2025
NORTH
AMERICA
COMMUNITY
MEETING

Code Red

A Cybersecurity Crime Drama

Jake Marcinko

Senior Technical Product Manager

PCI Security Standards Council


8
7
The Designated Driver Is The Life


NEW
YORKER


MHU
MHU
MHU


POLICE LINE DO NOT CROSS
POLICE


LÖGREGLAN

CSI:PCI


CRIME SCENE
CRIME SCENE
INVESTIGATION
EVIDENCE
2
2
EVIDENCE
EVIDENCE
1

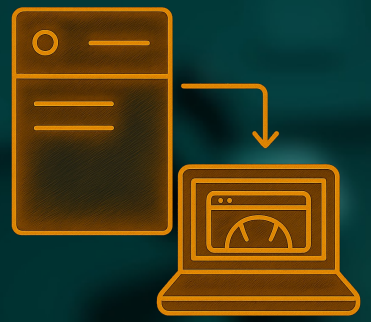

HORATIO CAINE


CODE
RED
CYBER ATTACK
CYBER
ATTACK
WARNING
CYBER ATTACK
WARNING
CYBER ATTACK

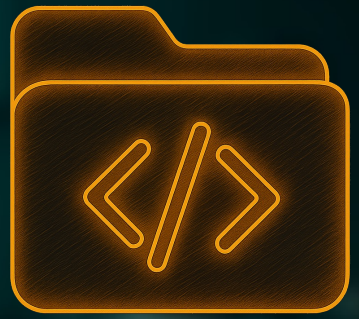
- Multiple customers reporting latest software update triggering anti-malware alerts.
- Malware communicating with C2 infrastructure.
- Outbound malware traffic traced to a recently-registered domain.
- All malware communications are encrypted.

Background

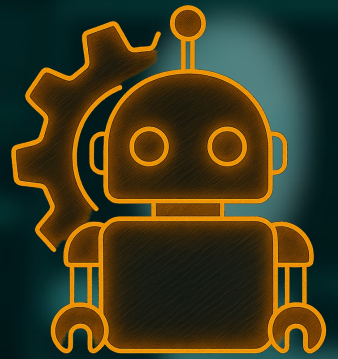
Software Architecture and Update Process



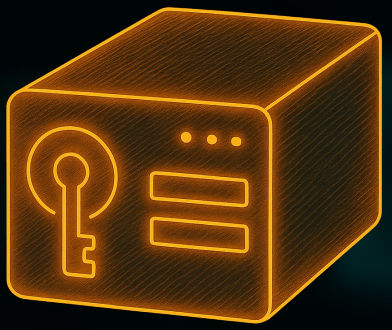
Client app with SaaS backend



Source code stored in GitHub Enterprise



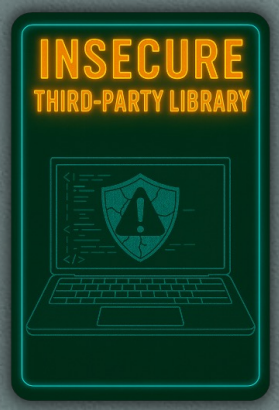
Jenkins to compile, sign, & deploy code

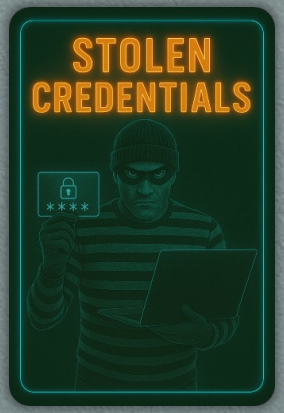


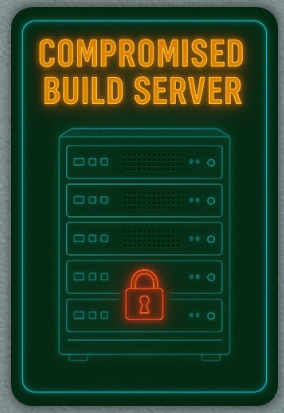
Code-signing keys stored in a secure HSM

