Dragon Advance Tech

The 2021 Blue Team Challenges

- Security Predictions for Hong Kong

Dragon Advance Tech

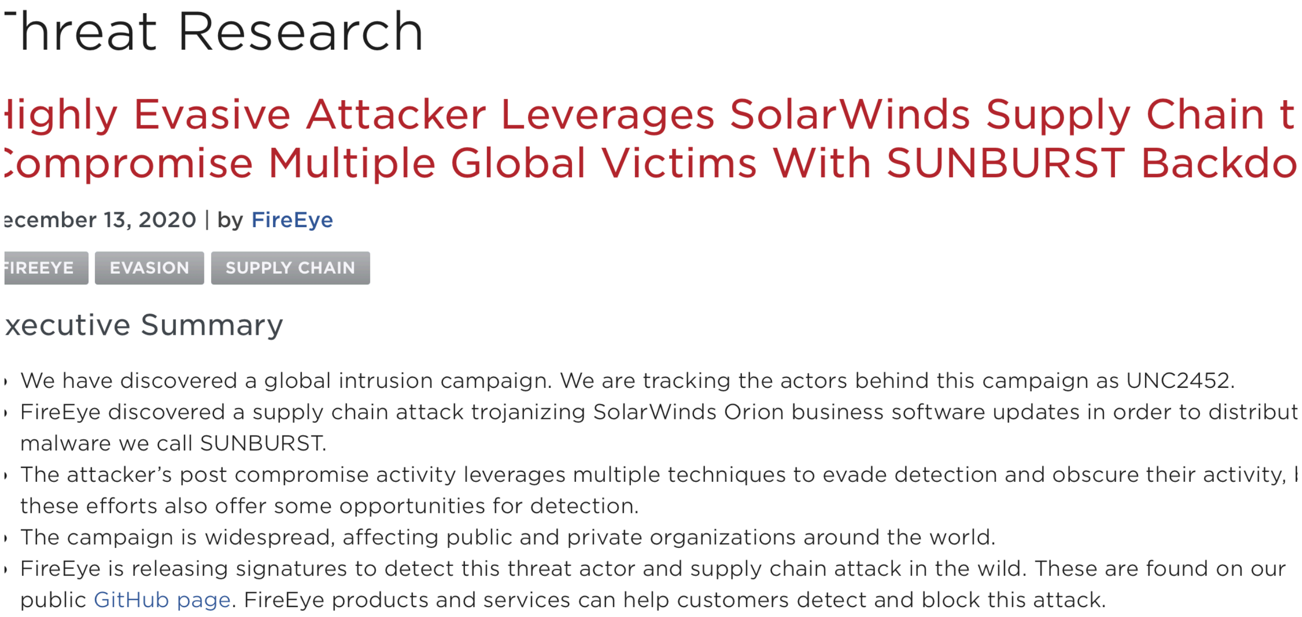
Agenda

- 10 Critical cybersecurity incidents in 2020
- The new normal
- My little cryptal ball predictions for Hong Kong
- The BT's challenges
  - Cybersecurity hygiene
  - Penetration testing / vulnerability scanning
  - Endpoint | network defense
  - Continuous monitoring
  - CTI and IR

10 Critical Cybersecurity incidents in 2020

1. Supply chain attacks
2. Phishing and BEC
3. Human operated ransomware
4. VPN vulnerabilities
5. Malware Emotet and Trickbot
6. Vulnerabilities and patching
7. Unauthorized access
8. RDDoS
9. APT
10. Hong Kong/APAC/Financial

Supply chain attacks



hreat Research

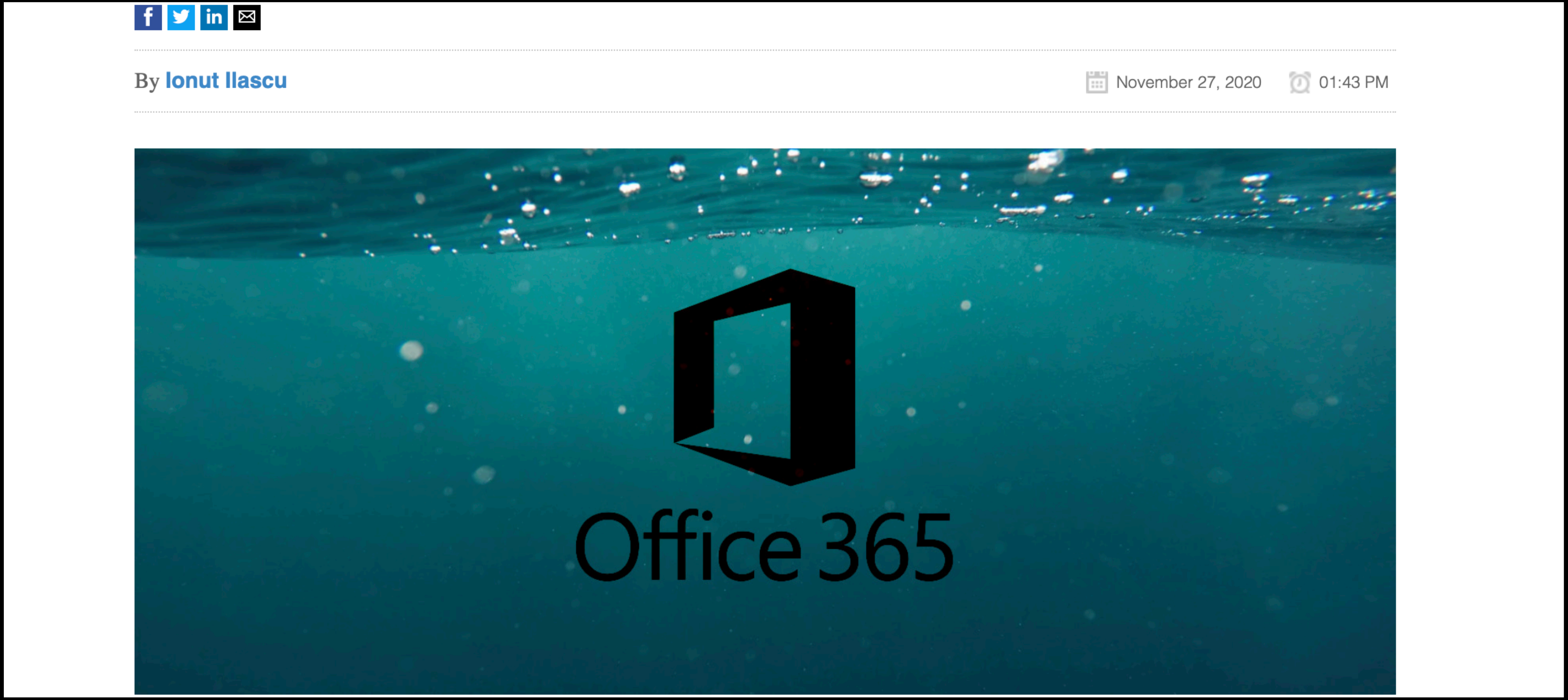
ighly Evasive Attacker Leverages SolarWinds Supply Chain t
ompromise Multiple Global Victims With SUNBURST Backdo

ecember 13, 2020 | by FireEye

IREEYE EVASION SUPPLY CHAIN

xecutive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribut malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

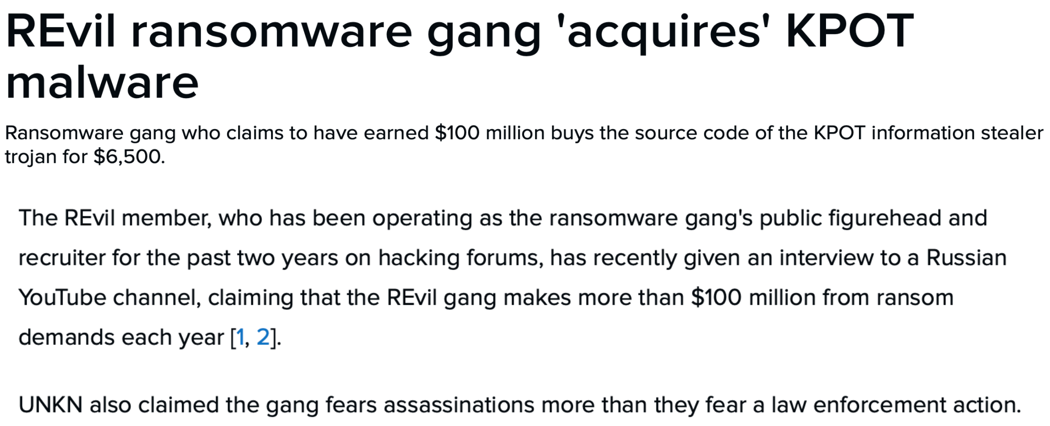


By Ionut Ilascu

November 27, 2020 01:43 PM

Phishing and BEC (on the cloud)

Human operated ransomware

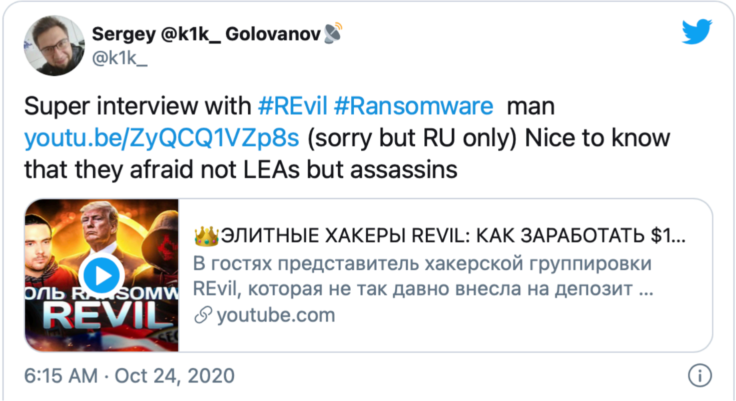


REvil ransomware gang 'acquires' KPOT malware

Ransomware gang who claims to have earned $100 million buys the source code of the KPOT information stealer trojan for $6,500.

