Industry Experts Speak Out on Advanced Evasion Techniques

What's Next

Presented by McAfee

intel Security

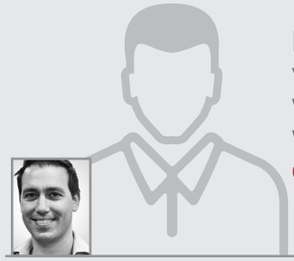
The Experts

Tony Bradley
Founder,
Bradley Strategy Group
@TonyBradleyBSG

Tony Bradley is a respected authority on technology. He writes for a variety of online and print media outlets. Before founding Bradley Strategy Group, he was chief marketing officer for Zecurion—a leading data loss prevention company. Prior to that, Mr. Bradley was director of security at Evangelyze, and was previously an IT administrator and information security consultant working with companies like General Motors, American Airlines, Marathon Oil, and PepsiCo / Frito Lay.

Lane Cooper
Editorial Director
Biz Tech Reports,
@LaneCooperTL

Mr. Cooper is the editorial director of BizTechReports, an independent reporting agency that analyzes user trends in business technology. He has over 20 years of experience as a researcher, reporter and editor analyzing the business and technology industry. On average, Mr. Cooper meets with 600 CIOs and senior enterprise executives every year to understand the impact of evolving technological developments on organizations of all sizes across all industries.



Robert Hansen
Vice President,
WhiteHat Labs at
WhiteHat Security
@fallingr0ck

Robert Hansen is the former chief executive of SecTheory and Falling Rock Networks which focused on building a hardened OS. He has worked for Cable & Wireless doing managed security services, and eBay as a sr. global product manager of Trust and Safety. Mr. Hansen has co-authored “XSS Exploits” by Syngress publishing and wrote the eBook, “Detecting Malice.”

Ed Kovacs
Security News Editor
Softpedia, Information
@EduardKovacs

Eduard Kovacs is Softpedia’s information security news editor. He has written thousands of articles for Softpedia and other publications, covering every possible topic related to cyber security, including enterprise security, Internet scams, data breaches, security research and cybercrime.

Mr. Kovacs’ goal is to teach people about online threats and to make organizations realize “we take security very seriously” should be more than something they write in the statements they publish after they get hacked.

The Experts

Lawrence Pingree
Research Director,
Gartner
@lpingree

Lawrence Pingree, research director at Gartner, has been an active member of the information security industry for many years. He has consulted for large financial institutions, corporations, and government entities on firewalls, intrusion detection, networks, system penetration, risk management, compliance, e-discovery and forensics. He has served as a chief security architect at both PeopleSoft and NetScreen.

Alan Shimmel
Editor-in-Chief,
DevOps.com
@ashimmy

As editor-in-chief of DevOps.com, Alan Shimel is attuned to the world of technology. Alan has founded and helped several technology ventures, including StillSecure, where he guided the company in bringing innovative and effective networking and security solutions to the marketplace. Shimel is an often-cited personality in the security and technology community and is a sought-after speaker at industry and government conferences and events.

Larry Walsh
CEO and Chief Analyst,
The 2112 Group
@lmwalsh2112
@channelnomics

Lawrence M. Walsh is CEO and chief analyst of The 2112 Group, a business strategy firm that specializes in improving the performance of technology companies' direct and indirect channels through a portfolio of market-leading products and services, including qualitative research, market analysis, tools, and enablement programs.

Mirko Zorz
Editor-in-Chief,
Help Net Security and
(IN)SECURE Magazine -
@helpnetsecurity

Mirko Zorz is editor-in-chief of *Help Net Security* and *(IN)SECURE Magazine,* responsible for all editorial decisions on both publications. He has a technical background and has worked as a senior security consultant for a Danish security company. He has focused on online media since early 2000. For the last 14 years, Mr. Zorz has traveled the globe to a myriad of information security events and continued to fuel his passion for information security.

Advanced evasion techniques, defined

Advanced evasion techniques, or AETs, are delivery mechanisms used to disguise advanced persistent threats (APTs) and permit them to slip through network security undetected.

