



# Sun Stroke

Kim Zetter

How SolarWinds hackers pulled off their attack - and scorched the underbelly of the software supply chain

## ***FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State***

The Silicon Valley company said hackers — almost certainly Russian — made off with tools that could be used to mount new attacks around the world.

Share full article



FireEye's clients after huge breaches have included Sony and Equifax. Hackers targeted its "Red Team" tools. David Becker/Reuters

# December 8, 2020

- Stole red-team tools
- Accessed info about gov customers
- Doesn't mention how long attackers were in network



“[W]e are witnessing an attack by a nation with top-tier offensive capabilities. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They used a novel combination of techniques not witnessed by us or our partners in the past [25 years].”

- Kevin Mandia, founder/CEO of  
FireEye's Mandiant division

Dec. 13, 2020

**MANDIANT**  
NOW PART OF Google Cloud

Platform Solutions Intelligence Services Resources

THREAT RESEARCH

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

FIREEYE

DEC 13, 2020 | 17 MIN READ | LAST UPDATED: AUG 09, 2023

No Mention that FireEye Was a Victim



# Dark Halo

## US Think Tank



Steven Adair

### Late 2019

- Stole email of executives/policy experts/IT staff
- 3 x a week
- Evicted but returned through 2016 backdoor

### March/April 2020

- Returned via unpatched RCE vuln in Exchange Control Panel
- Bypassed Duo 2FA to steal email - obtained secret key from registry to create token

### June/July 2020

- Returned again
- Breach in June; no activity until July



SolarWinds Orion server



(Image credit: manpuku7 via Getty Images)

## Orion Platform Products



**NETWORK PERFORMANCE MONITOR**



**NETFLOW TRAFFIC ANALYZER**



**NETWORK CONFIGURATION MANAGER**



**IP ADDRESS MANAGER**



**VOIP & NETWORK QUALITY MANAGER**



**USER DEVICE TRACKER**



**SERVER & APPLICATION MONITOR**



**SERVER CONFIGURATION MONITOR**



**STORAGE RESOURCE MONITOR**



**VIRTUALIZATION MANAGER**



**WEB PERFORMANCE MONITOR**



**LOG ANALYZER**

# Justice Department - Late May 2020







SolarWinds Orion server





- Microsoft - Mandiant - SolarWinds
- Vulnerability in Orion code?
- Vulnerability in DoJ server?



ツツ

Nov. 10, 2020



Samsung device had  
no phone #



Accessed VPN from  
wrong state



Simultaneous access



Access without  
username/password



**Henna Parviz**  
Senior Threat Intel  
Analyst Mandiant

**We traced the call.  
It's coming from  
inside the house.**





Nov. 17, 2020



- Living off the land
- Avoided known patterns
- Hijacked scheduled tasks for their own tasks
- Replaced legit tools with their own
- Stole FireEye/Mandiant red team tools
- Stole data about US gov customers

Nov. 20, 2020





“Every time you pulled on a thread, there was a bigger piece of yarn.”  
— Christopher Glycer





“Every time you pulled on a thread, there was a bigger piece of yarn.”  
— Christopher Glycer







SolarWinds Orion server





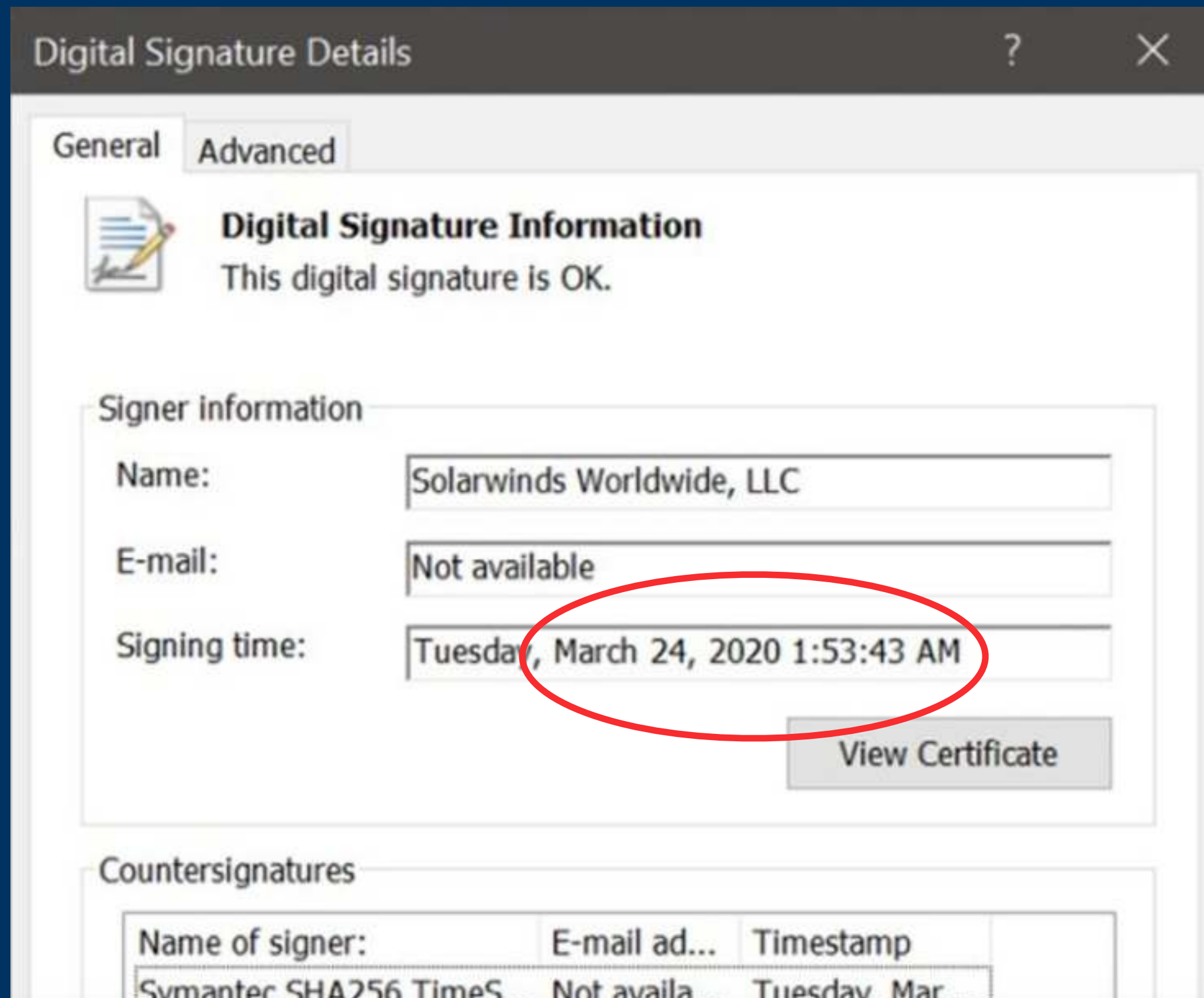
## Orion Platform

- 50,000 lines of code
- 18,000 files; 14 gigabytes of code/data



## Sunburst

- .dll file w/ 4,000 functions
- .dll sends customer usage telemetry to SolarWinds
- Not sending to SolarWinds

