Next-Gen DFIR
Mass Exploits & Supplier Compromise

Matt Durrin
IR Lead

Sherri Davidoff
CEO

LMG
SECURITY

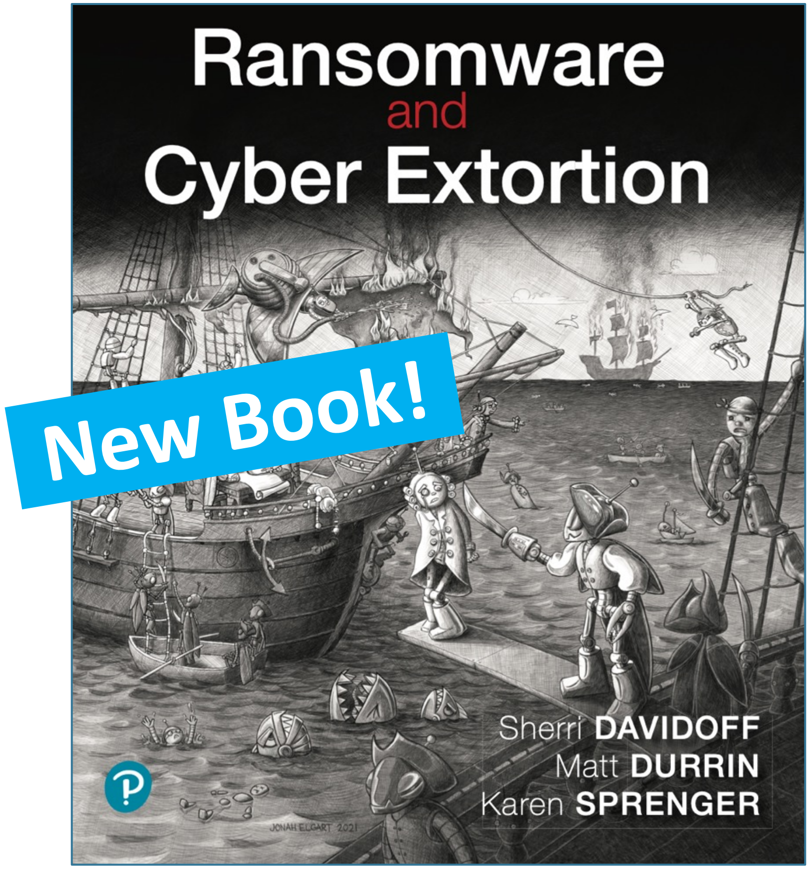
Who Are We?

Sherri Davidoff

Founder & CEO, LMG Security

“Alien” from “Breaking & Entering”

MIT EE/CS, GCFA, GPEN



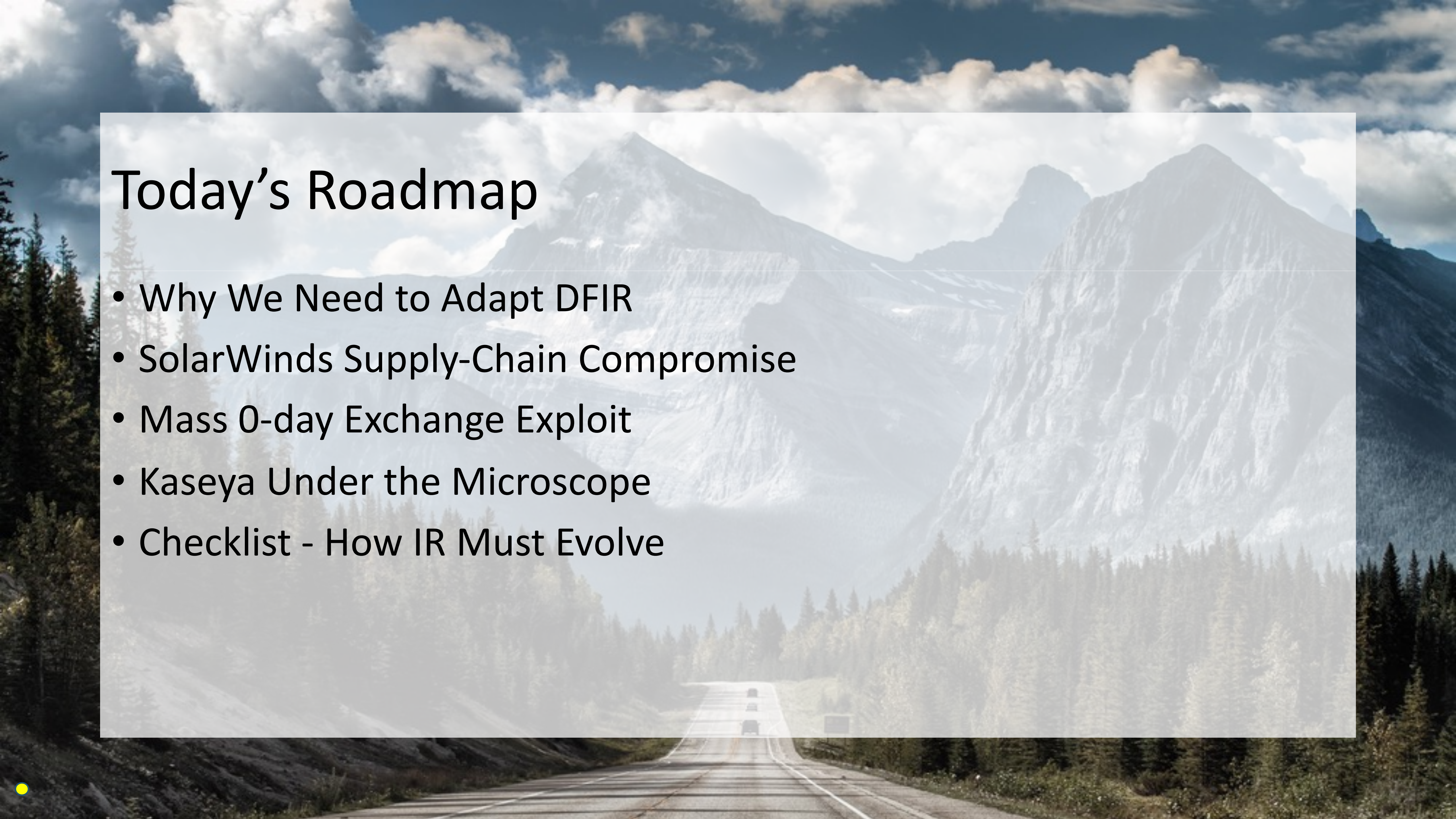
New Book!

Matt Durrin

IR Lead

Research & Development

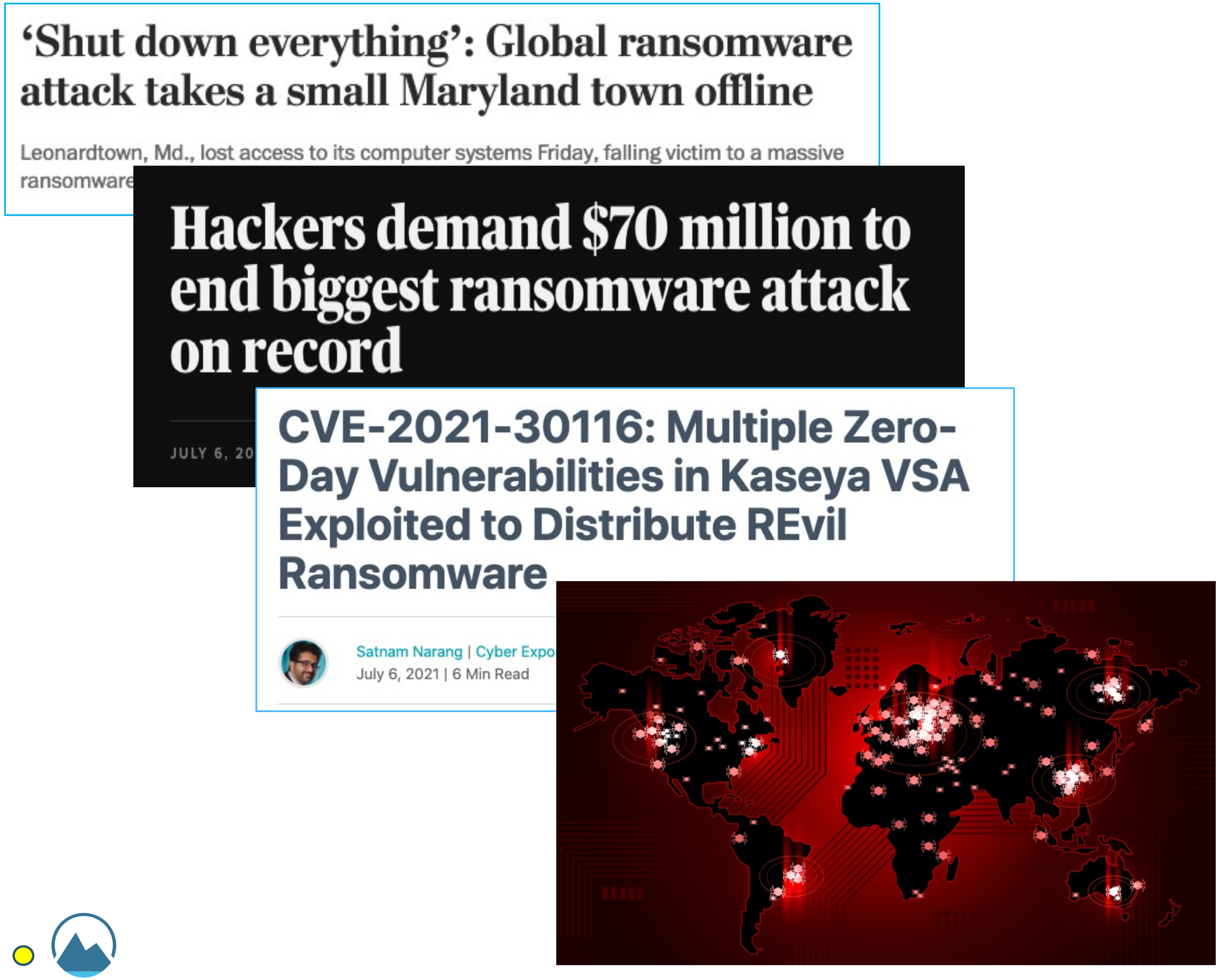
Evil, sometimes.



Today’s Roadmap

- Why We Need to Adapt DFIR
- SolarWinds Supply-Chain Compromise
- Mass 0-day Exchange Exploit
- Kaseya Under the Microscope
- Checklist - How IR Must Evolve

Kaseya Mass 0-Day Ransomware Attacks



‘Shut down everything’: Global ransomware attack takes a small Maryland town offline

Leonardtown, Md., lost access to its computer systems Friday, falling victim to a massive ransomware

Hackers demand $70 million to end biggest ransomware attack on record

JULY 6, 20

CVE-2021-30116: Multiple Zero-Day Vulnerabilities in Kaseya VSA Exploited to Distribute REvil Ransomware

Satnam Narang | Cyber Expo

July 6, 2021 | 6 Min Read

- 0-Day exploit discovered in the Kaseya VSA on-premise system
- Remote monitoring & mgmt system
- Revil ransomware gang/affiliate
- ~1,500 Organizations held for ransom
  - (Over 1,000,000 individual devices encrypted, according to REvil)
- Payment options available:
  - $70 Million for a master decryptor
  - $5 Million for an individual MSP
  - ~$44k and up for downstream customers

solarwinds

blackbaud®
› power your passion

Exchange

tyler technologies
HOME
SOLUTIONS & PRO

Accellion®

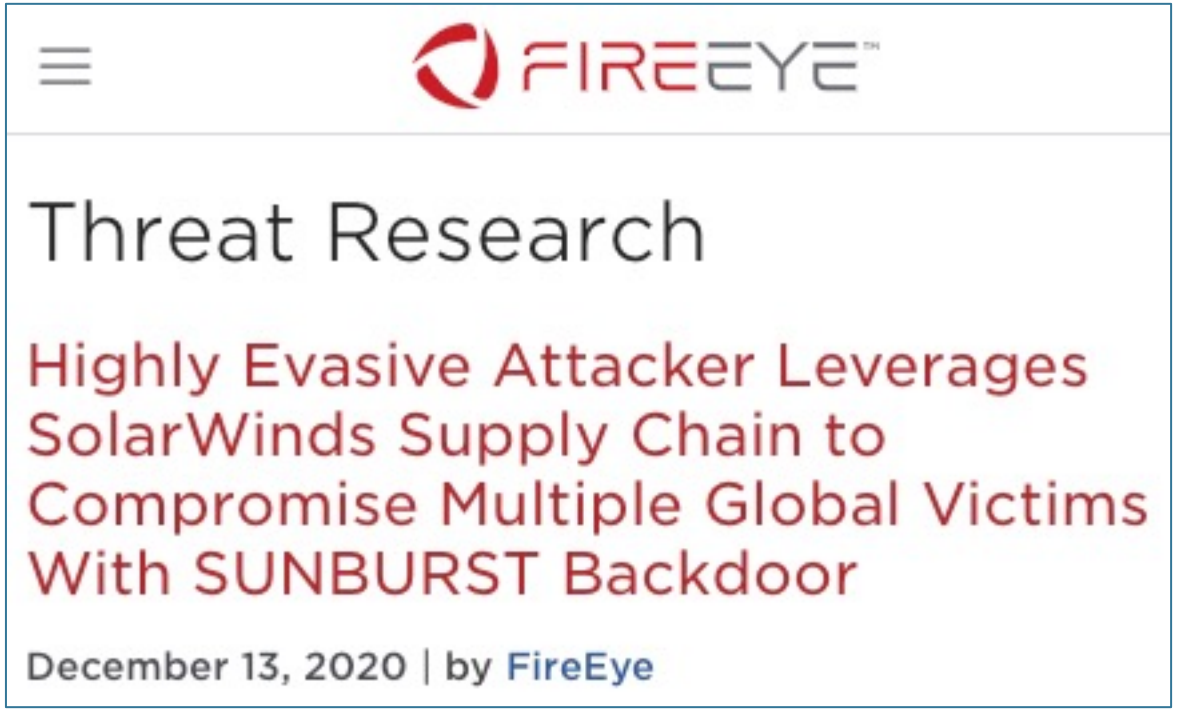
Supply Chain Attacks vs. Mass 0-Day Exploits

- **Supply Chain Attacks** = vector is through a 3rd party technology supplier
- **Mass 0-day Exploit** = exploitation of technology after deployment in victim environment

Response is surprisingly similar

SolarWinds – A Popular Technology Vendor Is Hacked!

- FireEye Announced a Supply-Chain Malware Infection
  - Dec 13
- SolarWinds "Orion" Network Monitoring Software
- Hacked since <Sept 2019
- Backdoor into customer networks
- **18,000 customers**



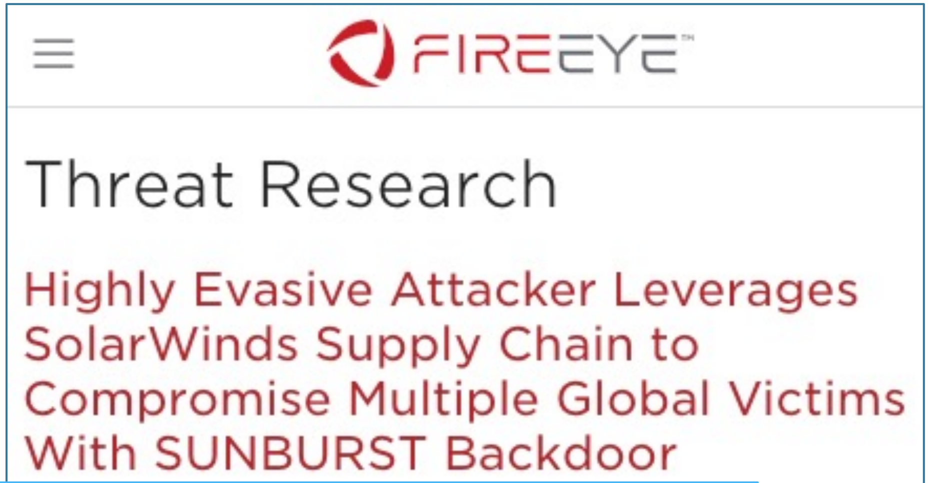
Threat Research

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

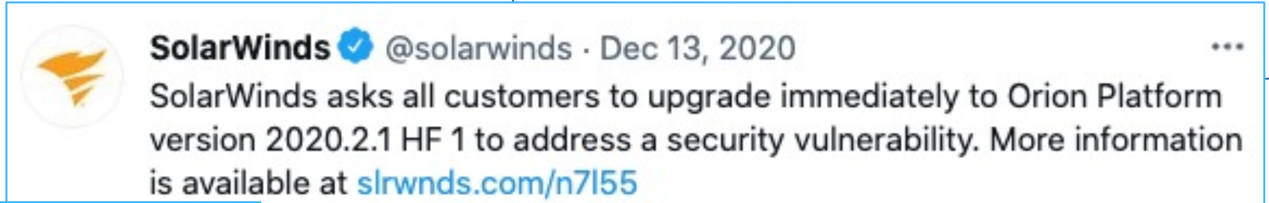
How Did Responders Find Out?

- SolarWinds did not detect the malware
  - Neither did 18,000 other customers
- FireEye (customer)
  - Public notification
  - Offensive security tools stolen
  - 15+ months after original hack
  - 9 months after backdoor rolled out



Threat Research

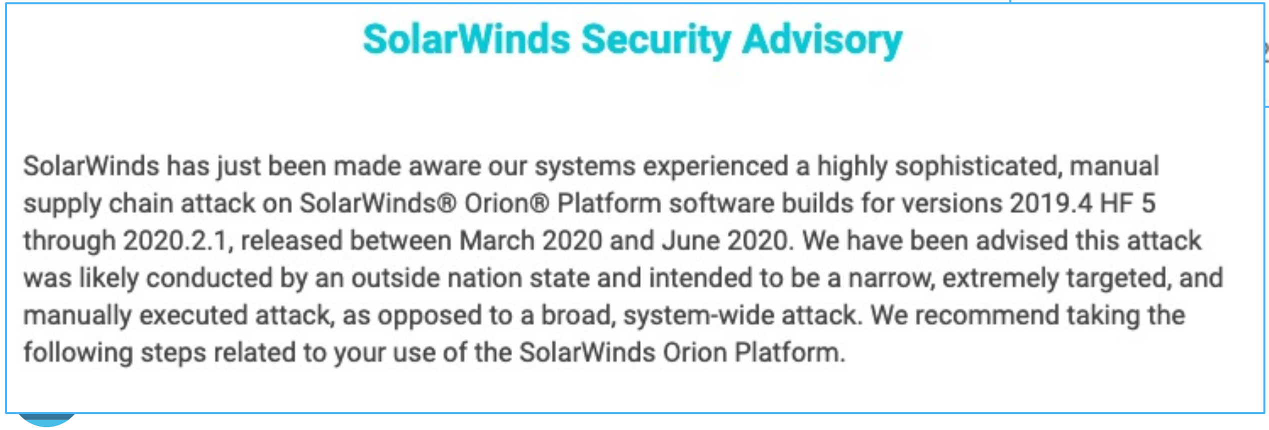
Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor



SolarWinds @solarwinds · Dec 13, 2020

SolarWinds asks all customers to upgrade immediately to Orion Platform version 2020.2.1 HF 1 to address a security vulnerability. More information is available at slrwnds.com/n7l55

757 753

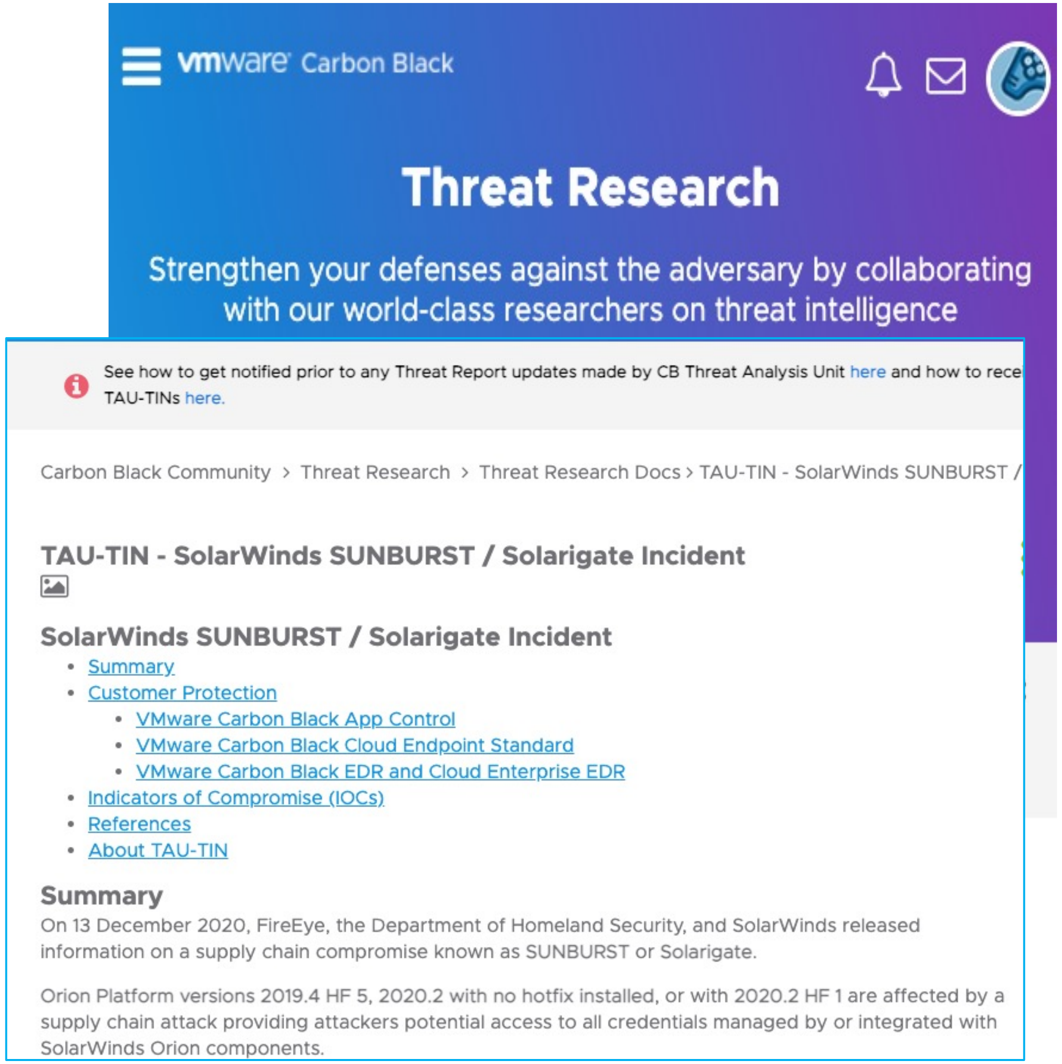


SolarWinds Security Advisory

SolarWinds has just been made aware our systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020. We have been advised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely targeted, and manually executed attack, as opposed to a broad, system-wide attack. We recommend taking the following steps related to your use of the SolarWinds Orion Platform.

