Cybersecurity and Information Security Newsletter

Issue 13 | December 6, 2021

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

Law enforcement agencies announce the arrest of ransomware suspects and asset forfeiture action

On November 8, 2021, the U.S. Department of Justice published unsealed indictments against Yaroslav Vasinskyi (Vasinskyi), a Ukrainian national, and Yevgeniy Polyanin (Polyanin), a Russian national, for their alleged role in deploying the Sodinokibi/REvil ransomware to initiate cyber attacks, including one involving Kaseya VSA software in July 2021. *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya*, available here. The Department also announced the seizure of $6.1 million in funds from an account on FTX Trading Limited, a cryptocurrency exchange incorporated in Antigua and Barbuda, in the name of Evegnii Igorevich Polianin and Evgeniy Igorevich Polyanin. *Warrant to Seize Property Subject to Forfeiture (Case No. 3:21-MJ-888BT)*, available here; *see also Jurisdiction, regulations, licensing, and practices*, available here. It alleges that these funds are traceable to ransom payments received by the Sodinokibi/REvil ransomware gang.

On October 8, 2021, Vasinskyi was arrested by Polish authorities at a border crossing in Dorohusk, Poland. *US seeks extradition of alleged Ukrainian scammer arrested at Polish border stop*, available here. Currently, he is still under Polish custody, likely pending extradition to the United States. At the time of publication, Polyanin is believed to be outside the United States and at large.

Both Vasinskyi and Polyanin are charged with (1) conspiracy to commit fraud and related activity in connection with computers, (2) intentional damage to a protected computer, and (3) conspiracy to commit money laundering. *Polyanin Indictment*, available here; *Vasinskyi Indictment*, available here.

In addition, Romanian authorities arrested two unnamed suspects for allegedly having ties to Vasinskyi and Polyanin for deploying the Sodinokibi/REvil ransomware across businesses and government IT systems between 2019 and 2021. *Five Affiliates To Sodinokibi/Revil Unplugged*, available here. Currently, the two unnamed suspects under Romanian custody have not yet been charged by the Department of Justice.

These arrests and the asset forfeiture came as a result of international law enforcement cooperation among 17 countries, Europol, Eurojust, and INTERPOL. *Five Affiliates To Sodinokibi/Revil Unplugged*, *supra*.

Analysis

Ransomware is a malicious program that surreptitiously encrypts data on a computer system. *Ransomware 101 (CISA),* available here. After the encryption operation is complete, the threat actor extorts the system owner to pay a ransom via cryptocurrency to decrypt encrypted files. Because cryptocurrency transactions are typically irreversible, ransomware threat actors are guaranteed to receive the ransom payment. On the other hand, victims are not always guaranteed to receive the decryption tools even after sending the ransom payment.

U.S. agencies discourage paying ransom to threat actors. *Ransomware (FBI)*, available here; *CISA And FBI Urge Organizations To Remain Vigilant To Ransomware Threats On Holidays, Including This Labor Day (CISA)*, available here. In fact, certain U.S. agencies have warned of potential criminal and civil liabilities for ransom payments. For example, on September 21, 2021, the Office of Foreign Assets Control of the U.S. Department of Treasury published

an updated advisory on potential sanction risks for facilitating ransom payments to sanctioned individuals. *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, available here. Because threat actors use modern encryption methods to encrypt the victim's files, only the threat actors have the necessary means (e.g., encryption key) to unlock the files *initially*. With government agencies discouraging ransomware payments, victims may feel stuck in not being able to resolve the situation. Ignoring these government advisories, some well-known ransomware victims have paid the ransom to restore system access. *E.g., Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, available here.

Inter-governmental action against the Sodinokibi/REvil ransomware gang demonstrates law enforcement's ability and willingness to commit swift action against cyber crime actors, even if sophisticated technologies, such as modern-day encryption and cryptocurrency, are used to facilitate the crime. U.S. Attorney General Merrick Garland noted that "[t]he United States, together with our allies, will do everything in our power to identify the perpetrators of ransomware attacks, to bring them to justice and to recover the funds they have stolen from the American people." *Attorney General Merrick B. Garland, Deputy Attorney General Lisa O. Monaco and FBI Director Christopher Wray Deliver Remarks on Sodinokibi/REvil Ransomware Arrest*, available here. FBI Director Christopher Wray specifically remarked that the FBI's investigation into the Kaseya attack yielded "a usable decryption key that allowed [the agency] to generate a capability to unlock Kaseya customers' data."

In early July 2021, when the Sodinokibi/REvil ransomware gang attacked Kaseya's systems, Huntress Labs, a third-party cybersecurity firm, reached out to Kaseya to alert the company to the ongoing cyber incident. *See Cybersecurity and Information Security Newsletter – Issue 9*, available here. Kaseya swiftly took action to contain the damage and notify law enforcement agencies, including the FBI. By notifying the FBI of the cyber incident early, Kaseya benefited from a coordinated response by both law enforcement and intelligence agencies to hold threat actors accountable for their actions. Without paying the ransom, Kaseya was able to acquire the decryption tool needed to unlock customers' files.

