Top 7 Network Attack Types in 2015

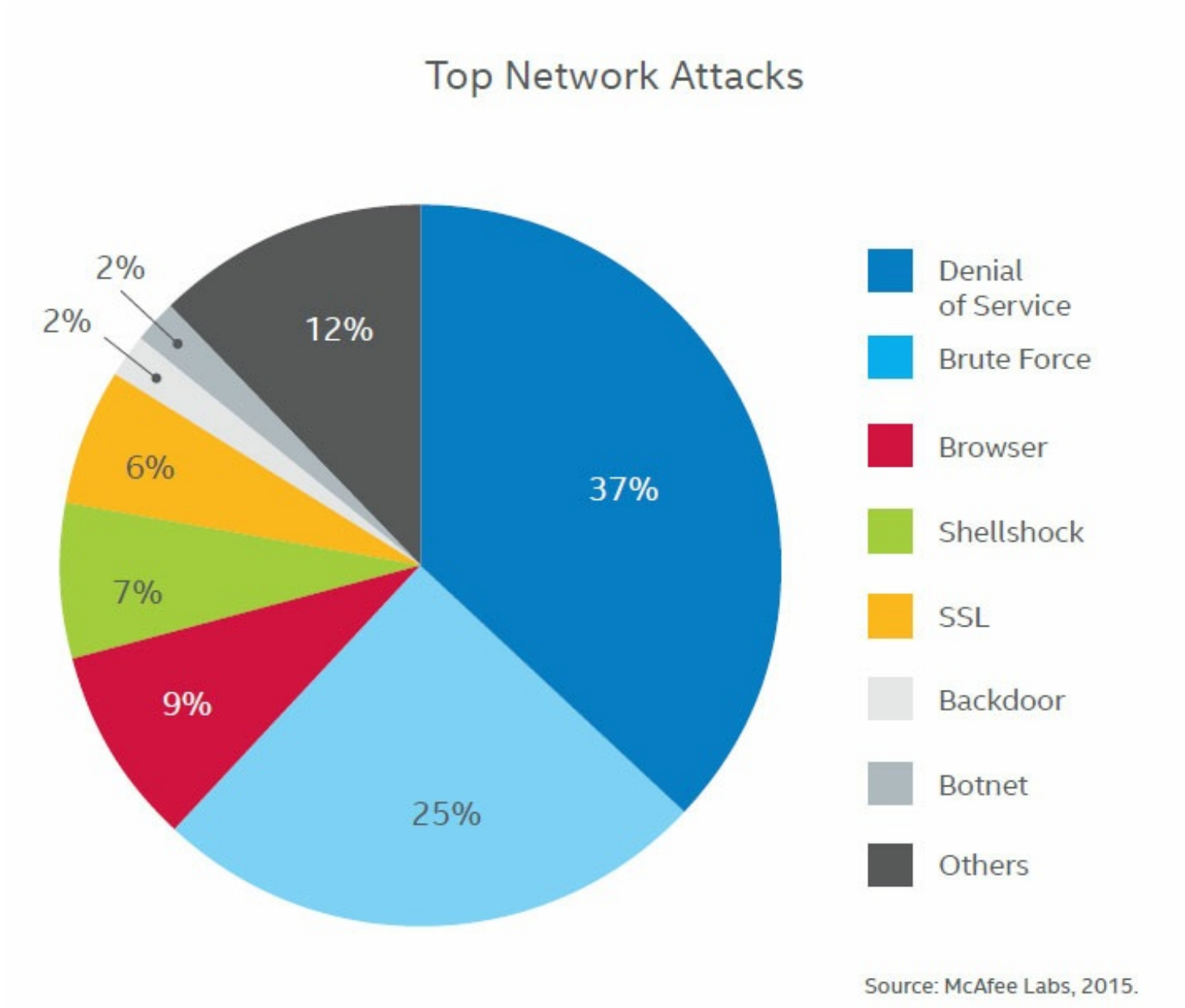
www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/

When you log in to an AccessEnforcer, or any UTM device, you will see a number of network attacks detected and blocked. The number may be in the thousands, or even hundreds of thousands.

Many of these attacks are scans – precursors to attack. Depending on your settings, a good number might also be firewall policy violations.

But what are other types of network attacks? What are the most common ones today?

One answer comes from the latest Threat Report from McAfee Labs. The chart below aggregates data from the company's network of millions of sensors across the globe. It shows the most common network attacks detected in Q1 2015.



We describe each of these common types of network attacks below.

Top 7 types of network attacks

Denial of service attacks – 37%

A denial of service (DOS) attack attempts to make a resource, such as a web server, unavailable to users. These attacks are very common, accounting for more than one-third of all network attacks reviewed in the report.

A common approach is to overload the resource with illegitimate requests for service. The resource cannot process the flood of requests and either slows or crashes.

