SUPPLY CHAIN ATTACKS & THIRD PARTY RISKS

GAURAV VERMA

#WHOAMI

Gaurav Verma

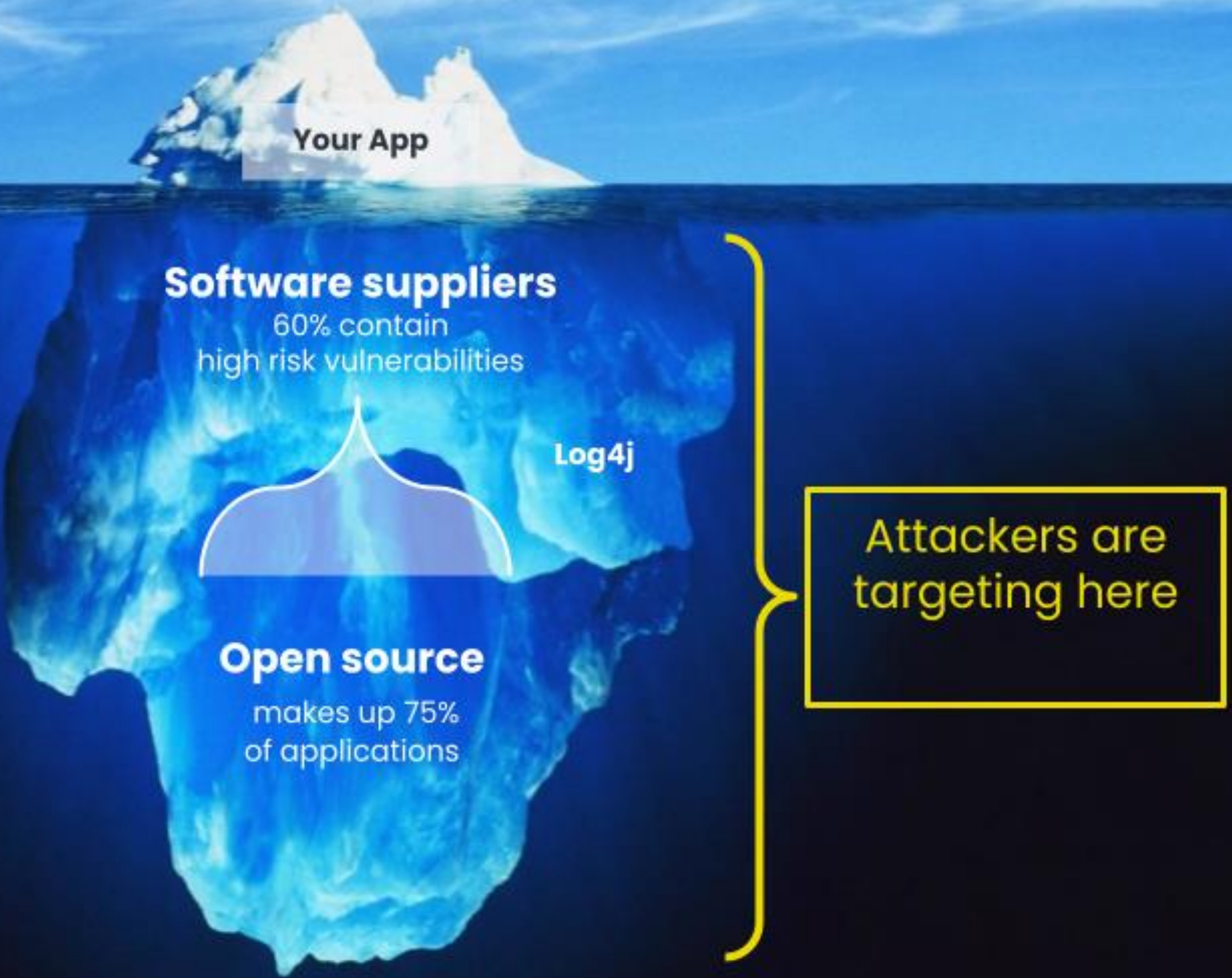
Head of IT Risk and Security

Axe Group

linkedin.com/in/cybersecguru

- 15+ Years experience
- PhD Student, University of Sydney
- Collaborated with Law Enforcement, Government Agencies & Universities
- Moved to Australia in 2021 on Distinguished Talent Visa in Cyber
- Global Certifications & Awards Winner

