CONTENTS

EXECUTIVE SUMMARY 3
VERISIGN-OBSERVED DDoS ATTACK TRENDS Q1 2015 4
Mitigations by Attack Size 4
Mitigations by Industry 5
FEATURE: THE MANY MOTIVATIONS BEHIND TODAY’S DDoS ATTACKS 6
CONCLUSION 8
EXECUTIVE SUMMARY

This report contains the observations and insights derived from distributed denial of service (DDoS) attack mitigations enacted on behalf of, and in cooperation with, customers of Verisign DDoS Protection Services and the security research of Verisign iDefense Security Intelligence Services. It represents a unique view into the attack trends unfolding online for the quarter, including attack statistics and behavioral trends.

For the period starting Jan. 1, 2015 and ending March 31, 2015, Verisign observed the following key trends:

- Verisign mitigated more attacks in Q1 2015 than any quarter in 2014, including seven percent more than Q4 2014.
- The frequency of attacks against both public sector and financial services customers increased; each grew from 15 percent in Q4 2014 to represent 18 percent of all Verisign mitigations in Q1 2015.
- Over half of all attacks peaked at more than one gigabit per second (Gbps), 34 percent of attacks peaked between one and five Gbps, and nearly 10 percent of attacks peaked at more than 10 Gbps.
- Volumetric DDoS attack sizes peaked at 54 Gbps/18 million packets per second (Mpps) for User Datagram Protocol (UDP) floods and 8 Gbps/22 Mpps for Transmission Control Protocol (TCP)-based attacks.
- IT Services/Cloud/SaaS was the most frequently targeted industry in Q1, representing more than one third of all mitigation activity.

Feature: The Many Motivations Behind Today’s DDoS Attacks

Since the early days of the Internet, malicious actors have used DDoS attacks as tools of protest, financial gain, retaliation and simple mischief. A look into the various reasons why these actors use this increasingly effective form of online attack can help victims and security professionals better understand, anticipate and prepare for these increasingly accessible and disruptive threats.
Mitigations by Attack Size

DDoS attack activity in the “1-5 Gbps” category experienced the greatest increase in Q1 2015, growing from 19 percent in Q4 2014 to represent more than 34 percent of all attacks (see Figure 1). In addition, nearly 10 percent of attacks in Q1 peaked at more than 10 Gbps. In all, over 50 percent of attacks peaked at more than one Gbps, which even today remains a significant amount of bandwidth for any network-dependent organization to over-provision for DDoS attacks.

Figure 1: Mitigation Peaks by Category

Attacks mitigated by Verisign in the first quarter of 2015 yielded a mean peak size of 3.64 Gbps (see Figure 2), which represents roughly a 50 percent decrease in average attack size from Q4 2014 and a 7 percent decrease over Q1 2014. As stated earlier, this remains a significant amount of bandwidth for any organization to over-provision for DDoS protection. Although the mean peak attack size decreased quarter over quarter, Verisign mitigated more attacks in Q1 2015 than in any quarter in 2014, including seven percent more than Q4 2014.

Figure 2: Mean Peak Attack Size by Quarter

The largest volumetric attack mitigated by Verisign in Q1 was primarily a UDP-reflection attack leveraging the Network Time Protocol (NTP) and Simple Service Discovery Protocol (SSDP) in combination with a lower volume of SYN flood traffic, which peaked at 54 Gbps/18 Mpps. This attack targeted an IT Services/Cloud/SaaS customer and persisted for approximately four hours.
**Mitigations by Industry**

DDoS attacks are a global threat and not limited to any specific industry, as illustrated in Figure 3. Verisign acknowledges that the attacks by vertical reported in this document are solely a reflection of Verisign’s protected customer base; however, this data may be helpful in understanding the evolution of attacks by industry and the importance of prioritizing security expenditures to help ensure protection mechanisms are in place.

In Q1 2015, IT Services/Cloud/SaaS customers experienced the largest volume of attacks (see Figure 3), representing more than one third of all attacks and peaking in size at just over 54 Gbps. Verisign predicts the trend in attacks against IT Services/Cloud/SaaS will continue as more organizations migrate IP assets to cloud-based services and infrastructure.

