KOVRR
Cyber Risk Modeling

www.kovrr.com

A Summer of Exploits

JULY 2021

Over the past few weeks several dramatic vulnerabilities were exposed in different ubiquitous products and platforms, including the Microsoft Windows OS, the Solarwinds Serv-U Managed File Transfer and Serv-U Secure FTP products, and Kaseya's services.

JUNE 8th
Microsoft published a patch for CVE-2021-1675 (a vulnerability in the Windows Print Spooler service)[1] nicknamed "PrintNightmare"

JUNE 21st
Microsoft's "PrintNightmare" patch notice was updated to indicate a critical severity and a potential for remote code execution (RCE) as well as local privilege escalation (LPE)

JUNE 29th
A PoC of a successful exploitation of "PrintNightmare" was published

JULY 1st
Another, separate, RCE vulnerability in Windows Print Spooler was published[2]

JULY 2nd
Kaseya's clients suffered a supply-chain ransomware attack[3]

JULY 4th
CISA released a public alert about the Kaseya attack[4]

JULY 5th
Kaseya CEO claimed that between 800 and 1,500 businesses around the world have been affected by a ransomware attack centered on the U.S.[5]

JULY 6th
Microsoft released an out-of-band patch for the second "PrintNightmare"

JULY 7th
Reports of Microsoft's patch being incomplete are released meaning the patch can be bypassed[6]

JULY 9th
SolarWinds announce that Microsoft discovered a zero-day vulnerability in some of SolarWinds products was exploited

JULY 10th
SolarWinds has developed a patch to fix a Serv-U Managed File Transfer Server and Serv-U Secure FTP vulnerability[8]

JULY 11th
Kaseya's SaaS-based VSA platform began a re-activated with security enhancements[9]

JULY 13th
REvil group's dark-web websites and servers disappeared without explanation

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
3. https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021
4. https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
5. https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/
6. https://arstechnica.com/gadgets/2021/07/microsofts-emergency-patch-fails-to-fix-critical-printnightmare-vulnerability/
7. https://arstechnica.com/gadgets/2021/07/microsoft-discovers-critical-solarwinds-zero-day-under-active-attack/
8. https://www.msspalert.com/cybersecurity-breaches-and-attacks/solarwinds-alerted-by-microsoft-patches-serv-u-vulnerability/
9. https://www.scmagazine.com/kaseya-cyberattack/kaseya-restores-vsa-services-shelved-after-ransomware-row/

Summary of the Events

Kaseya

What happened?

On July 2nd, a cyber attack was launched against the IT solutions company Kaseya.

Kaseya provides IT solutions including VSA, a unified remote-monitoring and management tool for handling networks and endpoints. In addition, the company provides compliance systems, service desks, and a professional services automation platform to over 40,000 organizations worldwide.

The cyberattack has been attributed to the REvil/Sodinikibi ransomware group whose ransomware was first detected in April 2019. The group's usual propagation method is phishing emails containing malicious links. Some of the group's most prominent victim industries in the last two years were healthcare facilities and local governments.

REvil has offered a decryption key, allegedly universal - able to unlock all encrypted systems, for the 'bargain' price of $70 million via bitcoin (BTC) cryptocurrency.

On July 13th, all of REvil's online activity stopped and the groups data-dump websites were shut down without further information, leaving the victims of their latest attacks hostage with encrypted files and no valid payment address or decryption keys.

Who was impacted?

On July 2nd Kaseya claimed that the attack affected only a small number of on-premise clients, In a press release published on July 5th the company estimated that the number of clients impacted by the attack is between 800 and 1500 businesses.

PrintNightmare

What happened?

On June 8th, Microsoft published a CVE advisory for a vulnerability in the Windows Print Spooler service which is enabled by default in all Windows clients and servers across almost all modern Windows versions. This vulnerability was initially categorized as a low severity local privilege escalation (LPE) vulnerability by Microsoft and a patch for it was released on June 21st. A week later, researchers published a successful PoC of the exploitation and claimed that the vulnerability is in fact a high severity RCE and PE vulnerability.

On July 1st, a separate vulnerability in the same Windows Print Spooler service was discovered, similar to the first vulnerability, this new “PrintNightmare’’ was also a RCE and LPE vulnerability that would allow attackers system privileges with which they could install programs; view, change, or delete data; or create new accounts with full user rights.