Risk in the Software Supply Chain



Your App

Software suppliers

60% contain
high risk vulnerabilities

Log4j

Open source

makes up 75%
of applications

Attackers are
targeting here

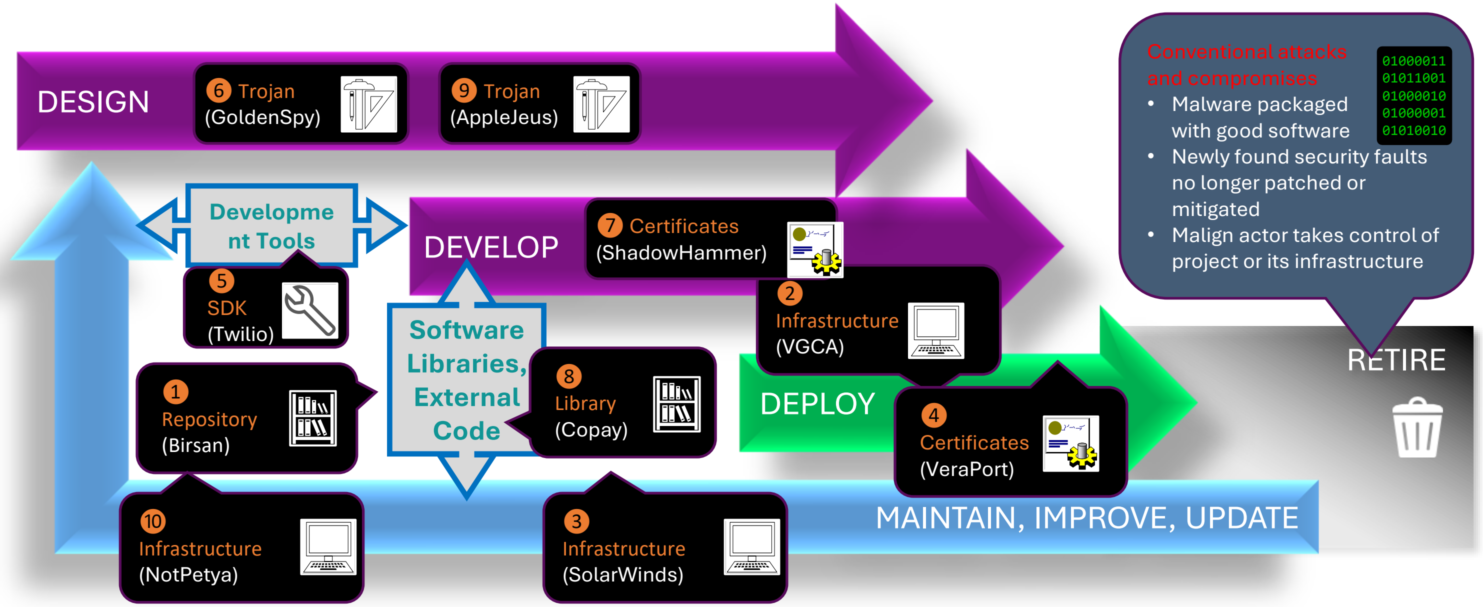
38
ATTACKER

CYBER RESILIENCE = BUSINESS RESILIENCE

Cyber resilience is the backbone of business resilience. It's more than just technology; it's a strategic approach to safeguard operations, protect data, and maintain customer trust.

SOFTWARE SUPPLY CHAIN ATTACKS

Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.