Based on the unsealed indictments, federal law enforcement moved swiftly to identify the Sodinokibi/REvil ransomware members and obtain grand jury indictments only nearly a month after the Kaseya ransomware incident was discovered. The swift pace of law enforcement action highlights the effectiveness of the newly established Ransomware and Digital Extortion Task Force at the U.S. Department of Justice. *See Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion*, available here.

Although other ransomware gangs may adjust their tactics to extort victims more successfully (e.g., threatening to leak sensitive stolen data unless a ransom is paid), or hide collected ransom payments more effectively (e.g., exclusively utilizing cryptocurrencies with enhanced privacy features), ransomware victims should be proactive by promptly contacting federal authorities to engage their assistance and resources. Furthermore, businesses and individuals should always utilize best practices in regularly backing up data. *The 3-2-1 Backup Strategy*, available here. Finally, ransomware victims should be wary about paying ransom to threat actors. Even if threat actors help decrypt encrypted files, ransom-paying victims may face legal liability stemming from the ransom payment. For example, if the ransomware threat actors happen to be members of a U.S. sanctioned organization, paying the ransom will

violate federal sanctions regulations. *See, e.g., Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, *supra*.

Compromised Google Cloud Platform used by threat actors to mine cryptocurrency at others' expense

Last month, Google published its first Google Cybersecurity Action Team Threat Horizons report (Report), in which it identified cyber threats emerging from cloud platforms. *Illicit coin mining, ransomware, APTs target cloud users in first Google Cybersecurity Action Team Threat Horizons report*, available here. The Cloud or cloud platform refers to an Information Technology (IT) system that provides on-demand provisioned resources (e.g., data storage, network transfer, CPU/GPU processing) to users without the need for direct active management. *What is cloud computing?*, available here. Unlike traditional IT systems, cloud platforms reside in a real-time virtual environment managed among different servers in various locations. Google Cloud Platform is managed by Google's IT infrastructure. *Google Cloud*, available here. Among many observed threats, the Report noted that threat actors have accessed compromised Google Cloud instances to conduct malicious activities, mainly mining cryptocurrencies.

According to the Report, threat actors took advantage of poor consumer security practices (e.g., having no or weak passwords) or vulnerable third-party software. *Threat Horizons, Cloud Threat Intelligence (November 2021, Issue 1)*, available here. They used automated means to scan for vulnerable Google Cloud Platform accounts and then deploy programs to those compromised accounts to initiate their malicious activities. According to Google's Cybersecurity Action Team, 86% of the compromised Cloud accounts were used for cryptocurrency mining, followed by 10% of the accounts used to scan for other cyber targets on the web, and 8% of the accounts used for launching cyber attacks against other targets on the Internet. (Note, totals of the percentages exceed 100% because some of the compromised instances were used for multiple purposes.)

The Google Cloud Platform is a service for which customers pay a fee. Therefore, threat actors take advantage of compromised cloud accounts to pursue malicious activities at the customers' expense. Certain Cloud features, such as cloud graphical unit processing, are expensive resources, and threat actors use them to accelerate their cryptocurrency mining operation.

The Report recommends that Cloud customers employ good cyber hygiene (e.g., multi-factor authentication), and take advantage of all the cloud security features the platform has to offer in order to mitigate threats.

Analysis

During the late 1990s and early 2000s, software piracy groups used various technical means to identify and hijack vulnerable but resource-rich systems on the Internet. *WAREZ All My Disk Space?*, available here. They aimed to use compromised systems to act as an online file storage server (e.g., FTP server) to upload and distribute pirated digital content (software and

media), also known as WAREZ. These threat actors took advantage of the large disk storage space and the high-speed network connection of compromised systems to publish the group's pirated content. In essence, WAREZ piracy groups took advantage of others' system resources to pursue their malicious activities.

Although cloud platforms offer novel on-demand resources for IT managers and developers, the threat landscape has not significantly changed. Poor cyber hygiene and vulnerable software can easily open up opportunities for threat actors to hijack cloud computing accounts. Unlike a few decades ago, however, threat actors can convert stolen cloud computing resources into financial funds in the form of cryptocurrency. By utilizing stolen cloud resources towards cryptocurrency mining operations, threat actors can financially profit at the cloud account holders' expense.

In addition to practicing good cyber hygiene, especially when logging into cloud computing accounts, proactive resource monitoring may provide early sign detection of threat actors maliciously using stolen cloud computing resources. If cloud computing account holders suspect that certain resources are being used abnormally, that may be an indication that an unauthorized program is utilizing cloud resources. *See, e.g., Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks (COVA CCI)*, available here.

Given that cloud computing resources are valuable threat actor targets, cloud computing account holders should consider a more assertive posture to safeguard cloud IT resources. With threat actors utilizing automated tools to scan and infiltrate cloud computing accounts, it is only a matter of time before threat actors initiate their attempts to infiltrate targeted cloud accounts. As such, cloud computing account holders should be vigilant in guarding their cloud resources (e.g., implementing multi-factor authentication and monitoring cloud resources regularly) or face the risk of threat actors hijacking them.