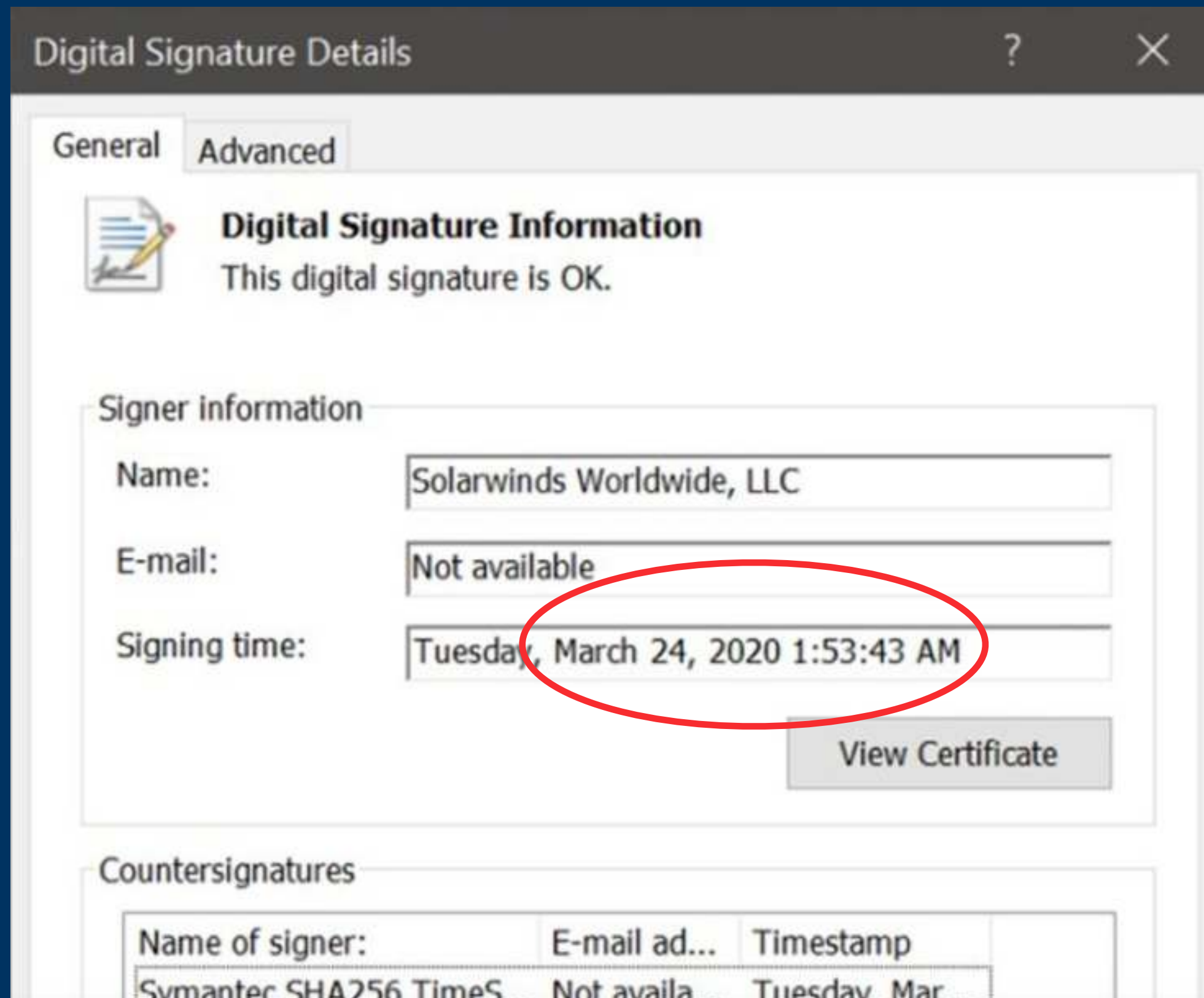


## How Did Sunburst Get Onto Mandiant Server?

Did they steal the certificate to sign their code?

or

Did they embed backdoor in Orion code and sign it on SolarWinds server?



Did they steal the certificate to sign their code?

or

~~Did they embed backdoor in Orion code and sign it on SolarWinds server?~~



33,000 Orion customers

### 5 product updates are available

The following updates are available for your Orion product(s).

| PRODUCT  | NEW VERSION AVAILABLE |
|--|-----------------------|
| <b>NetFlow Traffic Analyzer</b><br><a href="#">RELEASE NOTES »</a>         | <b>4.2.1.0</b>        |
| <b>Database Performance Analyzer</b><br><a href="#">RELEASE NOTES »</a>    | <b>10.2.0.0</b>       |
| <b>Storage Resource Monitor</b><br><a href="#">RELEASE NOTES »</a>         | <b>6.3.0.0</b>        |
| <b>Server &amp; Application Monitor</b><br><a href="#">RELEASE NOTES »</a> | <b>6.3.0.0</b>        |
| <b>Network Performance Monitor</b><br><a href="#">RELEASE NOTES »</a>      | <b>12.0.1.0</b>       |

[PLAN YOUR UPGRADE](#)

[Don't remind me again](#)





# 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                   |
| Cisco                        | Leggett and Platt         | Swisscom AG                 |
| CitiFinancial                | Level 3 Communications    | Symantec                    |
| City of Nashville            | Liz Claiborne             | Telecom Italia              |
| City of Tampa                | Lockheed Martin           | Telenor                     |
| Clemson University           | Lucent                    | Texaco                      |
| Comcast Cable                | MasterCard                | The CDC                     |
| Credit Suisse                | McDonald's Restaurants    | The Economist               |
| Dow Chemical                 | Microsoft                 | Time Warner Cable           |
| EMC Corporation              | National Park Service     | U.S. Air Force              |
| Ericsson                     | NCR                       | University of Alaska        |
| Ernst and Young              | NEC                       | University of Kansas        |
| Faurecia                     | Nestle                    | University of Oklahoma      |
| Federal Express              | New York Power Authority  | US Dept. Of Defense         |
| Federal Reserve Bank         | New York Times            | US Postal Service           |
| Fibercloud                   | Nielsen Media Research    | US Secret Service           |
| Fiserv                       | Nortel                    | Visa USA                    |
| Ford Motor Company           | Perot Systems Japan       | Volvo                       |
| Foundstone                   | Phillips Petroleum        | Williams Communications     |
| Gartner                      | Pricewaterhouse Coopers   | Yahoo                       |
| Gates Foundation             | Procter & Gamble          |                             |

# 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 Deuschlan       |                         |
| AT&T                         | GTE                      |                         |
| Bellsouth Telecommunications | H&R Block                |                         |
| Best Western Intl.           | Harvard University       |                         |
| Blue Cross Blue Shield       | Hertz Corporation        |                         |
| Booz Allen Hamilton          | ING Direct               |                         |
| Boston Consulting            | IntelSat                 |                         |
| Cable & Wireless             | J.D. Byrider             |                         |
| Cablecom Media AG            | Johns Hopkins Uni        |                         |
| Cablevision                  | Kennedy Space Ce         |                         |
| CBS                          | Kodak                    |                         |
| Charter Communications       | Korea Telecom            |                         |
| Cisco                        | Leggett and Platt        |                         |
| CitiFinancial                | Level 3 Communications   | Symantec                |
| City of Nashville            | Liz Claiborne            | Telecom Italia          |
| City of Tampa                | Lockheed Martin          | Telenor                 |
| Clemson University           | Lucent                   | Texaco                  |
| Comcast Cable                | MasterCard               | The CDC                 |
| Credit Suisse                | McDonald's Restaurants   | The Economist           |
| Dow Chemical                 | Microsoft                | Time Warner Cable       |
| EMC Corporation              | National Park Service    | U.S. Air Force          |
| Ericsson                     | NCR                      | University of Alaska    |
| Ernst and Young              | NEC                      | University of Kansas    |
| Faurecia                     | Nestle                   | University of Oklahoma  |
| Federal Express              | New York Power Authority | US Dept. Of Defense     |
| Federal Reserve Bank         | New York Times           | US Postal Service       |
| Fibercloud                   | Nielsen Media Research   | US Secret Service       |
| Fiserv                       | Nortel                   | Visa USA                |
| Ford Motor Company           | Perot Systems Japan      | Volvo                   |
| Foundstone                   | Phillips Petroleum       | Williams Communications |
| Gartner                      | Pricewaterhouse Coopers  | Yahoo                   |
| Gates Foundation             | Procter & Gamble         |                         |