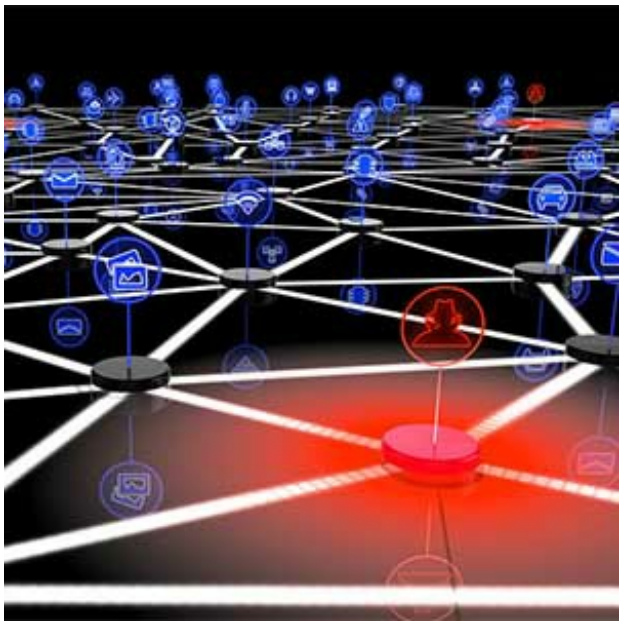
Distributed denial of service (DDoS) attacks are popular today. This approach distributes the task to a number of computers. Through automation, the computers are coordinated to flood a target, often without the knowledge of the computers' owners.

There are several types of DDoS attacks, which we have covered in earlier posts. These network attacks are growing more powerful every year and some send more than 100 Gbps at peak.

Related – Ransomware: How to prevent a crypto crisis at your business

---

Brute force attacks – 25%



Some attacks look for a back way in, but a brute force attack tries to kick down the front door. It's a trial-and-error attempt to guess a system's password.

One in four network attacks is a brute-force attempt. Automated software is often used to guess hundreds or thousands of password combinations.

There are many ways to defend against brute force attacks. One of the simplest is to lock accounts after a number of login attempts. Blocking IP addresses after multiple login failures is another. You can also restrict login access to certain IP addresses.

Browser attacks – 9%

Browser-based attacks target end users who are browsing the internet. The attacks may encourage them to unwittingly download malware disguised as a fake software update or application.

Malicious and compromised websites can also force malware onto visitors' systems. They often do this by exploiting a weakness in a visitor's browser or related software, typically caused by the software being out of date.

One of the best ways to avoid browser-based network attacks is to regularly update web browsers and browser-related services such as Java and Flash. This helps ensure newly discovered security vulnerabilities are patched before they can be exploited.

Shellshock attacks – 7%

“Shellshock” refers to vulnerabilities found in Bash, a common command-line shell for Linux and Unix systems.

When security researchers disclosed Shellshock in Sept. 2014, millions of systems and appliances – from web servers to thermostats – were vulnerable. Attackers have since started exploiting the flaws, using them to install malware that sends spam campaigns and DDoS attacks.

Since many systems are never updated, the vulnerabilities are still present across the Web. The problem is so widespread that Shellshock is the target of 7% of all network attacks reviewed in the report.

Related – Ransomware: How to prevent a crypto crisis at your business

---

SSL attacks – 6%

SSL attacks aim to intercept data that is sent over an encrypted connection. A successful attack enables access to the unencrypted information.

SSL attacks were more popular in late 2014, but they remain prominent today, accounting for 6% of all network attacks analyzed. A sharp rise in SSL attacks followed the disclosure last year of several security vulnerabilities in SSL and TLS, including the POODLE attack.

All versions of SSL (1.0 – 3.0) and TLS 1.0 encryption protocols are considered vulnerable to attack and should be avoided.

Backdoor attacks – 2%

A backdoor is a type of attack that bypasses normal authentication to allow remote access at will. Backdoors can be present in software by design. They can also be enabled by other programs or created by altering an existing program.

Backdoors are less common and often used as part of targeted attacks, according to Trend Micro. In these cases a backdoor can be custom-designed to avoid security detection and provide a disguised point of entry.

Botnet attacks – 2%

A botnet is a group of hijacked computers that are controlled remotely by one or more malicious actors. Networks are routinely hit with attempts to infect their computers with malware that will add them to a hacker’s robot army.

Attackers use botnets for malicious activity, or rent the botnet to perform malicious activity for others. From launching DDoS attacks, to sending out spam email, to practicing click-fraud, attackers use botnets for their dirty work.

Millions of computers can be caught in a botnet’s snare. The European Cybercrime Unit recently announced the takedown of the Ramnit botnet, which infected more than 3.2 million Windows computers.

Related resources

DDoS Attacks: Trends show a stronger threat in 2015

Top Threats: Massive denial-of-service attacks

Shellshock: New bug doesn’t shock IT service providers

Ransomware Prevention: 5 ways to avoid a crisis
