PICK YOUR POISON:
The Most Popular Cyber-Attacks of 2016

Necessity is the mother of invention. That certainly holds true in the world of cyber security. As security experts deploy new defenses, hackers develop new attack vectors to counter the countermeasures. The result is a plethora of attack types that, depending on industry trends, rise and fall in popularity. Based on Radware's *2016 – 2017 Global Application & Network Security Report*, this piece outlines the cyber-attacks that proved popular in 2016, and thus sheds light on what to expect in 2017.

Application vs. Network Attacks

At first glance, the 2016 research indicates a balance between application and network attacks. This contradicts last year's survey, which showed a significant increase in network-based attacks. This is based on what respondents pointed at the different attacks their organization experienced in 2016, with

	Experienced	Caused the Most Damage
(NET) Network	64%	46%
TCP-SYN Flood	40%	26%
UDP	33%	11%
ICMP	32%	9%
TCP-Other	29%	10%
IPv6	16%	6%
(NET) Application	63%	58%
(Subnet) Web	50%	35%
HTTP	42%	24%
HTTPS	36%	19%
DNS	37%	19%
SMTP	31%	14%
VoIP	9%	4%
IPv4	44%	16%
Other	3%	3%
None	20%	NA

Figure 1: Type of attack vector experienced in 2016 and which caused the most damage

about two-thirds reporting having faced either network- or application-based attacks. Further analysis finds that while network and application attacks occur at a similar frequency, application-based attacks cause a larger impact - particularly web attacks followed by TCP-SYN floods.

Hackers now launch multi-vector, blended campaigns that include higher-volume network vectors alongside more sophisticated application vectors. Thus, while the top attack types reported by respondents are more likely to be network-based attacks, the threat of application attacks is very real.

Top Trends within Vertical	TELECOM	PRO SVCS	TECH	FINANCE	EDU	GOV'T	RETAIL	HEALTH
Most Harmful Attack Types	Application: 65% Network: 63%	Network: 61%	Application: 61%	Network: 61%	Application: 54%	Application: 66%	Application: 50% Network: 50%	Application: 57% Network: 50%

Figure 2: Impact of attack vectors by business sectors

Frequency of Attacks

This year, Radware also explored attack frequency. More than one-quarter of respondents reported daily and weekly attacks in the past 12 months. Affecting just 9% of organizations, attacks over VoIP were the most infrequent; even so, the incidence of attacks over VoIP tripled from 2015 to 2016.

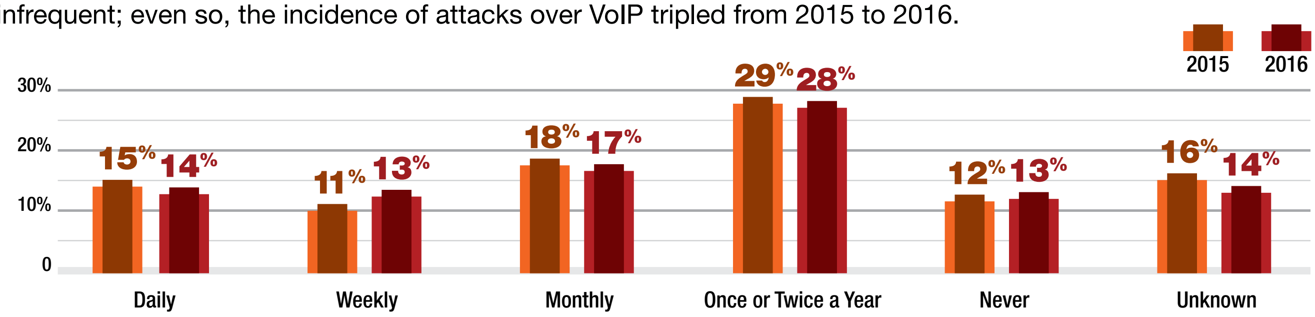


Figure 3: How often have you experienced cyber-attacks in the past 12 months?

