Introduction

Ransomware attacks on critical infrastructure are part of a disturbing trend increasingly affecting global security. By 2020, ransomware attacks had exceeded between twenty thousand and thirty thousand per day in the United States alone. Costing victims an average of nineteen days of network downtime and a median payout of $230,000 per incident. “In 2021 global costs associated with ransomware recovery exceeded $20 billion” (Lubin A, 2022). The focus of this paper, Kaseya, is a service provider of IT management software and cloud servers. Providing VSA (Virtual Server/System Administrator) all-in-one software tools for Remote Monitoring and Management (RMM) enabling Managed System Providers (MSPs) to remotely administer clients’ IT systems (Kaseya). On July 2, 2021, Kaseya, was subject to a ransomware attack using techniques similar to the SolarWinds attack (Center for Internet Security). By exploiting a zero-day authentication bypass vulnerability within Kaseya’s VSA software, the attackers were able to distribute a malicious payload, propagating malware through managed service provider (MSP) clients to downstream organizations. The attack was estimated to have cost millions of dollars and affected up to 2,000 organizations globally. The attackers: ransomware-as-a-service (RaaS) group REvil demanded a $70 million payment in bitcoin in exchange for a decryption tool that could help victims recover from the attack. In response to the attack, the company issued a customer security advisory and was forced to shut down its VSA cloud and SaaS servers to contain the infection.

Notably, the attack triggered a public response from President Biden, following a wave of ransomware attacks attributed to cybercriminal groups like REvil based out of Russia and culminating in the Kaseya attack. Biden issued a warning to Vladimir Putin, stating that if the Russian government didn’t take action to disrupt ransomware groups operating in Russia, then the United States would be forced to act unilaterally against those groups to protect American interests. By July 13th REvil websites and associated infrastructure vanished from the internet (Fung et al.) and by the 23rd Kaseya announced it had received a universal decryptor tool for the REvil-encrypted files from a "trusted third party" enabling

victims of the attack to decrypt their files. With the third order effects of the ransomware attack in mind, the next section will discuss the technical details of the attack.

Technical Analysis

As mentioned in the previous section, REvil exploited 0-day vulnerabilities, to bypass the company authentication mechanisms, infiltrate their network and execute actions enabling their extortion scheme through end user file encryption. The next few paragraphs will detail important elements of the attack. Culminating with the encryption of organizational files and delivery of REvil's extortion demands.

The first phase of the attack involved a zero-day SQL injection vulnerability CVE-2021-30116 (NVD). Kaseya VSA 9.5.7 offered a client installation page at https://x.x.x.x/dl.asp. When downloaded for Windows OS and installed, the file KaseyaD.ini is generated (C:\Program Files (x86)\Kaseya\XXXXXXXXXX\KaseyaD.ini). Containing an Agent_Guid and AgentPassword This Agent_Guid and AgentPassword was used to log in on dl.asp (https://x.x.x.x/dl.asp?un=840997037507813&pw=113cc622839a4077a84837485ced6b93e440bf66d44057713cb2f95e503a06d9). Authenticating the attacker's client and returning a sessionId cookie used for services not intended for us by agents*dl.asp, allowing acceptance of credentials via a GET request. Ultimately allowing the attackers to bypass platform authentication and enabling escalation of privileges as a Managed Service Provider (MSP).

The attackers then used their elevated MSP privileges to deliver a malicious payload to approximately two thousand downstream clients through a file: agent.crt disguised as a software update: "Kaseya VSA Agent Hot-fix". Once downloaded and opened, the malicious payload: agent.crt executed a script through Windows Poweshell: "cmd.exe /c ping 127.0.0.1 -n 1543 > nul & C:WindowsSystem32WindowsPowerShellv1.0powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection

$true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:WindowsSystem32certutil.exe C:Windowscert.exe & echo %RANDOM% >>C:Windowscert.exe & C:Windowscert.exe -decode c:kworkingagent.crt c:kworkingagent.exe & del /q /f c:kworkingagent.crt C:Windowscert.exe & c:kworkingagent.exe" (Zscaler)

The installed script first executed the following command '127.0.0.1 -n 1543 > nul' establishing a script execution timer of 1543 seconds or approximately 25 minutes. Then the next section of the script displayed below, disabled Microsoft Windows Defender real-time protection, network protection, scanning of downloaded files, sharing of threat information with Microsoft Active Protection Service (MAPS), and automatic sample submission features.