Out of 33,000 customers — 16,000 downloaded

- 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

# After Infection

- 12-14 days silence
- Beacon to C&C
- Drop Teardrop

**SUPPLY CHAIN ATTACK**  
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

**EXECUTION, PERSISTENCE**  
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

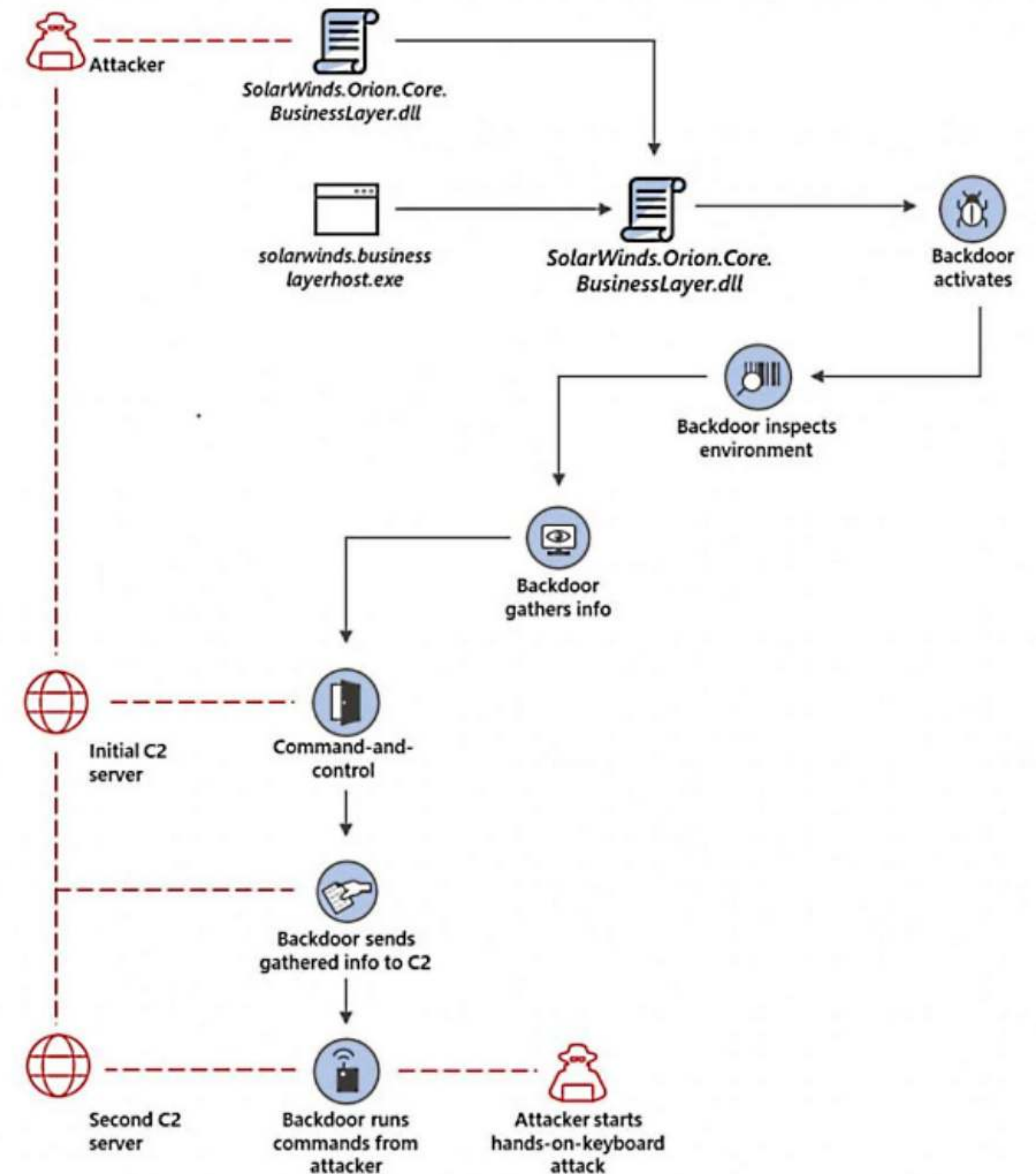
**DEFENSE EVASION**  
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

**RECON**  
The backdoor gathers system info

**INITIAL C2**  
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

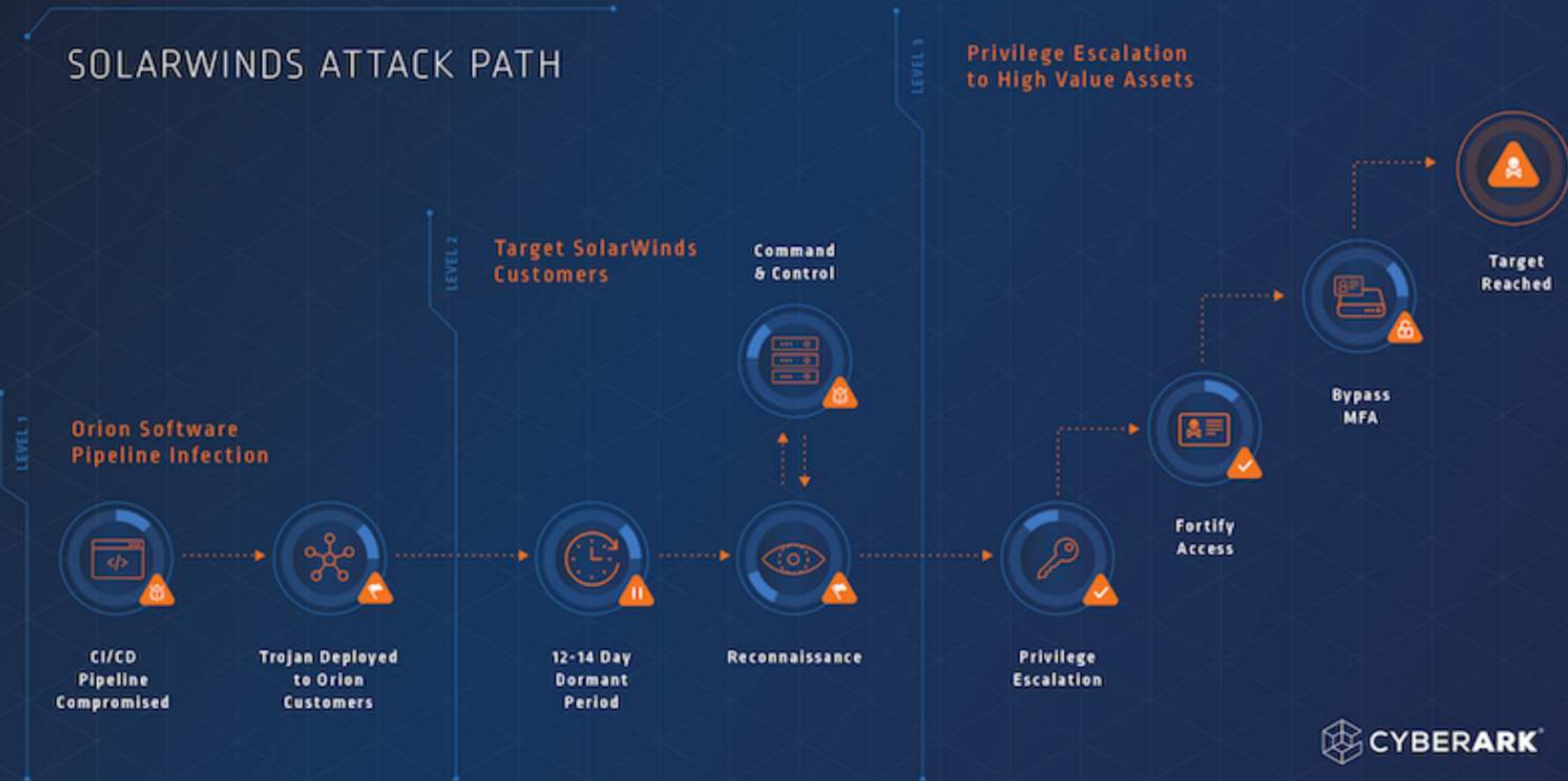
**EXFILTRATION**  
The backdoor sends gathered information to the attacker.

**HANDS-ON-KEYBOARD ATTACK**  
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



(Source: Microsoft)