EVIDENCE

Critical client vulnerability



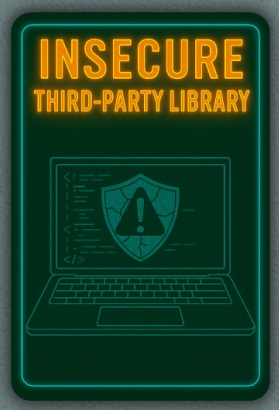


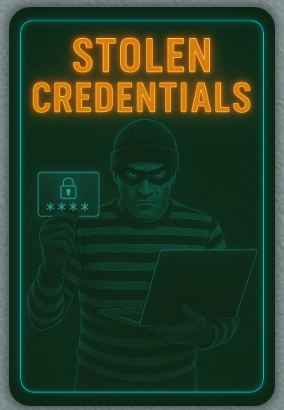


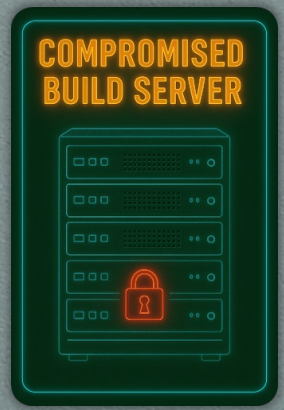
EVIDENCE

Critical client vulnerability

Critical API vulnerability





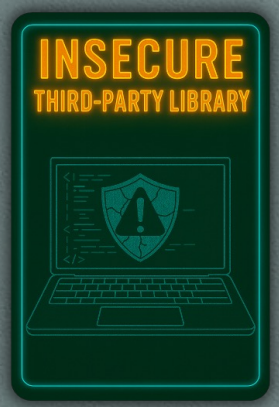


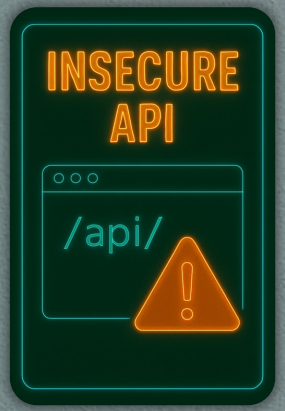
EVIDENCE

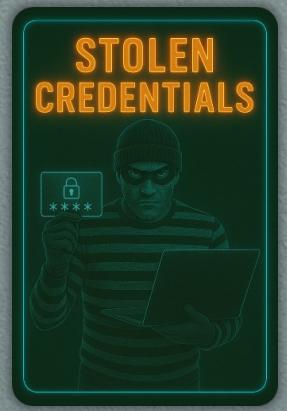
Critical client vulnerability

Critical API vulnerability

Company-signed malware







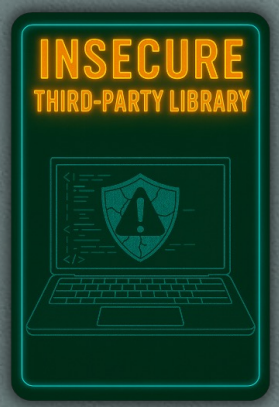
EVIDENCE

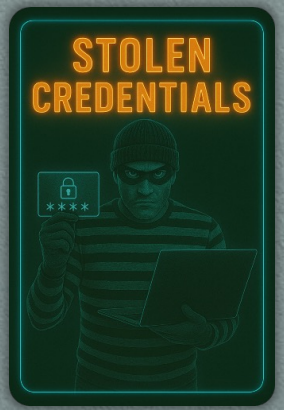
Critical client vulnerability

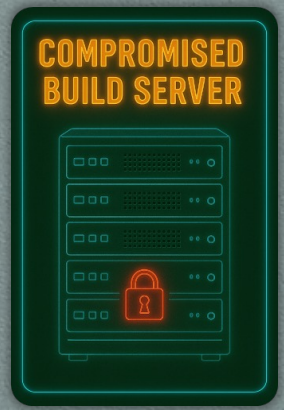
Critical API vulnerability

Company-signed malware

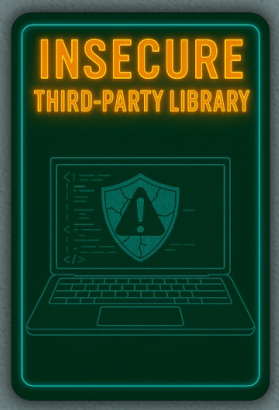
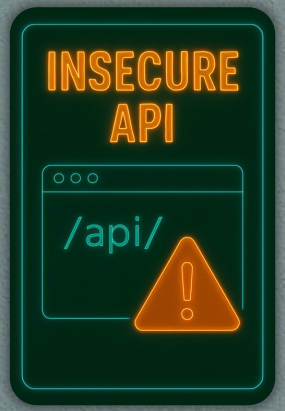
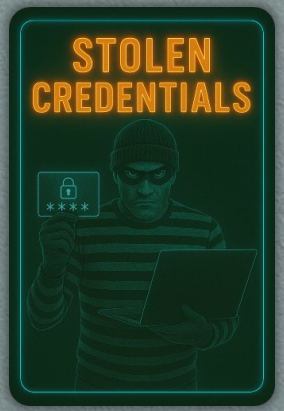
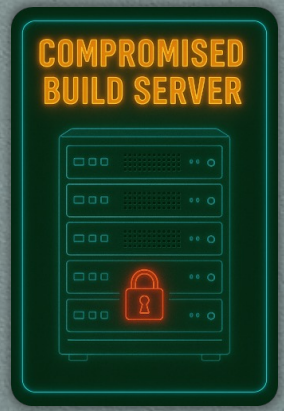
Suspicious login attempts







EVIDENCE

Critical client vulnerability	Critical API vulnerability	Company-signed malware	Suspicious login attempts	Suspicious child processes
				


HORATIO CAINE

What was the likely main attack vector?

