Examining Trends and Experiences of the Last Four Years of Socially Engineered Ransomware Attacks

William Seymour
Tidewater Community College

Examining Trends and Experiences of the Last Four Years of Socially Engineered Ransomware Attacks

William Seymour

COVA CCI

Abstract

This study examines and reports the trends of social engineering-based ransomware attacks over the past four years from three major technology corporations. The focus of the reports was on major threat actors and their attacks against the corporations and their clients. The data were organized chronologically by year, and prevalent or abnormal findings were shared in this report. It was found that social engineering attacks were tremendously effective. Many ransomware attacks stemmed from Phishing. Social engineering approaches allowed attackers to conduct breaches using ransomware applications like GandCrab and Ryuk. Humans are incredibly susceptible and fall for social engineering tactics- primarily Phishing. The information reflected in this report ought to be used to motivate businesses to increase spending and training opportunities for employees to help defend against these social engineering-based attacks.

Keywords: social engineering, Phishing, ransomware, Verizon, Malwarebytes, McAfee.

Table of Contents

Introduction

Social engineering is defined by the "Principles of Computer Security Fifth Edition" as "The process of convincing an authorized individual to provide confidential information or access, to an unauthorized individual" (Conklin, 2018, p. 73). This is a serious threat to security as it relies on a person making a mistake, not the computer. Whether that be Phishing, trying to bait a user into clicking an unsafe link, or pretexting, which is similar to Phishing but in a different form. Both strategies require either gaining the trust of the victim or a sense of urgency to be effective (Alturki, 2020). Social engineering attacks can cost corporations and their clients hundreds of thousands of dollars to billions (Salahdine, 2019). This being said, losses are not only financial. Attackers may also steal data during a breach to be used later and given to competing nation-states or organizations, perhaps as blackmail material or for separate auctions. The stakes are high when it comes to defending data. Everyone is at risk of being exploited by these social engineering attacks (Basset et al., 2021).

A ransomware attack is defined by the "Cybersecurity & Infrastructure Security Agency," as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption" (Cybersecurity & Infrastructure Security Agency, 2020, p. 2). Ransomware attacks are another serious threat that costs anywhere from hundreds of thousands to millions of dollars. What makes this attack so significant is that the threat is not always over when the ransom is paid. Frequently unencrypted data that is exfiltrated is used as blackmail material against the victim. (Multi-State Information Sharing and Analysis Center, 2021)

These two approaches to cybercrime are incredibly effective often combining the two, where a victim is first attacked through social engineering. After a foothold has been established

through that social engineering corridor, the ransomware prong of the attack kicks in, to where the data is encrypted, exfiltrated, and ransomed. An example of this would be the GandCrab ransomware campaign. The attack would use a social engineering attack, mainly Phishing, to bait users to click ransomware-filled links, which would download the GandCrab ransomware onto the victim's equipment. The data would be encrypted, and a ransom for that data would be forged. To explain the severity of the attack, it is estimated that more than two billion dollars in ransomware payments were made (DeepInstinct, 2020).

Using a social engineering attack to launch an effective ransomware attack has proved to be shockingly effective. This paper aims to look through the reports of several well-known corporations to see the trends and their experiences with these social engineering-based ransomware attacks over several years. Reading plenty of news articles, it also became apparent that socially engineered ransomware attacks were uniquely complicated and increasing in popularity because of the involvement of human interaction. As a result, understanding the data in this literature could act as an incentive to prioritize and invest in training for clients and employees, as awareness and exercises are the key mitigations to these types of attacks.

I will examine the findings of major tech companies' annual technical reports of their ransomware attacks. I will pay specific attention to social engineering attacks noting similarities and differences as the attack vectors evolve from 2018 to 2021.

Methods

There are many ways in which a system can be breached, both through hacking and social engineering. However, only the trends and experiences of socially engineered ransomware attacks in corporate entities over four years were explored. To do this, three entities were selected based on their visibility in cybersecurity. Verizon, McAfee, and Malwarebytes

were chosen because they all have deep investments in cybersecurity, are very public about their investigations, and have published their reports for numerous years. It is also recognized that these corporations worked together to verify their findings on multiple occasions. As a result of their technical reports, their data was explored to meet this project's research needs. For Verizon, the "Data Breach Investigation Report" was downloaded. For Malwarebytes, the "State of Malware Report" and "Crimeware Tactics and Techniques" were downloaded. For McAfee, the "Labs Threat Report" was downloaded. The findings will be from the past four years of annual technical reports, starting in 2018 and moving chronologically forward to 2021.

