TLP:WHITE

ISSUE | JANUARY 2021

CYBERSEC LINK

The Newsletter of Cybersec Infohub

Seek advice from Cybersec Connect

Do you have any cyber security related problems that would like to seek advice or insights from our Cybersec Connect experts? You can now share your questions via one of the following channels:

1. Create a post under the Cyber Security Support section after logging in Cybersechub.hk; or
2. Email your questions to connect@cybersechub.hk

A token of appreciation

Representatives who raise the first 10 questions in each calendar month would receive a HK$25 cash coupon*, starting from now to March 2021. To encourage more questions from different organisations, each organisation can get at most 2 coupons in each calendar month. The Service Desk will contact the eligible representatives in two weeks after each month ends.

** In case of any dispute, the Service Desk reserves the right of final decision and interpretation.*

Hot Topics

- Corporate mobile's protection
- FireEye hack: Cybersecurity firm says nation-state stole attacking tools
- Security risk of cloud service migration?
- SolarWinds supply chain attack
- 公司可以點防範釣魚攻擊？

Note: Some of the posts are accessible to members only.

Top 5 Tags

#1	Threat Intel
#2	Trends
#3	Malware
#4	Vulnerability
#5	Analysis

Active Contributors*

- Ban CHENG, Sangfor Technologies (Hong Kong) Limited
- Chester LAU, Palo Alto Networks
- Claudius LAM, Trend Micro
- IEONG Iat Meng, HKCERT
- Kev HAU, Check Point Software Technologies Limited
- Lawrence LAW, HKCERT
- Mike LO, Wizlynx Cyber Security Limited
- Peony CHUI, Lapcom Limited
- Perry YAN, HKCERT
- SC LEUNG, HKCERT

** Include active Cybersec Connect experts.*

Information Security Headline

Supply chain attack threatening organisations around the world

A security vendor who fell victim in a system breach earlier this month discovered that SolarWinds Orion, an IT monitoring and management solution, was compromised to deliver malware.

Malicious actors compromised the software build system of Orion and injected a backdoor called "SUNBURST" into the software build, which was then delivered via software update released between March and June 2020 to Orion users.

SUNBURST once loaded will try to connect to the command and control server for instructions. It can perform various malicious tasks on infected device like exfiltrate data, retrieve and run code or other malware, erase or tamper with files, etc. Those target victims can be subject to follow-on action and further infection ((e.g., Teardrop and a Cobalt Strike) by the malicious actors.

About 18,000 Orion customers using the infected version of the software could be impacted by the attack and were urged to apply the latest update (version 2020.2.1 HF 2) or disconnect the affected devices as soon as possible. The affected customers include organisations in various countries and from various sectors including government, telecommunication and technology.

Source: *CISA*, *FireEye*, *The Hacker News*, *Bleeping Computer*

Advice

- Apply the latest updates on the affected software.
- Developers should perform regular inspection on their codebase and check for any signs of tampering or malicious code.
- Identify the applications and software used in your environment and review their security risk levels.
- Monitor network traffic and review system logs for suspicious activities.

Cybersecurity Outlook 2021

"In 2021, Covid-19 will still be impacting our lives, businesses, and societies, and those impacts will change as the year progresses. So we need to be ready for a series of 'next normals' as we respond to those changes. Following the rush to remote working, organizations need to secure their new distributed networks and cloud deployments to keep their applications and data protected. Enforcing and automating threat prevention at all points of the network – from employees' mobiles and endpoints to IoT devices to clouds – to stop advanced attacks from spreading rapidly across organizations, and exploiting weaknesses to breach sensitive data. Automating prevention will be critical, as 78% of organizations say they have a cyber-skills shortage."

Mr. Kev HAU, Cyber Security Evangelist, Check Point

"In the New Normal era, business activities are conducted mostly online. Cyber attacks continue to evolve, leveraging critical system vulnerabilities, sophisticated social engineering techniques like vishing and deepfake, and advanced ransomware attacks leading to a data breach. In response to the evolving threats, users should focus on protecting digital identity, securing access control of sensitive data, hardening cloud-based service exposure, and building the human firewall in the organisation."

Mr. Lawrence LAW, Security Consultant, HKCERT

"As we begin to enter a post-pandemic world, the trend for remote working is likely going to stick for many organizations. We predict more aggressive attacks to target corporate data and networks. Security teams will need to double down on user training, extended detection and response and adaptive access controls. This past year was all about surviving: now it's time for businesses to thrive, with comprehensive cloud security as their foundation."

Mr. Tony LEE, Head of Consulting, Trend Micro Hong Kong

Industry Events

- Cyber Security Competition 2020/21
  HKPF | 22 Nov 2020 – 10 Apr 2021

- (CS)2AI ONLINE- Mission Kill: Process Targeting in ICS Attacks, with Joe Slowik
  (CS)2AI | 15 Jan 2021

- OWASP API Security Top 10
  OWASP Dhaka Chapter | 22 Jan 2021

By the end of December 2020, 320+ Members and 1040+Representatives participated in Cybersec Infohub.

Not yet a member?

Register for FREE at https://www.cybersechub.hk/en/register