Cyber Attack Trend Analysis

Presented by
Lawrence LAW
Security Consultant
HKCERT
5/2/2021

Cybersecurity - HKCERT

coordination of cybersecurity incident response for local enterprises and Internet Users.

HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

Hotline: 8105 6060

HKCERT services

01 Security Alert Monitoring and Early Warning

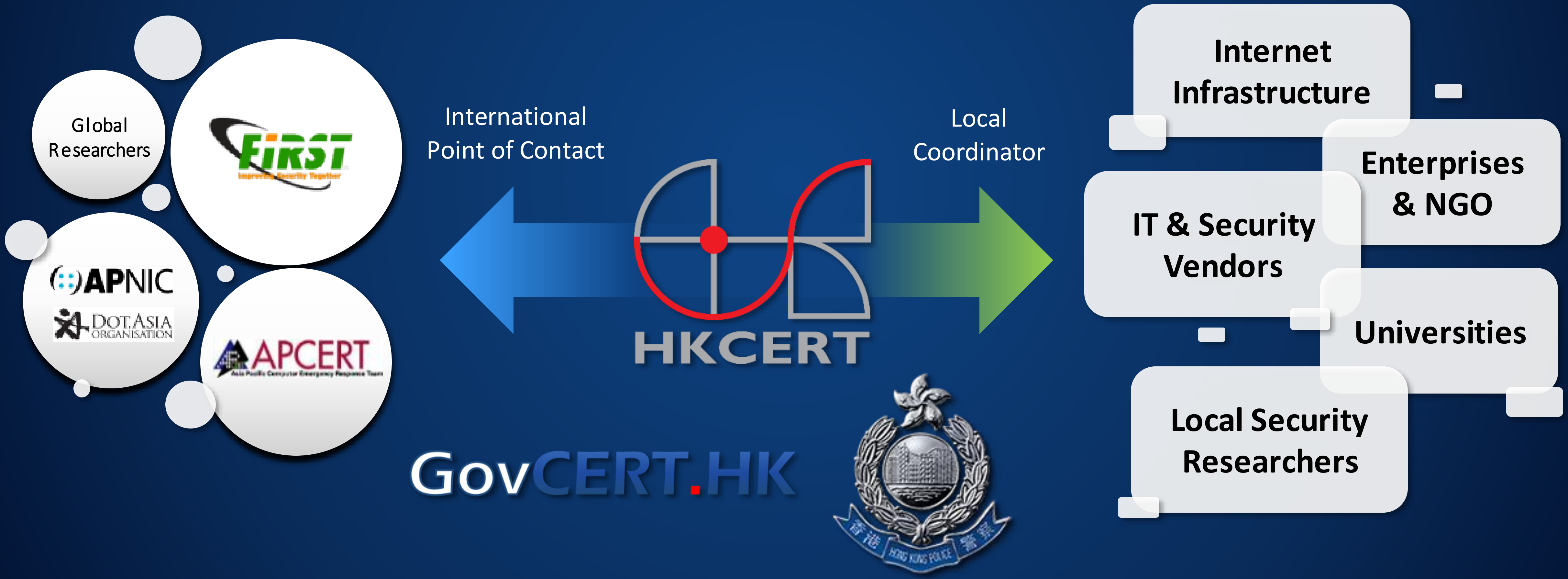
02 Report and Response

03 Publication of Security Guidelines and Informatior

04 Promotion of Information Security Awareness

HKCERT acts as

point of contact for cross-border cyber security incidents for Hong Kong



Global Researchers

FIRST

APNIC

DOT ASIA ORGANISATION

APCERT

International Point of Contact

HKCERT

Local Coordinator

GovCERT.HK

Internet Infrastructure

Enterprises & NGO

IT & Security Vendors

Universities

Local Security Researchers

Agenda

Security Threat and Challenges

Attack Tactics and Trends

Cyber Attack Case Studies

Security Advices

Threat landscape changes along with the "New Normal"

Remote Work

Distance Learning

Digital and Contactless Payments

Tele-Medicine

Online Entertainment

Robotics

Online Shopping

Image source: https://tech.sina.com.cn/i/2019-01-03/doc-ihqhqcis2680845.shtml

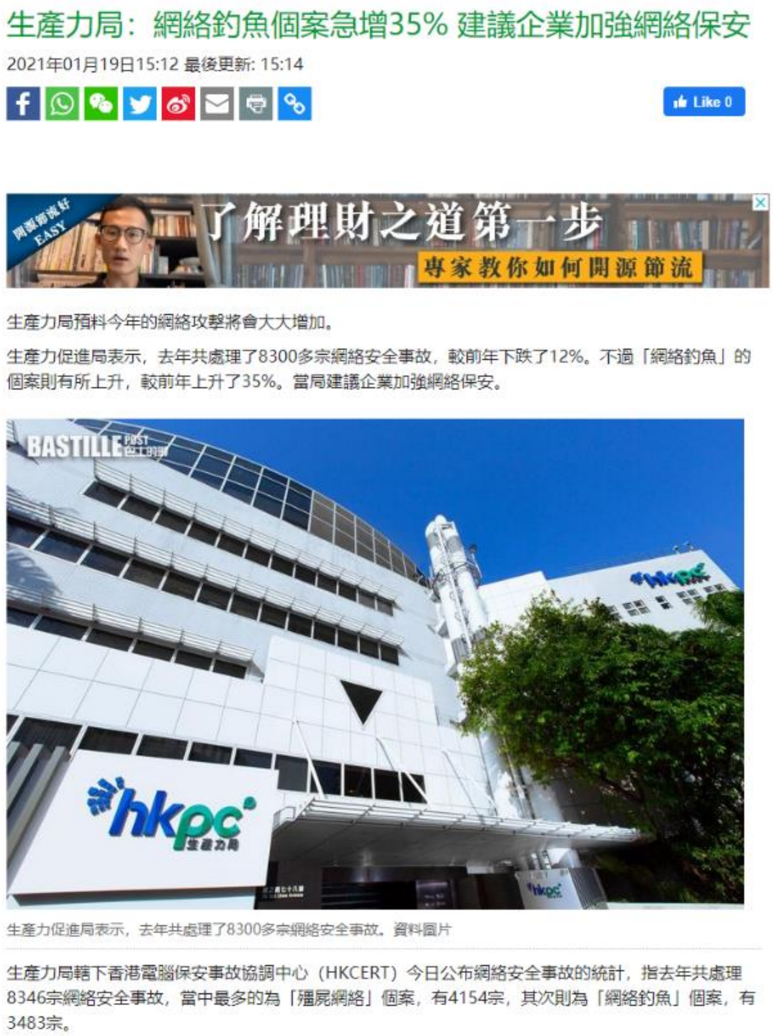
“The COVID-19 crisis illustrated how criminals actively take advantage of society at its most vulnerable. Criminals ***tweaked existing*** *forms of cybercrime to fit the* ***pandemic narrative****, abused the uncertainty of the situation and the public’s need for reliable information.”* – Europol Internet Organised Crime Threat Assessment 2020

Source: Europol Internet Organised Crime Threat Assessment 2020
(https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020)

HKCERT Security Incident Reports 2020

Phishing Cases (YoY)

↑ 35%



生產力局：網絡釣魚個案急增35% 建議企業加強網絡保安

2021年01月19日15:12 最後更新: 15:14

生產力局預料今年的網絡攻擊將會大大增加。

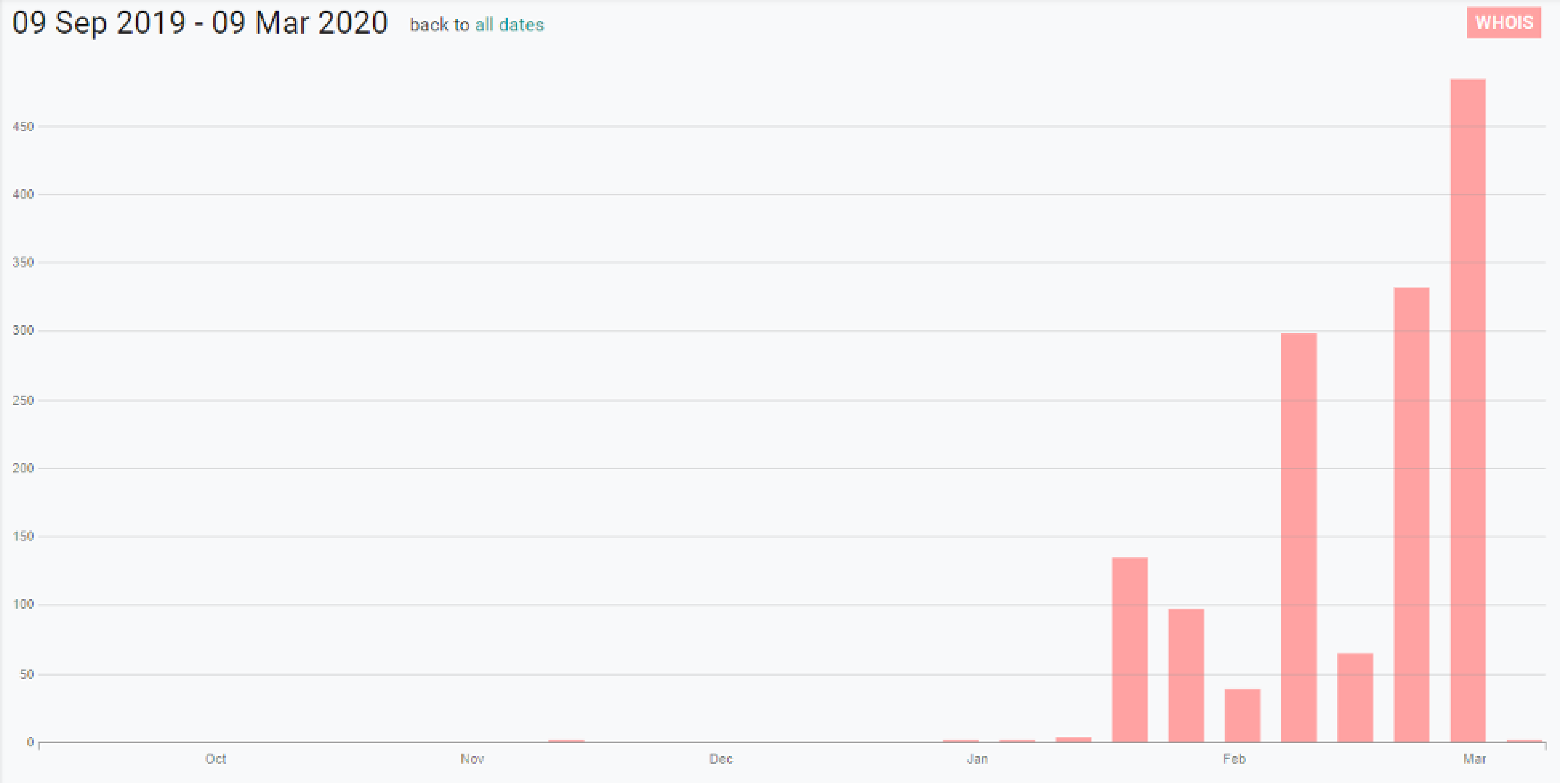
生產力促進局表示，去年共處理了8300多宗網絡安全事故，較前年下跌了12%。不過「網絡釣魚」的個案則有所上升，較前年上升了35%。當局建議企業加強網絡保安。

生產力促進局表示，去年共處理了8300多宗網絡安全事故。資料圖片

生產力局轄下香港電腦保安事故協調中心（HKCERT）今日公布網絡安全事故的統計，指去年共處理8346宗網絡安全事故，當中最多的為「殭屍網絡」個案，有4154宗，其次則為「網絡釣魚」個案，有3483宗。

Source: https://www.hkcert.org/press-center/hkpc-urges-enterprises-for-cyber-security-strategy-for-the-new-normal-and-new-technologies
https://www.bastillepost.com/hongkong/article/7824019-%E7%B6%B2%E7%B5%A1%E9%87%A3%E9%AD%9A%E5%80%8B%E6%A1%88%E6%80%A5%E5%A2%9E35-%E7%94%9F%E7%94%A2%E5%8A%9B%E5%B1%80%E5%BB%BA%E8%AD%B0%E4%BC%81%E6%A5%AD%E5%8A%A0%E5%BC%B7%E7%B6%B2%E7%B5%A1%E4%BF%9D

Surge in COVID-19-related domains

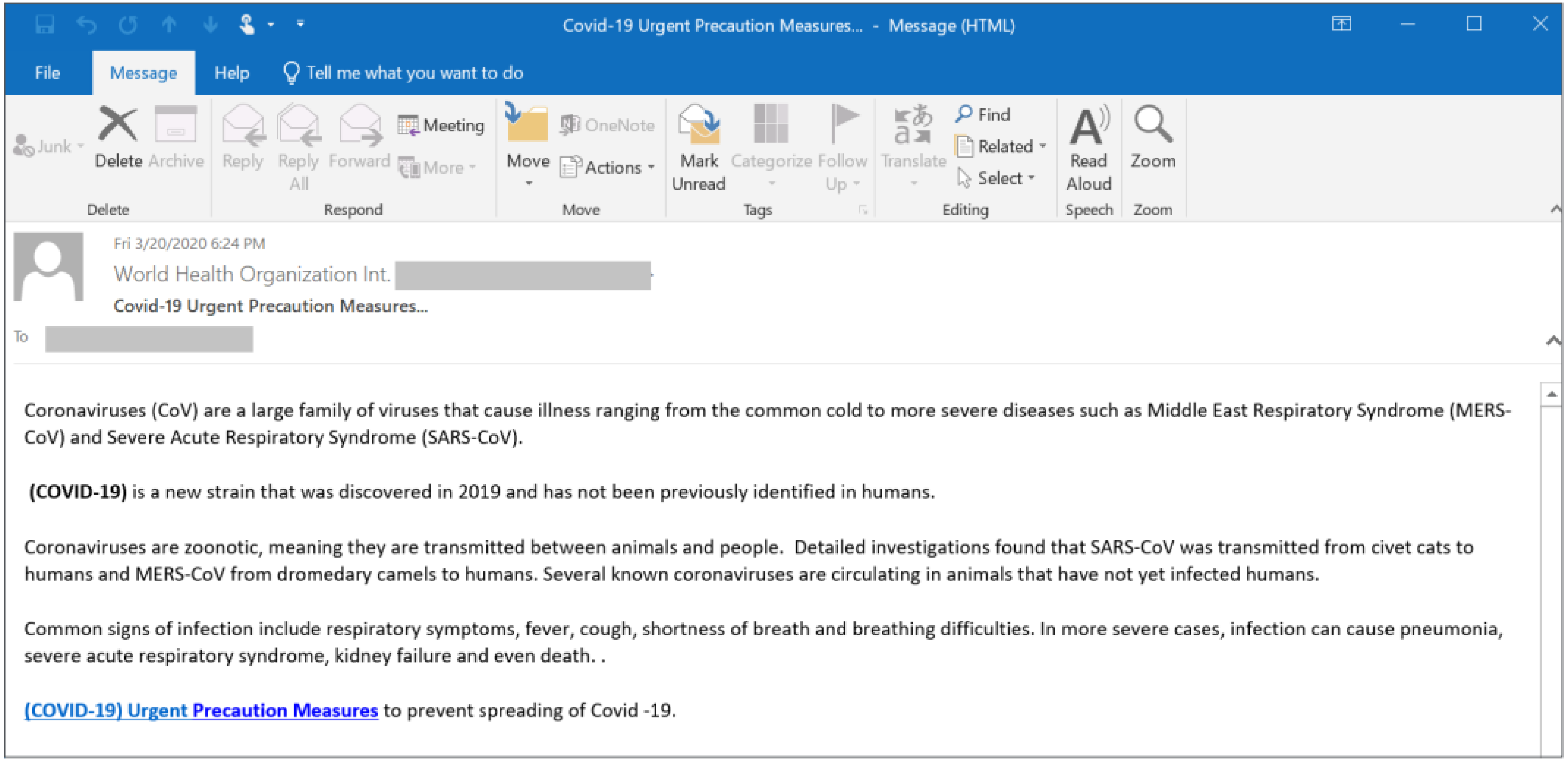


Source: Digital Shadows' Shadow Search

Source: https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/

Phishing Attacks Related to the Pandemic

- Fake health organisations



Fri 3/20/2020 6:24 PM

World Health Organization Int. [redacted]

Covid-19 Urgent Precaution Measures...

