CSC 405
Why Security?

Aleksandr Nahapetyan
anahape@ncsu.edu
(Slides adapted from Dr. Kapravelos)

Game Plan

01/12: Intro / Why Security

01/14: Primer on computer architecture and assembly

01/19: No class, university is closed

01/21: Software patching

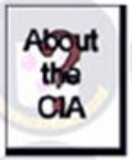
Welcome to the Central Stupidity Agency

We'd just like to say one thing.. And that's:

STOP LYING BO SKARINDER!!!

SLUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below:



Power Through Resistance would like to say: **FUCK YOU!** to the Central Intelligence Agency World Wide Web site you're all lame assholes.

Nowthisisalittletextofsystemvirusspawninginsecunitychamberstomakeallipsdieinstantly.....

never has so few braincells done so little for no one...

- The Swedish Hackers Association Protocol #3 - SHA Protocol #3.
- The Swedish Hackers Association Protocol #4 - SHA Protocol #4.
- Flashback - The Flashback.
- Subway - The Underground
- Other Intelligence Community Links - Other Web sites of interest.

This site was hacked by **Power Through Resistance**

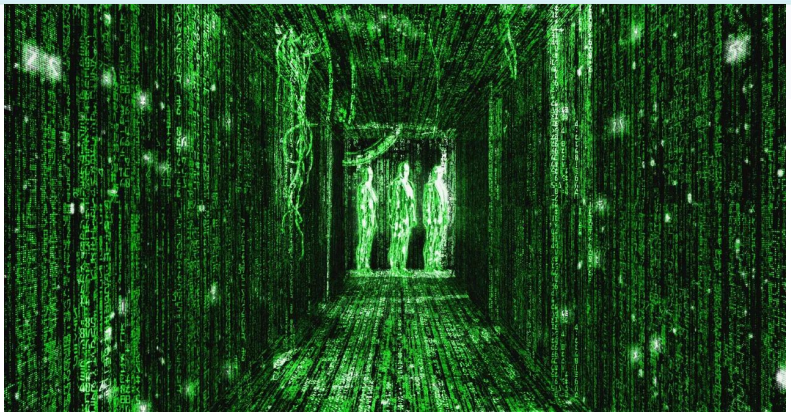
First time CIA.gov was defaced in 1996

Everyone is Getting Hacked, All the Time

Maybe put a firewall on that Minecraft server

The computer security problem

- Security is everywhere
- Developers are not aware of security (we should fix this!)
  - Buggy software
  - Legacy software
  - Social engineering
- Vulnerabilities can be very damaging (and expensive)
- There is financial incentive in finding and exploiting vulnerable systems



Black market for exploits

Last iOS exploit was sold for
more than 1 million dollars!

Hacking used to be cool

But now everything is done for profit!

Listed for $200,000

source

Twitter - DB/Scrape Leak 200+Mill Lines
by StayMad - Wednesday January 4, 2023 at 12:04 AM

