Alexander Moore

CEG 6422

Vance Saunders

9/23/21

Double Extortion Ransomware

Generally, normal ransomware involves malicious persons or groups encrypting the victim’s data and holding the data for ransom. The victim is ordered to pay this ransom for their data to be decrypted. Because many users began backing up their data on offline servers, they could avoid paying the ransom and simply revert to these backups. In response to this, the malicious persons and groups decided to create a new method called double extortion ransomware. “If the victim ignores ransom demands, some of the attackers will threaten to post the stolen information on the Internet to put additional pressure on their victims to pay the ransom” [8]. Essentially, the attackers offer to decrypt the victim’s data for a price, and if the victim is thoughtful enough to backup their data, the attacker will proceed to request more money and will leak the confidential information that they stole if they do not receive the payment. But attackers won’t only leak the information publicly; some “ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue” [9]. And ransomware extortion has been continuously evolving, even past double extortion. The next phase of extortion ransomware is triple extortion. Triple extortion adds “DDoS attacks to the aforementioned encryption and data exposure threats. These attacks could overwhelm a server or a network with traffic, which in turn could halt and further disrupt operations” [11]. The next phase in extortion, quadruple extortion, extends the ransomware to the stakeholders and customers of the victim. If an attack reaches this phase, it begins to affect a much larger spectrum of people and puts much more pressure on the victim(s). Multiple extortion ransomware is increasingly difficult to surmount because of the multiple threats it creates for the victim.

The first case of double extortion was implemented by a ransomware group known as TA2101 on Allied Universal, an American provider of security services, systems, and solutions. The attack, labeled Maze ransomware, happened in November 2019, and “When the victims refused to pay a ransom of 300 Bitcoins (approximately US$2.3 million), the attackers, who used the Maze ransomware, threatened to use sensitive information extracted from Allied Universal’s systems as well as stolen email and domain name certificates for a spam campaign impersonating Allied Universal” [7]. The attackers released a portion of the stolen information as an example of the leverage that they held over Allied Universal, and later raised the ransom after a certain amount of time. In all, TA2101 was threatening Allied Universal with uploading up to 5 GB of their confidential data to their website. Their established website is known for publishing the information and stolen data of victims of TA2101. The attacker group has since continued to torment other groups including publishing “the details of dozens of companies, law firms, medial service providers and insurance companies who have not given in to their demands” [7]. Additionally, 2020 has revealed that “ransomware groups increasingly turning to double extortion attempts with stolen data, while maintaining the traditional network encryption and ransom routine” [9]. Other ransomware groups have also followed behind the Maze ransomware with their own websites for publishing confidential information that they have stolen. One group, considered the successor to Maze ransomware, called Egregor ransomware cartel, was “arrested with the help of private-public sector partnerships, including Trend Micro” [11].

Another case of double extortion was executed by the Eastern European ransomware group known as DarkSide. On May 7, 2021, they attacked Colonial Pipeline, the largest pipeline system for refined oil products in the United States. “Stores of gasoline, diesel, home heating oil, jet fuel, and military supplies had been so heavily affected that the Federal Motor Carrier Safety Administration (FMCSA) declared a state of emergency in 18 states to help with the shortages” [12]. DarkSide stole over 100 GB of data from the company, supposedly gaining access through a multitude of methods including “phishing, remote desktop protocol (RDP) abuse, and exploiting known vulnerabilities” [12]. A typical ransom demand from DarkSide amounts “anywhere between US$200,000 and US$2 million” [12], with this specific case’s ransom around $2 million. Although DarkSide threatened such a large American company, a post on their website suggests that they do not actually want to harm anyone. In fact, in October 2020, “DarkSide donates US$20,000 stolen from victims to charity” [12]. This may make the group seem like a modern version of Robin Hood stealing from the rich and giving to the poor. However, they still committed a crime and need to be punished for it.

One major challenge for detecting and preventing double extortion ransomware is detecting phishing emails among the normal emails. While phishing emails were already an issue before 2019, the dawn of COVID-19 has resulted in a lot of companies converting their work online. This means that more people are online and susceptible to clicking on phishing email links. “Common phishing emails have included links for advice or news regarding COVID-19, stimulus payments, vaccine scheduling, and other current events” [4]. New online users may not be familiarized with online threats and seeing links to information about current events could be enticing to click on. This issue has not been resolved yet because of the circumstances in which everyone moved online. COVID-19 swept around the world very quickly, and a lot of companies had to hurry to implement online strategies for their employees to work with. This left little time for employers to instruct their employees how to navigate the internet safely and how to be vigilant of phishing scam links. Suggested solutions to phishing emails include “technical controls to detect and inhibit malware … educational controls for employees to react effectively … [and] effective response planning” [4]. These protocols are no different than the protocols against phishing emails prior to COVID-19, but they must be prioritized even more now that there is an increased number of users online.

