Weekly Intelligence Summary

Dec 28, 2020 (TLP: WHITE)

In the spotlight these LONG weeks:

- ESET disclosed a supply-chain attack against a certification authority in Southeast Asia on Dec 28. **#OperationSignSight**
- ESET disclosed another supply-chain attack against Able Desktop software on Dec 10. **#OperationStealthyTriden**
- Microsoft continues to investigate the extent of the recent nation-state attack on SolarWinds **# Solorigate**. Our goal is to provide the latest threat intelligence, Indicators of Compromise (IOC)s, and guidance across our products and solutions to help the community respond, harden infrastructure, and begin to recover from this unprecedented attack.
- FireEye has discovered a highly evasive global intrusion campaign by leveraging SolarWinds Supply Chain with **#SunbrustBackdoor**

TL;DR

This is my **last Weekly Intelligence Summary** for 2020.
As explained to friends in a webinar held on Dec 11, I want to provide the latest cyber threat intelligence updates to some of my clients who are working in cybersecurity roles for the financial institutions in Hong Kong. I understand the term Cyber Threat Intelligence (CTI) may have different meaning for different people. I found joys and pains on creating these summaries during the past 40-weeks. I always have the belief on the statement of "***IR is guided by CTI and CTI lives on the information collected from IR***". A friend who works in domestic bank (Hong Kong has no way to join FI-ISAC) asked me to recommend a good/cheap threat intel feed for banking sector in Hong Kong. I said: It depends on how you consume your "threat intel". I strongly feel that the banking industry in Hong Kong should not rely on buying a commercial feed to share between themselves for enhancing their threat intel capacity. What they should do is to allocate resources to build up the capacity on "intrusion analysis" covering their pre-compromise and post-compromise "incidents". If any TTP or IoCs can be extracted, such information should be shared through Sunshine laws. If IoCs are shared, we should consider to establish an ISAO and the information should be shared in (Peer-to-Peer or Hub-and-Spoke) TAXII formats. Wishing you guys have a safe and peach 2021 New Year.

(cisp-id:9804) Dec 28, 2020
Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia.
Just a few weeks after the supply-chain attack on the Able Desktop software, another similar attack occurred on the website of the Vietnam Government Certification Authority (VGCA): ca.gov.vn. The attackers modified two of the software installers available for download on this website and added a backdoor in order to compromise users of the legitimate application. According to ESET telemetry, ca.gov.vn was compromised from at least the 23rd of July to the 16th of August 2020. Two of the installers available for download, gca01-client-v2-x32-8.3.msi and gca01-client-v2-x64-8.3.msi, were modified to include a piece of malware known as PhantomNet or SManager and recently analyzed by NTT Security. We were able to confirm that those installers were downloaded from ca.gov.vn over the HTTPS protocol, so we believe it is unlikely to be a man-in-the-middle attack.
https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