The REvil member, who has been operating as the ransomware gang's public figurehead and recruiter for the past two years on hacking forums, has recently given an interview to a Russian YouTube channel, claiming that the REvil gang makes more than $100 million from ransom demands each year [1, 2].

UNKN also claimed the gang fears assassinations more than they fear a law enforcement action.

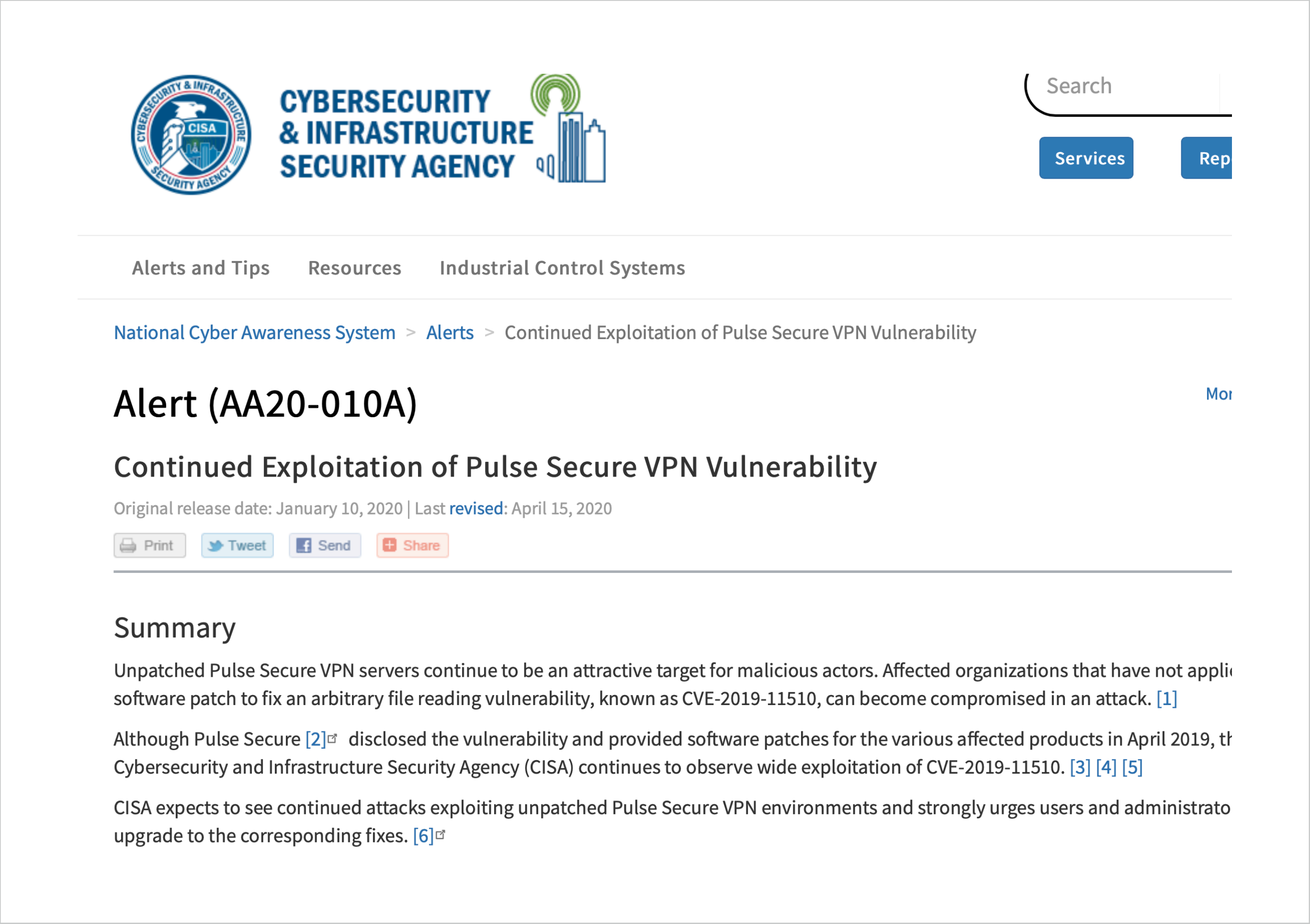


Sergey @k1k_ Golovanov
@k1k_

Super interview with #REvil #Ransomware man youtu.be/ZyQCQ1VZp8s (sorry but RU only) Nice to know that they afraid not LEAs but assassins

👑ЭЛИТНЫЕ ХАКЕРЫ REVIL: КАК ЗАРАБОТАТЬ $1...
В гостях представитель хакерской группировки REvil, которая не так давно внесла на депозит ...
youtube.com

6:15 AM · Oct 24, 2020



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
Search
Services
Rep
Alerts and Tips
Resources
Industrial Control Systems
National Cyber Awareness System > Alerts > Continued Exploitation of Pulse Secure VPN Vulnerability
Mor
Print
Tweet
Send
Share

Alert (AA20-010A)

Continued Exploitation of Pulse Secure VPN Vulnerability

Original release date: January 10, 2020 | Last revised: April 15, 2020

Summary

Unpatched Pulse Secure VPN servers continue to be an attractive target for malicious actors. Affected organizations that have not appli software patch to fix an arbitrary file reading vulnerability, known as CVE-2019-11510, can become compromised in an attack. [1]

Although Pulse Secure [2] disclosed the vulnerability and provided software patches for the various affected products in April 2019, th Cybersecurity and Infrastructure Security Agency (CISA) continues to observe wide exploitation of CVE-2019-11510. [3] [4] [5]

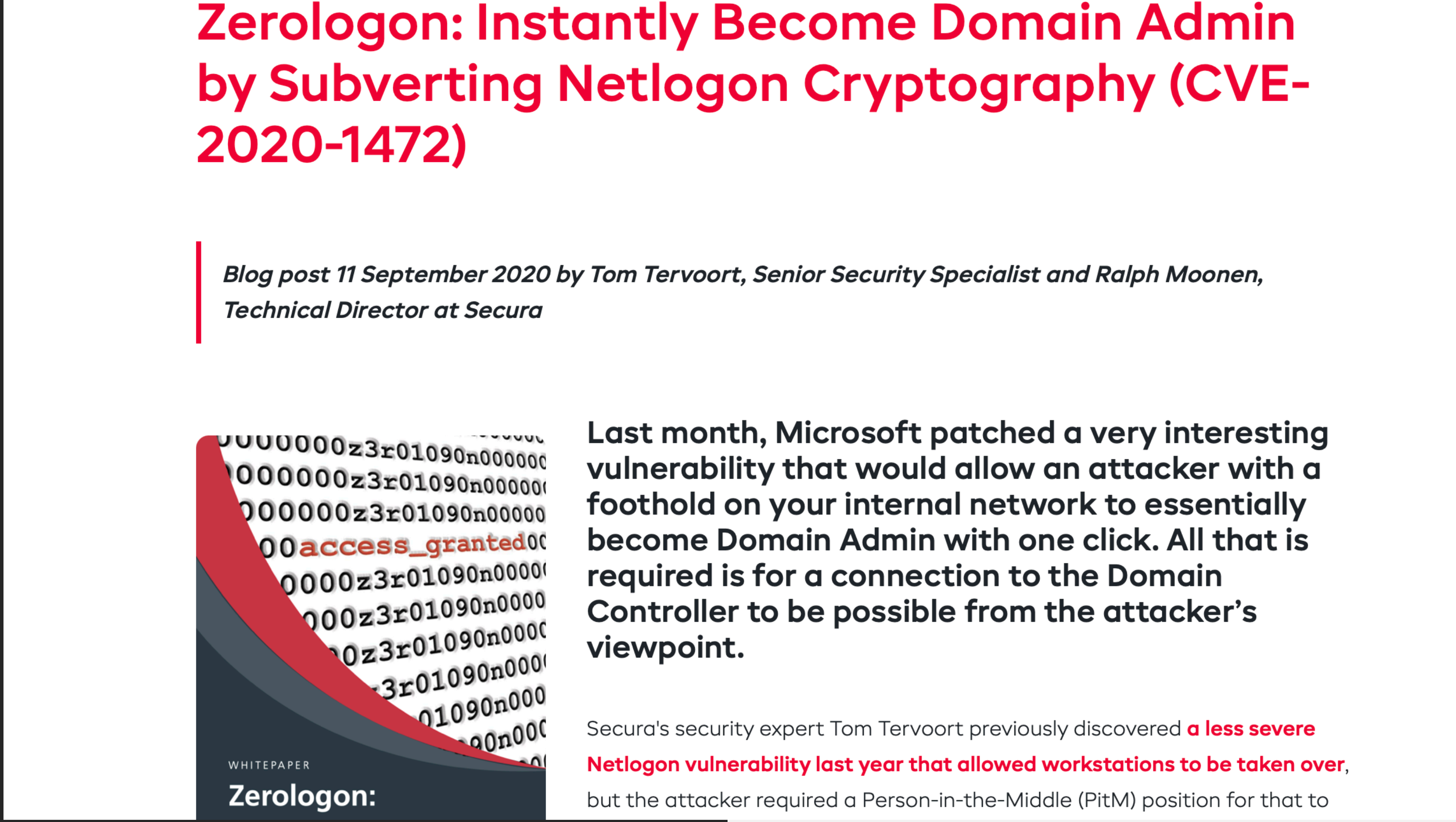
CISA expects to see continued attacks exploiting unpatched Pulse Secure VPN environments and strongly urges users and administrato upgrade to the corresponding fixes. [6]

