ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article Open Access

Social Engineering and Ransomware, Still the Top Threats in CyberSecurity Space, Why and How to Avoid?

Pranith Shetty

Information Security and Risk Lead, Cisco, New Jersey, USA

ABSTRACT

Social engineering and ransomware have been around for many years in the industry across sectors including manufacturing, technology and finance. The motive behind these techniques and attacks have always been gaining access to systems, data especially PII, MNPI. Most of these attacks were sponsored by nations at first, due to the amount of resources and effort needed at scale but it has now evolved into the top cybersecurity threats plaguing industries. In spite of the presence of various cybersecurity threats, evolving risk landscape, Social engineering and ransomware topping the charts is a mystery to professionals working outside of the security domain. This article aims at understanding the context behind these techniques and attacks, providing real time examples driving the relation between social engineering and Ransomware attacks, methods that are tried and tested, used by firms in the real world that has helped bring the numbers and frequency of these attacks down. This article also brings perspective from the various thought leaders, consulting firms working in Cybersecurity space.

***Corresponding author**
Pranith Shetty, Information Security and Risk Lead, Cisco, New Jersey, USA.

Received: November 16, 2022; **Accepted:** November 20, 2022; **Published:** November 27, 2022

Keywords: Social Engineering, Ransomware, Phishing, Zero Trust, Cybersecurity, Risk Management

Introduction

Social engineering attack by definition is when attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems [1]. It would be very challenging for the victim to guess the attacker since the person would appear unassuming and respectable, they would claim to be a new employee or repairman and even have valid credentials, however, by asking specific questions would one be able to ascertain the real identity. There are many forms of social engineering attacks that this article aims to cover in detail.

On the other hand Ransomware is an ever evolving form of malware designed to encrypt files on a device, rendering any files and systems that rely on them unusable [2]. Malicious actors then demand ransom in exchange for decryption. If the ransom is not paid, they threaten to sell or leak exfiltrated data.

Rationale for Study

Both Social engineering and ransomware have become increasingly common amongst varied businesses including technology, financial services, healthcare etc. PII, MNPI related information is extremely sensitive and of great value for threat attackers. Credit companies and hospitals have been targeted now more than ever which is quite evident in the data breaches across the landscape. As per this article Social engineering attacks are on the rise and 98% of cyber-attacks rely on social engineering in some capacity [3]. The popularity and usage of social media networks and channels like Facebook, Twitter have only aided to the social engineering techniques. Information has now become easily available and accessible. This technique preys on people who would always be the weakest link, when it comes to cybersecurity attack vectors.

Any organization that has untrained employees in cybersecurity or even in critical roles with access control provisions is prone to Social engineering attacks.

Meanwhile, Ransomware accounted for a significant number of reported cyber incidents amongst SMEs in 2022 as compared to 2021 as per this article [4]. The severity of attacks is increasing, however the frequency is not. Ransomware as a service expected to be amongst the biggest cyber threats in coming months.

In spite of increased number of threats and prevalent use cases for companies to learn from, these incidents are still plaguing the industry, this article and the next few sections aim at dissecting the concepts, learning some key statistics, reasons for these attacks to be still prevalent and what methods can help avoid, mitigate these attacks.

Key Concepts

Let's try to understand Social engineering and ransomware in detail, using industry use cases and definitions.