More than one-quarter of respondents reported daily and weekly attacks via TCP-SYN flood, TCP-Other, ICMP and UDP-flood attacks in the past year. The most infrequent attack was on IPv6 networks, although daily/weekly attacks in 2016 was higher than 2015.

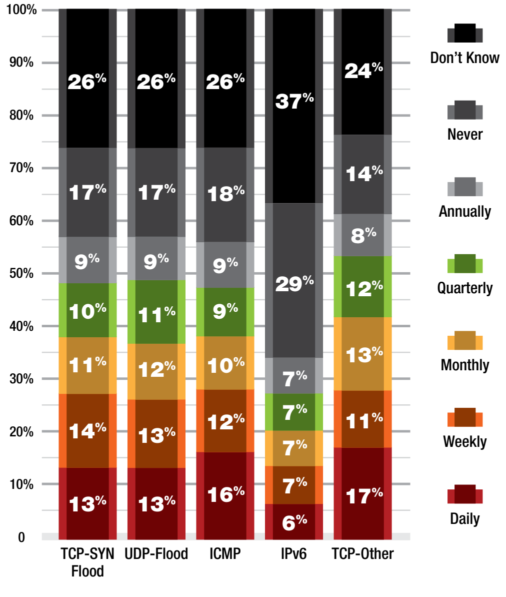


Figure 4: How often have you experienced the following network attacks in the last year?

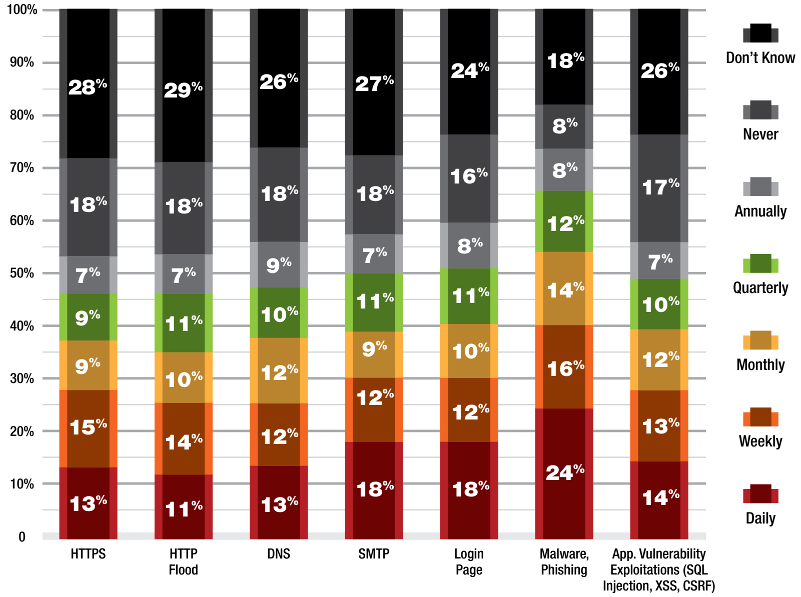


Figure 5: How often have you experienced the following application attacks in the last year?

The application with the highest attack frequency is malware and phishing, with two in five participants experiencing it on a daily/weekly basis. This rate is consistent with our findings in 2015. About a quarter of respondents experienced other application attacks daily or weekly.

About half of all respondents indicated that they did not experience any reflected amplification attacks this year. Roughly 30% said they had suffered from a reflected amplification attack but were able to mitigate the attacks. In 2016, Radware's Emergency Response Team (ERT) observed DNS attacks mainly targeting A and AAAA records. In addition to DNS, the ERT also observed 256,925 NTP monlist floods.

Multi-Vector Attacks

Hackers continue to move away from single vector attacks as advanced persistent DDoS campaigns become the norm. Attackers are still using burst attacks in an attempt to defeat mitigation processes. In 2016, Radware witnessed the rise of massive 1Tbps botnets using TCP attack vectors versus amplified and reflected vectors. In addition, attackers are exploring new techniques, such as GRE encapsulation, in hopes of bypassing ACL limitations.