EVIDENCE

Critical client vulnerability

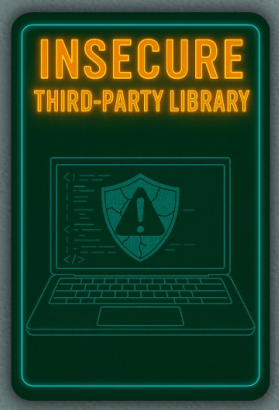
EOL library dependency

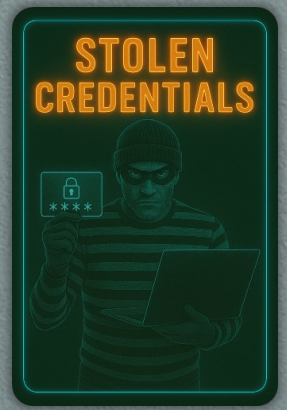
Critical API vulnerability

Company-signed malware

Suspicious login attempts

Suspicious child processes





EVIDENCE

Critical client vulnerability

EOL library dependency

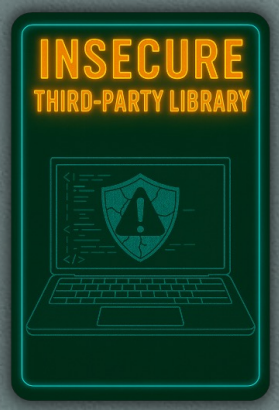
Critical API vulnerability

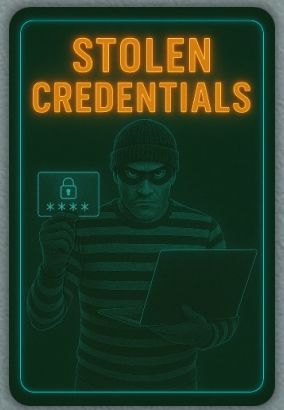
Insecure input handling

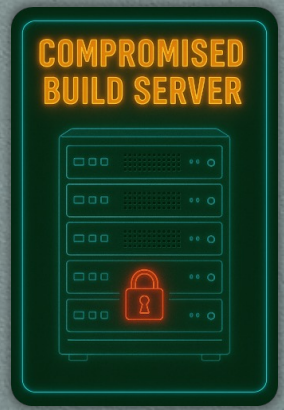
Company-signed malware

Suspicious login attempts

Suspicious child processes



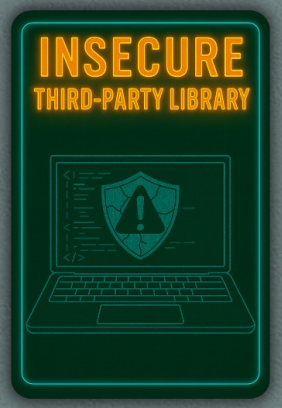




EVIDENCE

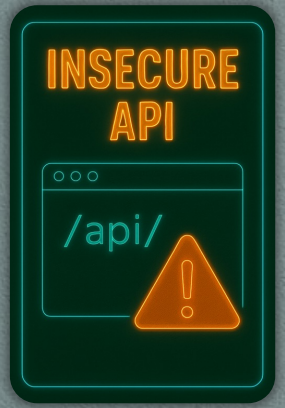
Critical client vulnerability

EOL library dependency



Critical API vulnerability

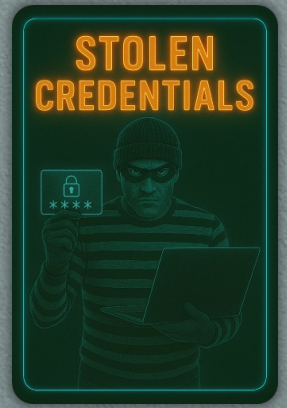
Insecure input handling



Company-signed malware

Unauthorized internal key exposure

Suspicious login attempts

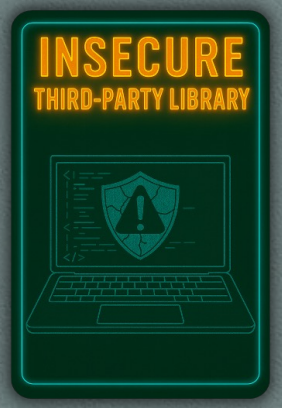


Suspicious child processes

EVIDENCE

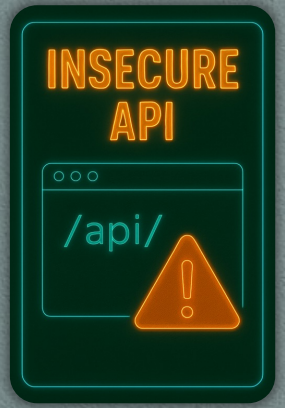
Critical client vulnerability

EOL library dependency



Critical API vulnerability

Insecure input handling

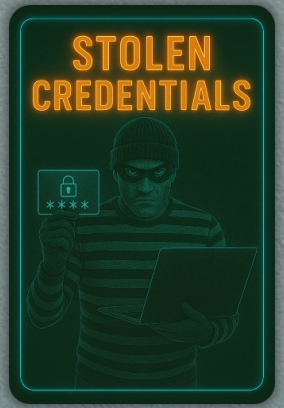


Company-signed malware

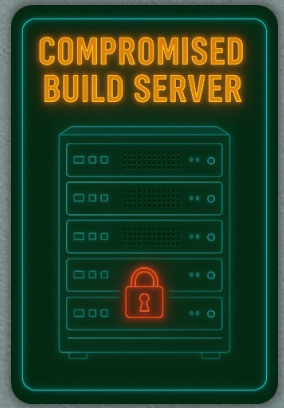
Unauthorized internal key exposure

Suspicious login attempts

DevOps targeted phishing attempts



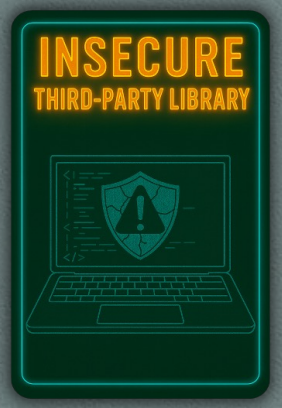
Suspicious child processes



EVIDENCE

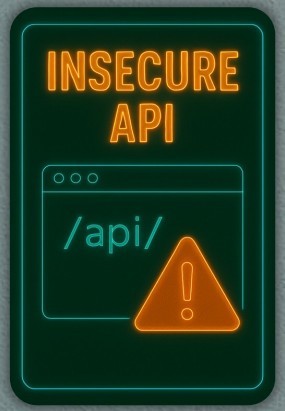
Critical client vulnerability

EOL library dependency



Critical API vulnerability

Insecure input handling

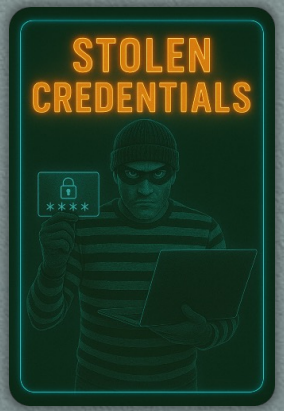


Company-signed malware

Unauthorized internal key exposure

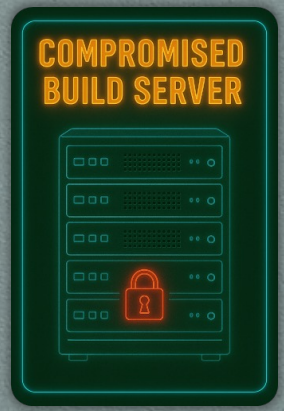
Suspicious login attempts

DevOps targeted phishing attempts



Suspicious child processes

Connections from unrecognized IPs




HORATIO CAINE

EVIDENCE

Critical client vulnerability

