## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>4</td>
</tr>
<tr>
<td>CYBERCRIME</td>
<td>6</td>
</tr>
<tr>
<td>Criminal Migration to the Darknet</td>
<td>6</td>
</tr>
<tr>
<td>Ransomware-as-a-Service</td>
<td>6</td>
</tr>
<tr>
<td>The Rise of DD4BC</td>
<td>7</td>
</tr>
<tr>
<td>Downloader Architecture Evolves</td>
<td>8</td>
</tr>
<tr>
<td>VULNERABILITIES</td>
<td>10</td>
</tr>
<tr>
<td>Increased Adobe Flash Exploitation</td>
<td>10</td>
</tr>
<tr>
<td>Proliferation of Exploit Kits</td>
<td>11</td>
</tr>
<tr>
<td>Hacking Team Hacked; Zero-Days Leaked</td>
<td>12</td>
</tr>
<tr>
<td>HACKTIVISM</td>
<td>14</td>
</tr>
<tr>
<td>Ideological Hacktivism in International Decline</td>
<td>14</td>
</tr>
<tr>
<td>Increase in Hacktivist OPSEC</td>
<td>15</td>
</tr>
<tr>
<td>Shift to Criminal and Notoriety Hacktivism</td>
<td>15</td>
</tr>
<tr>
<td>Increasing Size, Complexity of DDoS Attacks</td>
<td>16</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>18</td>
</tr>
<tr>
<td>ABOUT VERISIGN</td>
<td>18</td>
</tr>
</tbody>
</table>
INTRODUCTION

The Verisign iDefense 2016 Cyberthreats and Trends Report provides an overview of the key cybersecurity trends of the previous year and insight into how Verisign believes those trends will evolve over the coming year. The objective of this report is to assist in informing cybersecurity and business operations teams of the critical cyberthreats and trends impacting their enterprises, helping them anticipate key cybersecurity developments and more effectively triage attacks and allocate increasingly limited resources.

This report features conclusions drawn from Verisign iDefense Security Intelligence Services research and analysis covering cybercrime, hacktivism and vulnerabilities. These areas of coverage include public and zero-day vulnerabilities, threat tactics, distributed denial of service (DDoS) attacks, threat actors, threats to key infrastructure, strategic intent, malware tools, and threat and vulnerability management, mitigation and countermeasures.

Disclaimer: The information in this 2016 Cyberthreats & Trends Report (this “Report”) is believed by Verisign to be accurate at the time of publishing based on currently available information. Verisign provides this Report for your use in “AS IS” condition and at your own risk. Verisign does not make and disclaims all representations and warranties of any kind with regard to this Report including, but not limited to, any warranties of merchantability or fitness for a particular purpose.
EXECUTIVE SUMMARY

The growing reliance on the connected digital world for a variety of business tasks has forced professional security practitioners to accept an increasingly stark reality. Attackers are no longer interested solely in taking down large enterprise networks or just stealing data, nor are they limited by their own ingenuity and skill. Security teams in 2016 and beyond must now also guard against purely destructive and punitive threats, and not just to themselves, but also to their supply chains, social media channels and other elements of the business ecosystem, both online and off. Understanding the complexity of the cyberthreat landscape is critical to keeping pace with today’s cyber criminals, hacktivists and thrill seekers, who prove increasingly adept at leveraging security weaknesses and standardized technologies and practices for profit, notoriety, ideology or combinations of the three.

In 2015, cyberthreats evolved, as malicious actors updated their tactics, techniques and procedures (TTPs) to keep pace with an ever-growing and more lucrative threat landscape. Their wares of choice included new vulnerabilities and exploits, increasingly stealthy and automated malware, and readily available and affordable attack tools.

Even though international law enforcement agencies saw some success against cyber criminal groups and campaigns, the practice of leveraging cyber-attacks for financial gain itself grew and evolved in 2015. As cyber-criminals moved away from once-reliable communications and coordination channels to others offering more secrecy, some groups found new success using an old criminal method—extortion—to achieve their goals. Cyber-extortion, both manual (e.g., DD4BC) and automated (e.g., ransomware), is not new to cyber criminals’ repertoires, but 2015 saw the tactic not only become more refined, but more widespread than many could have predicted.