Social Engineering

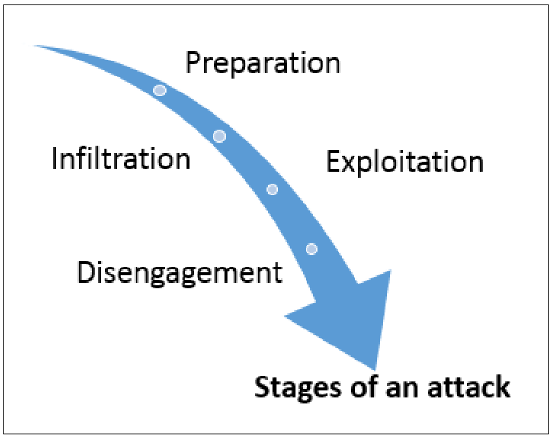


Figure 1: Stages of Social Engineering Attack

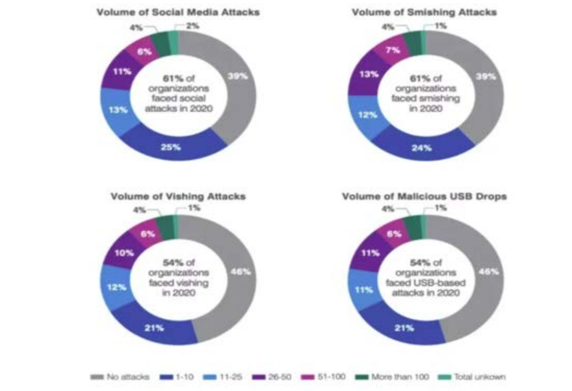
Social Engineering attacks aim to manipulate the victim(s) to disclose sensitive information that can be used for the benefit of Cyber threat actors [5].

In other words, it's an attempt by attackers to trick humans to give up access credentials, bank details or other sensitive information [6].

It occurs in 4 stages:

- **Preparation:** Attackers collect information about victims through social media, telephone calls, email, text messages, dark web or other sources.
- **Infiltration:** Attackers approach victims my masquerading and try to gain access to information.
- **Exploitation:** Attackers persuade victims to give sensitive information such as account credentials, payment account details and other information that they can use to conduct a cyber-attack. Persuasion will be subtle like an email with link, social media interaction etc.
- **Disengagement:** Attacker stops communicating with the victim, once access is gained, performs the attack and exits the system with data.

According to CSO, around COVID in 2020, there were many phishing and scam pages created with themes around covid, gift cards and gaming hacks [5]. Technology, finance and retail industries were targeted. US, Russia and British virgin islands were the countries hosting scams. Gmail was the most popular email service used.



Sources: https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html, https://cobalt.io/blog/cybersecurity-statistics-2021, https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

There are a few prominent techniques in Social engineering [6]:

- **Phishing:** In phishing, attacker uses a message to get victim's attention and call to action by asking for help, invoking emotional triggers, there are types of phishing such as email, voice, SMS etc.
- **Spear Phishing:** This is a type of target phishing attack intended for specific persons of interest.
- **Scareware:** This is a malware tactic used to trick victims into downloading or purchasing software or further infect their device, shows users pop up security alerts that appear like legitimate warnings from companies.
- **Watering Hole Attack:** This attack involves launching malicious code from a legitimate website which is commonly visited by targets of attack, for example – a financial news website that is poorly maintained might be visited by financial experts and management personnel who might end up being the targets of these attacks.
- **Pretexting:** Attackers create a fake profile and manipulate their victims into providing private information, for example – attackers might pose as IT service staff and gain access to your credentials.
- **Baiting Attack:** Attackers provide something that victims believe to be useful, for example, there might be an existing support issue and attacker might use that information to provide you with a malicious software to install.
- **Physical Breaches and Tailgating:** As the name suggests attackers try to forcefully gain entry to organizations using victim's id and credentials, sometimes victims hold the door out of courtesy.

Ransomware

Ransomware is a type of malware that locks a victim's data or device and threatens to keep it locked or worse, unless the victim pays a ransom to attacker, earliest Ransomware attacks used to encrypt data and ask for ransom, only then the attackers may be provide the encryption key but organizations had backups and used to get away with these attacks [7].

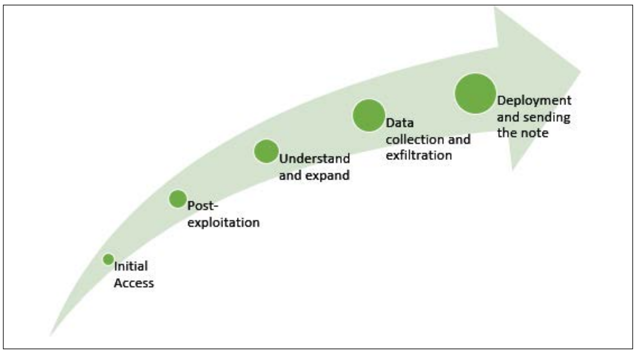

Initial Access
Post-exploitation
Understand and expand
Data collection and exfiltration
Deployment and sending the note