EOL library dependency

Malicious third-party code

Critical API vulnerability

Insecure input handling

Company-signed malware

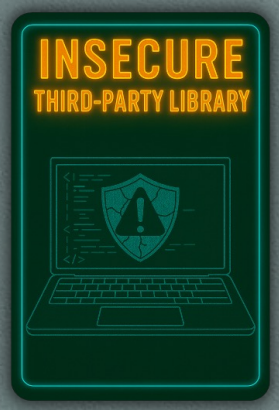
Unauthorized internal key exposure

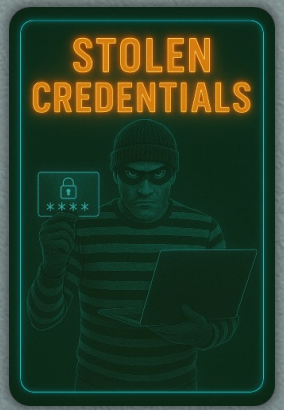
Suspicious login attempts

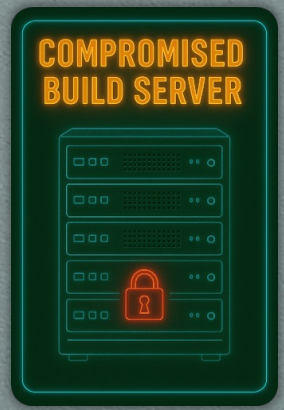
DevOps targeted phishing attempts

Suspicious child processes

Connections from unrecognized IPs







EVIDENCE

Critical client vulnerability

EOL library dependency

Malicious third-party code

Critical API vulnerability

Insecure input handling

Sensitive data disclosure

Company-signed malware

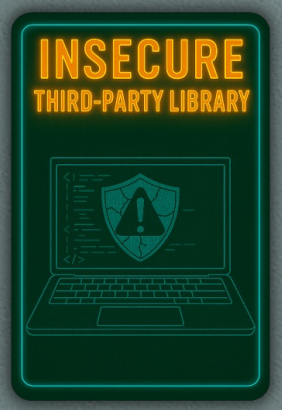
Unauthorized internal key exposure

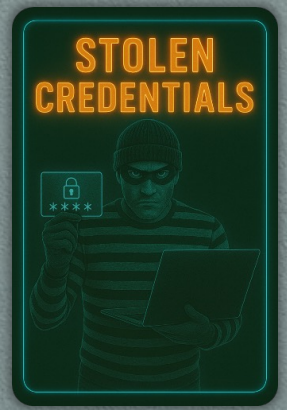
Suspicious login attempts

DevOps targeted phishing attempts

Suspicious child processes

Connections from unrecognized IPs





EVIDENCE

Critical client vulnerability

EOL library dependency

Malicious third-party code

Critical API vulnerability

Insecure input handling

Sensitive data disclosure

Company-signed malware

Unauthorized internal key exposure

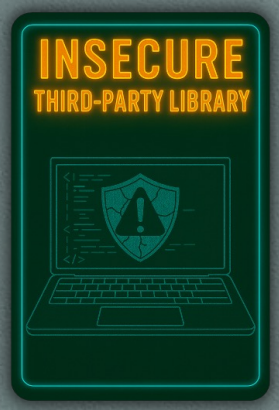
Suspicious signing activity

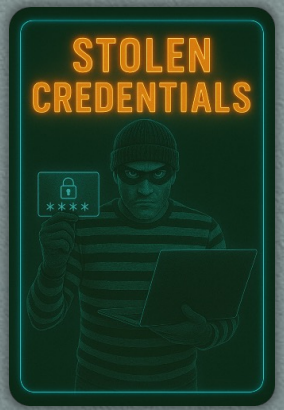
Suspicious login attempts

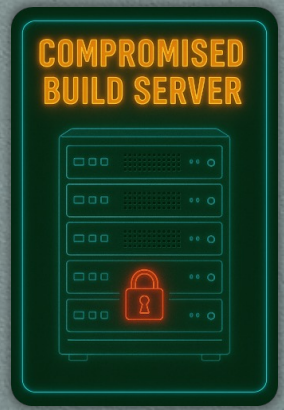
DevOps targeted phishing attempts

Suspicious child processes

Connections from unrecognized IPs

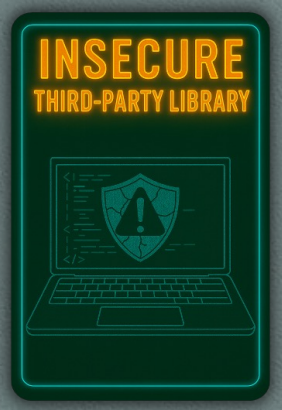


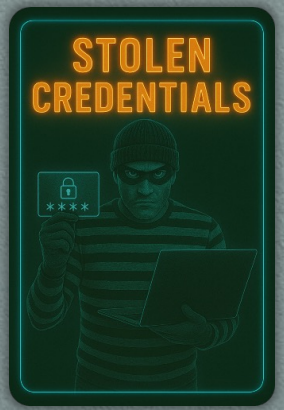


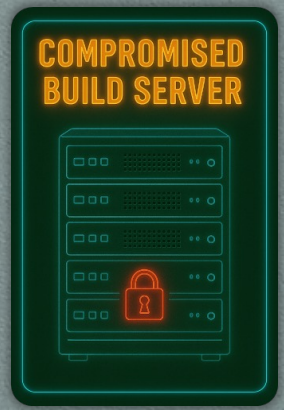


EVIDENCE

Critical client vulnerability	Critical API vulnerability	Company-signed malware	Suspicious login attempts	Suspicious child processes
EOL library dependency	Insecure input handling	Unauthorized internal key exposure	DevOps targeted phishing attempts	Connections from unrecognized IPs
Malicious third-party code	Sensitive data disclosure	Suspicious signing activity	Numerous password resets	