StayMad

GOD User

GOD

Posts: 2
Threads: 1

Today, 12:04 AM (This post was last modified: 11 hours ago by pompompurin.) #1

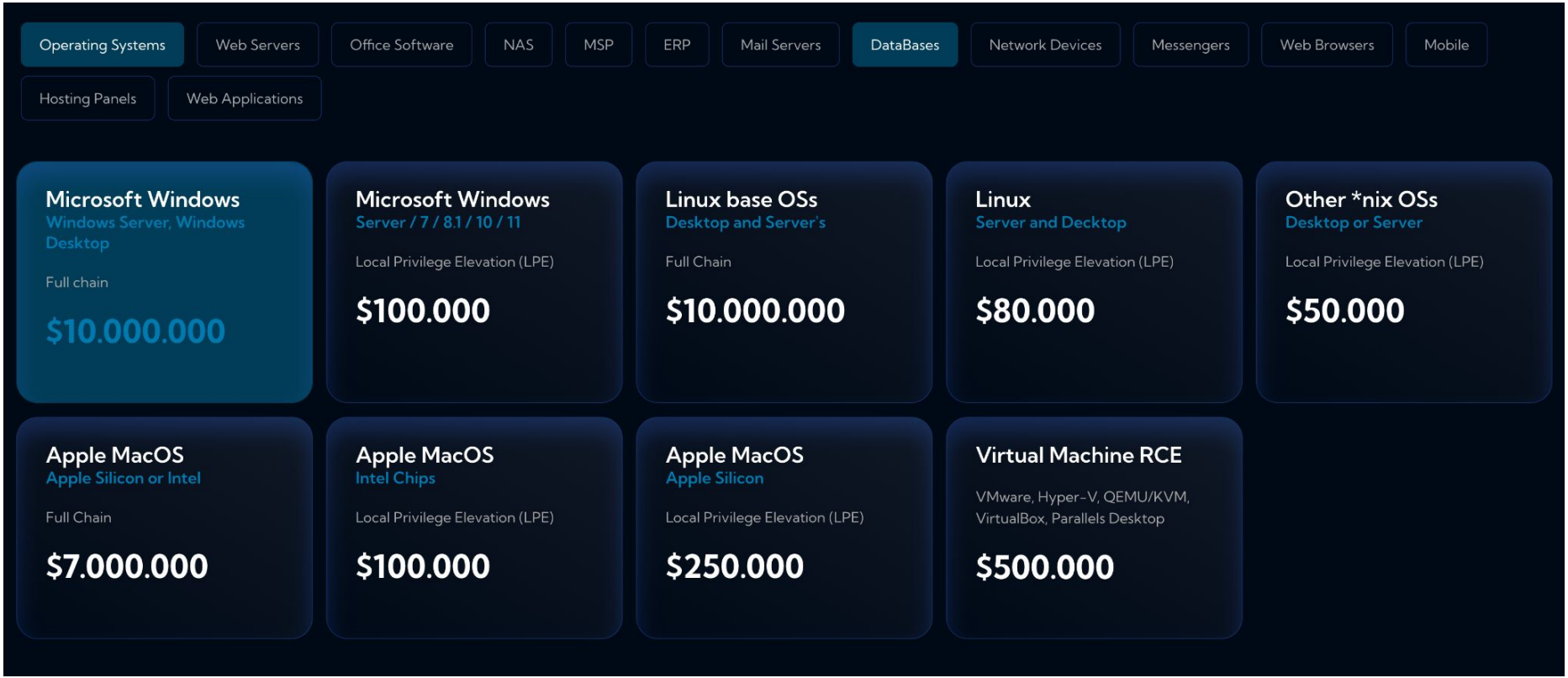
Twitter 200+ m DB/Scrape

Sample Format

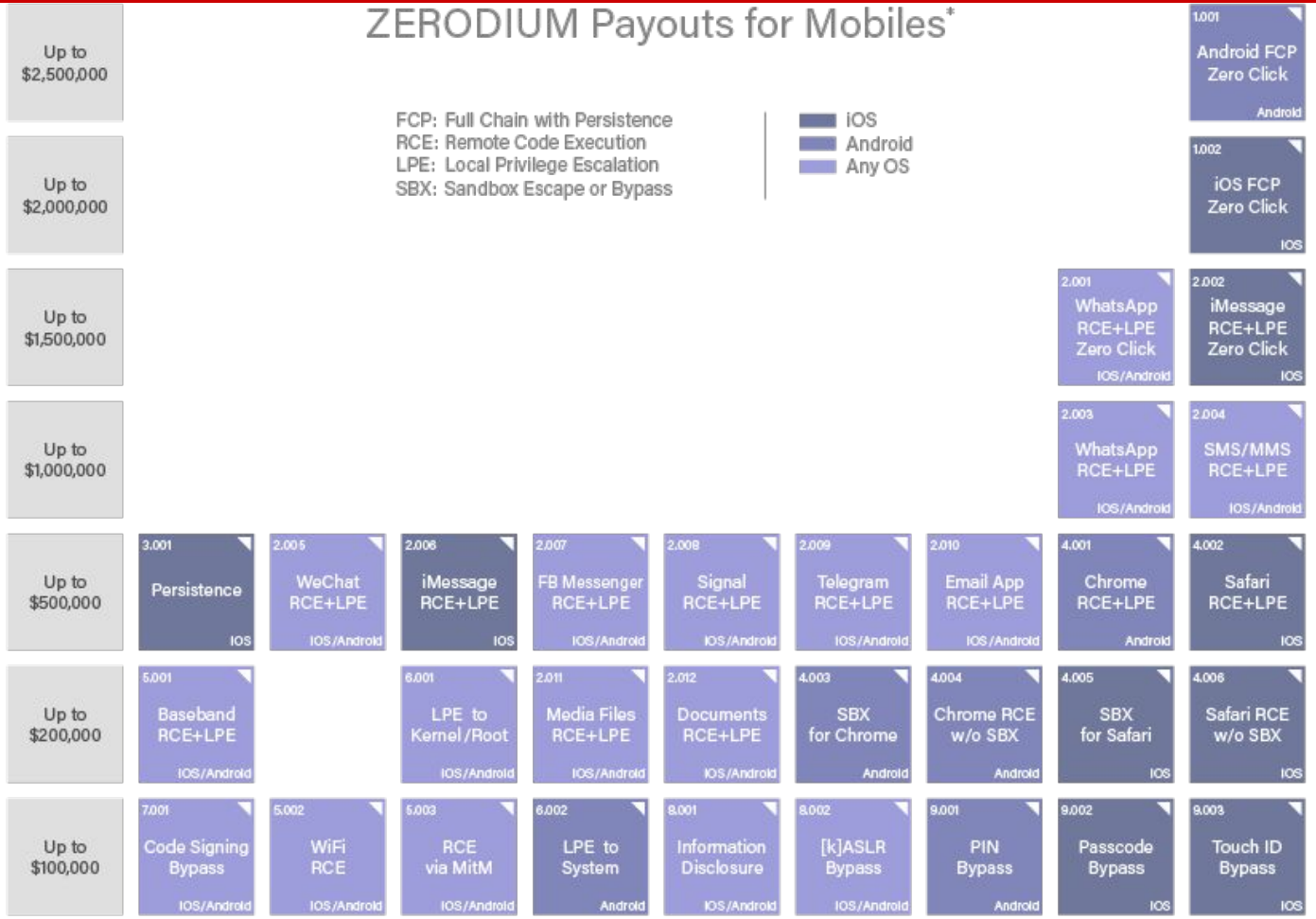
Quote:

Email:[redacted] - Name:[redacted] - ScreenName:[redacted] - Followers:[redacted] - Created At:[redacted]
2013
Email:[redacted] - Name:[redacted] - ScreenName:[redacted] - Followers:[redacted] - Created At:[redacted]
Email:[redacted] - Name:[redacted] - ScreenName:[redacted] - Followers:[redacted] - Created At:[redacted]

List of 100k Verified Accounts


Operating Systems
Web Servers
Office Software
NAS
MSP
ERP
Mail Servers
DataBases
Network Devices
Messengers
Web Browsers
Mobile
Hosting Panels
Web Applications
Microsoft Windows
