One Year After SolarWinds

Are Things Any Better on the Cybersecurity Playing Field

January, 26 2022

Seyfarth

MANDIANT®

Seyfarth

Legal Disclaimer

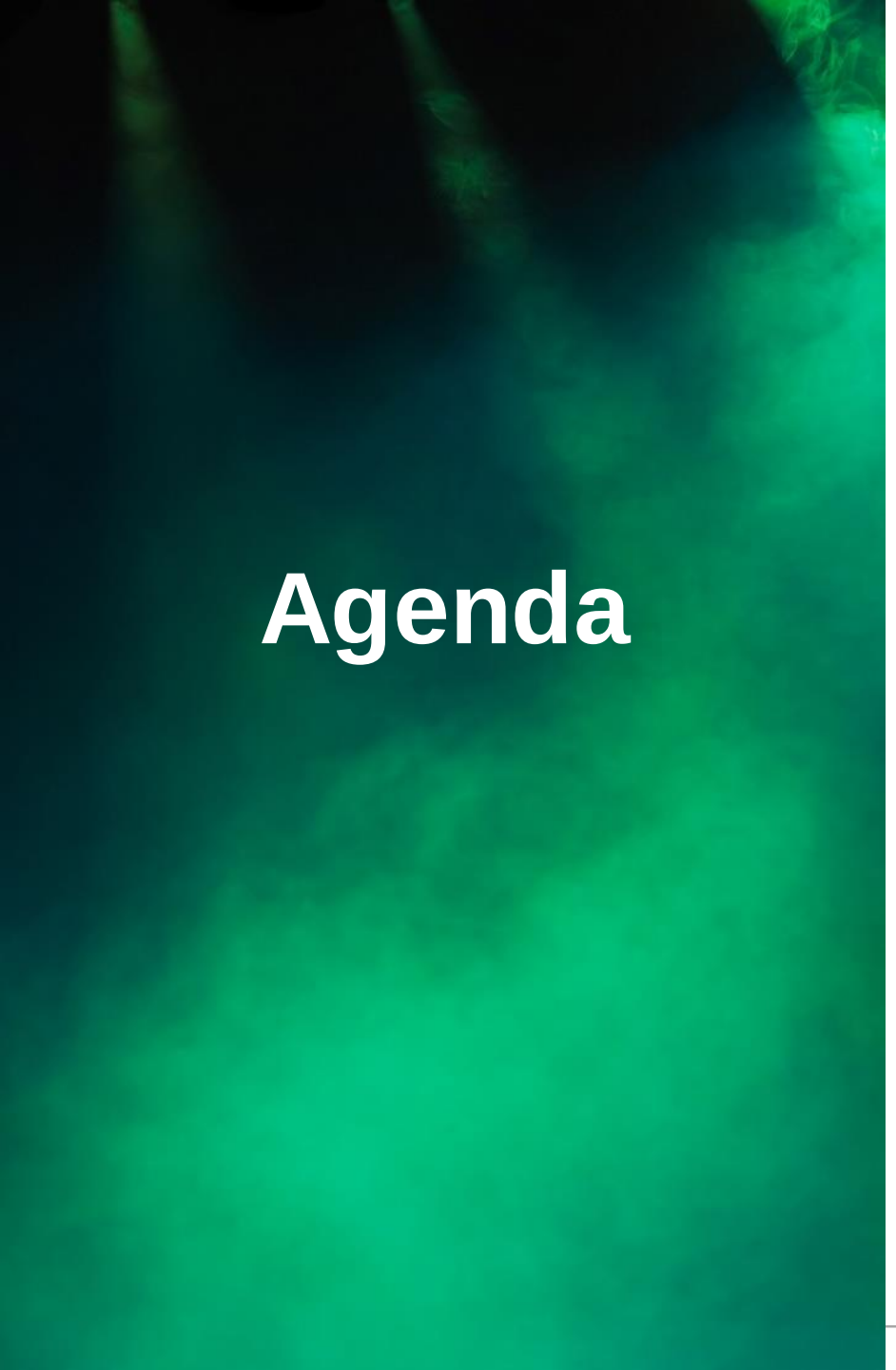
This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Speakers

