Evasions: A Growing Threat for Government Networks

DISCOVER WHY YOUR AGENCY MAY NOT BE AS PROTECTED AS YOU THINK

FORCEPOINT

Table of contents

Introduction: Why your agency may not be as protected as you think

The latest testing shows Federal agencies may unknowingly be exposed to exploits and malware, even if you use a name-brand next generation firewall (NGFW) or intrusion prevention system (IPS).

The prevalence of attack-masking evasions is making a growing number of organizations rethink their current defenses and how they secure their networks.

In a recent PulseReport by Gatepoint Research*, nearly half of respondents gave their network security a 99% efficacy rating. If that sounds too good to be true, that's because it is, according to NSS Labs. In this year's NGFW report, NSS Labs revealed many firewalls can be rendered defenseless in mere seconds.

The unfortunate reality is, many Network Security vendors have significant vulnerabilities to evasions.

In the latest NSS Labs NGFW testing,

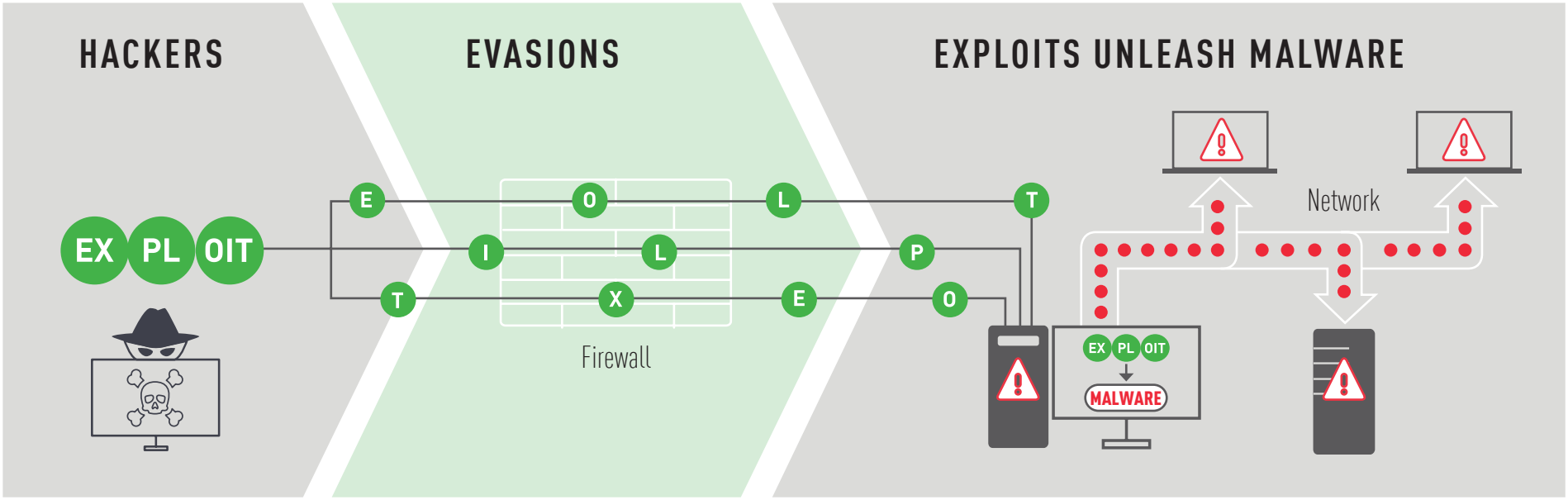
Many vendors found their security efficacy significantly compromised by evasions

Failure of a security device to correctly identify a specific type of evasion potentially allows an attacker to use an entire class of exploits for which the device is assumed to have protection. This renders the device virtually useless.

—NSS Labs, Next Generation Intrusion Prevention System (NGIPS) Test Report, p. 8

What is an evasion?

Evasions have changed the security landscape permanently. They take advantage of design flaws in many firewalls; there isn't a "quick fix" that can be applied by adding a new signature. If your network security isn't capable of handling evasions, your organization is vulnerable.



Hackers apply evasions to disguise exploits containing malware. One of the most common ways is to split malicious payloads into pieces, which are sent out of order, over different paths and rarely used protocols.

Traditional network defenses can't see the obscured payloads, allowing exploits and malware into the network and onto target machines. There, the payloads reassemble and unleash their malicious code.

Once malicious code gets onto target machines, it can silently launch attacks on databases, applications or other IT systems. Such attacks usually succeed when security defenses are focused on external threats and not paying attention to threats from inside.

