

Understand The Anatomy of Attacks to Stay One Step Ahead



Network (firewall) and endpoint (antivirus) defenses react to malicious communications and code after attacks have launched. OpenDNS observes Internet infrastructure before attacks are launched and can prevent malicious Internet connections. Learning all the steps of an attack is key to understanding how OpenDNS can bolster your existing defenses.

Each step of the attacker's operation provides an opportunity for security providers to observe its presence and defend its intrusion. On the next page, four detailed example attacks are laid out using a seven-step framework. Here is a high-level summary of the details:

- 1. RECON:** Many reconnaissance activities are used to learn about the attack target.
- 2. STAGE:** Multiple kits or custom code is used to build payloads. And multiple networks and systems are staged to host initial payloads, malware drop hosts, and botnet controllers.
- 3. LAUNCH:** Various Web and email techniques are used to launch the attack.
- 4. EXPLOIT:** Both zero-day and known vulnerabilities are exploited or users are tricked.
- 5. INSTALL:** Usually the initial payload connects to another host to install specific malware.
- 6. CALLBACK:** Nearly every time the compromised system callbacks to a botnet server.
- 7. PERSIST:** Finally, a variety of techniques are used to repeat steps 4 through 7.

It is not necessary to understand each tool and technique that attackers develop. The takeaway is to understand how multiple, and often repeated, steps are necessary for attackers to achieve their objectives.

Words of Wisdom

Compromises happen in seconds. Breaches start minutes later and continue undetected for months. Operating in a state of continuous compromise may be the new normal, but we cannot accept a state of persistent breach.








"Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms. All organizations should now assume that they are in a state of continuous compromise."

— Neil MacDonald | Peter Firstbrook
[Designing an Adaptive Security Architecture for Protection From Advanced Attacks](#)

Gartner

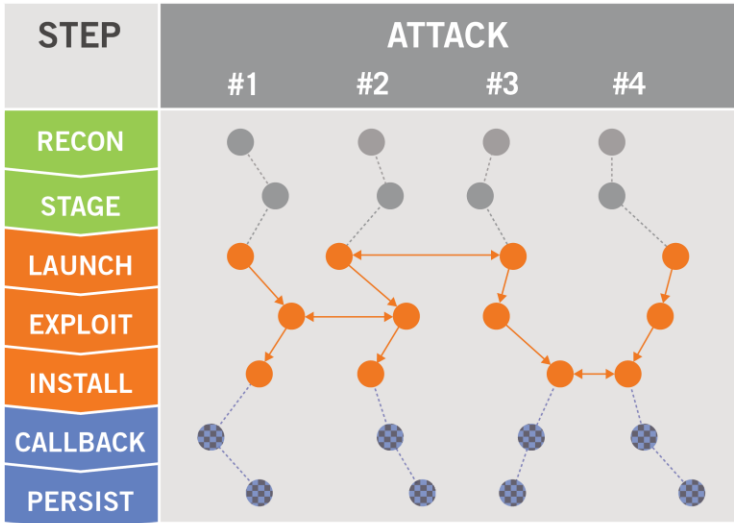
Example Attacks (Framework is based on Lockheed Martin's "Kill Chain")