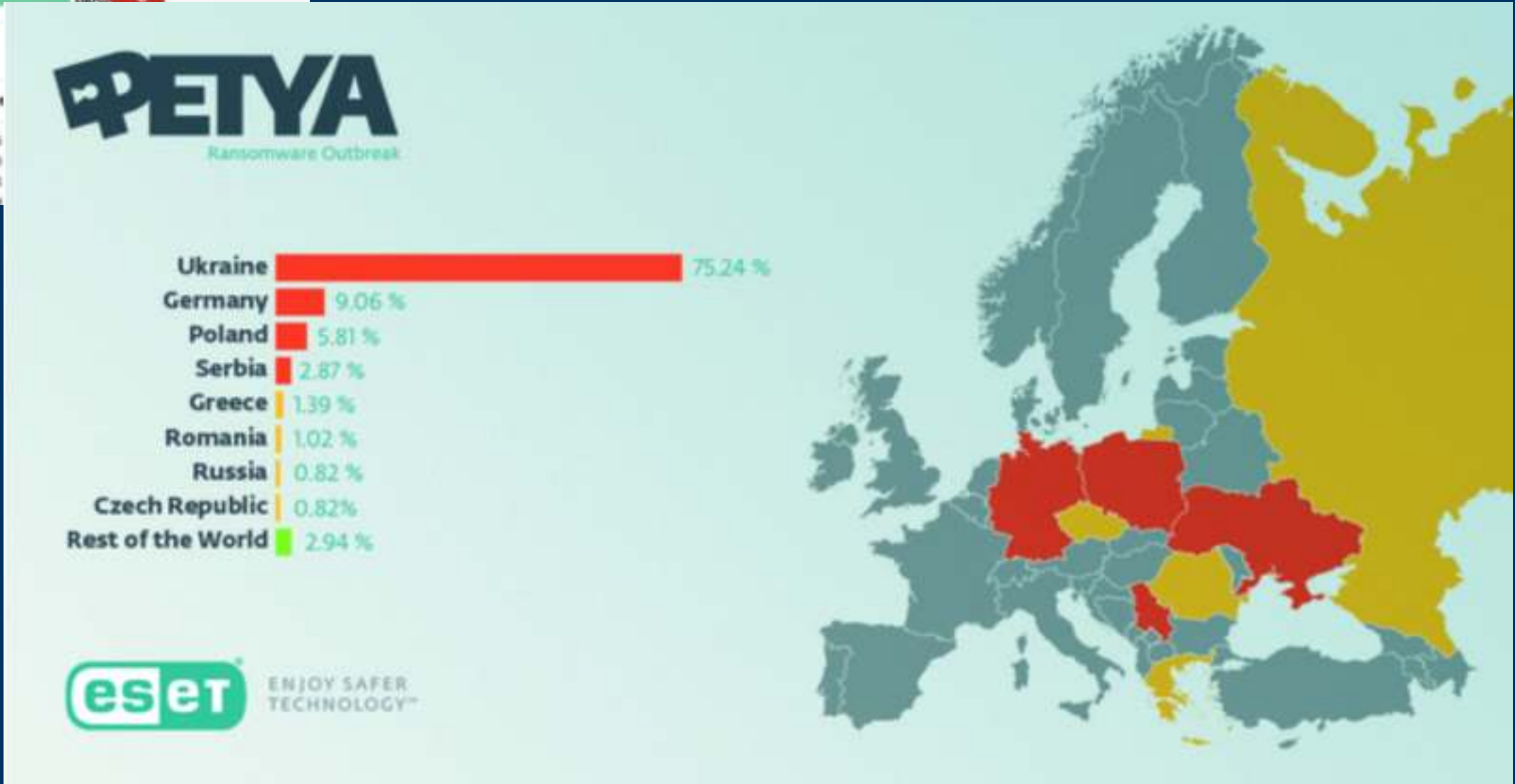
# SOLARWINDS ATTACK PATH



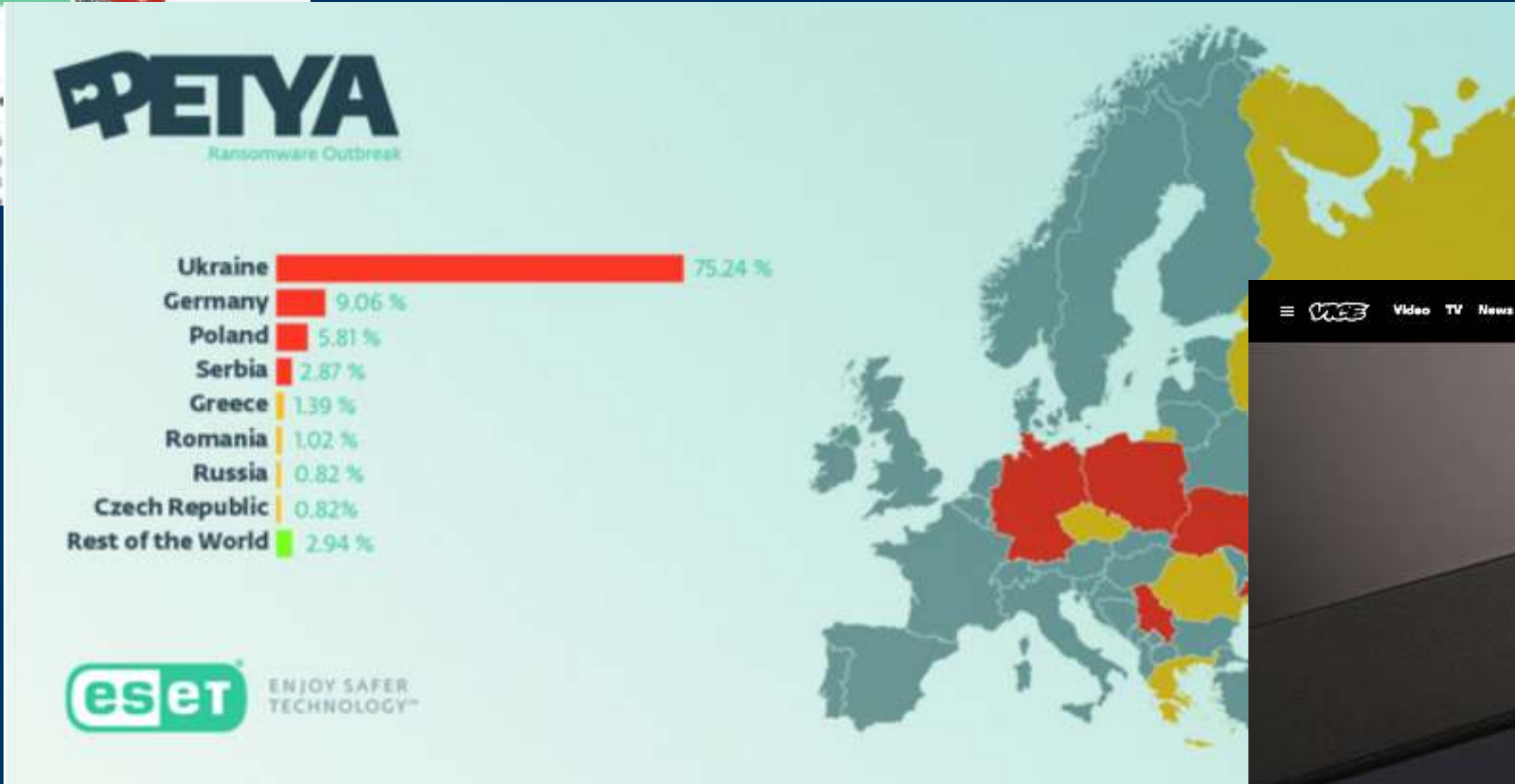
2017 - 2 million users



2017 - 2 million users



2017 - 2 million users



2018



**MOTHERBOARD  
TECHNOLOGY**

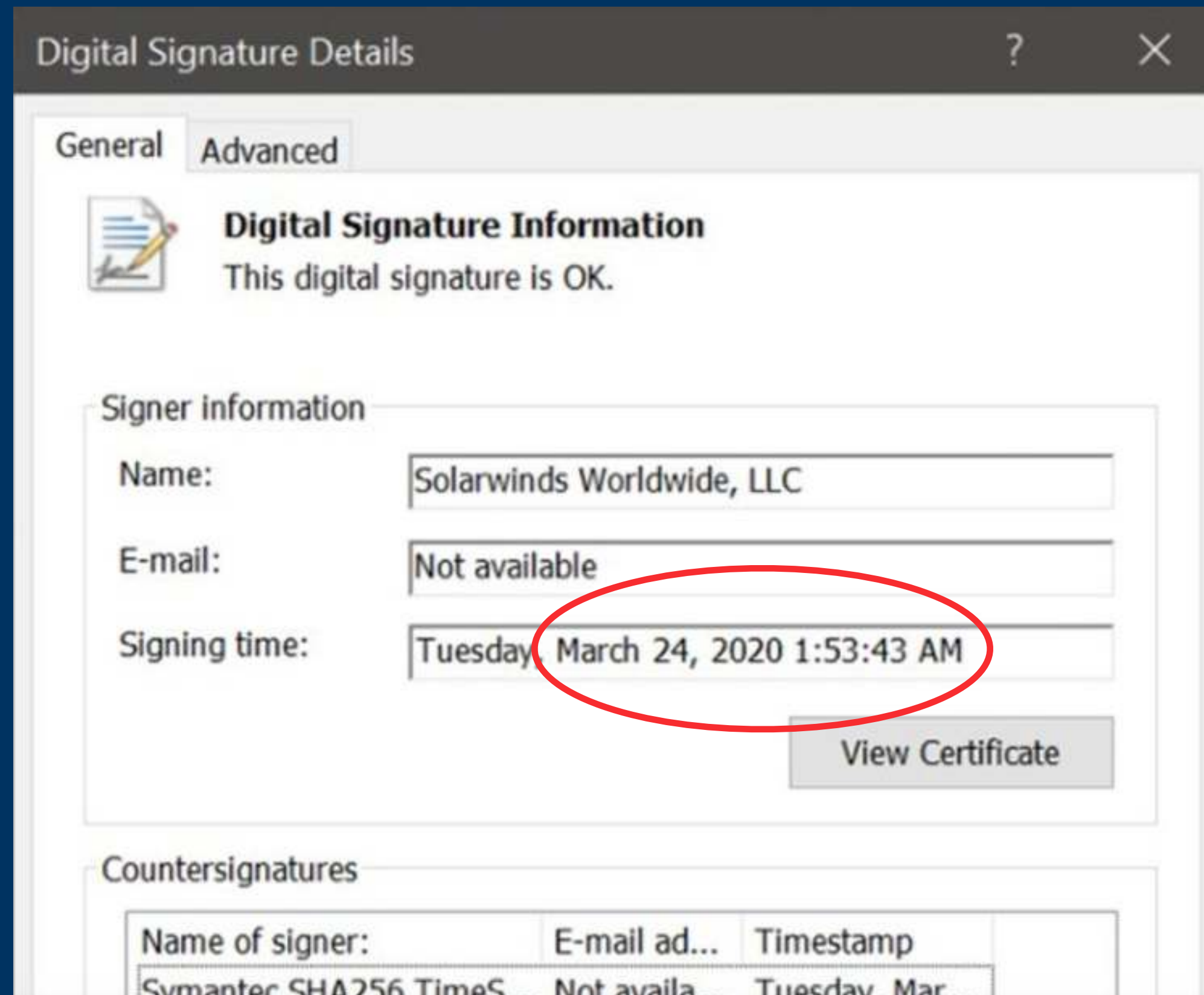
**Hackers Hijacked ASUS  
Software Updates to  
Install Backdoors on  
Thousands of Computers**