Another challenge to detecting and preventing double extortion ransomware is the use of Remote Desktop Protocol (RDP). Similar to phishing emails, remote access abuse has increased because of COVID-19 and the increase of users being online. “For many organizations during the pandemic it is the quickest way to provide remote access to internal resources” [5]. Unfortunately, opening the remote desktop connection directly on the internet could give ransomware attackers direct access to the victim’s desktop. “These connections exposed enterprises to brute-force and password-spraying attacks” [5]. A brute-force attack refers to an attacker submitting many passwords with the hope that they will eventually guess correctly. A password-spraying attack refers to the attacker using the one password on multiple different accounts before choosing a different password and repeating the entire process. In fact, brute-force attacks have increased so much that the “FBI has recently sent Private Industry Notifications to K-12 schools warning them about the risks of ransomware attacks leveraging open RDP connections” [5]. This challenge has not been resolved because using an RDP connection on the internet, while unsafe, is simple and fast. As mentioned above, a lot of users that are new to online work are not familiar with the need for secure practices online. If a remote desktop protocol is absolutely needed, a few suggestions would be to “limit access to those who really need it and use a mediation gateway to avoid exposing the system directly on the internet. As with VPNs, enforce multi factor authentication and network level authentication for RDP” [5]. However, if remote access is not required, it is suggested to “block access to the RDP ports (3389 TCP/UDP)” [5]. Other solutions may include updating systems as soon as new patches are released and assuring that passwords meet a certain standard.

A third challenge involved in detecting and preventing double extortion ransomware attacks is the slow meticulous way in which it takes over a network. Attackers “spend significant time conquering different parts of the victim’s network (a process that may take weeks or months) before they execute the ransomware payload, making such attacks look more like nation-state advanced persistent threat (APT) attacks instead of traditional ransomware incidents” [10]. By the time that the victim realizes that they are compromised, the attacker has been throughout their system for quite a bit of time. These attackers gain access to the victim’s network because of “weak credentials on exposed or externally facing services, and in some cases on critical vulnerabilities” [10]. Once within the system, the attacker can take advantage of their ability to laterally move without much resistance. The reason that this issue has not been resolved yet is because of its novelty and the fact that “operations like these are powered by evolved affiliate programs that give ransomware actors a hefty arsenal: customizable software, new and readily available technologies for better victim-targeting, and improved avenues for collaboration” [10]. One fairly new solution to this type of attack is the concept of zero trust security. “Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access” [6]. This increased authentication security technique makes it more difficult for attackers to move around a network even after they have gained initial access.

Yet another challenge involved in detecting and preventing double extortion ransomware comes with the fact that the attackers exploit software flaws in web applications to inject malicious codes and commands to download the ransomware into the victim’s devices and servers” [2]. Taking advantage of the vulnerabilities of these devices and applications allows the user to implement any code they want, which gives them complete control. The reason that this challenge has not mitigated yet is similar to the reason mentioned above for why slow meticulous attacks have not been resolved: the arsenal of programs that attackers have access to are constantly changing and are difficult to keep up with. One proposed solution is to “choose a reliable web application firewall to prevent web attacks, including those that inject malicious SQL scripts and JavaScripts into your applications and servers” [2]. Penta Security specifically recommends WAPPLES, “a logical web application firewall that uses machine learning technology to update its signature lists, designed for both on-premises and cloud environments” [2]. Other suggestions include keeping the software for the applications and devices up to date with the latest patches.

