Pick Your Poison: The Most Popular Cyber Attacks in 2015

Necessity is the mother of invention. That certainly holds true in the world of cyber security. As security professionals have developed new defenses to attack vectors, hackers have developed new tools to counter the countermeasures. The result is a plethora of attack types that, depending on industry trends, rise and fall in popularity throughout the year. Based on research and surveys of over 300 worldwide organizations by Radware, this paper outlines the attack vectors that proved popular in 2015, and thus sheds light on what to expect in 2016.

Application vs. Network Attacks

In 2015, the balance between application and network attacks was fairly even, and for a few reasons. First and foremost is the use of multi-vector, blended campaigns that include higher-volume network vectors alongside more sophisticated application attacks. Thus, while the numbers indicate that the three largest attack types are more likely to be network-based attacks, the threat of application attacks is still very much real.

In 2015, 65% of the three biggest cyber-attacks that organizations experienced were on the network, most frequently TCP-SYN floods, which comprised 24% of network attacks. 2015 also brought an increase in ICMP attacks (14% in 2015). Within application-based attacks, web HTTPS/S attacks represented only 15% of cyber assaults, while DNS-based attacks represented only 13% (see Figure 1).

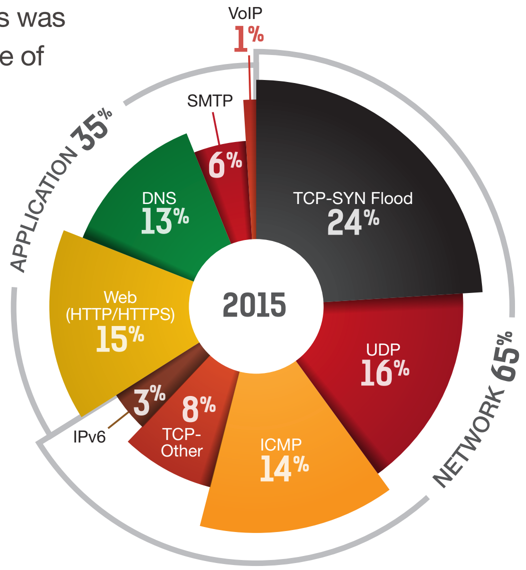

Figure 1: Biggest Cyber-Attacks in 2015

Frequency of Attacks

More than one-quarter of respondents reported daily and weekly attacks on TCP-other, TCP-SYN, ICMP and UDP flood attacks in 2015, while attacks on IPv6 networks represent the most infrequent network attack in 2015. At least one in five respondents experienced daily or weekly application attacks. Overall, research indicates a similar spread of frequency between network and application types of attacks (See Figures 2 & 3).

