Assignment One: Emerging Threats & Attacks

Ma'alona Mafaufau

Computing, Electrical and Applied Technology, Unitec Institute of Technology

HTCS6703: Network Security A

Christopher Lloyd

May 5, 2021

Abstract **3**

Discussion **4**

DDoS Attacks 4

DDoS Vulnerabilities 5

DDoS Security Controls 5

Phishing & Spear Phishing Attacks 6

Phishing/Spear-Phishing Vulnerabilities 7

Phishing/Spear-Phishing Security Controls 7

Analysis **8**

Github 2018 8

NZX 2020 9

Scoular Co. 2015 10

Ubiquiti 2015 11

Recommendations **13**

Github: 13

NZX: 13

Scoular Co. & Ubiquiti: 13

Conclusion **14**

References **15**

Abstract

This report examines two types of cyberattack methods often seen by the cybersecurity industry. For each attack, a discussion is provided which delves into historical and technical aspects of the attacks, as well as real-world case studies. In particular, two cyberattack methods are explored in this report: 1) attacks on the availability of customer facing resources (DDoS/DoS), and 2) attacks using the corporate email as a vector (Phishing and Email Security). Although the rising threat of said attacks is causing significant financial and reputational damage to many organizations globally, the findings of this report suggest there are persistent educational and technological cybersecurity gaps within businesses which worsen their exposure to being victims of cybercrime. Recommendations are provided to improve the security posture of the organizations identified, supported by literature from various cybersecurity vendors and authorities.

Keywords: Dos, DDoS, phishing, spear-phishing, cybersecurity

Discussion

DDoS Attacks

Distributed Denial-of-Service (DDoS) cyberattacks can have crippling effects on companies that use the Internet as its primary medium for hosting services (Corero, 2018, para. 1). Not only are these attacks becoming more complex in nature, their implementation has also evolved such that they are easier and cheaper for adversaries to carry out (Mirkovic & Reiher, 2004, para. 1; Palmer, 2020, para. 1). As it stands today, the use case of DDoS attacks has progressed to where cybercriminals can now sell attacks packaged as Software-as-a-Service with a starting point of $20 USD (Cloudflare, n.d.-b, para. 5).

At the heart of these attacks is the ability to manipulate certain Internet communication protocols. By doing so, an attacker overwhelms the services of an organization to a point where they can no longer perform their intended functions. The term that encapsulates this scenario is Denial-of-Service (DoS), as the service normally provided by a server is denied due to a stifling of its capacity to serve. What transforms a DoS attack into a formidable adversary for even the most advanced technology companies of our times is the coordinated and simultaneous orchestration of multiple compromised machines or Internet protocols to achieve DoS attack goals. As the attack is carried out by a distributed network of machines, it is aptly termed Distributed Denial-of-Service (DDoS) (Mirkovic & Reiher, 2004, Part 2).

The DDoS attack has had considerable time to mature, resulting in dramatic growth in its complexity and impact (Zhijun et al., 2020, Part 1). Consequently, methods have been developed in parallel by information security researchers in order to combat these malicious efforts (Mirkovic & Reiher, 2004, Part 1). As it is with the nature of criminal endeavors, there are varying reasons behind an adversary launching a DDoS attack or campaign, ranging from personal vendettas, to financial extortion. Subsequently, the victims of these crimes have equivalently varied backgrounds, including small business owners, large corporations, and even governments (Cloudflare, n.d.-b, para. 8; Mirkovic & Reiher, 2004, Part 2.3).

DDoS attacks are prolific. A 2020 report by NETSCOUT (2021, pp. 6-7) found that the average monthly DDoS attack rate was 839,083 - an increase of nearly 130,000 per month from the previous year. Considering the average attack was approximately 40 minutes and the average hourly downtime cost of one critical application in an enterprise is $300,000, when coupled with the attack frequency, the problem of DDoS is a costly one. As such, it has become a priority for any business that has an online presence to employ safeguards against such attacks.