Windows Server, Windows Desktop
Full chain
$10.000.000
Microsoft Windows
Server / 7 / 8.1 / 10 / 11
Local Privilege Elevation (LPE)
$100.000
Linux base OSs
Desktop and Server's
Full Chain
$10.000.000
Linux
Server and Decktop
Local Privilege Elevation (LPE)
$80.000
Other *nix OSs
Desktop or Server
Local Privilege Elevation (LPE)
$50.000
Apple MacOS
Apple Silicon or Intel
Full Chain
$7.000.000
Apple MacOS
Intel Chips
Local Privilege Elevation (LPE)
$100.000
Apple MacOS
Apple Silicon
Local Privilege Elevation (LPE)
$250.000
Virtual Machine RCE
VMware, Hyper-V, QEMU/KVM, VirtualBox, Parallels Desktop
$500.000

source

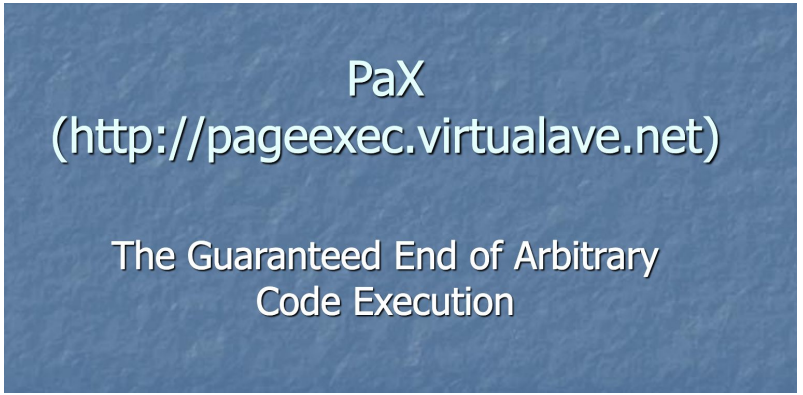


** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/09 © zerodium.com

Security is fun! And complicated!