"C:WindowsSystem32WindowsPowerShellv1.0powershell.exe Set-

MpPreference-DisableRealtimeMonitoring$true -DisableIntrusionPreventionSystem

$true-DisableIOAVProtection$true-DisableScriptScanning$true

EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -

Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend" (Zscaler)

It then created a copy of Windows certutil.exe with 'copy /Y C:WindowsSystem32certutil.exe C:Windowscert.exe & echo' and executed certutil.exe to decode the Base64 payload in the agent.crt file and save the decoded agent.exe in the target working directory using 'C:Windowscert.exe -decode c:kworkingagent.crt c:kworkingagent.exe'. The last section of the script 'del /q /f c:kworkingagent.crt C:Windowscert.exe & c:kworkingagent.exe' eliminated file agent.crt and the decipher while initiating the final phase of the attack. With agent.exe installed in the target working directory, it executed MsMpEng.exe, which is vulnerable to a DLL side-loading attack to load the REvil ransomware DLL file

mpsvc.dll located in the same directory. “Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process.” (MITRE)

With the library opened, execution of network discovery to identify hosts and follow on encryption of files located on those devices was executed. With a readme.txt ransom note copied into every directory and adding the content to a file from the image configuration value in the Windows %temp% directory, setting the infected systems wallpaper to use this file. The result of this attack was a 19-day shutdown of Kaseya’s VSA cloud and SaaS Servers and as of July 21, 2023, it is still not clear how long it would have taken Kaseya to restore services to its 2,000 affected customers without the universal decrpytor key delivered to the company on the 23rd of July, 2021.

Social Effects of Ransomware

The concept of extorting money from individuals is nothing new. But, with the advent of the internet increasing the interconnected nature of our global economy and society. The growth of ransomware as a highly lucrative criminal enterprise, scope, and magnitude of the damage these threat actors can and will do should not be underestimated. The US Treasury’s Financial Crimes Enforcement Network reported that ransomware payments by US victims rose to $1.2 billion in 2021 (FinCEN). This is only a small percentage of the actual figure, due to the numbers of victims who do not report these attacks to relevant authorities. So, it comes as no surprise that the financial, rather than social impact of ransomware attacks, receives the most coverage. This means that cybersecurity professionals, journalists and researchers need to do a better job in

articulating the broader costs of ransomware for national security, societal resilience, and individual informational privacy. Within the next few paragraphs, the consequences of ransomware attacks against services essential to a functioning society: healthcare, education and local government services will be discussed.

Access to healthcare services or lack thereof has direct correlations to increased infant and adult mortality rates, increasing chances that individuals will die from preventable and treatable illness, therefore disruptions to healthcare resources can have debilitating effects. This means that ransomware attacks can create grave consequences for healthcare services and patients: cancelled operations and chemotherapy sessions, diverted emergency services, and even deaths. According to a lawsuit filed in Alabama, a newborn baby ended up with severe brain injury because doctors were prevented from accessing information that would have detected the baby's umbilical cord was wrapped around the fetus' neck, due to an ongoing cyber-attack. Leading to brain damage at birth and subsequent death nine months later (Koplowitz Howard). Another example is the 2020 death of a women in Germany who died from an aortic aneurysm while being transported twenty miles from University Hospital Düsseldorf to a hospital in Wuppertal. All because of a ransomware attack that encrypted the hospital network, forcing them to turn the ambulance away and delaying the patient's treatment by an hour (Ralston).

These incidents are particularly troublesome when considering how vulnerable healthcare is to ransomware attacks in light of the sector's lack of cyber security maturity, reliance on digital infrastructure and continuous operations. But it is not the only critical service experiencing an increase in ransomware attacks. Educational institutions are also frequently subject to ransomware, as they are comparatively easy targets. According to Microsoft, educational organizations have been the target of more than 6.1 million malware attacks within

the last thirty days, while the second-most affected industry (business and professional services) has only seen 900,000 attacks (Microsoft). Disrupting network access required for distance or in person classroom instruction. Often these attacks target organizations that are conducting research where the data is highly confidential or focused on gaining unauthorized access to confidential and personally identifiable information (PII), which can contain financial details, names, addresses and Social Security numbers. This can lead to identity theft and lawsuits by students and faculty, against the schools, for the data breach or failure to remediate the damage afterword's. For example, a West Coast university was the victim of a ransomware attack involving data stored within their medical research department's network. Realizing hackers had encrypted valuable research data, the school chose to pay the $1.14 million in cryptocurrency and received a decryption key. However, only 2% of education organizations that paid the ransom were able to recover all their data.