Software vulnerabilities have always been at the root of many cyberthreats facing enterprises, but in 2015, threat actors looking to exploit software flaws in popular applications and critical infrastructure found new and better ways to increase the effectiveness and breadth of vulnerability-focused attacks. Notably, Verisign’s iDefense Security Intelligence Services team observed that Adobe Flash largely replaced Java as the vector of choice for attackers, and these attackers also proved capable at using these vulnerabilities to power new and more effective automated exploit kits. Making matters worse for enterprises, public disclosure of numerous zero-day vulnerabilities from the Hacking Team breach gave attackers even more fuel for their nefarious activities.

Fundamental shifts in motive, means and cause drove changes in the online activism, or hacktivism sphere. Ideological motivations largely took a back seat to more criminal- and notoriety-focused hacktivist attacks. Simultaneously, hacktivists seemingly learned from law enforcement successes and made secrecy and security of their operations a higher priority, which will no doubt make future attacks less predictable and more difficult to combat. DDoS attacks also grew in size, duration, complexity and frequency in 2015, likely due to the availability and affordability of DDoS-for-hire (or “booter”) services.²

In 2016, at-risk enterprises most likely will continue to find mixed success as they attempt to keep pace with the rapid changes in the security landscape that are being driven by successes and failures on both sides of the security equation. By maintaining awareness of not only the actors and technologies, but also the context surrounding their motivations and objectives, enterprises have an opportunity to anticipate and head off the next evolution in online threats.

**CYBERCRIME**

**Criminal Migration to the Darknet**

In 2015, iDefense observed that malicious actors began to increasingly adopt the “darknet” as a platform for cybercrime activities, despite several noteworthy darknet communities meeting their demise. Tor-based criminal communities flourished, though the lifespan of these forums and marketplaces was often shorter than those residing on the clearnet.

iDefense analysts observed that both clearnet and darknet criminal communities appeared at an alarming rate in 2015. The majority of clearnet criminal communities required little, if any, verification prior to joining. However, these clearnet communities appeared to gain momentum at a much slower pace than those residing in the darknet. The apparent extra layer of anonymity of darknet platforms such as Tor was, and remains, appealing for malicious actors despite past crackdowns by law enforcement and attack vectors revealed by the security community. iDefense research suggests that these setbacks have not dissuaded actors from continuing to offer illicit products and services within the darknet.

**Ransomware-as-a-Service**

During the course of 2015, iDefense observed numerous instances of ransomware – malware designed to block or limit access to a computer system until a sum of money is paid (see Figure 1) – for sale on the black market, including variants affecting both computers and mobile devices. Malicious actors also developed the concept of ransomware-as-a-service (RaaS). For example, in May, McAfee Labs identified Tox, short for “Toxicola,” an easy-to-deploy ransomware toolkit that encrypts files on an infected machine in a manner similar to Cryptolocker, although users reported that the ransomware failed to function as advertised. A few months later, iDefense encountered a similar RaaS kit dubbed “Encryptor RaaS” by its developer(s).

The emergence of several RaaS models is likely indicative of a future trend in which malicious actors will spend greater time developing ransomware with more advanced capabilities than both Tox and Encryptor. For now, the majority of ransomware variants available on the black market must be purchased manually through a vendor, which requires human interaction and is a more time-consuming process than using automated services, such as Tox and Encryptor.

---


---

![Figure 1: Ransomware Process](image)
The Rise of DD4BC

DD4BC, also known as DDoS for Bitcoin, is a group that launched DDoS attacks against targets of interest and extorted victims demanding ransom payments (see Figure 2) in the form of Bitcoin. Originally, the group targeted Bitcoin exchanges, online casinos and gaming sites; however, in 2015, iDefense observed that DD4BC expanded its target set to include financial institutions.\(^5\) To date, DD4BC has been hard to track as it utilized a slew of email and Bitcoin addresses (which are not related or consistent) to cover its tracks, which has allowed the identity of its members to remain unknown.

