# Cybersecurity and Information Security Newsletter

Issue 9 | August 9, 2021

**Table of Contents**

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

## Threat Actors conduct a series of Supply Chain attacks against Kaseya VSA software to spread ransomware to thousands of businesses

On July 2, 2021, cybersecurity firm Huntress Labs Inc. (Huntress Labs) announced that several Managed Service Providers (MSPs) utilizing Kaseya VSA software were compromised by ransomware, which affected at least 1,000 businesses worldwide. *Crticial [sic] Ransomware Incident in Progress*, available here. It discovered that threat actors used Kaseya VSA software as an attack vector to spread ransomware across networks. Huntress Labs reached out to Kaseya, an information technology (IT) company, to share threat intelligence and posted its findings on social media to inform other MSPs of the ongoing threat incident. Kaseya provided around-the-clock updates to inform its customers, and it published a security update on July 11, which addressed the security vulnerability used by these threat actors.

### Background

An MSP is a third party that assumes responsibility and control of day-to-day operations for IT infrastructure management for its customers. *What is a Managed Service Provider (MSP)?*, available here. MSPs use remote monitoring software, such as Kaseya VSA, to manage simultaneously thousands of IT systems which may include a combination of servers, desktop/laptop computers, printers, and other network devices. *Kaseya VSA*, available here.

Kaseya specializes in developing tools for managing IT infrastructure. *About Kaseya*, available here. Kaseya VSA (Virtual System/Server Administrator) is a remote monitoring and management software used primarily by MSPs. *Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware*, available here. Kaseya VSA is available as a Software-as-a-Service (SaaS) or as an on-premise server. *Kaseya VSA Supply Chain Cyberattack Details, RMM Recovery Timeline*, available here.

According to Huntress Labs, on July 2, 2021, at around 11 AM EST, several Kaseya VSA servers were used by threat actors to deploy ransomware. Threat actors exploited an arbitrary file upload (allowing threat actors to upload malicious code to a system) and code injection vulnerability (allowing threat actors to inject malicious code into a program that executes the malicious code) in Kaseya VSA software to upload and execute malicious code while bypassing security protocols. The malicious exploits enabled threat actors to take control of the compromised Kaseya VSA servers. They were also able to take direct control of thousands of business customers' IT systems. Threat actors installed ransomware on all accessible systems, which disrupted business operations among MSP customers.

After detecting a potential intrusion incident in progress, Huntress Labs contacted Kaseya to alert and share intelligence. In short order, both companies were collaborating, while Kaseya made the unprecedented decision to unilaterally shut down in-house managed Kaseya VSA servers. After publicizing the threat incident, Kaseya initiated an investigation to identify the threat and create an appropriate software patch to address any identified vulnerability.

Huntress Labs reached out to the MSP social media community to share the company's latest findings and aid those affected by the threat incident. *Crticial [sic] Ransomware Incident in Progress*, *supra*. Because threat actors were continuously deleting all traces of their activities by erasing system logs, Huntress Labs asked the MSP community to share any server logs from a compromised system. Through community effort, Huntress Labs collected enough evidence to determine the potential methodology used by the threat actors and even create a proof of concept of the intrusion.

On July 11, 2021, Kaseya released a software patch for MSPs using on-premise Kaseya VSA servers, and the company also applied the patch to its SaaS VSA infrastructure. *Important Notice July 29th, 2021*, available here. After reviewing the patch, Huntress Labs confirmed that the patch addressed the intrusion vulnerability, reassuring the MSP community that threat actors could no longer use the same intrusion method to hijack Kaseya VSA servers. *Crticial [sic] Ransomware Incident in Progress*, *supra*.

Although threat actors no longer had the means to hijack Kaseya VSA servers, the aftereffects of ransomware disrupted thousands of businesses' IT infrastructure. Based on screenshots of ransom notes, threat actors were open to accepting both Bitcoin and Monero as the means of payment for each compromised system of a business customer. Additionally, threat actors were open to releasing a universal decoder that could decrypt all files for every Kaseya victim in exchange for $70 million. *Hackers demand $70 million to unlock businesses hit by sprawling ransomware attack*, available here.

The REvil ransomware group has been identified as the threat actor behind the Kaseya attack. *Agent REvil Unveiled in Kaseya VSA Ransomware Attack,* available here. Earlier this year, this group was responsible for conducting a series of ransomware attacks and potential data infiltration attacks against JBS, one of the largest food processing companies in the world. *JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified*, available here. JBS was forced to halt meat processing operations in the US as a result of the cyber attack.

**Analysis**

When a cyber attack is underway, transparency is key to share intelligence and coordinate an incident response plan to mitigate the effects of the attack. When Huntress Labs received intelligence of a possible cyber attack against Kaseya VSA servers, it immediately reached out to Kaseya, which resulted in a Zoom call within a few minutes. *Rapid Response: Mass MSP Ransomware Incident*, available here. Although the ransomware may have impacted thousands of businesses, the quick intelligence-sharing may have severely limited the scope of the attack.