VPN vulnerabilities

Malware Emotet and Trickbot

TRICKBOT NOW OFFERS 'TRICKBOOT': PERSIST, BRICK, PROFIT

December 3, 2020 / Eclypsium



Zerologon: Instantly Become Domain Admin by Subverting Netlogon Cryptography (CVE-2020-1472)

Blog post 11 September 2020 by Tom Tervoort, Senior Security Specialist and Ralph Moonen, Technical Director at Secura

Last month, Microsoft patched a very interesting vulnerability that would allow an attacker with a foothold on your internal network to essentially become Domain Admin with one click. All that is required is for a connection to the Domain Controller to be possible from the attacker's viewpoint.

Secura's security expert Tom Tervoort previously discovered **a less severe Netlogon vulnerability last year that allowed workstations to be taken over**, but the attacker required a Person-in-the-Middle (PitM) position for that to

Vulnerabilities and patching

Threat Research

Unauthorized Access of FireEye Red Team Tools

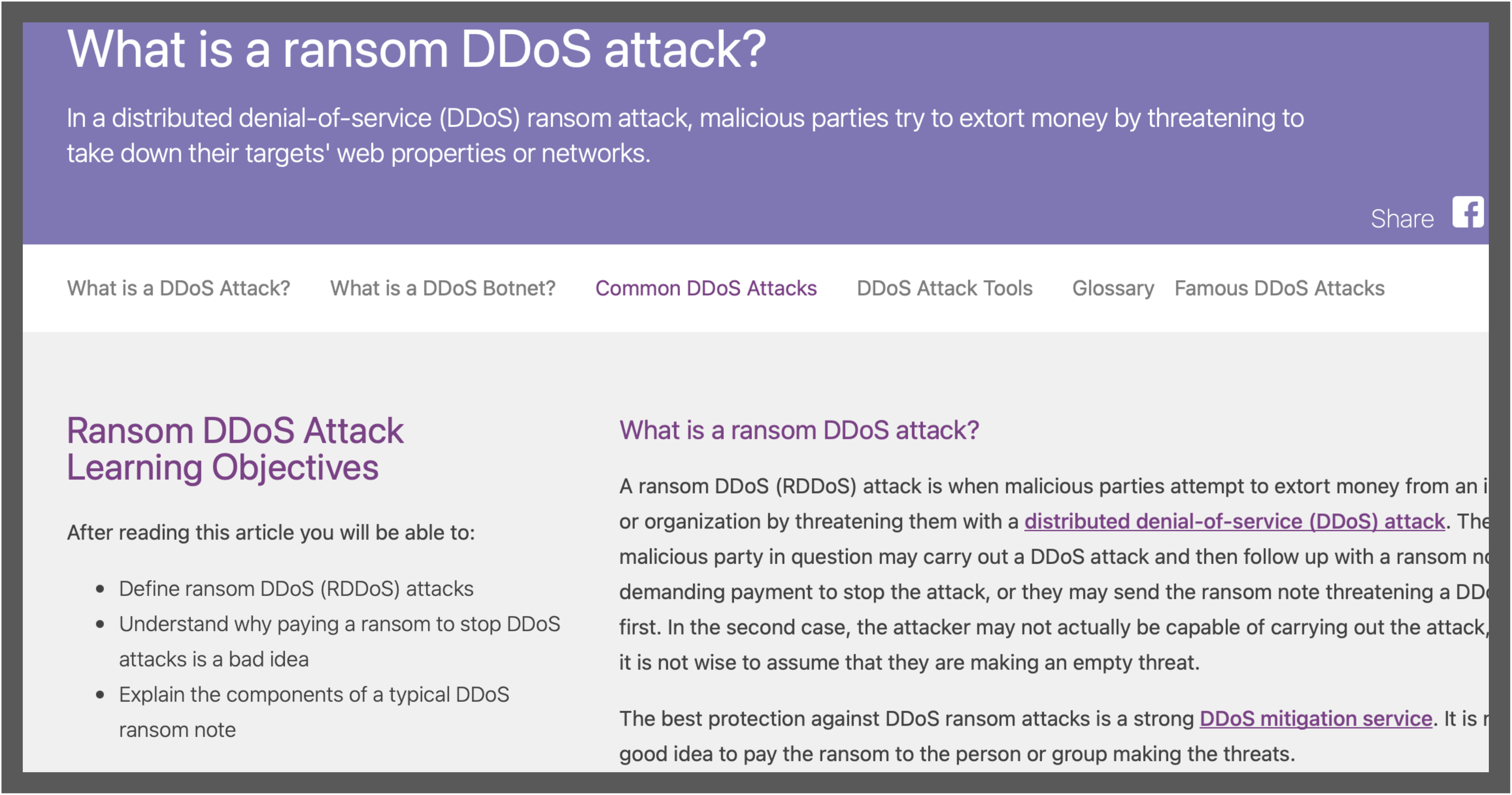
December 08, 2020 | by FireEye

FIREEYE TOOLS RED TEAM

Overview

A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools.

You can find a list of the countermeasures on the FireEye GitHub repository found HERE.



What is a ransom DDoS attack?

In a distributed denial-of-service (DDoS) ransom attack, malicious parties try to extort money by threatening to take down their targets' web properties or networks.

Ransom DDoS Attack Learning Objectives

After reading this article you will be able to:

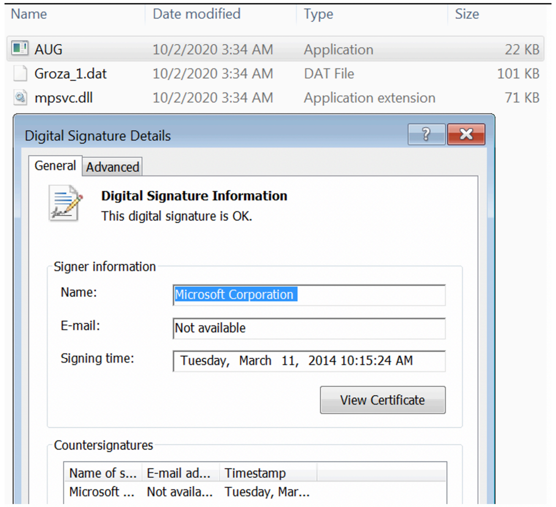
- Define ransom DDoS (RDDoS) attacks
- Understand why paying a ransom to stop DDoS attacks is a bad idea
- Explain the components of a typical DDoS ransom note

What is a ransom DDoS attack?

A ransom DDoS (RDDoS) attack is when malicious parties attempt to extort money from an i or organization by threatening them with a distributed denial-of-service (DDoS) attack. The malicious party in question may carry out a DDoS attack and then follow up with a ransom no demanding payment to stop the attack, or they may send the ransom note threatening a DD first. In the second case, the attacker may not actually be capable of carrying out the attack, it is not wise to assume that they are making an empty threat.

The best protection against DDoS ransom attacks is a strong DDoS mitigation service. It is r good idea to pay the ransom to the person or group making the threats.

APT



Name	Date modified	Type	Size
AUG	10/2/2020 3:34 AM	Application	22 KB
Groza_1.dat	10/2/2020 3:34 AM	DAT File	101 KB
mpsvc.dll	10/2/2020 3:34 AM	Application extension	71 KB

Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

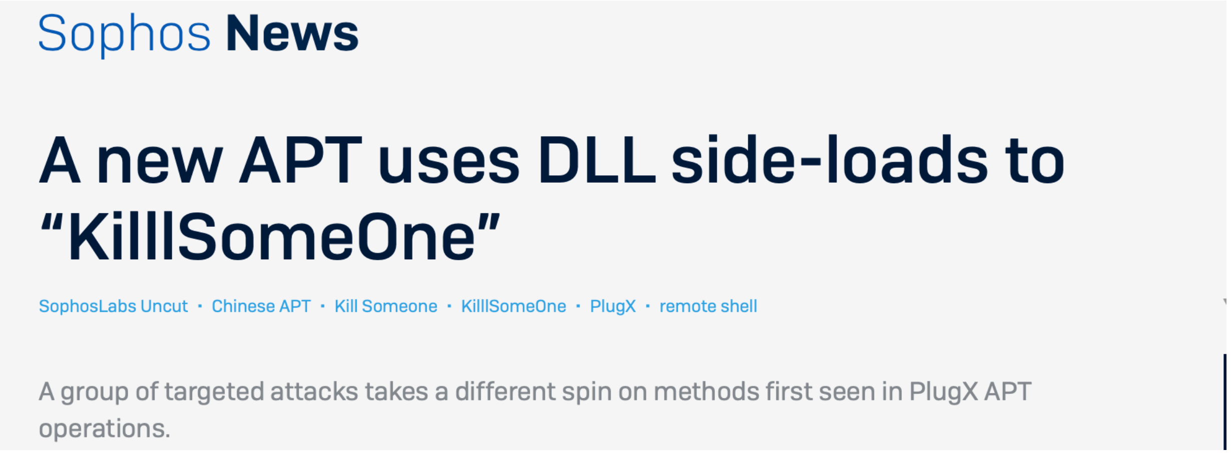
Name: Microsoft Corporation

E-mail: Not available

Signing time: Tuesday, March 11, 2014 10:15:24 AM

Countersignatures

Name of s...	E-mail ad...	Timestamp
Microsoft ...	Not availa...	Tuesday, Mar...