Ransom-based attacks were also a top attack vector; two in five experienced a ransomware attack in the past year. Of those surveyed, 39% reported being affected by ransomware while 17% received a ransom not as part of a RDoS campaign.

Thirty-nine percent of organizations report having experienced an SSL- or TLS-based attack. This represents continuous growth of 10% year-over-year, with 35% reporting the same in 2015.

Network Attacks Prevalence

TCP-SYN Flood	UDP	ICM	TCP (Other)	IPv6 1
40%	**33%**	**32%**	**31%**	**6%**

In 2016, 64% of organizations experienced attacks on their network infrastructure. Of those that experienced a network-based attack, 40% of them experienced a TCP-SYN flood, followed by UDP (33%) and TCP-Other (29%). Thirty-two percent of respondents experienced a ICMP attack and 16% experienced an IPv6 attack.

	TELECOM	PRO SVCS	TECH	FINANCE	EDU	GOV'T	RETAIL	HEALTH*
MOST FREQUENT NETWORK ATTACK TYPES (Daily)	TCP-Other: 21% UDP Flood: 19% TCP-SYN Fl: 18% ICMP: 17%	TCP-Other: 13% ICMP: 12%	ICMP: 12% TCP-Other: 11% TCP-SYN Fl: 9%	ICMP: 19% TCP-Other: 19% UDP Flood: 19% TCP-SYN Fl: 18%	TCP-Other: 13% ICMP: 13%	TCP-Other: 34% ICMP: 32% TCP-SYN Fl: 29% UDP Flood: 24%	TCP-SYN Fl: 11% ICMP: 11% TCP-Other: 11%	UDP Flood: 18%
MOST FREQUENT NETWORK ATTACK VECTORS	TCP-SYN Fl: 53% UDP: 48%	IPv4: 43% TCP-SYN Fl: 38%	IPv4: 41% TCP-SYN Fl: 40%	IPv4: 51%	IPv4: 46%	IPv4: 51% TCP-SYN Fl: 46%	TCP-SYN Fl: 32% IPv4: 27%	Ipv4: 53%

Figure 6: Most frequent network attack types

Application

Sixty-three percent of respondents experienced application-based attacks during the year. Forty-two percent indicated that they experienced an HTTP flood; 36% experienced an HTTPS flood.

	TELECOM	PRO SVCS	TECH	FINANCE	EDU	GOV'T	RETAIL	HEALTH*
MOST FREQUENT APPLICATION ATTACK TYPES (Daily)	MalPhshRns: 24% SMTP: 22% Login Page: 20%	MalPhshRns: 21% SMTP: 16% Login Page: 16%	MalPhshRns: 14% Login Page: 13% App Exploit: 12%	MalPhshRns: 26% SMTP: 24%	MalPhshRns: 33% Login Page: 17% SMTP: 17%	MalPhshRns: 32% SMTP: 27% Login Page: 27%	MalPhshRns: 30% Login Page: 19% SMTP: 19%	Login Page: 18% SMTP: 18%
MOST FREQUENT APPLICATION ATTACK VECTORS	Web: 55% DNS: 46%	Web: 44% DNS: 33%	Web: 58% DNS: 46%	Web: 55% DNS: 35% SMTP: 32%	Web: 50% SMTP: 39%	Web: 61% DNS: 49% SMTP: 44%	SMTP: 32% Web: 30%	Web: 41% DNS: 41%

Figure 7: Most frequent application attack types

New Attack Tools

This year we have seen several tools released in association with Anonymous campaigns. These tools are often released in closed networks for members of a specific operation to use during the campaign. In some cases, they may be released publicly as free-to-use tools—a ploy to generate more support for the operation. These tools are simple denial-of-service scripts or pre-packaged scripts in simple graphical user interfaces (GUIs). Attackers have also been observed using these script tools in cloud environments in an attempt to generate larger attacks from trusted sources.