- Offensive security is fun!
  - Find a way to break the software
  - Leverage the break for something
- Defenses are rarely perfect
  - PaX in 2001 was meant to end arbitrary code execution (ACE)
  - Spoiler: It was not a guaranteed end for ACE, but it definitely got harder
  - Did you see Unity games pushing an update to “Fix Unity runtime vulnerability”



CVE-2025-59489: Arbitrary Code Execution in Unity Runtime

Posted on October 3, 2025 • 6 minutes • 1072 words

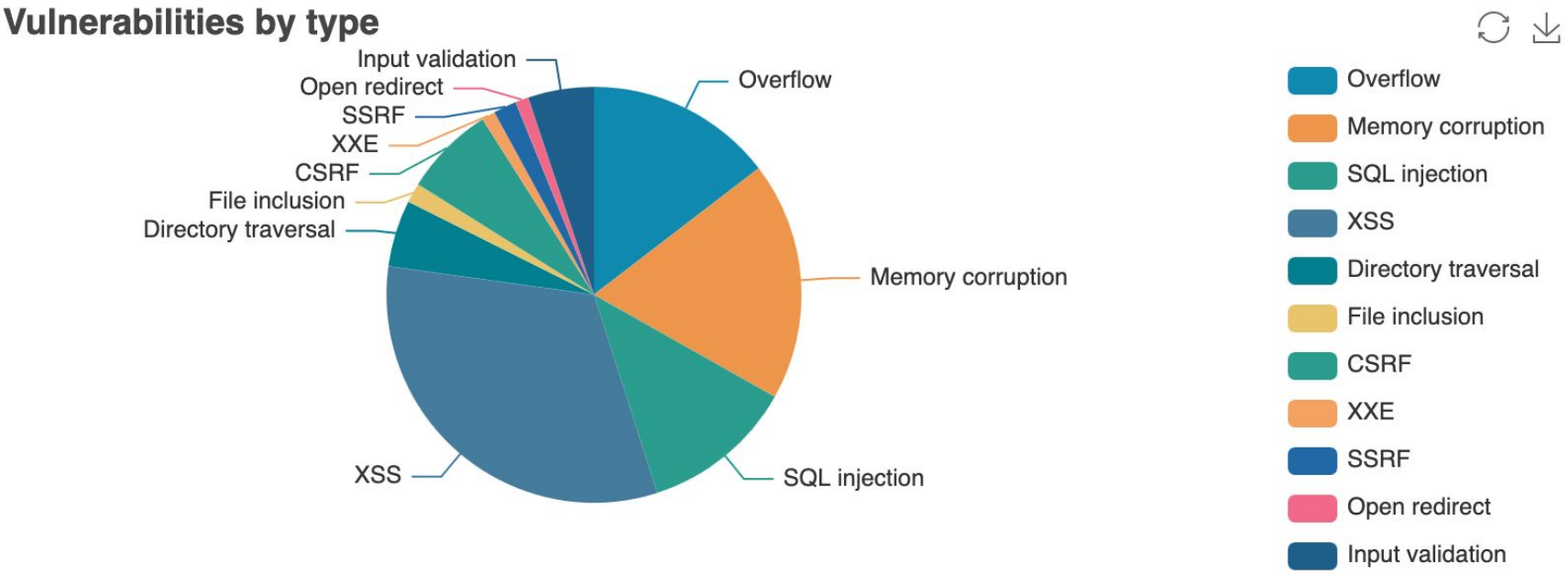
Table of contents

Vulnerabilities per product - as of 2026

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Linux Kernel	Linux	OS	13543
2	Debian Linux	Debian	OS	9715
3	Android	Google	OS	7890
4	Fedora	Fedoraproject	OS	5347
5	Windows Server 2016	Microsoft	OS	4388
6	Ubuntu Linux	Canonical	OS	4107
7	Windows Server 2019	Microsoft	OS	4066
8	Iphone Os	Apple	OS	3843
9	Chrome	Google	Application	3764
10	Windows Server 2012	Microsoft	OS	3657