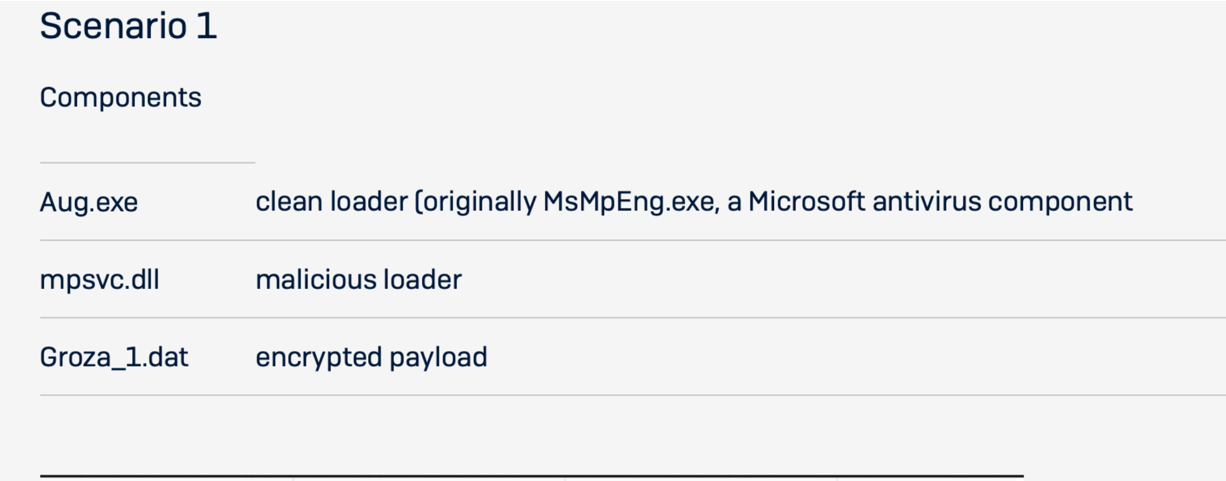


Sophos **News**

A new APT uses DLL side-loads to "KilllSomeOne"

SophosLabs Uncut • Chinese APT • Kill Someone • KilllSomeOne • PlugX • remote shell

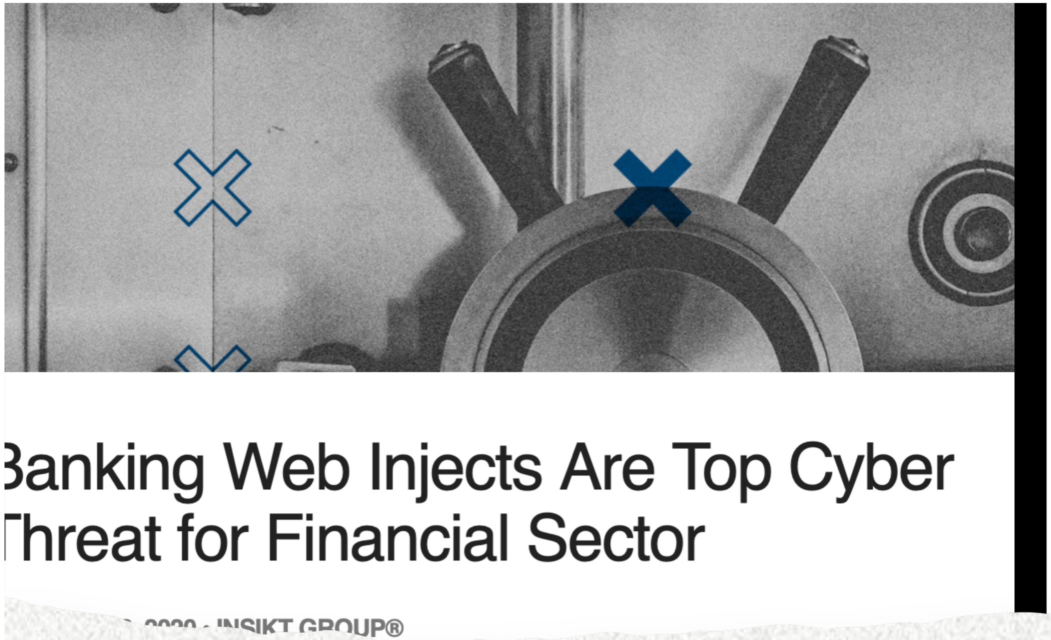
A group of targeted attacks takes a different spin on methods first seen in PlugX APT operations.



Scenario 1

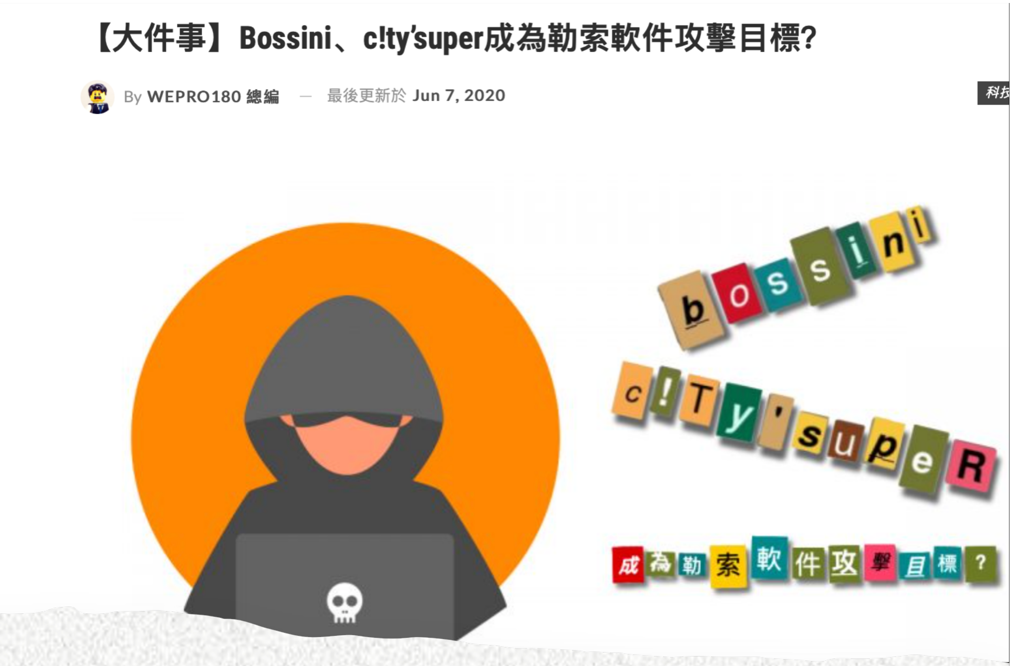
Components

Aug.exe	clean loader (originally MsMpEng.exe, a Microsoft antivirus component
mpsvc.dll	malicious loader
Groza_1.dat	encrypted payload



Banking Web Injects Are Top Cyber Threat for Financial Sector

2020 • INSIKT GROUP®



【大件事】Bossini、c!ty'super成為勒索軟件攻擊目標?