**Dec. 12**



**“We’re going public in 24 hours”**  
— Kevin Mandia to SolarWinds





## Three Software Updates

March 26

June 4

June 24

Out of 33,000 Orion customers,  
16,000 downloaded tainted updates

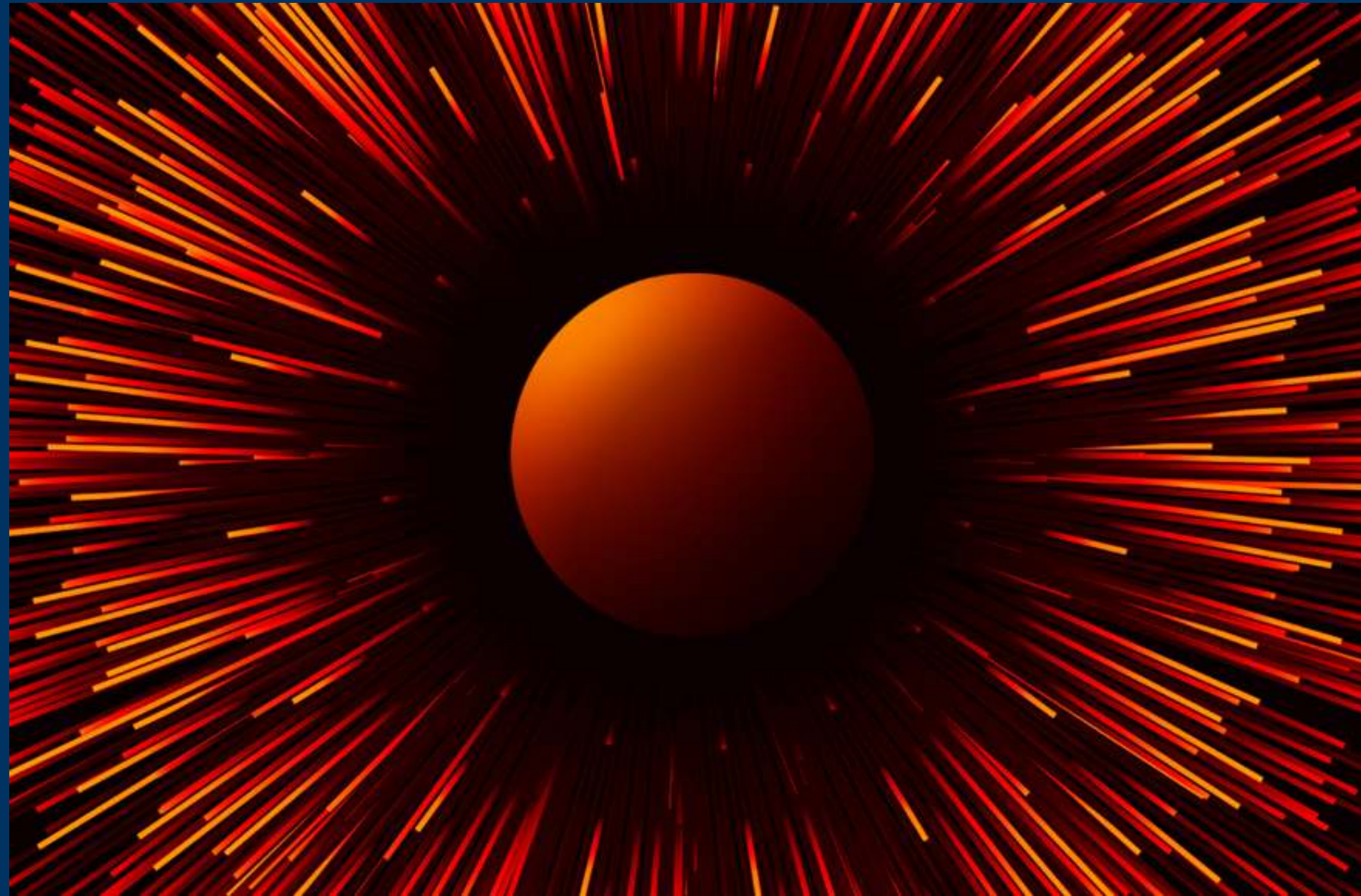
THREAT RESEARCH

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

FIREEYE

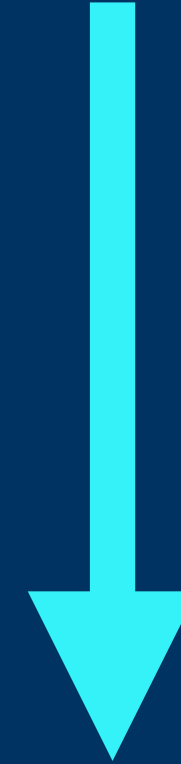
DEC 13, 2020 | 17 MIN READ | LAST UPDATED: AUG 09, 2023