DD4BC uses a variety of DDoS attacks against its victims. According to the Q2 2015 DDoS Trends Report, the Verisign DDoS Protection Services team mitigated attacks on behalf of its customers targeted by DD4BC in the form of small floods, typically Transport Control Protocol SYN (TCP) or User Datagram Protocol (UDP), consisting of Simple Service Discovery Protocol (SSDP) and Network Time Protocol (NTP) floods, in the range of 1 to 5 gigabits per second (Gbps) that subsided in less than an hour.\(^6\) In July 2015, the group targeted e-commerce online travel organizations with attacks peaking at 25 Gbps. The Verisign DDoS Protection Services team has observed DD4BC using NTP, UDP, SYN Flood and Wordpress XML-RPC reflection/amplification DDoS attacks. Additionally, DD4BC appears to use common UDP reflection DDoS attack techniques and SYN flood attacks that “spoof Google crawler IP addresses to mask malicious traffic.”\(^7\)

Verisign found evidence that DD4BC carried out DDoS attacks that sent data at 20 Gbps – suggesting the use of a functioning botnet – and suspects that the actors are renting DDoS-for-hire services.\(^8\)

Although, between January 2015 and June 2015, frequency and types of attacks attributed to DD4BC remained consistent, from June 2015 through late September 2015, attacks from DD4BC seemed to reduce in frequency. iDefense hypothesizes that DD4BC may have unofficially “retired” due to increased scrutiny from law enforcement officials and security researchers, or members have decided to undertake other and more lucrative activities. It is also possible that DD4BC members were apprehended and their arrests have not been publicly reported.

As Verisign reported in its Q2 2015 DDoS Trends Report, DD4BC created a trend that has inspired copycat attacks. In July 2015, the U.S. Federal Bureau of Investigation (FBI) revealed that more than 100 businesses, including large banks and brokerage firms, reported DDoS extortion attempts similar to those of DD4BC. However, the identities of the affected businesses were not made public, nor was DD4BC blamed for this rash of high-profile threats.\(^9\) Current details regarding other criminal organizations that leverage tactics identical to DD4BC are scarce. While it may not be the first group to attempt extortion through DDoS attacks, DD4BC is the most well-known thanks to media coverage in 2015.

---

7. ibid
8. ibid
Downloader Architecture Evolves

iDefense saw downloader malware increase in popularity in 2015 as a method for cybercriminals to deploy malware to victim machines. Downloader malware families like Andromeda, Pony and Upatre remained popular among cybercrime actors; these types of downloaders are typically used to download and execute a secondary payload while providing some layer of encryption or obfuscation. Moreover, the Pony family and other variants also possess their own information-stealing capabilities.

In addition, iDefense saw downloader malware analysis and detection techniques become more advanced and difficult to identify. In particular, malicious actors separated campaign targets into distinct stages through the use of downloaders, also known as “loaders.” This type of campaign architecture allows for a more modular approach, whereby actors can easily modify a downloader’s command-and-control (C&C) server to deliver a new, second-stage payload, push updates to the downloaders themselves and avoid anti-virus detection.

Further, use of multi-stage, or chained, downloads increased in 2015, most commonly with VBA macro and JavaScript downloaders. In one example, the macro will retrieve an encoded text file from a Stage 1 C&C server that, when decoded, will contain the URL for the Stage 2 C&C server. The downloader then contacts the recently decoded URL for the Stage 2 C&C server, which contains the Stage 3 URL for the final executable payload the downloader is ultimately delivering (see Figure 3).

iDefense analysts monitored several chained downloader architectures over their active lifespans and discovered that actors commonly repacked their final payloads in an attempt to further avoid detection, or delivered a new payload that used different C&C servers, instead of delivering an entirely different malware family.

Because most downloaders are distributed through phishing campaigns, iDefense recommends maintaining strict filtering on inbound emails, specifically looking for emails with Word, Excel, ZIP, CHM and JavaScript files as attachments.

Figure 3: Multi-stage Downloader Architecture
Conclusion: Cybercrime

In the coming year, iDefense hypothesizes that darknet criminal markets will continue to attract users at a much quicker pace than those residing on the clearenet. However, due to the continued rapid migration of cybercriminals to the darknet, these communities will attract a great deal of unwanted attention from law enforcement, security researchers and the media. As a result, the lifespan of darknet markets will reduce, which will contribute to an increase in more short-lived communities.

Ransomware prospered in 2015, with the release of numerous variants onto the black market. iDefense witnessed the inception of ransomware-as-a-service through the use of poorly deployed toolkits, such as Tox and Encryptor RaaS. However, the RaaS model opened the door to similar and potentially more lucrative criminal operations in the future. In 2016, iDefense anticipates that automated ransomware kits will appear with greater frequency and more advanced features, which may include the infection of mobile devices.