To [redacted]

Coronaviruses (CoV) are a large family of viruses that cause illness ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS-CoV) and Severe Acute Respiratory Syndrome (SARS-CoV).

(COVID-19) is a new strain that was discovered in 2019 and has not been previously identified in humans.

Coronaviruses are zoonotic, meaning they are transmitted between animals and people. Detailed investigations found that SARS-CoV was transmitted from civet cats to humans and MERS-CoV from dromedary camels to humans. Several known coronaviruses are circulating in animals that have not yet infected humans.

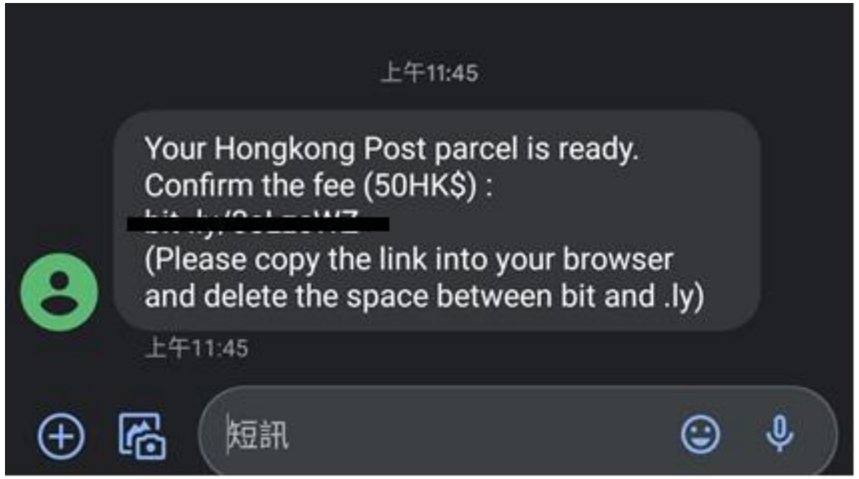
Common signs of infection include respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. In more severe cases, infection can cause pneumonia, severe acute respiratory syndrome, kidney failure and even death. .

(COVID-19) Urgent Precaution Measures to prevent spreading of Covid -19.

Source: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf

Phishing Attacks Related to the Pandemic

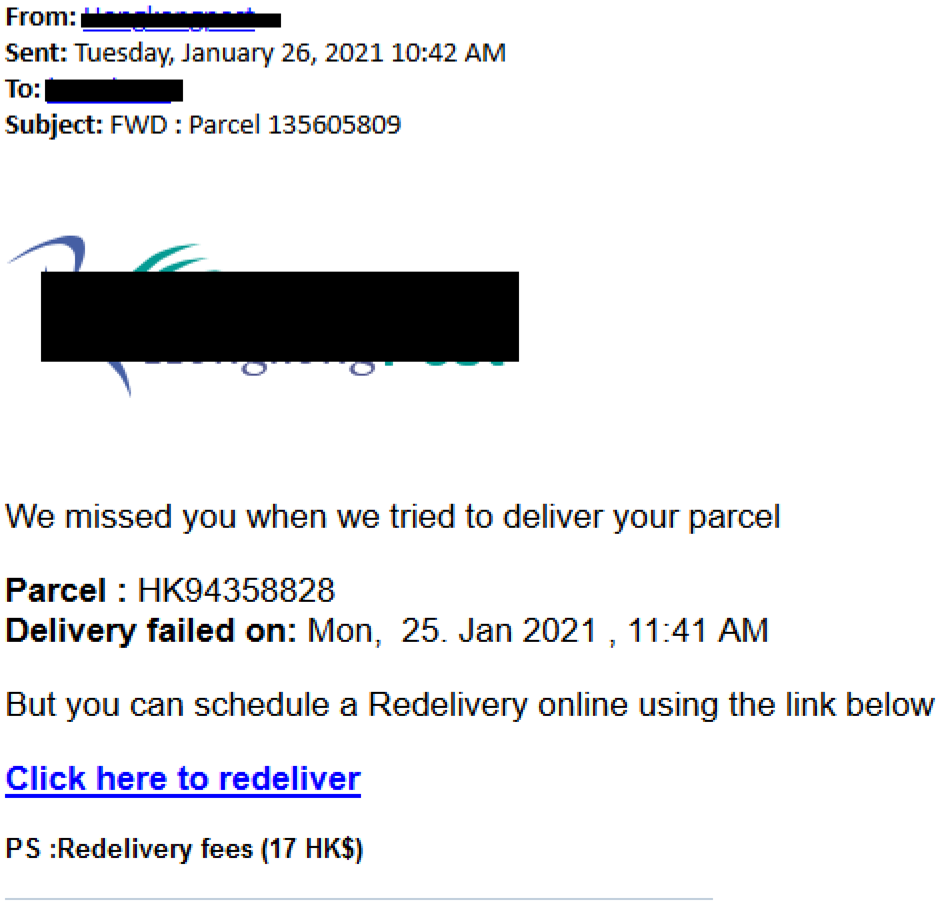
- Fake shipping information



上午11:45

Your Hongkong Post parcel is ready.
Confirm the fee (50HK$) :
[redacted]
(Please copy the link into your browser and delete the space between bit and .ly)

上午11:45



From: [redacted]
Sent: Tuesday, January 26, 2021 10:42 AM
To: [redacted]
Subject: FWD : Parcel 135605809

[redacted]

We missed you when we tried to deliver your parcel

Parcel : HK94358828
Delivery failed on: Mon, 25. Jan 2021 , 11:41 AM

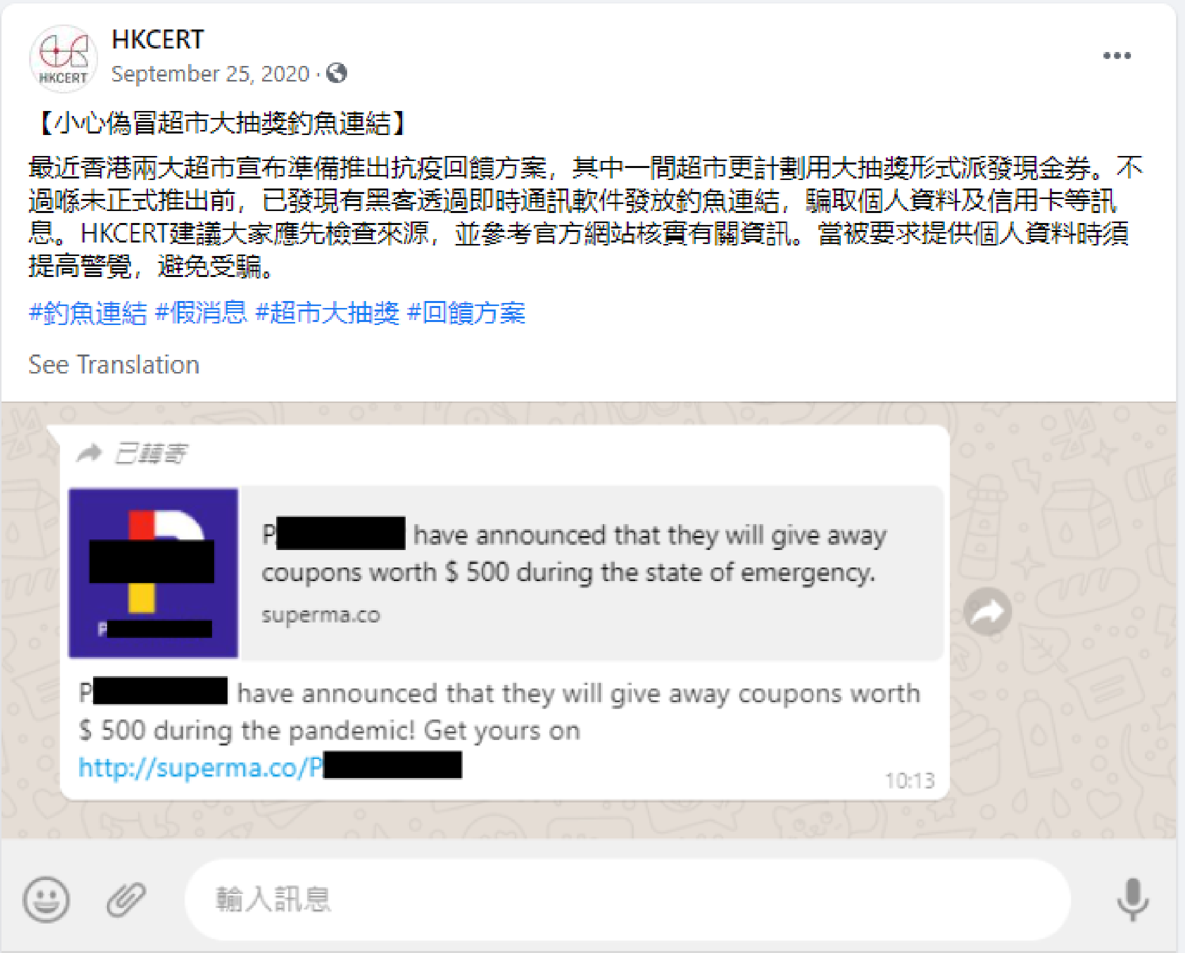
But you can schedule a Redelivery online using the link below

Click here to redeliver

PS :Redelivery fees (17 HK$)

Phishing Attacks Related to the Pandemic

- Fake supermarket information



HKCERT
September 25, 2020 ·

【小心偽冒超市大抽獎釣魚連結】

最近香港兩大超市宣布準備推出抗疫回饋方案，其中一間超市更計劃用大抽獎形式派發現金券。不過喺未正式推出前，已發現有黑客透過即時通訊軟件發放釣魚連結，騙取個人資料及信用卡等訊息。HKCERT建議大家應先檢查來源，並參考官方網站核實有關資訊。當被要求提供個人資料時須提高警覺，避免受騙。

#釣魚連結 #假消息 #超市大抽獎 #回饋方案

See Translation

已轉寄

P[redacted] have announced that they will give away coupons worth $ 500 during the state of emergency.
superma.co

P[redacted] have announced that they will give away coupons worth $ 500 during the pandemic! Get yours on http://superma.co/P[redacted]
10:13

輸入訊息

Source: https://www.facebook.com/hkcert/posts/1063246020762021

More Phishing Websites Using Digital Certificate

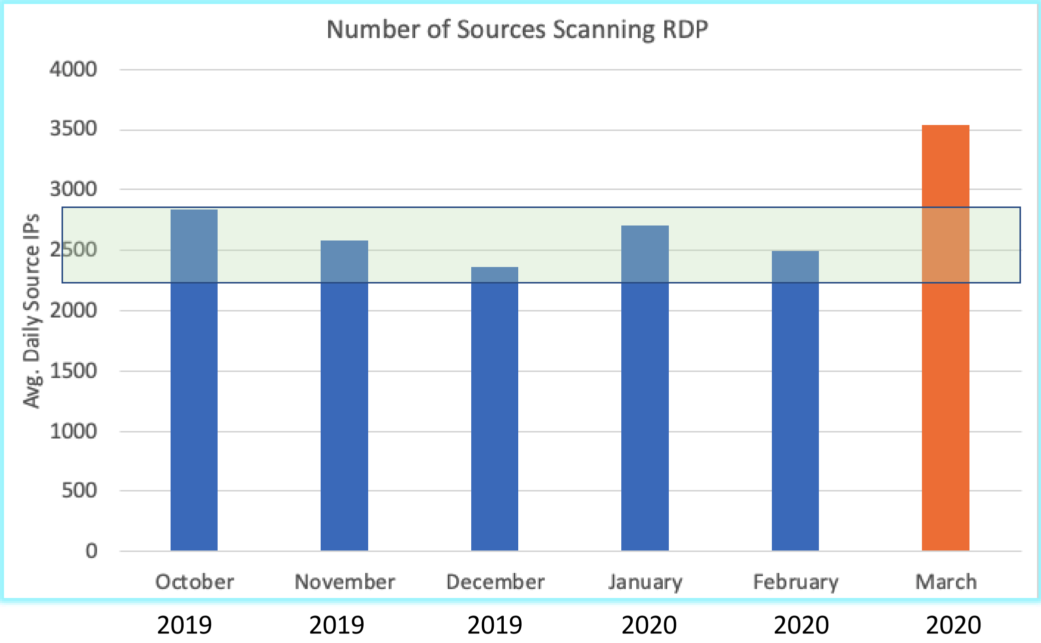
🔒 https:// Attackers make website look trustworthy by using digital certificates

HKCERT incident statistics

- 34% phishing sites using HTTPS in 2020 (YoY +9%)

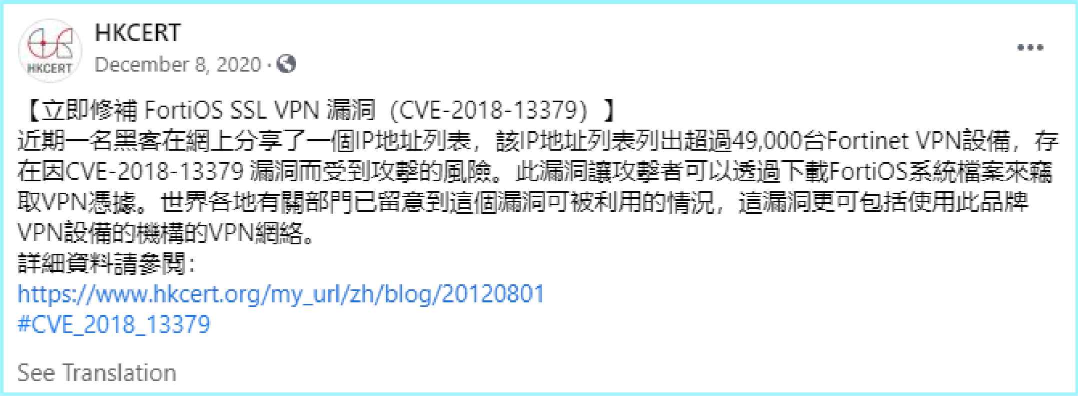
More Attacks Targeting Remote Access

- Internet-accessible Remote Desktop Protocol (RDP)

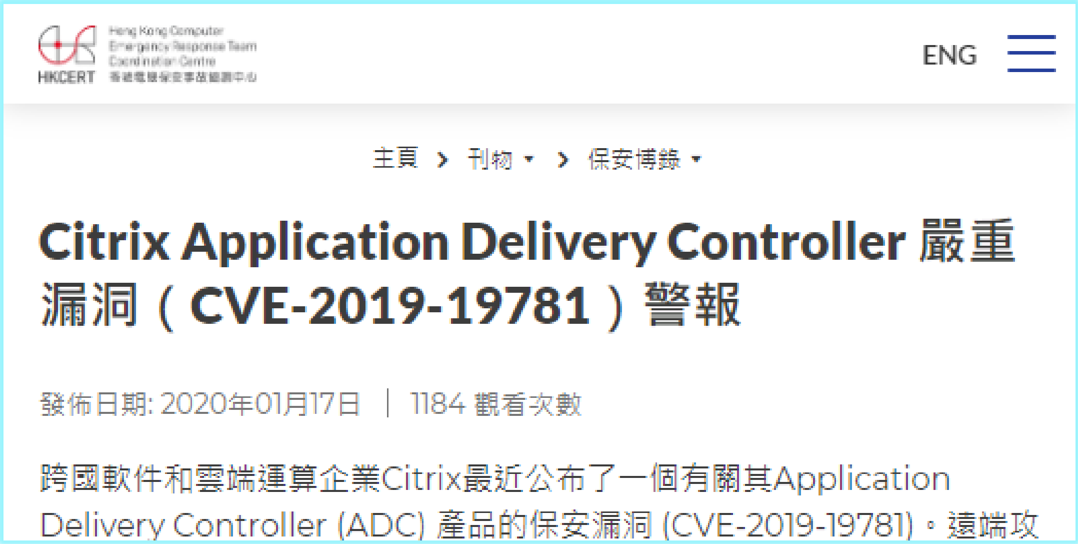


Source: Johannes B. Ullrich, Ph.D., Dean of Research, SANS Technology Institute

- VPN gateway vulnerabilities


HKCERT
December 8, 2020 ·

【立即修補 FortiOS SSL VPN 漏洞（CVE-2018-13379）】
近期一名黑客在網上分享了一個IP地址列表，該IP地址列表列出超過49,000台Fortinet VPN設備，存在因CVE-2018-13379 漏洞而受到攻擊的風險。此漏洞讓攻擊者可以透過下載FortiOS系統檔案來竊取VPN憑據。世界各地有關部門已留意到這個漏洞可被利用的情況，這漏洞更可包括使用此品牌VPN設備的機構的VPN網絡。
詳細資料請參閱：
https://www.hkcert.org/my_url/zh/blog/20120801
#CVE_2018_13379