Findings by Year

2018

Verizon noted that there were 53,000 incidents and 2,216 confirmed data breaches. Of these attacks, Phishing was the third most common type of attack, accounting for 236 of these confirmed breaches (Widup, 2018, p. 8). It is also noted that 56% of all malware incidents were ransomware attacks (Widup, 2018, p. 23). A large portion of these attacks are individuals falling for Phishing-based attacks. Their team notes that the healthcare industry is particularly vulnerable, with 70% of socially engineered attacks being Phishing-based (Widup, 2018, p. 34). Most people use it, so if healthcare-based systems are attacked and their data is stolen, it can affect most of the population. Medical data and other financial or other equipment-based data can be taken and ransomed for a higher amount of money, making it a highly incentivized target for ransomware.

Malwarebytes, notes a sharp rise in ransomware attacks that do not encrypt data but instead implement cryptocurrency mining systems. Spiking in May with more than 500 million detections (Kujawa et al., 2018), relatively new ransomware called GandCrab was adopted,

which thrived off of being activated through socially engineered Phishing attacks, where a user would be tricked into clicking an embedded link launching the GandCrab software. What made GandCrab so appealing in its sharp ascent in use was its adaptability to acquire cryptocurrency. The use of crypto mining replacing data being encrypted might seem better for the victim, as their data isn't directly being pawned off, the attacks are still serious because of a loss in performance resources. Crypto mining uses a computer's hardware and processing power to slowly "mine" the currency by solving algorithms. In short, this means that a victim's computer performance will drop severely, as the computer is focusing on solving algorithms and not what the user wants it to do.

McAfee notes the rise in the use of GandCrab, with a sudden spike from 2.5 million to just under 4 million new attacks to target cryptocurrency (Samani & Beek, 2018, p. 10). This is substantially more for the year, as in 2017 the new attacks being cryptocurrency-based were less than 250,000 at their height (Samani & Beek, 2018).

And, McAfee notes a new spike in Phishing URLs. Around the third quarter, more than 900,000 new Phishing URLs were created, which is more than the first two combined (Samani & Beek, 2018, p. 32). This is significant because the victim is tricked into believing that they are entering a well-known and protected site, however, the attacker spoofs the URL and changes it to look legitimate. When in reality, the victim feeds their data to the attacker. Upon acquiring the data, the attacker often ransoms it back to the user for a large sum of money.

Throughout 2018, the threat of healthcare was recognized as a specifically vulnerable target for social engineering-based ransomware attacks. Not only that but the potential of the cryptocurrency market has driven a sharp rise in ransomware attacks that target mining

cryptocurrencies. Combining these aspects with the increased cases of Phishing URLs is a popular attack method.

2019

Verizon, reports a noticeable 41,686 incidents and 2,013 breaches (Verizon, 2019). This implies that compared to last year, there were fewer overall incidents, however, there is a higher percentage of successful data breaches. Out of this, a stunning 33% of their attacks are social engineering-based, with 32% of them being Phishing-based (Verizon, 2019). Within these Phishing attacks, 370 of these Phishing and pretexting attacks focused on using fake W-2 forms as bait for the victims to click on (Verizon, 2019). Clearly, people have good intentions as they are trying to file their taxes, but instead are falling for these Phishing attempts. This allows attackers to get vital data and provides an opportunity to launch a ransomware attack on both the tax filer and their employer.

Notice how the crypto-criminals were not mentioned. As a result of a 77% drop in bitcoin value later in that year (Verizon, 2019), many attackers lost interest in it, switching back to the well-known ransomware ways of simply encrypting data holding people ransom. Money seems to be a key motive, and as a result, the changes in demand will often influence how and what professional hackers do.

Malwarebytes highlighted the use and rise of Phishing-based trojans. Trojans are similar to Phishing as they are disguised files that trick the victim into downloading them to launch their attacks. These types of attacks were up 132% from previous years, with “Emotet” and “Trickbot” becoming the prominent threat actors (Malwarebytes, 2019). Emotet had well over 700,000 detections at its peak, and Trickbot had over 80,000 detections (Malwarebytes, 2019). These systems were extremely effective because they targeted unpatched and un-updated

vulnerabilities. It is crucial to update devices. However, doing so is often overlooked and not a priority for many people (Morris, Becker, & Simon, 2019).