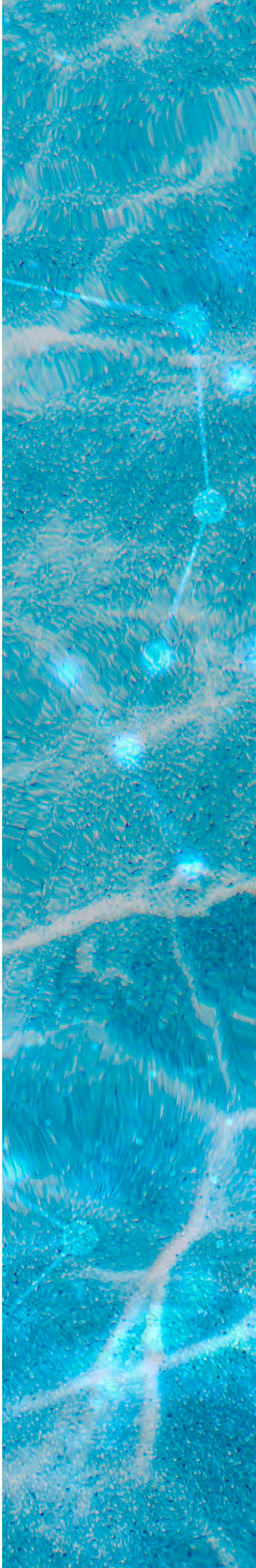
After the high severity of the vulnerability was acknowledged, Microsoft published an out-of-band patch on July 6th and claimed to have fully addressed the public vulnerability.

However, on July 7th researchers presented additional successful PoCs and claimed that the patch can be bypassed.

Who was impacted?

This vulnerability affects all modern unpatched client and server versions of Windows.

According to Kaspersky, the vulnerability was already exploited but no further information regarding victims is currently available.



Solarwinds

What happened?

On July 9th, Solarwinds published an announcement claiming that they were informed by Microsoft of an exploited zero-day vulnerability in their Serv-U Managed File Transfer and Serv-U Secure FTP products.

On July 10th, Solarwinds released a patch to fix the vulnerability and claimed that this event is unrelated to the Solarwinds supply chain attack that occurred in December of 2020.

The vulnerability allows an attacker to run arbitrary code with privileges, and then install programs; view, change, or delete data; or run programs on the affected system.

Who was impacted?

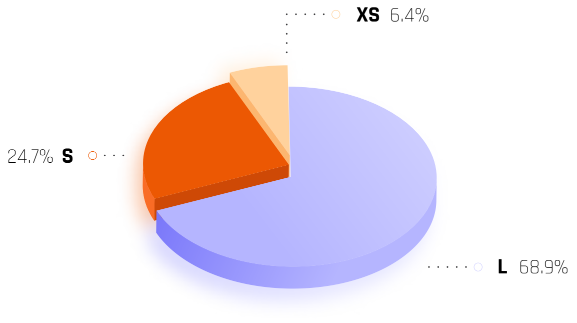
According to the latest published information the alleged victims of the attack are nine U.S. agencies and 100 private companies, although it is claimed that SolarWinds is unaware of the identity of the potentially affected customers.

The identity of the attackers also remains unknown at the moment.

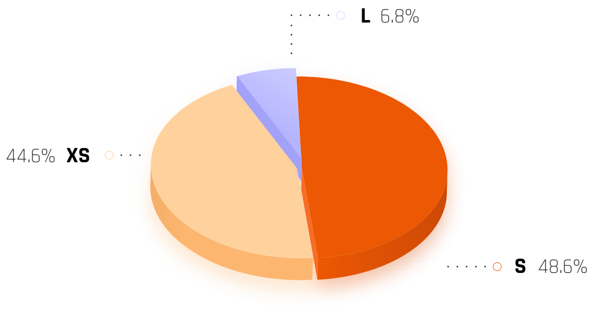
Case Study - Kaseya Ransomware

As the scope and identity of this event's victims remains mainly unknown it is hard to assess the exact financial damage the affected companies would suffer. In order to demonstrate the potential damage of this event, Kovrr has produced a demo portfolio of 1500 companies containing elements of a typical company buying affirmative cyber insurance coverage in the market. The companies' sizes, industries, and locations in the portfolio were based on information and ratios from multiple news reports regarding the attack. The financial damage calculation of the portfolio shows that large companies suffer the biggest losses in this situation and account for 69% of the overall damage while being only 7% of all companies in the portfolio.

FINANCIAL LOSS DISTRIBUTION BY COMPANY SIZE



COMPANY SIZE DISTRIBUTION



KOVRR
Cyber Risk Modeling

The Author

Geniya Brass Gershovich

Cyber Intelligence Analyst

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.
To learn more please contact the Kovrr team: contact@kovrr.com