DD4BC extorted victims by demanding ransom payments in 2015, and has already inspired copycat attacks. DD4BC expanded its attacks in 2015 beyond Bitcoin exchanges, online casinos and gaming sites. As a result, many other industry sectors are potentially at risk. iDefense believes that DDoS extortion attempts may evolve to include the compromise and disclosure of highly sensitive data if attackers’ demands are not met.

Actors will likely continue to heavily use executable downloaders and multi-stage downloaders throughout 2016 and beyond. Multi-stage downloader techniques are becoming more popular among malicious actors—both cybercrime and espionage—because they can easily modify URLs, or “links in the chain.” These techniques are attractive because actors simply update one of the links in the chain to point victims to a new payload. Actors can also replace the final payload with the executable of their choosing without modifying their initial downloaders or the campaigns delivering those downloaders.


In 2016, iDefense anticipates that automated ransomware kits will appear with greater frequency and more advanced features, which may include the infection of mobile devices.
VULNERABILITIES

Increased Adobe Flash Exploitation

Since its release in late 1996, Adobe Systems Inc.’s Flash Player has become one of the most highly used tools for streaming media. However, Adobe Flash vulnerabilities were successfully exploited and linked to many exploit kits throughout 2015.

The Hacking Team breach in 2015 revealed three major zero-day vulnerabilities affecting Adobe Flash: CVE-2015-5119,11 CVE-2015-512212 and CVE-2015-5123.13 Soon after being publicly disclosed, information about these vulnerabilities was released with Metasploit modules. Each one is a use-after-free (memory corruption) vulnerability and was used in multiple exploit kits.

CVE-2015-5119 was the first Adobe Flash vulnerability to be publicly disclosed and was used in seven exploit kits: Angler, Neutrino, Nuclear Pack, Magnitude, RIG, Hanjuan and Nullhole. iDefense observed this vulnerability in these kits just days after the Hacking Team breach.14 CVE-2015-5122 was the second vulnerability used by multiple exploit kits, including Angler, Neutrino, Nuclear Pack, RIG, Magnitude and Nullhole. Additionally, although not linked to any kits, CVE-2015-5123 has publicly available exploit code that is both accessible and user-friendly.

The release of proofs of concept (PoCs) for these Adobe Flash vulnerabilities made it easy for malicious actors to create these exploit kits and malicious code, leading to active and consistent exploitation. Because of the severity of the problem, many vendors that use Adobe Flash as a plug-in were forced to temporarily block it to prevent customers from being seriously affected by the exploits.

---

Proliferation of Exploit Kits

During late 2014 and into 2015, there was an overall increase in the use of exploit kits. One of the major factors that influenced this increase was the shift from Java to Adobe Flash vulnerabilities. The summary of exploit kits for 2015 in Figure 4 includes older exploit kits, such as Angler, RIG, Nuclear, Fiesta, Sweet Orange and Magnitude, but also the revamped Neutrino exploit kit, the seldom-seen Hanjuan and Nullhole exploit kits, and newcomers Hunter, Spartan and Sundown. iDefense considers Angler, Nuclear, Neutrino, RIG and Magnitude to be the most notable exploit kits for 2015.

However, while the number of exploit kits increased, older exploit kits seemed to vanish. iDefense believes one factor was the October 2013 arrest of Paunch, the developer of the Blackhole and Cool exploit kits, whose arrest slowed the deployment of older exploit kits and the development and deployment of new kits. To keep a low profile, developers behind the various exploit kits stopped selling or renting exploit kits to buyers.

Buyers, on the other hand, seemed less impressed with the remaining exploit kits available because of low exploitation rates and therefore scaled back their exploit kit purchases. In addition, the available exploit kits were using older, patched Java vulnerabilities. During this time, a number of exploit kits completely disappeared for good or for a considerable period of time, including the Whitehole and Sweet Orange exploit kits in October 2013 and the Neutrino exploit kit in early 2014.