source: https://www.cvedetails.com/top-50-products.php?year=0

Vulnerabilities per type - 2025



source: https://www.cvedetails.com/vulnerabilities-by-types.php

https://owasp.org/Top10/

OWASP Top 10 for LLM Applications 2025

1. Prompt Injection
2. Sensitive Information Disclosure
3. Supply Chain Risks
4. Data and Model Poisoning
5. Improper Output Handling
6. Excessive Agency
7. System Prompt Leakage
8. Vector and Embedding Weaknesses
9. Misinformation
10. Unbounded Consumption

source: https://genai.owasp.org/download/43299/

Bug bounty programs

- Companies will pay you money to report vulnerabilities
- Certain conditions and rules per program
  - No Denial-of-service attacks
  - Spam
  - … (depends on the program)
- l1ackerone
  - https://hackerone.com/hacktivity
- Intigriti
  - https://www.intigriti.com/

Exploits for modern software are extremely difficult to write!

Operation Triangulation' attack chain

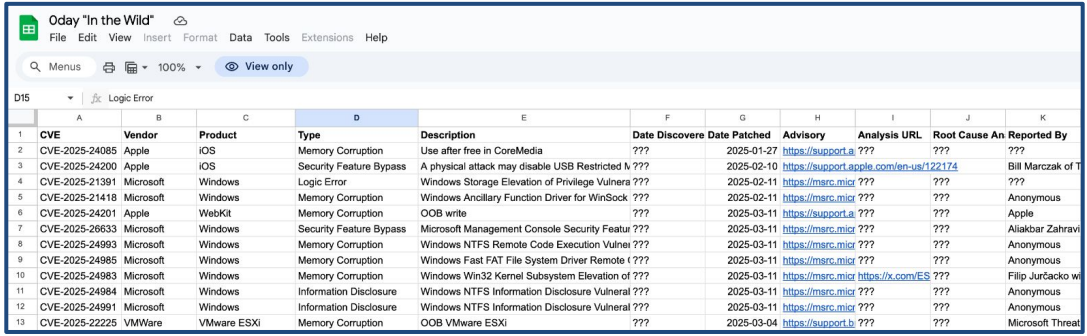
0-click iMessage attack
used four zero-days

Zero-days? N-days? 0-click?

- Vulnerability is a bug with security implications
- Exploit leverages that bug for some kind of a gain
- 0-day exploit: 0 days since a patch! Scary!
- N-days exploit: Vulnerability has been patched, and y'all keep things up to date, right?
- 0-click: no user interaction required!