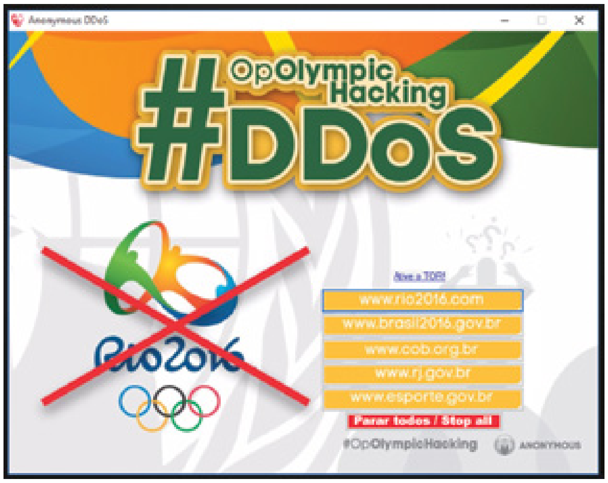


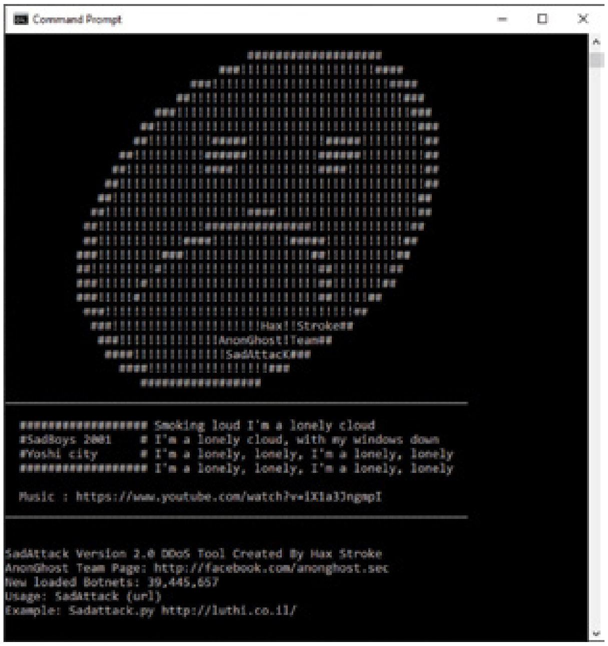
Figure 8: Anonymous DDoS tool for the Olympics

GUI - Anonymous DDoS (DDoS.exe)

Anonymous released a custom GUI tool for the 2016 Summer Olympics in Rio. This tool is capable of launching a TCP PSH+ACK flood through Tor. A PSH+ACK flood sends a TCP packet with the PUSH and ACK bits set to one. This method triggers the victim's system into unloading all data in the TCP buffer and sends an acknowledgement when completed. In addition to the tool, the group also published instructions on how to use the tool on Facebook.

Scripts - SadAttack and Saphyra

SadAttack and Saphyra are both HULK—that is, HTTP Unbearable Load King variants. Both tools obfuscate the source client by changing the user agent and referrer for every request. Ghost Squad hackers have loaded both scripts with additional user agents and referrers pointing to a number of prelisted websites. Hackers also have been seen modifying these scripts by adding user agents and referrers points. By randomly changing the user agent and referrer—and using Keep-Alive to maintain the connection—an attack can easily bypass caching methods and hit the server directly with these tools.