Figure 2: Stages of Ransomware Attack

Stages of Ransomware Attack [7]

- **Initial Access:** The most common access vectors for ransomware attacks continue to be phishing and vulnerability exploitation.
- **Post Exploitation:** Depending on initial access vector, this step involves remote access or malware prior to establishing interactive access.
- **Understand and Expand:** In this stage, attackers try to estimate the level of access and try for lateral attacks to other systems.
- **Data Collection and Exfiltration:** here the ransomware operators switch focus to identifying valuable data, exfiltrating

it and downloading or exporting a copy for themselves.

- **Deployment and Sending the Note:** Crypto ransomware begins identifying and encrypting files, some crypto ransomware will disable systems features as well. Once the objective is achieved of either encrypting the files and / or disabling the system, ransomware alerts the victim.

Types of Ransomware [7]

- **Leakware:** steals or exfiltrates sensitive data and threatens to publish it, while earlier forms of leakware stole data without encrypting it.
- Mobile Ransomware includes all ransomware that affects mobile devices.
- **Destructive Ransomware:** Threatens to destroy data if ransom isn't paid, Wiper is often suspected to be deployed by nation state actors.

Ransomware Trends

The following visual gives us an approximate breakdown of ransomware techniques, exploitation of remote services and credentials are the popular attack vectors for cyber criminals [8]

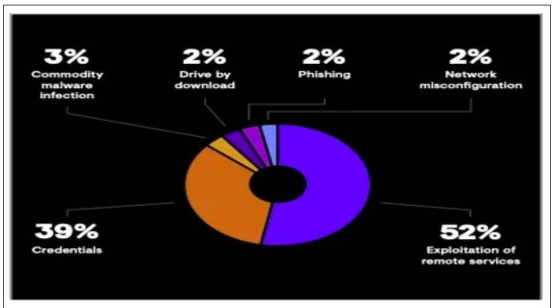


Image: SecureWorks. Initial access vectors for ransomware attacks, June 2021 to June 2022.

Social Engineering Facilitating Ransomware

There is a connection between social engineering and ransomware and that's the reason you would see or hear about both these attacks together, in some cases [7].

Phishing emails manipulate users into downloading malware that turn out into a whole blown ransomware attack with crucial systems and files locked down.

Credential attacks using social engineering techniques will eventually result in malwares being installed by attacker using victim's credentials.

Scare ware is another social engineering technique that preys on user's emotions to install malwares on victim devices.

Business email compromise is another ransomware related attack which originates via social engineering premise. There are a few more social engineering techniques like watering hole attacks that also result in ransomware attacks. The end goal of Social engineering attacks is gaining access to critical systems and data.

Method and Techniques

To protect oneself and organizations, all staff members especially Security staff members need to be trained and made aware of the various social engineering techniques & prevention methods, this training should be constantly updated with knowledge from industry standards and technologies since its continuously evolving so a method learnt now might not be useful down the line or say next year [9]. Simulation based exercises are key since that gives a clear understanding of live situations. Organization should also establish clear policies and procedures so that staff members are not conflicted in making choices, they can refer to those policies and bring any discrepancies to the attention of the authorities.

Contextual based MFA (Multi factor authentication) measures are also a good deterrent, for example in case the attacker is logging in from a system that has not been used before, or form a network that is unknown to the corporate perimeter and defense controls, or if the location of login is not the usual ones, accesses can be blocked with further verification requirements and brought to the attention of administrators as red flags who can then initiate the incident management process to narrow down or contain the attack, looping in all the relevant stakeholders.

Password management policies and discipline from staff, employees and everyone can also go a long way in protecting critical systems and resources

Email security with anti-phishing measures can minimize the threat of social engineering attacks and the ransomware attacks that follow.