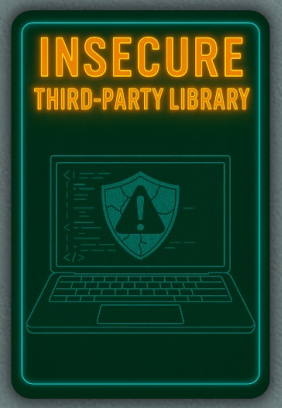


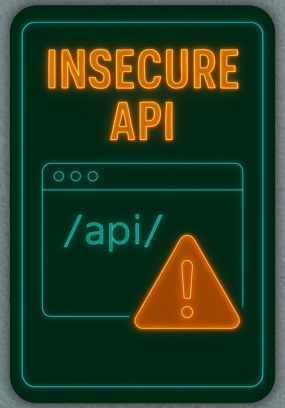


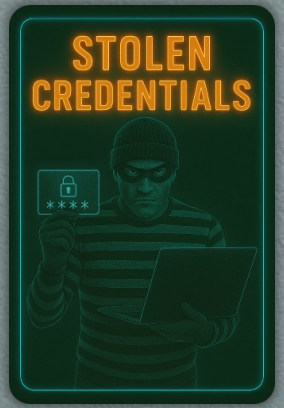


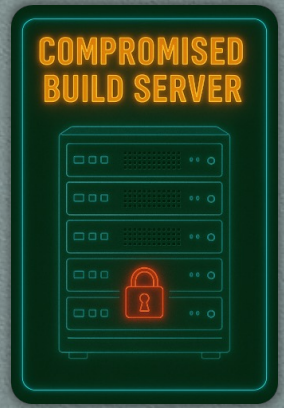
EVIDENCE

Critical client vulnerability	Critical API vulnerability	Company-signed malware	Suspicious login attempts	Suspicious child processes
EOL library dependency	Insecure input handling	Unauthorized internal key exposure	DevOps targeted phishing attempts	Connections from unrecognized IPs
Malicious third-party code	Sensitive data disclosure	Suspicious signing activity	Numerous password resets	MFA disabled for certain accounts





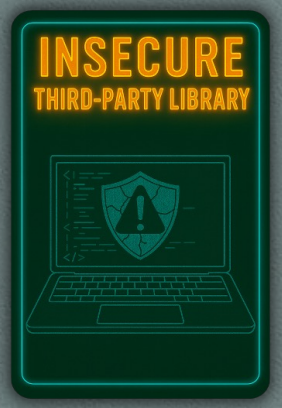


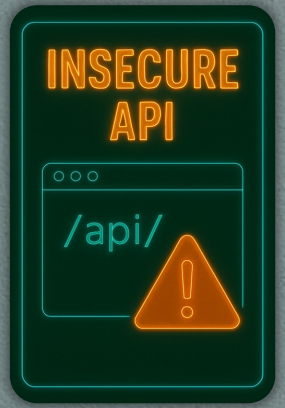


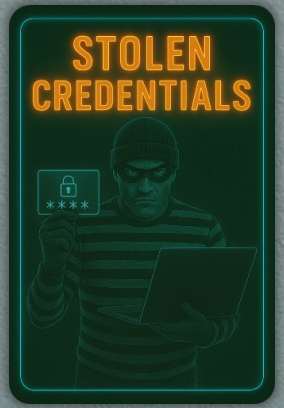
What was the likely main attack vector?

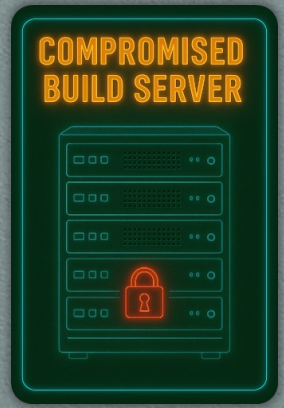
EVIDENCE

Critical client vulnerability	Critical API vulnerability	Company-signed malware	Suspicious login attempts	Suspicious child processes
EOL library dependency	Insecure input handling	Unauthorized internal key exposure	DevOps targeted phishing attempts	Connections from unrecognized IPs
Malicious third-party code	Sensitive data disclosure	Suspicious signing activity	Numerous password resets	MFA disabled for certain accounts