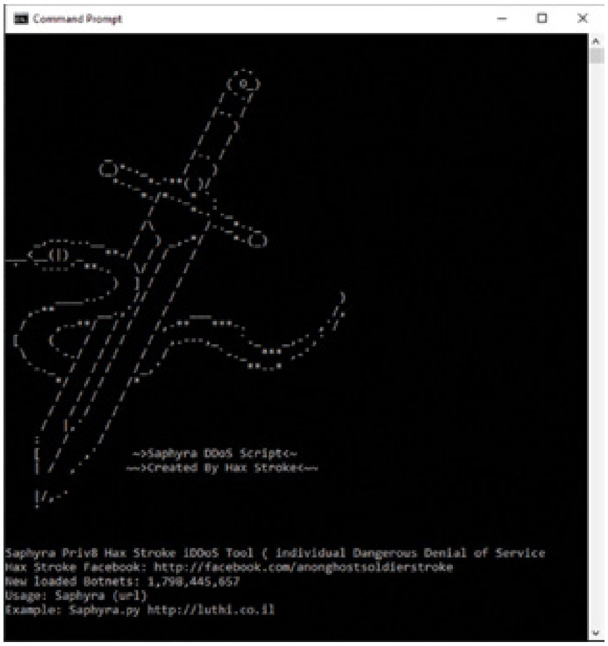


```
####################### Smoking loud I'm a lonely cloud
#SadBoys 2001     # I'm a lonely cloud, with my windows down
#Yoshi city       # I'm a lonely, lonely, I'm a lonely, lonely
####################### I'm a lonely, lonely, I'm a lonely, lonely

Music : https://www.youtube.com/watch?v=1X1a3JngmpI

SadAttack Version 2.0 DDoS Tool Created By Hax Stroke
AnonGhost Team Page: http://facebook.com/anonghost.sec
New loaded Botnets: 39,445,657
Usage: SadAttack (url)
Example: Sadattack.py http://luthi.co.il/
```

Figure 9: SadAttack.py

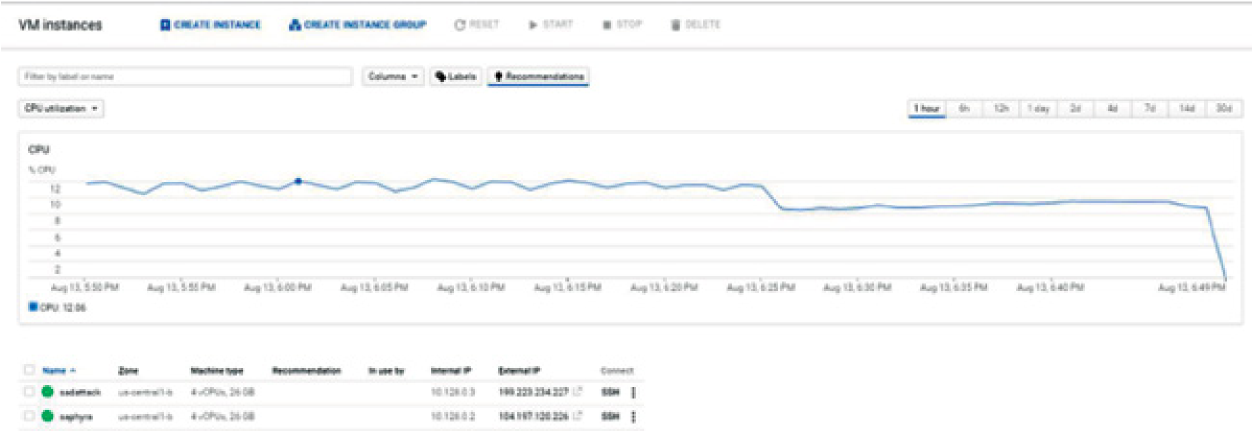
Cloud - Attacks from VPS's

In 2016, Radware has witnessed a number of hackers using cloud services to launch denial-of-service attacks. Hackers are using cloud platforms to load attack scripts and launch their assaults. One of the reasons attackers are using these services is because most organizations leverage cloud infrastructure for mission-critical business operations. That makes it very difficult to block communications with cloud services. In just an hour, an attacker can not only setup their tools on a VPS, but also access their toolset from mobile devices via SSH. Attack clouds provide hackers with more bandwidth and computing power, allowing them to easily scale their operation and attacks far beyond their home lab capabilities. The cost to conduct these attacks is much cheaper when conducting large-volume attacks versus renting a stresser service. Hackers were identified using Google Cloud Services to conduct attacks leveraging SadAttack and Saphyra. One hacker eventually shared a screenshot of how he leveraged a cloud instance to conduct several attacks for a number of operations, including OpIcarus, an Anonymous operation targeting the financial sector.



```
        ~>Saphyra DDoS Script<~
      ~~>Created By Hax Stroke<~~

Saphyra Priv8 Hax Stroke iDDoS Tool ( individual Dangerous Denial of Service
Hax Stroke Facebook: http://facebook.com/anonghostsoldierstroke
New loaded Botnets: 1,798,445,657
Usage: Saphyra (url)
Example: Saphyra.py http://luthi.co.il
```