A fifth challenge involved in detecting and preventing double extortion ransomware attacks is the lack of ability to prevent the attackers from doxing the victim, even if the victim pays the ransom. “Victims can’t trust attackers to follow through and not post their stolen information. Not only that, but they don’t want to support the ransomware business model to begin with” [1]. This challenge gets amplified by the fact that these attackers are often very efficient at staying anonymous. Because these attackers cannot be identified, it is extremely difficult for authorities to catch and punish them. As a result, the attackers often publish the contents they stole even if they do get paid. For example, “In total, more than 2 TB of stolen data is currently being hosted on DarkSide sites, and 100% of victims’ stolen files are leaked” [12]. So not only are the victim’s confidential materials being published either way, but the victim is also funding the ransomware groups and likely contributing to future ransomware attacks if they pay their own ransom. The main way to prevent being in this situation is to prevent the double extortion attack from being successful in the first place. Cybereason offers its own solutions to help prevent these double extortion ransomware attacks from occurring, including Endpoint Controls, Intelligence Based-Antivirus, NGAV, Fileless Ransomware Protection, Behavioral Document Protection, Anti-Ransomware and Deception [1]. However, if someone is unfortunate enough to become the victim of one of these attacks, it is suggested not to deliver the ransom payment to the attackers. As mentioned previously, it is unlikely that the attacker will even deliver on their promises.

Even though there are many challenges that come with double extortion that have not been fully resolved yet, there are many suggested solutions that can be implemented to help alleviate the issue. A basic knowledge of how to prevent normal ransomware may be useful as well. Check Point Software Technologies Ltd suggests five strategies to prevent ransomware: Robust Data Backup, Cyber Awareness Training, Strong Secure Authentication, Up-to-Date Patches, Anti-Ransomware Solutions [3]. Ultimately, making sure that people are aware of these threats and are given basic knowledge on how to avoid and detect potential attacks is the best first step to preventing this dilemma.

References

[1] Cybereason Security Team. “Rise of Double-Extortion Shines Spotlight on Ransomware Prevention.” *Cybereason*, Cybereason, 14 Apr. 2021, www.cybereason.com/blog/rise-of-double-extortion-shines-spotlight-on-ransomware-prevention.

[2] “How to Defend Against Double Extortion Ransomware Attacks.” *Penta Security*, Penta Security Systems Inc., 2 July 2020, www.pentasecurity.com/blog/defend-double-extortion-ransomware-attacks/.

[3] “How to Prevent Ransomware Attack?” *Check Point*, Check Point Software Technologies Ltd, www.checkpoint.com/cyber-hub/threat-prevention/ransomware/how-to-prevent-ransomware/.

[4] Jordan, Andrew. “Double-Extortion Ransomware: Be Aware & Prepare.” *Wolf & Company, P.C.*, Wolf & Company, P.C., 2021, www.wolfandco.com/resources/insights/double-extortion-ransomware-be-aware-prepare/.

[5] Passeri, Paolo. “Double Extortion Ransomware Attacks and the Role of Vulnerable Internet-Facing Systems.” *Info Security Group*, Reed Exhibitions Ltd, 16 Sept. 2020, www.infosecurity-magazine.com/blogs/double-extortion-ransomware/.

[6] Pratt, Mary K. “What Is Zero Trust? A Model for More Effective Security.” *CSO*, IDG Communications, 16 Jan. 2018, www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.

[7] “Ransomware Evolved: Double Extortion.” *Check Point Research*, Check Point Software Technologies LTD, 16 Apr. 2020, research.checkpoint.com/2020/ransomware-evolved-double-extortion/.

[8] “Ransomware Evolved: Double Extortion and Fake Decryptor.” *Hong Kong Computer Emergency Response Team Coordination Centre*, HKCERT, 13 July 2020, www.hkcert.org/blog/ransomware-evolved-double-extortion-and-fake-decryptor.

[9] “Ransomware: The Data Exfiltration and Double Extortion Trends.” *Center for Internet Security*, CIS, 2021, www.cisecurity.org/blog/ransomware-the-data-exfiltration-and-double-extortion-trends/.

[10] Trend Micro Research. “MODERN RANSOMWARE'S DOUBLE EXTORTION TACTICS AND HOW TO PROTECT ENTERPRISES AGAINST THEM.” *Trend Micro*, Trend Micro Incorporated, 8 June 2021, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

[11] Trend Micro Research. “Ransomware Double Extortion and Beyond: REvil, Clop, and Conti.” *Trend Micro*, Trend Micro Incorporated, 15 June 2021, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

[12] Trend Micro Research. “What We Know About the DarkSide Ransomware and the US Pipeline Attack.” *Trend Micro*, Trend Micro Incorporated, 12 May 2021, www.trendmicro.com/en\_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.