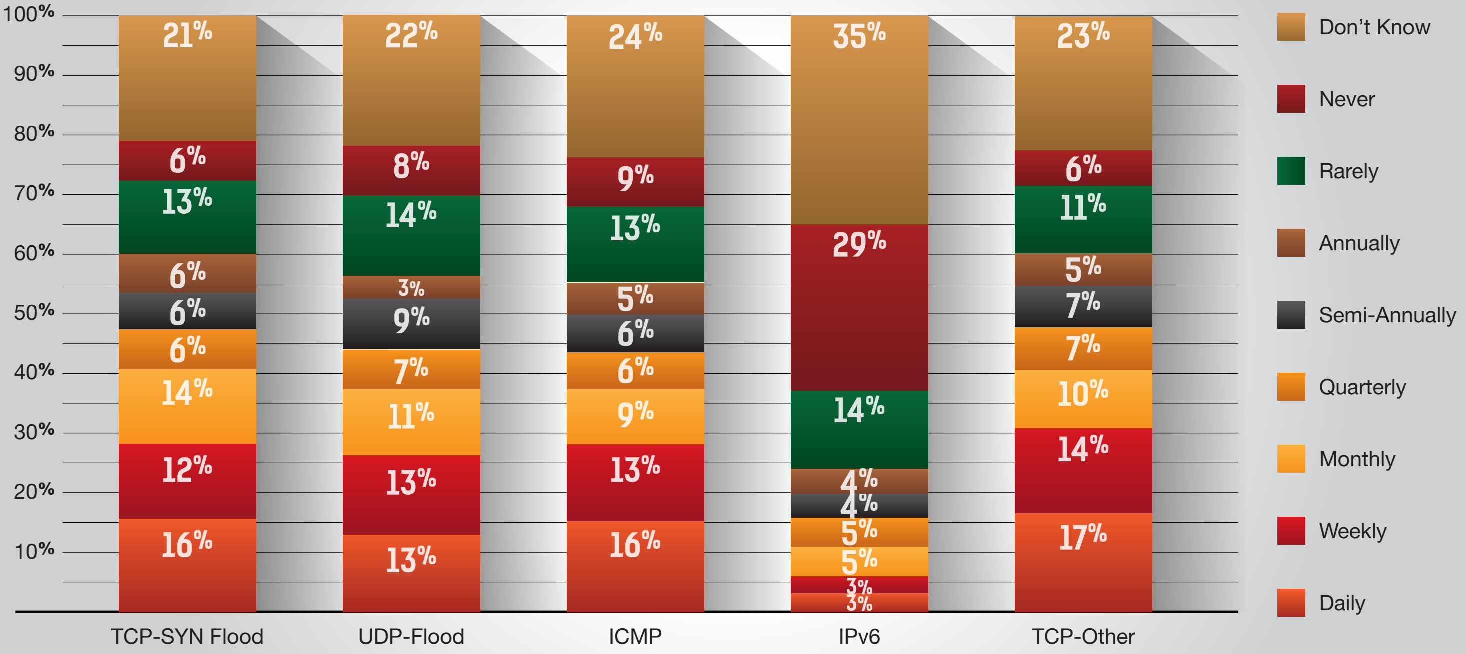

Figure 2: Frequency of Network Attacks in 2015

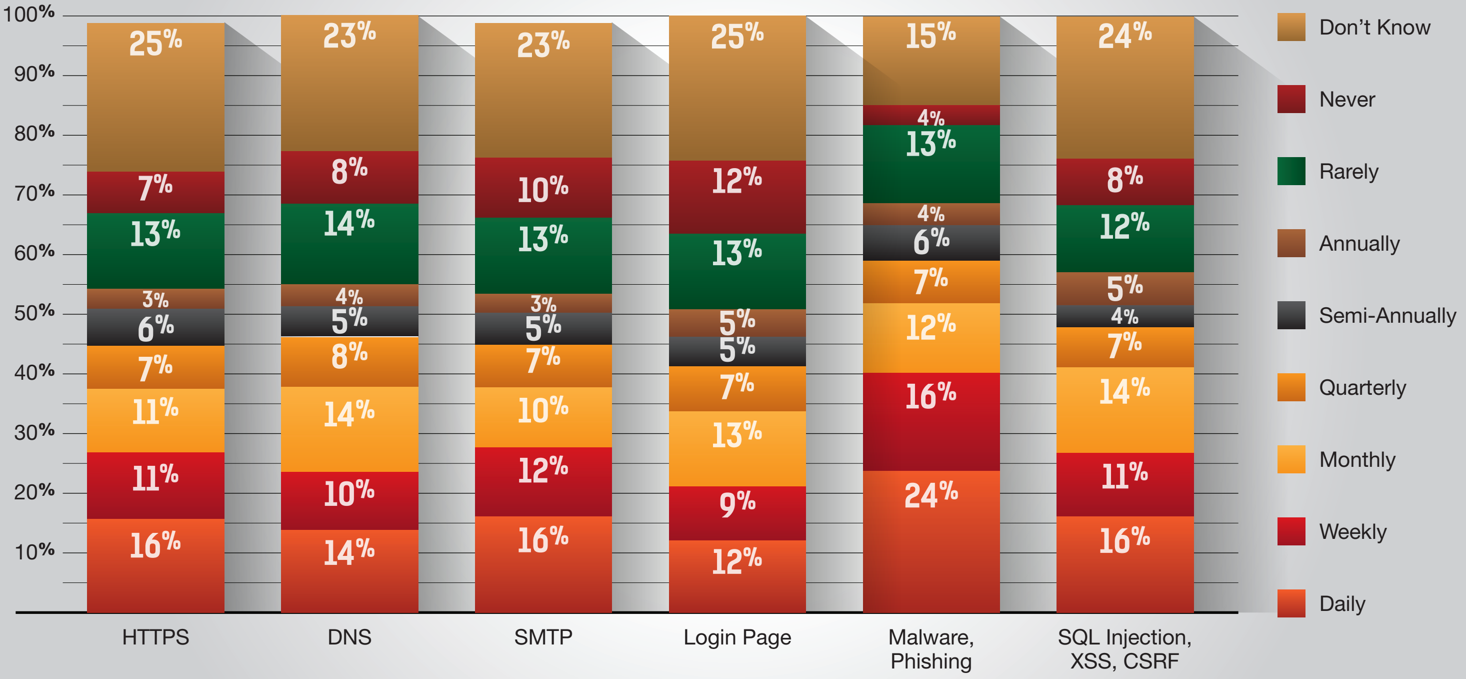

Figure 3: Frequency of Application Attacks in 2015

Multi-Vector Attacks

The popularity of multiple-vector attacks continues to grow. Attacks are now advanced persistent DDoS campaigns. What's more, attackers are changing vectors based on mitigation in "burst-like" patterns, leading the way to smarter, automated attacks. Every year, attackers find new vectors of attacks, such as Portmappers, mDNS and RIPv1.

Given the popularity in ransom-motivated attacks in 2015 (25% in 2015), as well as the overall rise in encrypted attacks, it's no surprise that more organizations (one-third of respondents) have experienced either a ransom attack or an SSL or TLS-based attack (see Figure 4).

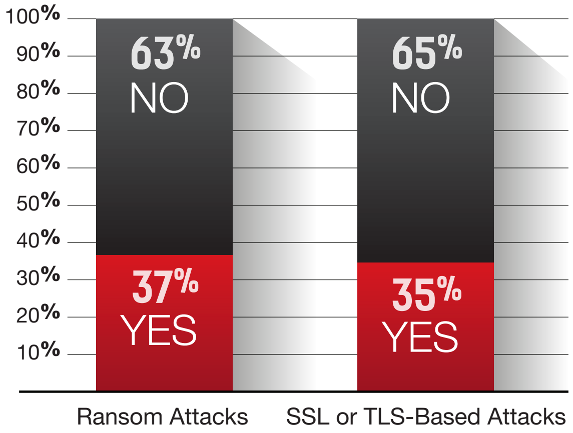

Figure 4: Ransom and SSL or TLS Attacks Experienced by Organizations in 2015

The increase in encrypted attacks contrasts sharply with the confidence organizations have in its existing SSL protection. About half of the respondents indicated that its security solution includes SSL attack protection, though they are uncertain of exactly what types. Only 30 percent said its solution provides complete protection from SSL-based attacks, and one-fifth reported that their solution does not include SSL attack protection (see Figure 5).