The debate on whether victims of ransomware attacks should pay demanded ransoms has been ongoing. The Federal Bureau of Investigation does not recommend paying a ransom to threat actors because it may encourage them to conduct further ransomware attacks. *Ransomware: What is it & What to do about it*, available here. Moreover, paying a ransom does not guarantee that threat actors will follow through with their promise to decrypt affected files.

With respect to ransom payments, threat actors behind the Kaseya attack have demonstrated one troubling trend—they now accept Monero cryptocurrency as a mode of payment. This is significant because, unlike Bitcoin, Monero has enhanced privacy features. With Bitcoin, all transaction records are observable by any third party, which helps law enforcement to track Bitcoin payments back to threat actors. With Monero, on the other hand, all transactions are confidential and untraceable, which means transaction records are not viewable by third parties. *What is Monero (XMR)*, available here. Monero's privacy features obstruct law enforcement's ability to monitor ransom payments, which may hamper investigating the real identities of ransomware threat actors.

Monero has not been adopted widely by major cryptocurrency exchanges, thereby preventing ransomware victims from purchasing it as a means of payment transfer. As such, it is currently unlikely that ransomware threat actors would demand ransom via Monero or other not-well-known privacy-centered cryptocurrencies. However, this issue should be monitored on the horizon as ransomware threat actors adapt to maintain their profitable venture.

## NSO Group's Pegasus spyware allegedly used against non-criminal civilians and journalists worldwide

According to an investigation by various media organizations and Amnesty International, an Israeli technology firm, NSO Group, was responsible for developing military-grade spyware, identified as *Pegasus*, that was allegedly used to infiltrate smartphone devices of journalists, human rights activists, elected leaders, and other non-criminal civilians around the world. *Takeaways from the Pegasus Project*, available here. Spyware refers to a malicious program that is designed to secretly observe activity on a device and send those observations to a third party. *What is spyware? How it works and how to prevent it*, available here. Evidence from the investigation indicates that NSO Group's spyware was used extensively to conduct a worldwide surveillance program, although it is unclear who or what entities initiated the alleged attacks.

The investigation began when the Paris-based journalism nonprofit Forbidden Stories and Amnesty International accessed allegedly leaked documents that list more than 50,000 phone numbers collected for NSO Group's surveillance program. An initial examination of the list revealed phone numbers of "at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials—including cabinet ministers, diplomats, and military and security officers". *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, available here.

The list also appeared to have timestamps of when an alleged surveillance attempt was made against a targeted phone number. The Washington Post notes that ". . . forensic analysis of the 37 phones shows that many display a tight correlation between time stamps associated with a number on the list and the initiation of surveillance attempts, in some cases as brief as a few seconds." *Takeaways from the Pegasus Project*, *supra*. Forbidden Stories and Amnesty International shared the leaked list to other media organizations to promote further research into NSO Group's surveillance program.

As of the publishing of this newsletter, the purpose of the list is unknown as well as whether *all* the phone numbers on the list were spied upon. *The Cybersecurity 202: The Pegasus Project raised the curtain on a vast spyware network. Here are four takeaways*, available here.

To check evidence of Pegasus spyware, Amnesty International's Security Lab (Security Lab) performed a forensic examination on 37 smartphones, both iOS and Android devices, whose numbers were on the list of 50,000 numbers. The Security Lab found that Pegasus spyware used a combination of network injection attacks (where threat actors attempt to inject malicious code within the data stream between the smartphone and another network of computers, e.g., the Internet) and zero-day vulnerabilities to install malicious spyware on the victim's device. *Forensic Methodology Report: How to catch NSO Group's Pegasus*, available here. It is worth noting that some of Pegasus' intrusion techniques did not use typical attack vectors, such as an email attachment. Instead, Pegasus employed vulnerabilities that would silently hijack the smartphone without the need for the user to inadvertently intervene for the spyware to install itself on the device. Victims would not know that their device was already compromised by Pegasus.

By examining system logs of infected devices, the Security Lab identified a network of servers NSO Group allegedly used to facilitate the surveillance spying operations. It is worth noting that some of these servers are hosted in the US. The phone's system logs also provided timestamps of the spyware's activity, which coincided with the timestamps of initiation of surveillance attempts against the particular device based on allegedly leaked NSO Group documents.

**NSO Group's Response**

According to NSO Group, the company's products "are used exclusively by government intelligence and law enforcement agencies to fight crime and terror." *About Us*, available here. The company claims that its "technology has helped prevent terrorism, break up criminal operations, find missing persons, and assist search and rescue teams." *Id.*

NSO Group maintains that claims made by unnamed sources to Forbidden Stories were based on "misleading interpretation of data from accessible and overt basic information, such as HLR Lookup." *Following The Publication Of The Recent Article By Forbidden Stories, We Wanted To Directly Address The False Accusations And Misleading Allegations Presented There*, available here. The company claims that the 50,000 list "is not a list of targets or potential targets of Pegasus" nor is the list related to NSO Group. *Enough Is Enough!*, available here. It states that information held by Forbidden Stories was not leaked from NSO Group's servers because "such data never existed on any of our servers." *Following The Publication Of The Recent Article By Forbidden Stories, supra.*

Maintaining the falsity of the Pegasus Project reporting, the company emphasized that it "sells technologies solely to law enforcement and intelligence agencies of vetted governments," and NSO Group does not operate the surveillance system and has no access to the system's data. *Id.* The firm also claimed that smartphones with a U.S.-based phone number (starting with a +1 international code) or foreign smartphones in the U.S. could not be targeted by the Pegasus spyware because it is "technologically impossible" in the words of NSO's spokesperson. *Key question for Americans overseas: Can their phones be hacked?*, available here.