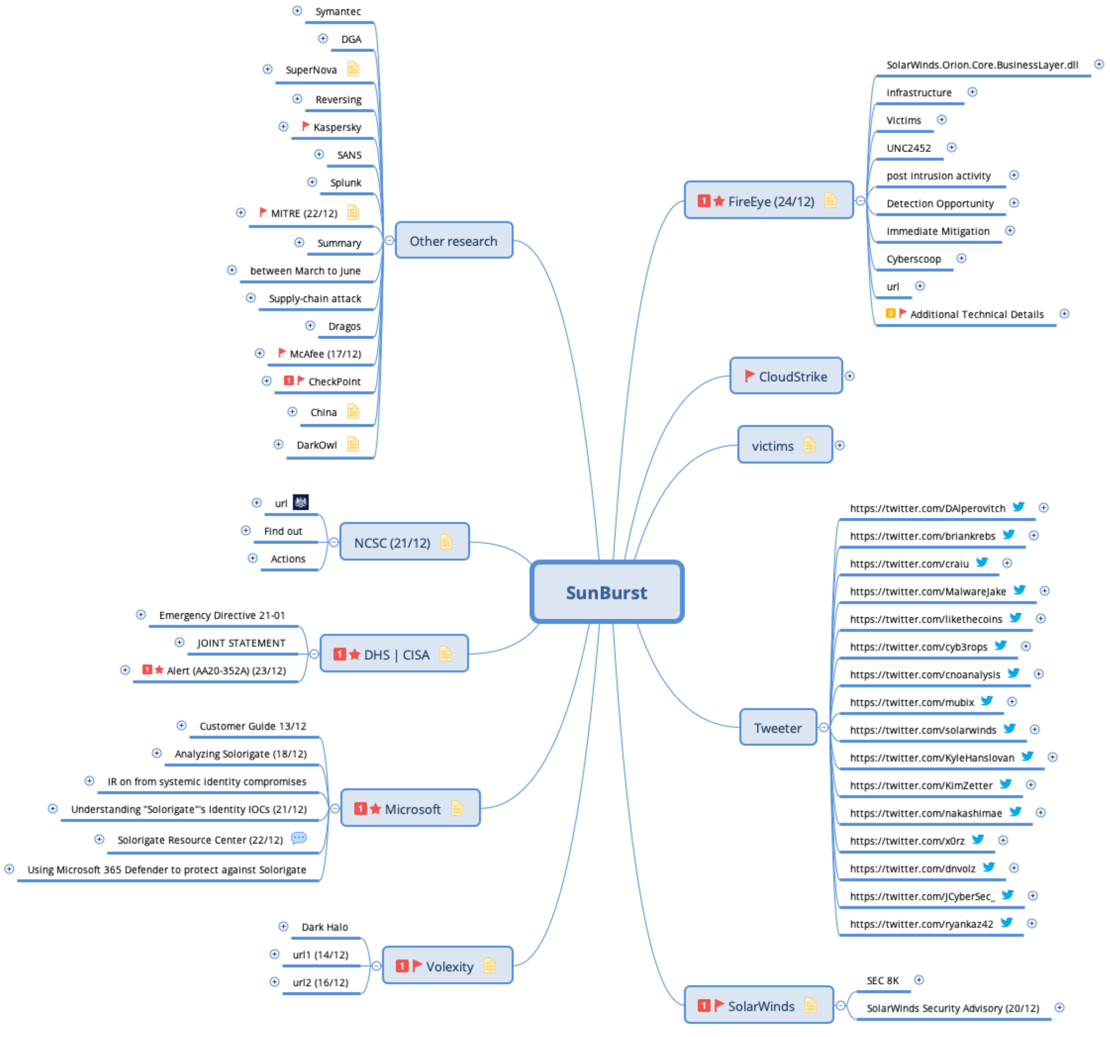
(cisp-id:9790) Dec 24, 2020
Russian crypto-exchange Livecoin hacked after it lost control of its servers.
Russian cryptocurrency exchange Livecoin posted on message on its official website on Christmas Eve claiming it was hacked and lost control of some of its servers, warning customers to stop using its services. Before Livecoin admins managed to gain back access to some of their systems during late December 24, the Bitcoin exchange rate had ballooned from the regular $23,000/BTC to more than $450,000/BTC, Ether grew from $600/ETH to $15,000. According to CoinMarketCap, Livecoin is ranked as the 173rd cryptocurrency exchange on the internet, with roughly $16 million in daily transactions.
https://www.zdnet.com/article/russian-crypto-exchange-livecoin-hacked-after-it-lost-control-of-its-servers/

(cisp-id:9785) Dec 23, 2020
Lazarus covets COVID-19-related intelligence.
While tracking the Lazarus group's continuous campaigns targeting various industries, we (Kaspersky) discovered that they recently went after COVID-19-related entities. They attacked a pharmaceutical company at the end of September, and during our investigation we discovered that they had also attacked a government ministry related to the COVID-19 response. Each attack used different tactics, techniques and procedures (TTPs), but we found connections between the two cases and evidence linking those attacks to the notorious Lazarus group.
https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/