DDoS Vulnerabilities

A typical vulnerability is the case where a router which may at most handle an inflow of internet traffic at say x Gbps is overwhelmed by an attacker sending y Gbps where y is much greater than x (Cloudflare, 2017, "Layer 3/4 attacks" section). This scenario is made more difficult to remedy if an organization has on-premises (on-prem) safeguards only, as it limits its ability to adapt to dramatic, sizable changes in incoming adversarial traffic (Cloudflare, 2017, p. 5).

On the other hand, cloud-only DDoS solutions may fall short in protecting against Layer 7 attacks, which often have a more obscured footprint (NETSCOUT, 2018, p. 2).

Finally, IP Spoofing is the mechanism by which criminal identities are shrouded, and vulnerabilities exist that further ensure an IP can be spoofed, such as minimal encryption and hashing procedures in TCP communications (Imperva, 2020, "SYN cookies" section), or the lack of implementation of what are known as Best Current Practices which aim to stop IP Spoofing through Source Address Validation (SAV), such as BCP38 and BCP84 (Baker & Savola, 2004; Ferguson & Senie, 2000).

DDoS Security Controls

Despite the power of DDoS attacks, there are solutions which can help effectively mitigate such events. One solution is upstream scrubbing: the process of rerouting DDoS-generated traffic to data centers which have the capacity for further processing data streams in a secured environment (Kordia, 2020, para. 10). These data centers are often situated globally and have enough resources to withstand sizable DDoS attacks, while simultaneously granting a non-malicious user access to a

desired service. Cloudflare and Imperva are examples of companies that offer such services, with Cloudflare stating that their solution “is able to prevent even a single packet of attack traffic from ever reaching a site protected by Cloudflare.” (2017, p. 2).

NetScout Arbor suggests a combination of on-prem and cloud-based solutions pay the highest dividends when considering extensive security controls. Their analysis shows Arbor APS, an on-prem solution, is effective against complex, application layer attacks while volumetric attacks are effectively handled by Arbor Cloud, their cloud solution. It is the coupling of these technologies that Arbor claims offers the most comprehensive protection against DDoS attacks. A further claim is that the loss magnitude of a company (i.e. the monetary impact of a loss event) is greatly reduced under this methodology (2018, p. 2).

A third DDoS security control requires organizations to treat cybersecurity as a first-class citizen, and not merely an afterthought, a habit still maintained by the majority of businesses (EY, 2020, p. 6). Doing the groundwork to understand the services an organization uses, as well as the risks involved in doing so, offers a proactive approach to gaining a comprehensive view of their attack surface while stepping towards reducing exposure to DDoS attacks. It is well known that certain services are commonly manipulated by adversaries to deliver DDoS attacks and are often defaulted to use certain ports (e.g. Memcached on UDP port 11211) (Lone et al., 2020, p. 7). If an organization knows they are users of such vulnerable services, the security-minded approach would be to harden the service by changing default settings, or employ rate-limiting on the corresponding ports (Vixie, 2014, "Conclusion" section), as seen offered by Cloudflare (n.d.-a).

Phishing & Spear Phishing Attacks

Phishing attacks seek to capitalize on a vulnerability which social psychologist, Roderick M. Kramer, hypothesizes humans have a natural predisposition towards - trust (Halevi et al., 2015, Part 2.5; Kramer, 2009, para. 3). Phishing abuses this trust by stealing any information an attacker can use against unsuspecting victims (CERT NZ, n.d.-a). The probability of a successful phishing campaign is further improved when skilled hackers tailor their communications in such a way that correspondence with them is near-identical to the correspondence style of entities they are impersonating. The

engineering of trust can be through convincing mannerisms, formatting of text or handwriting, and the people or events mentioned in a message (CERT NZ, n.d.-a, para. 2). This is especially true when an adversary is targeting the C-Suite, and is an attack known as spear-phishing (Halevi et al., 2015, "Abstract" section).