Monitor Threat Intelligence

- Identify your key software products & suppliers
- Setup your threat intel sources
  - Vendor alerts & social media
  - Threat intel sources
    - Commercial platforms
    - Security vendors (ie CriticalStack, Crowdstrike)
    - Academia, government, etc.
  - Cybersecurity news
    - Bleeping Computer, ZDNet, WSJ, etc
- Assign responsibility for responding to alerts
- Review & triage
- Feed into response processes
- Practice – tabletops etc.
- Make sure your suppliers are doing the same!



Threat Research

Strengthen your defenses against the adversary by collaborating with our world-class researchers on threat intelligence

See how to get notified prior to any Threat Report updates made by CB Threat Analysis Unit here and how to rece
TAU-TINs here.

Carbon Black Community › Threat Research › Threat Research Docs › TAU-TIN - SolarWinds SUNBURST /

TAU-TIN - SolarWinds SUNBURST / Solarigate Incident

SolarWinds SUNBURST / Solarigate Incident

- Summary
- Customer Protection
  - VMware Carbon Black App Control
  - VMware Carbon Black Cloud Endpoint Standard
  - VMware Carbon Black EDR and Cloud Enterprise EDR
- Indicators of Compromise (IOCs)
- References
- About TAU-TIN

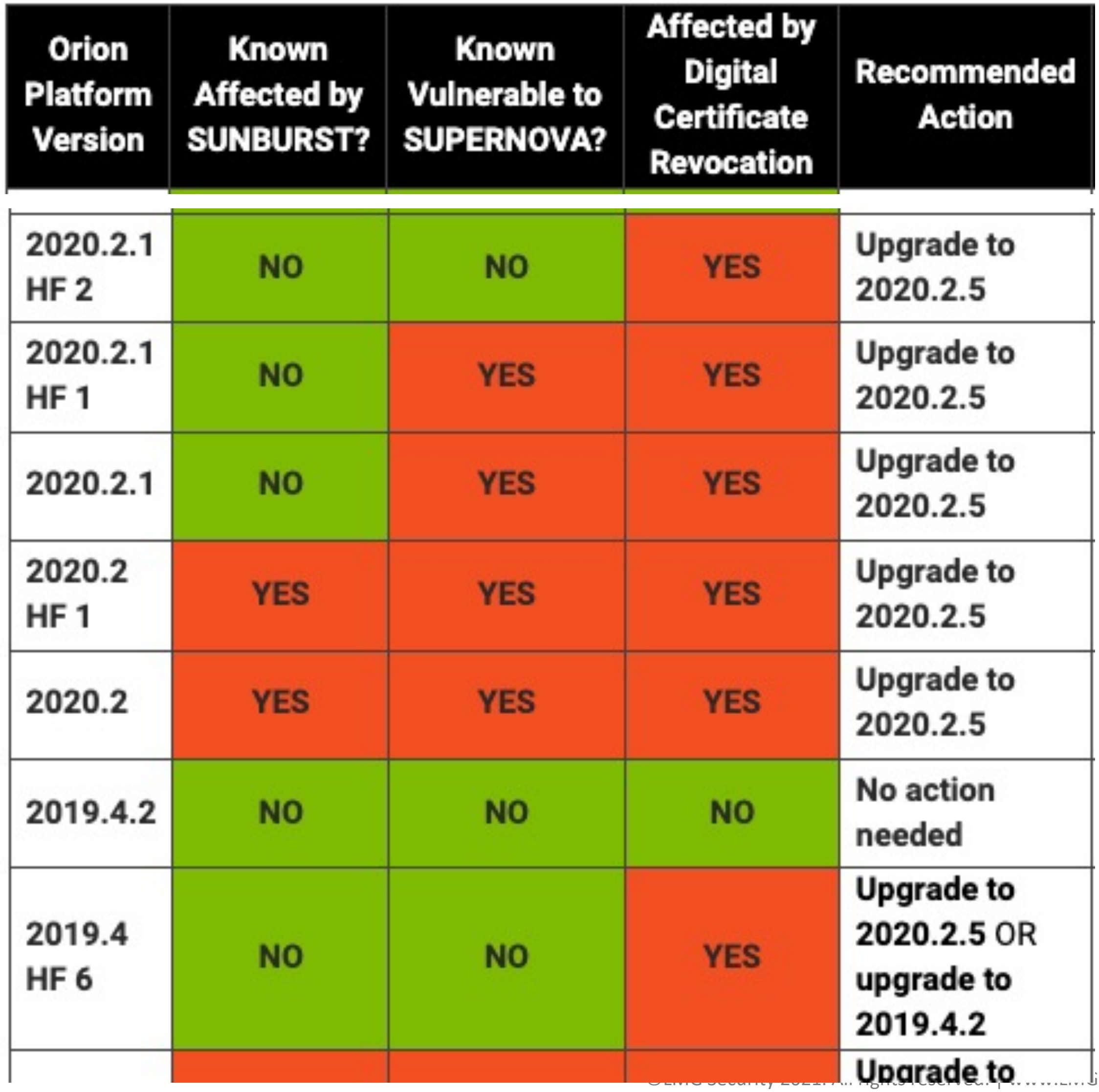
Summary

On 13 December 2020, FireEye, the Department of Homeland Security, and SolarWinds released information on a supply chain compromise known as SUNBURST or Solarigate.

Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, or with 2020.2 HF 1 are affected by a supply chain attack providing attackers potential access to all credentials managed by or integrated with SolarWinds Orion components.

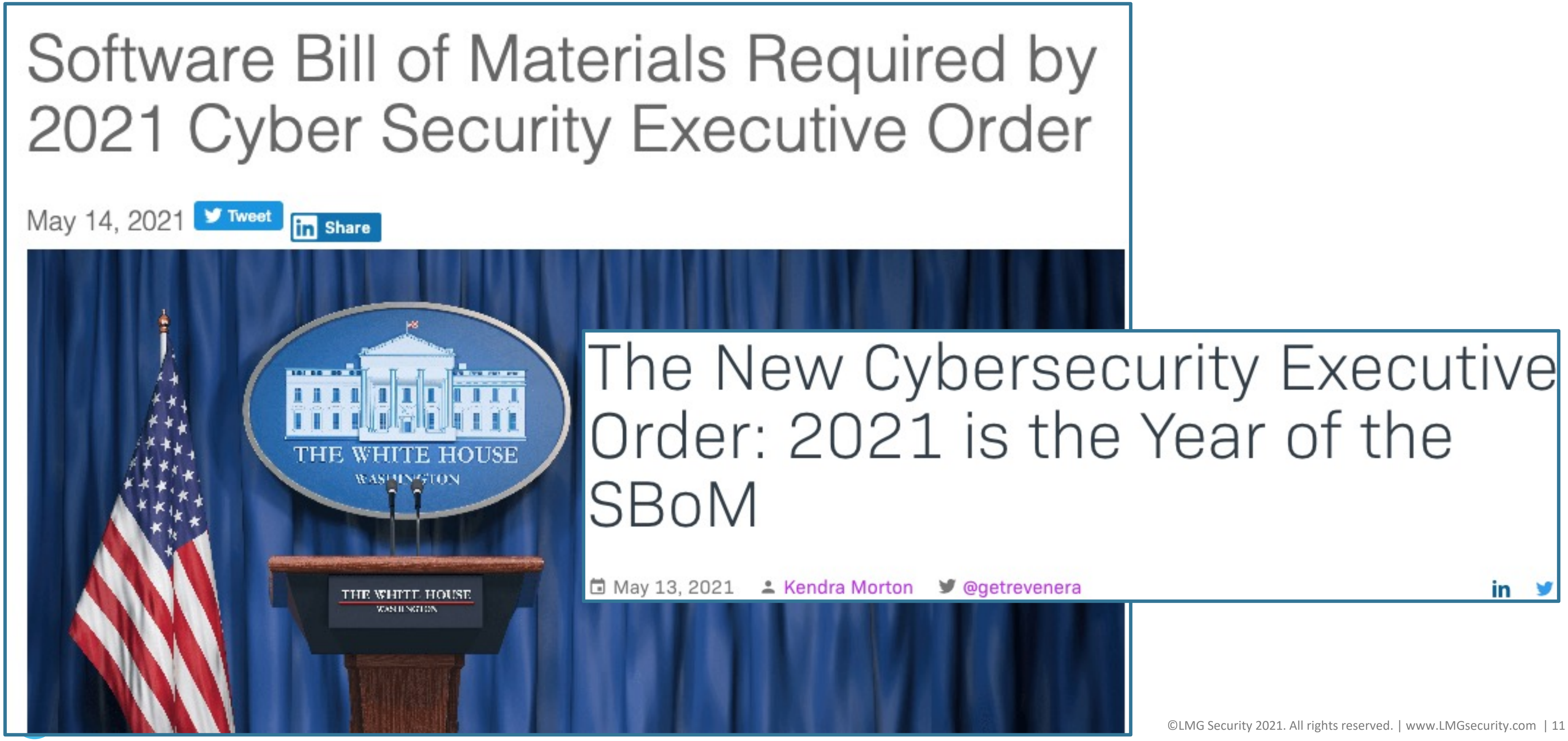
Evaluate Your Risk

- Affected versions of software
  - May not be immediately known
- Were you running an affected version during the period of compromise?
  - Change management logs
- What should you do if you’re not sure?
  - Plan ahead
  - Often, takedown software
  - Can be impactful
- Watch for changes
- Check suppliers, too…



Orion Platform Version	Known Affected by SUNBURST?	Known Vulnerable to SUPERNOVA?	Affected by Digital Certificate Revocation	Recommended Action
2020.2.1 HF 2	NO	NO	YES	Upgrade to 2020.2.5
2020.2.1 HF 1	NO	YES	YES	Upgrade to 2020.2.5
2020.2.1	NO	YES	YES	Upgrade to 2020.2.5
2020.2 HF 1	YES	YES	YES	Upgrade to 2020.2.5
2020.2	YES	YES	YES	Upgrade to 2020.2.5
2019.4.2	NO	NO	NO	No action needed
2019.4 HF 6	NO	NO	YES	Upgrade to 2020.2.5 OR upgrade to 2019.4.2
				Upgrade to

New! Software Bill of Materials



Software Bill of Materials Required by 2021 Cyber Security Executive Order

May 14, 2021 Tweet Share

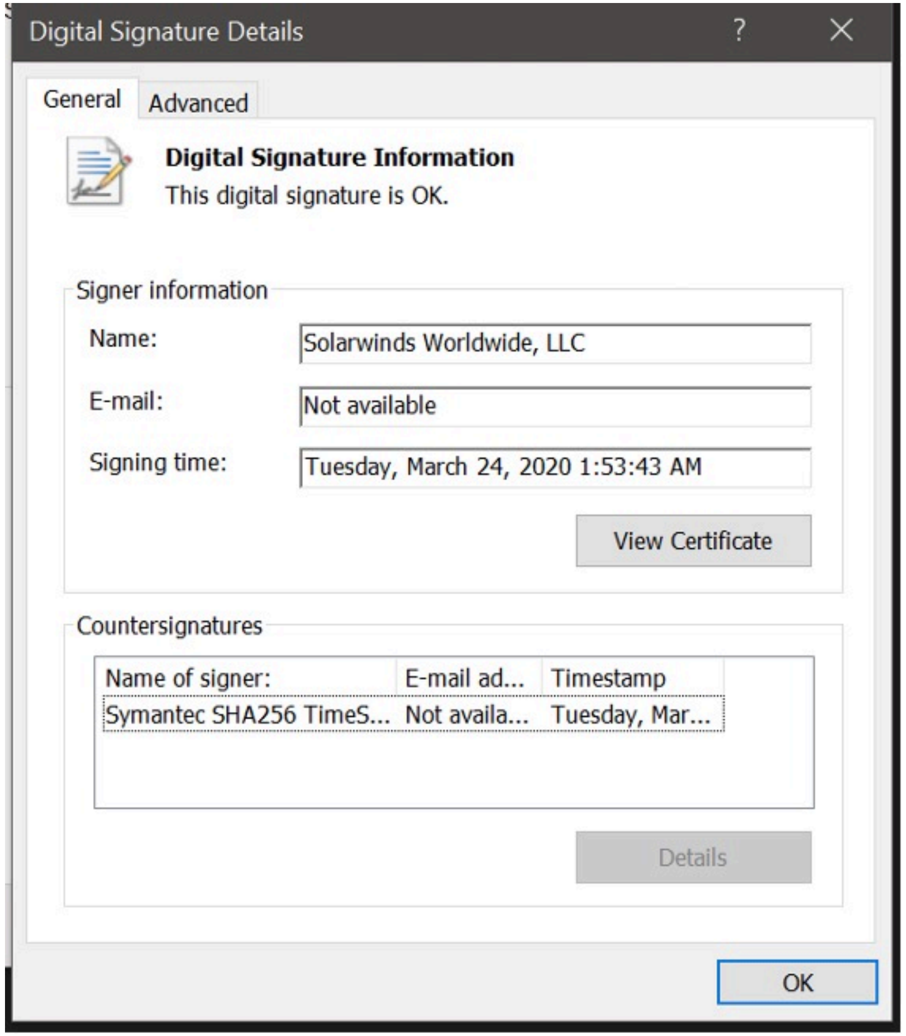
The New Cybersecurity Executive Order: 2021 is the Year of the SBoM

May 13, 2021 Kendra Morton @getrevenera

SolarWinds - Hacked Customers

Attackers can:

- Steal files
- Install new software
- Gather network information
- Reboot systems
- Disable security tools
- & more



Digital Signature Information

This digital signature is OK.

Signer information

Name: Solarwinds Worldwide, LLC

E-mail: Not available

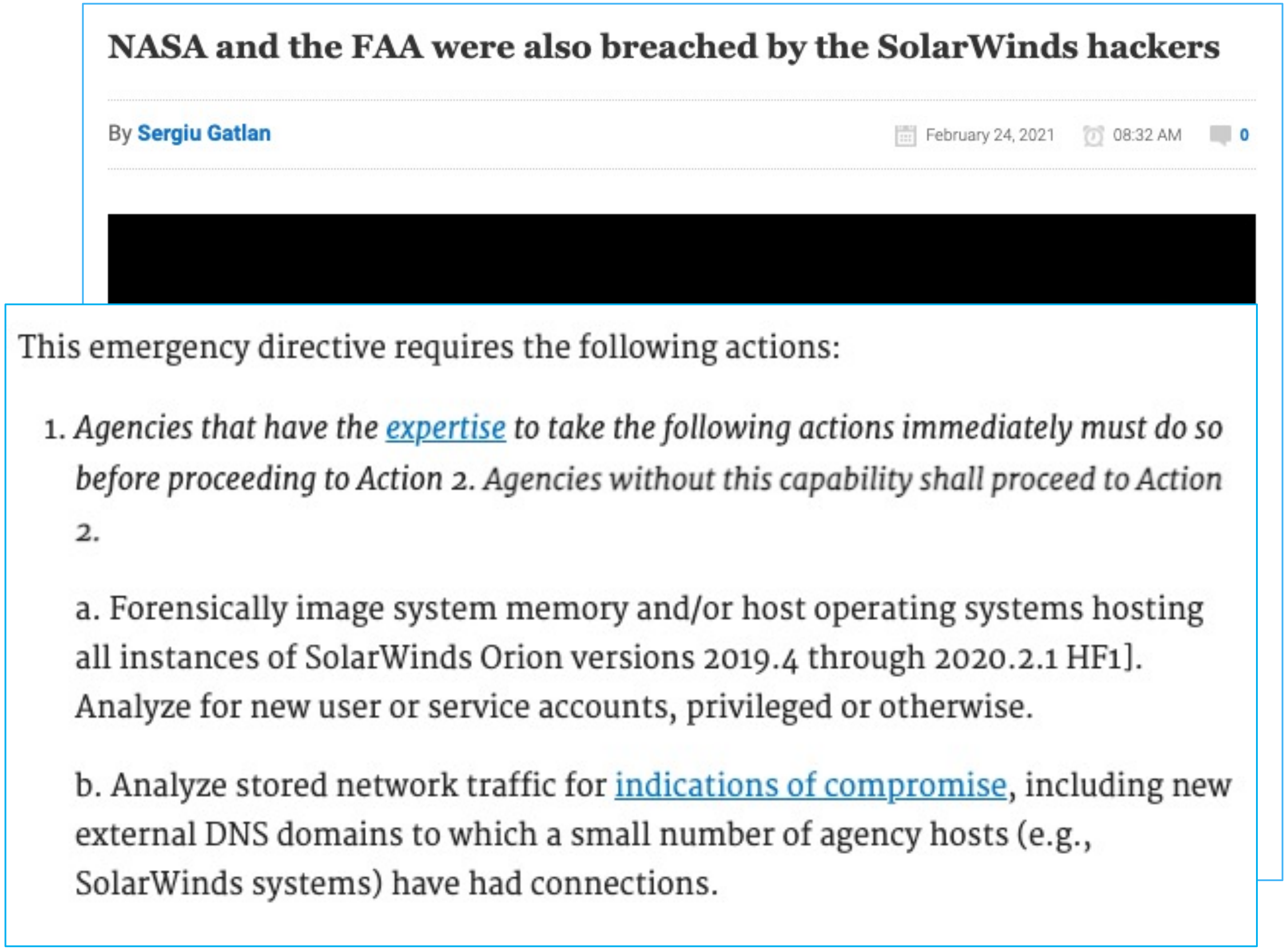
Signing time: Tuesday, March 24, 2020 1:53:43 AM

Countersignatures

Name of signer:	E-mail ad...	Timestamp
Symantec SHA256 TimeS...	Not availa...	Tuesday, Mar...

Preserve Evidence!

- Remember the risks…
- Potentially full takeover
  - May be a breach!
  - Reputational, legal, financial risks
- Bring in cyber insurer, breach coach, forensics team, etc.
- See CISA Emergency Directive 21-01



NASA and the FAA were also breached by the SolarWinds hackers

By Sergiu Gatlan

February 24, 2021 08:32 AM 0

This emergency directive requires the following actions:

1. *Agencies that have the expertise to take the following actions immediately must do so before proceeding to Action 2. Agencies without this capability shall proceed to Action 2.*

   a. Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1]. Analyze for new user or service accounts, privileged or otherwise.

   b. Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections.

