Nimitz News Publications

#2

Title: Q1-2019 Summary

Author: Nimitz
Published: 2019-07-31
Updated: N/A

2018 Summary

The distributed denial of service (DDoS) industry of 2018 was an eventful one. The first quarter saw the dawn of the Terabit Era. When the software development platform Github was targeted with a 1.35Tbps, 126.9 million packets per second (pps) attack on February 28th , only to be surpassed 5 days later by a 1.7Tbps attack against an undisclosed client of a U.S based service provider, verified via NETSCOUT Arbor. Both attacks exploited the memcache protocol over UDP, which is capable of generating a peak bandwidth amplification factor (BAF) of x51 000. As of this writing, these are considered to be the largest attacks to have been publicly disclosed when quantified in terms of bandwidth (bps).

Additional information can be found here:				
Memcache	Akamai	CloudFlare	KnownHost	Netscout

Following these events, 2018 saw a steady attenuation in DDoS attack frequencies. As evidenced by Kaspersky Labs, whos analysts had reported an average drop of 13% relative to the same times in the year prior. With a peak frequency drop off of 30% occuring in Q4, 2018.

One might speculate that this steady decline was in some part due to law enforcment agencies across the globe cracking down on booter/stressor for hire services in a major way as part of "Operation Power OFF". A multi-organizational effort coordinated by both Europol and the Joint – Cybercrime Task Force (J-CAT) in combination with several other European law enforcment agencies. Whos combined efforts oversaw the April 18th takedown of webstressor.org. At the time it was "believed to have been the world's [largest] marketplace to hire DDoS services, having helped launched over 4 million attacks for as little as €15.00 [($22.00 CAN)] a month"– Europol. This also led to the sites seizure and acquisition of data, regarding its ~150 000 registered users. For whom officers residing within the United Kingdom have taken initiative in confiscating electronic devices and laying the foundations for the prosecution of over 250 suspects, as an extension of "Operation Power OFF". In addition to this, the U.S. Department of Justice released a document on December 20th , 2018 stating that they had seized "15 internet domains associated with DDoS-for-hire services".

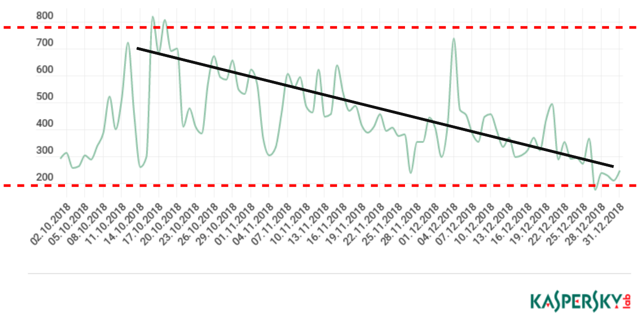
Including:				
Sites:	`critical-boot.com`	`downthem.org`	`quantumstress.net`	`ragebooter.com`

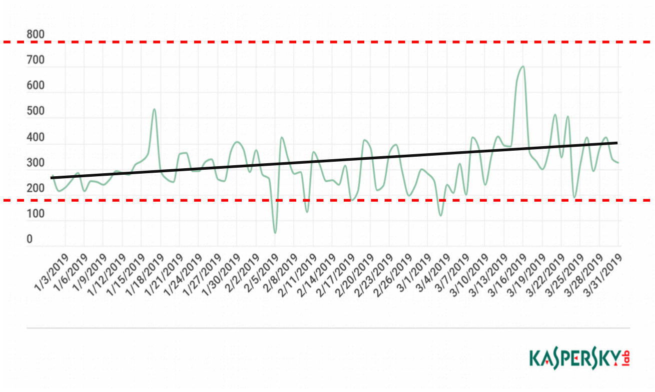
As part of an FBI investigation lead by their Anchorage field office and Cyber Initiative and Resource Fusion Unit (CIRFU). These events may have led to a market shortage in booter/stressor services that required some time to recover, heading into 2019.

Additional information can be found here:			
DDoS For Hire	Cloudflare	Imperva	Radware | Radware

2019 Q1

Distributed denial of service attacks have been on the rebound early in 2019, as DDoS for hire-services more than double: According to Nexusguard’s 2019 threat report.





Q4-2018 *Q1-2019*

--Duration

On May 21, Kaspersky Labs published their 2019 Q1 threat report. Data provided within the report suggests that one of the trends to lookout for in 2019 is the continued increase in average duration of DDoS attacks. Their data shows that the average duration of attacks lasting over 5 hours increased by 4.68%, up from 16.66% to 21.34%.