Conventional attacks and compromises

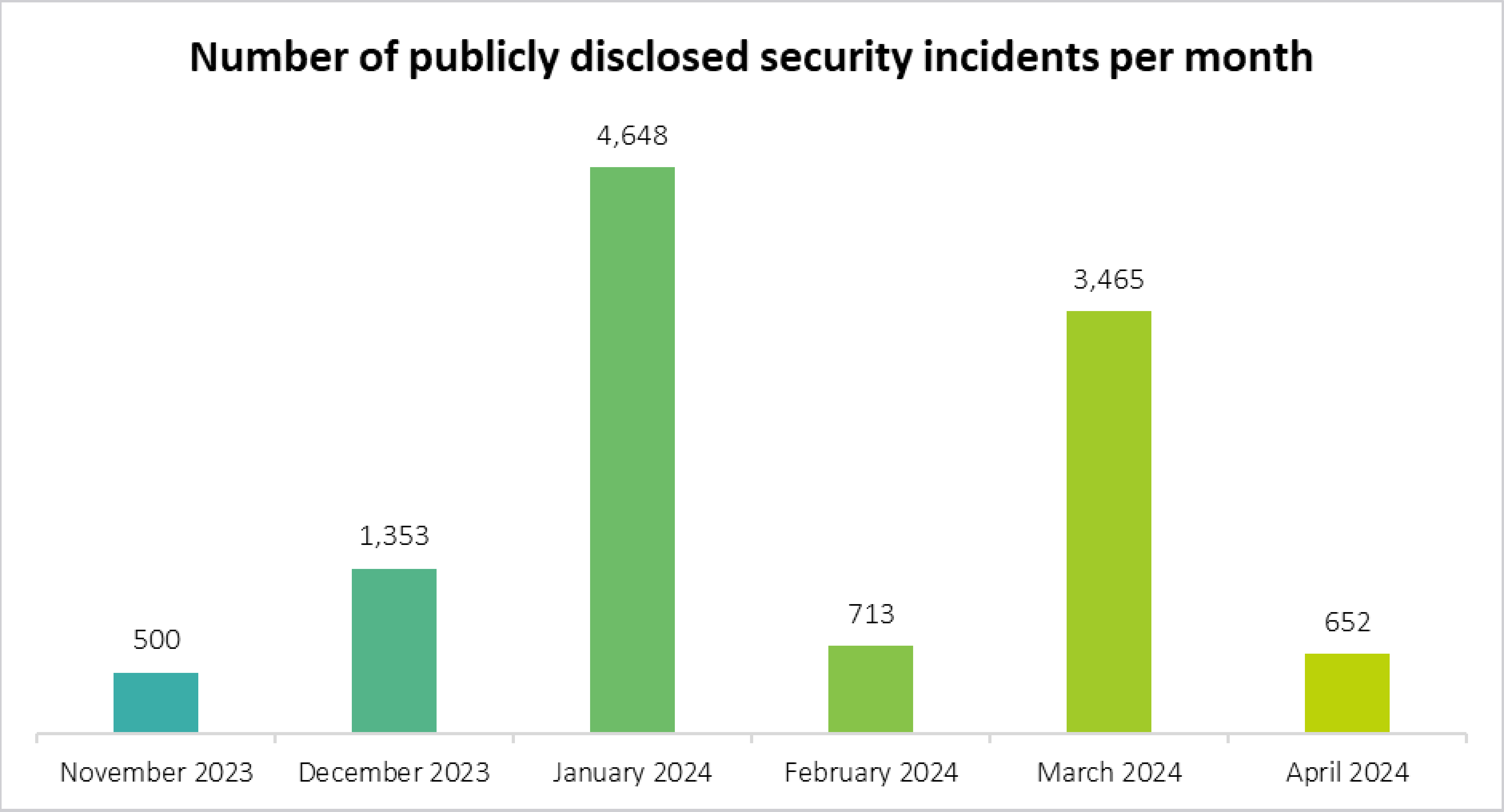
- Malware packaged with good software
- Newly found security faults no longer patched or mitigated
- Malign actor takes control of project or its infrastructure

Software Supply Chain Attacks can target products at any stage of the development lifecycle to achieve access, conduct espionage, and enable sabotage.