<table>
<thead>
<tr>
<th>Exploit Kit</th>
<th>Active?</th>
<th>Prevalence</th>
<th>2015 Adoption</th>
<th>New in 2015?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angler</td>
<td>Yes</td>
<td>High</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Fiesta</td>
<td>No</td>
<td>N/A</td>
<td>Medium</td>
<td>No</td>
</tr>
<tr>
<td>Hanjuan</td>
<td>Probably</td>
<td>Low</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Hunter</td>
<td>Probably</td>
<td>Low</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Magnitude</td>
<td>Yes</td>
<td>Low</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Neutrino</td>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Nuclear</td>
<td>Yes</td>
<td>High</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Nullhole</td>
<td>Probably</td>
<td>Low</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>RIG</td>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
<td>No</td>
</tr>
<tr>
<td>Spartan</td>
<td>Probably</td>
<td>Low</td>
<td>Unknown</td>
<td>Yes</td>
</tr>
<tr>
<td>Sundown</td>
<td>Yes</td>
<td>Low</td>
<td>Low</td>
<td>Yes</td>
</tr>
<tr>
<td>Sweet Orange</td>
<td>No</td>
<td>N/A</td>
<td>Medium</td>
<td>No</td>
</tr>
</tbody>
</table>

Figure 4: 2015 Status of Exploit Kits

Hacking Team Hacked; Zero-Days Leaked

In 2015, the network security of various companies was compromised by certain hacker groups or individuals and resulted in the disclosure of company information and intellectual property. Particularly, in early July 2015, an unknown actor compromised Hacking Team, a company that produces and sells surveillance software to governments and nation states. Some sources believe that an actor with the alias of Phineas Fisher could be the one responsible for the attack. This actor is also believed to be responsible for the Gamma Group International network compromise in August 2014. Similar to Hacking Team, Gamma Group International, also identified as Gamma FinFisher Inc., produces surveillance and monitoring software called FinSpy. Gamma Group International reportedly had as much as 40 GB of data stolen while Hacking Team had as much as 400 GB of data stolen and promptly uploaded to various sites for the public to download and inspect. The stolen information from Hacking Team included a list of the company’s customers, sales figures, emails and other intellectual property, which included several zero-day exploits.

iDefense currently has knowledge of seven zero-day exploits leaked from the Hacking Team breach, all subsequently patched by their respective vendors. These exploits trigger vulnerabilities in Microsoft’s Internet Explorer browser and Windows operating system, and Adobe Flash. Malicious actors included many of these exploits in their exploit kits shortly after being publicly released (see Figure 5) to attack other companies. Hacking Team offered its clients exploits that make remote code execution possible via the Internet and also provided an attacker with system-level privileges.

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2015-2425</td>
<td>Internet Explorer</td>
</tr>
<tr>
<td>CVE-2015-5122</td>
<td>Flash Player</td>
</tr>
<tr>
<td>CVE-2015-5123</td>
<td>Flash Player</td>
</tr>
<tr>
<td>CVE-2015-2426</td>
<td>Windows</td>
</tr>
<tr>
<td>CVE-2015-2387</td>
<td>Windows</td>
</tr>
<tr>
<td>CVE-2015-5119</td>
<td>Flash Player</td>
</tr>
<tr>
<td>CVE-2015-2433</td>
<td>Windows</td>
</tr>
</tbody>
</table>

Figure 5: Hacking Team Exploits and Respective Products


19 ibid
Conclusion: Vulnerabilities

Given the number of vulnerabilities, many vendors are considering whether or not to stay with Adobe Flash or make HTML5 the standard for all media in 2016. Some already decided to pull the plug on Adobe Flash believing their decision will protect consumers and reassure them of the importance placed on information security.20

It is likely that Adobe Flash will continue to be a major delivery mechanism used by exploit kits. iDefense believes most active exploit kits will leverage new Adobe Flash vulnerabilities quickly after PoC code is made publicly available or after Adobe has released a patch for vulnerabilities that could lead to memory corruption or remote code execution. It is also likely that actors will use other delivery mechanisms including browser-specific exploits in the coming year.

**HACKTIVISM**

**Ideological Hacktivism in International Decline**

Likely as a result of successful coordinated efforts by global law enforcement, iDefense has observed that international ideological hacktivism transitioned from organized attacks by coordinated groups to fragmented attacks by amorphous cells. This change led to a notable decrease in international cyber-attack operations in 2015. At present, there appears to be a lack of binding and overarching ideology to concentrate hacktivist efforts, accompanied by a lack of willingness to participate in a movement that has been steadily losing its “trendy” factor. Hacktivist groups continue to be decentralized and focused on regional or national issues, with those groups of actors carrying out scripted attacks as a form of concentrated social protest.

