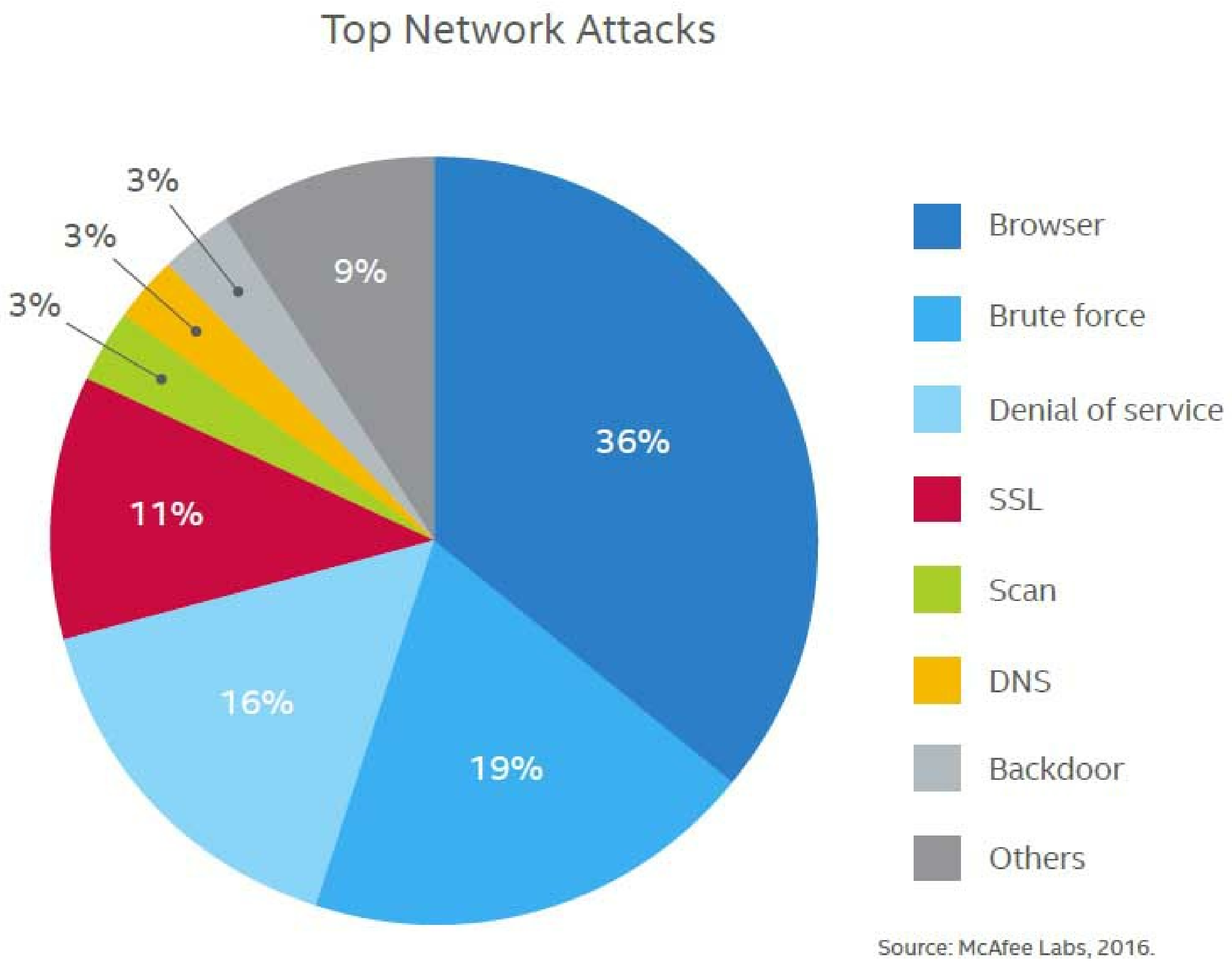
Top 7 Network Attack Types in 2016

www.calyptix.com/top-threats/top-7-network-attack-types-2016/

Criminals can pick from a long list of various network attack methods to employ against a small business. Some types are more common, and knowing them can make it easier to prioritize your cyber defenses.