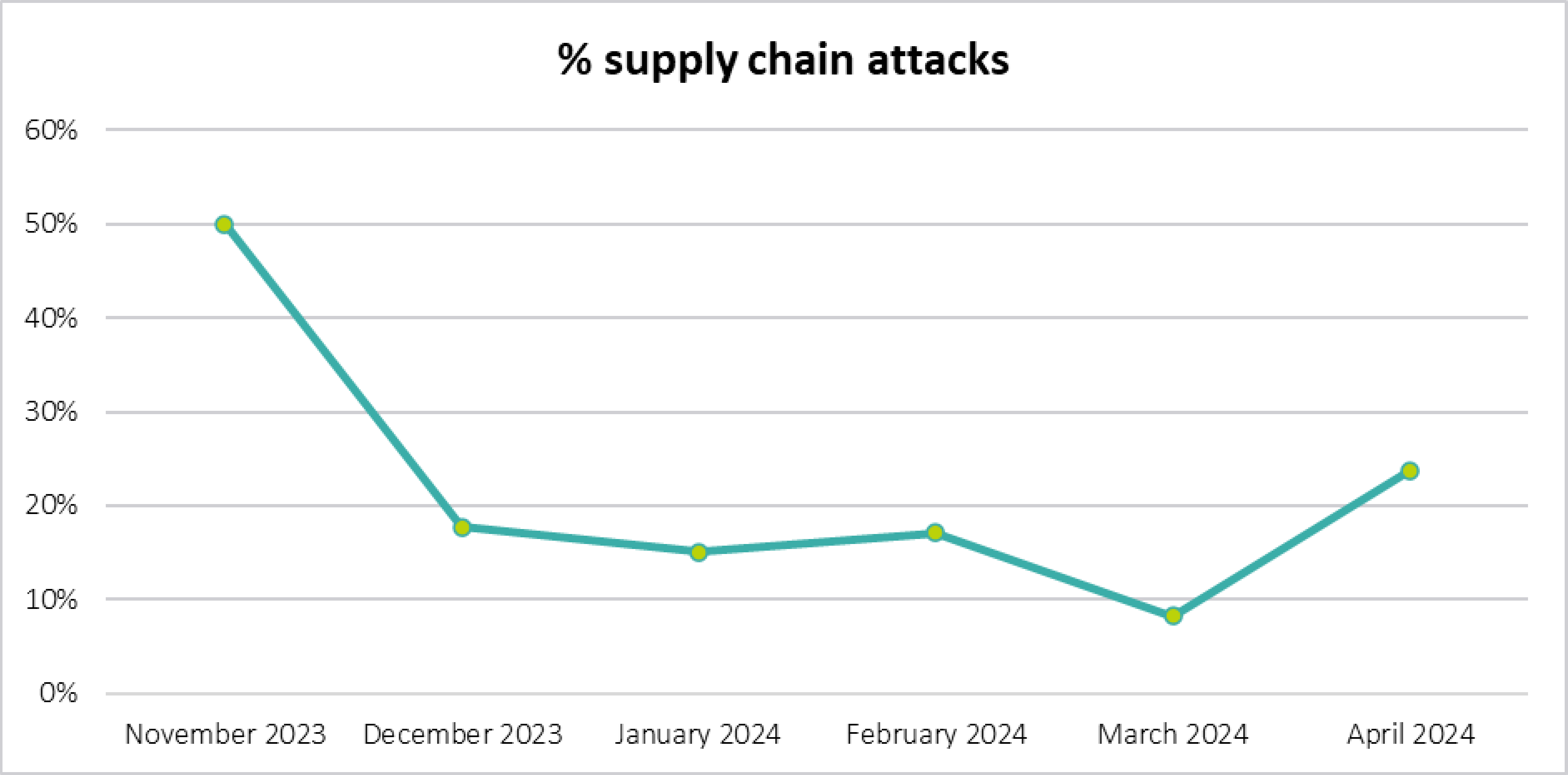
- **Software supply chain attacks can use simple deception techniques such as disguising malware as legitimate products, or use complex means to access and modify the source code of genuine programs.**
- **Adversaries may seek to exploit tools, dependencies, shared libraries, and third-party code in addition to compromising the personnel and infrastructure of developers and distributors.**
- **Using software after it reaches end-of-life increases exposure to conventional cyber attacks.**