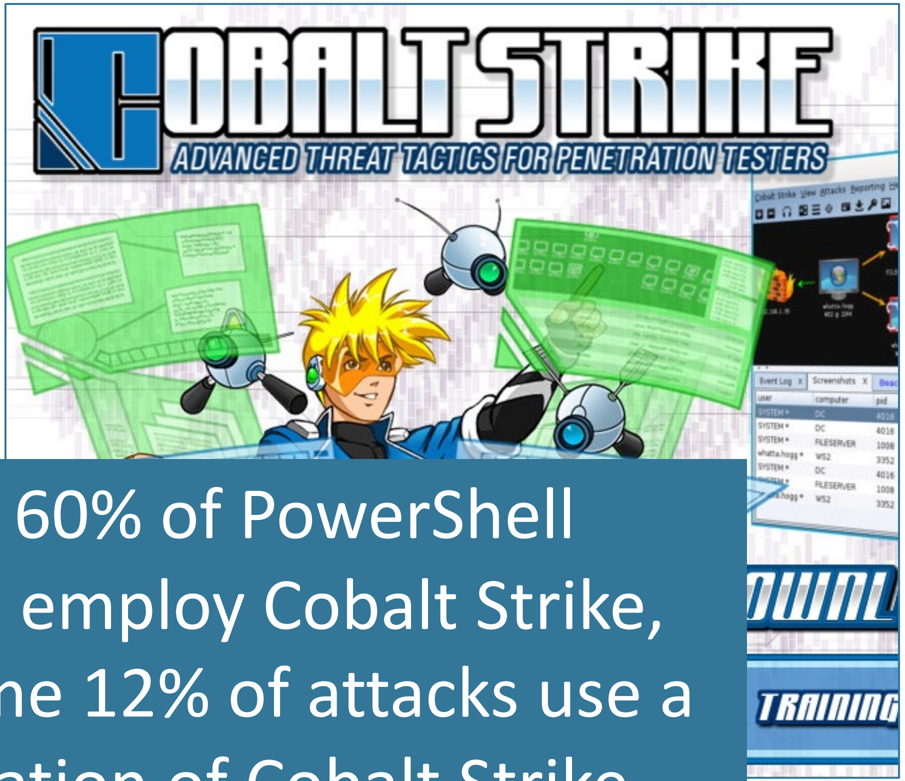
Contain the Damage

- Act quickly– with little or no information
- Government advisories can help…
- Standard options:
  - Yank the network/power
  - System-wide password reset
- Impacts:
  - Operational impacts
  - Help desk calls
  - Network visibility is limited
  - Evidence might be destroyed

"Affected agencies shall immediately **disconnect or power down SolarWinds Orion products…** Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package…"
~DHS ED 21-01

Pulling the Plug on SolarWinds Might Not Save You...

- TEARDROP – Memory-only dropper
- RAINDROP – Installed later; used to deliver Cobalt Strike
- Cobalt Strike BEACON
  - Legit pentesting software
  - Customized

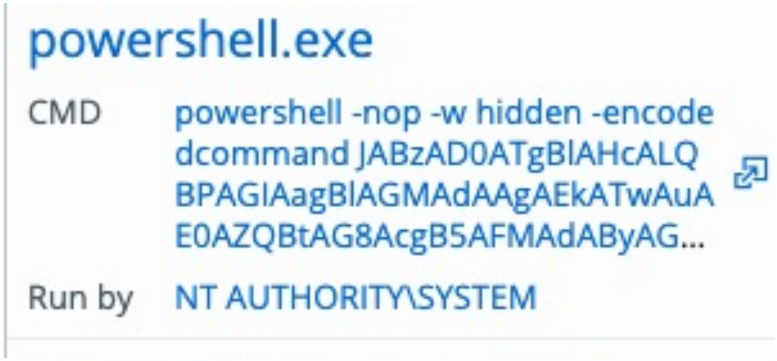


"Nearly 60% of PowerShell exploits employ Cobalt Strike, and some 12% of attacks use a combination of Cobalt Strike and Microsoft Windows tools PowerShell and PsExec."

https://www.darkreading.com/attacks-breaches/cobalt-strike-becomes-a-preferred-hacking-tool-by-cybercrime-apt-groups/d/d-id/1341073

Hunt for Threats

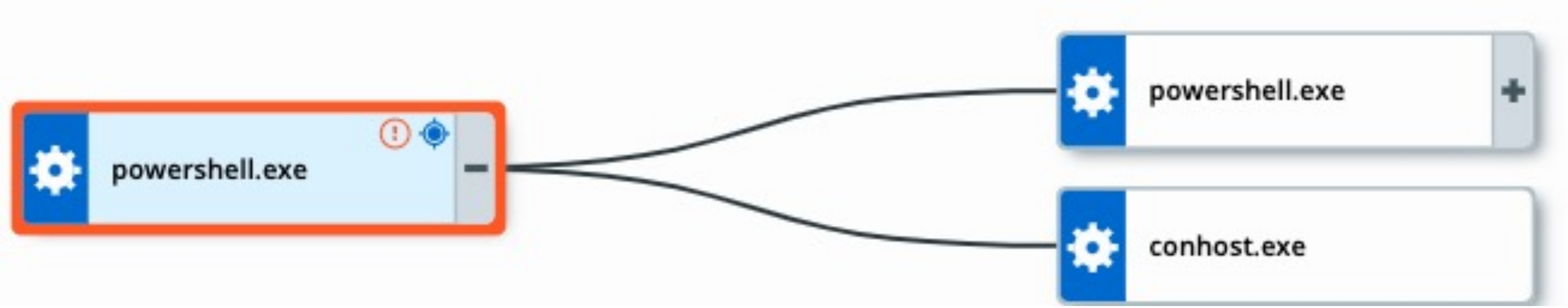
- We used Carbon Black!
- Finding Cobalt Strike beacons:



powershell.exe

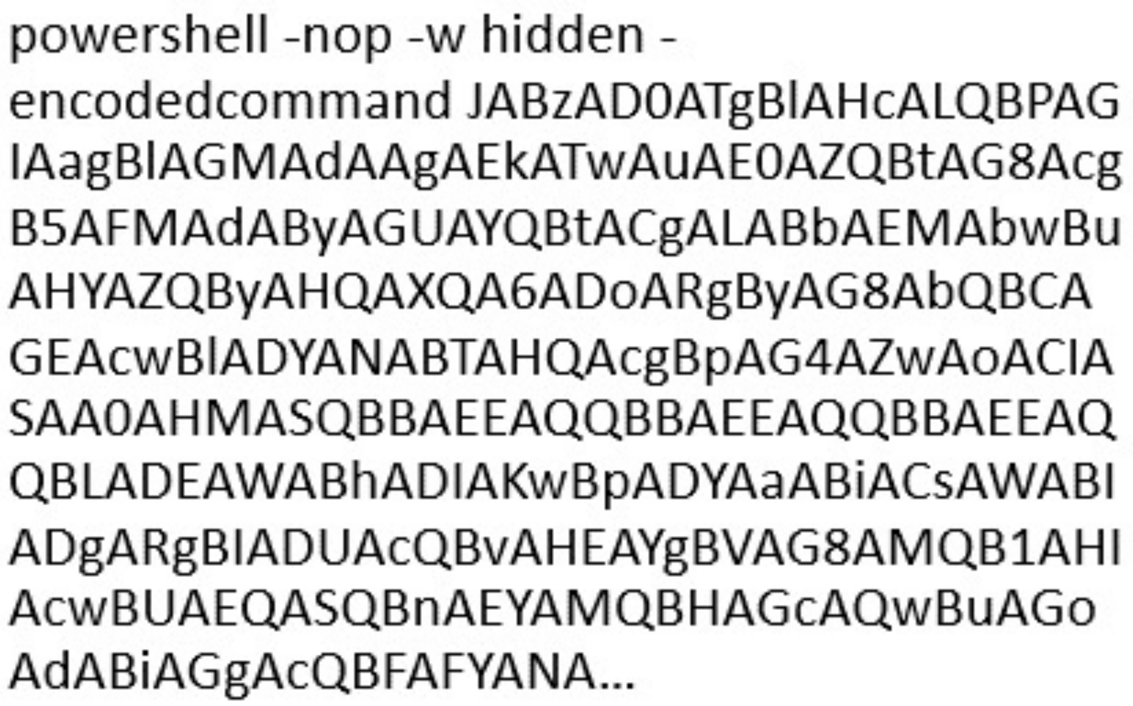
CMD powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAG...

Run by NT AUTHORITY\SYSTEM



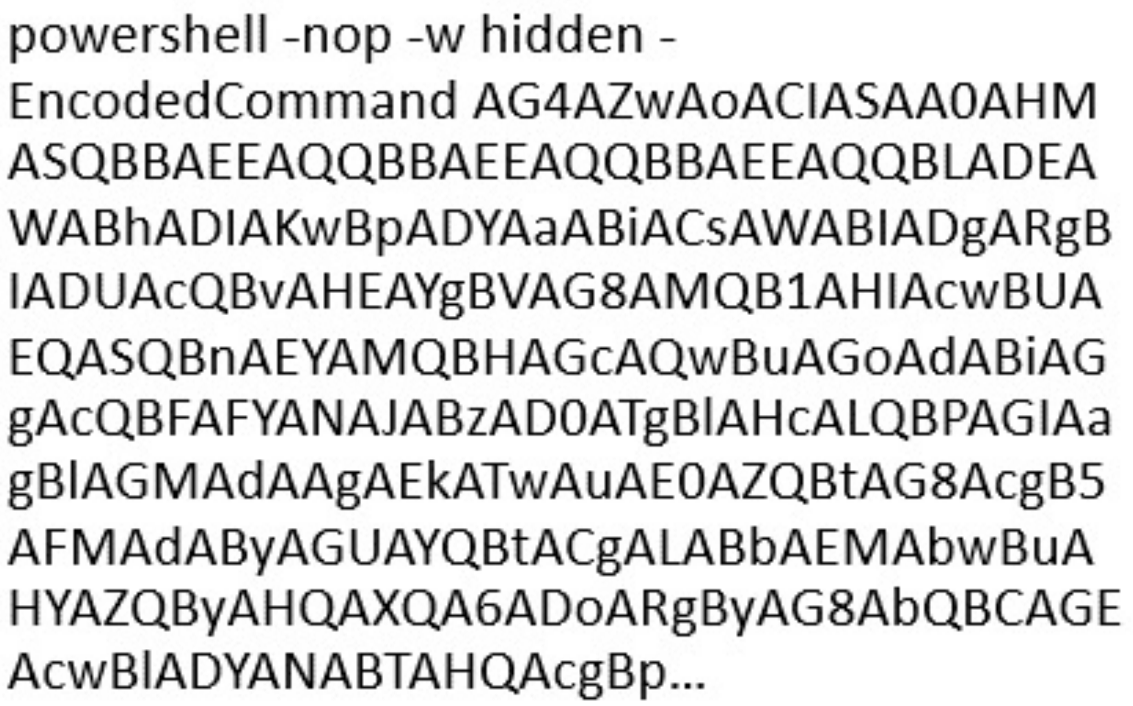
Beware of False Positives

- Cobalt Strike Beacon Payload



```
powershell -nop -w hidden -
encodedcommand JABzAD0ATgBlAHcALQBPAG
IAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8Acg
B5AFMAdAByAGUAYQBtACgALABbAEMAbwBu
AHYAZQByAHQAXQA6ADoARgByAG8AbQBCA
GEAcwBlADYANABTAHQAcgBpAG4AZwAoACIA
SAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQ
QBLADEAWABhADIAKwBpADYAaABiACsAWABI
ADgARgBlADUAcQBvAHEAYgBVAG8AMQB1AHI
AcwBUAEQASQBnAEYAMQBHAGcAQwBuAGo
AdABiAGgAcQBFAFYANA...
```

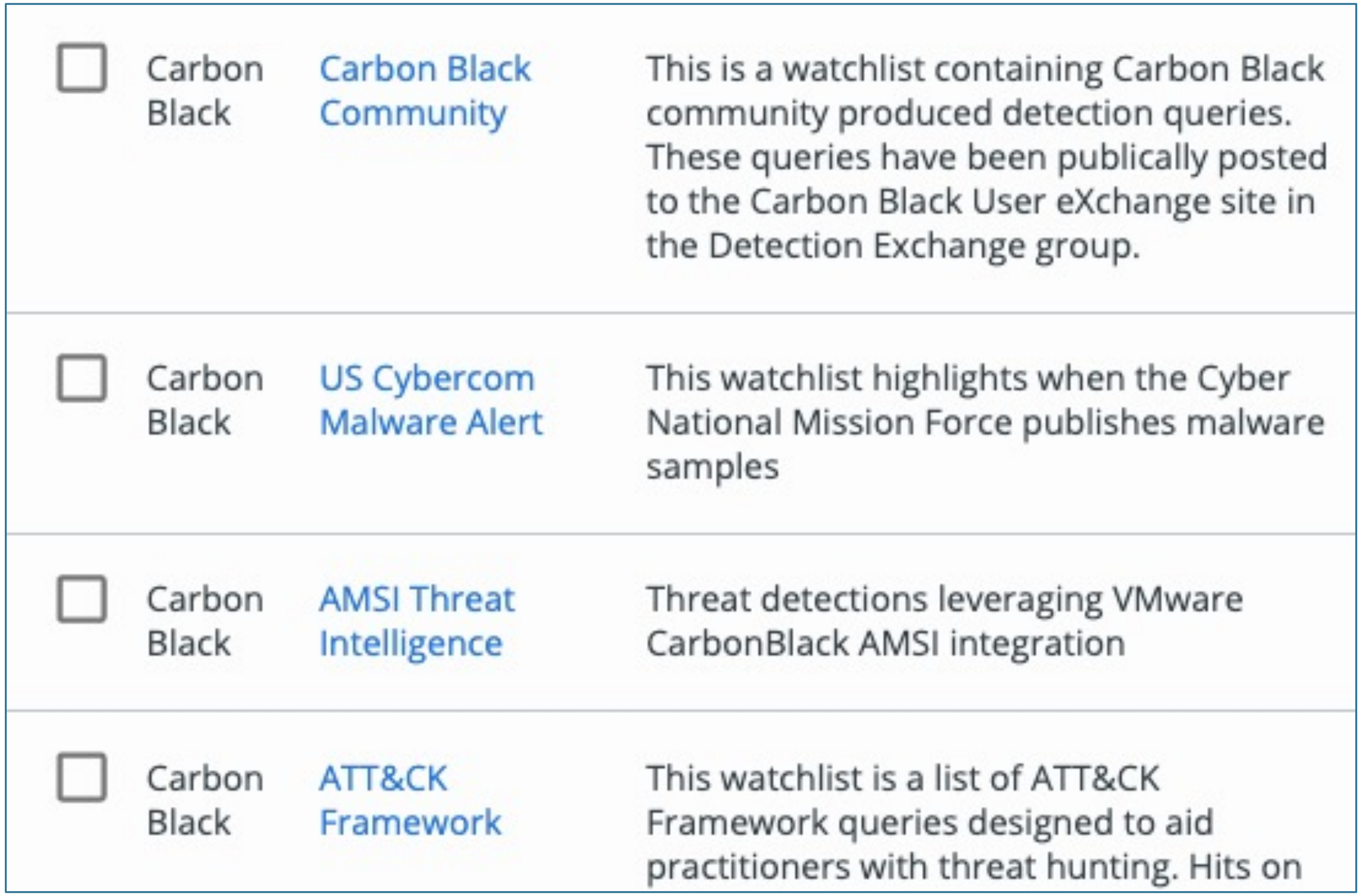
- Ansible Command



```
powershell -nop -w hidden -
EncodedCommand AG4AZwAoACIASAA0AHM
ASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEA
WABhADIAKwBpADYAaABiACsAWABIADgARgB
lADUAcQBvAHEAYgBVAG8AMQB1AHIAcwBUA
EQASQBnAEYAMQBHAGcAQwBuAGoAdABiAG
gAcQBFAFYANAJABzAD0ATgBlAHcALQBPAGIAa
gBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5
AFMAdAByAGUAYQBtACgALABbAEMAbwBuA
HYAZQByAHQAXQA6ADoARgByAG8AbQBCAGE
AcwBlADYANABTAHQAcgBp...
```

Obtaining IoCs

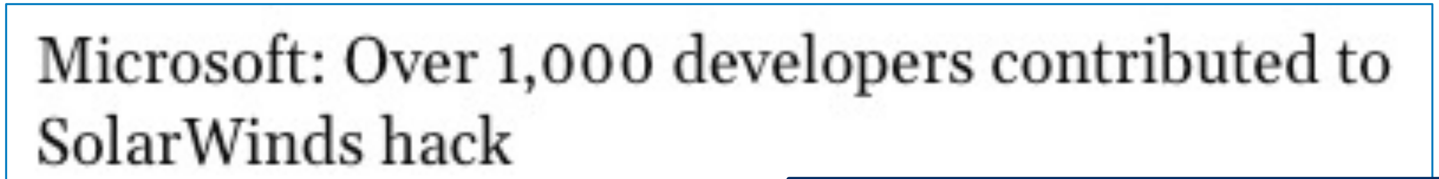
- Hacked customers (ie FireEye, Microsoft)
- Gov agencies (ie CISA)
- The vendor
- Security firms/researchers
- Threat hunting/intel software
  - Ie Carbon Black
- MISP - open-source threat intel
  - https://www.misp-project.org/
- Popular formats:
  - Structured Threat Information Expression (STIX)
  - YARA



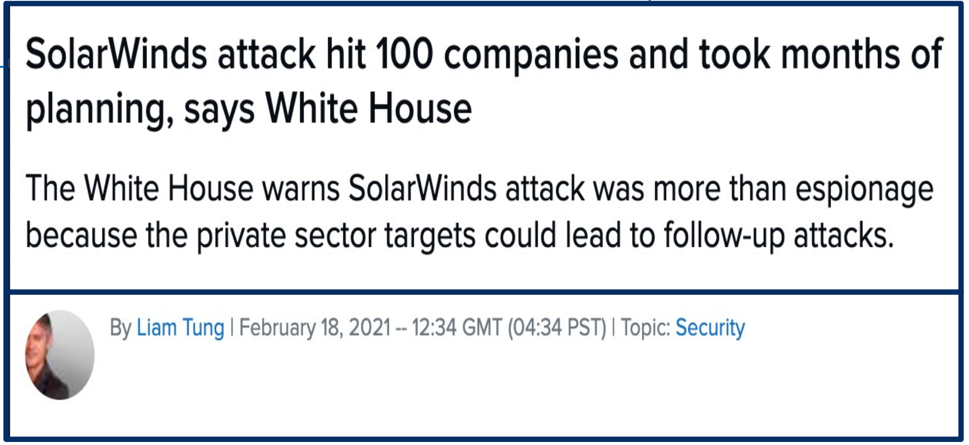
□	Carbon Black	Carbon Black Community	This is a watchlist containing Carbon Black community produced detection queries. These queries have been publically posted to the Carbon Black User eXchange site in the Detection Exchange group.
□	Carbon Black	US Cybercom Malware Alert	This watchlist highlights when the Cyber National Mission Force publishes malware samples
□	Carbon Black	AMSI Threat Intelligence	Threat detections leveraging VMware CarbonBlack AMSI integration
□	Carbon Black	ATT&CK Framework	This watchlist is a list of ATT&CK Framework queries designed to aid practitioners with threat hunting. Hits on

Nation-State Attack

- Russia
- Aka NOBELIUM
- Aka Cozy Bear
- Aka APT 29



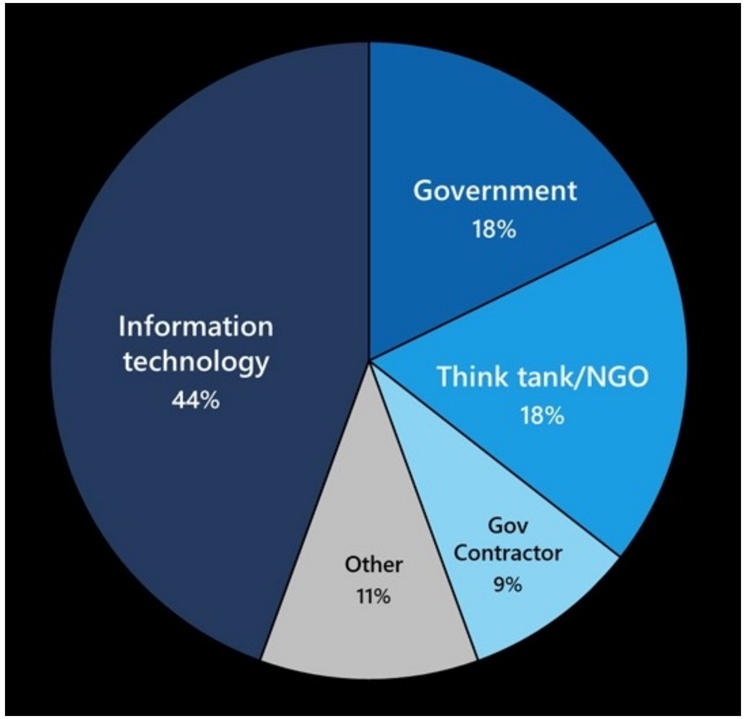
Microsoft: Over 1,000 developers contributed to SolarWinds hack



SolarWinds attack hit 100 companies and took months of planning, says White House

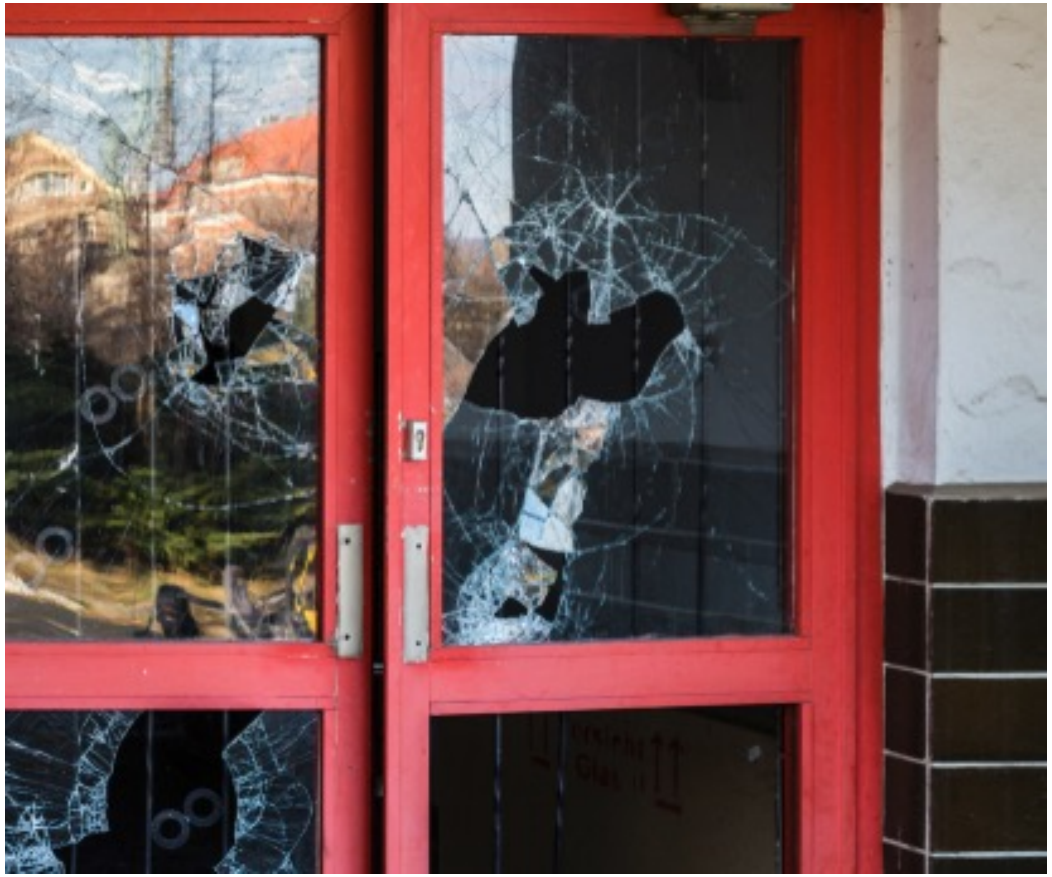
The White House warns SolarWinds attack was more than espionage because the private sector targets could lead to follow-up attacks.