Citrix Application Delivery Controller 嚴重漏洞（CVE-2019-19781）警報

發佈日期: 2020年01月17日 | 1184 觀看次數

跨國軟件和雲端運算企業Citrix最近公布了一個有關其Application Delivery Controller (ADC) 產品的保安漏洞 (CVE-2019-19781)。遠端攻

Source: https://www.facebook.com/hkcert/posts/1121504591602830
https://www.hkcert.org/tc/blog/critical-citrix-application-delivery-controller-vulnerability-cve-2019-19781-alert

Attack Tactics and Trends

Security Outlook for 2021

1. Security Risks of the New Normal

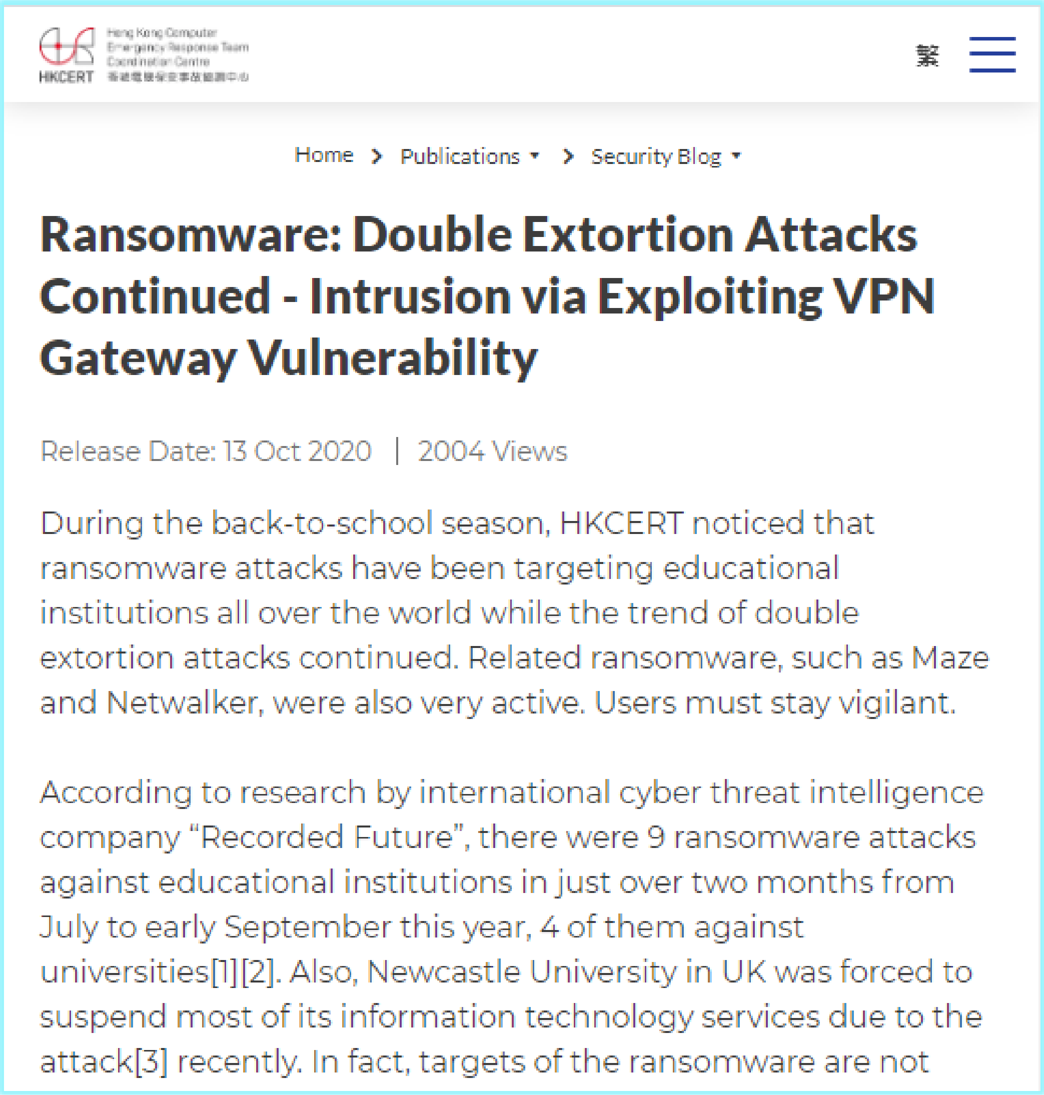
2. Security Risks of New Technologies

3. Security Risks of Mobile Financial Services

4. Proliferated Targeted and Organised Cyber Attacks

5. Escalated Supply Chain Attacks

Ransomware



HKCERT Hong Kong Computer Emergency Response Team Coordination Centre 香港電腦保安事故協調中心

繁

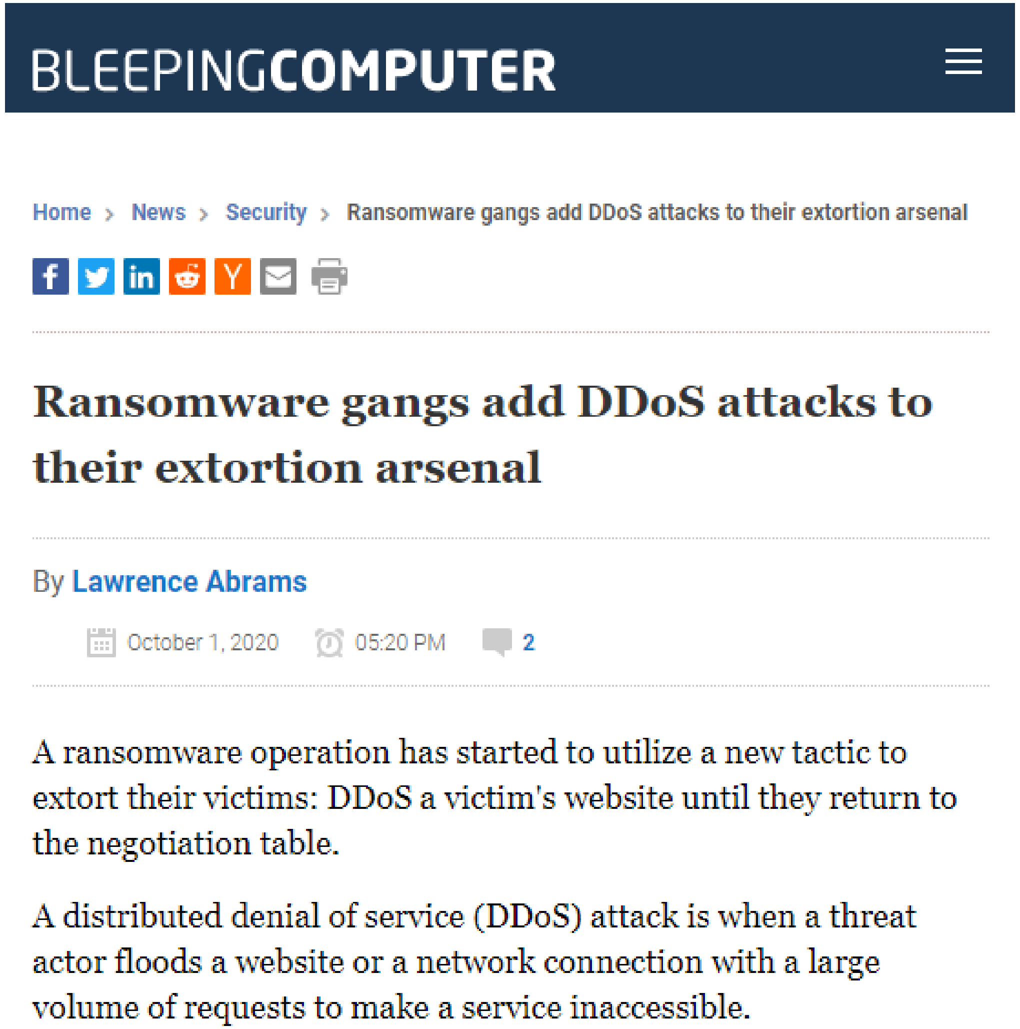
Home > Publications ▾ > Security Blog ▾

Ransomware: Double Extortion Attacks Continued - Intrusion via Exploiting VPN Gateway Vulnerability

Release Date: 13 Oct 2020 | 2004 Views

During the back-to-school season, HKCERT noticed that ransomware attacks have been targeting educational institutions all over the world while the trend of double extortion attacks continued. Related ransomware, such as Maze and Netwalker, were also very active. Users must stay vigilant.

According to research by international cyber threat intelligence company "Recorded Future", there were 9 ransomware attacks against educational institutions in just over two months from July to early September this year, 4 of them against universities[1][2]. Also, Newcastle University in UK was forced to suspend most of its information technology services due to the attack[3] recently. In fact, targets of the ransomware are not



BLEEPINGCOMPUTER

Home > News > Security > Ransomware gangs add DDoS attacks to their extortion arsenal

Ransomware gangs add DDoS attacks to their extortion arsenal

By Lawrence Abrams

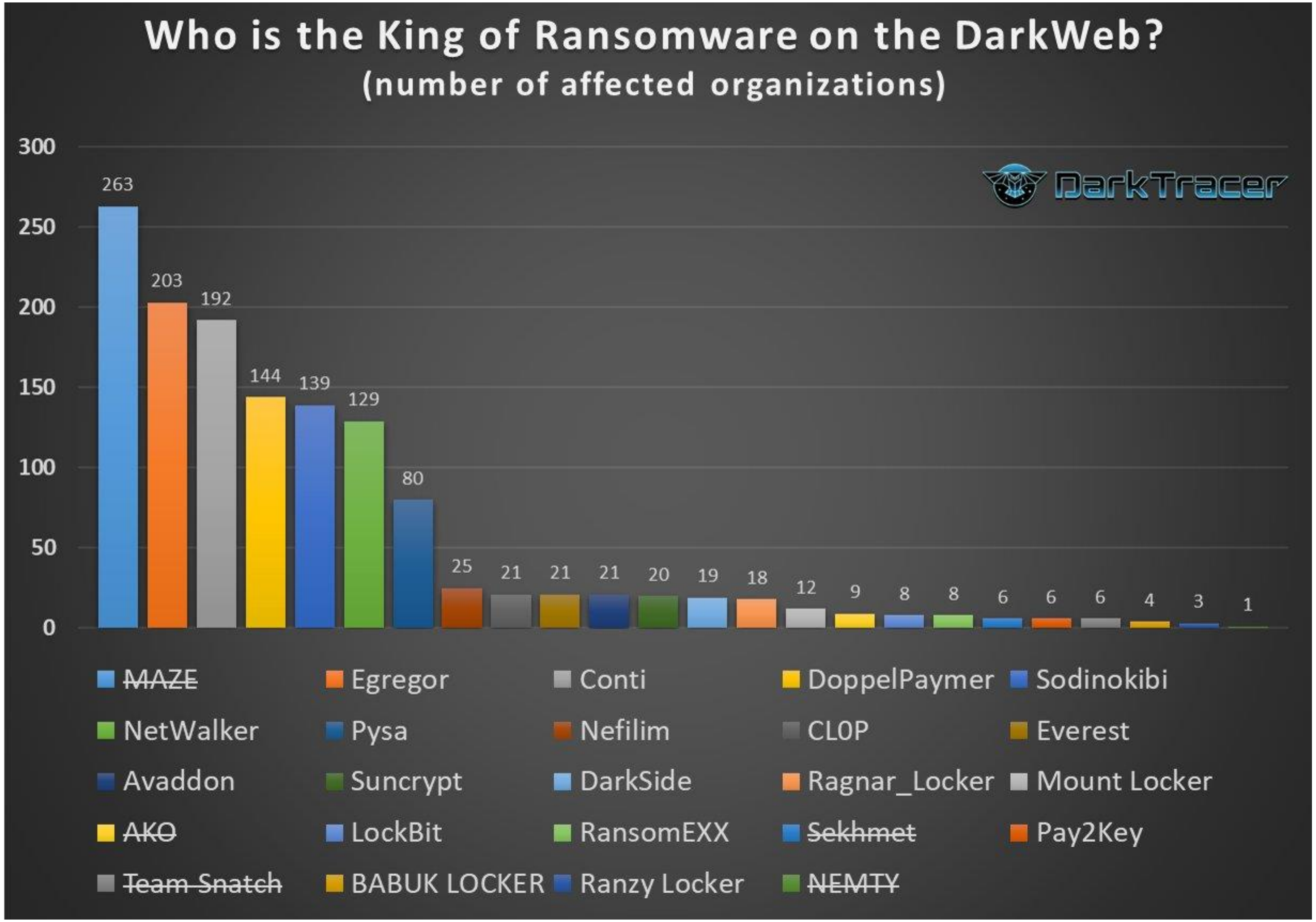
October 1, 2020 05:20 PM 2

A ransomware operation has started to utilize a new tactic to extort their victims: DDoS a victim's website until they return to the negotiation table.

A distributed denial of service (DDoS) attack is when a threat actor floods a website or a network connection with a large volume of requests to make a service inaccessible.

Source:
https://www.hk01.com/18%E5%8D%80%E6%96%B0%E8%81%9E/580230/%E7%B6%B2%E7%AB%99%E6%8C%87%E7%89%9B%E5%A5%B6%E5%85%AC%E5%8F%B8%E7% B6%B2%E7%B5%A1%E9%81%AD%E9%BB%91%E5%
AE%A2%E5%85%A5%E4%BE%B5-%E7%99%BC%E8%A8%80%E4%BA%BA%E8%AD%89%E4%BC%BA%E6%9C%8D%E5%99%A8%E5%8F%97%E5%BD%B1%E9%9F%BF%E8%87%B4ikea%E5%81%9C%E6%A5%AD

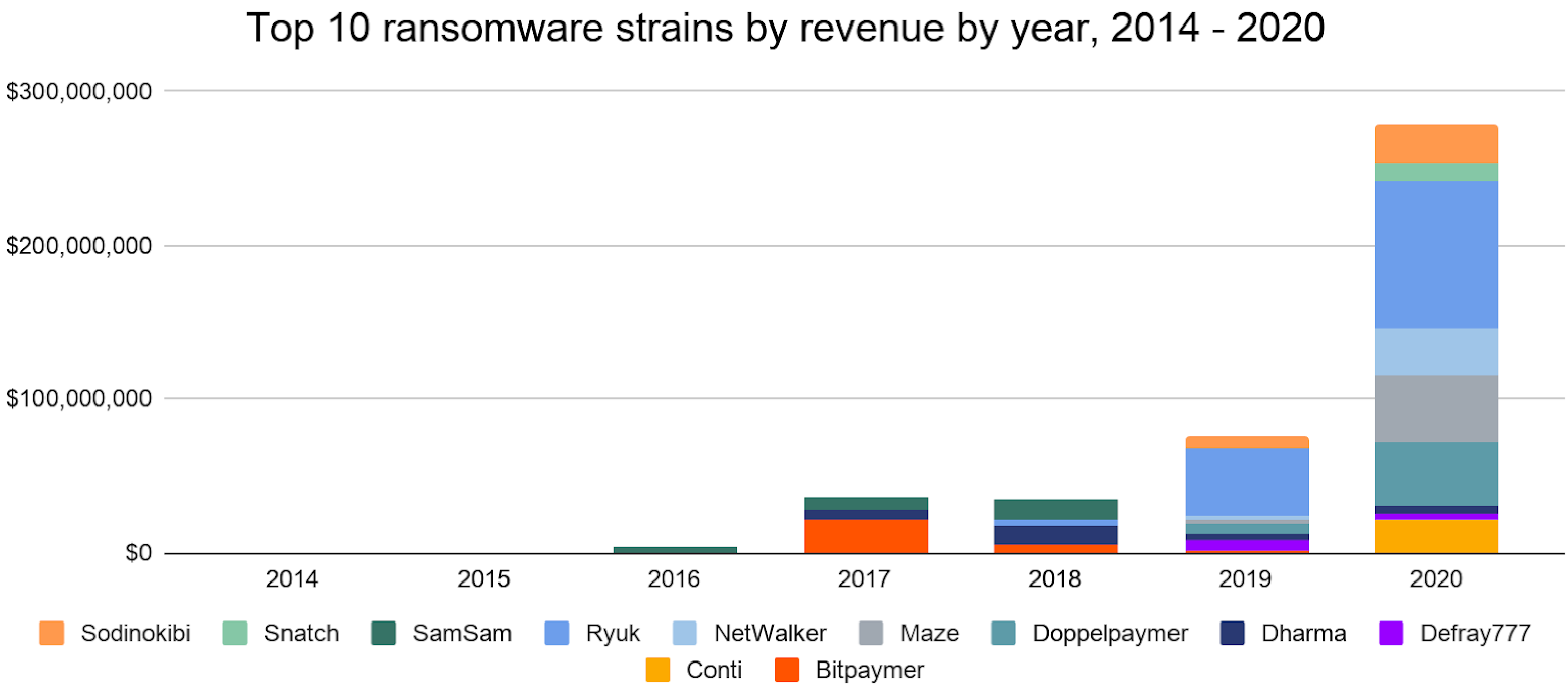
Ransomware Statistics



Who is the King of Ransomware on the DarkWeb?
(number of affected organizations)