Phishing/Spear-Phishing Vulnerabilities

Having unpatched software opens up the risk of an attacker utilizing a security hole which could be the initial foothold that is used in a more sinister spear-phishing campaign. This could look like attacking misconfigured email services to impersonate executives, or sending outdated browser exploits as links through email which are used to siphon sensitive company data (Sari, 2020). A lack of authorization protocols has often led to great monetary loss. In only the second quarter of 2020, researchers found the average wire transfer attempt was approximately $80,000 (F5 Labs, 2020, p. 5).

Phishing/Spear-Phishing Security Controls

As any asset of an organization is a potential phishing vehicle for an attacker, it is important to ensure systems are updated and patched regularly. This guarantees the latest security fixes and features are installed which provide additional layers of protection against phishing (CERT NZ, n.d.-b, "How to protect your business against phishing attacks" section).

Robust procedures for verifying the identities of highly targeted users and authorization of large financial transactions should be established. Part of this process could include the use of multi-factor authentication which can be effective against an adversarial email account takeover (F5 Labs, 2020, p. 36) as well as educating employees on how to recognize suspicious emails, recalibrating their tendencies to trust (Hunt, 2017, "Avoiding phishing in the first place" section).

A third security control against phishing attempts is the use of modern password managers. Not only does a password manager encourage healthy password hygiene, but used in conjunction with a browser extension, serves as a visual alert to potential phishing sites. This is achieved through the autofill capability of the password extension, where if a site regularly frequented seems suspicious, and the extension refuses to autofill a password, it is likely to be dubious (F5 Labs, 2020, p. 38).

Analysis

We now analyse four real-world case studies - two DDoS attacks, and two spear-phishing attacks.

Github 2018

Github was on the receiving end of a volumetric DDoS attack in February of 2018, with peak attack traffic hitting 1.35 Tbps. The american company is believed to have been targeted as they were exposed to vulnerable default settings in a widely used database caching system called Memcached (Quist & Kaiser, 2018, paras. 1–5). These memcached servers lacked authentication protocols, making them prime targets for malicious actors, and particularly enticing as their amplification ratio is 51,000:1. Shodan could also be utilised to discover approximately 88,000 vulnerable memcached servers as of February, 2018 (Louie, 2018, para. 3). A proof-of-concept showed how a relatively short Python script could use Shodan to find exposed memcached machines, and target them towards victims in only a matter of seconds (649 et al., 2018; Trend Micro, 2018).

Despite having never encountered an attack of this scale previously, Github was able to mitigate the DDoS attack in under 10 minutes. This is credit to two security controls that were already in place which proved effective under most standards. The first control was using a Network Monitoring System (NMS) capable of quickly recognizing abnormal traffic patterns, and responding by alerting appropriate personnel to investigate further (Kottler, 2018, "The incident" section). Although a specific NMS was not explicitly mentioned, online documentation for tools such as Splunk show how UDP amplification abuse can be detected (*Detecting UDP Service Amplification Abuse*, 2021). The second control was the use of upstream scrubbing services as mentioned in the DDoS Security Controls section. Github offloaded the attack traffic to a branch of Akamai which specializes in DDoS handling, called Prolexic (Kesavan, 2018, "Prolexic in BGP Path Confirms DDoS Attack" section). As a result, the attackers withdrew their efforts shortly after and Github recovered fully (Kottler, 2018, "The incident" section).