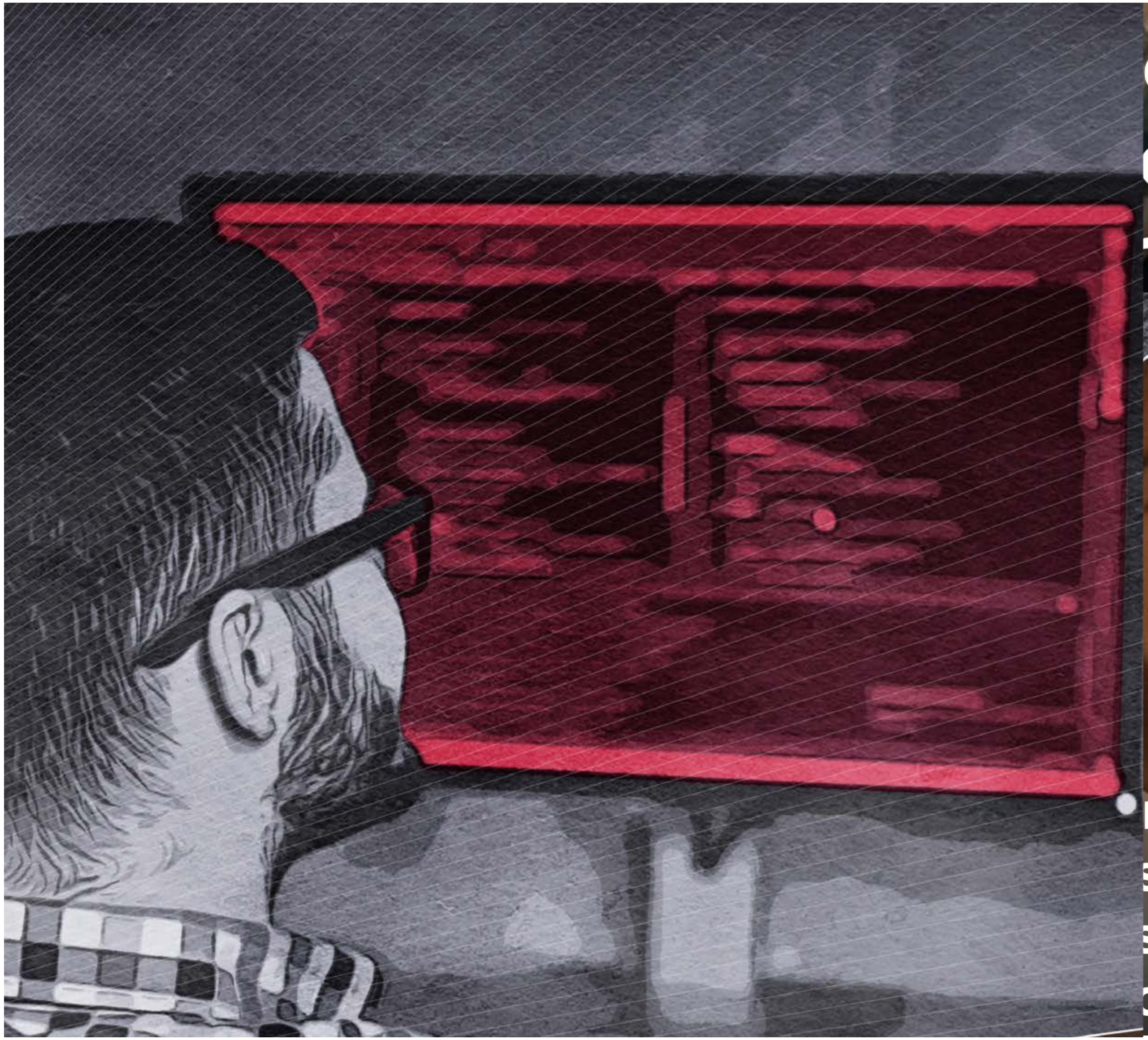
By WEPRO180 總編 — 最後更新於 Jun 7, 2020

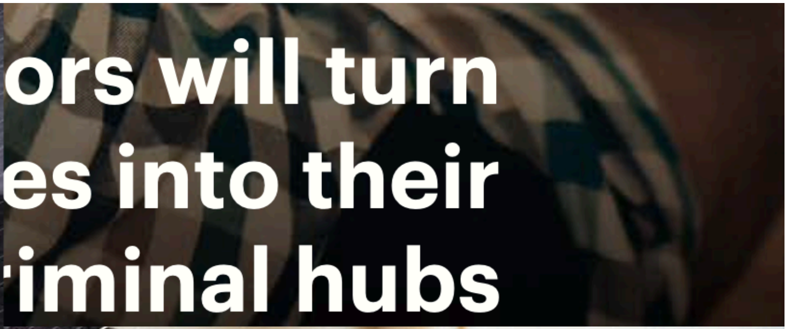
Hong Kong/APAC/Financial

The new normal

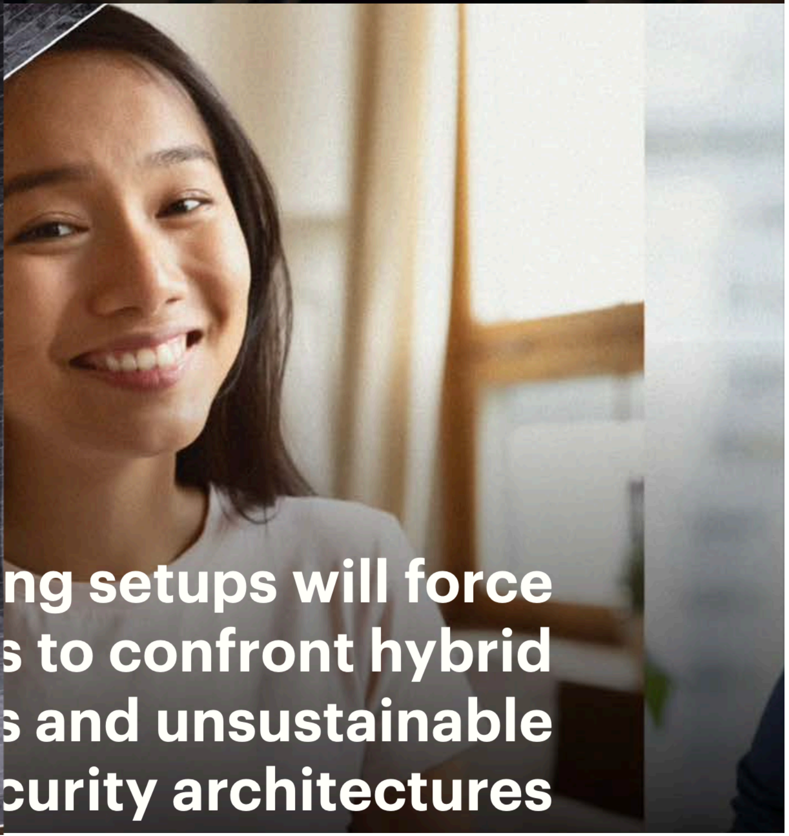
- Moving from corporate IT stack to
"Work from anywhere" workforce

Dragon Advance Tech





ors will turn
es into their
riminal hubs



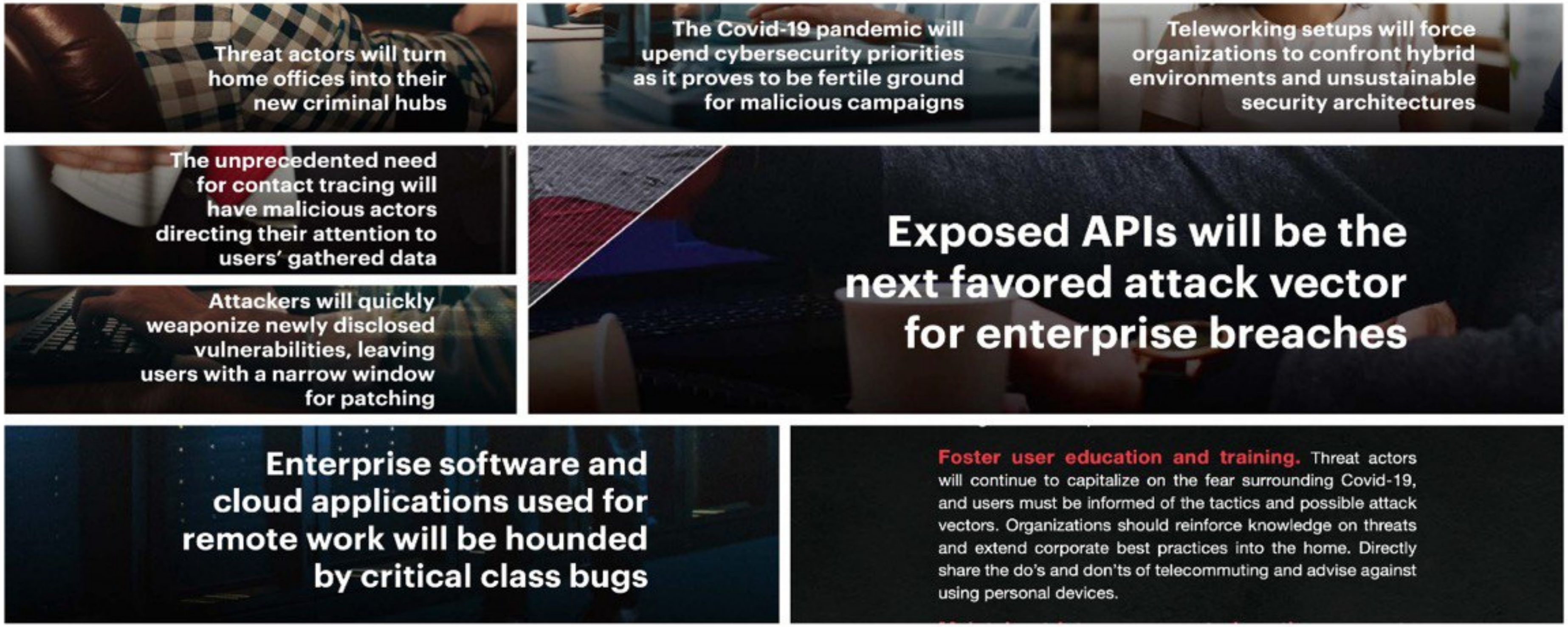
ng setups will force
s to confront hybrid
s and unsustainable
curity architectures

2021 Predictions for Hong Kong

- From my little cryptal ball

Dragon Advance Tech

2021 Cybersecurity Predictions



Threat actors will turn home offices into their new criminal hubs

The Covid-19 pandemic will upend cybersecurity priorities as it proves to be fertile ground for malicious campaigns

Teleworking setups will force organizations to confront hybrid environments and unsustainable security architectures

The unprecedented need for contact tracing will have malicious actors directing their attention to users' gathered data

Attackers will quickly weaponize newly disclosed vulnerabilities, leaving users with a narrow window for patching

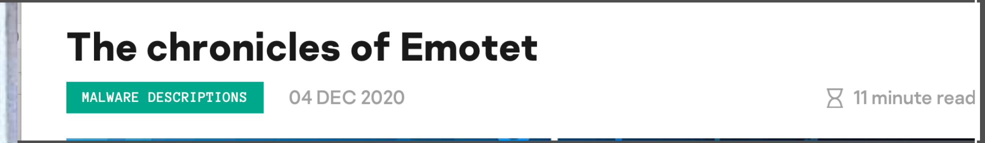
Exposed APIs will be the next favored attack vector for enterprise breaches

Enterprise software and cloud applications used for remote work will be hounded by critical class bugs

Foster user education and training. Threat actors will continue to capitalize on the fear surrounding Covid-19, and users must be informed of the tactics and possible attack vectors. Organizations should reinforce knowledge on threats and extend corporate best practices into the home. Directly share the do's and don'ts of telecommuting and advise against using personal devices.