Legend	Discovered	Incident	Entry Point	Compromised Stage	Affected Software	Initial Impact	Notes
1	Feb 2021	Birsan research (Ethical hacker)	Open-Source Libraries	Development (open-source library)	Multiple	Proof-of-concept	Security researcher Alex Birsan identified improperly configured package managers at multiple major companies and verified they would install unauthorized code from public repositories instead of limiting access to internal servers.
2	Dec 2020	VGCA compromise (SignSight)	Government Certification Authority Website	Deployment (infrastructure)	Digital Signature Toolkit	Targeted government and commercial entities	Compromised a Vietnam government certificate authority and added a backdoor component to installers for legitimate software.
3	Dec 2020	SolarWinds Orion compromise	Undisclosed	Development (infrastructure)	Network Monitoring and Management Platform	Espionage	The SolarWinds Orion source code compromise represents the most significant cyber incident impacting enterprise networks across the private sector, federal, state, and local governments to date.
4	Nov 2020	VeraPort compromise	Compromised Website (Watering Hole)	Deployment (digital certificates)	Computer Utility (Browser Plugin)	Targeted government and financial websites	Targeted South Korean users of a trusted download verification tool by prompting its browser plugin to install malware signed with stolen authentic digital certificates.
5	Jul 2020	Twilio SDK compromise	Misconfigured Public Cloud Storage Bucket	Development (SDK tool)	Cloud-Based Communications	Theft	Attackers injected malicious code within the SDK library of a Communications Platform as a Service (CPAAS) company through its misconfigured cloud-hosted infrastructure.
6	Jun 2020	GoldenSpy (MITRE ID: S0493)	Over Distribution with Hidden Malicious Properties	Design (intentional)	Business Software	Targeted specific Western companies	A Chinese bank compelled Western corporate clients to install tax software containing a hidden backdoor.
7	Jan 2019	Asus compromise (ShadowHammer)	Compromised Development Infrastructure	Development (digital certificates)	Computer Utility (Software Updater)	Targeted specific individuals	Compromised manufacturer to target a pool of specific customers by delivering malware via software updates signed with authentic certificates.
8	Nov 2018	Copay compromise	Open-Source Library	Development (open-source code)	Cryptocurrency Wallet	Cryptocurrency theft	Poisoned popular open-source JavaScript library by injecting malicious code to steal cryptocurrency stored in desktop and mobile wallet software.
9	Aug 2018	AppleJeus campaign	Overt Distribution with Hidden Malicious Properties	Design (intentional)	Cryptocurrency Apps	Cryptocurrency theft	Overt distribution of software with hidden malicious properties. Persistent campaign developed and distributed innocent-looking cryptocurrency applications that contained hidden malicious content.
10	Jun 2017	NotPetya (MITRE ID: S0368)	Compromised Software Update Infrastructure	Deployment (infrastructure)	Business Software	Data destruction; disrupted commerce and services	Self-propagating data-destruction malware delivered through a software update from the developer's compromised infrastructure.

PUBLICLY DISCLOSED SECURITY INCIDENTS



SUPPLY CHAIN ATTACKS (2024)



2015- Ukraine

- Power Grid Hacked
- Disabled Power
- 250,000 Customers Impacted
- Destroyed Critical Servers & Infra
- Took Call Centres Offline