Dec. 13, 2020



# SUNBURST

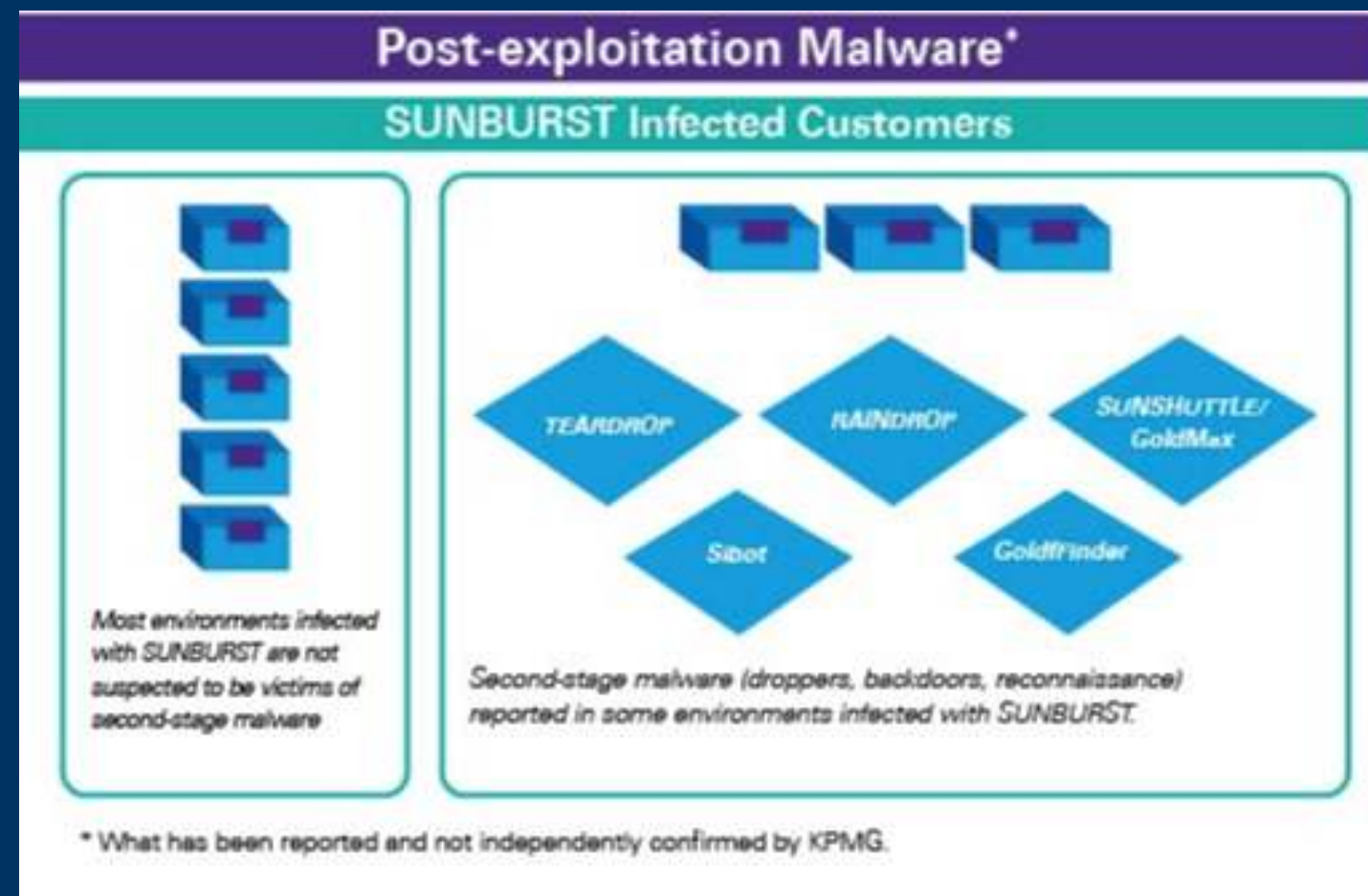
16,000



TEARDROP  
(fewer than 100)



CobaltStrike



# Victims

50 % - software makers, IT services, hardware providers

18 % - government agencies and telecoms

18 % - think tanks

# 9 Gov Agencies:



Commerce



Defense



Treasury



DHS



DoE



Justice Dept

## Email



- Commerce — sanctions
- DoE — nuclear facilities/stockpiles
- DHS — vulnerabilities in critical infrastructure
- Federal court system — sealed documents (search warrants, indictments, wiretap orders)

Backdoor was useless unless Orion server was connected to internet

20-30 % had them connected

Many configured them improperly

Mandiant blocked external connections

**We traced the call.  
It's coming from  
inside the house.**



BUT WHEN SHE TRACED THE  
KILLER'S IP ADDRESS... IT WAS  
IN THE 192.168/16 BLOCK!

GASP!

- 71 email accounts monitored
- 50 software programs examined
- Revoked certs
- Recompiled/signed all software
- **19,000** calls from customers/governments
- SEC filing



“Adding a single comma will cost \$20,000”