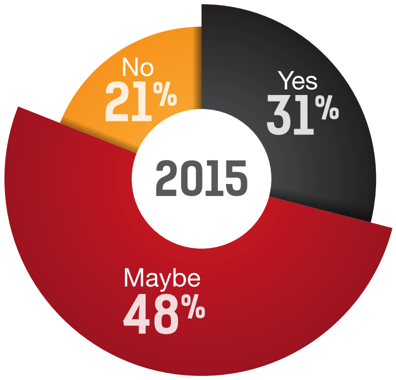

Figure 5: Availability of SSL Flood Attack Protection

Attack Size: Does It Matter?

In 2015, less than one in 10 server attacks qualified as "extra-large" (10Gbps and higher). The most common attacks—experienced by two in five respondents—were below that threshold. The number of 10Mbps to 100Mbps attacks increased in 2015 to 25% (compared to 7% in 2014), while the attacks ranging from 100Mbps to 1Gbps declined to 15% (versus 25% in 2014).

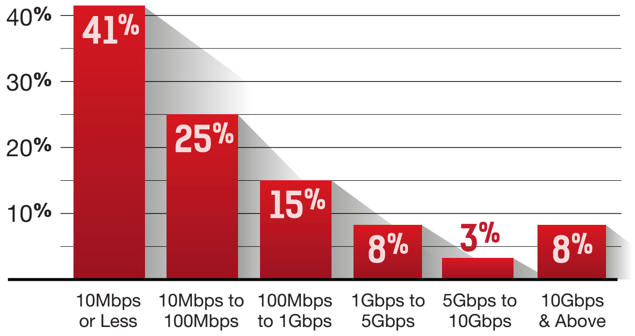

Figure 6: Availability of SSL Flood Attack Protection

More than one-third of respondents indicated that the biggest attacks impacted the Internet pipeline, with nearly three in ten reporting impact on a server. One in five said the firewall was impacted. At 3%, load balancer impact was the least affected.

In terms of defense, the numbers aren't encouraging either. One-third of respondents feel its organizations have a volumetric pipe saturation weakness; another quarter feel vulnerable to network and HTTPS/SSL attacks.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.