Duration:	<5hrs	5-9hrs	10-19hrs	20-49hrs	50-99hrs	100-139hrs	>140hrs
Kaspersky	Total: 78.66% ↓4.68%	Total: 10.13% ↑0.73%	Total: 10.13% ↑2.06%	Total: 0.38% ↑1.32%	Total: 1.51% ↑0.50%	Total: 0.11% ↓0.03%	Total: 0.21% ↑0.10%

--Taxonomy

In addition to this, Syn-Floods have made a significant leap in terms of total DDoS volume composition, moving from 58.20% to 84.10% of total attacks. This is concerning, largly due to the fact that Syn-Floods are one of the more resource intensive attack vectors. With {Syn,Ack} floods sitting in top spot. Especially in todays high bandwidth networks, where bits per second (bps) no longer serve as an accurate threat measure when under denial of service. Currently the most accurate metric of an attacks severity is its packets per second (pps) in combination with its protocol stack. As these will dictate the degree of resource exhaustion occuring at targeted points and hence, damage.

Taxonomy:	Syn	UDP	HTTP	TCP	ICMP
Kaspersky	Total: 84.10% ↑25.90%	Total: 8.90% ↓22.20%	Total: 3.30% ↓1.10%	Total: 3.10% ↓5.30%	Total: 0.06% ↑0.50%

Interestingly Link11, a European based IT security company released a Q1 threat report on May 2 of this year stating that their primary attack sources were UDP based. With DNS (Domain Name

System) leading CLDAP (Connectionless Lightweight Directory Protocol). Suggesting that geography might play a role in attack vectors of choice.

Additional information can be found here:				
DNS	Bind9	CloudFlare	US-Cert	Wiki
CLDAP	Akamai	RFC-1798	RFC-3352	Wiki

Link11 also reported that of their total attacks experienced within Q1 of this year, 46% were multi-vector (54% single vector). From these 46% the majority utilized either 2-vectors (40.00%) or 3-vectors (39.10%). This is substantially less than that Reported in Neustars Q1, 2019 report. Which analyzed approximately ~77% of their attacks as multi-vector. In either case this mostly likely indicates increased sophistication from attackers, who are now exploiting targets through various stages of a connection (e.g. bandwidth, middleboxes, endpoints). In order to increase their effectiveness and avoid detection.

Vectors:	1	2	3	4	5	6
Link11	N/A 54.00%	40.00% 18.40%	39.10% 17.99%	16.50% 7.59%	3.50% 1.61%	0.80% 0.37%
Neustar	21.00%	26.00%	44.00%	7.00%	*Remaining 2% Unspecified	

--Dynamics

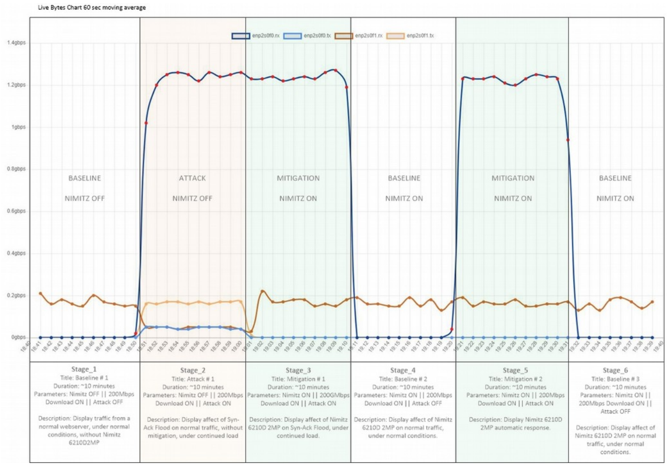
Not surprisingly, data provided by Kaspersky showed that the most active attack day of the week was Saturday (16.65%). With the least busy being Sunday (11.41%). This is close to the same reported by Link11 who saw Fridays as their peak day (17.00%) and Mondays as their lowest day at 12.00%.

Days:	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Kaspersky	11.41% ↓0.61%	12.61% ↓1.58	13.92% ↓0.84%	14.83% ↑0.54%	15.18% ↓0.56%	15.39% ↓0.01%	16.65% ↑3.06%
Link11	--	12.00%	--	--	--	17.00%	--