However, there are security controls that could have been put in place that might have avoided or further dampened the Github attack. In fact, a Chinese cybersecurity research team by the name of 0kee presented work at the annual Korean POC conference in November 2017 detailing exactly how memcached servers were susceptible to DDoS amplification attacks. Their presentation also listed possible mitigation methods that would later be reiterated by numerous other security companies such as Cloudflare and CERT NZ following the events of February 2018. Some of these methods include urging upstream ISPs to enforce BCPs 38/84, as well as port rate limiting UDP port 11211, as mentioned in DDoS Security Controls (0kee Team, 2017, "Network Mitigation Measures" section). Prior to POC 2017, Ivan Novikov outlined further memcached vulnerabilities at BlackHat USA 2014 (Wallarm, 2014). As the saying goes, “Hindsight is always 20/20”, and it is not trivial to stay current on all potential vulnerabilities present in the services one uses. Nonetheless, as impressive as the Github response was to such a large attack, there were warnings voiced by the security community that could have helped keep Github one step ahead of the adversaries.

A thorough search of relevant literature yielded no indication of the identity of the perpetrators behind the attack. However, it is worth noting that Github previously withstood a 2015 attack alleged to have originated from Chinese state-sponsored actors (Anthony, 2015).

NZX 2020

In contrast to the attack on Github, August of 2020 saw New Zealand’s Stock Exchange (NZX) become the victim of a DDoS attack that ensued long enough to halt critical trading services for approximately four days (Fonseka, 2021, para. 8). The motive appeared to be financial extortion, with the attacker sending an email seeking Bitcoin payment (Puller-Strecker, 2020). Although investigators are not confident of the identity of the adversaries, state-sponsored actors have been ruled out, with the main culprit suspected to be a criminal group based out of eastern Europe. Reports show the hacker group utilized a botnet of devices originating from the likes of Russia and China (Reidy, 2020; Tarabay, 2021). Following the attacks, NZX has been used as an example in further DDoS efforts by what appears to be the same group, stating in their ransom notes that victims

perform, “a search for NZX or New Zealand Stock Exchange in the news, you don’t want to be like them, do you?” (Tarabay, 2021).

There have been many criticisms, both nationally, and abroad, regarding the minimal approach to security initiated by the NZ organization. NZX commissioned independent cybersecurity specialist, InPhySec, to review their security posture post-attack. Their assessment concluded that an attack of this nature was, “unprecedented” and that the sophistication seen in the adversary’s methodology, “fundamentally changed expectations about this sort of attack for the industry.” (NZX, 2020). These findings are in direct contradiction to a Financial Markets Authority (FMA) targeted review of NZX’s technology which stated that in fact, DDoS attacks were “foreseeable” and mitigation plans should have been made a priority well in advance (FMA - Financial Markets Authority, 2021, p. 13). US-based media company, Bloomberg, also provided some commentary where they interviewed Cloudflare CTO John Graham-Cumming regarding the incident. His opinion was that NZX was attacked with a “dated style of hack”, while also being, “the simplest, dumbest attack you can do.” (Tarabay, 2021). Although the aforementioned InPhySec report was never publicly disclosed (O’Neill, 2020), NZ-based IT security consultant Daniel Ayers believes NZX was too leveraged on a pair of ill-equipped local servers, unable to quickly adapt to the attacks that took place (Tarabay, 2021). It is inferred that NZX had no ability to reroute the bombardment of malicious traffic, as the FMA report disclosed that NZX only subsequently consulted with Akamai to discuss upstream scrubbing capability.

Scoular Co. 2015

Coverage by Hubbard (2015) details how Omaha-based commodities trader Scoular Co. lost $17.2 million after falling victim to an elaborate spear-phishing campaign. At the time, Scoular boasted $6.2 billion in annual revenue, and garnered international attention after being recognized by Forbes magazine as being in the top 60 largest private U.S. companies. A profile such as theirs makes for an attractive research target for a hacker, as large transactions are often common day-to-day operations.