**Analysis**

Federal law generally protects the privacy of communications in transit and at rest. Title I of the Electronic Communications Privacy Act (ECPA) prohibits the intentional interception, attempted interception, or procurement of other persons to intercept of any wire, oral, or electronic communications. 18 U.S.C. § 2511(1)(a), available here. Title II of the ECPA prohibits intentional access without authorization to a facility where electronic communication service is provided to obtain, alter, or prevents authorized access to a wire or electronic communication. 18 U.S.C. § 2701(a), available here.

In essence, Title I of the ECPA protects the privacy of communications *in transit*, while Title II of the ECPA protects the privacy of communications stored *at rest* by service providers. Electronic Communications Privacy Act of 1986 (ECPA), available here. The ECPA provides certain exceptions for government entities (to facilitate law enforcement activities with an approved court order) and identified private entities (to maintain certain business practices).

Amnesty International's Security Lab determined that NSO Group allegedly employed U.S.-based servers to facilitate the surveillance operation. Assuming that this is the case, NSO Group's activities through servers in the U.S. would fall under U.S. jurisdiction. If NSO Group did not obtain proper consent or court order to conduct its alleged spyware campaign, then it would be liable under the ECPA for unlawfully accessing communications in transit and at rest from victims' devices.

U.S. Attorneys of the Department of Justice have a history of prosecuting individuals for unlawfully utilizing spyware against victims. *See, e.g., Man Pleads Guilty for Selling "StealthGenie" Spyware App and Ordered to Pay $500,000 Fine*, available here. For example, on January 10, 2018, a federal grand jury indicted Phillip R. Durachinsky of various illegal wiretap charges for installing spyware on computers used by minors. *United States of America v. Durachinsky, Indictment, Case: 1:18-cr-00022-SO*, available here. As of August 9, 2021, the U.S. District Court for the Northern District of Ohio has not yet scheduled a jury trial. If NSO Group did not have a valid legal basis for allegedly operating part of their Pegasus Project in the U.S., then it may face criminal charges for violating U.S. wiretap laws.

The reporting by Forbidden Stories, Amnesty International, and other media outlets suggests a rampant actor utilizing advanced intrusion techniques to install malware and spy on victims' smartphone devices. By NSO Group's own admission, the company provides advanced spyware technologies to vetted law enforcement and government entities around the world.

However, there is a lack of attribution as to whether NSO Group was the principal actor in using Pegasus spyware to conduct a worldwide surveillance operation. It is possible that a different actor may have used NSO Group's technologies, including software and technical know-how, to conduct surveillance operations on its own. It may also be possible that a said actor may have stolen NSO Group's technologies to perform unsanctioned surveillance operations as well. Finally, a legitimate customer of Pegasus spyware may be behind the alleged surveillance campaign.

Even if NSO Group did not actively participate in any surveillance activities, the Computer Fraud and Abuse Act (CFAA) criminalizes knowingly transmitting "a program, information, code, or command, and as a result of such conduct, *intentionally causes damage without authorization*, to a protected computer." 18 U.S.C. § 1030(5)(A) (emphasis added). Therefore, the transmission of malicious code knowingly, potentially including spyware, may incur criminal liability. *See Intl. Airport Centers, L.L.C. v. Citrin,* 440 F.3d 418 (7th Cir.

2006), available here (abrogated by *Van Buren v. U.S.,* 141 S. Ct. 1648 (2021), available here).

There are policy implications for allowing an authorized industry of spyware development to assist law enforcement operations. From the legal perspective, subject to the recent U.S. Supreme Court ruling in *Van Buren* (covered in Issue 8 of the newsletter) and other potential legal exemptions, NSO Group may not be allowed to transmit its spyware technologies in the U.S. due to CFAA. It should be noted, however, NSO Group was never prosecuted by U.S. authorities for spyware transmission.

Furthermore, authorizing spyware development may create a conflict of interest in cybersecurity policy. Should the U.S. government promote the sharing of information about discovered vulnerabilities to create a more resilient cybersecurity landscape, or should certain vulnerabilities be guarded against public knowledge to be exploited for law enforcement and national security purposes?

A proactive response by government entities is required to resolve the ethical and policy dimensions of authorizing spyware development by private entities and clarifying the legality of allowing such practice. Currently, sanctioned spyware *development* by private actors resides within the murky grey area of law and policy.