- Kevin Thompson, SolarWinds CEO



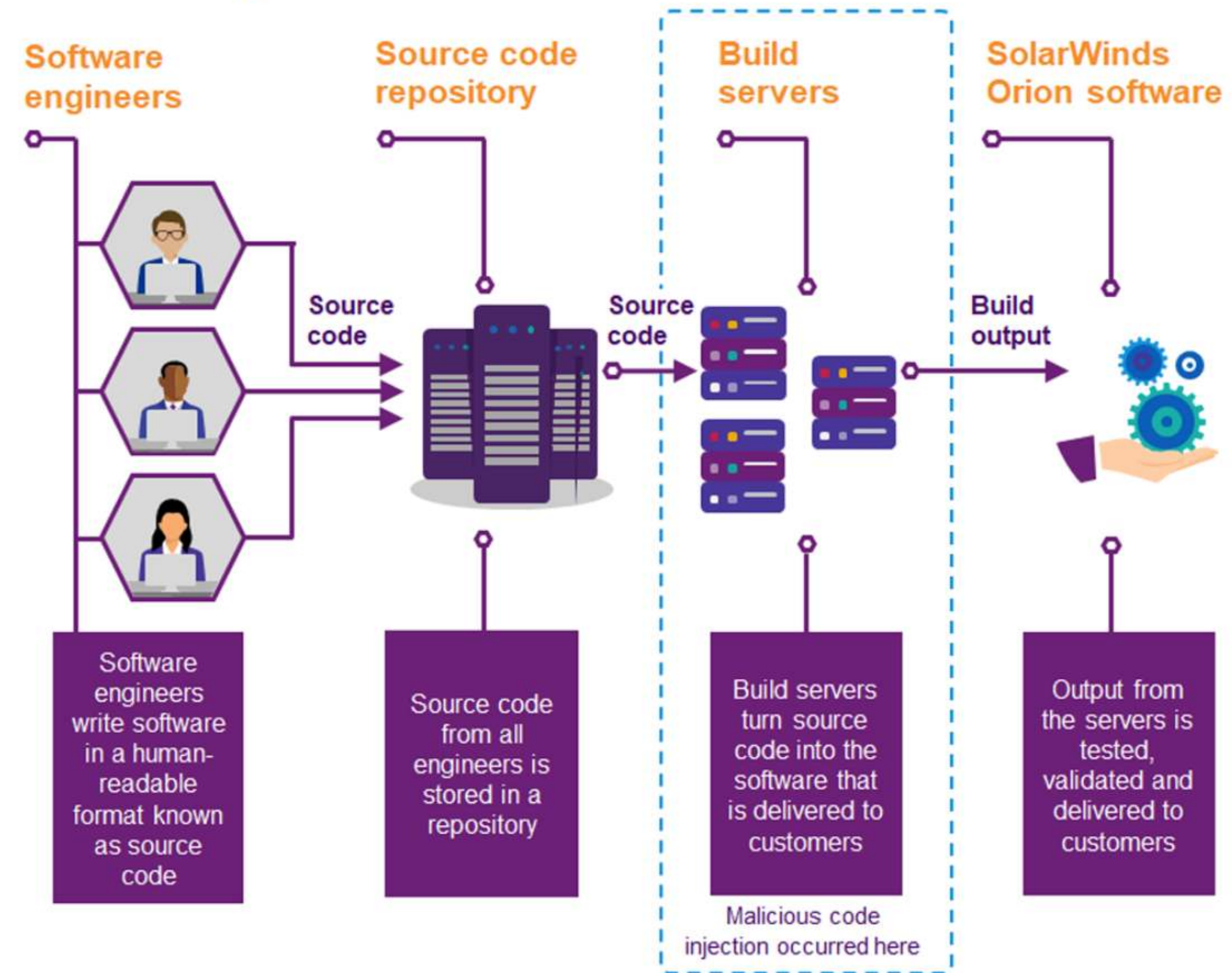
Jan. 5, 2021



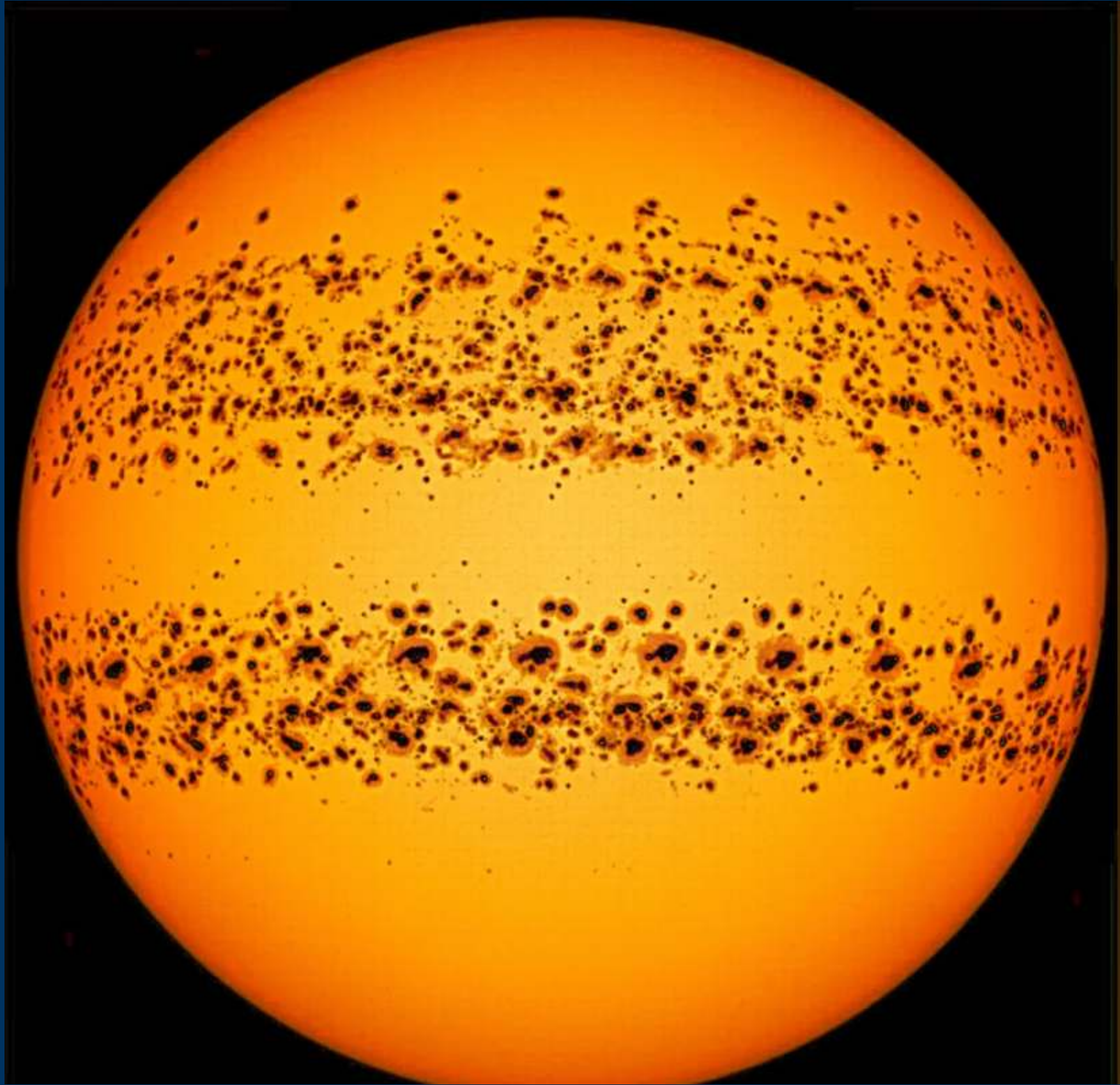
3,500 lines of code

JetBrains - Team City  
100 VMWare virtual machines

## Creating SolarWinds Orion Software



(Source: KPMG)



“Sheer elegance”

“It was just this moment of fear amongst all of us”

KIM ZETTER SECURITY MAR 3, 2010 11:05 PM

# 'Google' Hackers Had Ability to Alter Source Code

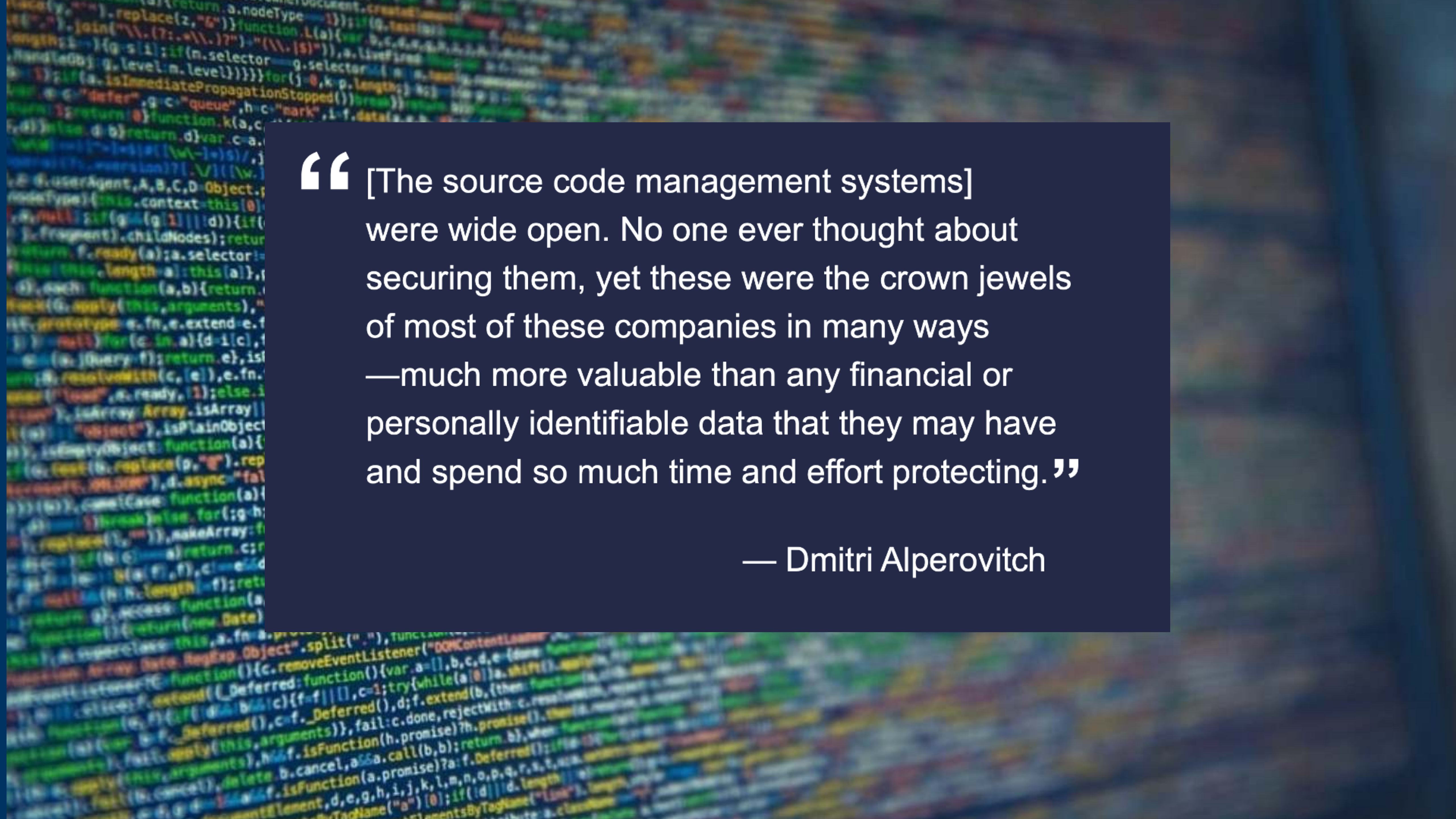
Hackers who breached Google and other companies in January targeted source-code management systems, security firm McAfee asserted Wednesday. They manipulated a little-known trove of security flaws that would allow easy unauthorized access to the intellectual property the system is meant to protect. The software-management systems, widely used at businesses unaware that the holes exist, were [...]



TRENDING NOW

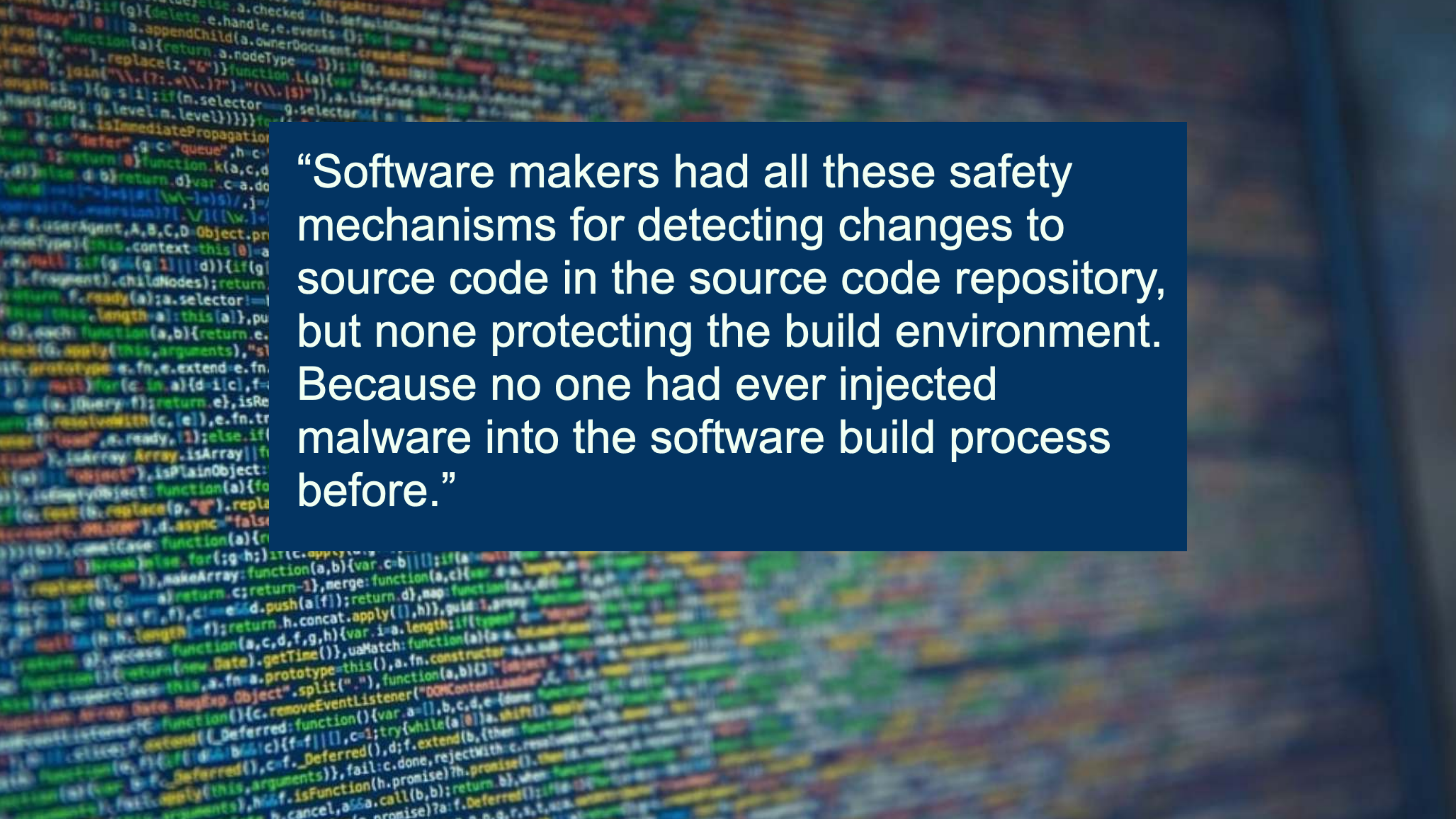
Internet Expert Debunks Cybersecurity Myths