By Liam Tung | February 18, 2021 -- 12:34 GMT (04:34 PST) | Topic: Security

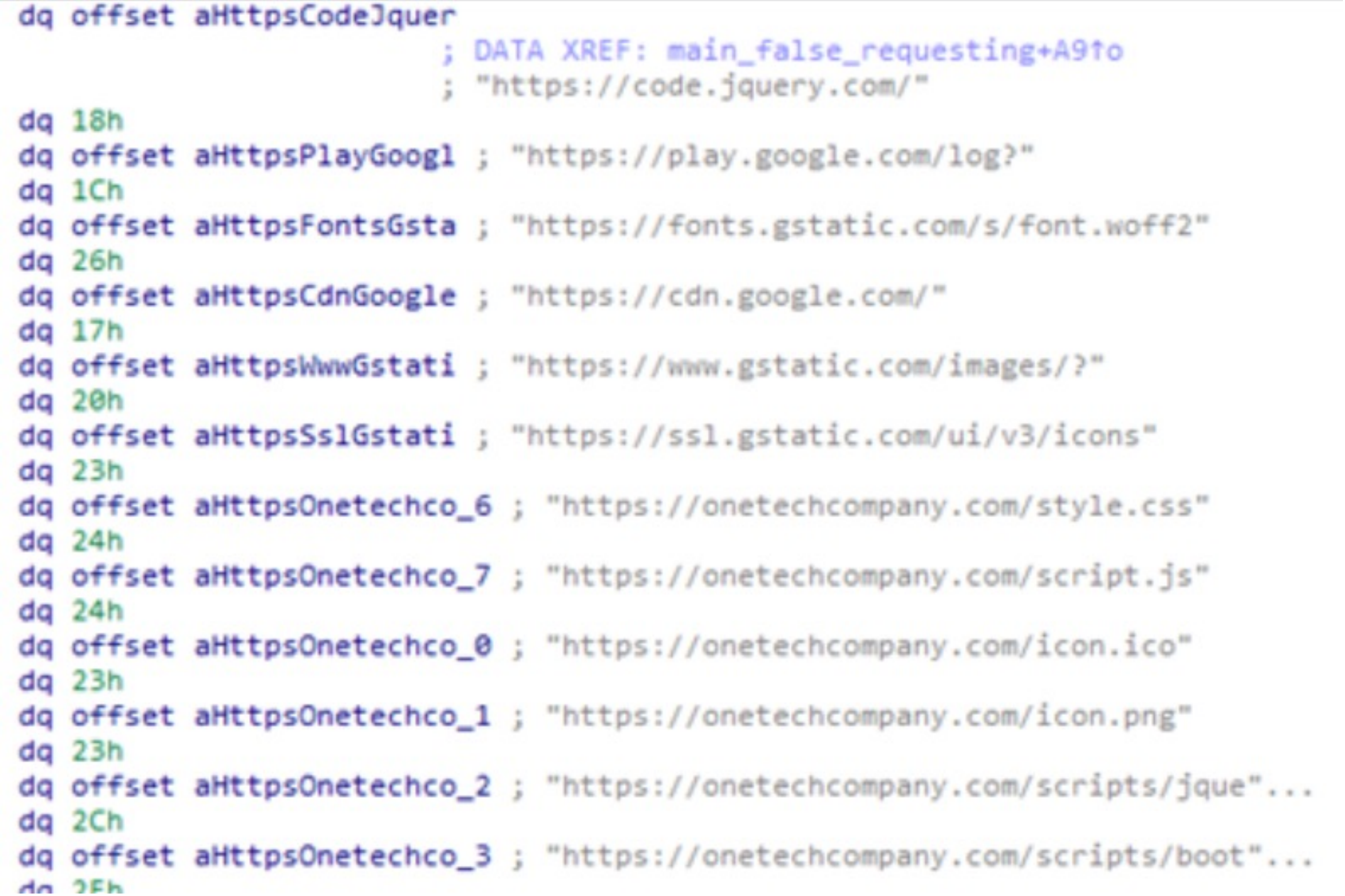


Difficult to Obtain IoCs

- Sunburst malware is designed to evade detection
- 12-14 day sleep timer
- Verifies specific DLL name
- Randomly delays execution of later phases
- Multiple domain checks
- Security/analysis software checks



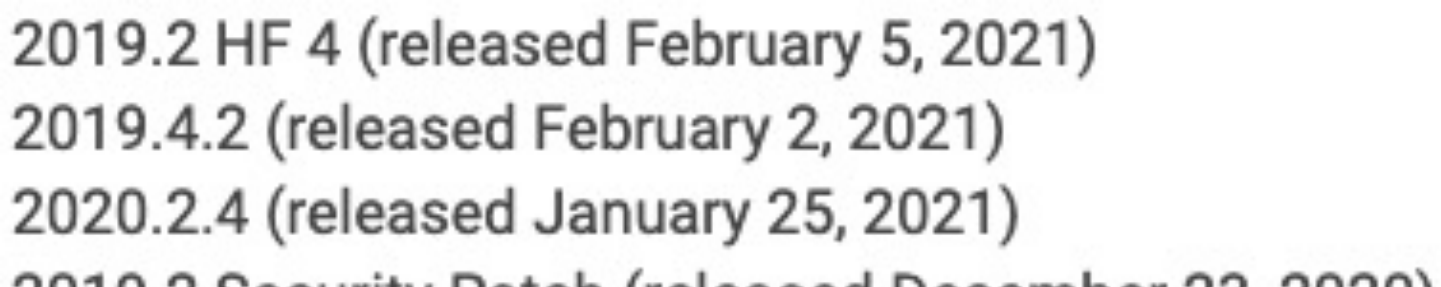
Decoy Traffic



```
dq offset aHttpsCodeJquer
                                        ; DATA XREF: main_false_requesting+A9↑o
                                        ; "https://code.jquery.com/"
dq 18h
dq offset aHttpsPlayGoogl ; "https://play.google.com/log?"
dq 1Ch
dq offset aHttpsFontsGsta ; "https://fonts.gstatic.com/s/font.woff2"
dq 26h
dq offset aHttpsCdnGoogle ; "https://cdn.google.com/"
dq 17h
dq offset aHttpsWwwGstati ; "https://www.gstatic.com/images/?"
dq 20h
dq offset aHttpsSslGstati ; "https://ssl.gstatic.com/ui/v3/icons"
dq 23h
dq offset aHttpsOnetechco_6 ; "https://onetechcompany.com/style.css"
dq 24h
dq offset aHttpsOnetechco_7 ; "https://onetechcompany.com/script.js"
dq 24h
dq offset aHttpsOnetechco_0 ; "https://onetechcompany.com/icon.ico"
dq 23h
dq offset aHttpsOnetechco_1 ; "https://onetechcompany.com/icon.png"
dq 23h
dq offset aHttpsOnetechco_2 ; "https://onetechcompany.com/scripts/jque"...
dq 2Ch
dq offset aHttpsOnetechco_3 ; "https://onetechcompany.com/scripts/boot"...
dq 2Fh
```

Apply Emergency Patches/Software Updates

- May not exist
- May not work
- May break things
- Expect multiple updates
- Do you want to be an early adopter?
  - Decide in advance
  - Tabletops/response plan



2019.2 HF 4 (released February 5, 2021)

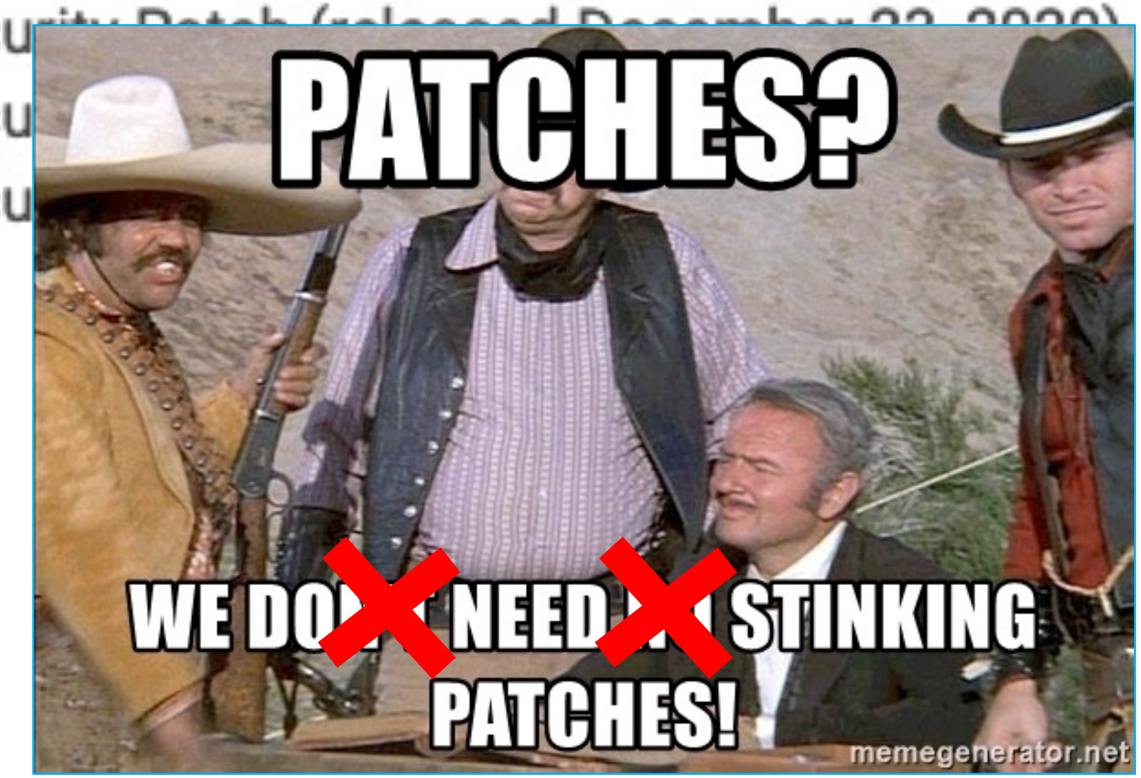
2019.4.2 (released February 2, 2021)

2020.2.4 (released January 25, 2021)

2019.2 Security Patch (released December 22, 2020)

2018.4 Secu

2018.2 Secu



Plan for Elevated Risks

- For you and affected suppliers/technology
- Hackers may have extensive data
  - Employee emails
  - Internal data
  - Passwords, keys & more
- APTs & additional malware
- Software source code & vuln details
- MSP customer lists
- Remember: suppliers may not have detected/announced all hacks

Home > News > Security

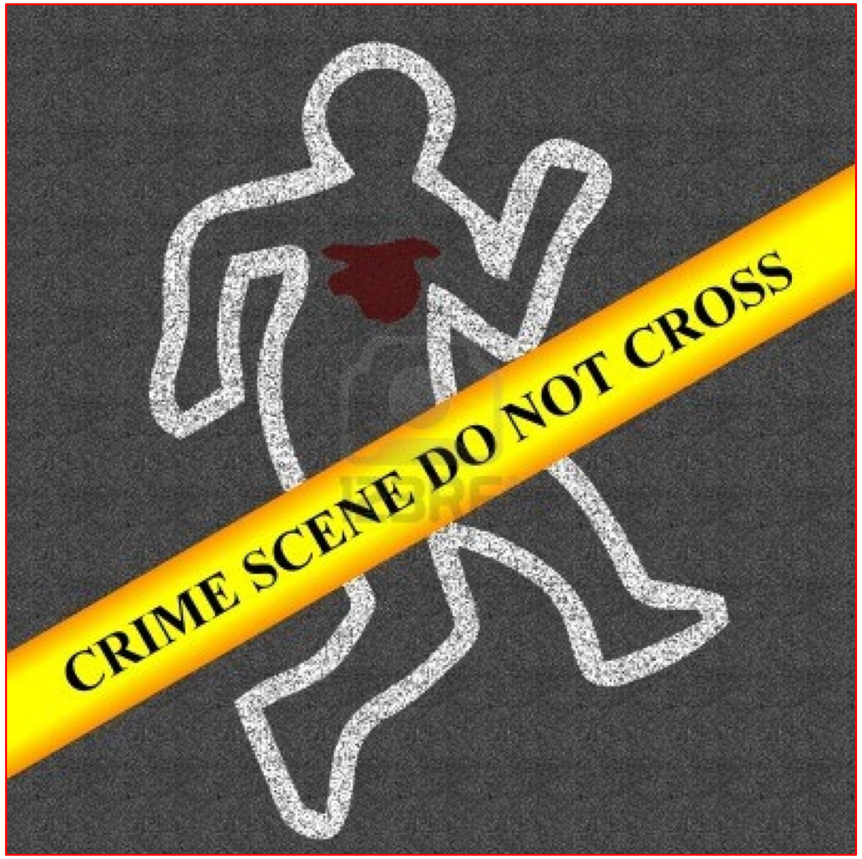
Microsoft Warns of Continued Attacks by the Nobelium Hacking Group

Microsoft says the Nobelium hackers who have targeted SolarWinds, USAID, and other organizations accessed information stored on one of its employee's devices.

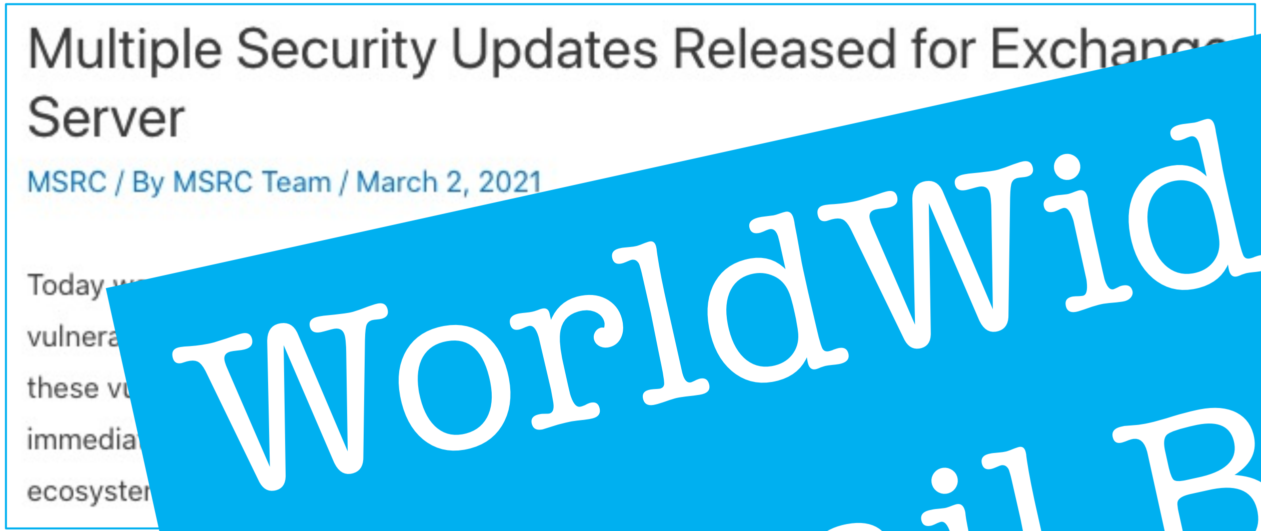
By Nathaniel Mott June 26, 2021

Responding to Supply Chain Attacks

1. Monitor threat intelligence
2. Evaluate the risk
3. Preserve forensic evidence
4. Contain the damage
5. Hunt for threats
6. Apply emergency patches/updates
7. Plan for elevated risks



Exchange Zero-Day Vuln is Publicly Announced!