EVIDENCE

Critical API vulnerability

Insecure input handling

Sensitive data disclosure

Company-signed malware

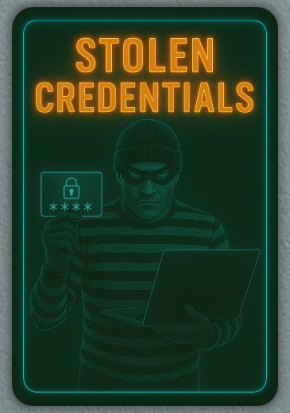
Unauthorized internal key exposure

Suspicious signing activity

Suspicious login attempts

DevOps targeted phishing attempts

Numerous password resets



Suspicious child processes

Connections from unrecognized IPs

MFA disabled for certain accounts

EVIDENCE

Company-signed malware

Suspicious login attempts

Suspicious child processes

Unauthorized internal key exposure

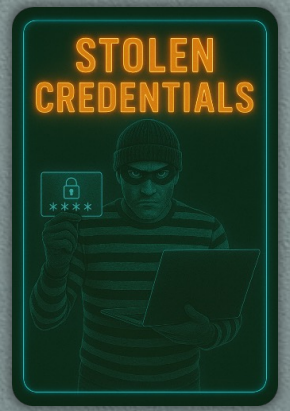
DevOps targeted phishing attempts

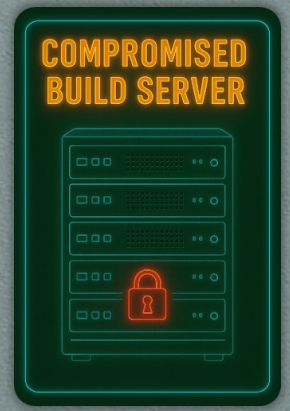
Connections from unrecognized IPs

Suspicious signing activity

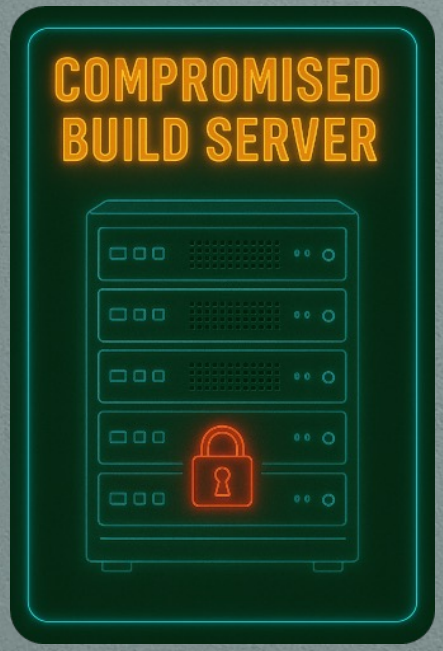
Numerous password resets

MFA disabled for certain accounts





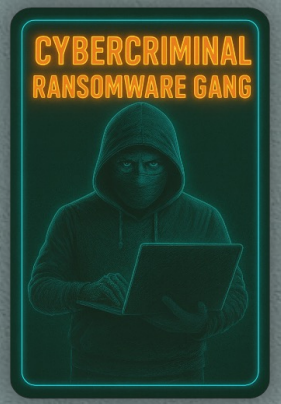
EVIDENCE




HORATIO CAINE

EVIDENCE

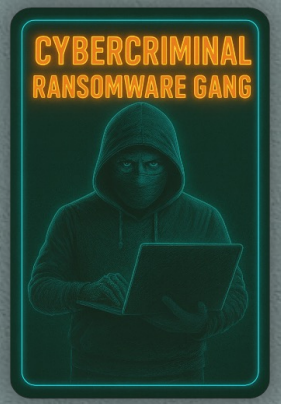
Suspicious Git activity



EVIDENCE

Suspicious Git activity

Ransomware fragments



EVIDENCE

Suspicious Git activity

Ransomware fragments

Overlapping APT signatures

EVIDENCE

Suspicious Git activity

Ransomware fragments

Overlapping APT signatures

Related social media chatter

EVIDENCE

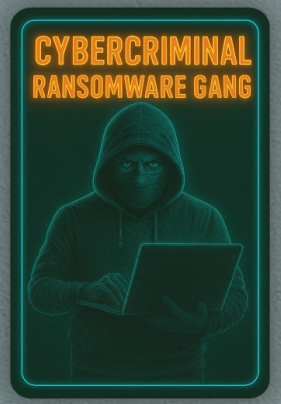
Suspicious Git activity

Ransomware fragments

Overlapping APT signatures

Related social media chatter

Vulnerability press leaks



Who is most likely the perpetrator?

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Ransomware fragments

Overlapping APT signatures

Related social media chatter

Vulnerability press leaks

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Ransomware fragments

Suspicious domain registrations

Overlapping APT signatures

Related social media chatter

Vulnerability press leaks

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Ransomware fragments

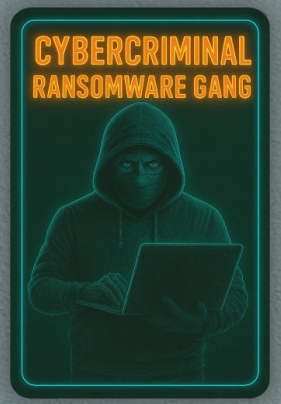
Suspicious domain registrations

Overlapping APT signatures

Outbound traffic to nation-state infrastructure

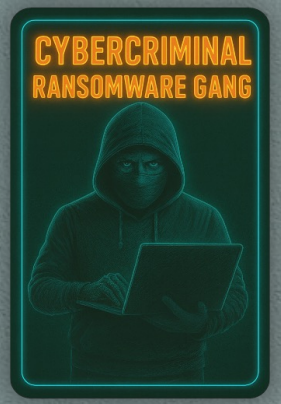
Related social media chatter

Vulnerability press leaks



EVIDENCE

Suspicious Git activity	Ransomware fragments	Overlapping APT signatures	Related social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans	



EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Ransomware fragments

Suspicious domain registrations

Overlapping APT signatures

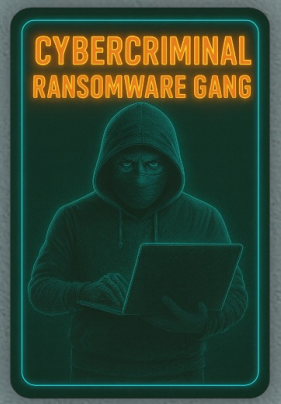
Outbound traffic to nation-state infrastructure

Related social media chatter

Malware artifacts with ideological slogans

Vulnerability press leaks

Performance degradation code



EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Suspicious domain registrations

Overlapping APT signatures

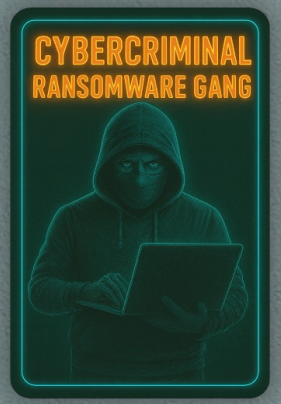
Outbound traffic to nation-state infrastructure

Related social media chatter

Malware artifacts with ideological slogans

Vulnerability press leaks

Performance degradation code



EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Suspicious domain registrations

Ransomware note snippets

Overlapping APT signatures

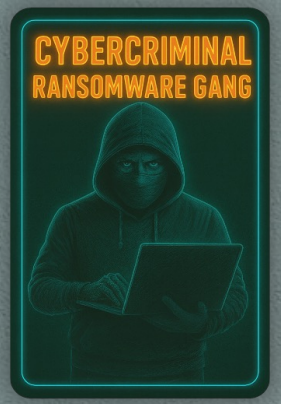
Outbound traffic to nation-state infrastructure