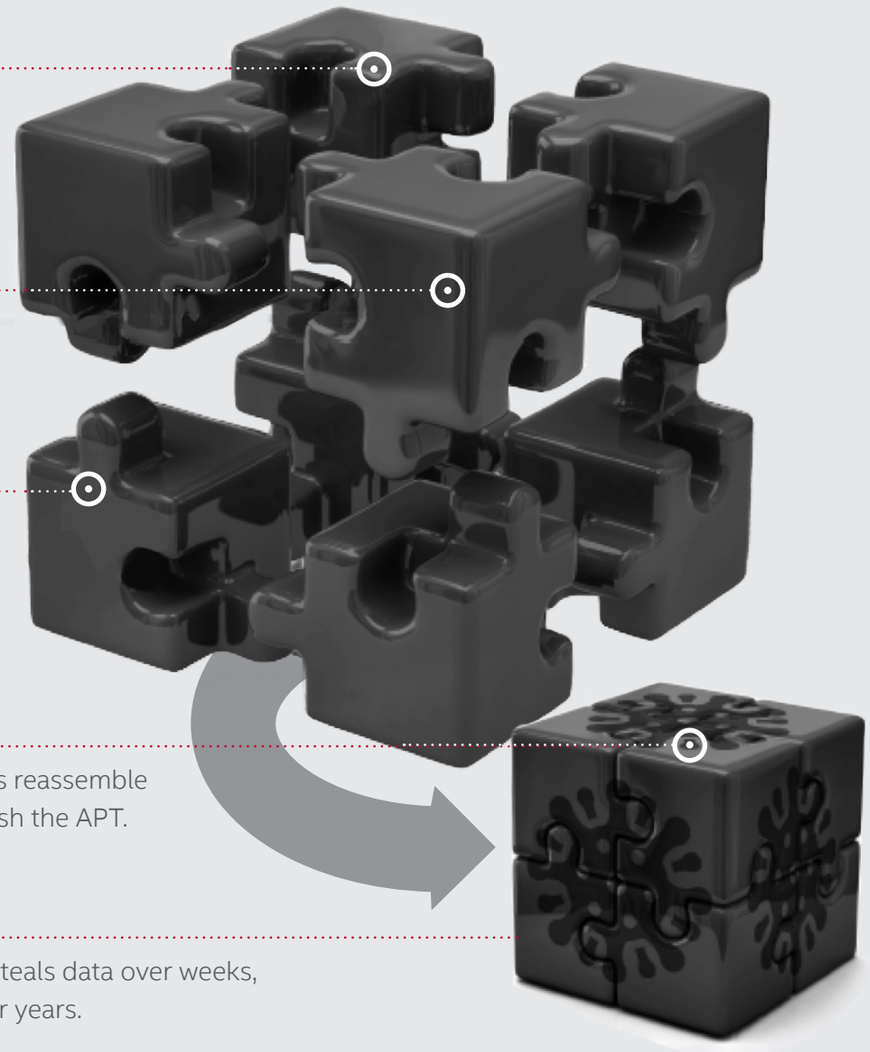
AETs work by splitting up malicious payloads into smaller pieces, disguising them, and delivering them simultaneously across multiple and rarely used protocols. Once inside, AETs reassemble to unleash malware and continue an APT attack.

Put the pieces together: **AETs disguise APTs by:**

Splitting up malicious code into multiple benign payloads.

Sending disguised payloads across rarely used or lax protocols.

Slipping pieces of malicious code through firewalls.



The pieces reassemble and unleash the APT.

The APT steals data over weeks, months, or years.

AETs can be extremely difficult to detect for **two reasons:**

ONE They are shape shifters

AETs creat millions of “new” evasion techniques from only a few combinations.

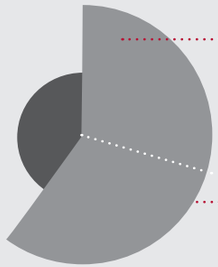
Security pros believe there are **330K** AETs in existence.

The actual number of AETs is **800M+**

<1% of AETS are detected by most firewalls.

TWO They are misunderstood

AETs get confused with APTs, creating a false sense of security.



61%
believe they have a network security solution to defend against AETs.

Of these **50%**
use a combination of network security solutions that can’t detect AETs.

1 The Phantom Menace

AETs present a growing problem, but opinions vary regarding the level of threat posed:

Expert insights

Lane Cooper

"This new threat is a rapidly growing problem that challenges the core thinking behind current intrusion prevention strategies."

Ed Kovacs

"AETs are definitely a growing problem. However, since AETs are used mostly by a few cybercriminal groups to target high-profile organizations, we can't see the effects as we do with other, more common tactics."

Lane Cooper

"These techniques have evolved, but for the most part they are all based on the simple issue that the vast majority of security software still uses a combination of lists, and those lists are often trivial to evade if the attacker knows that they're doing."

Tony Bradley

"It's hard to say if AETs are a growing problem because they've been lurking in the background, but we're only just beginning to pay attention. It does seem like it's a growing problem, and it makes sense that it would be a growing problem. Finding a vulnerability and developing an exploit is only one small part of the attack equation. The bad guys focus on AETs because they need to get the malware past the network defenses."

The experts believe awareness of the threat posed by AETs is dangerously low.

Larry Walsh

"The AET forecast is probably one in which threats and incidents will escalate in the coming 12 to 24 months. Many enterprises, and probably security vendors, are unaware of AET threats."

70%

of CIOs and security managers believe they know what an AET is

but fewer than

50%

can correctly define advanced evasion techniques.

"My belief is that many security practitioners are largely unaware of the risks that advanced evasion techniques represent to their security."

Lawrence Pingree

2 At Risk

AET-cloaked attacks pose a threat to companies of all sizes, though the experts agreed larger and higher-profile companies face the greater risk. AETs require a degree of organization and discipline that may be overkill against smaller or less well-prepared systems.

That said, the experts also agree large organizations—and the deeper resources at their disposal—are likely in a better position to mitigate the threat posed by AETs.

22%

of CIOs and security managers say their networks were breached in the last 12 months.

63%

have trouble convincing top management that AETs exist and are costly.