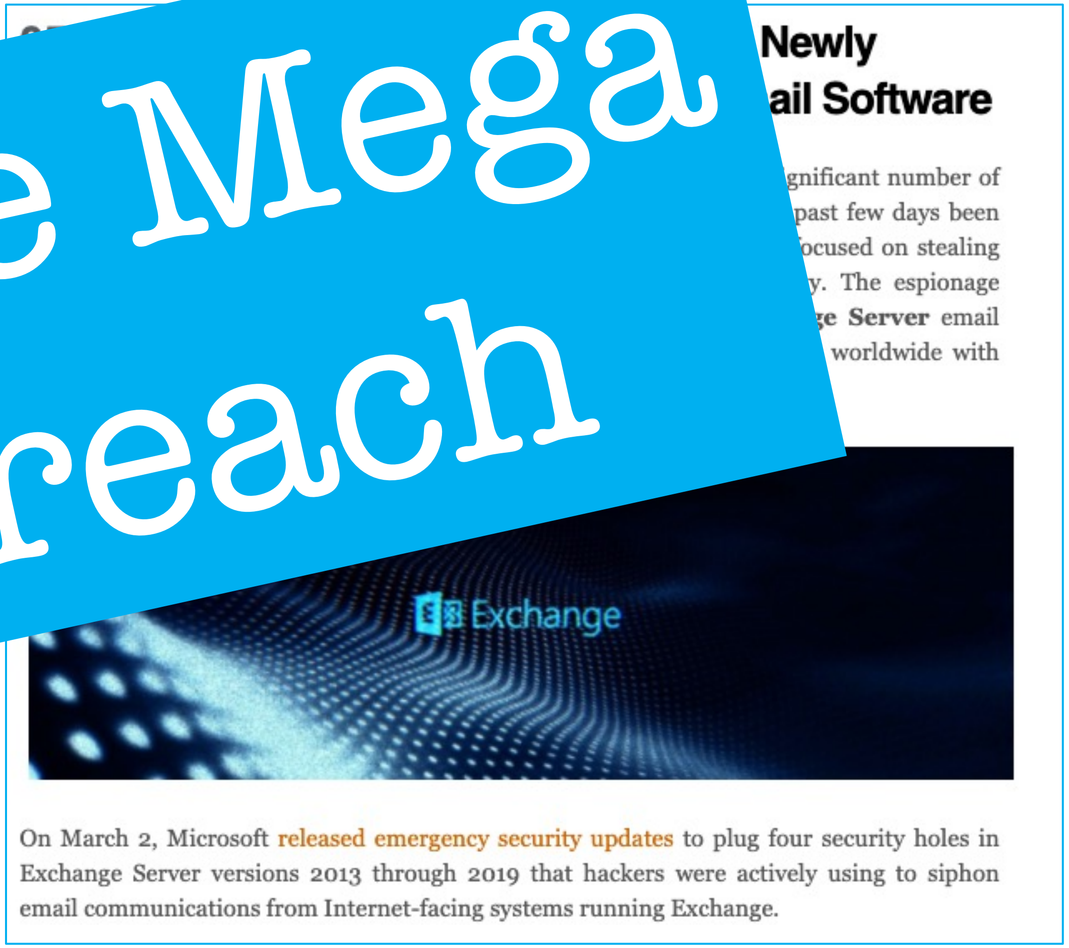
Multiple Security Updates Released for Exchang
Server

MSRC / By MSRC Team / March 2, 2021

Today w
vulnera
these vu
immediat
ecosyster

Micro
Morph

By William Turton
March 6, 2021, 5:4
pdated on March 8, 2021, 1:01 AM MST



Newly
ail Software

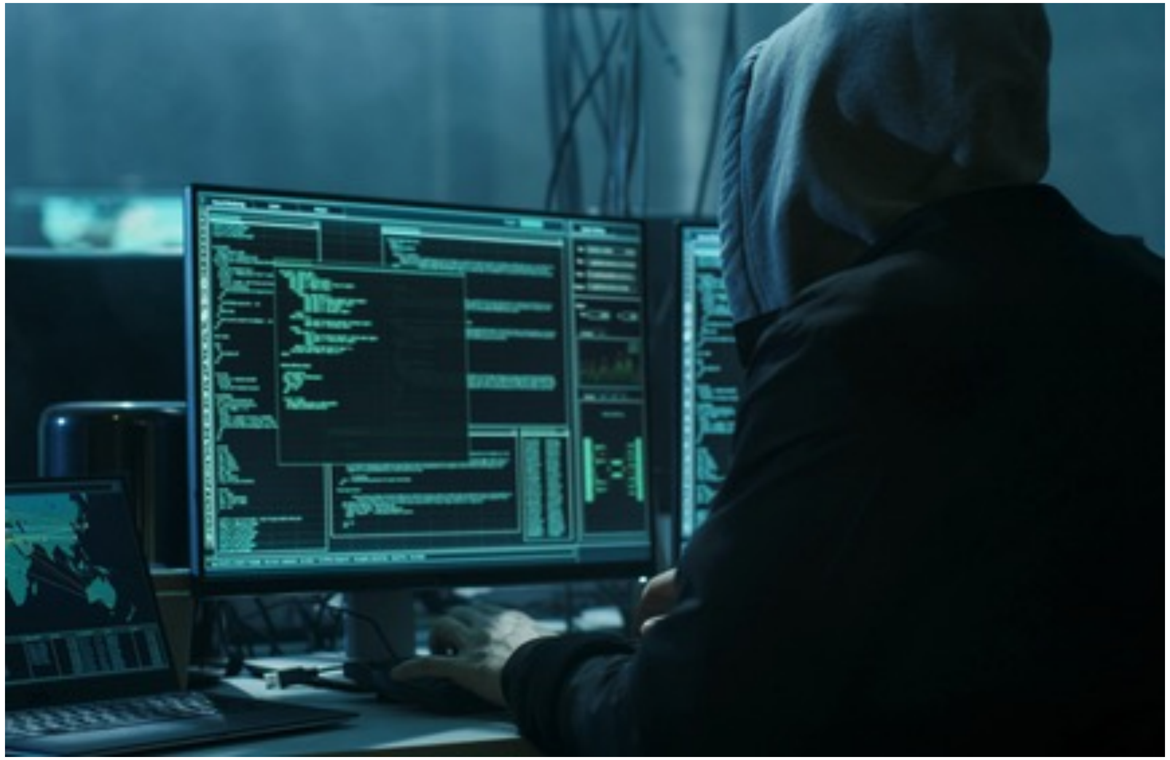
gnificant number of
past few days been
ocused on stealing
y. The espionage
ge Server email
worldwide with

On March 2, Microsoft released emergency security updates to plug four security holes in Exchange Server versions 2013 through 2019 that hackers were actively using to siphon email communications from Internet-facing systems running Exchange.

WorldWide Mega
Email Breach

What Can the Hackers do?

- Gain full administrator control of the exchange server
- Steal email
- Steal credentials
- Install more malware
- Infect other computers on the network



How Do You Find Out?

Most people found out here

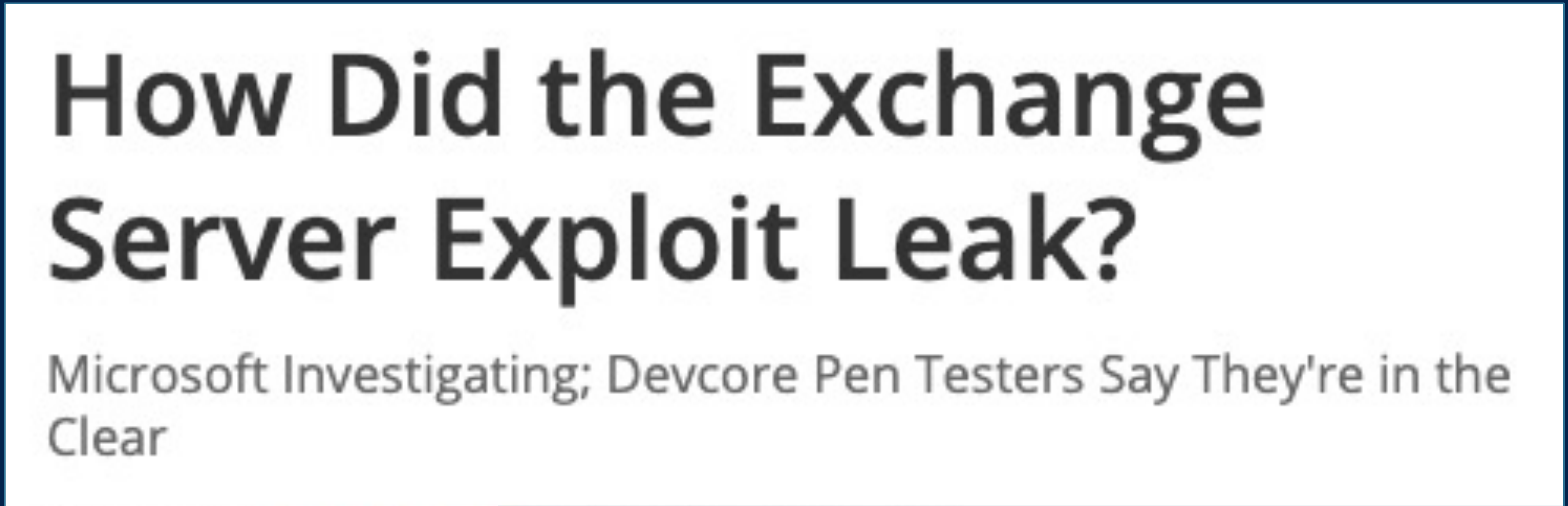
- Jan 5, 2021: DEVCORE alerts Microsoft of a newly identified RCE exploit
- Jan 8, 2021: Microsoft confirms the findings
- Jan 27, 2021: Security firm Dubex reports active exploitation of Exchange in the wild
- Feb 23, 2021: Micro code with MAPP partners
- Feb 26, 2021: Attacks explode into full mass scanning and exploitation

Shared w key partners

Too late!

- Mar 2, 2021: Microsoft releases patches for 4 discovered vulnerabilities
- Mar 3, 2021: Tens of thousands Exchange servers are compromised prior to being patched
- Mar 5, 2021: Brian Krebs reports o mass exploitation of Exchange serve
- Mar 6, 2021: CISA issues an emergency advisory about the exploit

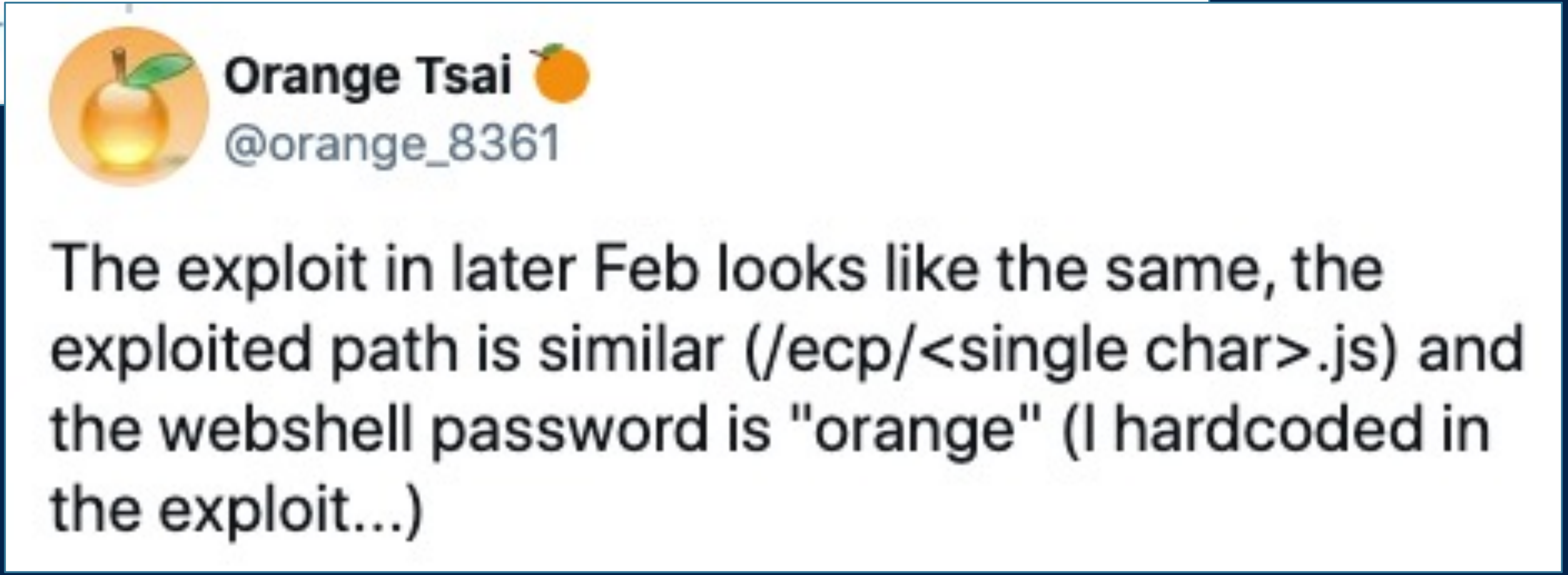
Really really too late!



How Did the Exchange Server Exploit Leak?

Microsoft Investigating; Devcore Pen Testers Say They're in the Clear

Jeremy Kirk (jeremy_kir



Orange Tsai 🍊

@orange_8361

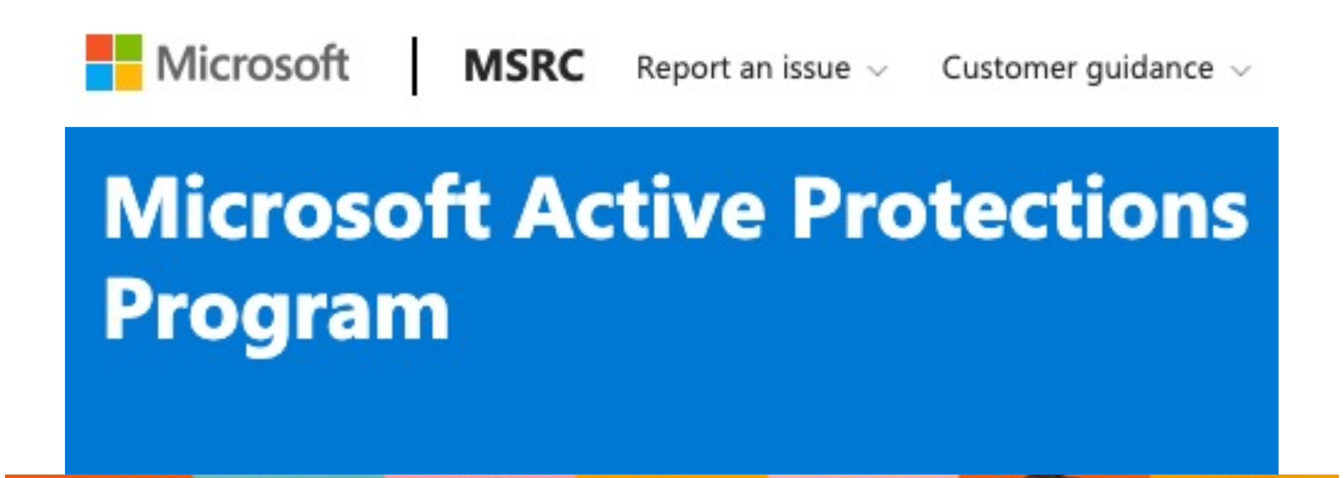
The exploit in later Feb looks like the same, the exploited path is similar (/ecp/<single char>.js) and the webshell password is "orange" (I hardcoded in the exploit...)

Three Can Keep a Secret

- But Can Eighty-Two?

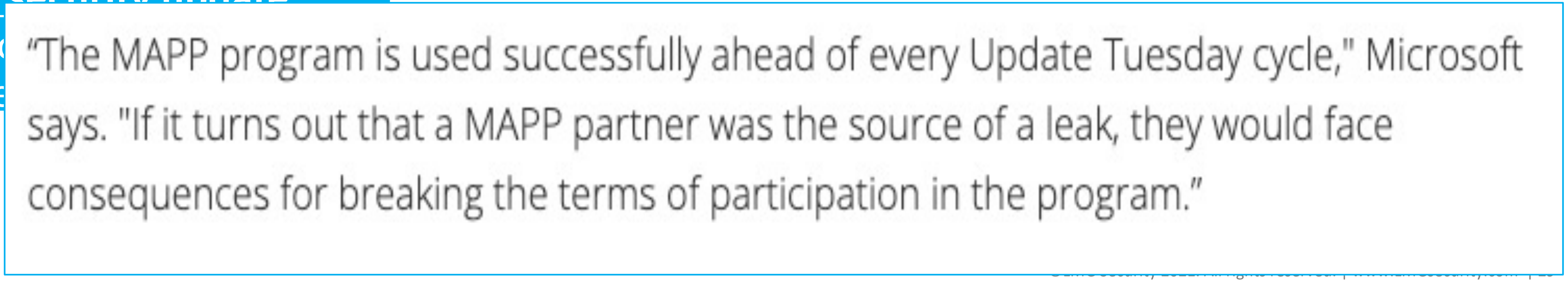
“The **Microsoft Active Protections Program (MAPP)** is a program for security software providers that gives them early access to vulnerability information so that they can provide updated protections to customers faster.

“Members of MAPP receive security vulnerability information from the **Microsoft Security Response Center** in advance of Microsoft’s **monthly security update** They can use this info quickly provide prote



Microsoft | MSRC Report an issue Customer guidance

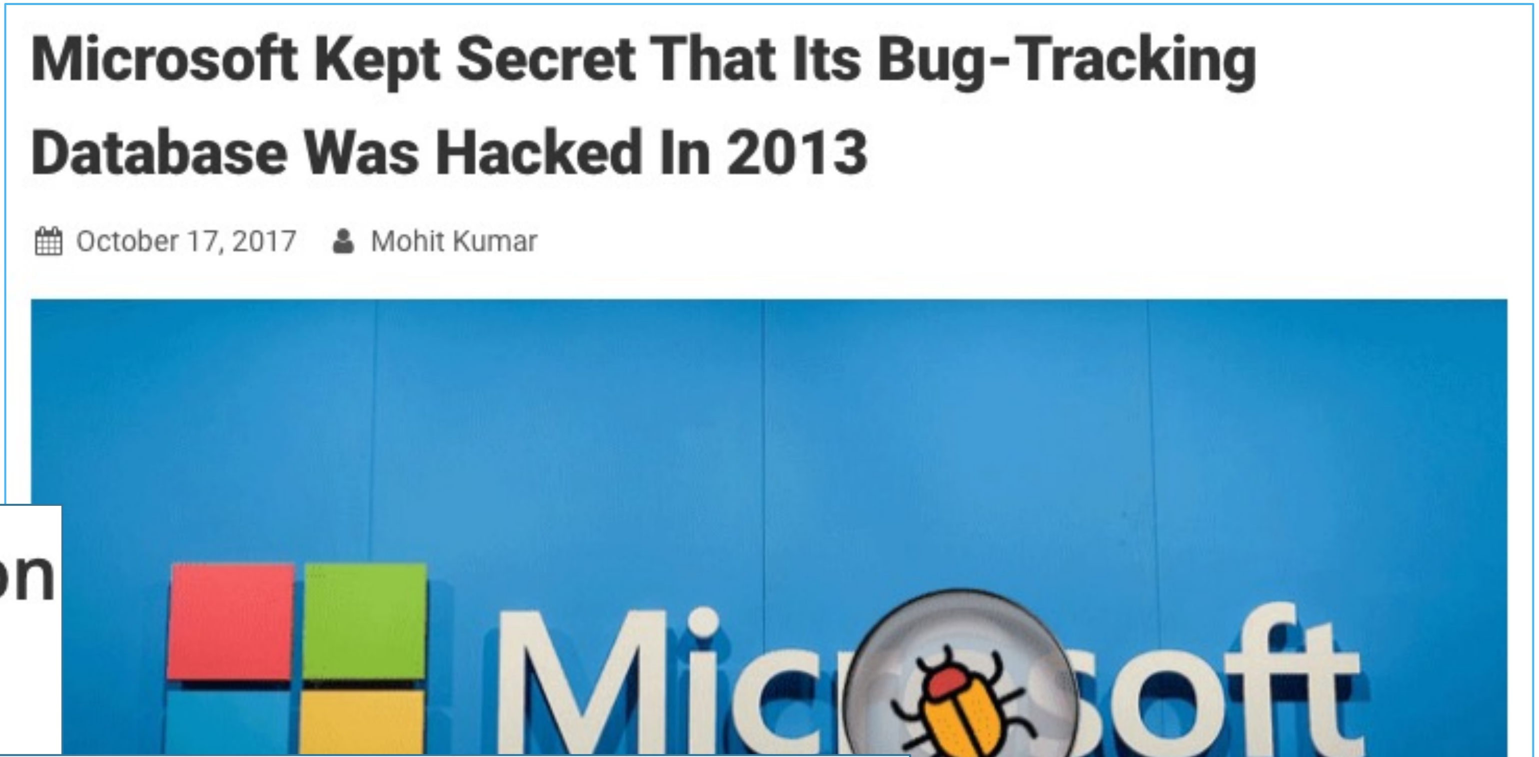
Microsoft Active Protections Program



“The MAPP program is used successfully ahead of every Update Tuesday cycle," Microsoft says. "If it turns out that a MAPP partner was the source of a leak, they would face consequences for breaking the terms of participation in the program.”

Hackers Target Source Code & Bug Info

- Break into bug tracking DBs
- Analyze stolen source code
- Tech firms & researchers
- No notification laws
- Few contractual obligations



Microsoft Kept Secret That Its Bug-Tracking Database Was Hacked In 2013

October 17, 2017 Mohit Kumar

Microsoft Offers Details on Hack of Vulnerability Researchers

North Korean APT Group Appa

Akshaya Asokan (asokan_akshaya) · Ja

Source code management a weak spot in Aurora attacks

By Robert McMillan

IDG News Service | MAR 4, 2010 4:56 AM PST

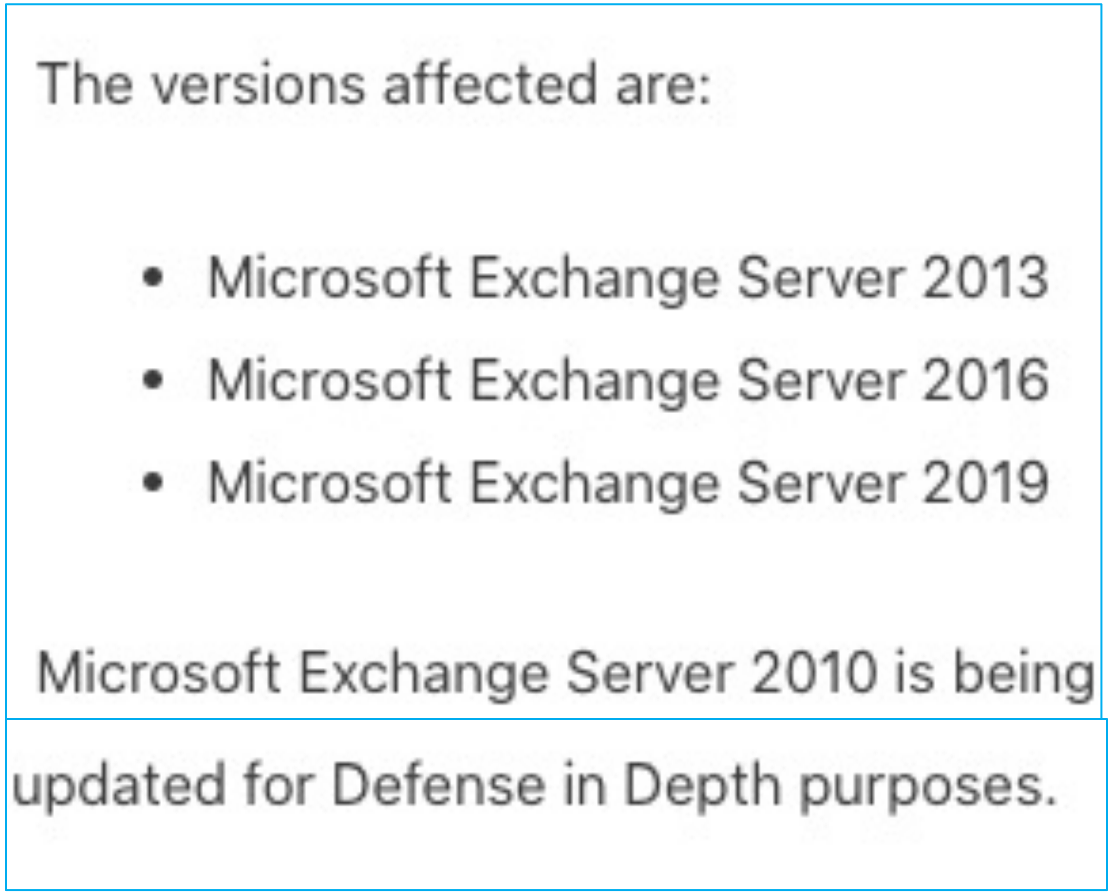
Mozilla: data stolen from hacked bug database was used to attack Firefox

A privileged user's account was compromised at least as early as September 2014.