Related social media chatter

Malware artifacts with ideological slogans

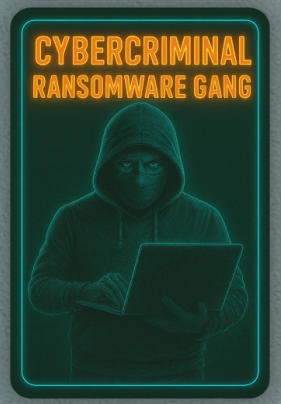
Vulnerability press leaks

Performance degradation code



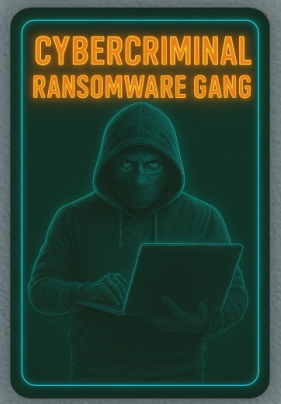
EVIDENCE

Suspicious Git activity	Ransomware fragments	Overlapping APT signatures	Related social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans	Performance degradation code
Unrevoked admin rights	Ransomware note snippets	Highly-tailored phishing emails		



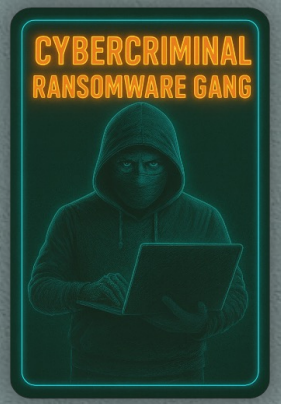
EVIDENCE

Suspicious Git activity	Ransomware fragments	Overlapping APT signatures	Related social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans	Performance degradation code
Unrevoked admin rights	Ransomware note snippets	Highly-tailored phishing emails	Defacement functionality	



EVIDENCE

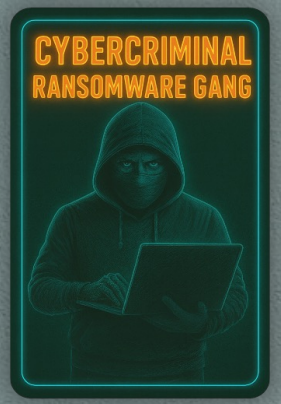
Suspicious Git activity	Ransomware fragments	Overlapping APT signatures	Related social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans	Performance degradation code
Unrevoked admin rights	Ransomware note snippets	Highly-tailored phishing emails	Defacement functionality	Package hash mismatch



Who is most likely the perpetrator?

EVIDENCE

Suspicious Git activity	Ransomware fragments	Overlapping APT signatures	Related social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans	Performance degradation code
Unrevoked admin rights	Ransomware note snippets	Highly-tailored phishing emails	Defacement functionality	Package hash mismatch



EVIDENCE

Suspicious Git activity	Ransomware fragments	Overlapping APT signatures	Related social media chatter
Code commits from dormant accounts	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans
Unrevoked admin rights	Ransomware note snippets	Highly-tailored phishing emails	Defacement functionality

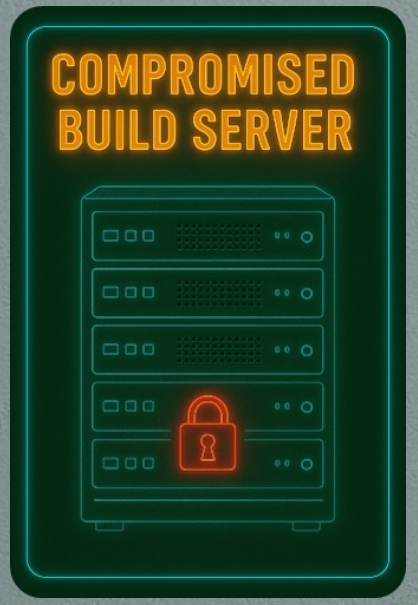

HORATIO CAINE

EVIDENCE

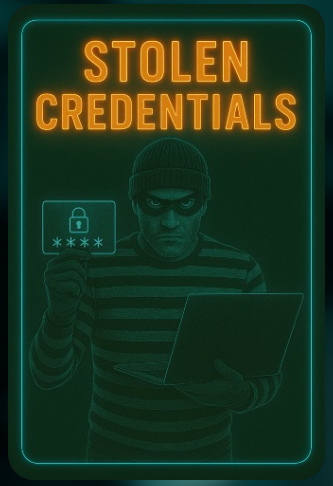
Ransomware fragments	Overlapping APT signatures	Related social media chatter
Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Malware artifacts with ideological slogans
Ransomware note snippets	Highly-tailored phishing emails	Defacement functionality

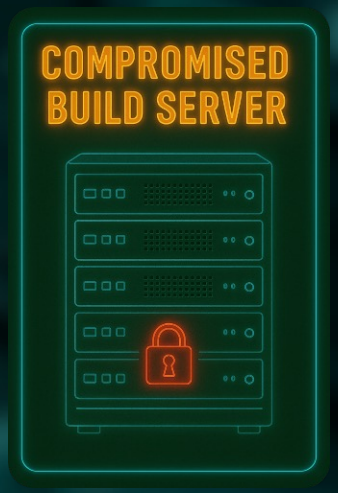
EVIDENCE

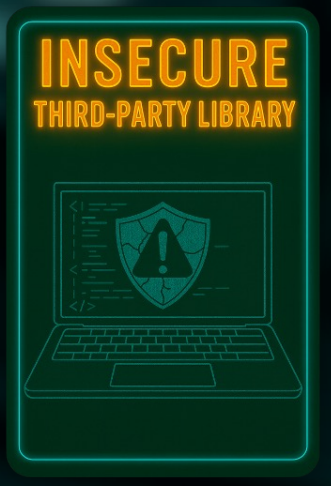
EVIDENCE



Potential Attacks and Attackers







PCI Software Security Framework

Overview

Secure Software Standard

- Requirements for ensuring software products sufficiently protect their sensitive assets*