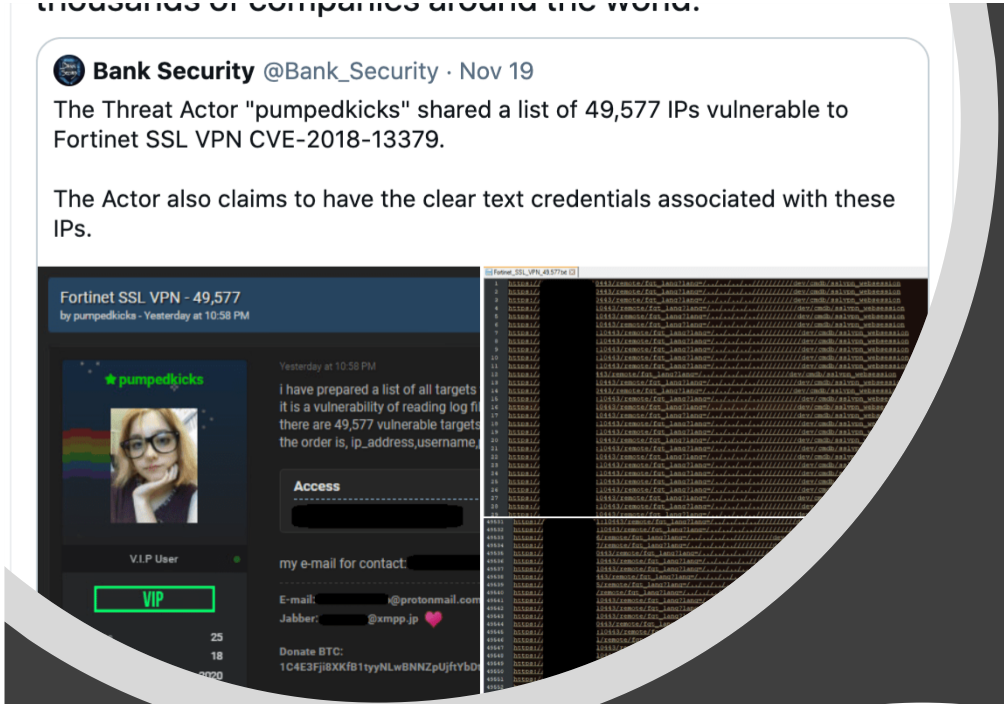
Source: TrendMicro

5


The chronicles of Emotet

MALWARE DESCRIPTIONS 04 DEC 2020 ⌛ 11 minute read

- Emotet was first discovered in June 2014 by TrendMicro.
- In 2015, a new Emotet was released, using built-in public RSA key with ATS scripts for web injection.
- The 2016 version infected web-surfing victims using the RIG-E and RIG-V exploit kits.
- Emotet could send spam independently in 2017.
- Starting from 2018, Emotet started distributing the banking Trojan Panda.
- In 2019, Emotet again modified HTTP protocol, switching to POST requests and using a dictionary to create the path.



thousands of companies around the world.

Bank Security @Bank_Security · Nov 19

The Threat Actor "pumpedkicks" shared a list of 49,577 IPs vulnerable to Fortinet SSL VPN CVE-2018-13379.

The Actor also claims to have the clear text credentials associated with these IPs.

Fortinet SSL VPN - 49,577
by pumpedkicks - Yesterday at 10:58 PM

Yesterday at 10:58 PM

i have prepared a list of all targets
it is a vulnerability of reading log fi
there are 49,577 vulnerable targets
the order is, ip_address,username,

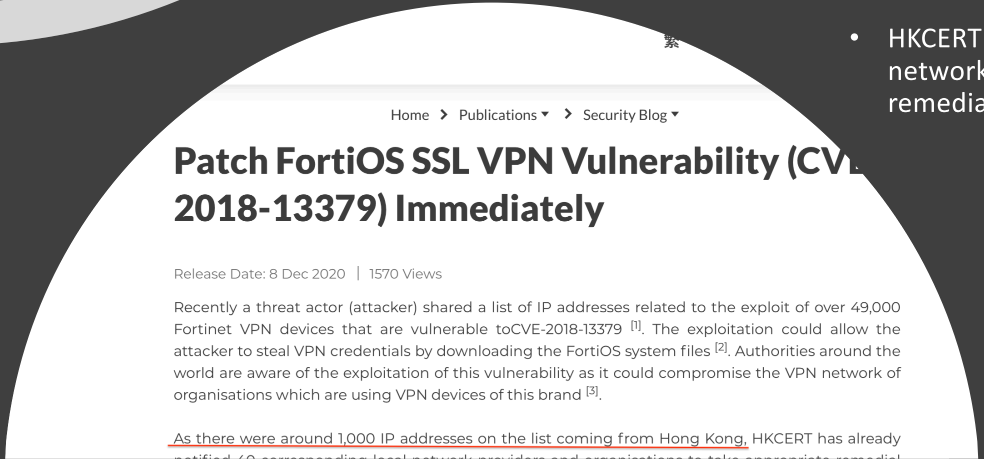
Access

[redacted]

my e-mail for contact: [redacted]

E-mail: [redacted]@protonmail.com
Jabber: [redacted]@xmpp.jp

Donate BTC:
1C4E3Fji8XKfB1tyyNLwBNNZpUjftYbD



Patch FortiOS SSL VPN Vulnerability (CVE-2018-13379) Immediately

Release Date: 8 Dec 2020 | 1570 Views

Recently a threat actor (attacker) shared a list of IP addresses related to the exploit of over 49,000 Fortinet VPN devices that are vulnerable toCVE-2018-13379 [1]. The exploitation could allow the attacker to steal VPN credentials by downloading the FortiOS system files [2]. Authorities around the world are aware of the exploitation of this vulnerability as it could compromise the VPN network of organisations which are using VPN devices of this brand [3].

As there were around 1,000 IP addresses on the list coming from Hong Kong, HKCERT has already notified 40 corresponding local network providers and organisations to take appropriate remedial

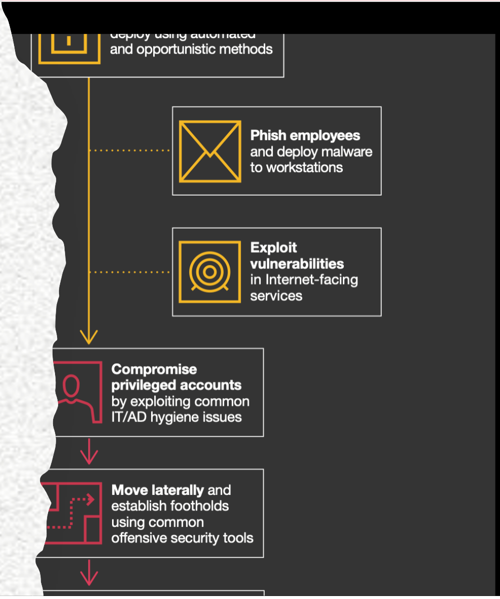
4

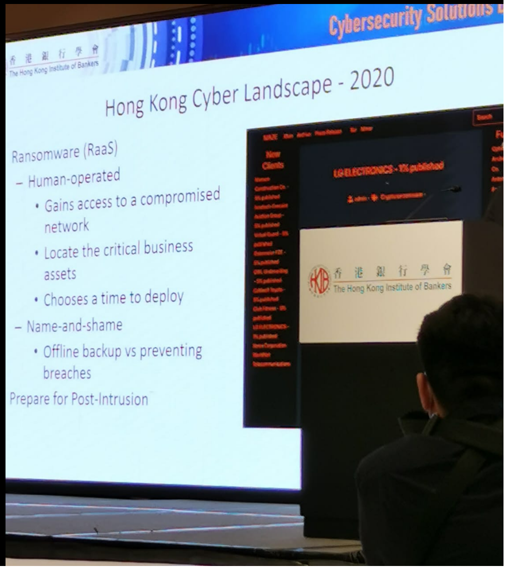
- The vulnerability is CVE-2018-13379, a path traversal flaw impacting a large number of unpatched Fortinet FortiOS SSL VPN devices.
- A hacker has posted a list of one-line exploits to steal VPN credentials from almost 50,000 Fortinet VPN devices.
- The list of vulnerable targets are domains belonging to banks and government organizations from around the world.
- Meh Chang(@mehqq_) and Orange Tsai(@orange_8361) published their works on 2019年8月10日 星期六.
- HKCERT has already notified 40 corresponding local network providers and organisations to take appropriate remedial actions promptly.