On the other hand, McAfee notes that there was a remarkable rise in ransomware attacks by roughly 118%, continuing to use Phishing as a common platform when launching these attacks (Beek et al., 2019). It could be implied that the spike in these attacks is to compensate for the volatile nature of cryptocurrency markets, as mentioned prior. Another reason for the spike in more conventional ransomware attacks, as opposed to crypto-based ransomware attacks, is the result of GandCrab being patched out and mitigated in many instances. McAfee teams were able to create a decryption tool for GandCrab versions 1, 4, and any versions 5-5.1 (Beek et al., 2019). For reference, at the time there are five known GandCrab versions, each having its own variations (Usharani et al., 2021). While the cat and mouse chase between cybersecurity experts and attackers continue, large strides have been made in creating decryption software to defeat large ransomware giants like GandCrab.

However, it seems that with the fall of one giant, another one rises. Another ransomware takes the stage, named “Ryuk.” Ryuk is ransomware that made its debut by targeting publishing services such as the “New York Times” and the “Wall Street Journal” using Phishing as a means to cultivate their ransomware (Beek et al., 2019). The specific publishing giants that were attacked are especially worth mentioning, as they host large databases of valuable and personal information built up over several decades.

In 2019, there was a noticeable change in landscape as the crypto-mining market began to take a dip. This paved the way for more conventional ransomware attacks launched with Phishing creatively using Trojans, like Emotet and Trickbot, and new forms such as fake W-2s.

2020

Verizon shows an exponential change in the year, acknowledging that 157,525 incidents were reported, with 3,950 of the incidents being confirmed data breaches (Basset et al., 2020). Of these attacks, 22% of them were social engineering-based attacks. Phishing has become the most common variety of breaches this year, being greater than 20% of the confirmed breaches (Basset et al., 2020). Notice the spike in 2020 compared to 2019. It could be implied that this is a result of large quantities of business activity being moved online due to the COVID-19 pandemic. Phishing in this new target-rich environment became a low effort and high reward for attackers. The rapid adaption of online services causes many new potential victims to be targeted who were not already aware of such attacks, subsequently falling for Phishing attempts, causing the loss and encryption of their own and their employer's data. People became more of reliability as they did not know that they were falling for such attacks.

Malwarebytes' report showed bitcoin, and other crypto mining ransomware attacks dropped by 46% (Kujawa et al., 2020). This is again likely a result of the inconsistent nature of cryptocurrencies. This being said, it seems that the downshift in crypto mining-based ransomware attacks has been compensated by a monstrous 463% rise in Adware cases (Kujawa et al., 2020, p. 12). Adware is a social engineering attack that baits victims into clicking on fake ads that act like a trojan or Phishing attempt to which ransomware can be launched.

Emotet becomes a large attacker in play, triumphantly making its return, noting an increase in 73% of Emotet detections (Kujawa et al., 2020) with the United States accounting for 71.58% of the detections and the United Kingdom accounting for another 23.63% (Kujawa et al., 2020). However, fortunately, they seem to drop off as the year progresses. One of course couldn't be mentioned without the other. We see the return of Trickbot adding to its toolkit as a new

opportunity allowing it to bypass two-factor authentication, leading to the compromise of over 250 million accounts (Kujawa et al., 2020). The common factor for these two thorns seems to be the prevalence of Phishing to continue making it possible, so the cat and mouse chase to patch them out continues.

McAfee notes a more consistent number of new ransomware attacks, roughly 1.25 million in the first several quarters (Beek et al., 2020). Notably, the team at McAfee directly addresses COVID-19 as being a catalyst for cyberattacks in the online world (Beek et al., 2020). As mentioned prior, their team specifically looks at a spike in fake COVID-19 related emails that are made to look like the government sent them containing fake malware-loaded links designed to harvest your credentials. Therefore, when victims try to keep themselves updated and informed, they instead harm themselves. Within this particular fake government information Phishing campaign, attackers utilize an access vulnerability of the Microsoft OneDrive to acquire the data (Beek et al., 2020).

Clearly, 2020 presented us with a major shift in cybersecurity, as the introduction of a new catalyst, COVID-19, transitions more and more into the online world. This transition without proper awareness or training of social engineering attacks. Overwhelmed people are becoming victims at a much higher rate than in previous years.

2021

Verizon, reported 79,635 incidents with 5,258 data breaches. This would imply that while there were fewer incidents overall than in 2020, there was a much higher percentage of successful breaches. Furthermore, a much higher rate, 43%, of these breaches had roots in social engineering (Basset et al., 2021). Their team continued to show a general upward trend in social engineering breaches since 2017.