Although Scoular CEO Chuck Elsea appeared to have no concerns about their apparent lack of spear-phishing security controls, stating full confidence in both internal and external communication systems, losses in the millions would suggest that it would be detrimental to continue to hold this view. No record was found of any security controls such as the ones mentioned in the Phishing/Spear-Phishing Security Controls section of this paper, and in particular, an obvious lack of authentication for large wire transfers. This result is consistent with reports detailing the email chain between the adversary and the financial controller who ultimately succumbed to the attacker's campaign, Keith McMurty. At no stage did McMurty perform any type of security check against the emails, and his interviews with the FBI revealed absolute confidence in the legitimacy of the wire transfer requests.

No threat actor has been identified in reports covering the Scoular attack, however the emails are said to have come from a Russian server, while the phone number listed in the phony emails belonged to a Skype account belonging to an Israeli IP address

Ubiquiti 2015

On June 5, 2015, Robert Pera, Billionaire Ubiquiti founder and CEO (Forbes, 2021), received an email from the FBI alerting him they believed his company had been conned into paying scammers millions (Spicer, 2021, "The Ubiquiti Scandal" section). Upon further investigation, he found Chief Accounting Officer at the time, Rohit Chakravarthy unwittingly wired $46.7 million to fraudsters over the course of 17 days. Chakravarthy had only just stepped into the role in response to the sudden resignation of Ubiquiti's CFO, Craig Foster. Foster believes Ubiquiti was likely targeted due to his leaving, suspecting the attackers capitalized on the absence of what would normally be his close watch of all financial transactions (Vardi, 2016, para. 11).

Although one account of the events states that Chakravarthy overruled "standard industry procedure", it is unclear whether standard industry procedures were specifically set at Ubiquiti (Spicer, 2021, "The Ubiquiti Scandal" section). Similar to what was seen in the Scoular case, a lack of authentication procedures for large wire transfers saw approximately 10% of Ubiquiti's cash assets removed from their accounts (Vardi, 2016, para. 3).

In a subsequent report to shareholders, Ubiquiti stated an audit committee launched an independent investigation, and found Ubiquiti lacked effective financial controls. Considering that Chakravarthy seemingly acted alone, it is assumed that some of the controls missing include robust authentication procedures, perhaps consisting of two-factor or multi-factor protocols. It is also concerning that had the FBI not already been investigating a separate case involving monitoring a bank account Ubiquiti deposited millions into, further wire transfers would have ensued. Following recommendations from the audit, Ubiquiti began taking necessary steps towards improving their security processes (SEC - Securities and Exchange Commision, 2015).

The identities of any threat actors responsible elude authorities, with only the knowledge that the accounts to which money was transferred were from Hungary, Poland, Russia, and China (Vardi, 2016, para. 4).

Recommendations

The following are recommendations that would aid in securing against the attacks seen against the four organizations identified in this report.

Github:

- As recommended by CERT NZ, the use of SAV via BCP38 and BCP84 would help in validating legitimate traffic from spoofed traffic (CERT NZ, 2018, "What to do" section).
- The 0kee Team recommend rate-limiting inbound UDP port 11211 traffic, or firewall the port completely (0kee Team, 2017, "Network Mitigation Measures" section).

NZX:

- Secure a DDoS mitigation vendor such as Akamai for upstream scrubbing capability
- As recommended by FMA, embed key security personnel, such as Head of IT Security, Head of Architecture, Chief Risk Officer, into the heart of the organization. This ensures that the infrastructure the business is built upon can robustly scale with business demands as well as ensuring cybersecurity is top priority (FMA - Financial Markets Authority, 2021, p. 15).

Scoular Co. & Ubiquiti:

- As recommended by F5 labs, both organizations should continue to educate employees to spot modern spear-phishing tactics, as well as ensuring multifactor authentication is a mandatory policy (F5 Labs, 2020, p. 36).
- Following the suggestions of Anderson Technologies, large wire transfers should be verified by a second authority, preferably in person or via phone call, or any other medium other than email (Spicer, 2021, "Preventing Your Own Ubiquiti" section).