2020- US Hospital

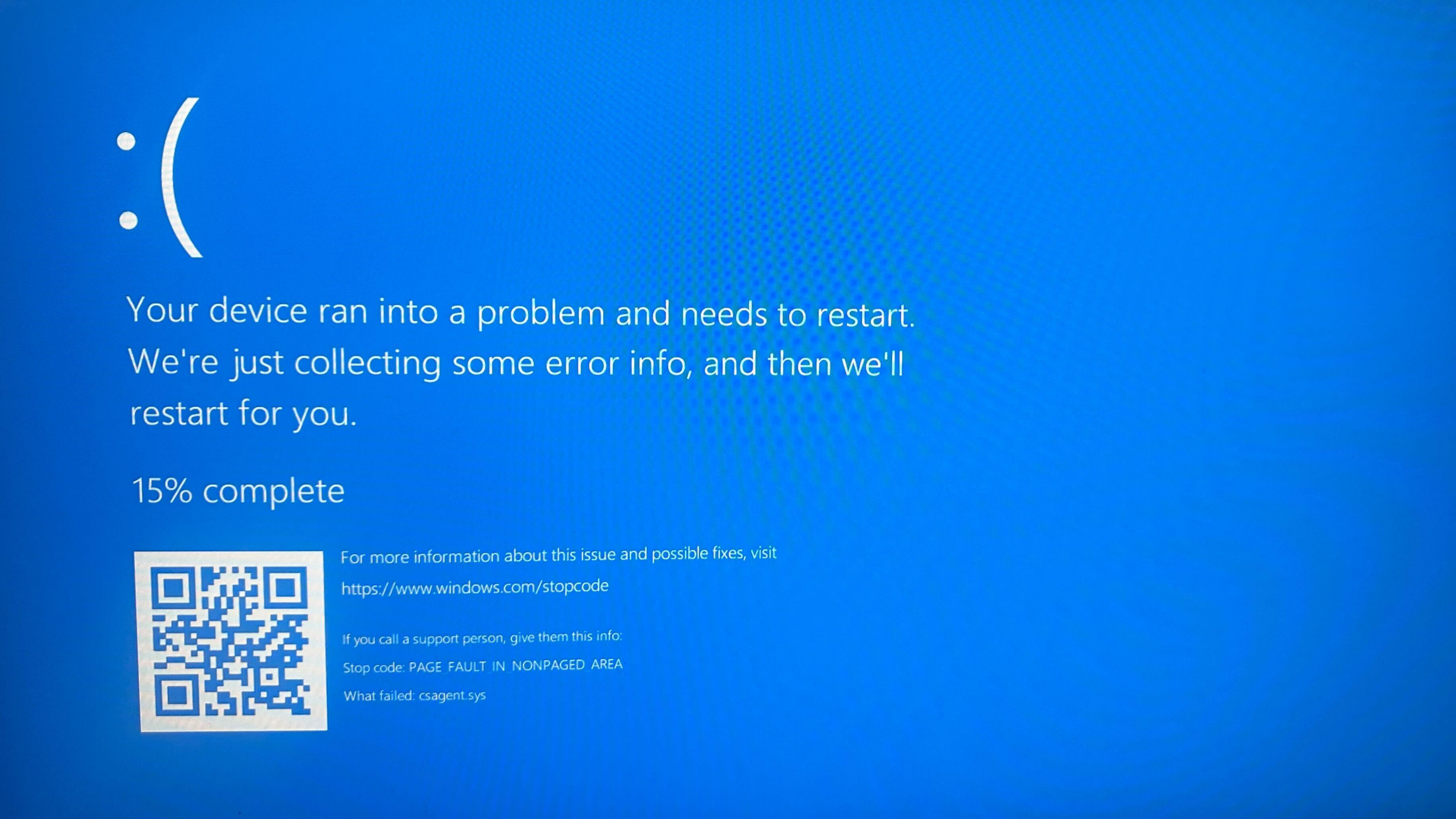
- Ransomware Attack
- Computers Disabled
- Life Altering and at times, fatal impact

2021- Colonial Pipeline

- First incident in 57 years
- Resulted in massive fuel shortage
- $4 million ransom paid to threat actors