STEP		ATTACK #1	ATTACK #2	ATTACK #3	ATTACK #4
TARGET	RECON Attacker discovers trusted email & website addresses; also probes networks and systems for weaknesses	Social Networks & Engineering harvest friends' emails and profile social activities	Bash Shellshock [CVE-2014-6271] webshell gathers email addresses and password files	Exposure Maps Nmap, Nessus, ping IPs, port scan, app fingerprinting, Google dorking	Surveillance capture CEO's DNS requests by pharming on hotel's guest wi-fi
	STAGE 0 Attacker builds payload or acquires tools for exploit, install and callback steps	Zeus Build Kit w/O-day exploit & domain generation algorithm (DGA)	Custom Coded w/known exploit & domain generation algorithm (DGA)	SpyEye Build Kit w/O-day exploit & double fast flux P2P callbacks	Nuclear Build Kit w/O-day exploit & 256 bit encrypted P2P callacks
	Attacker builds or shares infrastructure for launch, install and callback steps	4.2.55.0/24 w/No-IP.com to host DNS records	23.88.2.0/28 w/DynDns.org to host DNS records	32.13.31.0/26 infected devices are nameservers	42.18.31.0/24 own nameservers host DNS records
COMPROMISE	LAUNCH  Attacker sends or spoofs emails, or injects malicious ads or scripts into websites	Spear Phishing pal@gmail.com Subject: Hilarious check out this pic! facebookpic.com	Spear Phishing ceo@acme.de Subject: Important new stock options email attachment	Malvertising ads.yahoo.com ad's javascript redirects to asdfaa.com	Watering Hole https://news.com [malicious iframe code planted] java-se.com
	EXPLOIT  Vulnerable software executes code or user is tricked to excute code	Flash "Shellcode" Vulnerability CVE-2014-1776 animated.swf	Old PowerPoint Vulnerability CVE-2014-6352 stock.ppt	Social Engineering [Fake AV Popup] avast.exe	Heartbleed Vulnerability CVE-2014-0160 ...
	INSTALL  Code infects system, modifies privileges, scans environment then connects to malware drop host	Windows Trojan C:\...\IEUpd.exe [polymorphic] add to Windows startup folder	Keylogger C:\...\random.exe [salesforce login] user: cfo@acme.de pw: 123456789	Mac Trojan C:\...\hi.jpg.exe [polymorphic] installs as a service	Rootkit C:\...\fsm32.exe [polymorphic] installs as a WIndows service
BREACH	CALLBACK  Attacker gains command and control channel to receive new instructions, or if target data is acquired, steal it	HTTP Connection over Port 443 sdsdffil.ru y5asf3s.cn erasdf2ds.us	IRC Connection over Port 1440 gm234mal.de yyys22sjks.biz ijsdfaa.us	P2P Connection over Port 5455 12323.btt.com 32231.btt.com 24222.btt.com	P2P Connection over Port 6441 stock.wwwls.com
	PERSIST  Attacker maintains persistence until actions on their objectives are fully achieved. Repeat steps EXPLOIT → PERSIST	Hidden Backdoor valid VPN or PKI credential allow the attacker to disguise as a legitimate user	Lateral Movement Bash Shellshock [CVE-2014-6271] to takeover an internal server	Internal Recon gather org charts, network maps, business calendars on wiki or portal	More Footholds install more RATs (remote access trojan) onto other systems

Your Challenge: Existing defenses cannot block all attacks.

Firewalls and antivirus stop many attacks during several steps of the “kill chain”, but the velocity and volume of new attack tools and techniques enable some to go undetected for minutes or even months.

Firewall/Antivirus View of Attacks



Without visibility of where attacks are staged, breach activity appears unique and isolated from compromise activity.

- Firewalls know whether the IP of a network connection matches a blacklist or reputation feed. Yet providers must wait until an attack is launched before collecting and analyzing a copy of the traffic. Then, the provider will gain intelligence of the infrastructure used.
- Antivirus solutions know whether the hash of the payload matches a signature database or heuristic. Yet providers must wait until a system is exploited before collecting and analyzing a sample of the code. Then, the provider will gain intelligence about the payload used.



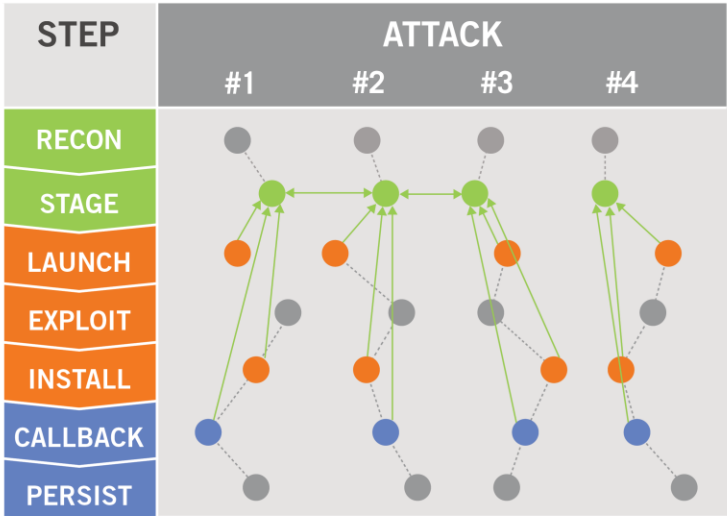
“The reality is that no one security technology is enough. Hackers are always working to defeat the latest defense. So you have to invest in defenses for the latest threat as well as every threat experienced in the past.”

— Lawrence Pingree (Gartner analyst), New York Times, “Tech Security Upstarts Enter Fray”

Our Solution: Stop 50 to 98 percent more attacks than firewalls and antivirus alone by pointing your DNS traffic to OpenDNS.

OpenDNS does not wait until after attacks launch, malware install, or infected systems callback to learn how to defend against attack. By analyzing a cross-section of the world’s Internet activity, we continuously observe new relationships forming between domain names, IP addresses, and autonomous system numbers (ASNs). This visibility enables us to discover, and often predict, where attacks are staged and will emerge before they even launch.

OpenDNS View of Attacks



Observe Internet infrastructure as attacks are staged to stay ahead of the subsequent launch, install and callback steps.

- We see that the IP prefixes (4.2.55.0/24, 23.88.2.0/28, 32.13.31.0/26) of all three attacks are related to the same **Internet infrastructure (AS32442)**.
- Web redirects or email links use domains (facebookpic.com, asdfaa.com) that all have DNS records mapping back to these **IP prefixes**.
- Many callback connections use domains (123.btt.com, 321.btt.com, 222.btt.com) that have DNS records mapping back to these **IP prefixes**.
- But other callback connections use domains (sdfil.ru, y53s.cn, er2ds.us, gmmal.ru, ...) that are generated by a common **algorithm**. This is discovered by observing co-occurrences over short time intervals, matching authoritative nameservers or **WHOIS** information.used.

Your Challenge:

Why keep firewalls and antivirus at all?

Once we prove our effectiveness, we are often asked: “can we get rid of our firewall or antivirus solutions?” While these existing defenses cannot stop every attack, they are still useful—if not critical—in defending against multi-step attacks. A big reason is threats never expire—every piece of malware ever created is still circulating online or offline. Signature-based solutions are still effective at preventing most known threats from infecting your systems no matter which vector it arrives: email, website or thumbdrive. And firewalls are effective at defending both within and at the perimeter of your network. They can detect recon activities such as IP or port scans, deny lateral movements by segmenting the network, and enforce access control lists.



“One of AV’s biggest downfalls is the fact that it is reactive in nature; accuracy is heavily dependent on whether the vendor has already seen the threat in the past. Heuristics or behavioral analysis can sometimes identify new malware, but this is still not adequate because even the very best engines are still not able to catch all zero-day malware.”

— Chris Sherman, [Prepare For The Post-AV Era](#)

FORRESTER

About OpenDNS

OpenDNS provides a cloud-delivered network security service that blocks advanced attacks, as well as malware, botnets and phishing threats regardless of port, protocol or application. Our predictive intelligence uses machine learning to automate protection against emergent threats before your organization is attacked. OpenDNS protects all your devices globally without hardware to install or software to maintain.

Your Solution:

Rebalance investment of existing versus new defenses.

Here are a couple examples of how many customers free up budget for new defenses.

- Site-based Microsoft licenses entitle customers to signature-based protection at no extra cost. Microsoft may not be the #1 ranked product, but it offers good protection against known threats. OpenDNS defends against both known and emergent threats.
- NSS Labs reports that SSL decryption degrades network performance by 80%, on average. OpenDNS blocks malicious HTTPS-based connections by defending against attacks over any port or protocol. By avoiding decryption, appliance lifespans can be greatly extended.

Contact Us

Have a question?

BIS

Phone Number: 251-410-7601

Email: sales@askbis.com

www.company.com



BUSINESS INFORMATION SOLUTIONS

We Get *IT* Done!