Conclusion

Cybercriminals are becoming increasingly sophisticated in their attack methodologies, while the financial costs of them doing so declines. On the contrary, businesses across the globe are losing millions each year as they struggle to implement even the simplest cybersecurity measures to protect themselves. However, as outlined in this report, effective solutions exist to combat attacks like DDoS and phishing, but requires an overhaul in how cybersecurity is prioritized. This paradigm shift must start from the heads of organizations in order to trickle down to the rest of their employees. Failing to do so can cost an organization severe financial and reputational damage. Alongside the progression of cybercriminal research is the growth of protections against cyber attacks driven by researchers globally. Businesses who stay tapped in to this research establish themselves as international leaders who can thrive in an environment where cybercriminal activity is ever growing.

References

0kee Team. (2017, November). *How to generate 2TB/s reflection DDoS data flow via family network* [Slides]. POC. https://powerofcommunity.net/poc2017/shengbao.pdf

649, delirious-lettuce, khast3x, & DmACKGL. (2018, February 25). *649/Memcrashed-DDoS-Exploit*. GitHub. https://github.com/649/Memcrashed-DDoS-Exploit

Anthony, S. (2015, March 31). *GitHub battles "largest DDoS" in site's history, targeted at anti-censorship tools*. Ars Technica. https://arstechnica.com/information-technology/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/

Baker, F., & Savola, P. (2004, March). *BCP 84 - Ingress Filtering for Multihomed Networks*. IETF - Internet Engineering Task Force. https://tools.ietf.org/html/bcp84

CERT NZ. (n.d.-a). *Phishing*. Retrieved May 2, 2021, from https://www.cert.govt.nz/individuals/common-threats/phishing/

CERT NZ. (n.d.-b). *Phishing scams and your business*. Retrieved May 2, 2021, from https://www.cert.govt.nz/business/common-threats/phishing-scams-and-your-business/?gclid=CjwKCAjwm7mEBhBsEiwA_of-TA1sBLgpE2h5GKrmd038NKlj4knZfOgeZiIClHQwjS_N4X3T9g2_IBoCDloQAvD_BwE

CERT NZ. (2018, February 28). *Memcached reflection denial-of-service*. https://www.cert.govt.nz/it-specialists/advisories/memcache/

Cloudflare. (n.d.-a). *Rate Limiting | Advanced Network Rate Limiting*. Retrieved May 2, 2021, from https://www.cloudflare.com/en-in/rate-limiting/

Cloudflare. (n.d.-b). *What is a DDoS Booter/IP Stresser? | DDoS Attack Tools*. Retrieved May 2, 2021, from

https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/#:%7E:text=Booters%2C%20also%20known%20as%20booter,bring%20down%20websites%20and%20networks.&text=Packages%20may%20offer%20a%20one,or%20even%20%E2%80%9Clifetime%E2%80%9D%20access.

Cloudflare. (2017). *Cloudflare Advanced DDoS Protection*. https://www.cloudflare.com/media/pdf/cloudflare-whitepaper-ddos.pdf

Corero. (2018, April 23). *DDoS Attacks Can Cost Organizations $50,000 Per Attack*. Corero Network Security. https://www.corero.com/blog/ddos-attacks-can-cost-organizations-50000-per-attack/

Detecting UDP service amplification abuse. (2021, January 12). Splunk Lantern. https://lantern.splunk.com/hc/en-us/articles/360049245053-Detecting-UDP-service-amplification-abuse

EY. (2020). *How does security evolve from bolted on to built-in?* (No. 22). https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf

F5 Labs. (2020). *2020 Phishing and Fraud Report*. https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf

Ferguson, P., & Senie, D. (2000, May). *BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. IETF - Internet Engineering Task Force. https://tools.ietf.org/html/bcp38

FMA - Financial Markets Authority. (2021, January). *Market Operator Obligations Targeted Review - NZX*. https://www.fma.govt.nz/assets/Reports/Market-Operator-Obligations-Targeted-Review-NZX.pdf