(cisp-id:9791) Dec 22, 2020
Solorigate Resource Center – updated December 28th, 2020.
Alongside our industry partners and the security community, Microsoft continues to investigate the extent of the recent nation-state attack on SolarWinds. Our goal is to provide the latest threat intelligence, Indicators of Compromise (IOC)s, and guidance across our products and solutions to help the community respond, harden infrastructure, and begin to recover from this unprecedented attack. As new information becomes available, we will make updates to this article at https://aka.ms/solorigate. on 17/12 We posted an article from Brad Smith on the need for a unified approach to cybersecurity and how we respond to attacks. on 13/12 We published a blog from John Lambert outlining this dynamic threat landscape and the principles with which we are approaching the investigation and Important steps for customers to protect themselves. On 13/12 We published a summary of what we know about the actors methods. This post will be updated with new information as the investigation continues.
https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/

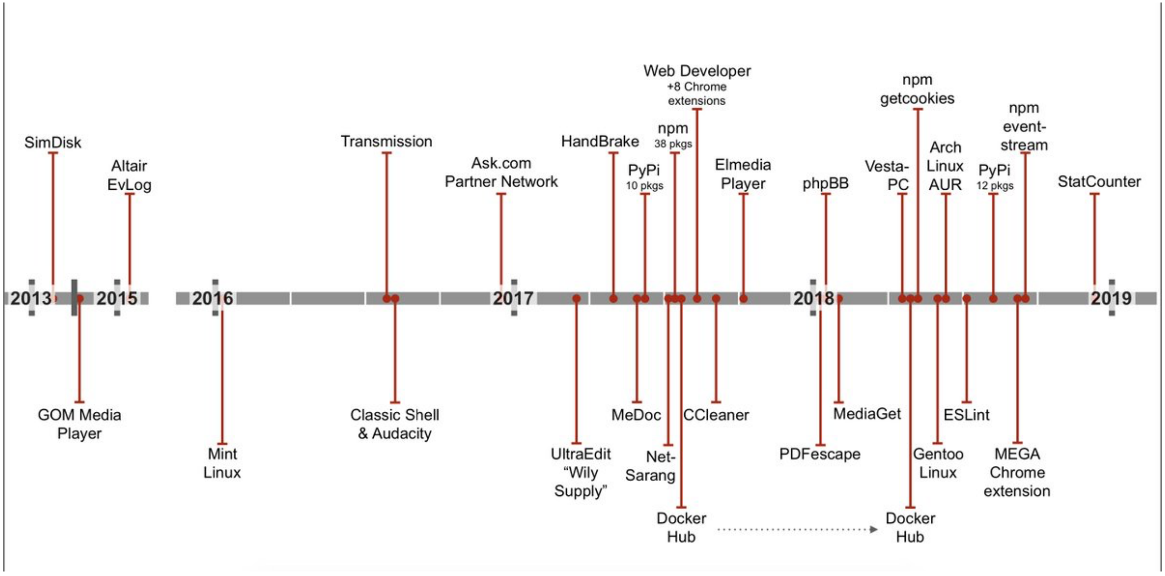
(cisp-id:9809) Dec 13, 2020
Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.
We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452. (a) FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST. (b) The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection. (c) The campaign is widespread, affecting public and private organizations around the world. (d) 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.
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

We summaries the SolarWinds incident by way of a continuously updated mind map. You can download the Xmind file at: https://www.dropbox.com/s/97byaygf0u6xmoi/SunBurst.xmind?dl=0