Secure Software Lifecycle Standard

- Requirements for ensuring software providers design, develop, maintain, and operate** their software in a secure manner

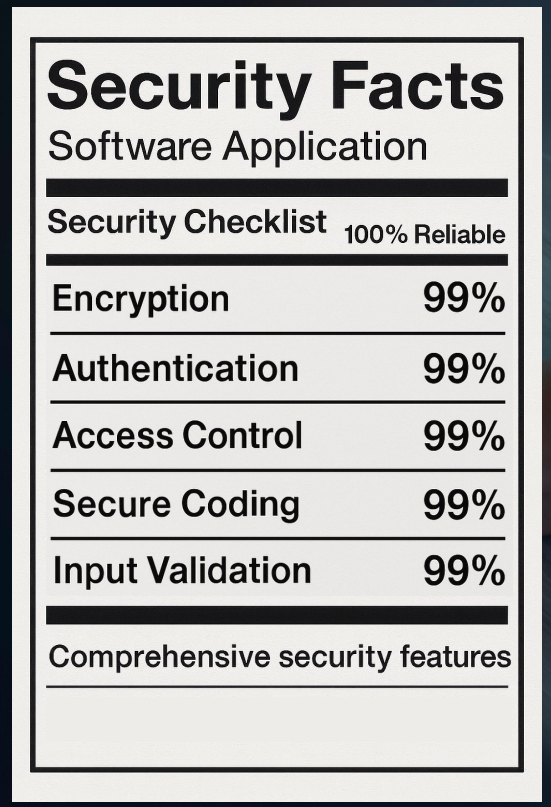
Associated Validation and Listing Programs

- Assessments and assessors
- Listings
- Supporting materials, templates, guidance, etc.

* Term and scope is defined in the Standard.
** Where all or some of software operations are managed by the software provider.

PCI Software Security Framework

Listings

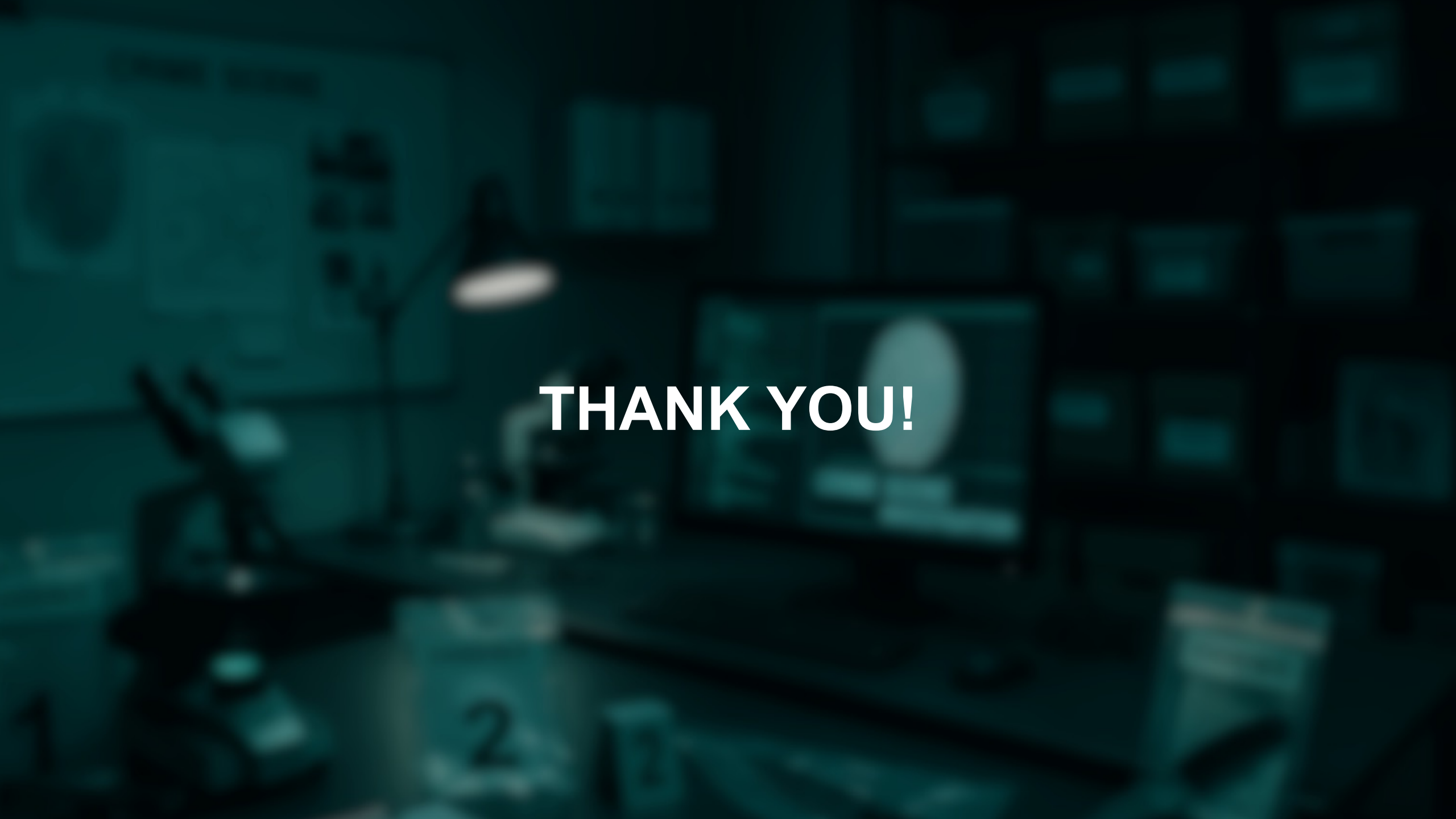



UPDATE
2.0


DIGITAL
ASSETS


Search
UPDATE.....


Software@pcisecuritystandards.org


THANK YOU!

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING