Why firewalls and antivirus alone are not enough.

Network (firewall) and endpoint (antivirus) defenses react to malicious communications and code after attacks have launched. Cisco Umbrella 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 Umbrella 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.

Gartner

"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

Example attacks (Framework is based on Lockheed Martin's Cyber Kill Chain®)

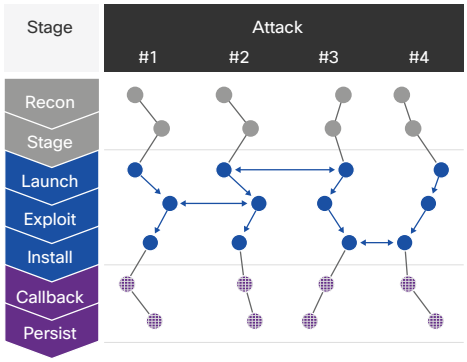
	Step	Attack #1 Steal credit card data from point-of-sale systems	Attack #2 Manipulate customer data to impact stock value	Attack #3 Deface website due to geopolitical remarks in the press	Attack #4 Steal product designs to resell on blackmarket
Target	**Recon** Attacker discovers trusted email & website 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 Attacker builds payload or acquires tools for exploit, install and callback steps	Zeus Build Kit w/0-day exploit & domain generation algorithm (DGA)	Custom Coded w/known exploit & domain generation algorithm (DGA)	SpyEye Build Kit w/0-day exploit & double fast flux P2P callbacks	Nuclear Build Kit w/0-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 execute code	Flash "Shellcode" Vulnerability CVE-2014-1776 animated.swf	Old PowerPoint Vulnerability CVE-2014-6352 stock.pp	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.wwxls.com
	Persist Attacker maintains persistence until actions on their objectives are fully achieved repeat steps 4-7	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 porta	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.

- 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.

Firewall/Antivirus view of attacks



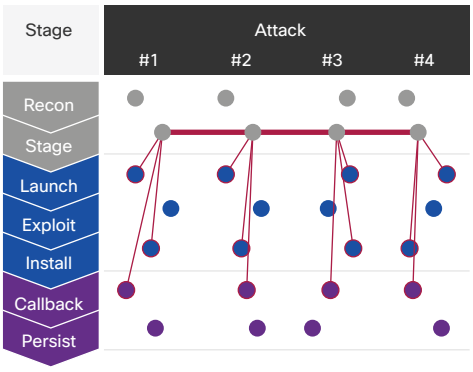
Without visibility of where attacks are staged, each step is unique and isolated.

Our solution: Stop 50 to 98 percent more attacks than firewalls and antivirus alone by pointing your internet traffic to Umbrella.

Umbrella does not wait until after attacks launch, malware installs, or infected systems callback to learn how to defend against attacks. 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.

- We see that the IP prefixes (4.2.55.0/24, 23.88.2.0/28, 32.13.31.0/26, 42.18.31.0/24) of all four attacks are related to the same internet infrastructure (AS32442).
- Web redirects or email links use domains (facebookpic.com, asdfaa.com, java-se.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, stck.wwxls.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.

Umbrella's view of attacks



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

"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

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.

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. Umbrella defends against both known and emergent threats.
- NSS Labs reports that SSL decryption degrades network performance by 80%, on average. Umbrella blocks malicious HTTPS-based connections by defending against attacks over any port or protocol. By avoiding decryption, appliance lifespans can be greatly extended.

About Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first layer of defense against threats on the internet wherever users go. By learning from internet activity patterns, Umbrella automatically uncovers current and emerging threats. And because it's built into the foundation of the internet, Umbrella blocks threats before they ever reach your network or endpoints.

FORRESTER®

"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