Source: https://twitter.com/darktracer_int/status/1348535472759341059

Ransomware Statistics

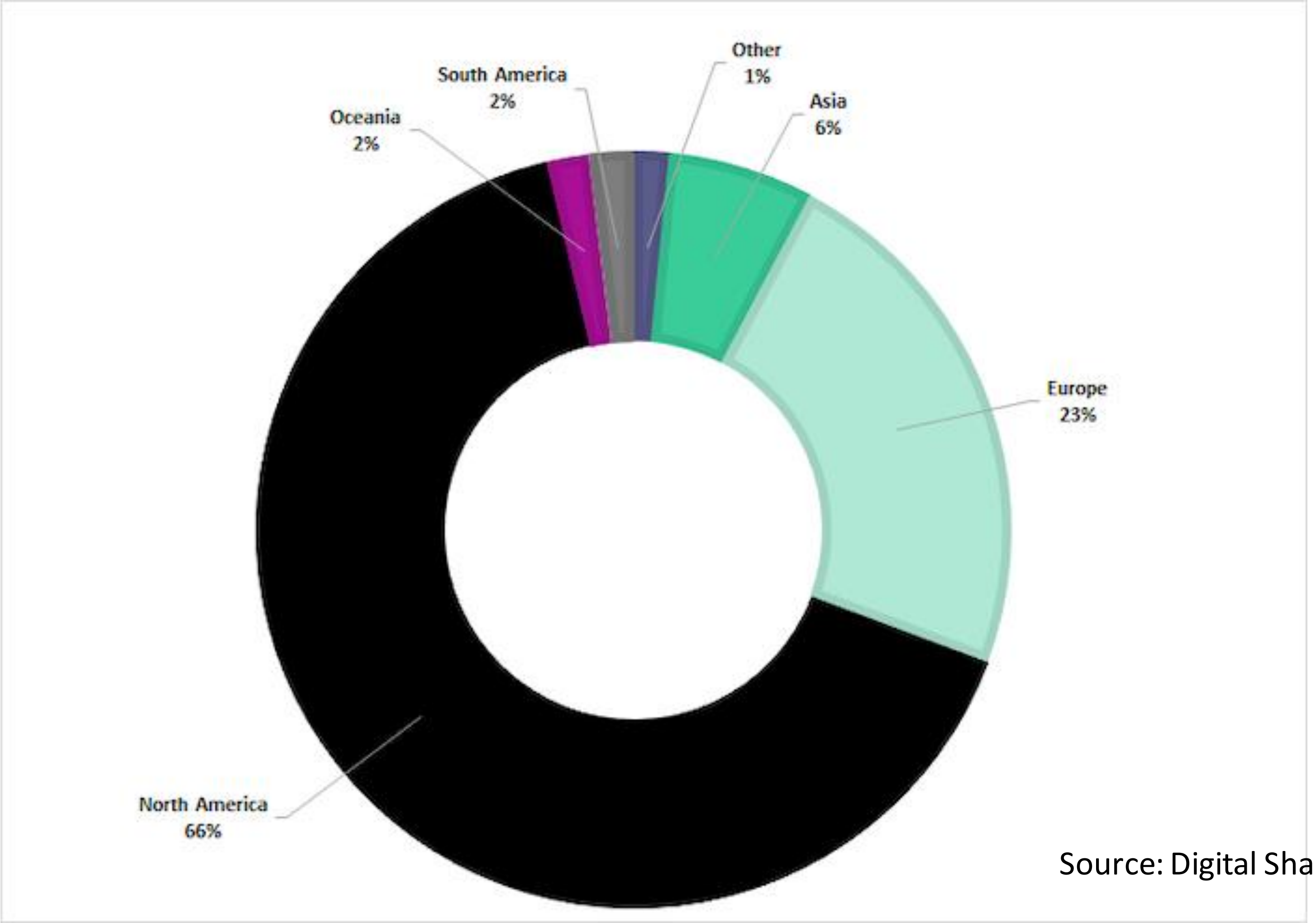


Source: Chainalysis

Source: https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest

Ransomware Statistics

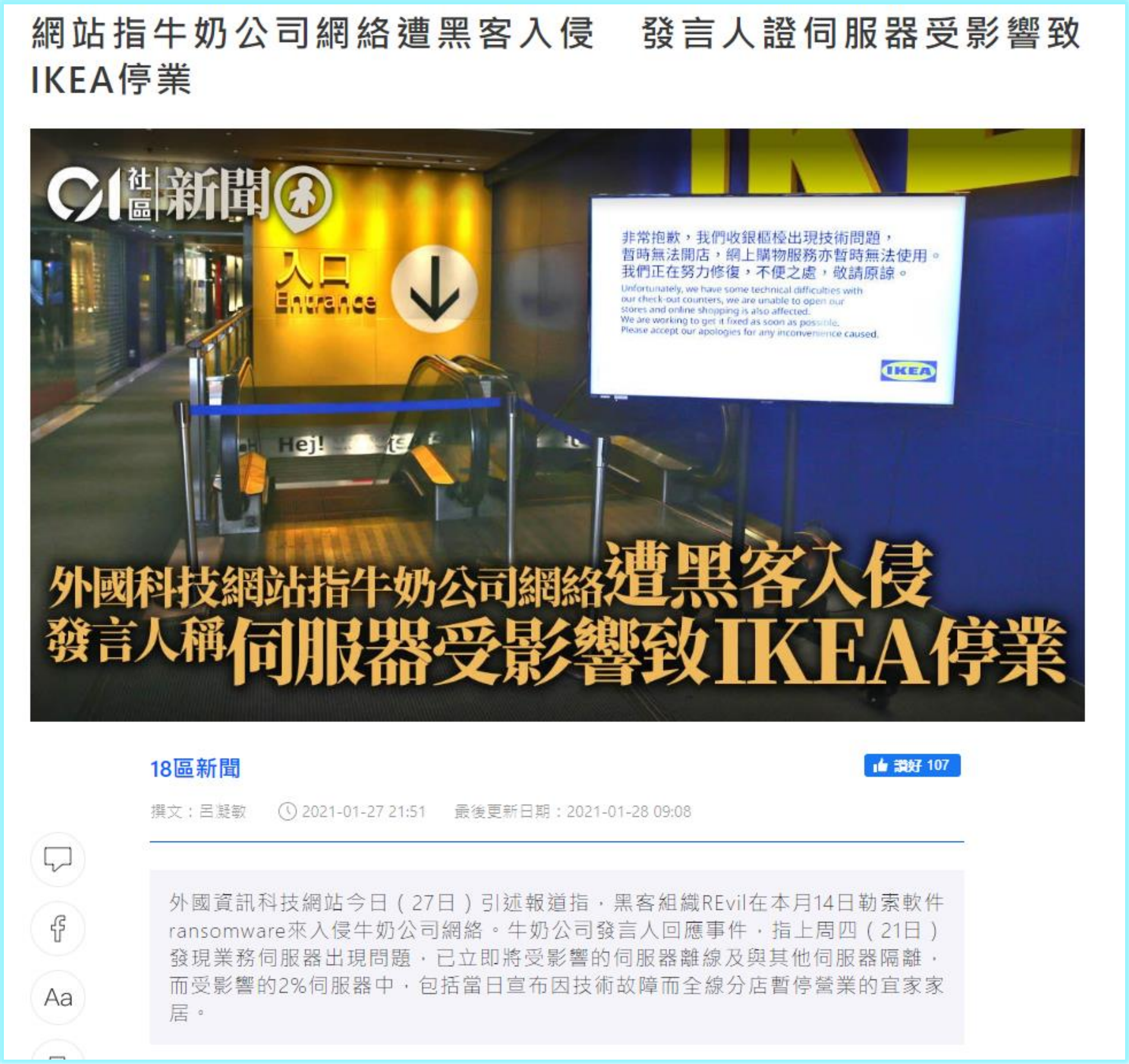
Breakdown of target locations throughout 2020



Source: Digital Shadows Intelligence

Source: https://www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/?mkt_tok=eyJpIjoiT0RsaFpESTFPRGMxWkRjMSIsInQiOiJSQ0NFNHFEdkdWZDJyNldHVDdJa01HclI0QUYxMU54QTJUeURPQXBFQnp0WTRQU1NpS01UMVFuN3ZaNFV6dDl2VjdCUXdscDJHemg0QWxtTXFKYzNRYkRBcEwyMVhZblNMYkNXTDZWQTJOT1NMdVg0dDhETlR6TEZUdFcxdGpXViJ9

Ransomware targets enterprise for higher return



01 社區新聞
入口
Entrance
Hej!
非常抱歉，我們收銀櫃檯出現技術問題，
暫時無法開店，網上購物服務亦暫時無法使用。
我們正在努力修復，不便之處，敬請原諒。
Unfortunately, we have some technical difficulties with
our check-out counters, we are unable to open our
stores and online shopping is also affected.
We are working to get it fixed as soon as possible.
Please accept our apologies for any inconvenience caused.
IKEA
外國科技網站指牛奶公司網絡遭黑客入侵
發言人稱伺服器受影響致IKEA停業
讚好 107
Aa

網站指牛奶公司網絡遭黑客入侵　發言人證伺服器受影響致IKEA停業

18區新聞

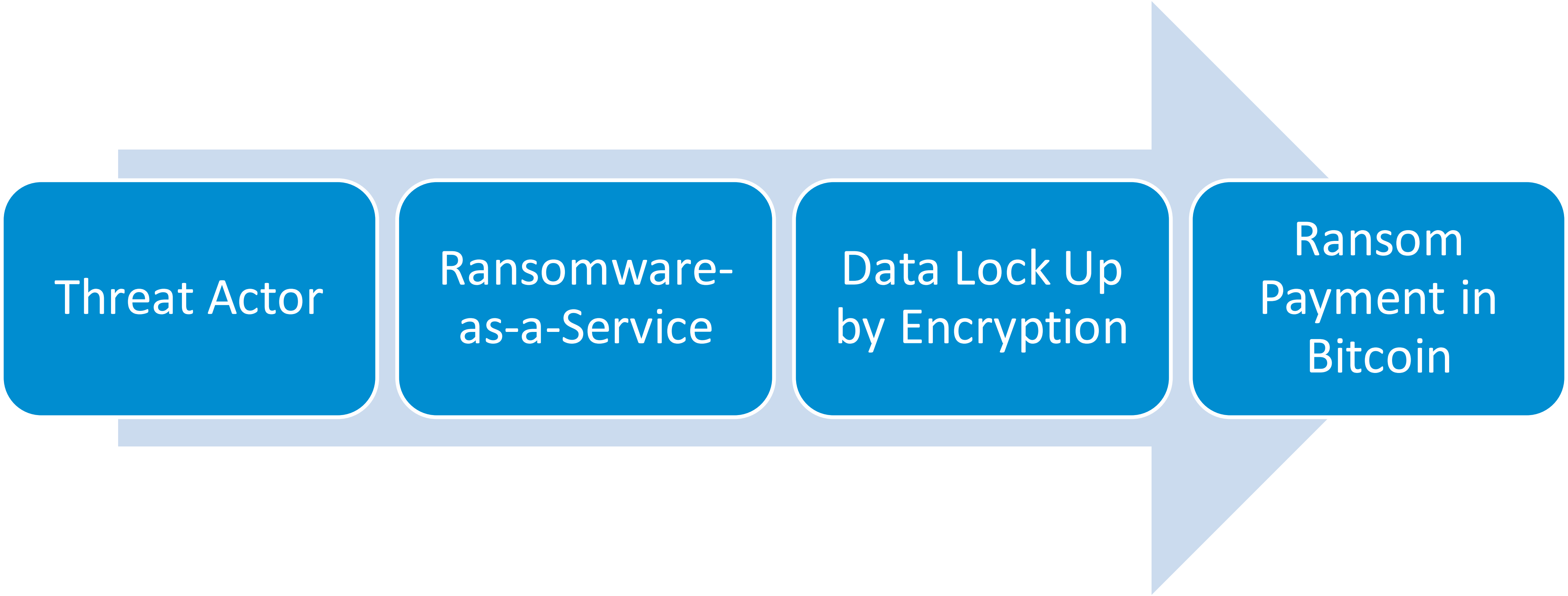
撰文：呂凝敏　2021-01-27 21:51　最後更新日期：2021-01-28 09:08

外國資訊科技網站今日（27日）引述報道指，黑客組織REvil在本月14日勒索軟件ransomware來入侵牛奶公司網絡。牛奶公司發言人回應事件，指上周四（21日）發現業務伺服器出現問題，已立即將受影響的伺服器離線及與其他伺服器隔離，而受影響的2%伺服器中，包括當日宣布因技術故障而全線分店暫停營業的宜家家居。

Source: https://www.hk01.com/18%E5%8D%80%E6%96%B0%E8%81%9E/580230/%E7%B6%B2%E7%AB%99%E6%8C%87%E7%89%9B%E5%A5%B6%E5%85%AC%E5%8F%B8%E7%B6%B2%E7%B5%A1%E9%81%AD%E9%BB%91%E5%AE%A2%E5%85%A5%E4%BE%B5-%E7%99%BC%E8%A8%80%E4%BA%BA%E8%AD%89%E4%BC%BA%E6%9C%8D%E5%99%A8%E5%8F%97%E5%BD%B1%E9%9F%BF%E8%87%B4ikea%E5%81%9C%E6%A5%AD

Ransomware Attack Tactics is Evolving

- Traditional Approach
  - Indiscriminate campaigns spreading the malware to variety of victims