Another trend that was recognized is where the social engineering attacks are being detected from. Out of 234 participants, only one report was filed by an internal employee. The rest of the reports came from a third party and other external sources (Basset et al., 2021). The lack of internal reports could be implied by the victims not knowing that they are being hacked, which seems to be an unfortunately common trend and the goal of the infiltrator.

Continuing further, each of their industries faced severe challenges over the year. Whether they are from Phishing or pretexting, social engineering attacks have become fifteen times more common than in the previous year (Basset et al., 2021). Their team found a concerningly high amount of social engineering in each department and industry in the company. Whether it be from Mineral Extraction and utilities having 98% of their breaches being socially engineered, Manufacturing seeing 82%, Financial and Insurance seeing 81%, Educational Services seeing 86%, the list goes on (Basset et al., 2021). Every department noticed that more than 70% of the data breaches were from socially engineered attacks (Basset et al., 2021). Of these socially engineered breaches, many of them had a ransomware follow-up as opposed to a traditional exfiltration of data. 90% of these incidents had no financial loss (Basset et al., 2021). To be more precise, 23% of the successful ransomware attacks had a base in Phishing, while another 20% were socially engineered web application-based derivatives (Basset et al., 2021). Breaking it down, all of the industries that participated suffered from these social engineering attacks. These attacks were both persistent and effective, leading to multiple breaches in each domain.

Malwarebytes reported many social engineering campaigns being conducted during the COVID-19 pandemic. It is acknowledged that attacks on healthcare continue to become more

prevalent. Attacks against medical facilities have ramped up because they have become more target-rich throughout the pandemic (Malwarebytes, 2021).

McAfee shows that socially engineered Phishing and Spear-Phishing attacks made the top five most common avenues of attack. Meanwhile, these types of attacks remained in the top three initial access techniques (Beek et al, 2021 June, p. 20). These attacks affected thousands of establishments globally and remained a critical vulnerability.

Furthermore, there are fewer new ransomware attacks, roughly 2.51 million, over the first quarter (Beek et al., 2021). In comparison, the fourth quarter of 2020 saw a spike at 5.12 million (Beek et al., 2021). This being said, Ryuk makes a reappearance. It remains a top threat right under REvil/Sodiniokibi and RansomeXX (Beek et al., 2021). This implies that while the quantity of the attacks has toned downward, the quality of the attacks has not. Ryuk remains on the stage, proving that Phishing attacks are still brutally effective.

In 2020 we saw the rise of higher quality attacks leading to breaches in many industries. Meanwhile, the attacks on healthcare-based facilities have seemed to continue to rise, as well as old ransomware returning and retaining its potency on the world stage.

Conclusions

The human remains simultaneously the essential component in any industry and the most vulnerable one. Falling victim to Phishing and pretexting is the constantly growing theme throughout the reports across the last four years. Attacks result in the loss of enormous quantities of money and data from both corporate and personal entities. Everyone is at risk; every organization is liable to fall for these attacks. These attacks are persistent, relentless, and consistent. Motives may change, whether they be crypto-oriented, medical facilities with the rise

of COVID-19, or are just targeting large government databases. But, the methods of Phishing or pretexting are effective, so implementation has remained consistent over the last few years.

Glossary:

URL Uniform Resource Locator

References

Alturki, A., Alshwihi N., Algarni A. (2020, April 29). *Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks*. Retrieved April 11, 2022, from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9096355

Basset, G., Hylender, C., Langlois, P., Pinto, A., Widup, S. (2020). *Data breach 2020 investigations report - Verizon business*. Retrieved April 10, 2022, from https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf

Basset, G., Hylender, C., Langlois, P., Pinto, A., Widup, S. (2021). *(PDF) 2021 Verizon Data Breach Investigations Report*. Retrieved April 10, 2022, from https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report

Beek, C., Cashman, M., Fokker, J., Gaffney, M., Grobman, S., Hux, T., Minihane, N., Munson, L., Palm, C., Polzer, T., Samani, R., Schmugar, C. (2021, June). *McAfee Labs Threat*. Retrieved April 10, 2022, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-jun-2021.pdf

Beek, C., Dolezal, A., Fokker, J., Gaffney, M., Holden, T., Hux, T., Laulheret, P., McKee, D., Munson, L., Palm, C., Polzer, T., Povolny, S., Samani, R., Solanki, P., Velasco, L. (2021, October). *Advanced Threat Research Report, October 2021*. Retrieved April 10, 2022, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-oct-2021.pdf