Hackers who breached Google and other companies in

The background of the entire image is a dense, blurred field of multi-colored text, resembling source code from a programming language like JavaScript. The colors include shades of green, blue, yellow, and white, creating a vibrant, abstract pattern.

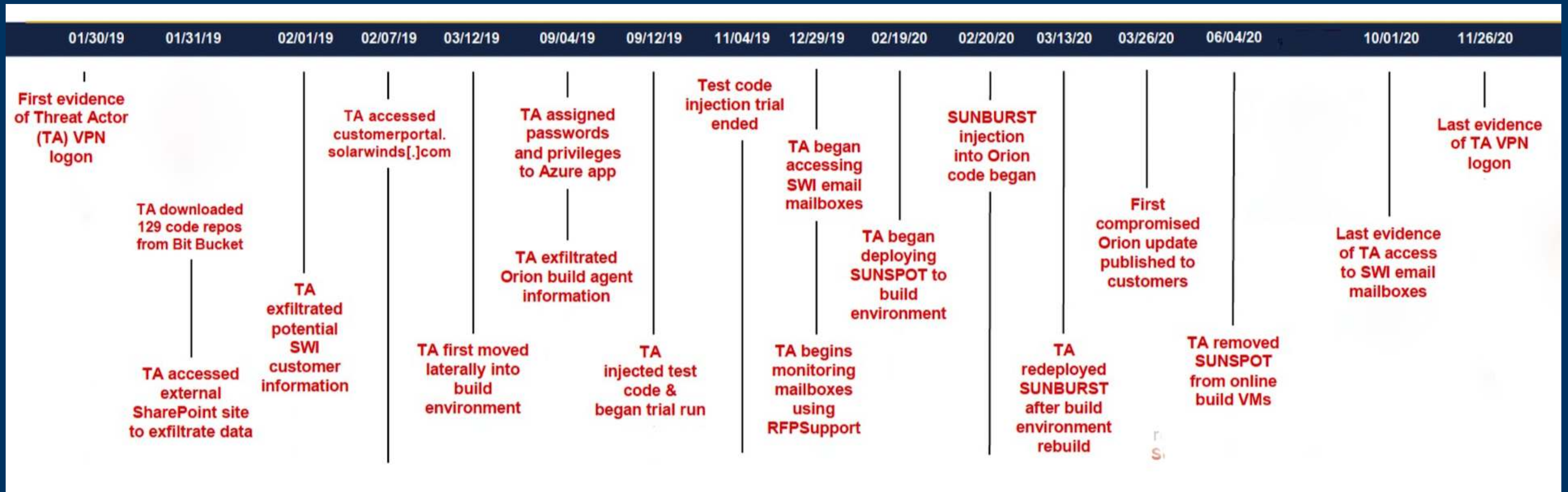
“ [The source code management systems] were wide open. No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways —much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting.”

— Dmitri Alperovitch

The background of the image is a dense, colorful blur of code, likely JavaScript or a similar programming language, with various colors like green, blue, and yellow. The text is overlaid on a dark blue rectangular area.

“Software makers had all these safety mechanisms for detecting changes to source code in the source code repository, but none protecting the build environment. Because no one had ever injected malware into the software build process before.”

# Timeline



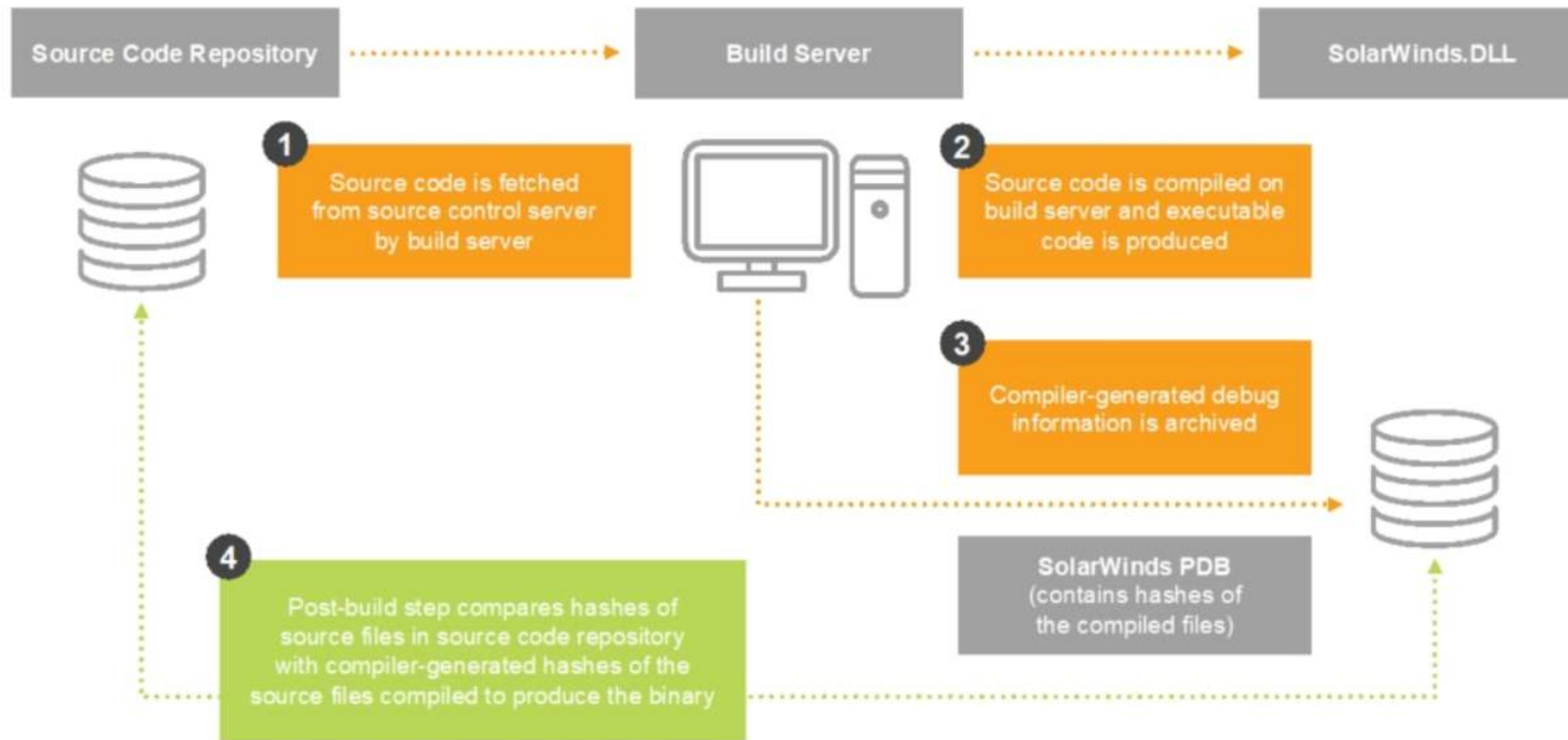


## What We Don't Know



- When did campaign begin?
- Identities of all the 100 or so victims
- What did they do on infected machines?
- Are they still in networks?
- Were other supply chains compromised?

# SolarWinds Post-Build Verification





**Kim Zetter**  
**@kimzetter**  
**[kzetter@gmail.com](mailto:kzetter@gmail.com)**