Fonseka, D. (2021, April 27). *NZX and Reserve Bank cyberattacks expose lax cybersecurity approach, Mega execs say*. Stuff. https://www.stuff.co.nz/business/124934012/nzx-and-reserve-bank-cyberattacks-expose-lax-cybersecurity-approach-mega-execs-say

Forbes. (2021). *#100 Robert Pera*. https://www.forbes.com/profile/robert-pera/?sh=1300b01335c7

Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal*. Published. https://poseidon01.ssrn.com/delivery.php?ID=258105111101104124122116001028104088038002035054002027096002013102000123002126084071043103049011103001110086111021025123108092058017008015072081006105064127025096022060049084091099117107070125124004110075011092019119110026098122103090003093100091083065&EXT=pdf&INDEX=TRUE

Hubbard, R. (2015, February 5). *Impostors bilk Omaha's Scoular Co. out of $17.2 million*. Omaha World-Herald. https://omaha.com/business/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html

Hunt, G. (2017, September 11). *Spotting fake invoice scams – think twice before you pay that invoice!* TitanHQ. https://www.titanhq.com/blog/dont-risk-your-career-think-twice-before-you-pay-that-invoice/

Imperva. (2019). *Imperva DDoS Protection*. https://www.imperva.com/resources/datasheets/ImpervaDDoSProtection_Updated082019_v2.1.pdf

Imperva. (2020, September 30). *What is a TCP SYN Flood | DDoS Attack Glossary | Imperva*. https://www.imperva.com/learn/ddos/syn-flood/

Imtiaz, F. (2021, March 25). *The Looming Cyber Threat of a DDoS Attack*. GISPP - Global Information Security Society for Professionals of Pakistan. https://www.gispp.org/2021/03/25/the-looming-cyber-threat-of-a-ddos-attack/#:%7E:text=In%20a%20non-volumetric%20DDoS%20attack%2C%20the%20target%20is,4%20and%20Layer%207%20of%20the%20OSI%20model.

Kesavan, A. (2018, March 1). *How GitHub Successfully Mitigated a DDoS Attack*. ThousandEyes. https://www.thousandeyes.com/blog/how-github-successfully-mitigated-ddos-attack

Kordia. (2020, September 15). *Four Questions About DDoS Attacks Answered*. https://www.kordia.co.nz/news-and-views/questions-about-ddos-attacks-answered

Kottler, S. (2018, March 1). *February 28th DDoS Incident Report*. The GitHub Blog. https://github.blog/2018-03-01-ddos-incident-report/

Kramer, R. M. (2009, June). *Rethinking Trust*. Harvard Business Review. https://hbr.org/2009/06/rethinking-trust

Lone, Q., Korezynski, M., Ganan, C., & Eeten, M. V. (2020). SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers. *Workshop on the Economics of Information Security*. Published. https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final31.pdf

Louie, C. (2018, March 26). *Shodan me the Memcache!!* Chris Louie, CISSP. https://www.chrislouie.net/blog/2018/3/26/shodan-me-the-memcache

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156

NETSCOUT. (2018, July). *How to Analyze and Reduce the Risk of DDoS Attacks*. https://www.netscout.com/sites/default/files/2018-07/SECWP_005_EN-1802-How-to-Analyze-and-Reduce-the-Risk-of-DDoS-Attacks_0.pdf

NETSCOUT. (2021). *NETSCOUT Threat Intelligence Report* (No. 6). https://www.netscout.com/sites/default/files/2021-04/ThreatReport_2H2020_FINAL_0.pdf

NZX. (2020, December 4). *Independent reports on NZX IT and cybersecurity completed*. https://www.nzx.com/announcements/364459

O'Neill, R. (2020, December 4). *NZX will not release report into DDoS attacks, shares summary*. Reseller News. https://www.reseller.co.nz/article/684968/nzx-will-release-report-into-ddos-attacks-shares-summary/

Palmer, D. (2020, November 11). *DDoS attacks are cheaper and easier to carry out than ever before*. ZDNet. https://www.zdnet.com/article/ddos-attacks-are-cheaper-and-easier-to-carry-out-than-ever-before/#:%7E:text=One%20of%20the%20reasons%20that,take%20control%20of%20the%20them.

