DDoS attacks increase over 125 % year over year

Akamai's most recent State of the Internet Security Report reveals internet and web attacks are increasing in number, severity, and duration.

By Steven J. Vaughan-Nichols for Networking | June 8, 2016

The internet is under heavier attacks than ever. In Akamai's *Q1 2016 State of the Internet - Security Report*, the content delivery network (CDN) company found there's been a 125 percent increase in distributed denial of service (DDoS) attacks year over year.

Major DDoS attacks are happening far more often.

But, wait, there's more. Much more. There's also been a 35 percent increase in the average attack duration. In the first quarter of 2015, the average attack lasted almost 15 hours. Now, they're up to just over 16 hours.

Adding insult to injury, truly massive DDoS attacks, 100 Gigabits per second (Gbps), are now more common than ever. The first quarter of 2016 saw 19 such attacks compared to 2015's eight assaults. That's an increase of 137.5 percent.

That last one is even worse than it sounds. In just the first three months of 2016, there were 19 100Gbps attacks. In 2015's last quarter there were only five.

All together in 2016's first quarter, Akamai witnessed 4,523 DDoS attacks. That's a significant increase from the previous quarter's 3,693 attacks. This increase was largely driven by repeat attacks on customers rather than cyber crooks going after more targets.

In the first quarter of 2015, there was an average of 15 attack events per targeted customer in 2015. By the first quarter of 2016, the average number of attacks had grown to 29.

It used to be that attackers would see that a site or network was protected and move on. Now, they hammer away at the target hoping that the defenses might drop. This is most often the case with gaming sites, where even the slightest latency can have a noticeable effect on online gamers. Another reason for the increase in repeat attacks is that DDoS attack platforms have become cheap and easy to use.

Indeed, DDoS attacks no longer require any hacking or networking skills. DDoS-for hire sites now enable anyone with Bitcoin to launch multiple simultaneous attacks from an easy-to-use interface with a menu of attacks.

How bad has it gotten? Akamai's most frequently attacked customer in Q1 2016 was targeted with 283 DDoS attacks. Count it up. That's three separate attacks per day.

The largest recent DDoS attack came to 289 Gbps. That's a 20-Gbps drop over the largest attack in the previous quarter: 309 Gbps.

Compared to the all-time worst DDoS attack, on a French website in 2014 that almost reached 400Gbps, the biggest attacks have gone down in volume. That's because the methods used to create monster attacks, while much easier to use, are less efficient as ISPs have gotten better at protecting their network services.

Still, six DDoS attacks in the first quarter exceeded 30 million packets per second (Mpps). Two attacks peaked at more than 50 Mpps. The packet rate can affect some routers and networks more than the number of bytes per packet. That's because even the smallest packets can consume memory, thus tying up router resources.

Online gaming has been hit the hardest. 55 percent of all DDoS attacks were made on gaming sites. This comes as no surprise, since gaming has been the hardest-hit since 2014.

Of these attacks, four methods -- UDP Fragment, NTP, DNS amplication, and Chargen -- made up nearly 70 percent of the attacks. There's nothing new about any of these methods. They prey on inherent weaknesses in the TCP/IP-based internet.

Lately, DDoS attackers are combing attack methods. Multi-vector attacks now account for 59 percent of all DDoS attacks. This continued rise of multi-vector attack suggests that attackers or their attack tools are growing more sophisticated. This, in turn, makes life harder for security and network professionals since they must deploy different defences for each unique attack vector.

It's not just the network itself that's getting attacked more often -- the websites are also getting hammered more often. Since the last quarter, web application attacks increased by 25.5 percent.

The most common attack type no longer includes the once popular cross-site scripting (XSS) attack. Instead, the most popular attacks over HTTP were SQL Injection (SQLi) and Local File Inclusion (LFI) at 47 percent and 35 percent respectively. On HTTPS, LFI came first with 38 percent with SQLi taking second with 31 percent. Believe it or not, on HTTPS, the long fixed Shellshock hole is still in third place with just over 20 percent.

SQLi is an attack where an attacker's content is inserted directly into a SQL statement before parsing, rather than being safely conveyed to the website's database engine. SQLi has been on the Open Web Application Security Project (OWASP) Top 10 web security problem list for over a decade, but companies still allow it to be exploited. It's a solvable problem. It only requires web developers use coding techniques that include security checks. But, even now programmers in a hurry don't fix it.

There's even less of an excuse for Shellshock still being a problem. The Shellshock patches have been in place since the fall of 2014.

LFI is also an old-style attack, which still catches companies out. In it a malicious user is able to gain unauthorized read access to local files on the web server.

You may be asking why there are so many attacks over the "secure" HTTPS. The reason is simple. HTTPS only encrypts data between you and the web server. It does nothing whatsoever to protect vulnerable applications.

For web application attacks, it's retailers, not gamers, that suffer the most: 43 percent. The hotel and travel industry came in second while being targeted with 13 percent of attacks. These were followed by financial services, at 12 percent; high technology, 9 percent; media and entertainment, 7 percent; the public sector, 3 percent; Software-as-a-Service (SaaS), 3 percent; and business services, 2 percent.

Looking ahead, Akamai expects "the heavy barrage of DDoS attacks against the gaming industry to continue, as players keep looking for an edge over competitors". As for web service attacks, retailers will continue to suffer the most, given the potential financial gains for attackers. Akamai predicts, "SQLi and LFI will remain favourite vectors, because free and open-source tools are plentiful to find these vulnerabilities".

The moral of the story for businesses? Now, more than ever, you need to defend your websites against both DDoS and web services attacks. Their number will only increase as it becomes ever easier for attackers to launch assaults against your sites.