Figure 10: Saphyra.py



□	Name	Zone	Machine type	Recommendation	In use by	Internal IP	External IP	Connect
□	● sadattack	us-central1-b	4 vCPUs, 26 GB			10.128.0.3	199.223.234.227	SSH
□	● saphyra	us-central1-b	4 vCPUs, 26 GB			10.128.0.2	104.197.120.226	SSH

Figure 11: Attacker using Google Cloud in combination with SadAttack and Saphyra

Attack Size: Does It Matter?

In 2016, fewer than one in 10 server attacks qualified as extra-large (10Gbps or higher). Seven in 10 of the biggest server attacks were below 100Mbps, and 50% were 10Mbps or less. The number of attacks that were 100Mbps or less was stable, while there was an increase in attacks 10Mbps or less and fewer attacks 10Mbps to 100Mbps. Those ranging from 10Gbps to 50Gbps decreased from 8% in 2015 to 3% in 2016.

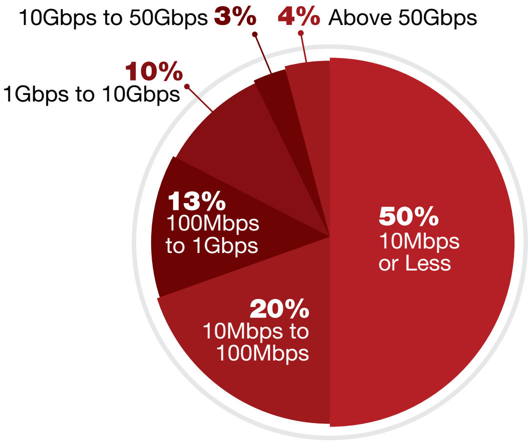


Figure 12: What are the three biggest cyber-attacks you have suffered by bandwidth?

> Despite the record-breaking volumes we've seen in 2016, non-volumetric DDoS is still prevalent. This denial-of-service technique is still proven to be very efficient in exhausting network and server resources. Moreover, a non-volumetric attack can evade detection mechanisms and consume bandwidth and resources without the target knowing—affecting service-level quality.

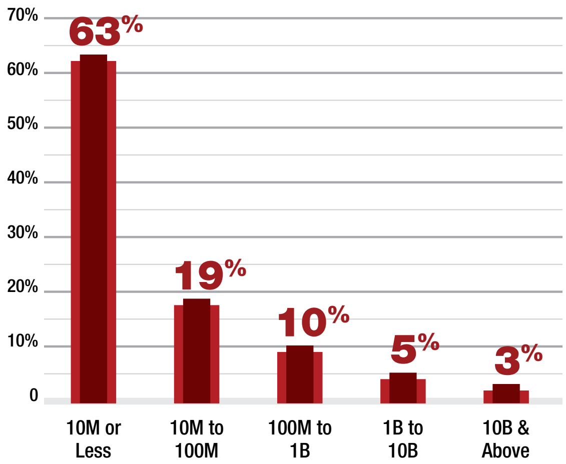


Figure 13: What are the three biggest cyber-attacks you have suffered by PPS?

Three in five respondents report a cyber-attack that is 10 million packets-per-second (PPS) or less, and about one fifth indicated they suffered an attack between 10 million PPS and 100 million PPS. The number of attacks that were 100 million PPS or less increased from 76% in 2015 to 82% in 2016. Those with 10 million PPS or less were up, too—increasing from 50% in 2015 to 63% in 2016.

> Combining firewall, IPS and load balancers, we learn that stateful devices fail when at least 36% of attacks hit. They simply cannot handle all kinds of cyber-attacks, and a dedicated attack mitigation solution is required to maintain availability at all times.

Download the 2016-2017 Global Application & Network Security Report to learn more.

www.radware.com/ert-report-2016

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.