The financial services and public sector industries tied for the second-most frequently attacked customers in Q1, representing 18 percent each. Verisign observed an increase in attacks targeting these industries in Q4 2014, and the trend continued in the first quarter of 2015. Verisign believes this increase in attacks may be partially attributed to an increased employment of DDoS attacks as part of political activism, or hacktivism, against financial services firms and various international governing organizations. Verisign also believes that these attacks may be in reaction to various well-publicized events throughout the quarter, including the Charlie Hebdo terrorist attacks in Paris, France, and protests in Venezuela, Saudi Arabia and the United States. The ready availability of an increased number of DDoS toolkits and DDoS botnets for hire, as highlighted in Verisign’s Q4 2014 DDoS Trends Report, may also have contributed to increased attacks against these industries in Q1.

<table>
<thead>
<tr>
<th>IT Services/Cloud/SaaS</th>
<th>Financial</th>
<th>Public Sector</th>
<th>Manufacturing</th>
<th>Media &amp; Entertainment</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>34%</td>
<td>18%</td>
<td>18%</td>
<td>13%</td>
<td>12%</td>
<td>5%</td>
</tr>
</tbody>
</table>

-Figure 3: Q1 2015 Mitigations by Industry-
THE MANY MOTIVATIONS BEHIND TODAY'S DDoS ATTACKS

Since the early days of the Internet, malicious actors have used DDoS attacks as tools of protest, financial gain, retaliation and simple mischief. A look into the various reasons why these actors use this very effective form of online attack can help victims and security professionals better understand, anticipate and prepare for these increasingly accessible and disruptive threats.

Activism and Protest

Dec. 21, 1995: an entity calling itself the “Strano Network” delivers an announcement to various online bulletin boards calling for its members and sympathizers to simultaneously visit a selection of French government websites in an effort to knock them offline.1

Simply put, online activism, or “hacktivism,” is attributed to attackers motivated by ideology to affect change. DDoS attacks have risen to prominence as one of the main weapons of choice for attackers when it comes to cyber protest.

A hacktivist DDoS attack is usually triggered by a notable event or grievance that is often publicized by mainstream media and amplified through social media. Such a campaign generally capitalizes on negative sentiment toward the target organization. The global reach of interconnected technology, however, means the targets are not necessarily limited to just the primary “wrongdoers,” but can easily expand to other related targets, including affiliates, third-party providers, advertisers and even customers.

Though the Strano Network “electronic sit-in” is sometimes cited as one of the earliest hacktivist attacks aimed at disrupting access and availability of Internet sites for ideological reasons (the actors took specific umbrage with the French government’s stance on nuclear arms), the first prominent modern Internet protest movement to adopt DDoS attacks as a tool is largely considered to be “Operation Payback” (or “OpPayback”).2

OpPayback started as retaliation by the Anonymous collective for attacks on distributed content-sharing sites, such as The Pirate Bay. The first OpPayback attacks targeted the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA). Soon after OpPayback, a series of DDoS attacks codenamed “Operation Avenge Assange” targeted and successfully brought down the websites for PayPal, Visa and MasterCard. This operation was launched as a protest against the decision by the targeted organizations to suspend transactions for the whistleblower site WikiLeaks.3

Since OpPayback, groups under different banners have carried out ideologically motivated DDoS attacks against various targets. Some of these attacks are crowdsourced while others are launched using botnets. Most of these protest-type attacks are accompanied by announcements from various groups about the attacks beforehand and claims of responsibility for the attacks after the fact. Social media sites often become the bulletin boards for these announcements.

Cyber Crime

What distinguishes cyber crime from hacktivism is its targeted goal, which is generally financial gain instead of ideological supremacy. Actors in this category seek to profit directly or indirectly by launching DDoS attacks or owning DDoS infrastructure.