2021- Kaseya

- 50 Service Providers, 1500 Customers
- 1M Endpoints



:(

Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

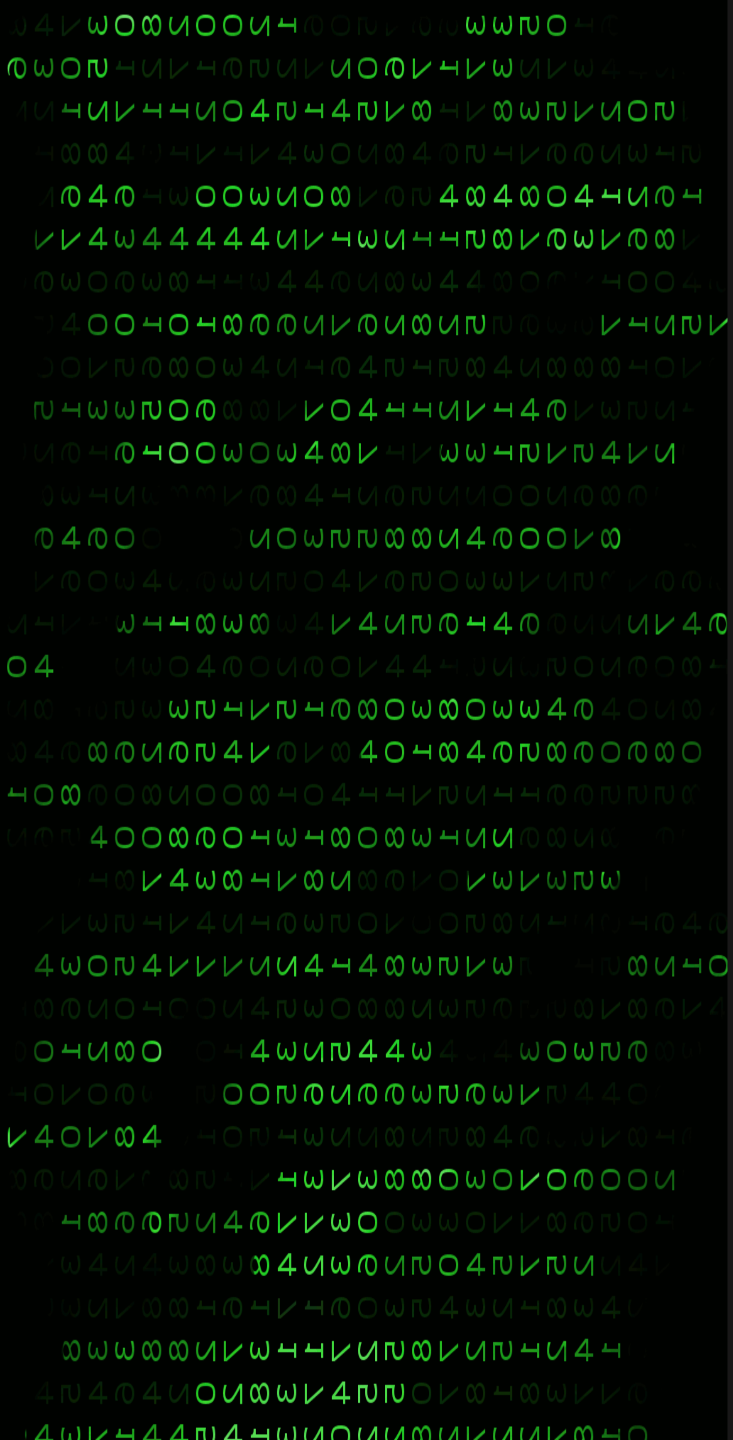
15% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