MEGAN GEUSS - 9/4/2015, 5:04 PM

Running On-Prem Exchange? You’re Affected

- **ANY** public facing Exchange server is potentially compromised
- All email data and user data is at risk
- The vulnerable code had been in place for over 10 years
  - That’s 2011, kids



The versions affected are:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

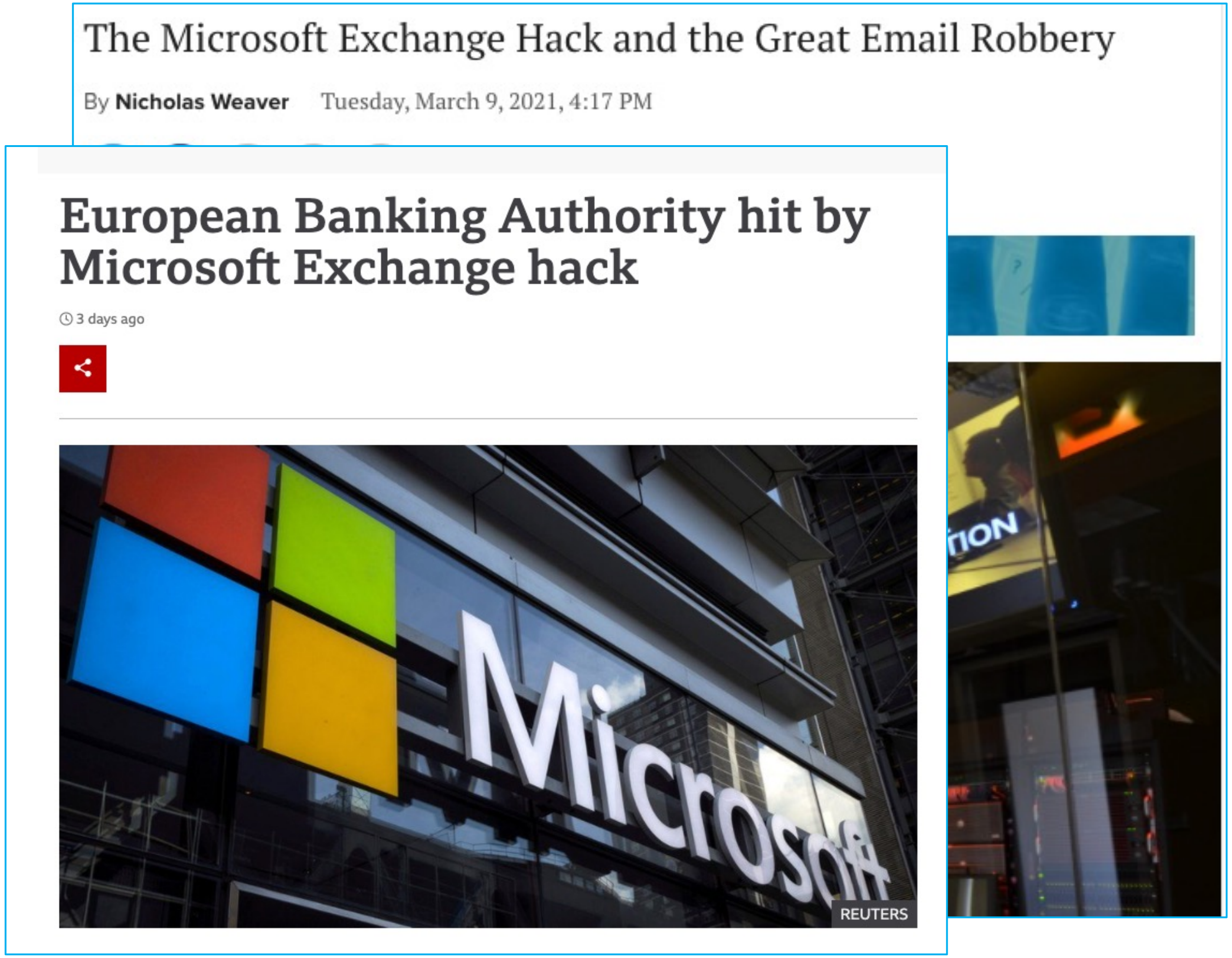
Microsoft Exchange Server 2010 is being updated for Defense in Depth purposes.

Mass-Seeding Event

- Scanning and seeding appear automated
- Any vulnerable organization may already have malicious web shells installed
- Scanning and attacks are ongoing
- Very aggressive adversaries

Forensic Preservation

- Forensically image all ~~Solarwinds~~ Exchange servers
- Obtain volatile memory
- Preserve network/IIS logs
- Very important because of BEC/data breach concerns
- Check for unauthorized access
- Determine risk of email access/acquisition



The Microsoft Exchange Hack and the Great Email Robbery

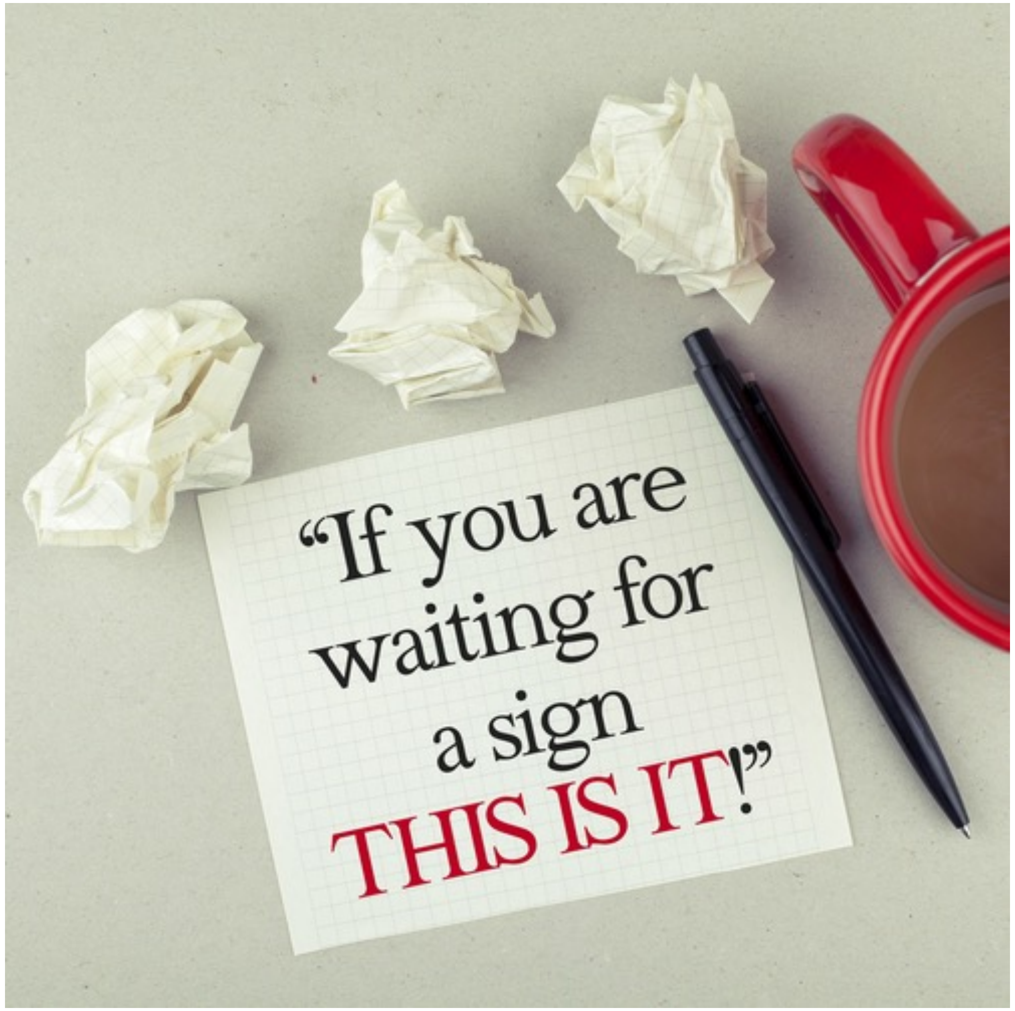
By **Nicholas Weaver** Tuesday, March 9, 2021, 4:17 PM

European Banking Authority hit by Microsoft Exchange hack

3 days ago

Contain the Damage

- Act yesterday!
  - Or at least today
- CISA & Microsoft guidance for "ProxyLogon" remediation
- Standard options:
  - Yank the network/power
  - Domain-wide password reset
    - Attacker use of procdump to capture pwds
- Impacts:
  - Operational impacts
  - Help desk calls
  - Email is down
  - Evidence might be destroyed

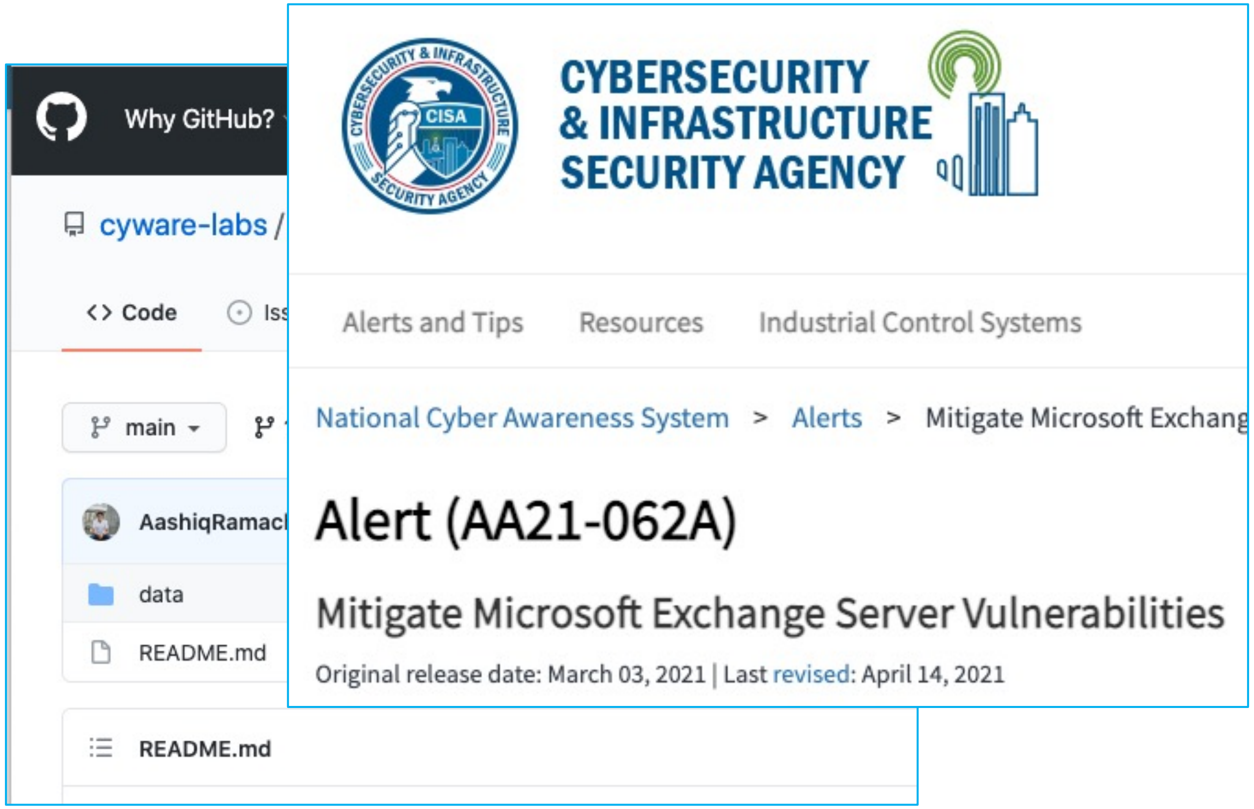


☑ Hunt for Threats

- Microsoft & CISA published IoCs right away
- Example: Financial services firm
- We used Carbon Black for overall network
- Targeted analysis of IIS logs
  - Exchange-specific activities
- Known Hafnium behavior
  - Identified hundreds of attempts to exploit the vuln on the server
  - Some were successful, others not

Indictors of Compromise

- Eight-character .aspx files in c:\inetpub\wwwroot\aspnet_client\system_web\
- Web shells present on the server
- Encoded PowerShell activity
- Challenges:
  - Lots of false positives
  - Too many IoCs!

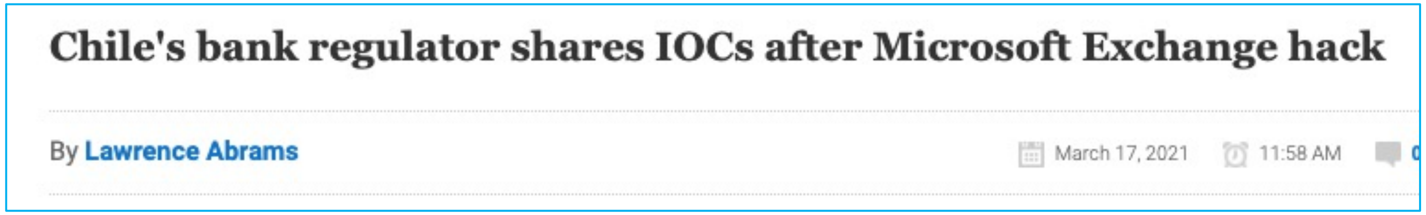


National Cyber Awareness System > Alerts > Mitigate Microsoft Exchang

Alert (AA21-062A)

Mitigate Microsoft Exchange Server Vulnerabilities

Original release date: March 03, 2021 | Last revised: April 14, 2021

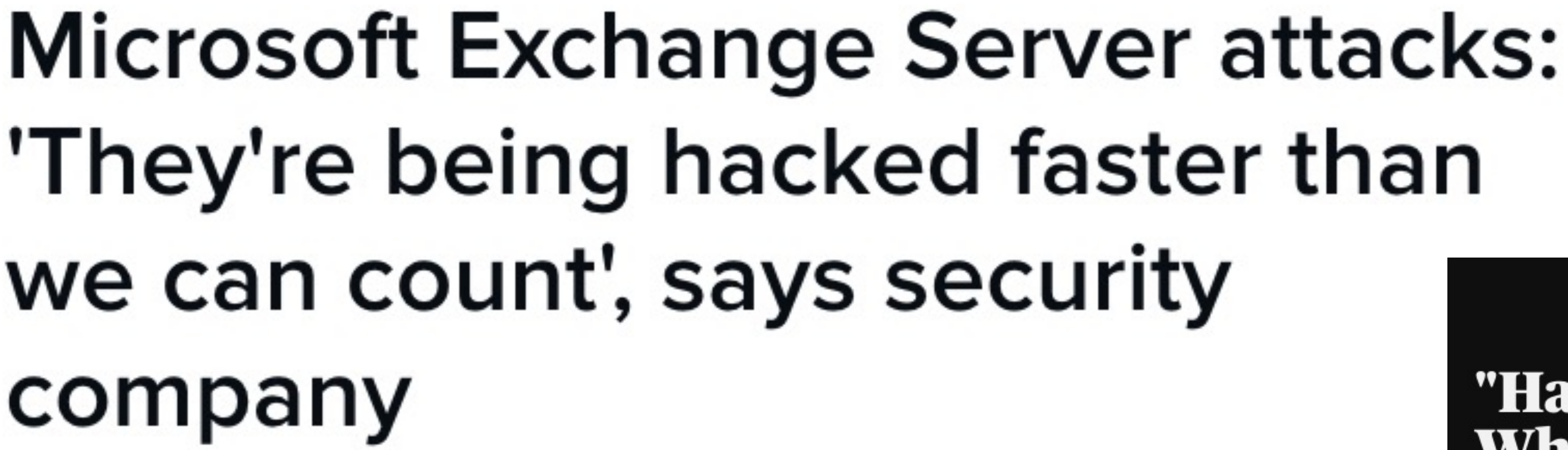


Chile's bank regulator shares IOCs after Microsoft Exchange hack

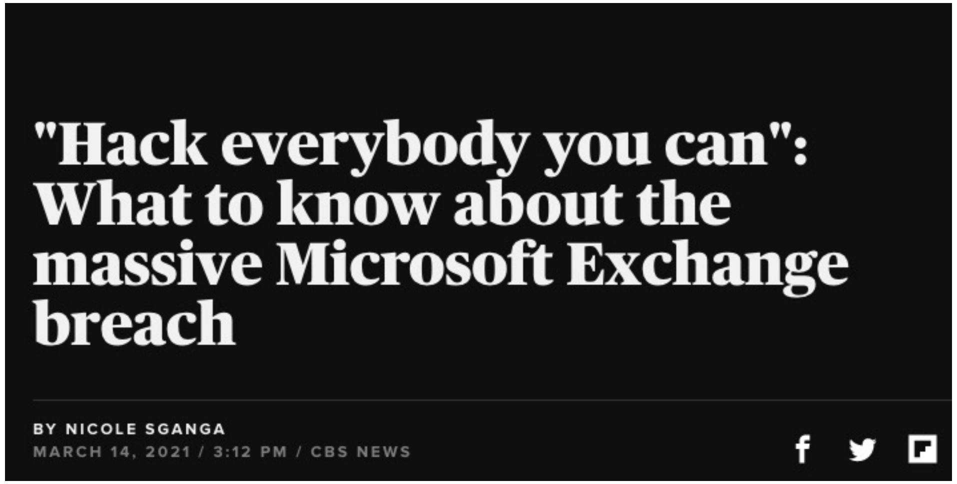
By Lawrence Abrams

March 17, 2021 11:58 AM

The IoCs Keep Changing!



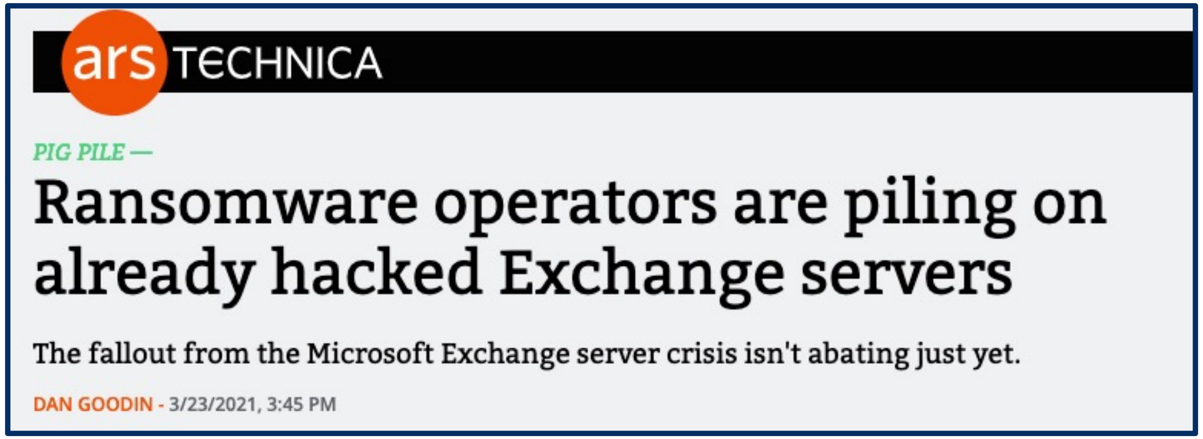
Microsoft Exchange Server attacks: 'They're being hacked faster than we can count', says security company



"Hack everybody you can": What to know about the massive Microsoft Exchange breach

BY NICOLE SGANGA

MARCH 14, 2021 / 3:12 PM / CBS NEWS



ars TECHNICA

PIG PILE —

Ransomware operators are piling on already hacked Exchange servers

The fallout from the Microsoft Exchange server crisis isn't abating just yet.

DAN GOODIN - 3/23/2021, 3:45 PM

Network Recon Using Encoded Powershell

- Encoded string example:
- GET /aspnet_client/supp0rt.aspx 552623bfb61e74baaaf03ef4506c7fcf=dmFyIHA9U3lzdGVtLkRpYWdub3N0aWNzLlByb2Nlc3MuR2V0UHJvY...

- Translates to:

```
var p=System.Diagnostics.Process.GetProcesses();

var str="";for(vari=0;i<p.Length;i++)
{str+=p[i].ProcessName+":"+p[i].Id+"\r\n";} \
str=Convert.ToBase64String(System.Text.Encoding.UTF8.
GetBytes(str));

str="oamoisjmdo"+str+"sodknousfnfdklj";

Response.Write(str);
```

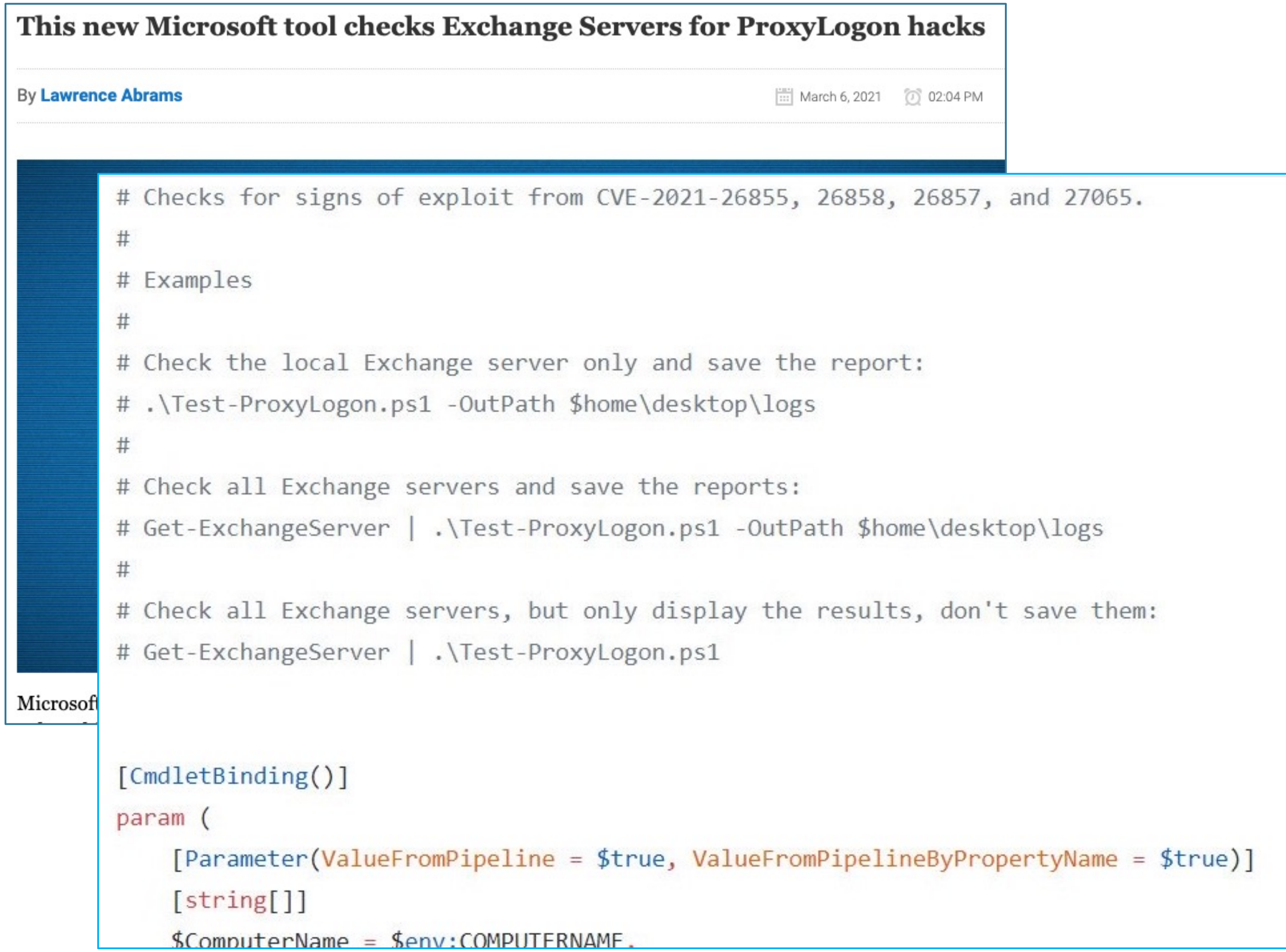
Detecting Post-Exploit Behavior – Legit Toolkits

- Collection - 7zip Archiving Outlook Data Files Detected
- Persistence - Potential Web Shell Behavior Detected
- Defense Evasion - Unusual Location of OWAAUTH.dll
- Execution - Psexec Detected
- Defense Evasion - Renamed Psexec Process Detected
- Masquerading WinRar - Renamed Process
- Credential Access - Credential Dumping via Sysinternals Procdump Detected
- Credential Access - Credential Theft Detected via API Execution

https://community.carbonblack.com/t5/Threat-Research-Docs/Microsoft-Exchange-0-Days-CVE-2021-26855-CVE-2021-26857-CVE-2021/ta-p/101318

Microsoft Detection & Remediation Scripts

- Microsoft had time to prepare
  - Unlike SolarWinds
- March 6 release
- Test-ProxyLogon
  - Checks for vuln & known IoCs
- Exchange On-Premise Mitigation Tool (EOMT)
- Automates remediation
- But!
- Can destroy evidence



This new Microsoft tool checks Exchange Servers for ProxyLogon hacks

By Lawrence Abrams   March 6, 2021   02:04 PM

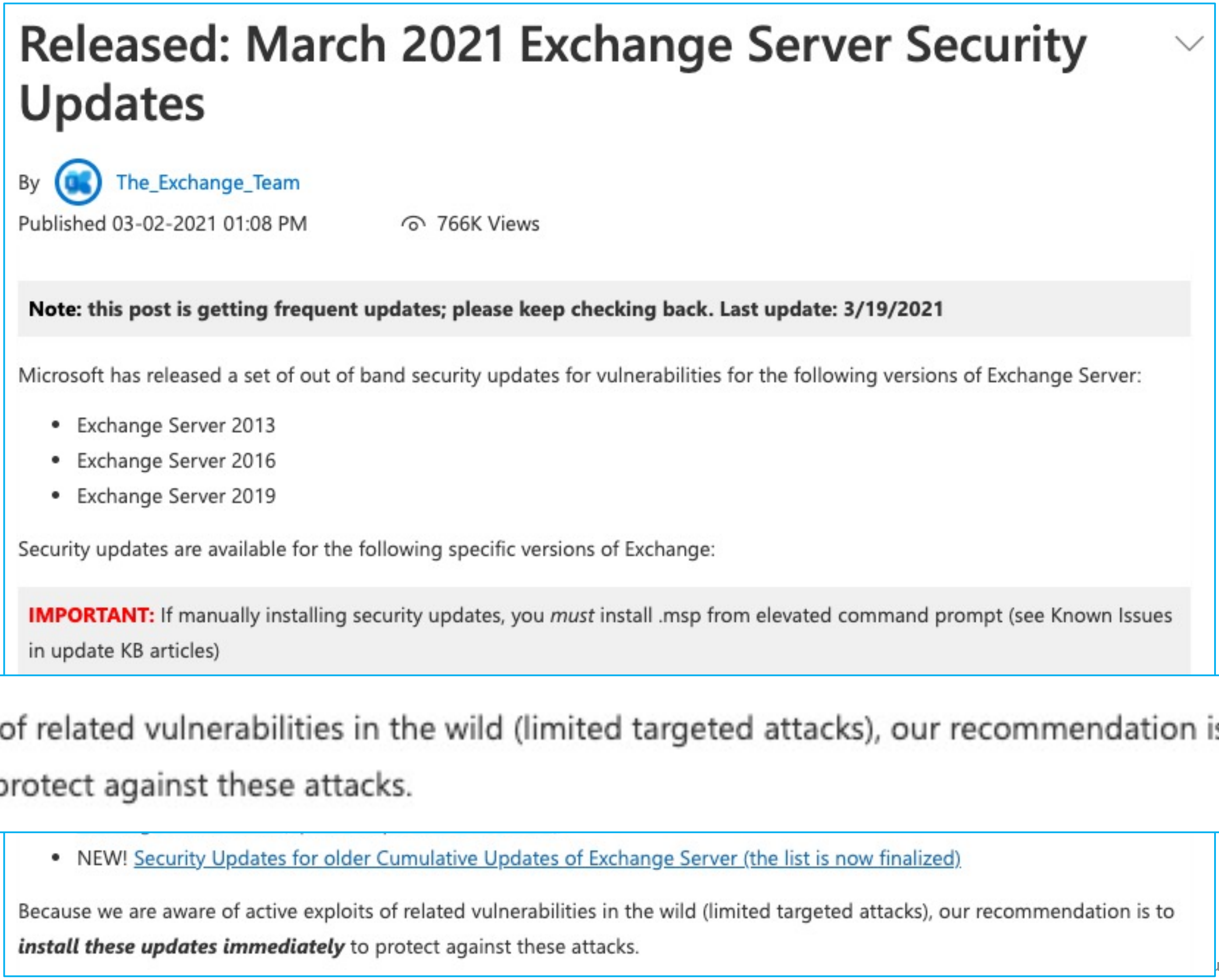
Microsoft

```
# Checks for signs of exploit from CVE-2021-26855, 26858, 26857, and 27065.
#
# Examples
#
# Check the local Exchange server only and save the report:
# .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
#
# Check all Exchange servers and save the reports:
# Get-ExchangeServer | .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
#
# Check all Exchange servers, but only display the results, don't save them:
# Get-ExchangeServer | .\Test-ProxyLogon.ps1


[CmdletBinding()]
param (
    [Parameter(ValueFromPipeline = $true, ValueFromPipelineByPropertyName = $true)]
    [string[]]
    $ComputerName = $env:COMPUTERNAME,
```

Apply Emergency Patches/Updates

- Ready on March 2 (day of public announcement)
- Not everybody was ready to patch
- If you didn’t, you were likely hacked
  - Quite possibly already hacked, anyway



Released: March 2021 Exchange Server Security Updates

By The_Exchange_Team

Published 03-02-2021 01:08 PM   766K Views

Note: this post is getting frequent updates; please keep checking back. Last update: 3/19/2021

Microsoft has released a set of out of band security updates for vulnerabilities for the following versions of Exchange Server:

- Exchange Server 2013
- Exchange Server 2016
- Exchange Server 2019

Security updates are available for the following specific versions of Exchange:

IMPORTANT: If manually installing security updates, you *must* install .msp from elevated command prompt (see Known Issues in update KB articles)

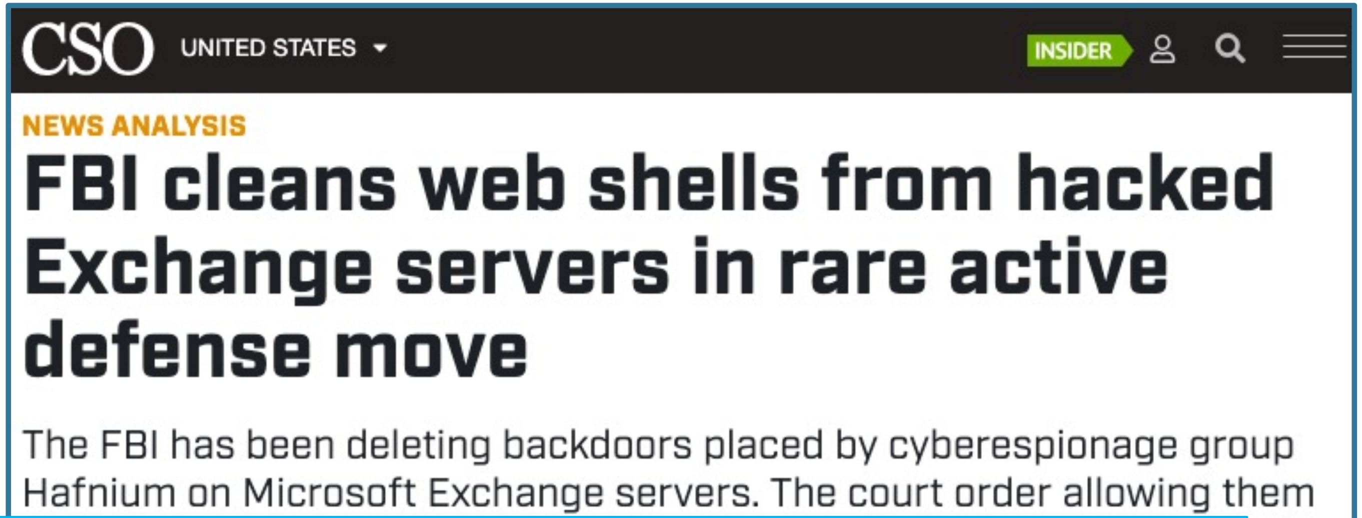
- NEW! Security Updates for older Cumulative Updates of Exchange Server (the list is now finalized)

Because we are aware of active exploits of related vulnerabilities in the wild (limited targeted attacks), our recommendation is to ***install these updates immediately*** to protect against these attacks.

Because we are aware of active exploits of related vulnerabilities in the wild (limited targeted attacks), our recommendation is to ***install these updates immediately*** to protect against these attacks.

Law Enforcement Intervention

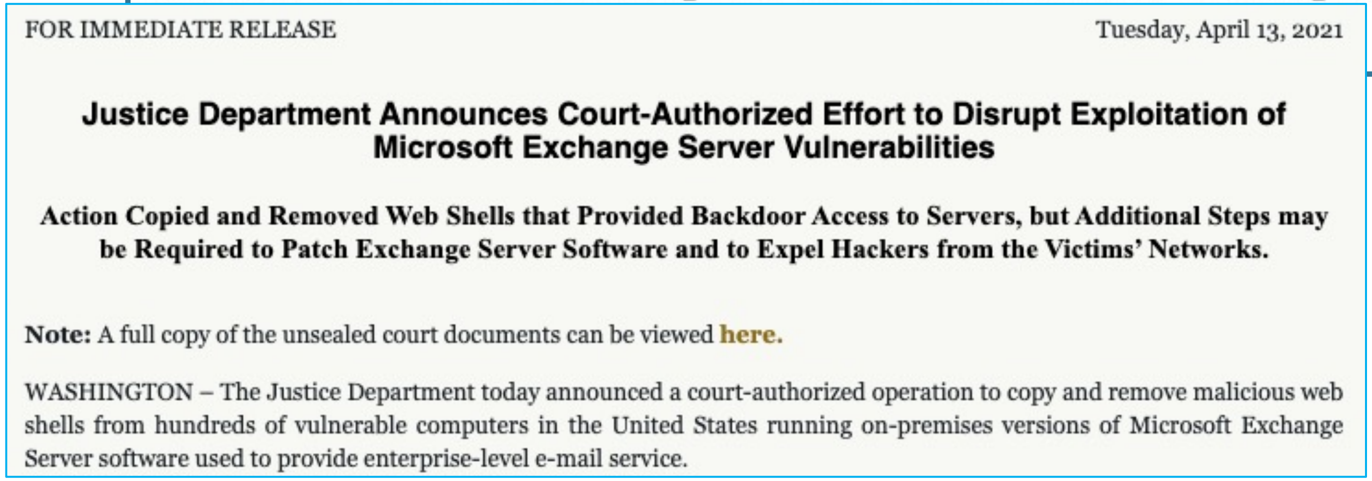
- FBI court-authorized to hack in and remove web shells
- "Attempting to provide notice"
- Pros and Cons
- Reduce risk of hackers/ransomware
- Can destroy evidence
- Confuse investigators
- Potential operational impacts
- Will it happen again?



NEWS ANALYSIS

FBI cleans web shells from hacked Exchange servers in rare active defense move

The FBI has been deleting backdoors placed by cyberespionage group Hafnium on Microsoft Exchange servers. The court order allowing them



FOR IMMEDIATE RELEASE

Tuesday, April 13, 2021

Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities

Action Copied and Removed Web Shells that Provided Backdoor Access to Servers, but Additional Steps may be Required to Patch Exchange Server Software and to Expel Hackers from the Victims' Networks.

Note: A full copy of the unsealed court documents can be viewed **here.**

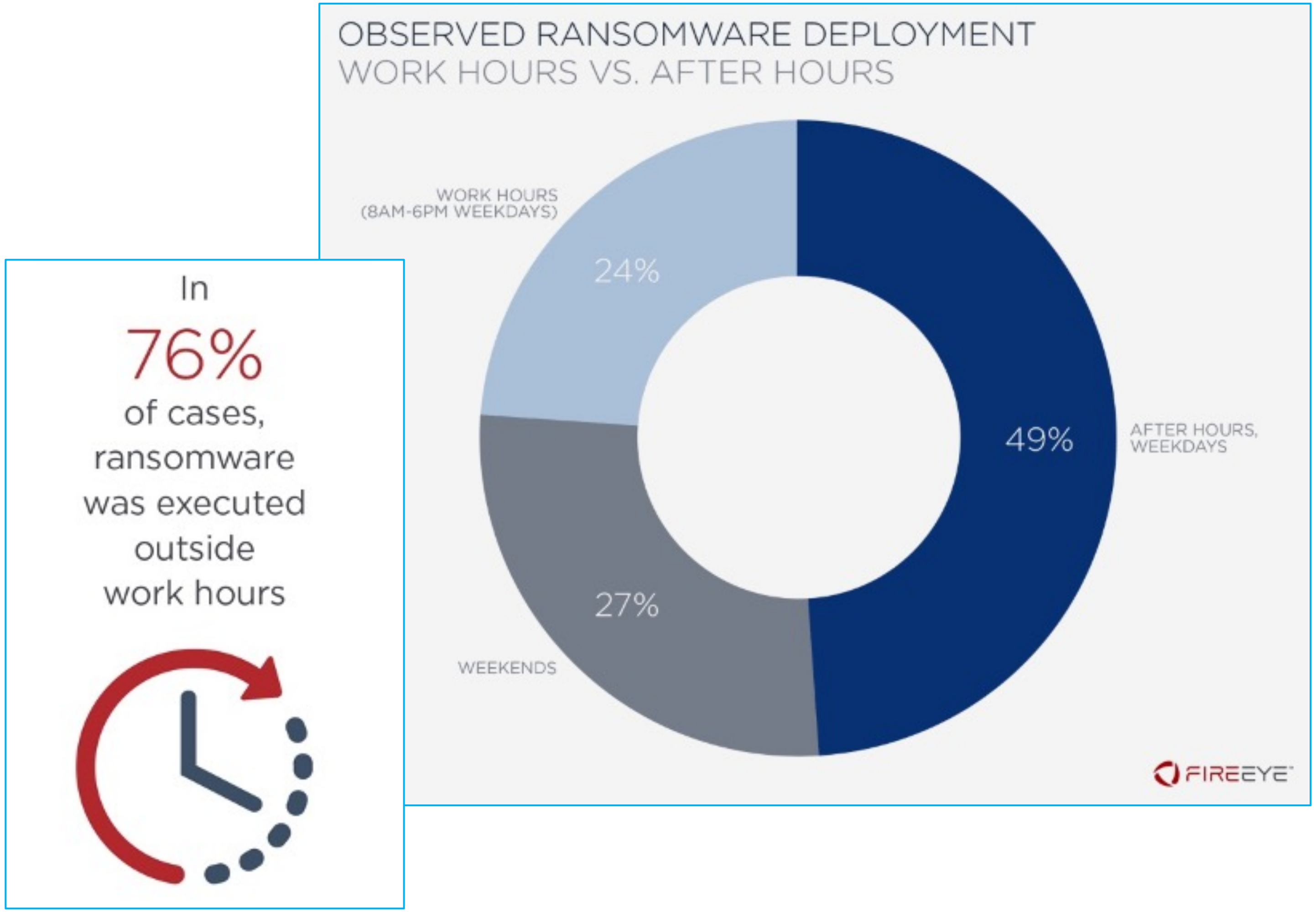
WASHINGTON – The Justice Department today announced a court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level e-mail service.

Plan for Elevated Risks

- Email theft can be very impactful
- Financial fraud
- Targeted follow-on attacks
- Stolen credentials
- Pivoting into network undetected
- Additional malware

Back to the Recent Kaseya Ransomware Attacks…

- Fourth of July weekend
  - Coincidence? Unlikely
  - “Forensics Friday” @LMG
- Locked up w ransomware
- Who’s on call for your organization?
- Are your MSPs monitoring threat intelligence?
- How quickly do MSPs notify their customers?