The third and final service essential to society is local government services. Disruptions in police, sanitation, water treatment and mass transit can seriously affect public safety. In December 2019 New Orleans suffered a ransomware attack in which Cybercriminals crippled the city's systems, with more than 4,000 computers affected by the cyberattack. Emergency response, Police communications and city services were disrupted, taking over thirty days to restore. In March of 2021 cybercriminals used unknown ransomware to target a water facility in Nevada. The malware affected SCADA and backup systems. Another incident occurred in July of that year, at a facility in Maine. Hackers deploying the ZuCaNo ransomware, (CISA) which infected a wastewater SCADA computer. The treatment system was forced to run manually until the SCADA computer was restored using local control. The third attack took place in August. Extortionists, deploying ransomware on the systems of a water plant in California, were able to

infect three SCADA servers. With the infections discovery a month after the initial breach. These attacks against local infrastructure threaten emergency services, diminish law enforcement capabilities, and cripple Water and Wastewater facilities effectiveness to provide clean, potable water and effectively manage the wastewater of their communities. Each of the previous examples pose unacceptable risks to public safety and welfare. But they also undermine trust in local, state, and federal entities capability to provide stable services and call into question their ability to protect essential services from organized cybercriminal groups.

In closing, Ransomware attacks represent an unacceptable risk to our economy, healthcare and critical infrastructure providing essential services. In 2021 the Department of Homeland Security designated Ransomware a national security threat. As such, it can be argued that these groups should be subject to the same military and law enforcement efforts applied to organizations on the terror watch list. Additionally, more needs to be done to convince individuals and corporate entities that timely reporting and information sharing with relevant government entities is in both their best interest and the long-term interests of the country's security.

Works Cited

Lubin, A. (2022, August 6). The law and politics of Ransomware. SSRN. Retrieved April 7, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4181964/ .

"The Solarwinds Cyber-Attack: What You Need to Know." *CIS*, 9 Nov. 2021, https://www.cisecurity.org/solarwinds/ .

Kaseya, https://www.kaseya.com/wp-content/uploads/dlm_uploads/2022/08/Kaseya-Product-Brief-Manage-Automate-All-IT-VSA.pdf/

Fung, Brian, et al. "Ransomware Gang That Hit Meat Supplier Mysteriously Vanishes from the Internet | CNN Business." CNN, Cable News Network, 14 July 2021, www.cnn.com/2021/07/13/tech/revil-ransomware-disappears/index.html.

NVD, nvd.nist.gov/vuln/detail/CVE-2021-30116. https://nvd.nist.gov/vuln/detail/CVE-2021-30116

"Kaseya Supply Chain Ransomware Attack: Zscaler Blog." *Zscaler*, www.zscaler.com/blogs/security-research/kaseya-supply-chain-ransomware-attack-technical-analysis-revil-payload.

"Hijack Execution Flow: DLL Side-Loading." Hijack Execution Flow: DLL Side-Loading, Sub-Technique T1574.002 - Enterprise | MITRE ATT&CK®, https://attack.mitre.org/techniques/T1574/002/ . Accessed 21 July 2023.

FinCEN Ransomware Advisory, www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

hkoplowitz@al.com, Howard Koplowitz |. "Alabama Mom Claims Baby Died Because of Undisclosed Cyberattack, Fights for Hospital Records." Al, 1 Oct. 2021, www.al.com/news/2021/10/alabama-mom-claims-baby-died-because-of-undisclosed-cyberattack-fights-for-hospital-records.html#:~:text=An%20Alabama%20mother%20filed%20a%20wrongful%20death%20suit,involved%20in%20the%20incident%2C%20according%20to%20court%20records.

Ralston, William. "The Untold Story of a Cyberattack, a Hospital and a Dying Woman." WIRED UK, 11 Nov. 2020, www.wired.co.uk/article/ransomware-hospital-death-germany

"Cyberthreats, Viruses, and Malware - Microsoft Security Intelligence." Microsoft, www.microsoft.com/en-us/wdsi/threats

"Ongoing Cyber Threats to U.S. Water and Wastewater Systems: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 20 July 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a