Threat Actor

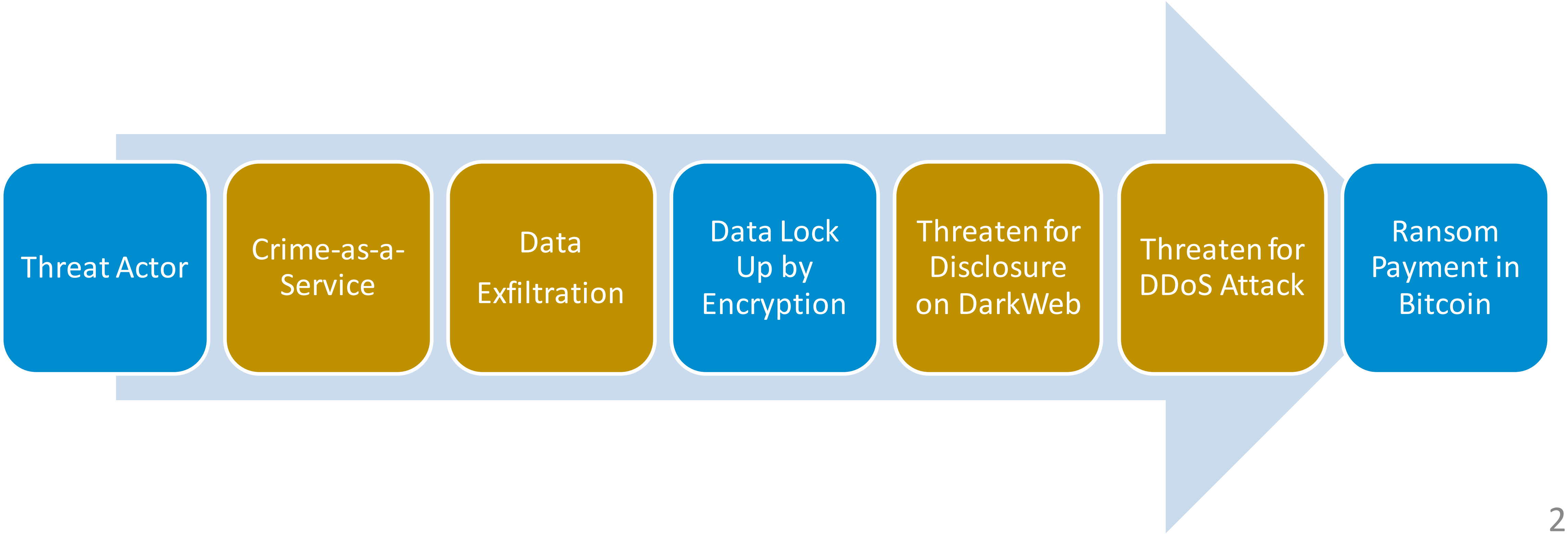
Ransomware-as-a-Service

Data Lock Up by Encryption

Ransom Payment in Bitcoin

Ransomware Attack Tactics is Evolving

- More targeted and sophisticated approach
    - Targeting large companies and demanding huge payments



Threat Actor

Crime-as-a-Service

Data Exfiltration

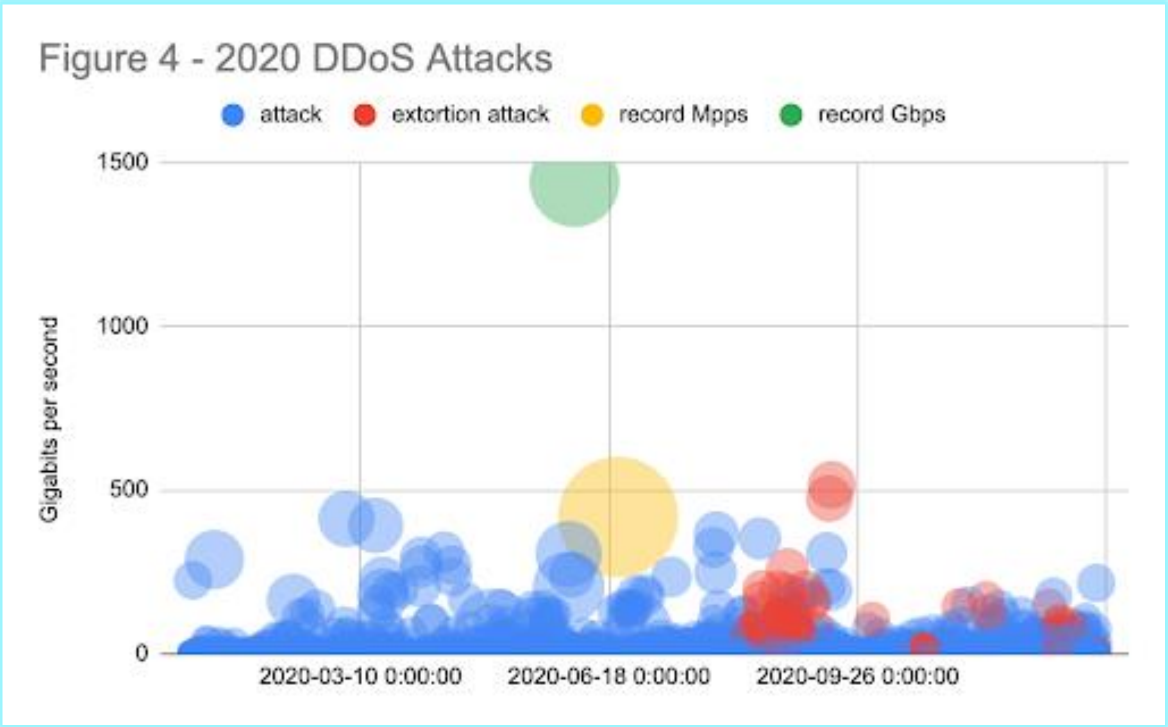
Data Lock Up by Encryption

Threaten for Disclosure on DarkWeb

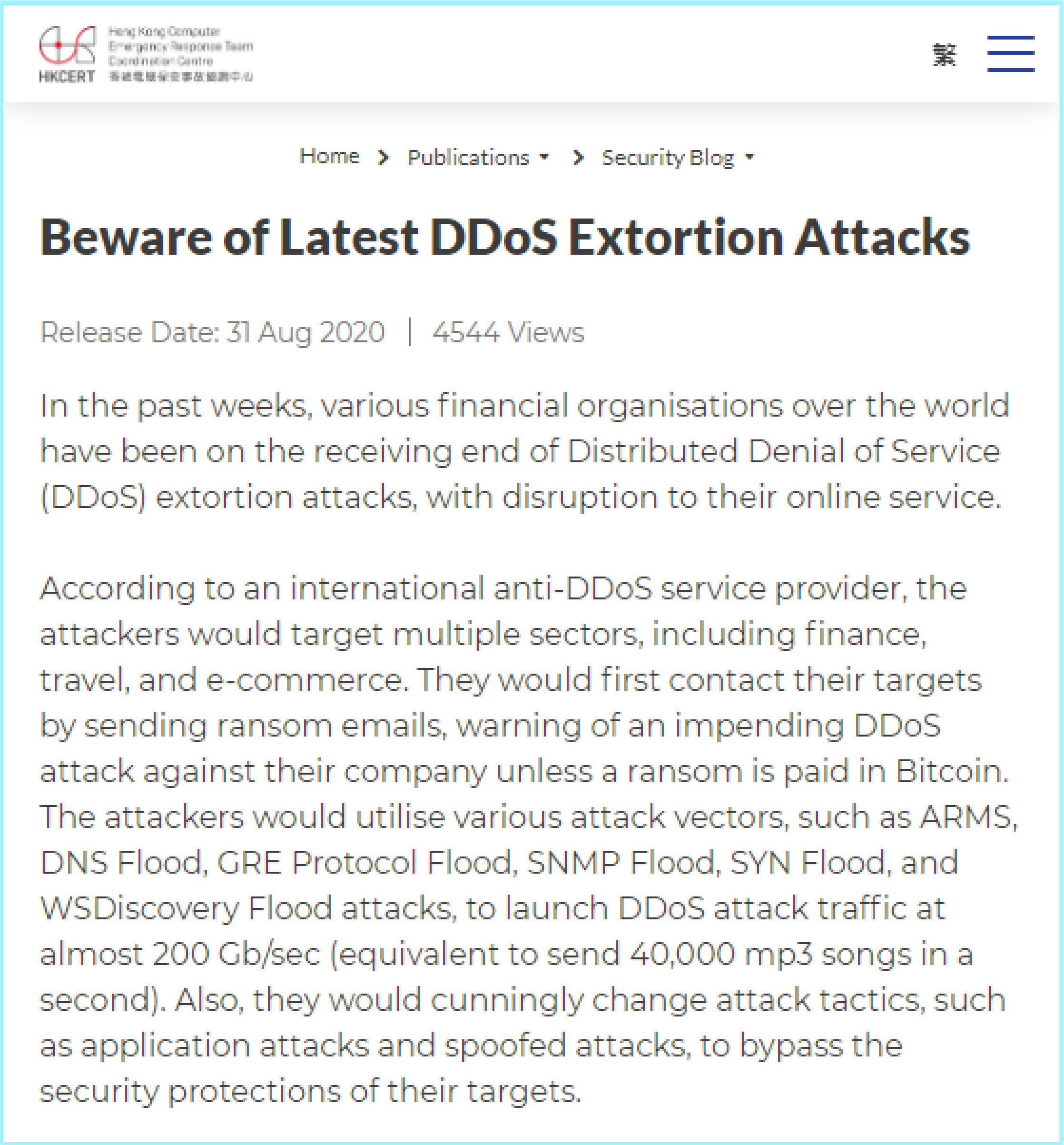
Threaten for DDoS Attack

Ransom Payment in Bitcoin

DDoS Extortion



Source: Akamai



Beware of Latest DDoS Extortion Attacks

Release Date: 31 Aug 2020 | 4544 Views

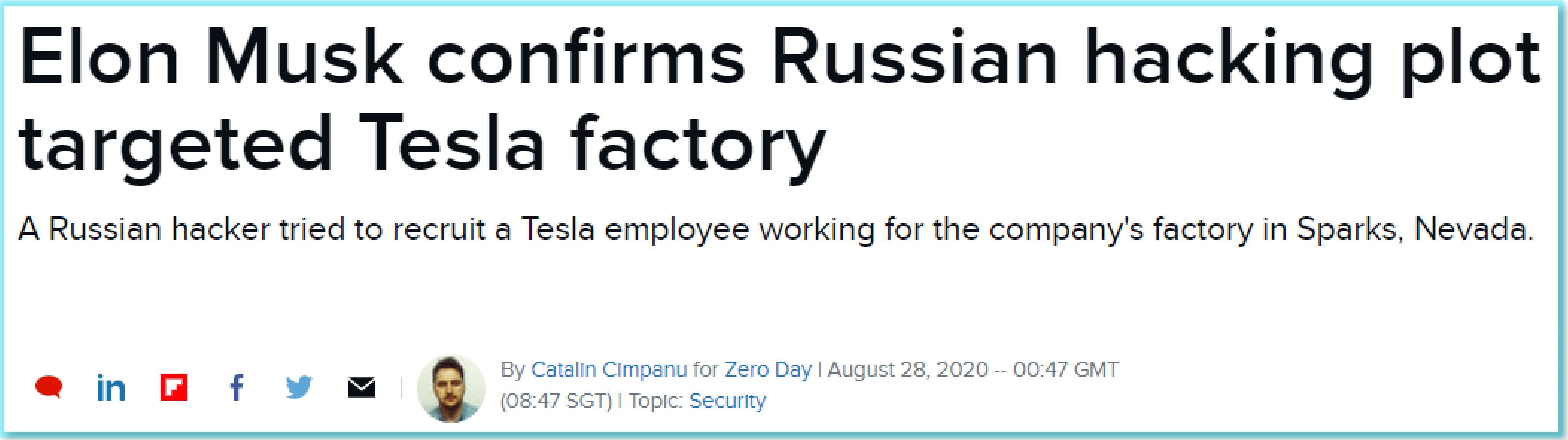
In the past weeks, various financial organisations over the world have been on the receiving end of Distributed Denial of Service (DDoS) extortion attacks, with disruption to their online service.

According to an international anti-DDoS service provider, the attackers would target multiple sectors, including finance, travel, and e-commerce. They would first contact their targets by sending ransom emails, warning of an impending DDoS attack against their company unless a ransom is paid in Bitcoin. The attackers would utilise various attack vectors, such as ARMS, DNS Flood, GRE Protocol Flood, SNMP Flood, SYN Flood, and WSDiscovery Flood attacks, to launch DDoS attack traffic at almost 200 Gb/sec (equivalent to send 40,000 mp3 songs in a second). Also, they would cunningly change attack tactics, such as application attacks and spoofed attacks, to bypass the security protections of their targets.

Source: https://blogs.akamai.com/2021/01/part-i-retrospective-2020-ddos-was-back-bigger-and-badder-than-ever-before.html
https://www.hkcert.org/blog/beware-of-latest-ddos-extortion-attacks

Cyber Attack Case Studies

Social Engineering Attack



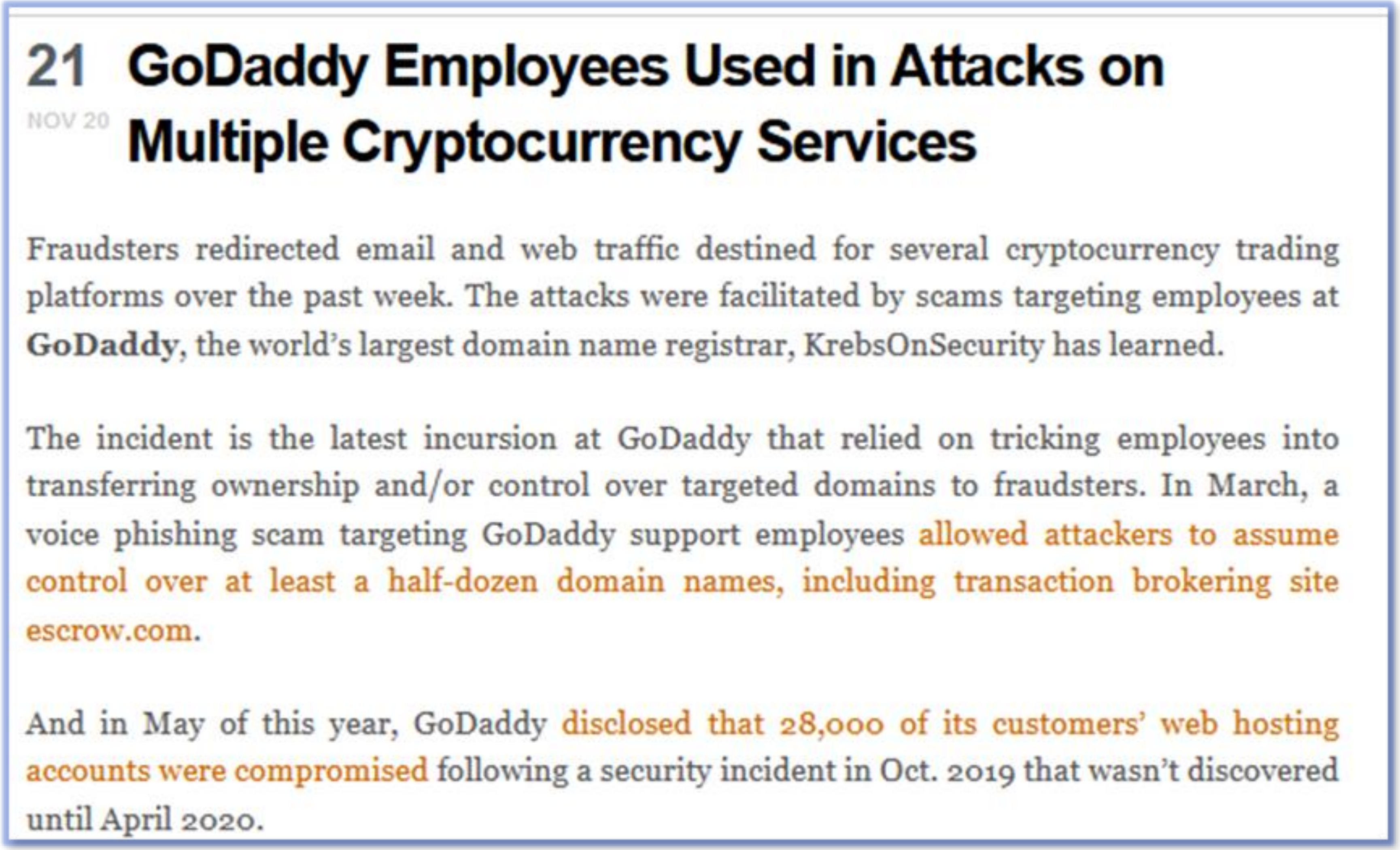
Elon Musk confirms Russian hacking plot targeted Tesla factory

A Russian hacker tried to recruit a Tesla employee working for the company's factory in Sparks, Nevada.