Evasions leave you vulnerable and at risk

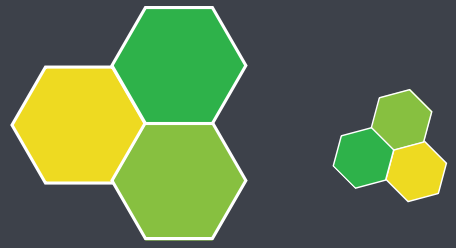
Hackers use evasions across different layers of the network stack. Evasions are often used together, and possible combinations can number in the millions.

Exploit kits such as MetaSploit make it easy to add evasions to attacks. Doing so is a slam dunk for attackers, given how quickly they can evolve their malicious code (e.g.,"Petya" added new spreading techniques beyond those seen in the infamous "WannaCry" just weeks prior).

The scale of the problem can be compared to the early days of the antivirus industry, when everyone knew that a massive problem existed but only few were able to understand how big the problem would grow to be. Today, the antivirus industry has all but stopped counting the number of viruses and virus variations in existence; the number is simply too large. We face a similar scenario with regard to evasions.

Federal agency heads are now accountable for the effective management of the cyber risk within their respective agencies, under President Trump's 2017 executive order for cybersecurity. While agency heads have always been accountable, this explicit assignment of responsibility elevates the issue that agencies must focus more attention on addressing vulnerabilities. Action must be taken to prevent security events and breaches from malware from occurring in the future.

The need for automated means of defeating evasions is critical.



Evasions Exist at All Layers

Layer	Example Evasion
APP HTML, SQL, etc.	▸ Code Obfuscation ▸ String Encoding
TCP	▸ Overlapping ▸ Extraneous
IP	▸ Out of Order ▸ Fragmentation

Most network security devices don't make the cut

- **Many network security devices use packet-based inspection.**
  This simplistic approach attempts to identify each and every evasion combination, determine whether or not it's dangerous, and then creates its own customized defense. Yet, each combination of evasions provides a new way to bypass traditional networking checks. Network security devices need to be designed upfront to defeat evasions so that their inspection engines can do their jobs.

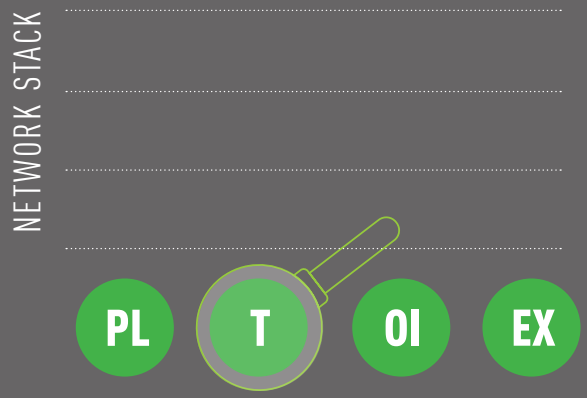
- **Patches for known exploits are ineffective against advanced evasions.**
  Most organizations experience a delay before they are able to deploy patches for known vulnerabilities. Intrusion prevention, whether part of a next generation firewall or a standalone IPS, is intended to detect signs that an attacker is trying to exploit vulnerabilities that haven't been patched. However, evasions can hide these exploits from detection by traditional intrusion detection devices, allowing them to target endpoints, servers, databases, and other systems.

- **Many devices take shortcuts that sacrifice security for speed.**
  Network security devices should defend against evasions at each layer in the networking stack, but many products take shortcuts, favoring speed over security. While this sometimes allows devices to operate faster, it leaves the network wide open to attack.

- **Lab testing may only be limited to previously identified exploits.**
  Many security vendors tout performance against simulated and recorded evasions produced in predefined lab environments. When facing evasions, these systems typically go blind and allow exploits and malware into your systems and data.

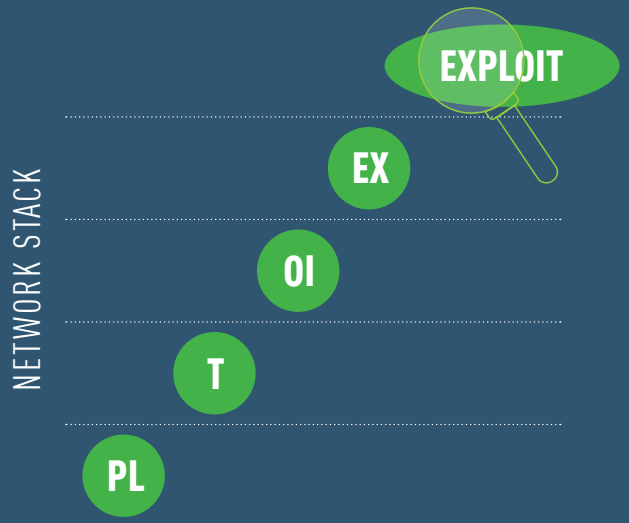
To know whether your current defenses protect against evasions, it's best practice to test the anti-evasion capabilities of your network security devices within your own environment, policies, and configurations.