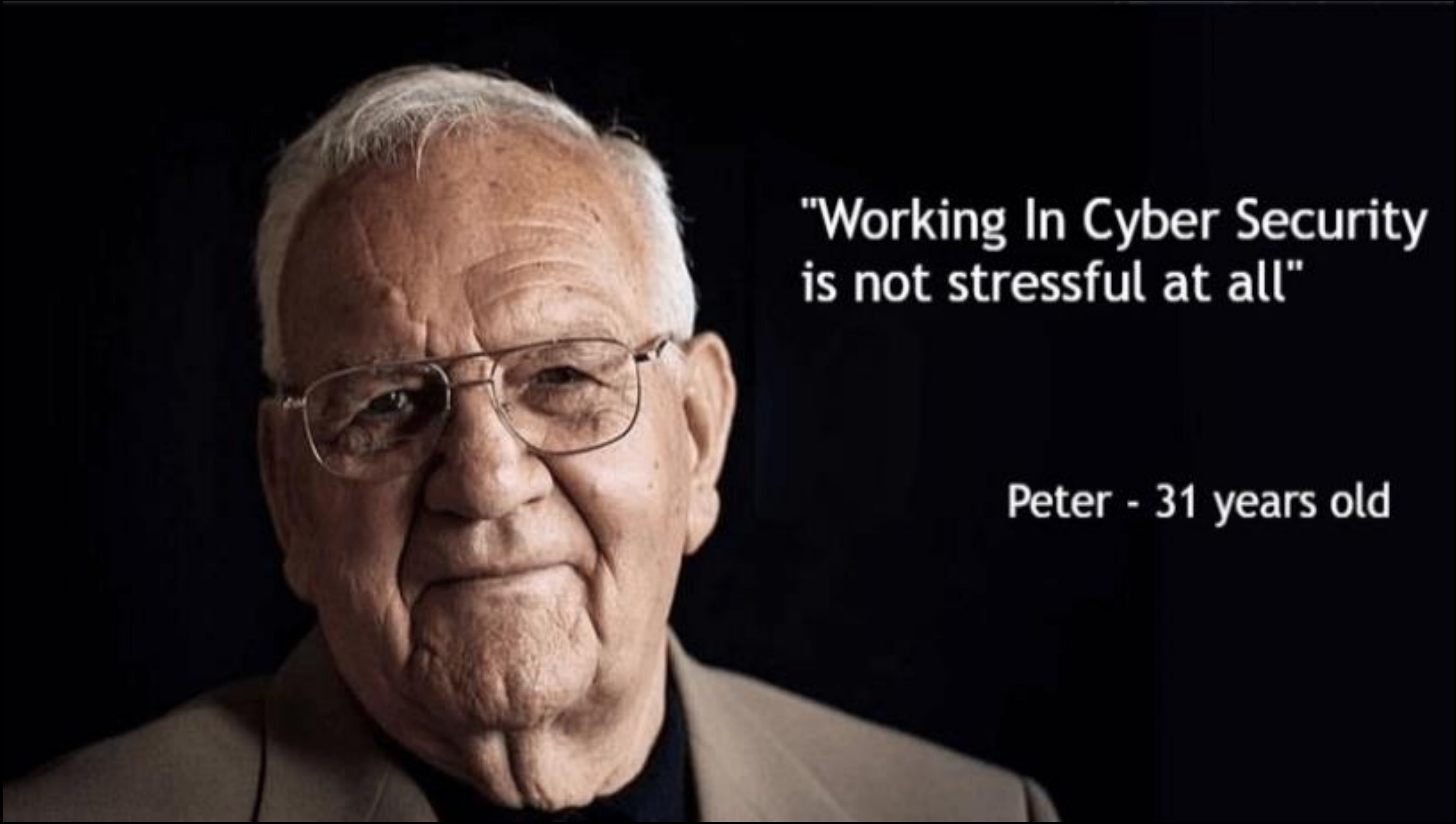
Stop code: PAGE_FAULT_IN_NONPAGED_AREA

What failed: csagent.sys



RECOMMENDATIONS FOR MANAGING SUPPLY CHAIN SECURITY

- INTEGRATE SUPPLY CHAIN RISK MANAGEMENT ENTERPRISE-WIDE
- BUILD A ROBUST THIRD PARTY RISK MANAGEMENT POLICY & FORMAL SUPPLY CHAIN RISK MANAGEMENT PROGRAM
- IDENTIFY & MANAGE CRITICAL SUPPLIERS
- MONITOR FOURTH PARTY FOR KEY THIRD PARTY SUPPLIERS
- ENHANCE IDENTITY & MANAGEMENT CONTROLS
- NEVER TRUST AND ALWAYS VERIFY
- FOSTER CYBER LEARNING AND AWARENESS ENVIRONMENT
- COLLABORATE CLOSELY WITH KEY SUPPLIERS & INCLUDE IN RESILIENCE ACTIVITIES
- INCLUDE SUPPLY CHAIN ATTACKS SCENARIOS IN TABLE TOP EXERCISES



"Working In Cyber Security
is not stressful at all"

Peter - 31 years old