Maintaining backups of sensitive data can help in business continuity and soften the impact, help buy time to respond [7]

Applying patches regularly and updating security tools can protect from malwares and softwares that aim at exploiting the known vulnerabilities and gaps in the software

Intrusion detection systems and closing unnecessary open ports are all an effort towards improving defenses against both social engineering and ransomware.

Furthermore, NIST (National Institute of Standards and Technology) has defined a Cybersecurity Ransomware Profile, which identifies security objectives from the NIST Cybersecurity Framework that support preventing, responding to, and recovering from ransomware events. The profile can be used as a guide to managing the risk of ransomware events. That includes helping gauge an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events.

Conclusion

The way we do business is constantly changing and evolving, prior to the Covid pandemic, businesses and employees used to operate from office, but later with remote work, employees can work from anywhere creating more challenges for IT and security teams, as a result paving for cybersecurity threats, however Social engineering and Ransomware have continued to be the biggest cybersecurity threats even in 2022, entering into 2023, since the whole premise of these attacks are gaining access to victim's credentials, systems, data and that has not changed.

In spite of being the biggest threats at the moment, the numbers and frequency have gone down considerably [10].

The measures and controls listed in this article, if followed will help bring down the instances and numbers down further, and help mitigate these risks, oncourse risks can never be completely resolved but mitigating them to an extent below the risk appetite is what organization across business sectors strive for [11-18].

References

1. (2021) Avoiding Social Engineering and Phishing Attacks. Cybersecurity and Infrastructure Security Agency CISA https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks.
2. Ransomware 101. CISA https://www.cisa.gov/stopransomware/ransomware-101.
3. Security M (2022) Are Social Engineering Attacks on the Rise. MitnickSecurity https://www.mitnicksecurity.com/blog/are-social-engineering-attacks-on-the-rise.
4. Gia Snape (2022) Is social engineering the next big cyber risk. Insurance Business https://www.insurancebusinessmag.com/us/news/cyber/is-social-engineering-the-next-big-cyber-risk-428245.aspx.
5. Kieran Roberts (2021) The Effectiveness of Social Engineering Explained. Bulletproof.co.uk https://www.bulletproof.co.uk/blog/why-is-social-engineering-so-effective.
6. Gonzalez C (2022) Top 5 Social Engineering Techniques and How to Prevent Them. Exabeam https://www.exabeam.com/information-security/top-8-social-engineering-techniques-and-how-to-prevent-them-2022/.
7. (2022) What is Ransomware. IBM https://www.ibm.com/topics/ransomware.
8. Pernet C (2022) 2022 State of the Threat: Ransomware is still hitting companies hard. TechRepublic https://www.techrepublic.com/article/state-of-the-threat-ransomware-hitting-companies-hard/.
9. (2022) What is social engineering in cybersecurity. CISCO https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html.
10. Josh Fruhlinger (2020) Ransomware explained: How it works and how to remove it. CSO https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html.
11. Risk management - Glossary CSRC. NIST https://csrc.nist.gov/glossary/term/risk_management.
12. Risk Appetite - Glossary CSRC. NIST https://csrc.nist.gov/glossary/term/Risk_Appetite.
13. C C for C Security (2021) Cyber threat bulletin: The ransomware threat in 2021. Canadian Centre for Cyber Security https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021.
14. Barker W, Scarfone K, Fisher W, Souppaya M (2021) Cybersecurity Framework Profile for Ransomware Risk Management. NIST https://csrc.nist.gov/pubs/ir/8374/ipd.
15. Security C T (2022) What is Social Engineering: The Ultimate Guide. CYBERTECSECURITY https://info.cybertecsecurity.com/what-is-social-engineering.
16. (2021) Ransomware Attacks: Is WannaCry Still a Threat. CybelAngel https://cybelangel.com/wannacry-still-a-threat/.
17. Weiner S (2021) The growing threat of ransomware attacks on hospitals. AAMC https://www.aamc.org/news/growing-threat-ransomware-attacks-hospitals.
18. Wolf A (2022) Top Three Cybersecurity Challenges. Arctic Wolf https://arcticwolf.com/resources/blog/top-three-cybersecurity-challenges/.