Cyber Threat Intelligence insights

> *Who knows his enemy and himself, won’t fear the result of a hundred battles*
>
> Sun Tzu (544 – 496 av.JC)

Cyber-Weather

Monthly News Roundup

March

Weak signals for Strategic CTI

New information and issues about the SolarWinds compromise

Although more than four months old, the compromise of SolarWinds' Orion software continues to be the subject of new information as investigations into the scope of the attack make progress.

Recently, reputable sources reported to Associated Press (AP) news agency that **the threat group** responsible for the breach **had access to the mailboxes of several U.S. Department of Homeland Security (DHS) officials**, including Chad Wolf, former DHS Secretary between 2019 and 2021.

As a reminder, some US officials attribute SolarWinds' compromise to the Russian **APT group APT29** *aka* Cozy Bear supposedly affiliated to the Russian domestic and/or foreign intelligence services SVR and FSB). Moreover, key-stakeholders of the DHS' cybersecurity staff could have also been victims of compromised mailboxes, including ones in charge of hunting operations against foreign threat activities.

The "Big Brother effect" allowed by supply-chain attacks shed light to the thorny issue of technological convergence with a restricted number of solutions sold and used by a large part of enterprises and public sector organizations.

Software supply chain attacks leverage either the source code, update mechanism, or build processes of vendor software to compromise victims throughout three main vectors (3rd party updates, malware installed on connected devices or application installers) while being often overlooked by organizations.

Some can compare supply-chain attacks as a new way to benefit from efficient cyber weapons : most recent examples encompass a supply chain attack against Centreon unveiled by ANSSI or the PHP Git' code source compromise announced by Nikita Popov on Sunday, 28th 2021 (knowing that 79% of websites use this side-programming language).

All of these elements raise questions about the ability of nation-state-sponsored threat groups to gain access to information that would allow these ones to benefit from both strategic and operational intelligence. Thus, cyber espionage operations seem to be taking a new turn, which for the time being seems complex to counter.

SolarWinds, DHS, supply-chain, APT, APT29, COZY BEAR, Orion, PHP, cyber-weapons, CISA, CHIRP

#

APT groups operations could **form alliances of interest to target a supply chain from which all parties could benefit** despite strategic and geopolitical differences. Others may jump into the breach out of sheer opportunism.

It's highly likely that supply-chain attacks are going to be increasingly popular in short/mid term amongst threat actors to **access enterprises and public sector jewels crown**.

Supply-chain attacks like SolarWinds allow threat groups to **target a large variety of sectors without a geographical distinction.**
This tactic enables to reach a wide spectra of vulnerable services and then choose and target the victims they're interested in. Supply-chain attacks could be also part of the cyberpowers race to the zero-days that could lead to **cyber-weapons**.

Zero Trust Architecture (ZTA) developed by the NIST is one of the **most effective solutions for limiting the impact of supply chain attacks**.

The US cybersecurity agency (**CISA**) **published** a new tool dubbed **CHIRP allowing** hunting teams **to detect SolarWinds' compromise related footprints**.
Adversary Simulation engagements can help your organization mitigating successful attacks on an operational environment

Threat highlights

FBI publishes its annual report on cyber-crime

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

The **Internet Crime Report** 2020 from the FBI shows that cybercrime activity continues to grow. Last year **$4 billion losses** were due to cyber-attacks all over the world. The number of complaints received by the Bureau represented a **69% increase over 2019**.

Considering ransomware attacks, their induced loss is estimated at **$29.1 million**, but suspected to be much more because some companies do not contact the FBI because they advise not to pay, which can mean the complete loss and the publication of their private data.

The most impacted country are **the United-States**, far beyond the others with **791,790** complaints received (all threats combined). Next in line comes the United-Kingdom with 216,633 complaints and Canada in third with 216,633. **France is 7th with 1,640**.

The top entry points for ransomware attacks are **RDP credential use, phishing, and software vulnerabilities**.

FBI, IC3, Internet Crime Report, Ransomwares #

9 Media Entertainment (Australia) hit by Medusa Locker

https://itwire.com/security/windows-medusalocker-ransomware-likely-used-in-nine-attack-for-profit.html

End of March, one of the biggest TV channels available to Australians was hit by a cyber-attack. All systems were down, and the media was unable to broadcast nor to print production of its newspapers.

The ransom note points **towards Medusa Locker, a ransomware known since Sept. 2019 being operated by ANTHROPOID SPIDER. The latter** is neither a big player in the ransomware ecosystem nor does hold a DLS (dedicated leak site), though a fork dubbed Ako does.

The Taiwanese CERT likns ANTHROPOID SPIDER with **FIN7/Carbanak,** a financiary motivated threat actor. Its modus operandi is to **infiltrate internal networks in order to steal information they might monetize** such as credentials. Leading **FIN7 members were arrested** but attacks using their infrastructure and TTPs were spotted in the wild afterwards. It is possible that the remaining members of the group got together again, or even some members have gone their way with part of the infrastructure. In this case **the ransom might just be a diversion,** or a way to display their capabilities to attract new affiliates.