Paul Ferrillo
Partner
Seyfarth Shaw LLP

Charles Carmakal
SVP and CTO
Mandiant

Steven Stone,
Senior Director,
Advanced Practices
Mandiant



Agenda

1 | Introduction

2 | SolarWinds - third party software update

3 | Kaseya — ransomware

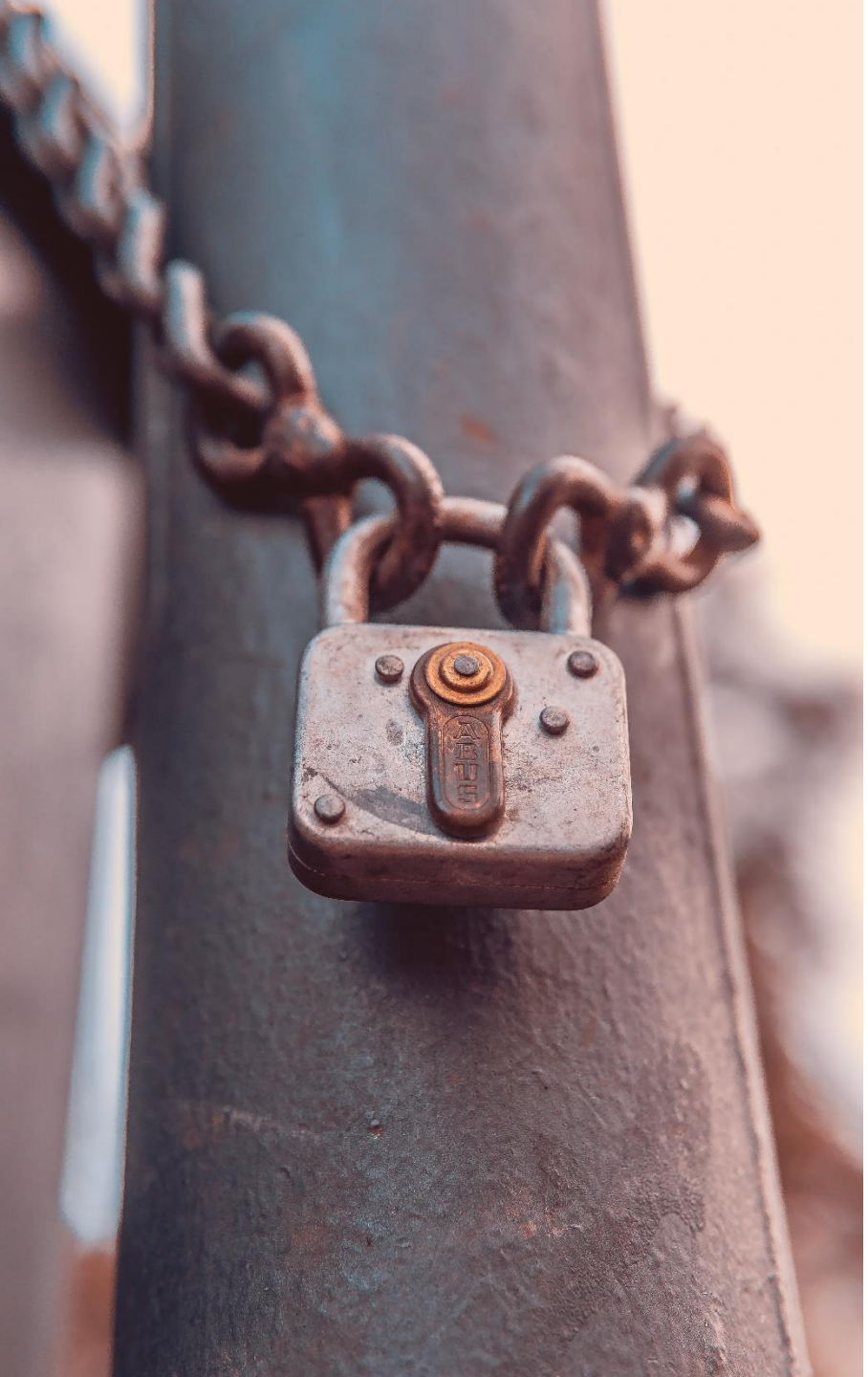
4 | JBS meats — ransomware

5 | Log4j vulnerability

6 | Discussion of the cases

7 | Are we any better off today then we were a year ago? If not why not?

8 | What can us corporations do to better respond to today's risks?