By Catalin Cimpanu for Zero Day | August 28, 2020 -- 00:47 GMT (08:47 SGT) | Topic: Security

Source: https://www.zdnet.com/article/elon-musk-confirms-russian-hacking-plot-targeted-tesla-factory/

Social Engineering Attack



21
NOV 20

GoDaddy Employees Used in Attacks on Multiple Cryptocurrency Services

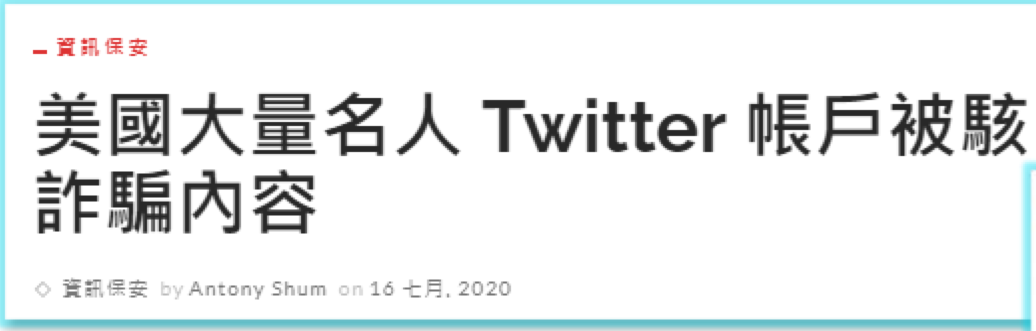
Fraudsters redirected email and web traffic destined for several cryptocurrency trading platforms over the past week. The attacks were facilitated by scams targeting employees at **GoDaddy**, the world's largest domain name registrar, KrebsOnSecurity has learned.

The incident is the latest incursion at GoDaddy that relied on tricking employees into transferring ownership and/or control over targeted domains to fraudsters. In March, a voice phishing scam targeting GoDaddy support employees allowed attackers to assume control over at least a half-dozen domain names, including transaction brokering site escrow.com.

And in May of this year, GoDaddy disclosed that 28,000 of its customers' web hosting accounts were compromised following a security incident in Oct. 2019 that wasn't discovered until April 2020.

Source: https://krebsonsecurity.com/2020/11/godaddy-employees-used-in-attacks-on-multiple-cryptocurrency-services/

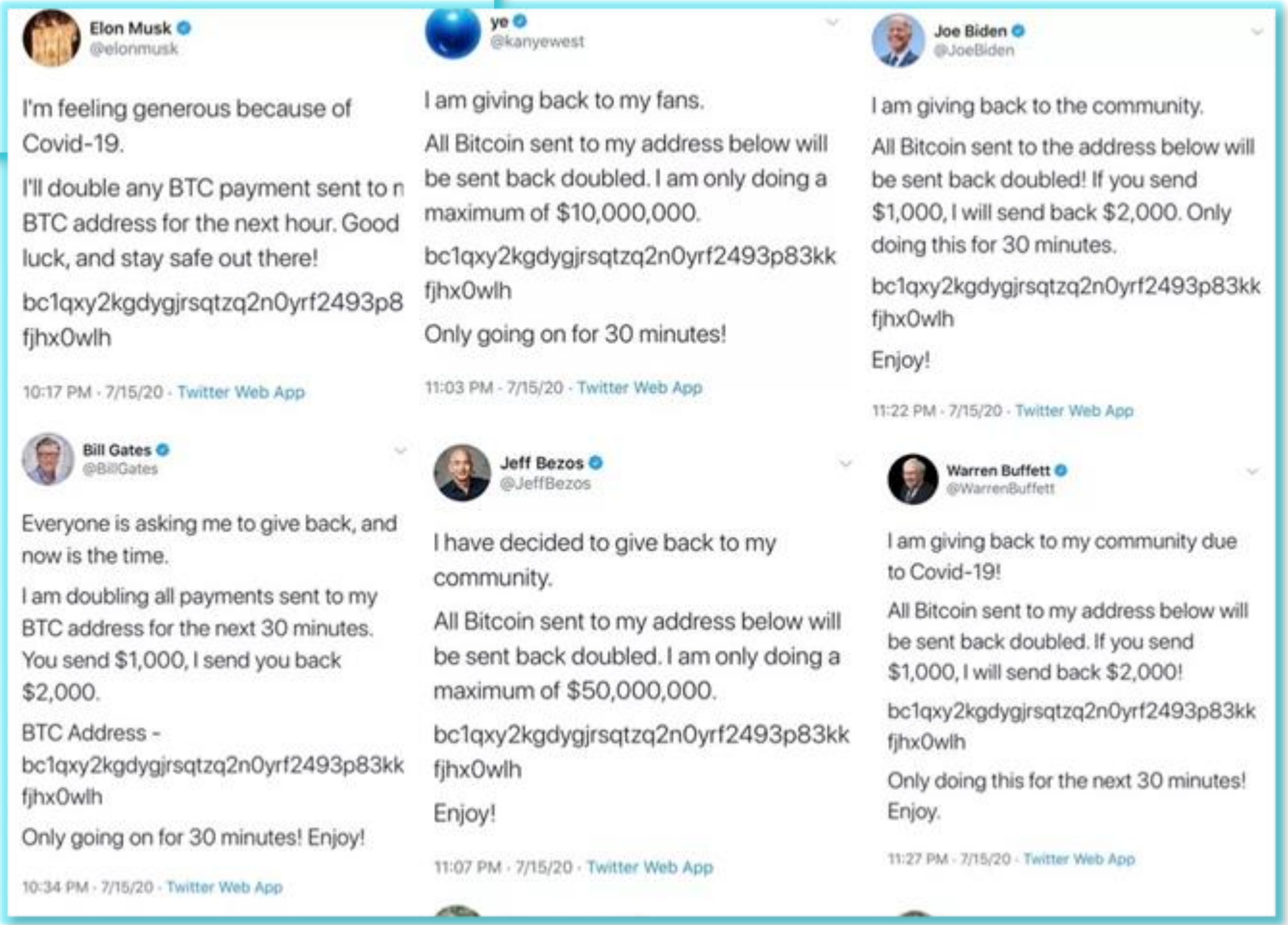
Case Study – Twitter Bitcoin Scam



資訊保安

美國大量名人 Twitter 帳戶被駭　散播 Bitcoin 詐騙內容

◇ 資訊保安 by Antony Shum on 16 七月, 2020



Elon Musk
@elonmusk

I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to n BTC address for the next hour. Good luck, and stay safe out there!

bc1qxy2kgdygjrsqtzq2n0yrf2493p8 fjhx0wlh

10:17 PM · 7/15/20 · Twitter Web App

ye
@kanyewest

I am giving back to my fans.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $10,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk fjhx0wlh

Only going on for 30 minutes!

11:03 PM · 7/15/20 · Twitter Web App

Joe Biden
@JoeBiden

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk fjhx0wlh

Enjoy!

11:22 PM · 7/15/20 · Twitter Web App

Bill Gates
@BillGates

Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

BTC Address -
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk fjhx0wlh

Only going on for 30 minutes! Enjoy!

10:34 PM · 7/15/20 · Twitter Web App

Jeff Bezos
@JeffBezos

I have decided to give back to my community.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $50,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk fjhx0wlh

Enjoy!

11:07 PM · 7/15/20 · Twitter Web App

Warren Buffett
@WarrenBuffett

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

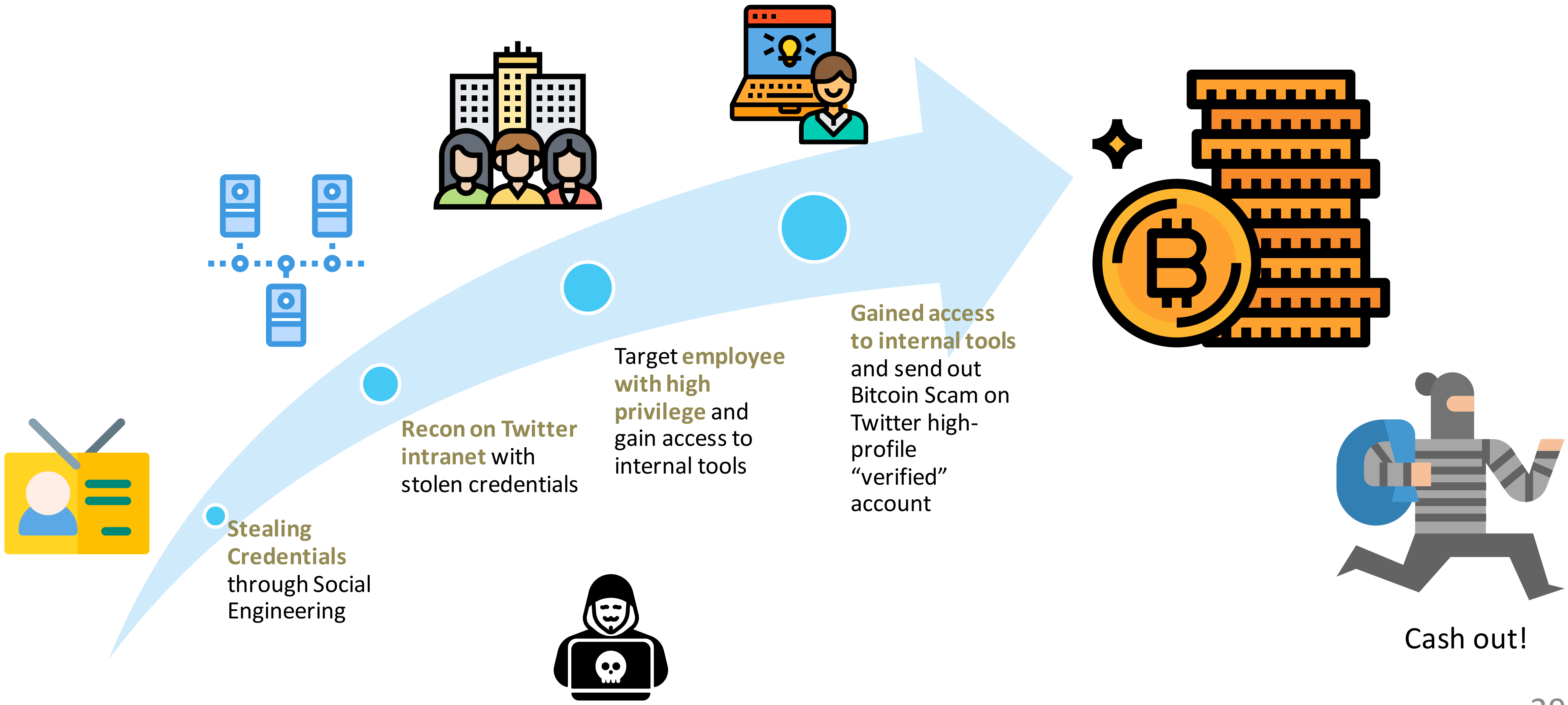
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk fjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

11:27 PM · 7/15/20 · Twitter Web App

Image Source: https://www.investopedia.com/twitter-shares-fall-after-hackers-pull-off-bitcoin-scam-5071449
https://unwire.pro/2020/07/16/major-us-twitter-accounts-hacked-in-bitcoin-scam/security/

Bitcoin Scam Attack Process



Stealing Credentials through Social Engineering

Recon on Twitter intranet with stolen credentials

Target **employee with high privilege** and gain access to internal tools

Gained access to internal tools and send out Bitcoin Scam on Twitter high-profile “verified” account

Cash out!

Source: https://www.dfs.ny.gov/Twitter_Report

Cash Out Amount by Threat Actor

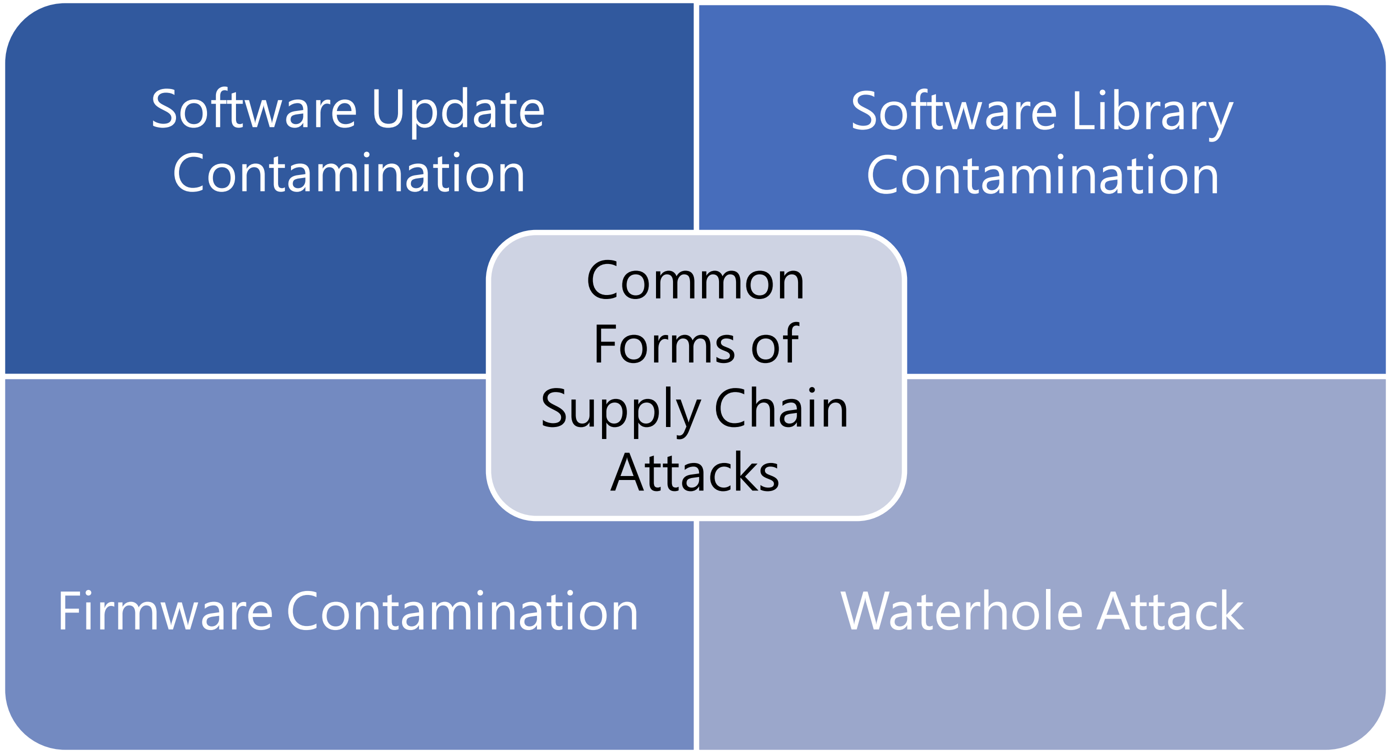
12.83 bitcoins

equivalent to

HK$ 1,166,000

What is Supply Chain Attack?

- Leveraging on our **trust** on our supply chain partners to **bypass traditional defenses** and compromise a large number of computers.
- Target **weak points** in the supply chain to launch their initial attacks.
- The compromised software spread to other parties **downstream**.



