Cyrus Bharry (cssb2)

CO558

The Coronavirus pandemic has brought on an influx of threat actors to exploit on the increased use of remote working and the sudden shift in security needed to keep data safe from new channels of attacks. In September 2020, CGI's Security Operations Centres reported a surge of '30,000% increase in threats related to COVID-19, including malware, weaponised websites, and phishing emails [1], a number which is sure to rise as time goes on as the pandemic continues.

As a result of the social distancing and the work from home approach, employees will likely be required to use equipment and or software which they may not be familiar with. The rapid move to online business has meant training opportunities may have been limited to bring all employees up to the industry standard of knowledge in security that specialists have, resulting to exposure of potential gaps in security which can be targeted by attackers. This vulnerability that a company is exposed to could be critical to operations, as in some cases if a company's reputation over data protection and integrity, then the trust of that business could be damaged beyond salvation in this new era of online working, as well as paying for damages in a data breach. An increase in working from home results in there being more areas which attackers could penetrate as not many of the homes being worked from have the same level of protection/deterrent measures in place compared to their usual working environment this is supported by a report conducted by Hayes Connor Solicitors on data breach statistics at home discovering that in their study of a sample of UK office workers '1 in 5 (employees) said they had recieved no training at work for GDPR, cyber security, or handling company data.' [2] The first step to mitigate this new gap in security is to conduct comprehensive training for employees.

Phishing attempts have seen an increase due to the pandemic. Google's Threat Analysis Group (TAG) in April 2020 detected '18 million malware and phishing Gmail messages per day related to COVID-19, in addition to more than 240 million COVID-related daily spam messages.' [3] Again the mass hysteria of the pandemic has rendered these attempts successful as most users act fast trusting these sources. Personal email accounts are not the only place that have been targeted by these phishing attacks, attackers posing to be from official government pages have been used to ransom data from their victims. One such case of this is a phishing attempt impersonating the World Heath Organization, malicious emails were sent by actors which deployed hidden keyloggers and various trojans. [4] The implication from these attacks resulted in data being stolen and sold, as validation from the sender could not be confirmed many of these email attacks were successful. Reparations are being made over these attacks with official government backed pages publishing reports on how to detect fraudulent emails and how to report such emails for investigation, however unless further measures in authentication can be derived these forms of phishing attacks will prevail.

Another form of attack which has seen a significant gain over the course of the pandemic is the frequency of Distributed Denial of Service (DDoS) attacks. A report by Nexusguard found that DDoS attacks 'rose more than 278% compared to Q1 2019 (in Q1 2020) and more than 542% compared to … (Q4 2019)' [5] as the pandemic unfolded. These sorts of attacks can be critical if performed correctly as it can halt an entire businesses online presence in an instant, this is especially crucial in today's world were working from home has increased and attackers can target remote access gateways to halt work from being done. Activision Blizzard's Battle.net was targeted with a DDoS attack which left many of their 15 million players [6] unable to connect to game servers during the height of quarantine lockdown causing a loss in revenue and player base and due to working from home policies this meant turn around times for bringing servers back online were extended causing more revenue to be lost. VPNs can be used to protect servers of an organisation; however eventually attackers will start targeting popular VPN services instead to disrupt business.

Overall, COVID-19's impact on cyber security has been enormous, due to the work from home approach it has led to many key areas of exploitation to be discovered not only in personal use, but in business and government cases. New areas of exploitation lead to new ways of defence which will have to be developed soon to combat the new generation of attacks brought on by the pandemic.

[1] Richard Lush. *Helping defend against a 30,000% increase in phishing attacks related to COVID-19 scams*

https://www.cgi.com/uk/en-gb/blog/cyber-security/helping-defend-against-a-30000-increase-in-phishing-attacks-related-to-covid-19-scams

[2] Hayes Connor Solicitors. *Data Breach Statistics 2020*

https://www.hayesconnor.co.uk/news-and-resources/reports/data-breach-statistics-2020/

[3] Shane Huntly. *Findings on COVID-19 and online security threats*

https://blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/

[4] David Ruiz. *Coronavirus scams, found and explained*

https://blog.malwarebytes.com/scams/2020/03/coronavirus-scams-found-and-explained/

[5] Nexusguard *DDoS Threat Report 2020 Q1*

https://blog.nexusguard.com/threat-report/ddos-threat-report-2020-q1

[6] Fraser Brown. *Blizzard is investigating Battle.net problems and a DDoS attack*

https://www.pcgamer.com/blizzard-is-investigating-battlenet-problems-and-a-ddos-attack/