Other hypothesis attributes the attack either to the **Russians or the Chinese**. 9 Media was about to release a documentary about Putin and Australia banning Huawei hardware from its 5G network.

nine
MEDIA CORPORATION

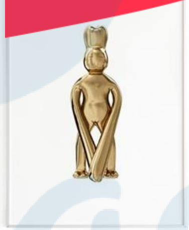
Medusa Locker, Ransomware, doxing, media #

Bab(u|y)k: First new Ransom/doxware of 2021

- This year started with the appearance of a new ransomware dubbed **Babuk** (aka Babyk), discovered by a cybersecurity researcher at McAfee Labs
- This family of ransomware joined already the recent trend of **double extorsion** conducted by the top-tier1 of the ransomware ecosystem and falls into the scope of **big-game hunting** (the process of cybercriminals focusing on high-value data or assets within businesses)
- Babuk's codebase and artifacts (such as ransom notes) bear enough similarities to the **Vasa Locker** group to consider them aligned if not synonymous
- its operators **hit several corporations in a relative short range of time** amongst which, the prominent global government outsourcer **Serco** exhibiting a revenue of over £ bn in 2019 and being **behind NHS Test and Trace**
- **Babuk attacks are on the rise** since the beginning of March **thanks to a ransomware-as-a-service business model**

- Babuk' MO is compatible with **an opportunistic actor motivated by a profit motive** while this ransomware may have been developed hastily
- The techniques, tactics and procedures (TTPs) used are **classic** and have not shown the use of particularly sophisticated attack techniques
- The **entry vector remains unknown** (to our knowledge)
- The **C++** coded ransom is based on **public libraries** and its specific code is very **short**
- The ideology displayed as **anti-capitalist** backed by a conservative societal ideology (**anti-LGBT**) is compatible with a **hacktivist group of Muslim** faith echoing the mention of 'sultan' Babuk found on a telegram channel

- This new ransomware/doxware comes **without** any code source **obfuscation** mechanisms (though a packed version was reported)
- It uses nonetheless a **robust encryption scheme** being (almost) **unbreakable** leveraging a home made **SHA256 algorithm Chacha8** for the encryption and protects the keys with ECDH, which uses 256 bits long keys
- **It lacks « kill-switches »** that is a common feature usually tailored by the top-tier ransomware ecosystem when detecting languages of the **Commonwealth of Independent States** (CIS) set as default



- For the CERT Sogeti ESEC, Babuk's developers are **Russian speaking** and are located in a **Central Asia** country, with a medium probability for **Kazakhstan** (thanks to SOCMINT-oriented research)
- Babuk being the name of a **slavic deimon**, we conjecture it could be the origin of the ransomware's name
- We noticed several **OPSEC (Operations Security) errors** *i/* those cited in Chuong Dong analysis about the code (thread management, encryption errors) that we could confirm *ii/* other flaws related to their **onion doxing website** from which we could gather intelligence

- After having identified two set of variants from available Babuk' samples in the wild **we proposed two types of vaccines**
- We are providing **proof of concepts** that can **pre-empt the observed Babuk threat** from encrypting your assets

Python script

Cyber-Weather

Spotlight

APT

Hafnium

Hafnium is an alleged chinese state-sponsored APT group that heavily leveraged **Microsoft Exchange servers' flaws** also known as Proxy Logon in early March 2021. Microsoft researchers believe that the mission of **Hafnium** was to conduct **cyberespionage operations primarily on US enterprises and public sectors to gather intelligence**.

While Hafnium is believed to be a new threat group according to Microsoft, **several other researchers don't attribute Proxy Logon' attacks to a unique APT group** but to a broader cluster encompassing a large scope of Chinese APT groups.

Hafnium, China, APT, Microsoft Exchange, Proxy Logon, China Chopper #

China

- Medical research
- Defense contractors
- Law firms
- Universities

- Proxy Logon's flaws exploitation
- China Chopper webshells
- Data exfiltration through MEGA

E-crime

Indrik Spider / TA505

Indrik Spider (aka TA505) is suspected to operate from **Commonwealth of Independent States** nations (CIS) and uses widespread phishing campaigns to distribute malware. They target mostly US, European and East Asian countries and they attack mostly the financial sector, retail and hospitals.
Recently, researchers spotted **a shift on Indrik' operations** with the spread of new ransomware variants known as **Hades** and **Phoenix**. It could be a trick for the group to diversify its extorsion operations adding two new "options" on its toolset.

Indrik Spider, TA505, Dridex, Hades, Phoenix, Ransomware #

C.I.S

- Hospitals
- Retail
- Financial sector
- Logistics

- Hades ransomware
- Phoenix Locker ransomware ?

Vulnerability

Mass exploitation of Microsoft Exchange 0-days

An updated timeline was published in a blog post from **Domaintools** that takes a new look on the possibility of an exploitation of the **CVE-2021-26855** as early as **November 2020**. This information is **of paramount importance for post-mortem threat hunting** to ensure the absence of any compromise.
Beyond the large cluster of Chinese APTs that were reported in the wake of Hafnium, the **ecrime ecosystem** also joined the playground of Microsoft Exchange exploits to drop either **ransomwares** or **coinminers** such as **#DLTMiner, #DearCry, #BlackKingdom, #LemonDuck** (botnet previously seen to exploit EternalBlue).

ProxyLogon, 338377, DearCry, BlackKingdom, LemonDuck, HAFNIUM, CVE-2021-26855, Microsoft-Exchange #

Course of action

Patched, Mitigation Tool, remediation, Microsoft, Github #

Malicious actors were seen mitigating the **CVE-2021-26855** (SSRF) thus a **full investigation** of the systems that were exposed **is needed**, even if they have been **fully patched and mitigated**, per traditional incident response process.

Last tips in a nutshell:

- **Check** whether or not **your organization was impacted** via a Victim Notification Site CheckMyOWA
- Hunt for webshells dropped on the vulnerable servers **even if you have promptly patched**
- Check for spikes in the GPU/CPU usage that would point towards the presence of coin miners
- Customers without dedicated security teams can leverage Microsoft one-click Mitigation Tool to mitigate **CVE-2021-26855** against highest risks before patching