security solutions.

There are a few striking pieces of evidence from the survey that indicate that confusion between APTs and AETs has led to a false sense of security in the networks of our respondents. The majority of the survey respondents (61%) signified they have a solution in place to track/detect AETs today. Of these, half (50%) reported that their organization protects against AETs with IPS (this jumps to 60% in Brazil), IDS (57% in Australia), and/or endpoint security—despite anti-evasion technology being absent from these solutions. Half (50%) responded that they knew vendors that offered AET solutions. Of these, over 75% of respondents selected security vendors that do not currently offer an advanced evasion prevention solution.

It seems that many organizations believe they are protected against AETs when, in fact, they are only protected against malware or exploits.

It seems that many organizations believe they are protected against AETs, when in fact they are only protected against malware or exploits.

This false sense of security could be caused by publicized industry benchmarking tests on AET detection that some vendors prepare for in advance. These vendors, in turn, use the favorable, yet skewed, results to create the perception that they can identify evasions. One such vendor claims they can protect against only 60 AETs when more than 800 million known AET variants have been identified to date.

"There are millions of working combinations and permutations of AETs that may alter form during attacks," said Pat Calhoun, senior vice president of network security for McAfee. "This is why traditional signature or pattern-match detection, the methods used by the majority of today's network security solutions, cannot effectively combat AETs."

To provide true visibility into evasions, McAfee offers a free tool, Evader, which your IT security team can use to determine whether there are AETs on your network. However, your IT organization needs to be cautious, as some vendors have created workarounds that give the appearance that their offering identifies and stops AETs.

The Costs of Keeping a Secret

This confusion and false sense of security have come at a very high cost. Almost one quarter (22%) of surveyed IT decision makers admit that their network security has been breached within the last 12 months, with an additional one in 20 (6%) claiming to not know whether their organization has experienced a breach or not. The numbers were even higher in Germany (31%) and the US (29%).

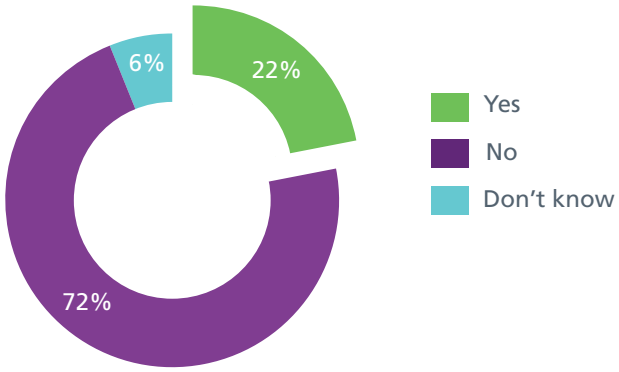


Figure 4. Responses to the question: "*Has your network security been breached within the last 12 months?*" This was asked of 800 total respondents.

"This percentage is most likely even higher than reported, as this is something most security professionals do not like to admit," said Calhoun.

Respondents whose organizations had experienced a network breach in the past 12 months estimate the average cost to the business to be $931,006. Australia, which reported a lower number of breaches at 15%, indicated a much higher average cost per breach at $1.5 million. The cost to US respondents also exceeded $1 million on average. And the hit to the financial services sector was the greatest, with an estimated cost of more than $2 million per breach globally.

In addition to the financial costs of a breach, the damage to a company's brand and reputation may be irrecoverable. Public disclosure laws, such as the European Union's Data Protection Regulation and the The Health Insurance Portability and Accountability Act (HIPPA) in the US, require that organizations report and notify the public when customer data has been compromised, in addition to paying steep fines to their governing agencies. The lost trust and degraded confidence in the company after such a notification may result in customers and business partners looking elsewhere for their goods and services, causing long-term damage to the profitability and growth of any business.

Five Key Requirements of an AET Solution

Traditional firewalls do not protect against AETs and many other threats. Businesses must look for solutions that offer the following features:

1. *Protection against increasingly sophisticated threats*—The sophistication of network threats has exploded in the past 18 months, especially as it relates to preventing botnets, enabling secure access to Web 2.0 applications, and cloud computing environments.
2. *Detailed, real-time inspection*—The rise of Software-as-a-Service (SaaS) and HTTP/HTTPS traffic has overwhelmed first-generation firewalls. In fact, nearly 85% of all network traffic is HTTP/HTTPS. First-generation firewalls either fail to inspect—or at least, thoroughly inspect—web traffic in real time. In many cases, firewalls have to be manually configured to support this traffic, which is crucial to facilitating business operations. The end result is an increase in the number of security breaches caused by human error in the manual firewall configuration process.
3. *High availability*—Network availability continues to be an immense concern for today's enterprises. First-generation firewalls are very limited in what they can do to support network availability. They do not facilitate the active/active clustering of firewalls which allows organizations to add capacity on demand, nor do they support ISP and VPN load balancing. Separate solutions are required for clustering, load balancing, and failover.
4. *Correlation capabilities and network visibility*—The inability of first-generation firewalls to correlate network events greatly inhibits an enterprise's ability to proactively manage and detect network threats. This presents a major roadblock to network visibility. At best, most first-generation firewalls can only provide a snapshot of network activity through a basic management console. The ability to drill down and investigate specific threats is virtually impossible—especially as today's enterprise networks typically include dozens of firewalls from different vendors. For example, a first-generation firewall may alert you to a threat but is unable to pinpoint the specific firewall. Rather than immediately resolving the threat and updating all network firewalls to prevent a similar attack, administrators spend valuable time simply trying to find the point of origin. This inefficiency is a threat in itself.
5. *Simplicity and ease of management*—First-generation firewalls have to be managed individually and configured manually. Today's networks are made up of a complex configuration of network devices, all of which have to be monitored and updated on a routine basis. Without an easy way to see network activity and configure devices, managing first-generation firewalls can be chaotically inefficient. This is compounded by the fact that today's networks are typically made up of devices from various vendors, all of which have their own separate management console. Finally, as virtual network devices gain popularity, device management becomes exponentially more difficult as network visibility decreases. With first-generation firewalls, enterprises have no way to manage *all* virtual and physical security devices from a single point of view.

Conclusion

Understanding how AETs play a critical role in an APT attack is vital to protecting any organization. Understanding the difference between APTs and AETs, and being able to visualize the threat landscape, will help mitigate the risk to the network and the company.

Links to AET Resources

- *Advanced Evasion Techniques For Dummies*
- Free Evader tool: http://evader.mcafee.com
- *Protect Against Advanced Evasion Techniques* white paper

About McAfee Next Generation Firewall

McAfee® Next Generation Firewall uses built-in technology that decodes and normalizes network traffic for inspection on all protocol layers, creating evasion-free traffic, free of exploits. McAfee provides the most effective protection available against the most determined attacks. Always up-to-date, this layer of security is critical to stop emerging network-based attacks that can bypass traditional network security solutions.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60982rpt_aet_0314_fnl_ETMG