North American campaign efforts largely addressed race-related issues and alleged police brutality, with hacktivists conducting DDoS attacks, information leaks and “d0xes” against municipal government and law enforcement domains for OpBaltimore. iDefense has observed Central and South American actors concentrating their operations on local political corruption, with defacements and DDoS attempts against local Venezuelan, Guatemalan and Mexican government domains and political parties. European actors were unexpectedly subdued, with little sentiment roused towards the European debt crisis or the ongoing European refugee/migrant issues.

With the exception of relatively small-scale pro-animal-rights campaigning, combined global hacktivist operations were limited in 2015. iDefense believes this trend has the potential to be partially reversed in 2016 if international factions pool their energies behind one or two particularly egregious or controversial developments.

---


Increase in Hacktivist OPSEC

In 2015, iDefense observed increased operational security (OPSEC) implemented by hacktivist actors and groups who heightened privacy in their communications and campaign planning. There was a significant move away from Internet Relay Chat (IRC) communications platforms to invite-only chat channels and forums, with actors blocking suspicious participants who failed to contribute to discussions. The availability and use of encrypted communication also filtered down into the hacktivist community, which became increasingly aware and suspicious of infiltration and monitoring following successful law enforcement operations.

Campaign organizers are also opting not to publicize campaign TTPs and targets on the open Web, presenting challenges to the security community. However, a positive benefit from the lack of publicity is that it also hinders the spread of and participation in hacktivist operations, resulting in smaller-scale campaigns carried out by limited numbers of trusted individuals. Although these smaller operations may not comprehensively target high-profile organizations, they are causing damage to low-level targets and doing so with relative anonymity and success.

Shift to Criminal and Notoriety Hacktivism

iDefense believes that young hackers have been dissuaded from entering into hacktivism following notable law enforcement successes in 2015, diminishing international hacktivist campaigns and the dwindling credibility of associating with hacktivism. As such, actors appear to be concentrating their energies and skills towards cybercriminality, which provides ample financial incentive.

iDefense also witnessed the expansion of the DDoS-for-hire, or “booster” market, as individuals with access to sizeable botnets are opting to rent out so-called “stressers” to the hacking community instead of utilizing the tool for personal use – as was the tendency in the past. Actors are similarly using their capabilities to access premium account credentials, which they sell on criminal forums both in the darknet and clearnet.

Separately, there was an increase in malicious notoriety hacking, with young actors seeking to emulate the perceived successes of Lizard Squad, who garnered international media attention in 2014 with its high-profile targeting. Notoriety hackers attack for entertainment and infamy, choosing high-profile organizations in headline-grabbing efforts that serve no higher purpose than self-aggrandizement.

---


In addition, collectives such as TeamBudyBear\(^{25}\) and OurMine\(^{26}\) conducted malicious attacks—most frequently DDoS-based—against a range of targets, often belonging to the online gaming industry, but also encompassing financial institutions, government organizations and other industries. Often, the claims made by these groups were made to draw attention to themselves; however, the success ratio of domain or server outages—particularly within the gaming industry—rose in 2015, a trend likely related to the ease and affordability associated with renting high-powered DDoS stressers.

iDefense predicts that malicious activity for the sake of notoriety will likely continue, if not increase, as the availability and accessibility of high-powered booters continues to multiply alongside the social media frenzy surrounding these notoriety-seeking actors.

**Increasing Size, Complexity of DDoS Attacks**

In 2015, Verisign observed a continued upward trend in the size, frequency and complexity of DDoS attacks against its customer base, including rising average attack sizes and increased targeting of IT Services organizations. In addition, Verisign observed increasing availability of DDoS-as-a-service offerings from hacktivist and cybercriminal groups, and the prevalence of DDoS malware targeting the open-source Linux operating system.

For the **first three quarters of 2015**, Verisign noted a marked and steady increase in average attack sizes against its DDoS Protection Services customer base (see Figure 6). The total increase across these three quarters nearly doubled, from 3.64 Gbps in the first quarter to more than 7 Gbps at the end of Q3. Verisign expects this trend to continue into 2016.