SolarWinds Supply Chain Attack in 2020

- SolarWinds is a Delaware company providing IT infrastructure management software
- Supply chain attack involving a section of malicious code inserted into an Orion software update, providing the threat actor access to the system
  - The code was inserted and present in updates between March and June 2020
- The attack is believed to have been orchestrated by a Russian intelligence group, likely the Russian Foreign Intelligence Service
- Reuters first reported that an attack had occurred on December 13, 2020
- On December 15, Reuters updated their article to include the “solarwinds123” password and a statement that the malicious updates were still available for download days after SolarWinds discovered the attack

SolarWinds Supply Chain Attack in 2020

- SolarWinds has approximately 33,000 companies and entities that generally use their IT infrastructure software
- Companies and entities downloaded updates to the software that contained the malicious code
- The code allowed the threat actors to gain backdoor access to the technology systems of companies, and they used that access to install further malware to monitor IT systems and data
- Up to 18,000 of SolarWinds' clients were potentially impacted, including leading technology companies and national security agencies (though we have seen smaller numbers of companies actually affected).

Kaseya Supply Chain Ransomware Attack in 2021

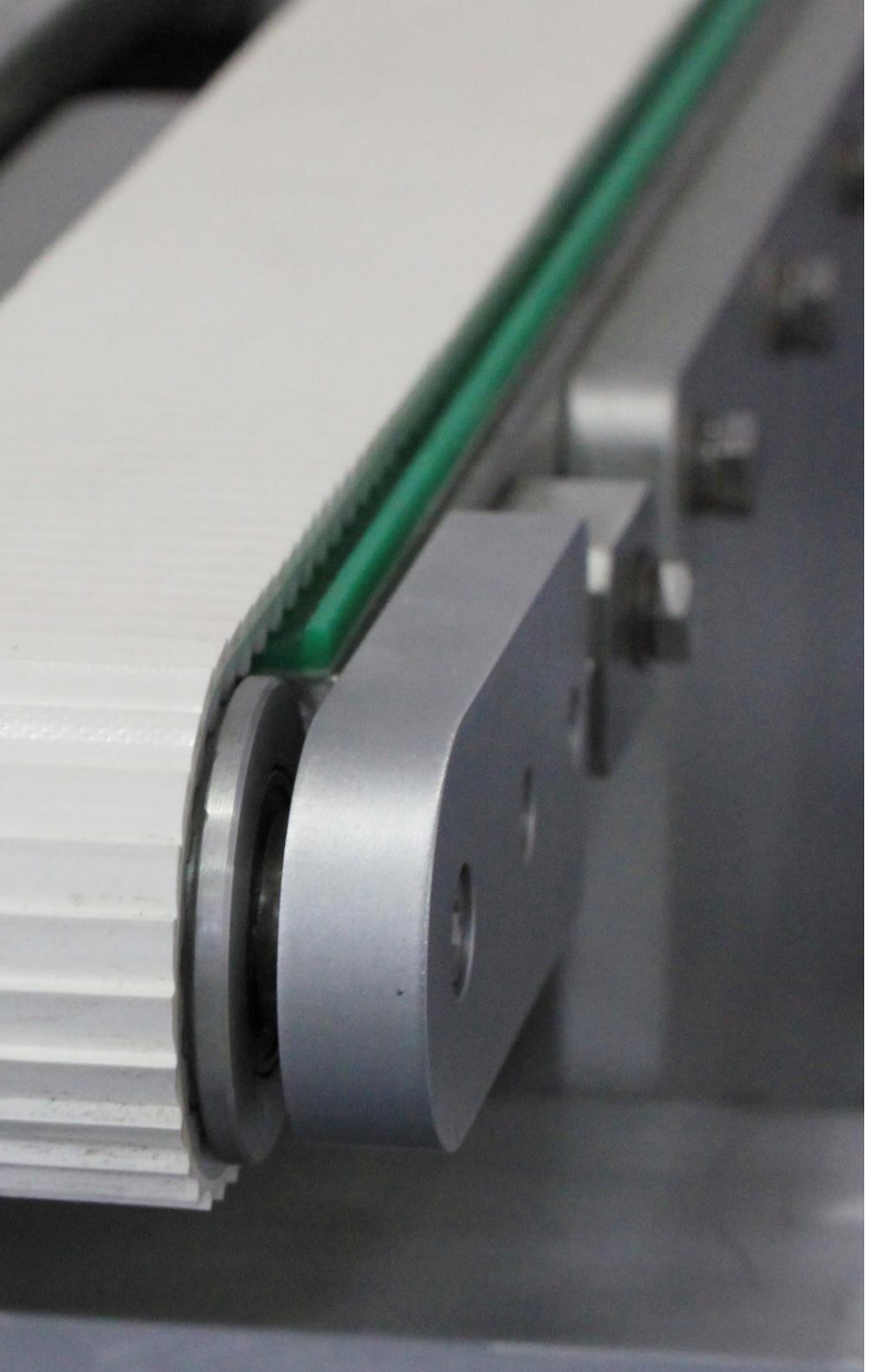
- Kaseya is a global IT infrastructure provider with headquarters in Dublin and Miami and operations in 10 countries
- Ransomware attack on July 2, 2021 resulting from a hack which used their Virtual System Administrator software to install ransomware through an automatic update
- Some cybersecurity experts have concluded that the attack used an authentication bypass vulnerability in the web interface
- Kaseya's Virtual Systems Administrator software is used to manage the complete infrastructure of a company's IT system