One common criminal use for DDoS attacks is blackmail. Individuals or groups that have access to botnets capable of launching DDoS attacks can blackmail organizations into paying a ransom (or meeting other demands) to avoid being attacked or to stop an attack in progress. Victims of ransom attacks often do not publicly acknowledge the attack for reputational reasons. In addition, not every ransom attack is successful, since some targets are capable of mitigating such attacks without impacting their organizations. Basecamp, an online collaboration and project management service, and Meetup, a social event organizing service, were subject to such extortion attempts, but thwarted and acknowledged the attacks in early 2014.4,5

Another popular criminal use for DDoS attacks involves otherwise legitimate businesses attacking competitors or perceived competitors to gain a business advantage. The availability of online resources and tools, including email, e-commerce and productivity applications and services can serve as the lifeblood of Web-reliant businesses; competing businesses can seek to disrupt their competitors’ Web-based assets in an attempt to hinder the victim’s ability to function. One such incident came to light nationally in 2004 when the U.S. Federal Bureau of Investigation (FBI) indicted the owner of satellite TV retailer Orbit Communication Corp. on charges that he allegedly recruited attackers to leverage DDoS attacks against three competing businesses. The sting, dubbed “Operation Cyberslam,” is touted as one of the first widely known instances of DDoS-for-hire services being targeted toward a competitor.6

Finally, criminally minded attackers can use DDoS attacks as an effective smokescreen to launch other types of intrusions into networks, often with financial goals in mind. While intrusion-response teams focus on DDoS mitigation, attackers have a greater chance of evading notice while conducting data and financial theft, including fraudulent wire transfers from victimized accounts.7 A 2012 joint statement from the FBI, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Internet Crime Complaint Center (IC3) noted the then-new trend of using DDoS attacks as a diversion, and identified malware dubbed “DirtJumper” as one of the tools of choice for the attackers. The joint statement warned financial institutions described DirtJumper as “a commercial crimeware kit that can be bought and sold on criminal forums for approximately $200.8

---

5 “We are standing up against a DDoS attack.” March 3, 2014. Meetup. http://blog.meetup.com/411/were-standing-up-against-a-ddos-attack/.
Retaliation and Mischief

Not all DDoS attackers’ motives, however, fit neatly inside the boundaries of ideological or financial gain.

Some DDoS attacks seem to serve little other purpose than retaliation. The DDoS attack launched against non-profit anti-spam company Spamhaus in March 2013, stemmed from the company’s support of blacklisting servers it felt were responsible for sending unsolicited emails. In response to being blacklisted by Spamhaus, controversial hosting provider CyberBunker reportedly launched a retaliatory DDoS attack against Spamhaus, unintentionally affecting several Internet relay points in addition to its target, and slowing Internet traffic noticeably.9

The ready availability and access to DDoS botnets via tools such as the infamous Low-Orbit Ion Cannon (LOIC), along with DDoS-for-hire “bother” services, have made attacks simple for those interested in little else but causing mischief. A spate of attacks levied at various elements of the video games industry throughout 2014 could be placed into this category, as there appear to be no apparent financial or ideological motives behind them.10 Attacking online gaming services seems to have become an increasingly effective means for these actors to gain public notoriety and status among members of the underground community, harkening back to earlier days when skilled but largely marginalized actors performed website defacements and other intrusions simply to prove they were capable of doing so.

A more recent example of DDoS attacks used for this purpose includes attacks in late March 2015 against government websites related to the American state of Maine. State-government-related sites came under attack several times, effectively preventing visitors from accessing online public services and information on those sites. According to a report by the Portland Press Herald, a Twitter user purportedly affiliated with the responsible group claimed on the social media platform that “the group was conducting the attacks for fun and to demonstrate its cyber attacking (sic) prowess.”11

CONCLUSION

Today’s DDoS attackers choose their targets and tactics for a number of reasons, many of which may not be clearly evident to the victims or the security professionals and law enforcement organizations who assist them. Understanding the various potential motives behind DDoS attacks can help defenders anticipate and ideally prevent these attacks before they cause irreparable damage to business operations, online revenue generation and reputation. Regardless of their motivations, however, DDoS attackers are proving more adept and effective than ever at disrupting their targets, and network-dependent organizations of all industries, types and sizes should consider their risk and prepare accordingly.