Beek C., Dunton, T., Fokker, J., Grobman, S., Hux, T., Polzer, T., Lopez, M., Roccia, T., Saavedra-Morales, J., Samani, R., Sherstobitoff, R. (2019, August). *McAfee Labs Threats Report August 2019*. Retrieved April 10, 2022, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

Beek, C., Chandana, S., Dunton, T., Grobman, S., Gupta, R., Holden, T., Hux, T., McGrath, K., McKee, D., Munson, L., Narayan, K., Olowo, J., Pak, C., Palm, C., Polzer, T., Ryu, S., Samani, R., Sarukkai, S., Schmugar, C. (2020, November). *McAfee Labs Threats Report, November 2020*. Retrieved April 10, 2022, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

Kujawa, A., Zamora, W., Umawing, J., Arntz, P., Ruiz, D. (2019). *Cybercrime Tactics and Techniques*. Retrieved April 10, 2022, from https://www.malwarebytes.com/resources/files/2019/11/191028-mwb-ctnt_2019_healthcare_final.pdf

Conklin A., White, G., Cothren, C., Davis, R., Williams, D., Rogers, B. (2021). *Principles of Computer Security: Comptia security+ and beyond*. McGraw-Hill.

Cybersecurity & Infrastructure Security Agency (2020, September). *CISA MS-ISAC Ransomware Guide*. Retrieved April 11, 2022, from https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

DeepInstinct (2020). *Deep instinct - prevention case studies - Ciosummits.com*. Retrieved April 11, 2022, from https://www.ciosummits.com/Deep_Instinct_-_Prevention_Case_Studies.pdf

Kujawa A., Zamora, W., Umawing, J., Segura, J., Tsing, W., McNeil, A., Boyd, C., Arntz, P. (2018). *Cybercrime tactics and techniques: Q2 2018*. Retrieved April 10, 2022, from https://www.malwarebytes.com/resources/files/2018/07/malwarebytes_cybercrime-tactics-and-techniques-q2-2018.pdf

Kujawa A., Zamora, W., Segura, J., Reed, T., Collier, N., Umawing, J., Boyd, C., Arntz, P., Ruiz, D. (2020). *Presents 2020 State of Malware Report*. Retrieved April 10, 2022, from https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report.pdf

Malwarebytes (2020). *Cybercrime Tactics and Techniques 2020*. Retrieved April 10, 2022, from https://www.malwarebytes.com/resources/files/2020/06/ctnt_q1_2020_covid-report_final.pdf

Malwarebytes (2021). *State of Malware Report 2021*. Retrieved April 10, 2022, from https://www.malwarebytes.com/resources/files/2021/04/mwb_stateofmalware2021_exec-summary_with-cta_final.pdf

Malwarebytes (2019). *Malwarebytes labs 2019 State of Malware Report*. Retrieved April 10, 2022, from https://www.malwarebytes.com/resources/files/2019/01/malwarebytes-labs-2019-state-of-malware-report-2.pdf

Morris, J. (2019). *In control with no control: Perceptions ... - NDSS symposium*. Retrieved April 11, 2022, from https://www.ndss-symposium.org/wp-content/uploads/2019/02/usec2019_02-5_Morris_paper.pdf

Multi-State Information Sharing and Analysis Center. (2021). *Ransomware: The Data Exfiltration and Double Extortion trends*. Retrieved April 11, 2022, from https://www.cisecurity.org/wp-content/uploads/2021/04/Ransomeware-Data-Exfiltration-and-double-extortion-trends-.pdf

Salahdine, F & Kaabouch, N. (2019, April 2). *Social Engineering Attacks: A survey*. Retrieved April 11, 2022, from https://res.mdpi.com/futureinternet/futureinternet-11-00089/article_deploy/futureinternet-11-00089.pdf

Samani, R., & Beek, C. (2018, December). *McAfee Labs Threats Report December 2018*. Retrieved April 10, 2022, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

Usharani, S, Manjuy Bala, P., Martina Jose Mary, M. (2021). *Dynamic Analysis on Crypto-ransomware by using Machine Learning: GandCrab Ransomware*. GandCrab Ransomware. Retrieved April 11, 2022, from https://iopscience-iop-org.eztcc.vccs.edu/article/10.1088/1742-6596/1717/1/012024/pdf

Verizon, (2019). *2019 DBIR introduction*. Verizon Enterprise. Retrieved April 10, 2022, from https://www.verizon.com/business/resources/reports/dbir/2019/introduction/

Widup, S. (2018, April). *(PDF) 2018 Verizon Data Breach Investigations Report*. Retrieved April 10, 2022, from https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report