Kaseya Supply Chain Ransomware Attack in 2021

- Threat actors used the Virtual Systems Administrator software to install ransomware in the systems of Kaseya customers
- Some of Kaseya's customers are Managed Service Providers which perform IT operations for thousands of other companies and organizations
- "Approximately 60 Kaseya customers, all of whom were using the VSA on-premises product, who were directly compromised by this attack. While many of these customers provide IT services to multiple other companies, we understand the total impact thus far has been to fewer than 1,500 downstream businesses. We have not found evidence that any of our SaaS customers were compromised," Kaseya said in an update on the attack.

Kaseya Supply Chain Ransomware Attack in 2021

- On July 2, the CEO initially reported a potential attack that was limited to a “small number of on-premise customers”
- On July 4, Kaseya revised the statement to include that they were the victim of a sophisticated cyberattack and had begun employing forensic experts to investigate
- Attack was discovered to be the work of REvil, an affiliate of a Russian ransomware gang
- REvil demanded $70 million to reverse the impact of their attack on Kaseya’s system



JBS Ransomware Attack in 2021

- JBS is the world's largest meat processor, responsible for roughly a fifth of the meat in the US
- Experienced a ransomware attack on May 30, 2021 which affected some of the servers that maintain its IT systems in North America and Australia
- In response, they suspended the operation of their IT systems
- The suspension of IT operations required the shut down of production plants, causing meat shortage fears in North America
- JBS paid the $4.4 million ransom to eliminate the threat against their systems ~~ some of the ransom was recovered back by the US government one week later.
- Four days after the attack, JBS announced that it had resumed operations in all global facilities

JBS Ransomware Attack in 2021

- Attack was also the work of REvil, an affiliate of a Russian ransomware gang
- REvil has made significant profits in recent years through similar types of ransomware attacks where files are encrypted until a bitcoin payment is received
- After receiving payment, REvil generally gives the company a decryptor program and alleges that they won't release any uncovered data to the public
- REvil (the organization/infrastructure) was recently taken down by the Russian government—apparently due to the request of the US.

Log4j vulnerability in 2021, 2022, and future years- the most serious vulnerability ever seen?

- Log4j is the name given to a commonly used section of code that allows software applications to log/“record keep” previous activities on their systems
- Developers frequently use the existing log4j code in their software (available for free on the internet), and some cybersecurity experts have concluded that a large portion of internet services include the code
- In late 2021, cybersecurity experts began discussing how the log4j code would execute malicious code, if present in the system, and allow threat actors to access servers running that code
- Software engineers at many companies have begun investigating how to eliminate log4j from their code to remove the vulnerability

Log4j vulnerability in 2021, 2022, and future years

- A cybersecurity software company, Check Point, has stated that they believe threat actors have already tried to use log4j to infiltrate almost half of all corporate networks across the globe
- They also stated that threat actors had sent out 60 variations of the original code exploitation in one day
- On December 15, 2021, a threat actor backed by the Iranian government used log4j to attempt to access the Israeli government and private organizations
- The Cybersecurity and Infrastructure Security Agency had previously set a deadline of December 24, 2021 for federal civilian agencies to remove the log4j vulnerability from their systems, while other companies and organizations continue to race to remove the code from their system software

thank you

For more information please contact us.

Paul Ferrillo: pferrillo@seyfarth.com

Mandiant: info@mandiant.com