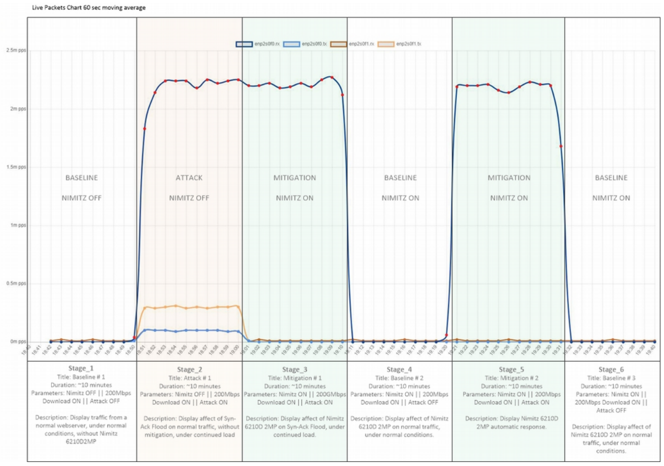
--Closing Statements

As distributed denial of service attacks continue to increase in frequency and duration. And as malicious agents become more sophisticated in their implementation of those attacks through the utilization of multiple vectors. The ability to mitigate attacks efficiently at the moment of occurence will slowly disappear. This will force service providers and business owners to increase spending on 24/7 security experts, who will not be able to deliver guaranteed protection. Unfortunately, research done by Corero indicates that the majority of attacks that occur are less than 5Gbps (94% < 5Gbps, 81% <1Gbps). Meaning that those with less physical and financial resources will feel the greatest impact.

That is where Nimitz Ltd comes in. Our DDoS mitigation technology utilizes proprietary software that is integrated with commodity hardware to provide industrial level protection at a fraction of the cost of top leading experts. Clients are protected by hardware that runs 24/7 and responds to attacks automatically without any form of human intervention. Thus eliminating the need for full-time security staff and emergency response units, trying to detect or mitigate potential threats.



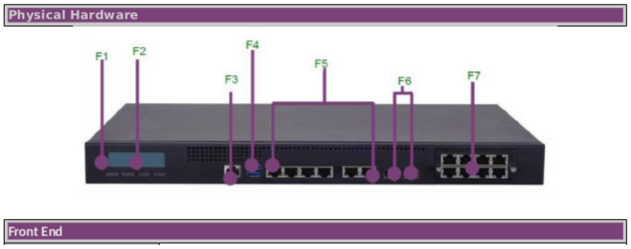
Bytes Per Second - {Syn-Ack} Flood



Packets Per Second – {Syn-Ack} Flood

*Click on images to enlarge

Backed by a novel form of signature detection, Nimitz provides clients with a guaranteed threshold of protection that is quantified in millions of packets per second (pps). With optimizations that allow for aggressive over provisioning. In order to accomodate situations in which a client may be hit with short, large bursts of traffic. Allowing them to temporarily exceed performance metrics by as much as 75%.



The end result is an on-site DDoS mitigation appliance that provides universal protection. And liberates you of 3rd party protection services that degrade your network.

Resources

[0] https://github.blog/2018-03-01-ddos-incident-report/

[1] https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era

[2] https://github.com/memcached/memcached/wiki

[3] https://www.us-cert.gov/ncas/alerts/TA14-017A

[4] https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/ddos-reflection-attack-memcached-udp.jsp

[5] https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/

[6] https://www.knownhost.com/wiki/developmental/memcrashed-what-is-it-memcache

[7] https://www.netscout.com/blog/security-17tbps-ddos-attack-makes-history

[8] https://securelist.com/ddos-attacks-in-q4-2018/89565/

[9] https://www.europol.europa.eu/newsroom/news/authorities-across-world-going-after-users-of-biggest-ddos-for-hire-website

[10] https://www.justice.gov/opa/pr/criminal-charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos

[11] https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/

[12] https://www.imperva.com/learn/application-security/booters-stressers-ddosers/

[13] https://blog.radware.com/security/2018/03/putinstresser-booter-stresser-service/

[14] https://blog.radware.com/security/2016/08/the-rise-of-booter-and-stresser-services/

[15] https://www.nexusguard.com/newsroom/press-release/ddos-for-hire-websites-make-a-comeback-despite-fbi-crackdown-according-to-nexusguard-threat-report

[16] https://www.link11.com/en/company/

[17] https://www.bind9.net/rfc

[18] https://new.blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

[19] https://www.us-cert.gov/ncas/alerts/TA13-088A

[20] https://en.wikipedia.org/wiki/Domain_Name_System

[21] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf

[22] https://tools.ietf.org/html/rfc1798

[23] https://tools.ietf.org/html/rfc3352

[24] https://ldapwiki.com/wiki/Connection-less%20Lightweight%20Directory%20Access%20Protocol

[25] https://www.corero.com/resources/reports/h1-ddos-trends-report/

[26] https://nimitz.ca/

Disclosure: If anyone reading this article is the originator of any of the content and feels that the information/ data utilized within this article was not properly represented or cited and would like it removed or edited: please contact info@nimitz.ca.