YET

40%

of those breached think AETs played a key role.

39%

lack methods to detect and track AETs.

Expert insights

"Neither enterprises nor SMBs are particularly capable of addressing any sort of AET beyond anecdotal, one-off situations. Large companies lack the ability to get 100% coverage across their networks, and smaller organizations lack the funds necessary for the investment."

Robert Hansen

Lawrence Pingree

"Most small companies are unaware of evasion [because] they have little to no security expertise or practitioners, many of them rely on an external managed security service provider for their security. So if the MSSP doesn't notify them and fix the issue, they continue to have a false sense of security.

Larger organizations certainly do have security practitioners … but many of their guiding principles mean that they only do exactly what it is they must do to comply. I think AETs are often off their risk management radar."

Ed Kovacs

"AETs are not easy to implement (they require a lot of time and resources), so it's less likely that an attacker would bother using AETs [against a smaller company] when social engineering tactics would probably do the job better."

Mirko Zorz

"Cybercriminals are either after money or information that they can turn into money. Big companies have more of both, which means they are definitely at risk."

3 Escalation

AETs are generally regarded as uplevel attacks. The experts agree that the weakest point in network security is the human element.

Expert insights

Alan Shimel

"The overwhelming majority of breaches are low-hanging breaches because people are people. They make mistakes, and they may not even know they're making them."

Larry Walsh

"Too often, enterprises make security choices based on cost-benefit analyses. Many of the high-profile security breaches such as Target and TJX had nothing to do with advanced evasion, but rather the failure of the organization to make reasonable security investments and administer sound practices."

"Cybercriminals have two options. First, they can try to exploit the weakest link in the chain, namely humans. Social engineering is still a successful tactic. On the other hand, they can try to come up with ways to evade these new types of security systems. This is where AETs come in."

Ed Kovacs

76%

of data breaches involve exploiting weak or stolen credentials.

29%

used social engineering (including phishing).

4 The Cyber Cold War

As a group, the experts expressed diffidence at the notion either AETs or methods to combat them could achieve sustained dominance over the cybersecurity landscape. “Cat-and-mouse,” “Cold War,” and similar terms were frequently used to describe the situation.

“It’s like a Cold War mentality. The mission is never accomplished. It’s a zero sum game. You can’t win. So instead of playing the game, let’s change the rules.”

Alan Shimel

Expert insights

Ed Kovacs

“It will be a cat-and-mouse game, just like … many other attack techniques. More and more attackers will come to realize that AETs could be the answer to breaching high-profile targets that might be better protected against common threats.”

Lane Cooper

“AETs are the next step in the dynamic and accelerating arms race between malware producers and the enterprise security community.”

Larry Walsh

“The net result of this arms race is an ever-shifting balance in which the white and black hats are constantly teetering on the advantage.”

Lawrence Pingree

“Security is a cat-and-mouse game, and attackers will always from time to time get ahead of our defenses so providers must always seek to augment their technologies and strategies to compensate and mitigate the latest techniques.”

Tony Bradley

The bad guys working on the AETs will probably hold a slight advantage. It’s a reflection of the basic premise of security: the good guys have to try and proactively defend against every possible known and unknown attack vector, but the bad guys only have to find one unique method that works.”

Robert Hansen

“They will most likely evolve at the same rate as each next-generation firewall rule or technique is created, the adversaries will react and defeat them as necessary.”

5 Change the Rules

Faced with the prospect of constant escalation, the experts suggest the solution moving forward involves both a focus on security fundamentals that are all too often overlooked or compromised out of expedience and a willingness to break the cycle and explore new approaches to cybersecurity. In the words of Frank Underwood from House of Cards, "If you don't like how the table is set, turn over the table."

"The real danger is the lack of consistent, rational focus and execution on security planning. If enterprises addressed the 80% of well-known threats with conventional security technologies, advanced evasion threats would be far more addressable."

Larry Walsh

Expert insights

Lawrence Pingree

"Security practitioners must put network evasion as well as other advanced evasion techniques on their radar. Their risk management process should include penetration testing that seeks to find and fix evasion techniques."

Tony Bradley

"An older technique [like AETs] may have greater success in some cases. So much attention is being devoted to cutting-edge attack techniques, that security vendors and IT organizations may no longer feel the older techniques are a viable threat, and let their guard down."

Alan Shimel

"For so long, security infrastructure has been built around the moat and castle, barbarians at the gate mentality. Perimeter defense. But the world is changing the rules. Megatrends like big data, cloud and mobility are forcing us to adjust our thinking. We need to figure out how to adapt."

Lane Cooper

"The emergence of AET provides further evidence that 100 percent intrusion prevention is impossible. Defense in-depth strategies must be taken to their next level."

Mirko Zorz

"Even though most emerging threats are complex and protecting large networks is a demanding job, I believe a crucial aspect of ensuring a more secure future lies in an alternative approach."

6 What's Next?

You've just heard from industry experts that the game must change if organizations are going to be capable of meeting the security threats of tomorrow.

WHAT DO YOU THINK?

Join the discussion
#NGFW
#WhatsNext