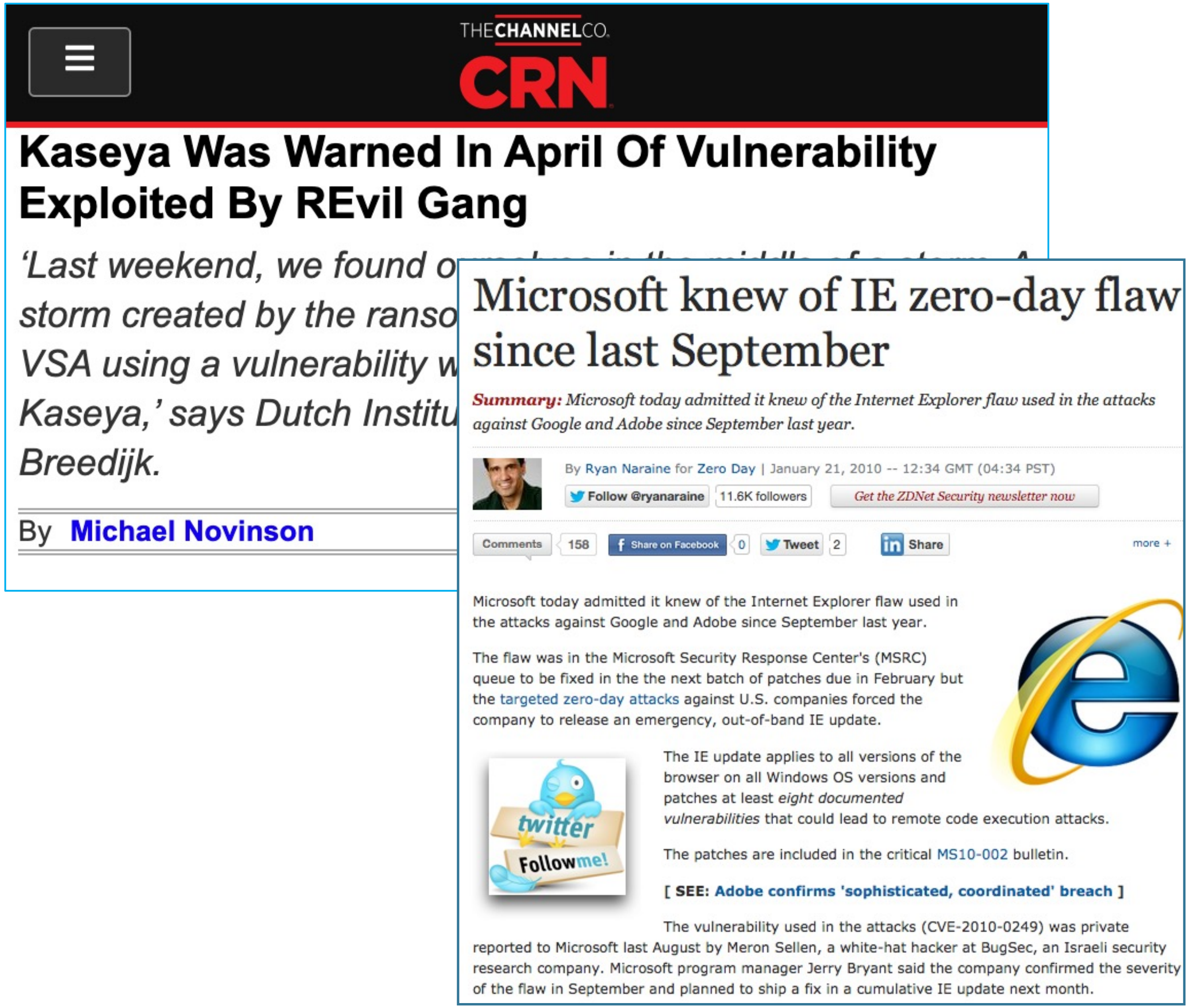


In 76% of cases, ransomware was executed outside work hours

https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

Vulnerability Timeline

- Dutch Institute for Vulnerability Disclosure (DIVD)
- Discovered at least 7 vulns
  - + 2200 vulnerable systems
- April 6 - Disclosed to Kaseya
- 90-day disclosure agreement
- April 10 & May 8 – 4 vulns patched
- Impending release of 3 vulns & patches
- Hackers strike just before release!
  - Suspicious timing
- Hack before the patch – an old problem



Kaseya Was Warned In April Of Vulnerability Exploited By REvil Gang

'Last weekend, we found o
storm created by the ranso
VSA using a vulnerability w
Kaseya,' says Dutch Institu
Breedijk.

By **Michael Novinson**

Microsoft knew of IE zero-day flaw since last September

Summary: *Microsoft today admitted it knew of the Internet Explorer flaw used in the attacks against Google and Adobe since September last year.*

By Ryan Naraine for Zero Day | January 21, 2010 -- 12:34 GMT (04:34 PST)

Microsoft today admitted it knew of the Internet Explorer flaw used in the attacks against Google and Adobe since September last year.

The flaw was in the Microsoft Security Response Center's (MSRC) queue to be fixed in the the next batch of patches due in February but the targeted zero-day attacks against U.S. companies forced the company to release an emergency, out-of-band IE update.

The IE update applies to all versions of the browser on all Windows OS versions and patches at least *eight documented vulnerabilities* that could lead to remote code execution attacks.

The patches are included in the critical MS10-002 bulletin.

[SEE: Adobe confirms 'sophisticated, coordinated' breach]

The vulnerability used in the attacks (CVE-2010-0249) was private reported to Microsoft last August by Meron Sellen, a white-hat hacker at BugSec, an Israeli security research company. Microsoft program manager Jerry Bryant said the company confirmed the severity of the flaw in September and planned to ship a fix in a cumulative IE update next month.

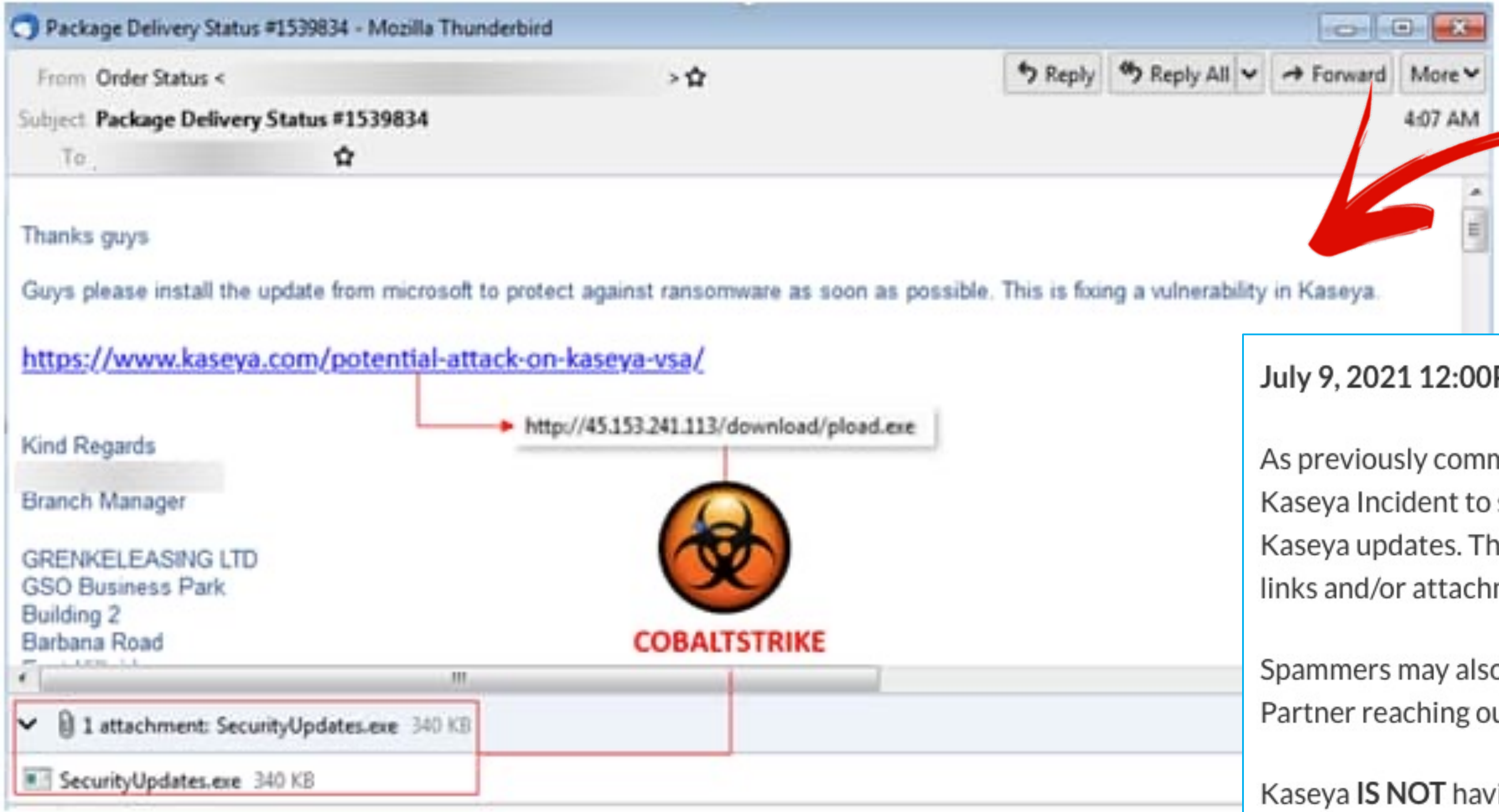
Supplier Communication Challenges

- What should you expect for communications from your suppliers?
- 2019 – MSP hit by Revil
- Over 100 dental office impacted
- REvil/Sodinokibi ransomware delivered using MSP remote management tools
- $700k demanded for a master decryptor
- MSP refused payment
- Tight-lipped & did not want to share info
- Refused to provide log data

Colorado MSP Attack Compromises Supported Dental Offices

December 10, 2019 By Emil Hozan

You Can’t Trust Just Anybody



Package Delivery Status #1539834 - Mozilla Thunderbird

From Order Status <[redacted]>

Subject Package Delivery Status #1539834 4:07 AM

To [redacted]

Thanks guys

Guys please install the update from microsoft to protect against ransomware as soon as possible. This is fixing a vulnerability in Kaseya.

https://www.kaseya.com/potential-attack-on-kaseya-vsa/

http://45.153.241.113/download/pload.exe

Kind Regards
[redacted]
Branch Manager

GRENKELEASING LTD
GSO Business Park
Building 2
Barbana Road

1 attachment: SecurityUpdates.exe 340 KB

SecurityUpdates.exe 340 KB

July 9, 2021 12:00PM EDT

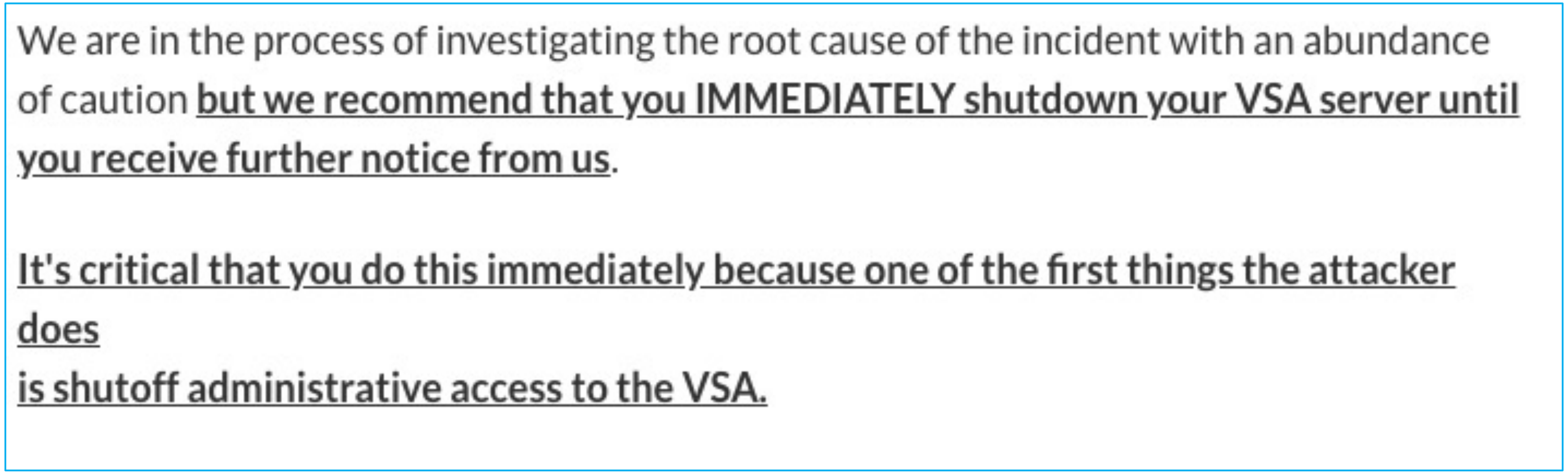
As previously communicated, spammers are using the news about the Kaseya Incident to send out fake email notifications that appear to be Kaseya updates. These are phishing emails that may contain malicious links and/or attachments.

Spammers may also be making phone calls claiming to be a Kaseya Partner reaching out to help.

Kaseya **IS NOT** having any partners reach out – **DO NOT** respond to any phone calls claiming to be a Kaseya Partner.

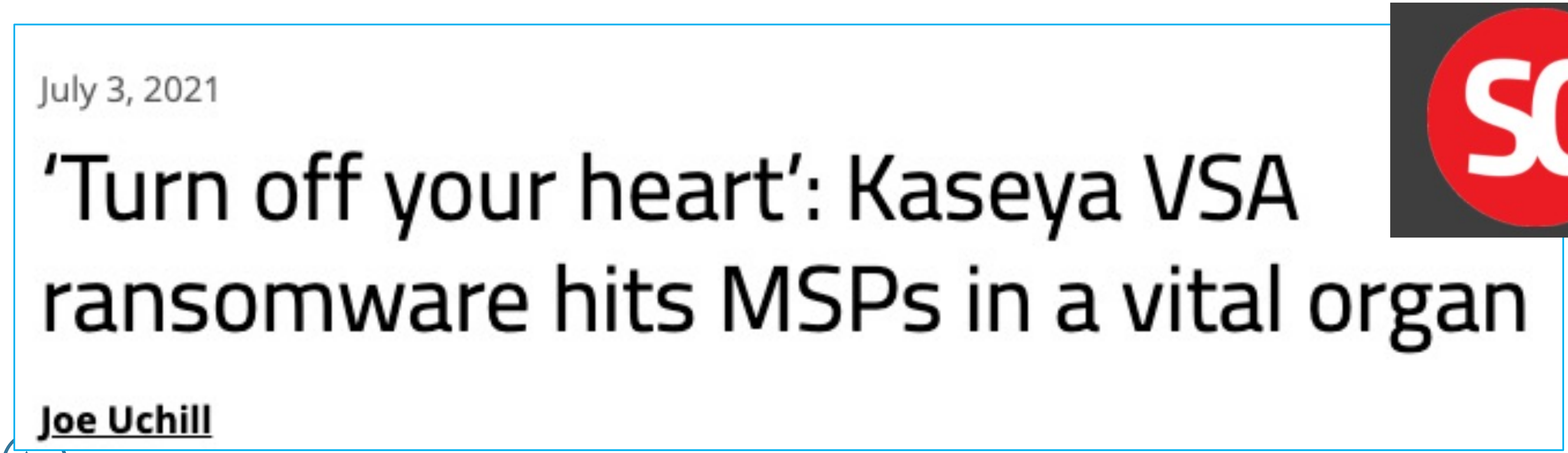
DO NOT click on any links or download any attachments in emails claiming to be a Kaseya advisory.

Containment



We are in the process of investigating the root cause of the incident with an abundance of caution but we recommend that you IMMEDIATELY shutdown your VSA server until you receive further notice from us.

It's critical that you do this immediately because one of the first things the attacker does
is shutoff administrative access to the VSA.



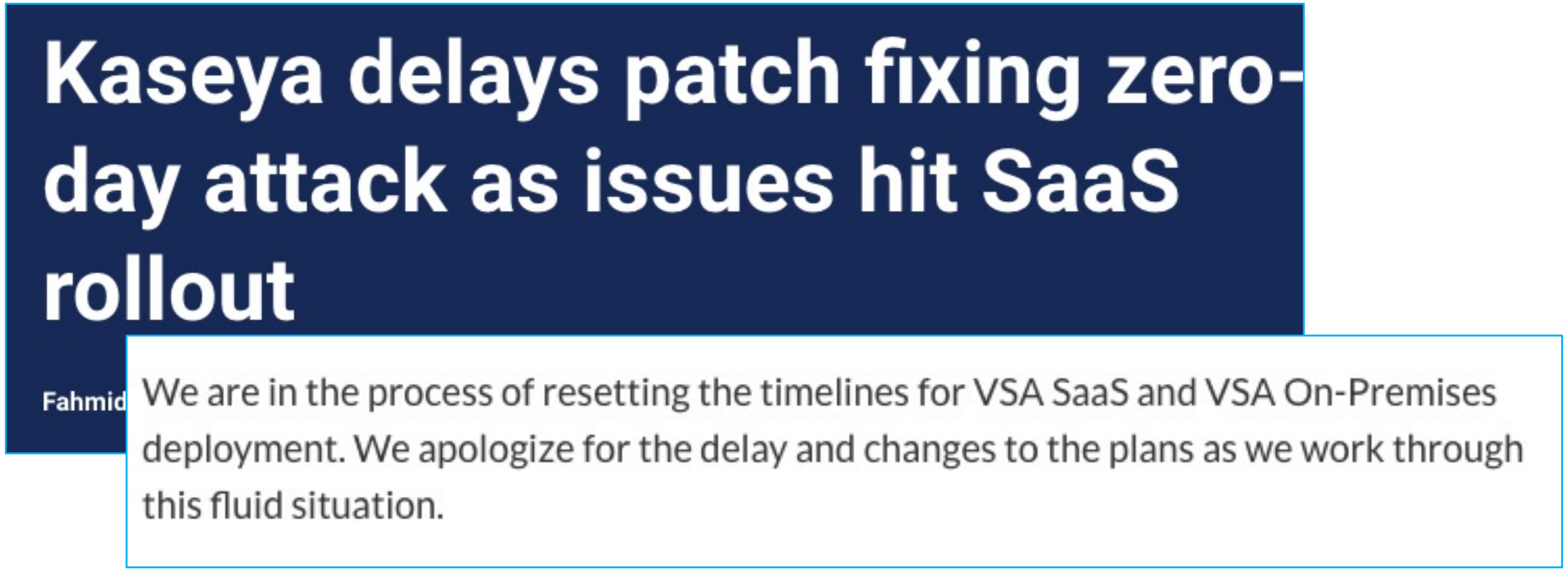
July 3, 2021

‘Turn off your heart’: Kaseya VSA ransomware hits MSPs in a vital organ

Joe Uchill

Patch Problems

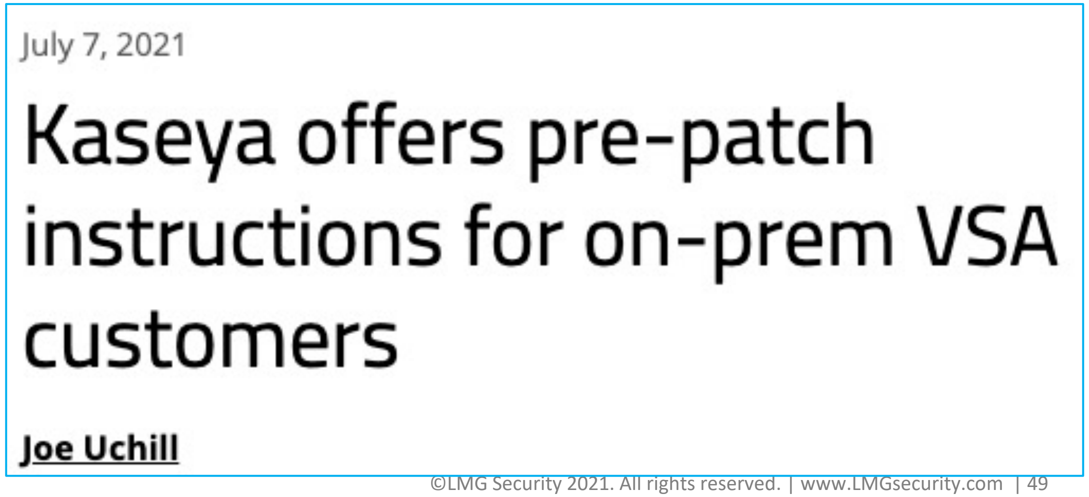
- Apply emergency patches/updates
- Patches SO not ready in time
- If they were, would you deploy them?
- What is your MSP’s policy?
- Risks either way
- What do you do when patches aren’t ready, or YOU aren’t ready?
- What if there’s another vuln?



Kaseya delays patch fixing zero-day attack as issues hit SaaS rollout

Fahmid

We are in the process of resetting the timelines for VSA SaaS and VSA On-Premises deployment. We apologize for the delay and changes to the plans as we work through this fluid situation.



July 7, 2021

Kaseya offers pre-patch instructions for on-prem VSA customers

Joe Uchill

This Will Happen Again

- Hackers want the most ROI
- Target widely-used software
- Leverage technology service providers
- Breaches lead to more breaches

Adapt Your DFIR Processes!

1. Monitor Threat Intelligence
2. Evaluate your risk
3. Conduct forensic preservation
4. Contain the damage
5. Hunt for Threats
6. Apply emergency patches/updates
7. Plan for elevated risks

Questions?

- Sherri Davidoff & Matt Durrin
- info@LMGsecurity.com
- @LMGSecurity
- Find us on LinkedIn

LMG SECURITY

Ransomware and Cyber Extortion

New Book!

Sherri DAVIDOFF
Matt DURRIN
Karen SPRENGER

BREAKING BREACHES