Common Forms of Supply Chain Attacks

Software Update Contamination

Software Library Contamination

Firmware Contamination

Waterhole Attack

Source: https://www.hkcert.org/security-guideline/understanding-and-tackling-supply-chain-attack#What_is_Supply_Chain_Attack

Supply Chain Attacks in 2020

2020 State of the Software Supply Chain

The 6th Annual Report on Global Open Source Software Development

sonatype

Revolution

muse.dev

- Malicious NPM packages to install remote access trojan

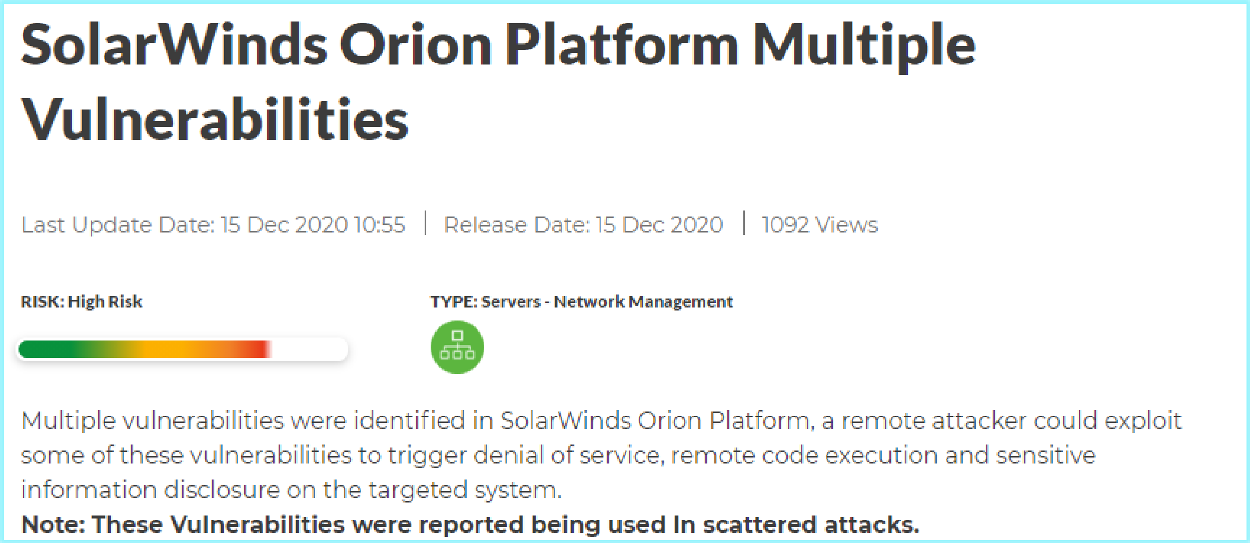
- Trojanised Solarwinds Orion software (2020-Dec) Solarwinds Orion
  - Affected 18,000 customers
    - Over 425 of Fortune 500
    - Top 10 US Telcos
    - US military and government departments

- Supply chain attacks increased by 430% in 2020

(Source: Sonatype State of the Software Supply Chain 2020)

Source: https://www.bleepingcomputer.com/news/microsoft/malicious-npm-packages-used-to-install-njrat-remote-access-trojan/

Supply Chain Attack Case Study - SUNBURST



SolarWinds Orion Platform Multiple Vulnerabilities

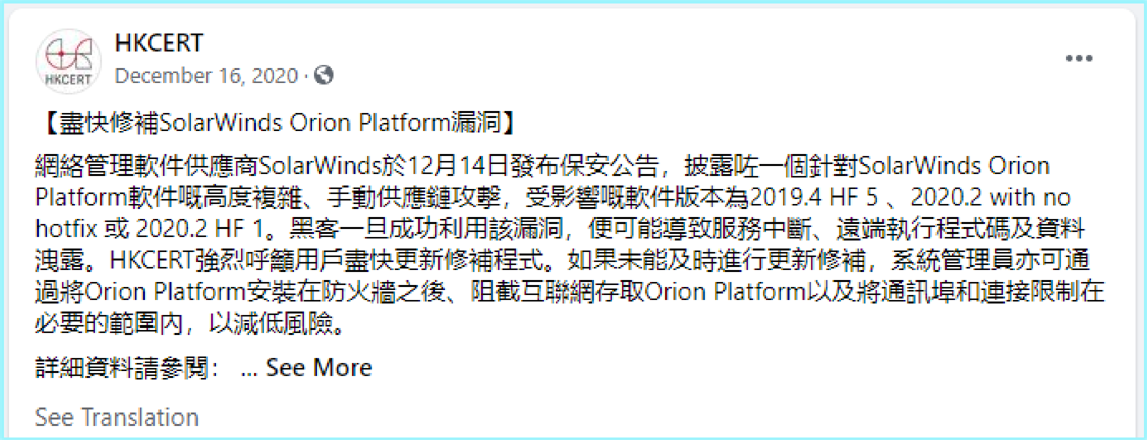
Last Update Date: 15 Dec 2020 10:55 | Release Date: 15 Dec 2020 | 1092 Views

RISK: High Risk

TYPE: Servers - Network Management

Multiple vulnerabilities were identified in SolarWinds Orion Platform, a remote attacker could exploit some of these vulnerabilities to trigger denial of service, remote code execution and sensitive information disclosure on the targeted system.

Note: These Vulnerabilities were reported being used In scattered attacks.



HKCERT

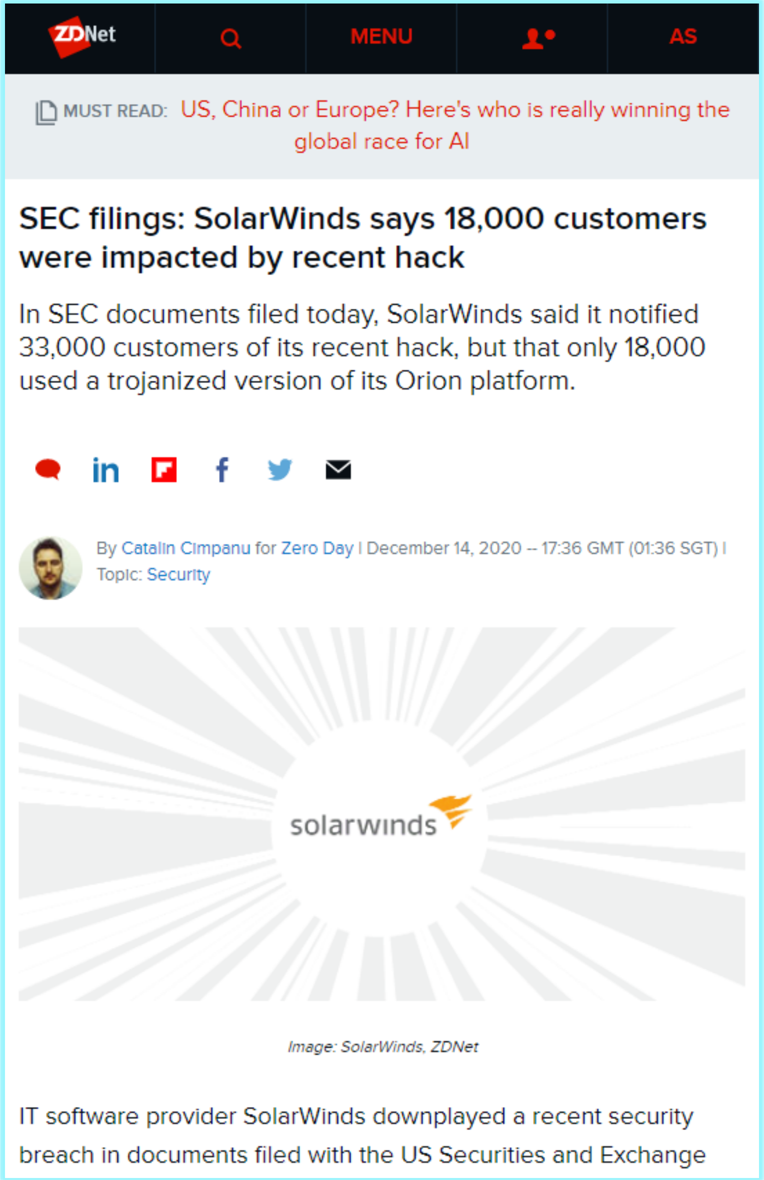
December 16, 2020 ·

【盡快修補SolarWinds Orion Platform漏洞】

網絡管理軟件供應商SolarWinds於12月14日發布保安公告，披露咗一個針對SolarWinds Orion Platform軟件嘅高度複雜、手動供應鏈攻擊，受影響嘅軟件版本為2019.4 HF 5 、2020.2 with no hotfix 或 2020.2 HF 1。黑客一旦成功利用該漏洞，便可能導致服務中斷、遠端執行程式碼及資料洩露。HKCERT強烈呼籲用戶盡快更新修補程式。如果未能及時進行更新修補，系統管理員亦可通過將Orion Platform安裝在防火牆之後、阻截互聯網存取Orion Platform以及將通訊埠和連接限制在必要的範圍內，以減低風險。

詳細資料請參閱： ... See More

See Translation



MUST READ: US, China or Europe? Here's who is really winning the global race for AI

SEC filings: SolarWinds says 18,000 customers were impacted by recent hack

In SEC documents filed today, SolarWinds said it notified 33,000 customers of its recent hack, but that only 18,000 used a trojanized version of its Orion platform.

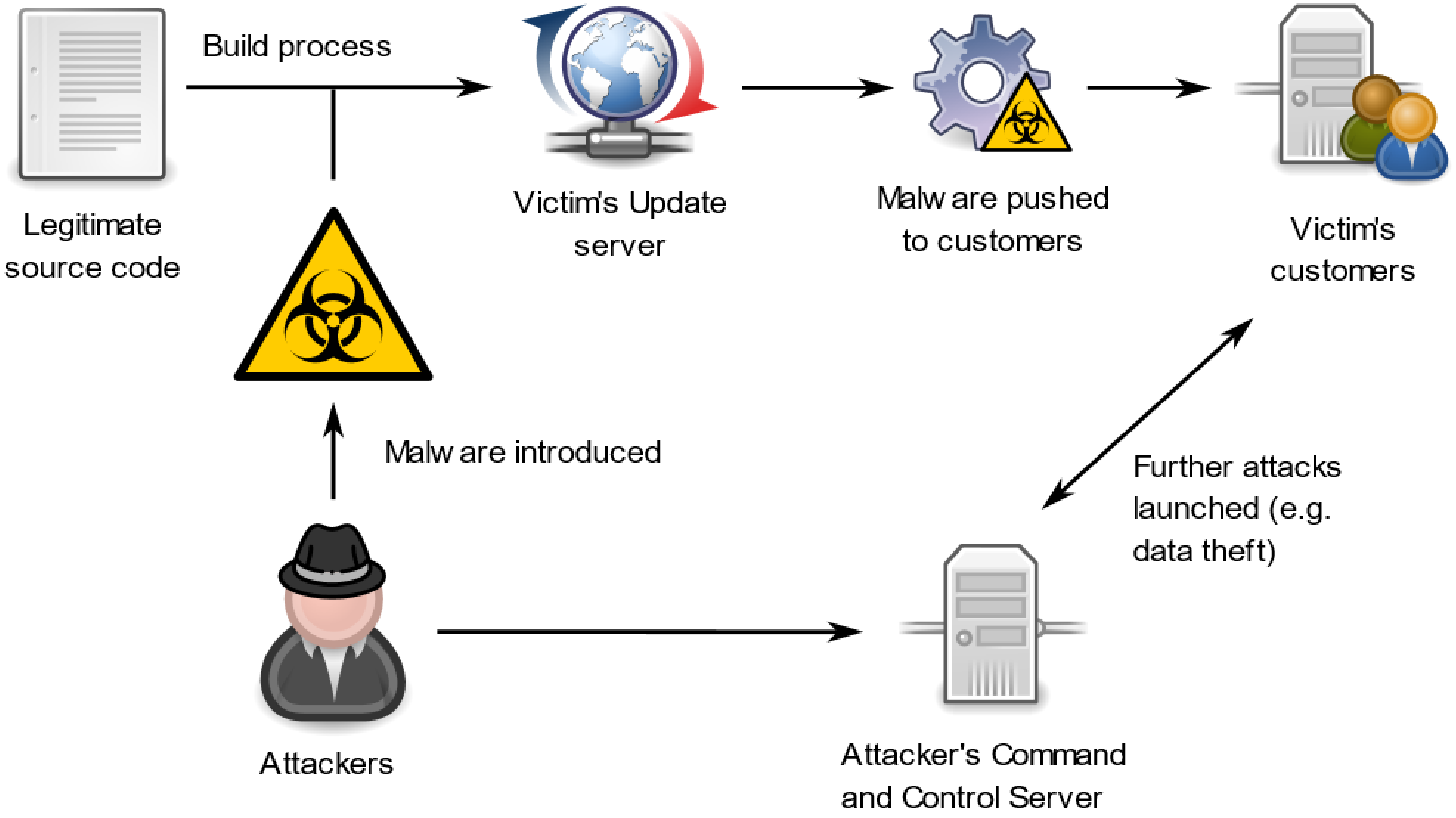
By Catalin Cimpanu for Zero Day | December 14, 2020 -- 17:36 GMT (01:36 SGT) | Topic: Security

Image: SolarWinds, ZDNet

IT software provider SolarWinds downplayed a recent security breach in documents filed with the US Securities and Exchange

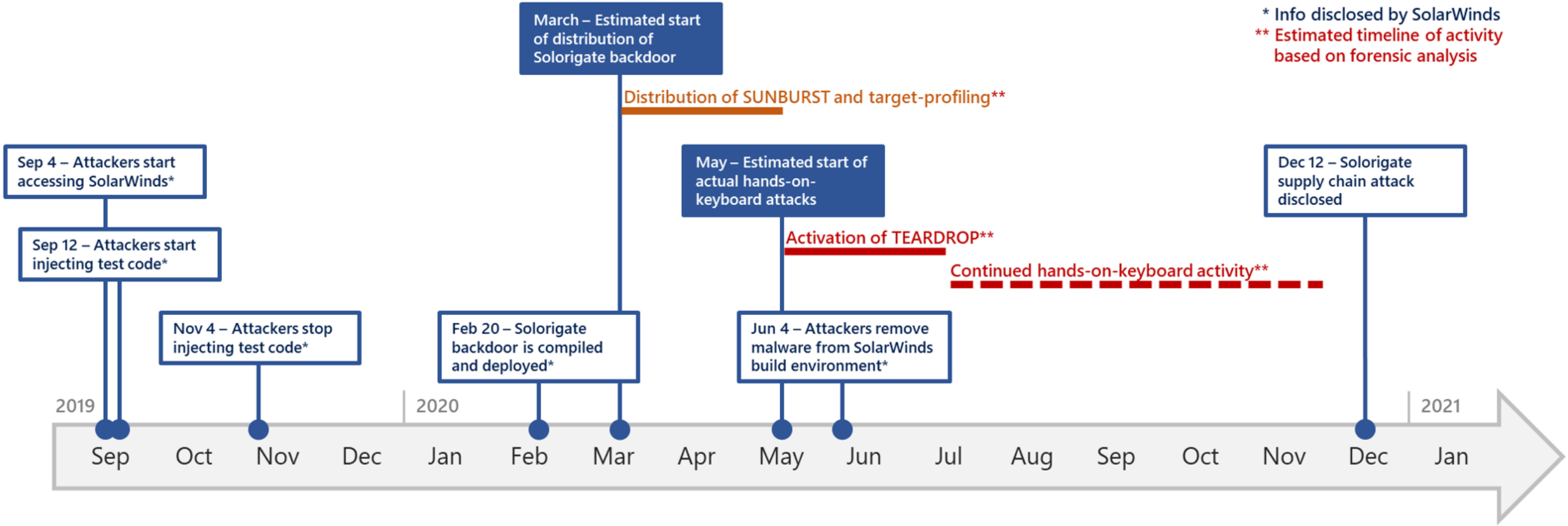
Source: https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/

Attack Process


Build process
Legitimate source code
Victim's Update server
Malw are pushed to customers
Victim's customers
Malw are introduced
Further attacks launched (e.g. data theft)
Attackers
Attacker's Command and Control Server

Source: https://www.breachlock.com/the-solarwinds-hack-and-the-arrival-of-software-supply-chain-attacks/