While the increase in average attack size was observed across the entire protected customer base, IT Services customers in particular experienced steadily increasing attack frequency over the course of 2015 (see Figure 7). Verisign believes this trend is an indication that, while IT Services companies may have made DDoS protection a larger priority in 2015, this industry still represents a preferred target for attackers. This may be because these organizations tend to be more Web-reliant than others, and because their products and services run other targets’ supply chains, online services and Web presences.

In addition to these quantitative trends, iDefense observed a number of behavioral trends in the DDoS space.

---


\(^{26}\) Ibid
The increasing availability of DDoS-for-hire services – also known as “booters” – presents a huge risk for security professionals, as they enable virtually anyone to hire skilled cybercriminals to launch a targeted DDoS attack. DDoS-for-hire capabilities advanced in both success and popularity in 2015, and surprisingly, can be employed today for a staggeringly marginal fee; many can be hired for just $5 USD an hour— and some as low as $2 USD an hour, according to Verisign research. Additionally, massive and longstanding attacks can be deployed for as little as $800 USD for an entire month.

iDefense observed that the malware of choice for hacking groups looking to attack Linux in 2015 was Ballpit, a Linux client-server-based botnet believed to power Lizard Squad’s denial of service (DoS) tool, LizardStresser.su. iDefense also published intelligence in late 2015 on the infrastructure of a Ballpit variant that now also includes a Microsoft Windows payload. The infrastructure spans at least six C&C server IP addresses, all of which iDefense believes are managed by the same actors.

**Conclusion: Hacktivism**

iDefense anticipates that hacktivism may experience a relative rejuvenation of collaborative hacktivist campaigning, following, comparatively speaking, a very quiet year in 2015. Global events, such as the Brazil Olympics and the French UEFA European Championship, may serve as a catalyst for hacktivist operations, as international sporting events have resulted in fruitful campaign activity in the past.

Global financial stability concerns may separately increase hacktivist campaigning, should social circumstances deteriorate as a result. Other 2015 geopolitical trends included escalation of international military participation in the ongoing conflicts in the Middle East, alongside developments of racial tensions and migration crises in North America and Europe. Should hacktivists manage to pull together to capitalize on international sentiments against grievances, coupled with strong leadership, operational planning and comprehensive tactical targeting, iDefense anticipates that there may be a relative increase in activity during the remainder of 2016 and into the next year.

Future attacks are likely to continue to capitalize on the availability and affordability of DDoS-for-hire services, allowing actors to carry out a high frequency of DDoS attacks against low-to-medium-level targets, such as regional government departments, academic institutions or local law enforcement websites. Information disclosures are also likely to be popular, as novice actors continue to utilize scanning and penetration-testing tools widely available within the community and publish personal information details to popular paste-sharing sites.

---

The cat-and-mouse game of cybersecurity means that new trends emerge almost daily, requiring at-risk organizations in all industries to stay ahead of these new and evolving risks to revenue and reputation.

CONCLUSION

Each year, enterprises around the globe dedicate increasing levels of time, budget and labor in identifying, preventing and mitigating online threats. The cat-and-mouse game of cybersecurity means that new trends emerge almost daily, requiring at-risk organizations in all industries to stay ahead of these new and evolving risks to revenue and reputation.

Throughout 2015, iDefense observed cybercriminals migrating to the darknet, the rise of ransomware-as-a-service, an increase in the operational security of hacktivist operations and notable trends in DDoS attacks against a widening field of victims across all industries. Critical vulnerabilities in prominent software applications have enabled malicious actors to increase their exploitation activities and level of impact in 2015, likely setting the stage for a new wave of breaches to make headlines in 2016.

LEARN MORE

To learn more about how Verisign iDefense Security Intelligence Services can help keep you ahead of cyberthreats and vulnerabilities, please visit Verisign.com/iDefense.

ABOUT VERISIGN

Verisign, a global leader in domain names and Internet security, enables Internet navigation for many of the world’s most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key Internet infrastructure and services, including the .com and .net domains and two of the Internet’s root servers, as well as performs the root-zone maintainer functions for the core of the Internet’s Domain Name System (DNS). Verisign’s Security Services include intelligence-driven Distributed Denial of Service Protection, iDefense Security Intelligence and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit Verisign.com.