3

- Human-operated ransomware campaigns pose a significant and growing threat to businesses.
- In these hands-on-keyboard attacks, which are different from auto-spreading ransomware like WannaCry or NotPetya, adversaries employ credential theft and lateral movement methods like those from APT actors.
- They exhibit extensive knowledge of sysadmin and common security misconfigurations to what they discover in a compromised network.

The number of ransomware actors has grown steadily throughout 2020, encourage by the profits derived from high-profile attacks


deploy using automated and opportunistic methods
Phish employees and deploy malware to workstations
Exploit vulnerabilities in Internet-facing services
Compromise privileged accounts by exploiting common IT/AD hygiene issues
Move laterally and establish footholds using common offensive security tools


香港銀行學會
The Hong Kong Institute of Bankers
Cybersecurity Solutions

Hong Kong Cyber Landscape - 2020

Ransomware (RaaS)
- Human-operated
  - Gains access to a compromised network
  - Locate the critical business assets
  - Chooses a time to deploy
- Name-and-shame
  - Offline backup vs preventing breaches

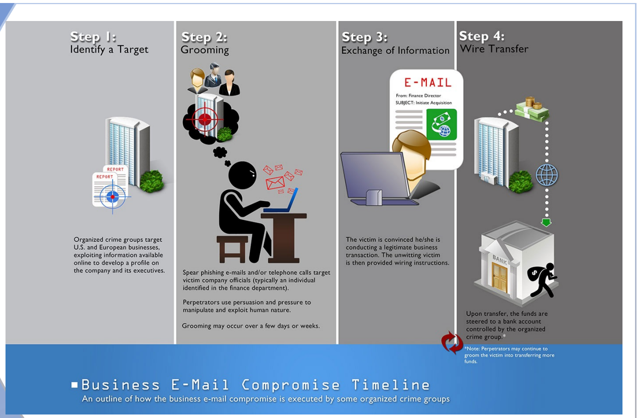
Prepare for Post-Intrusion

LG ELECTRONICS - 1% published
香港銀行學會
The Hong Kong Institute of Bankers

2

Phishing and BEC

- BEC is not a new type of attack but has greatly evolved over the past eight or nine years.
- FBI started tracking BEC attacks in 2013.
- BEC attacks are a combination of social engineering and phishing.
- These attacks rely on the actor being able to trick selected people to provide some amount of funds based on directions provided via email.
- The attacker would send an email to someone in finance, pretending to be the CEO, asking them to transfer money.
- The fake email can be difficult to identify.
- This technique has been surprisingly effective.



Step 1: Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

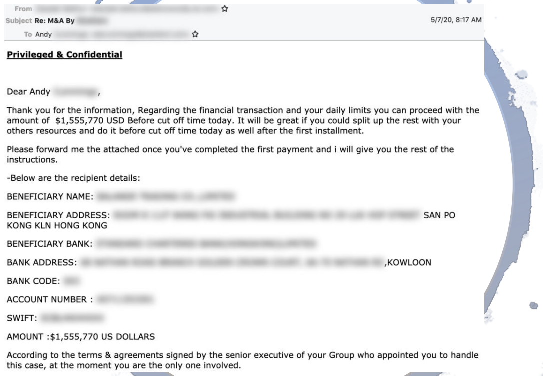
Step 4: Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

■ Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups



From [redacted] ☆
Subject Re: M&A By [redacted] 5/7/20, 8:17 AM
To Andy [redacted] ☆

Privileged & Confidential

Dear Andy [redacted],

Thank you for the information, Regarding the financial transaction and your daily limits you can proceed with the amount of $1,555,770 USD Before cut off time today. It will be great if you could split up the rest with your others resources and do it before cut off time today as well after the first installment.

Please forward me the attached once you've completed the first payment and i will give you the rest of the instructions.

-Below are the recipient details:

BENEFICIARY NAME: [redacted]

BENEFICIARY ADDRESS: [redacted] SAN PO KONG KLN HONG KONG

BENEFICIARY BANK: [redacted]

BANK ADDRESS: [redacted] ,KOWLOON

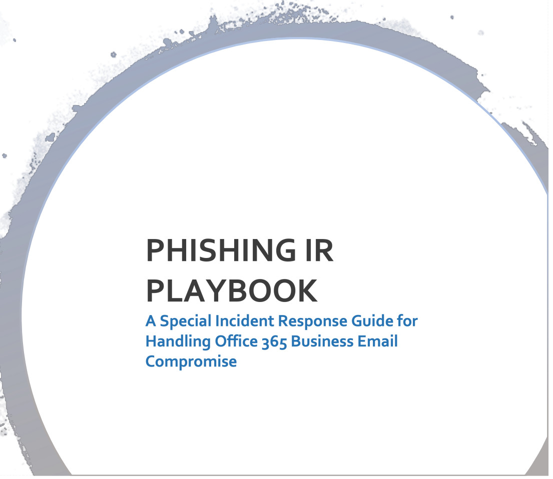
BANK CODE: [redacted]

ACCOUNT NUMBER : [redacted]

SWIFT: [redacted]

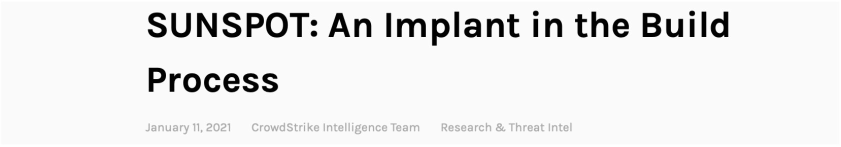
AMOUNT :$1,555,770 US DOLLARS

According to the terms & agreements signed by the senior executive of your Group who appointed you to handle this case, at the moment you are the only one involved.



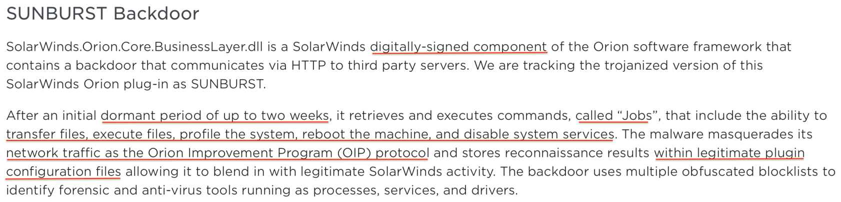
PHISHING IR PLAYBOOK

A Special Incident Response Guide for Handling Office 365 Business Email Compromise



SUNSPOT: An Implant in the Build Process

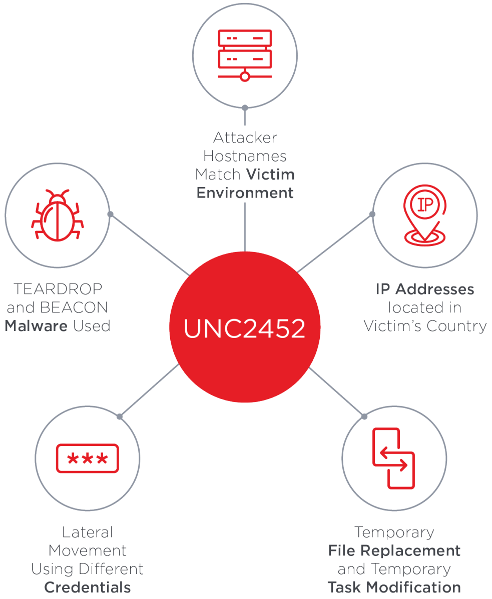
January 11, 2021 CrowdStrike Intelligence Team Research & Threat Intel

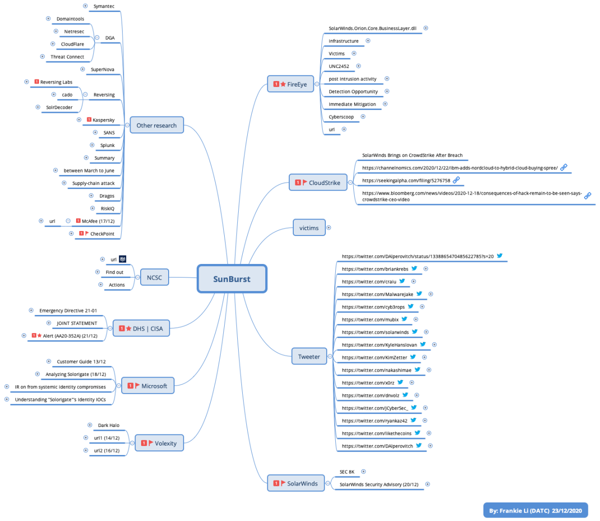


SUNBURST Backdoor

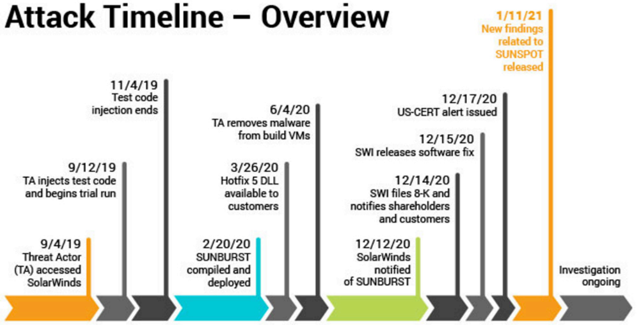
SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. We are tracking the trojanized version of this SolarWinds Orion plug-in as SUNBURST.

After an initial dormant period of up to two weeks, it retrieves and executes commands, called "Jobs", that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.