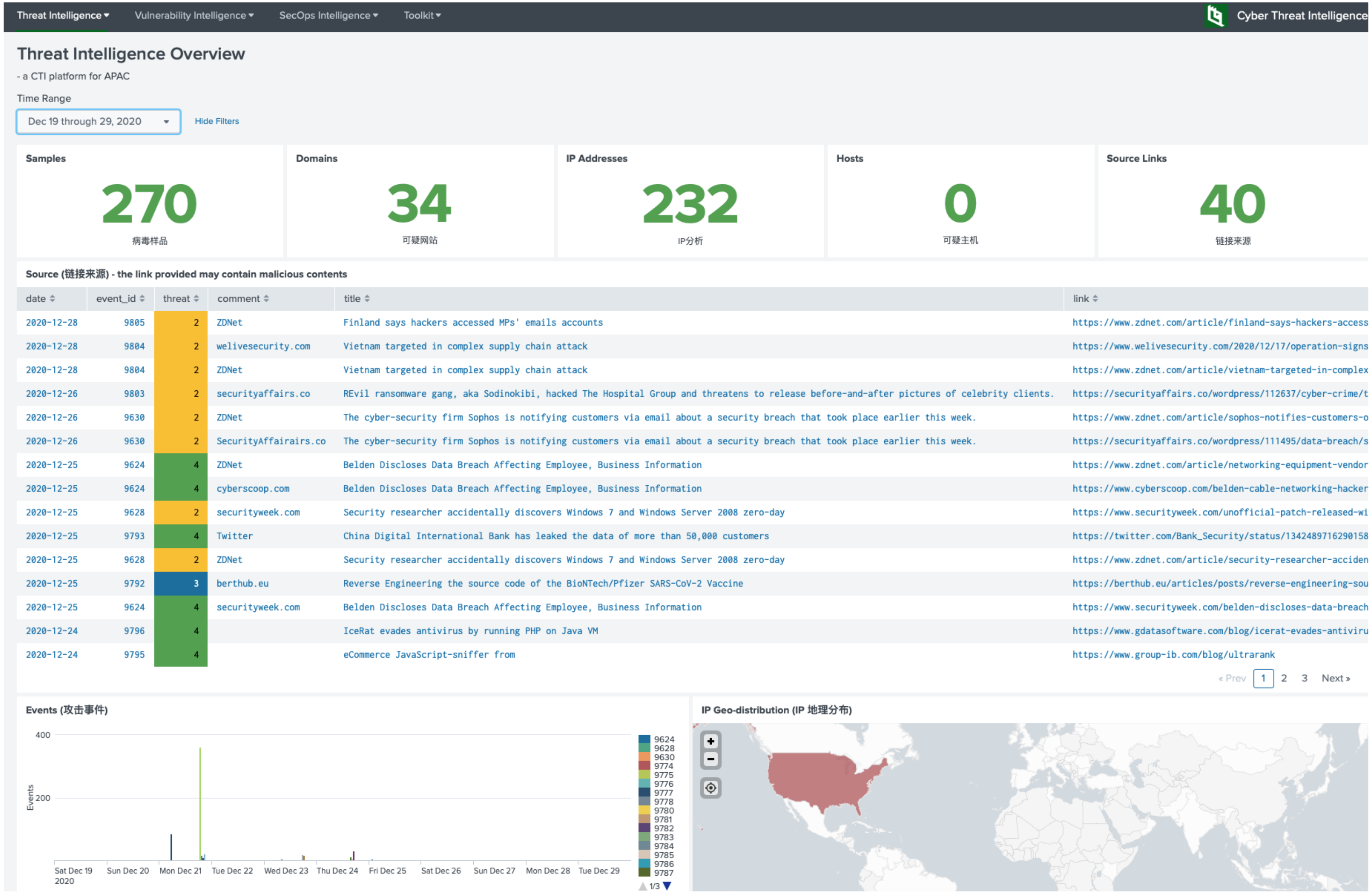

SunBurst
Other research
Symantec
DGA
SuperNova
Reversing
Kaspersky
SANS
Splunk
MITRE (22/12)
Summary
between March to June
Supply-chain attack
Dragos
McAfee (17/12)
1 CheckPoint
China
DarkOwl
NCSC (21/12)
url
Find out
Actions
1 DHS | CISA
Emergency Directive 21-01
JOINT STATEMENT
1 Alert (AA20-352A) (23/12)
1 Microsoft
Customer Guide 13/12
Analyzing Solorigate (18/12)
IR on from systemic identity compromises
Understanding "Solorigate"'s Identity IOCs (21/12)
Solorigate Resource Center (22/12)
Using Microsoft 365 Defender to protect against Solorigate
1 Volexity
Dark Halo
url1 (14/12)
url2 (16/12)
1 FireEye (24/12)
SolarWinds.Orion.Core.BusinessLayer.dll
infrastructure
Victims
UNC2452
post intrusion activity
Detection Opportunity
Immediate Mitigation
Cyberscoop
url
2 Additional Technical Details
CloudStrike
victims
Tweeter
https://twitter.com/DAlperovitch
https://twitter.com/briankrebs
https://twitter.com/craiu
https://twitter.com/MalwareJake
https://twitter.com/likethecoins
https://twitter.com/cyb3rops
https://twitter.com/cnoanalysis
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
1 SolarWinds
SEC 8K
SolarWinds Security Advisory (20/12)