Puller-Strecker, T. (2020, September 2). *GCSB examining extortion email sent to NZX ahead of DDoS attack*. Stuff. https://www.stuff.co.nz/business/122636582/gcsb-examining-extortion-email-sent-to-nzx-ahead-of-ddos-attack

Quist, N., & Kaiser, D. (2018, March 8). *Detecting Memcached DDoS Attacks Targeting GitHub*. LogRhythm. https://logrhythm.com/blog/detecting-memcached-ddos-attacks-targeting-github/

Reidy, M. (2020, December 21). *NZX admits cyber security standards were not met ahead of attacks as industry reports surge in Kiwi tech systems targeted*. Newshub.

https://www.newshub.co.nz/home/money/2020/12/nzx-admits-cyber-security-standards-were-not-met-ahead-of-attacks-as-industry-reports-surge-in-kiwi-tech-systems-targeted.html

Research and Markets Ltd. (2020, May). *DDoS Prevention and Mitigation Market - Forecasts from 2020 to 2025*. https://www.researchandmarkets.com/reports/5067481/ddos-prevention-and-mitigation-market-forecasts?utm_source=GNOM&utm_medium=PressRelease&utm_code=pb3dwf&utm_campaign=1450415+-+DDoS+Prevention+and+Mitigation+Market+-+Global+Forecasts+from+2020+to+2025&utm_exec=chdo54prd

Sari, O. (2020, November 24). *10 Email Security Risks in 2020 - Anti-phishing Solution and Security Awareness Training - Keepnet Labs anti-phishing solution*. Anti-Phishing Solution and Security Awareness Training - Keepnet Labs. https://www.keepnetlabs.com/anti-phishing-solution-threat-simulation-2/

SEC - Securities and Exchange Commision. (2015, August). *FORM 8-K*. https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

Spicer, M. (2021, January 7). *Busting Business Email Compromise*. Anderson Technologies. https://andersontech.com/busting-business-email-compromise/

Tarabay, J. (2021, February 5). *How a Dated Cyber-Attack Brought a Stock Exchange to its Knees*. Bloomberg. https://www.bloomberg.com/news/articles/2021-02-04/how-a-dated-cyber-attack-brought-a-stock-exchange-to-its-knees

Trend Micro. (2018, March 8). *PoC Exploits for Memcached DDoS Attacks Published Online*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/poc-exploits-for-memcached-ddos-attacks-published-online

Vardi, N. (2016, February 8). *How A Tech Billionaire's Company Misplaced $46.7 Million And Didn't Know It*. Forbes. https://www.forbes.com/sites/nathanvardi/2016/02/08/how-a-tech-billionaires-company-misplaced-46-7-million-and-didnt-know-it/?sh=7546749f50b3

Vixie, P. (2014). Rate-limiting State: The Edge of the Internet is an Unruly Place. *Queue*, *12*(2), 10–15. https://doi.org/10.1145/2578508.2578510

Wallarm. (2014). *The New Page of Injections Book: Memcached Injections*. https://www.blackhat.com/docs/us-14/materials/us-14-Novikov-The-New-Page-Of-Injections-Book-Memcached-Injections-WP.pdf

Whalen, K. (2018, April 11). *The Business of Botnets*. NETSCOUT. https://www.netscout.com/blog/business-botnets

Zhijun, W., Wenjing, L., Liang, L., & Meng, Y. (2020). Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey. *IEEE Access*, *8*, 43920–43943. https://doi.org/10.1109/access.2020.2976609