Attacker Hostnames Match Victim Environment
IP Addresses located in Victim's Country
Temporary File Replacement and Temporary Task Modification
Lateral Movement Using Different Credentials
TEARDROP and BEACON Malware Used
UNC2452
***
IP


SunBurst
Other research
Symantec
DGA
Domaintools
Netresec
CloudFlare
Threat Connect
SuperNova
Reversing
Reversing Labs
cado
SolrDecoder
Kaspersky
SANS
Splunk
Summary
between March to June
Supply-chain attack
Dragos
RiskIQ
McAfee (17/12)
url
CheckPoint
NCSC
url
Find out
Actions
DHS | CISA
Emergency Directive 21-01
JOINT STATEMENT
Alert (AA20-352A) (21/12)
Microsoft
Customer Guide 13/12
Analyzing Solorigate (18/12)
IR on from systemic identity compromises
Understanding "Solorigate"'s identity IOCs
Volexity
Dark Halo
url1 (14/12)
url2 (16/12)
FireEye
SolarWinds.Orion.Core.BusinessLayer.dll
infrastructure
Victims
UNC2452
post intrusion activity
Detection Opportunity
Immediate Mitigation
Cyberscoop
url
CloudStrike
SolarWinds Brings on CrowdStrike After Breach
https://channelnomics.com/2020/12/22/ibm-adds-nordcloud-to-hybrid-cloud-buying-spree/
https://seekingalpha.com/filing/5276758
https://www.bloomberg.com/news/videos/2020-12-18/consequences-of-hack-remain-to-be-seen-says-crowdstrike-ceo-video
victims
Tweeter
https://twitter.com/DAlperovitch/status/1338865470485622785?s=20
https://twitter.com/briankrebs
https://twitter.com/craiu
https://twitter.com/MalwareJake
https://twitter.com/cyb3rops
https://twitter.com/mubix
https://twitter.com/solarwinds
https://twitter.com/KyleHanslovan
https://twitter.com/KimZetter
https://twitter.com/nakashimae
https://twitter.com/x0rz
https://twitter.com/dnvolz
https://twitter.com/JCyberSec_
https://twitter.com/ryankaz42
https://twitter.com/likethecoins
https://twitter.com/DAlperovitch
SolarWinds
SEC 8K
SolarWinds Security Advisory (20/12)
By: Frankie Li (DATC) 23/12/2020

Attack Timeline – Overview



All events, dates, and times approximate and subject to change; pending completed investigation.

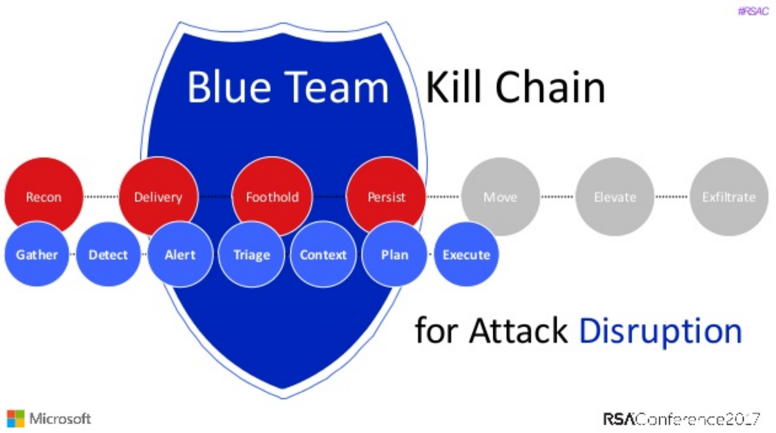
Supply chain attacks

The BT’s challenges

Dragon Advance Tech

Blue team’s defense

	Emotet	Vulnerable VPN	Human-operated Ransomware	BEC	SolarWinds
Hygiene	Some helps	Some helps	Some helps	Some helps	NO
Red Team	Phishing Tests	Yes, for Known vulnerability	Yes Lateral movements	Some helps on Phishing Tests	NO
EDR | IDS	Prevention Detection	Prevention Detection	Prevention Detection	no	Some helps
SOC | MSSP	Prevention Detection	Prevention Detection	Prevention Detection	Possible for M 365	NO
CTI & IR	Root cause	Escalation monitoring	Root cause	Mitigation & Root cause	Mitigation & Root cause



Q & A

Dragon Advance Tech

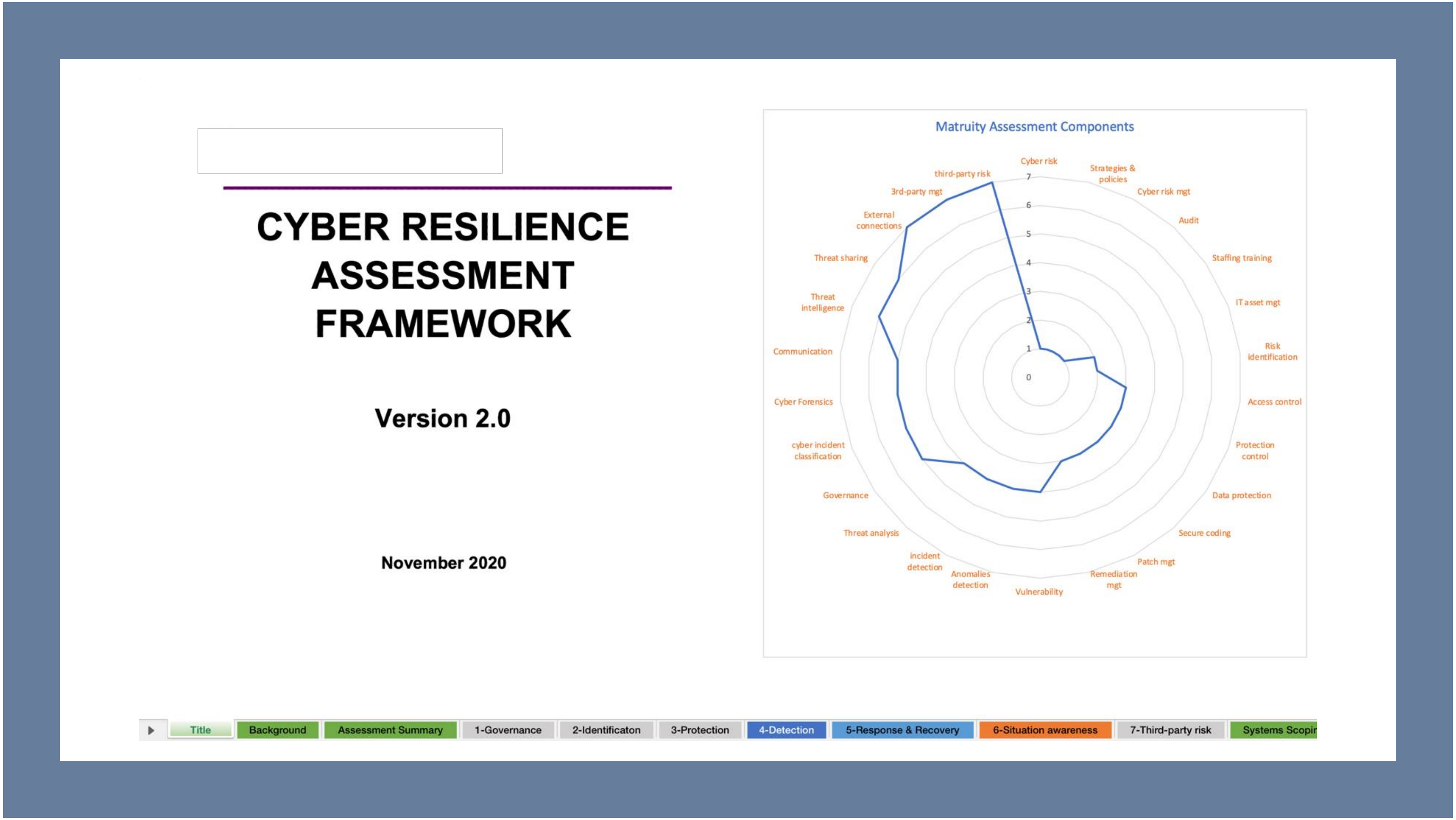
A follower's handbook: C-RAF 2.0

Feb 5, 2021 3:30pm-4:30pm

The Hong Kong Monetary Authority (HKMA) announced on 3 November 2020[1] the launch of an upgraded Cybersecurity Fortification Initiative (CFI) 2.0, following industry consultation. The initiative is underpinned by three pillars: the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Programme (PDP), and the Cyber Intelligence Sharing Platform (CISP).

As a long term follower of the initiative, I spent some time to study on what are actually changed on the CFI 2.0, or mainly the C-RAF 2.0. I have studied the official document and all referenced materials[2] to prepare this follower's handbook as quick reference for my friends in financial industry. I have also created an Excel spreadsheet (*C-RAF 2.0 Technical Implantation Tool*) which contains *the 7-Domains dive into the respective 26 Control Components of the Maturity Assessment* with my implementation guides for my own easy reference.

In this webinar, I shall ***share out*** and ***discuss*** on how to use my C-RAF 2.0 Technical Implantation Tool (Fig. 1) together with my recommended implementation guidelines on the Maturity Assessment Domain 4, 5 and 6. Attendants are welcome to join me as panel to ask questions and discuss your comments on the compliance requirements.



CYBER RESILIENCE ASSESSMENT FRAMEWORK

Version 2.0

November 2020