By: Frankie Li (Ran2) 28/12/2020
@espionageware

The last 2 weeks of 2020 ends with flooded information about SolarWinds Supply Chain Attacks. I found the following screen capture from twitter but not able to provide its source. We should re-consider topics of secure DevOps and new cybersecurity posture again in 2021. #SANS #SEC534



Our Threat Intelligence Platform (http://dashboard.cisp.org.hk/) is ready for public access.



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Dec 19 through 29, 2020

Samples	Domains	IP Addresses	Hosts	Source Links
270	34	232	0	40
病毒样品	可疑网站	IP分析	可疑主机	链接来源

Source (链接来源) - the link provided may contain malicious contents

date	event_id	threat	comment	title	link
2020-12-28	9805	2	ZDNet	Finland says hackers accessed MPs' emails accounts	https://www.zdnet.com/article/finland-says-hackers-access
2020-12-28	9804	2	welivesecurity.com	Vietnam targeted in complex supply chain attack	https://www.welivesecurity.com/2020/12/17/operation-signs
2020-12-28	9804	2	ZDNet	Vietnam targeted in complex supply chain attack	https://www.zdnet.com/article/vietnam-targeted-in-complex
2020-12-26	9803	2	securityaffairs.co	REvil ransomware gang, aka Sodinokibi, hacked The Hospital Group and threatens to release before-and-after pictures of celebrity clients.	https://securityaffairs.co/wordpress/112637/cyber-crime/t
2020-12-26	9630	2	ZDNet	The cyber-security firm Sophos is notifying customers via email about a security breach that took place earlier this week.	https://www.zdnet.com/article/sophos-notifies-customers-o
2020-12-26	9630	2	SecurityAffairairs.co	The cyber-security firm Sophos is notifying customers via email about a security breach that took place earlier this week.	https://securityaffairs.co/wordpress/111495/data-breach/s
2020-12-25	9624	4	ZDNet	Belden Discloses Data Breach Affecting Employee, Business Information	https://www.zdnet.com/article/networking-equipment-vendor
2020-12-25	9624	4	cyberscoop.com	Belden Discloses Data Breach Affecting Employee, Business Information	https://www.cyberscoop.com/belden-cable-networking-hacker
2020-12-25	9628	2	securityweek.com	Security researcher accidentally discovers Windows 7 and Windows Server 2008 zero-day	https://www.securityweek.com/unofficial-patch-released-wi
2020-12-25	9793	4	Twitter	China Digital International Bank has leaked the data of more than 50,000 customers	https://twitter.com/Bank_Security/status/1342489716290158
2020-12-25	9628	2	ZDNet	Security researcher accidentally discovers Windows 7 and Windows Server 2008 zero-day	https://www.zdnet.com/article/security-researcher-acciden
2020-12-25	9792	3	berthub.eu	Reverse Engineering the source code of the BioNTech/Pfizer SARS-CoV-2 Vaccine	https://berthub.eu/articles/posts/reverse-engineering-sou
2020-12-25	9624	4	securityweek.com	Belden Discloses Data Breach Affecting Employee, Business Information	https://www.securityweek.com/belden-discloses-data-breach
2020-12-24	9796	4		IceRat evades antivirus by running PHP on Java VM	https://www.gdatasoftware.com/blog/icerat-evades-antiviru
2020-12-24	9795	4		eCommerce JavaScript-sniffer from	https://www.group-ib.com/blog/ultrarank

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

Get access? please send an email to: admin@dragonadvancetech.com