The list below is based on a chart from the 2016 McAfee Labs Threat Report (pdf). It highlights the top 7 network attack types in Q4 2015, based on data from millions of sensors across file, web, message, and network vectors.



Source: McAfee Labs, 2016.

Top 7 types of network attacks

Browser attacks – 36%

Browser based attacks are the most common network attack shown in the data. They try to trick internet surfers into downloading malware that is disguised as a software application or an update.

Cyber criminals also target popular operating systems and applications by employing an exploit, which can be a piece of data or a series of commands, that takes advantage of a vulnerability in the system.

Browser attacks can be thwarted by regular updates to both the browser and related applications, such as Flash and Java.

Brute force attacks – 19%

Pay attention to your passwords! A brute force attack is when a hacker tries to decode a password or pin number through trial and error. Almost a fifth of cyber attacks in Q4 2015 were perpetrated by brute force.

Numerous consecutive guesses are generated by automated software try to crack the password code. The guesses are often common passwords (123455, or football) or combinations of letters and numbers. The dictionary attack is a tact that goes through all the words in a dictionary.

Brute force is a type of network attack that is time consuming, and success is a result of computing power and weak passwords.

Users can protect themselves by changing their passwords often, and by using odd combinations of numbers, letters, symbols and cases. Limiting log-in attempts can also help.

Denial of service attacks – 16%

A Denial of Service (DOS) attack prevents legitimate users from accessing services or information. It succeeds when an attacker overloads a server with more requests than the server can process.

DOS attacks target computer networks, or the network of sites the computer is trying to use. Online banking, email, and commercial websites are often targeted.

Distributed Denial of Service (DDoS), is when an attacker takes control of computers and uses them to flood a particular email with messages, or a website with enormous blocks of data. Numerous types of DDoS attacks have been covered in previous reports.

Anti-virus software, firewalls, and email filters can ward off a DOS attack and help manage unwanted traffic.

SSL attacks – 11%

Secure Sockets Layer (SSL) establishes an encrypted link between a website and a browser, or a mail server and a mail client. It is a standard security technology that enables secure information to be safely delivered. A website secured by SSL begins with https.

An SSL attack type intercepts the encrypted data before it can be encrypted, giving the attacker access to sensitive data including credit card information and social security numbers.

POODLE attacks have exploited the vulnerability of SSL 3.0 with CBC mode ciphers, allowing attackers to access passwords, cookies, and other authentication tokens. The POODLE vulnerability was patched in 2014, and SSL 3.0 is considered an obsolete protocol.

Scans – 3%

Port scans (pdf) are hostile searches on the internet for open ports through which attackers can gain access to a computer. Rather than one of the true types of network attacks, they are typically reconnaissance and seen as potential precursors to attack.

The intruder sends a message to a port. The response can reveal the status of the port, and help the attacker identify the operating system and its vulnerabilities, which can help the intruder launch a future attack.

DNS attacks – 3%

Domain name servers (DNS) maintain a directory of domain names, and translate them into IP addresses.

DNS spoofing is when data is introduced into the domain name system cache, causing the name server to return an incorrect IP address, which redirects traffic to an alternate computer selected by the attacker. DNS queries come through Port 53, which traditional firewalls leave open.

DNS hijacking is a type of network attack that redirects users to a bogus website when they are trying to access a legitimate one. Many companies do not protect DNS because they don't realize it is a threat vector.

Solutions include using a random source port, and keeping your servers patched and up-to-date.

Backdoor attacks – 3%

Backdoors are applications that allow computers to be accessed remotely. Many backdoors are designed to bypass intrusion detection systems.

Several attack strategies, including port binding, connect-back, and connect availability use can be employed through backdoors. Both hardware and software components can allow hackers access through malicious backdoors.

Related resources

Top 7 Network Attack Types in 2015

DDoS Attacks: Trends show a stronger threat in 2015

Backdoor Use in Targeted Attacks

Top Threats: Massive denial-of-service attacks

Ransomware Prevention: 5 ways to avoid a crisis