Traditional Approach for Detecting Exploits & Malware



Packet inspection misses fragmentation

The Forcepoint NGFW & IPS Difference



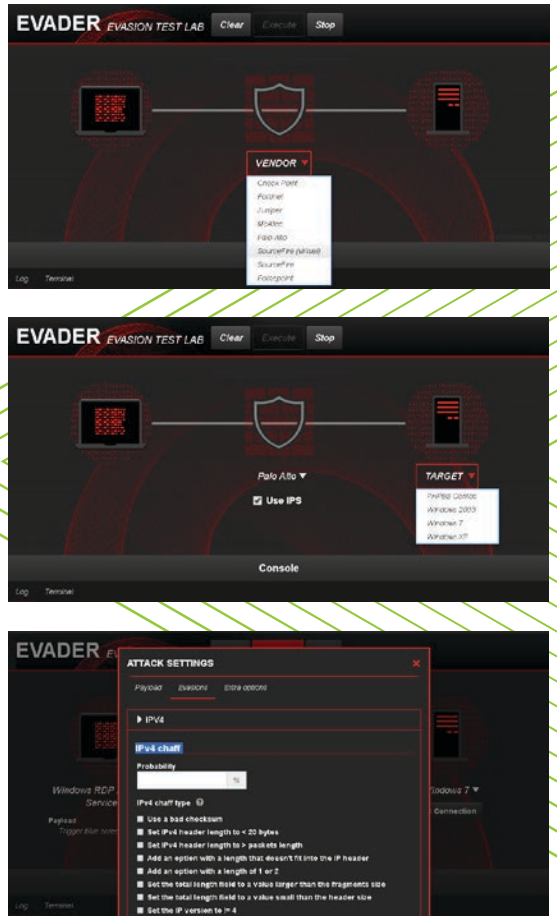
Stream reassembly defeats many evasions

Test your defenses against evasions with Evader

To take the first step toward true network security, it's vital to know where your firewalls and IPS defenses stand against evasions. Use Evader, "Forcepoint's premier software-based test environment," to interactively test your firewalls and IPS devices to see whether they detect, block, and report evasion-disguised exploits coming through public or internal networks.

- **Launch controlled evasion-borne attacks at network security devices**
- **Interactively combine and adjust evasions**
- **See evasion results immediately**

See Evader in Action & Schedule a Live Interactive Demo of Evader



Note: Evader is not a hacking tool or a penetration test intended to transmit arbitrary exploits. It is offered solely for testing and should not be used against any systems outside your environment. Evader tests whether or not a known exploit can be delivered through security devices you specify to a target host.

Forcepoint: The industry's #1 rated security for NGFW and IPS

Network security must evolve as applications move to the cloud and threats rapidly evolve. For many years, **Forcepoint Sidewinder proxy firewalls** have secured some of the most sensitive mission-critical environments. Now, the best of Sidewinder's application proxy technology is now incorporated into the **Forcepoint NGFW, providing even greater protection.**

Agencies can leverage next-generation capabilities without sacrificing evasion protection or the application-level security relied upon to protect mission critical data.

Forcepoint NGFW offers a more effective and efficient approach, performing deep, full-stream inspection that:

- Works uniformly across Physical, Virtual, and Cloud deployment
- Can be used as a standalone IPS or a full-function NGFW
- Is unsurpassed in detecting malicious traffic
- Is the pioneer in defeating evasion techniques
- Provides interactive visibility across the entire enterprise network
- Makes it easy to block offending sessions permanently

Forcepoint NGFW has been ranked at the top in both of NSS Labs' key tests of network security, including NGFW and NGIPS. Forcepoint also offers the industry's leading technology for detecting advanced malware.

Connect and protect your network with Forcepoint NGFW, the firewall with the industry's strongest security, smartest manageability, and highest availability.

The security effectiveness of the Forcepoint NGFW 3301 was unsurpassed in the NSS Labs 2017 NGFW test. The Forcepoint NGFW should be on every company's short list.

— Thomas Skybakmoen, Distinguished Research Director, NSS Labs

Learn more

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact

[EBOOK_FORCEPOINT_EVASIONS_EN] 800006.120517