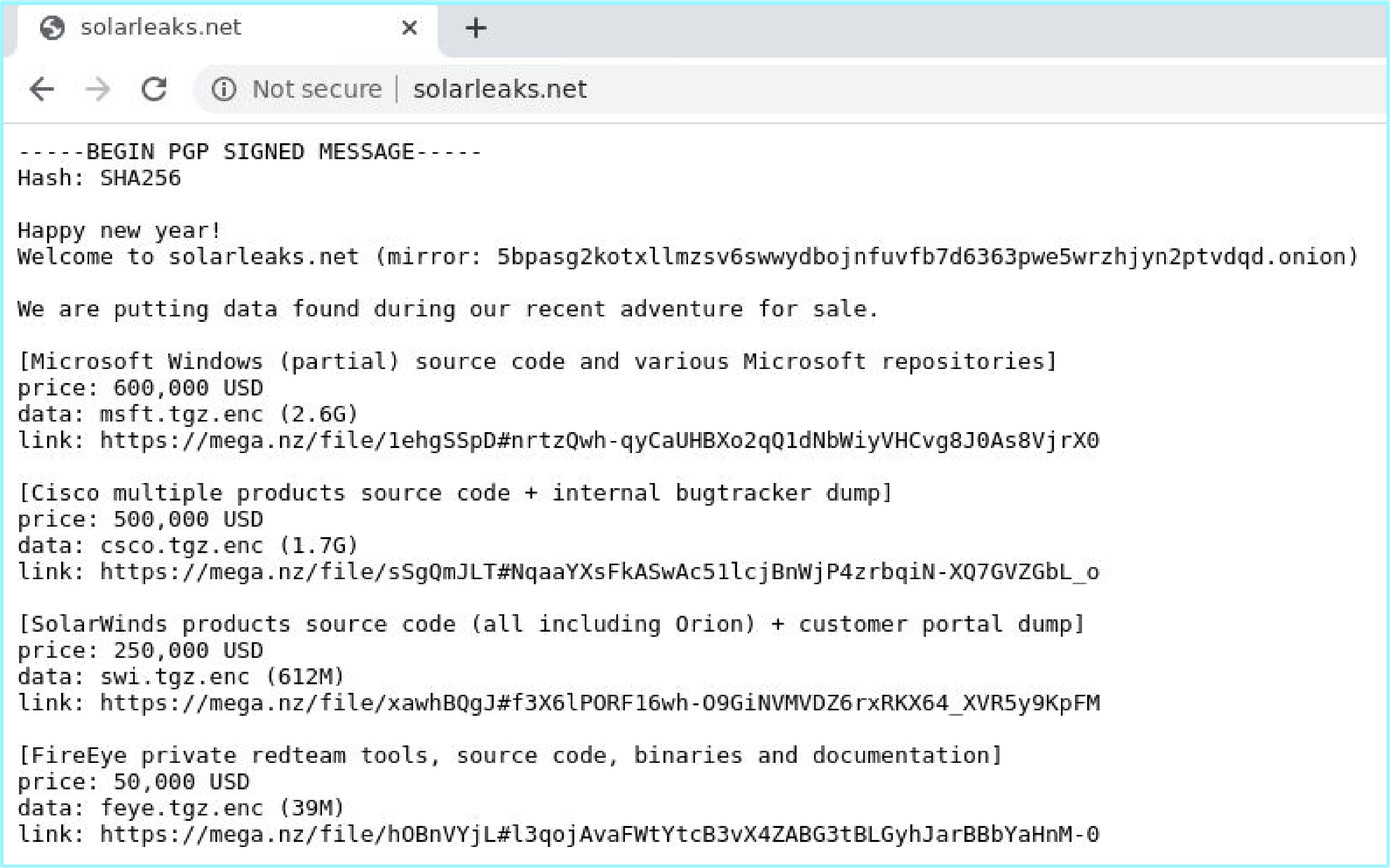
Attack Timeline



* Info disclosed by SolarWinds
** Estimated timeline of activity based on forensic analysis
March – Estimated start of distribution of Solorigate backdoor
Distribution of SUNBURST and target-profiling**
Sep 4 – Attackers start accessing SolarWinds*
Sep 12 – Attackers start injecting test code*
Nov 4 – Attackers stop injecting test code*
Feb 20 – Solorigate backdoor is compiled and deployed*
May – Estimated start of actual hands-on-keyboard attacks
Activation of TEARDROP**
Continued hands-on-keyboard activity**
Jun 4 – Attackers remove malware from SolarWinds build environment*
Dec 12 – Solorigate supply chain attack disclosed
2019
2020
2021
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan

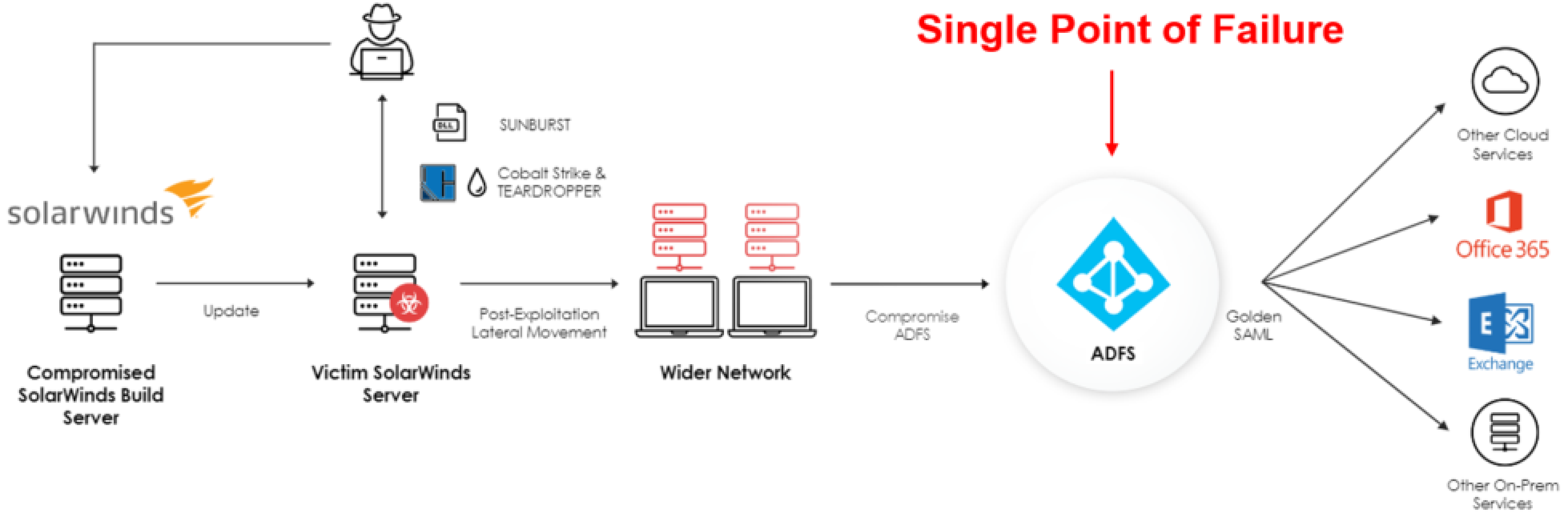
Source: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Threat actor claims to sell breaches of data



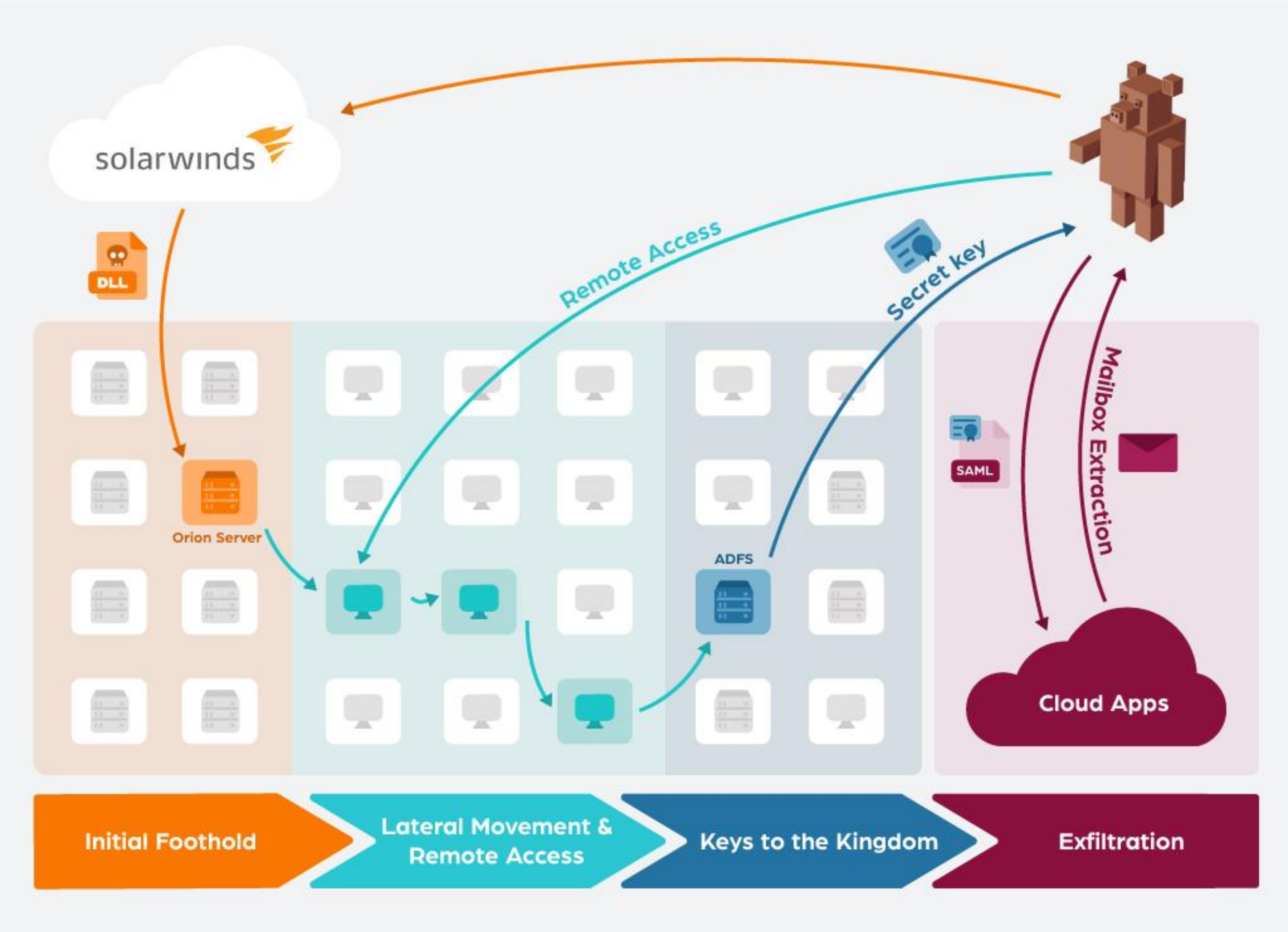
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Happy new year!
Welcome to solarleaks.net (mirror: 5bpasg2kotxllmzsv6swwydbojnfuvfb7d6363pwe5wrzhjyn2ptvdqd.onion)

We are putting data found during our recent adventure for sale.

[Microsoft Windows (partial) source code and various Microsoft repositories]
price: 600,000 USD
data: msft.tgz.enc (2.6G)
link: https://mega.nz/file/1ehgSSpD#nrtzQwh-qyCaUHBXo2qQ1dNbWiyVHCvg8J0As8VjrX0

[Cisco multiple products source code + internal bugtracker dump]
price: 500,000 USD
data: csco.tgz.enc (1.7G)
link: https://mega.nz/file/sSgQmJLT#NqaaYXsFkASwAc51lcjBnWjP4zrbqiN-XQ7GVZGbL_o

[SolarWinds products source code (all including Orion) + customer portal dump]
price: 250,000 USD
data: swi.tgz.enc (612M)
link: https://mega.nz/file/xawhBQgJ#f3X6lPORF16wh-O9GiNVMVDZ6rxRKX64_XVR5y9KpFM

[FireEye private redteam tools, source code, binaries and documentation]
price: 50,000 USD
data: feye.tgz.enc (39M)
link: https://mega.nz/file/hOBnVYjL#l3qojAvaFWtYtcB3vX4ZABG3tBLGyhJarBBbYaHnM-0
```

More attacks evolving from this incident



Source: https://www.authomize.com/blog/lessons-learned-for-the-next-solarwinds-attack/

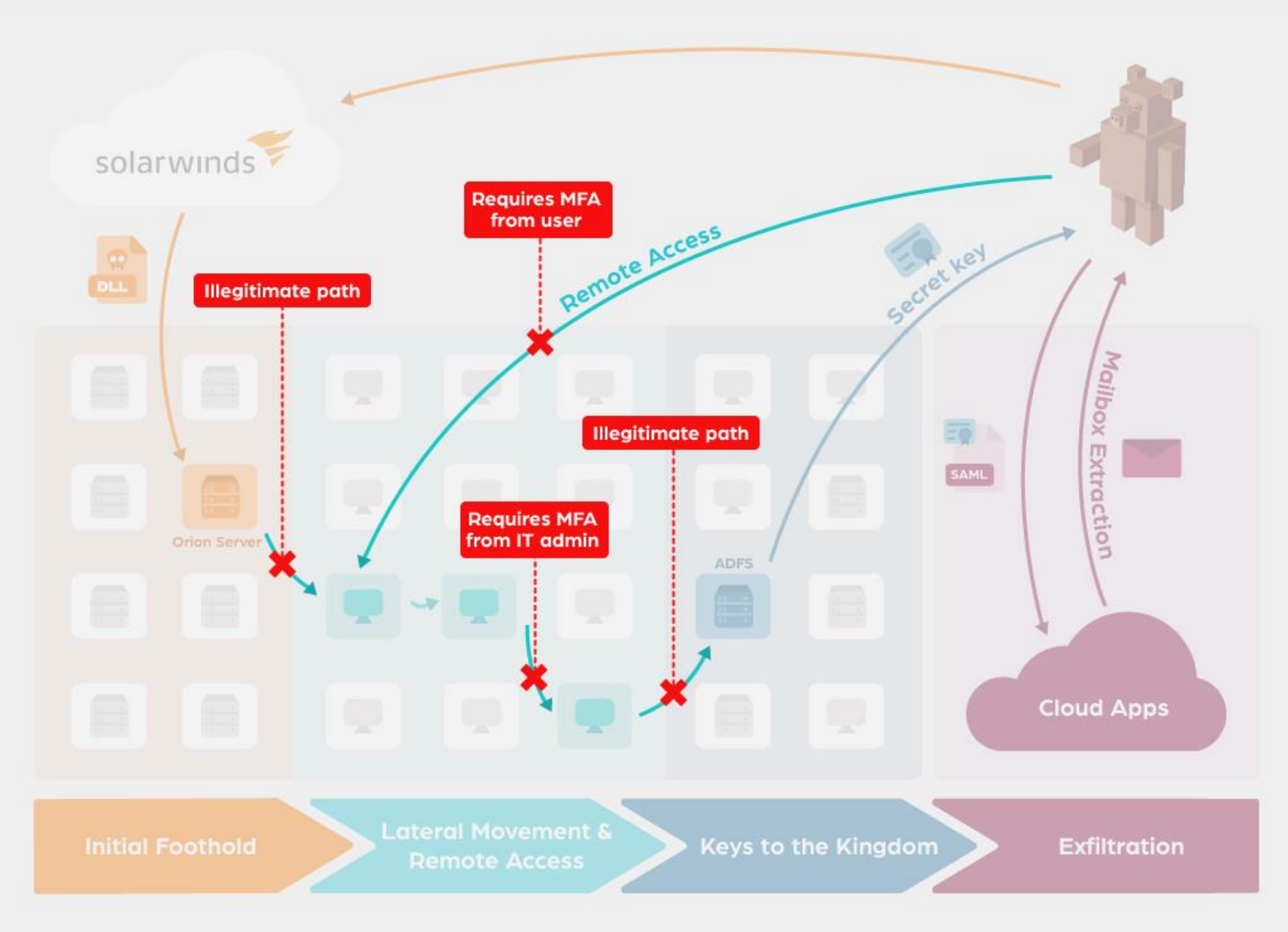
Phases of The Attack



Can we stop the attack?

Source: https://zeronetworks.com/blog/examining_solarwinds_supply_chain_attack/

Phases of The Attack



Source: https://zeronetworks.com/blog/examining_solarwinds_supply_chain_attack/

Security Advices

Managing New Cyber Security Risks

1. Formulate Security Strategy for the New Normal

SMEs and Enterprises

- Provide WFH security guideline
- Plan for capacity resilience for remote working
- Protect remote access facilities and endpoints
- Raise user security awareness

Employees and Users

- Ensure privacy and security of working environment
- Keep business and leisure apart
- Think before connecting or entering credentials
- Report suspicious activity

Useful Guidelines

Six Security Tips for Home Office
https://www.hkcert.org/security-guideline/six-security-tips-for-home-office

Assessing the Security of Remote Access Services Guideline
https://www.hkcert.org/security-guideline/assessing-the-security-of-remote-access-services-guideline

Managing New Cyber Security Risks

2. Manage Security Risks of New Technologies

- Understand security implication of new technologies, (e.g. 5G/IoT, cloud computing or mobile financial services)

3. Conduct Security Health Check

- Assess network and system security regularly
- Continuously monitor IT assets exposed to the Internet

4. Monitor Third Party Security Risks

HKCERT Security Awareness Videos

https://www.youtube.com/user/hkcert

PLAY

HKCERT

Hong Kong Computer
Emergency Response Team
Coordination Centre

🖥 https://www.hkcert.org/

☎ 8105 6060

✉ hkcert@hkcert.org

f HKCERT

in HKCERT

Q & A