THREAT ANALYSIS GROUP

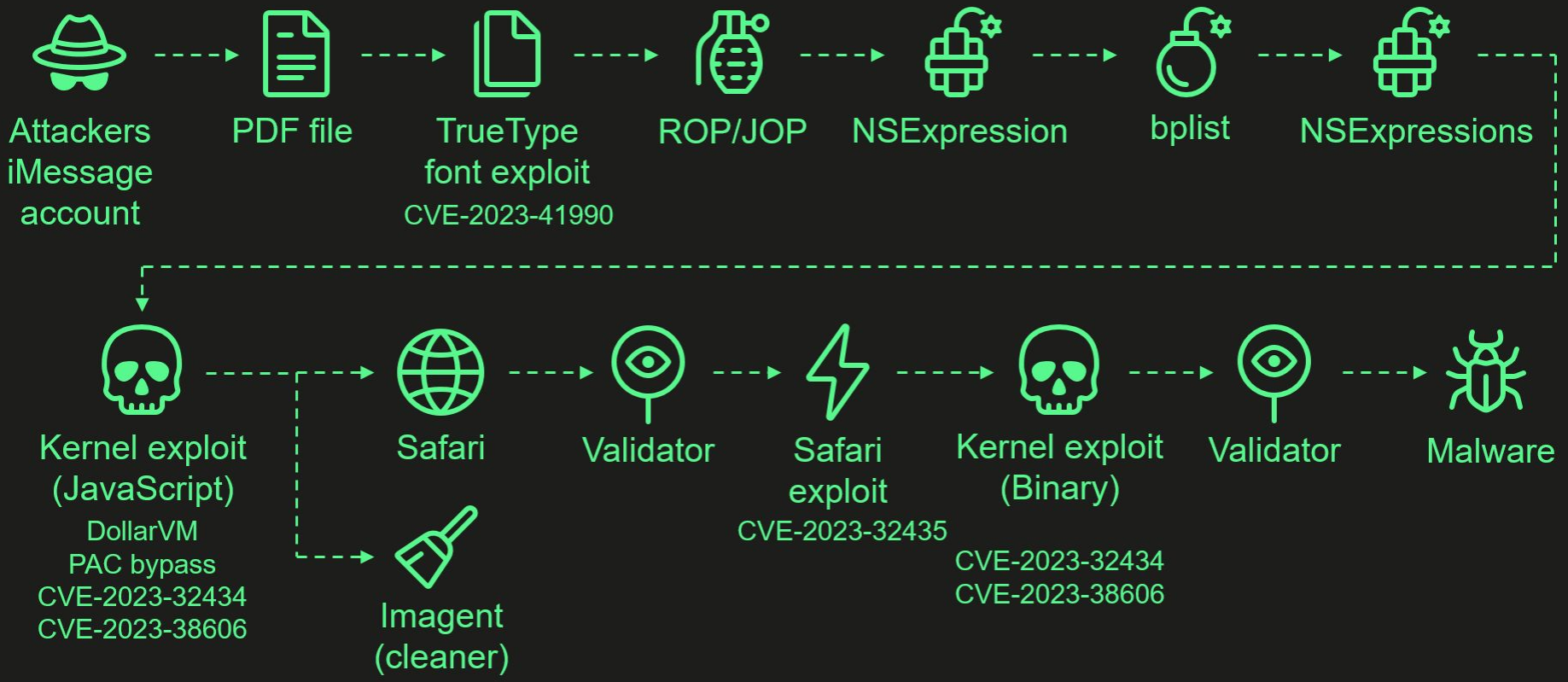
Spyware vendors use 0-days and n-days against popular platforms



	A	B	C	D	E	F	G	H	I	J	K
1	CVE	Vendor	Product	Type	Description	Date Discovere	Date Patched	Advisory	Analysis URL	Root Cause An	Reported By
2	CVE-2025-24085	Apple	iOS	Memory Corruption	Use after free in CoreMedia	???	2025-01-27	https://support.a	???	???	???
3	CVE-2025-24200	Apple	iOS	Security Feature Bypass	A physical attack may disable USB Restricted M	???	2025-02-10	https://support.apple.com/en-us/122174			Bill Marczak of T
4	CVE-2025-21391	Microsoft	Windows	Logic Error	Windows Storage Elevation of Privilege Vulnera	???	2025-02-11	https://msrc.micr	???	???	???
5	CVE-2025-21418	Microsoft	Windows	Memory Corruption	Windows Ancillary Function Driver for WinSock	???	2025-02-11	https://msrc.micr	???	???	Anonymous
6	CVE-2025-24201	Apple	WebKit	Memory Corruption	OOB write	???	2025-03-11	https://support.a	???	???	Apple
7	CVE-2025-26633	Microsoft	Windows	Security Feature Bypass	Microsoft Management Console Security Featur	???	2025-03-11	https://msrc.micr	???	???	Aliakbar Zahravi
8	CVE-2025-24993	Microsoft	Windows	Memory Corruption	Windows NTFS Remote Code Execution Vulner	???	2025-03-11	https://msrc.micr	???	???	Anonymous
9	CVE-2025-24985	Microsoft	Windows	Memory Corruption	Windows Fast FAT File System Driver Remote (	???	2025-03-11	https://msrc.micr	???	???	Anonymous
10	CVE-2025-24983	Microsoft	Windows	Memory Corruption	Windows Win32 Kernel Subsystem Elevation of	???	2025-03-11	https://msrc.micr	https://x.com/ES	???	Filip Jurčacko wi
11	CVE-2025-24984	Microsoft	Windows	Information Disclosure	Windows NTFS Information Disclosure Vulneral	???	2025-03-11	https://msrc.micr	???	???	Anonymous
12	CVE-2025-24991	Microsoft	Windows	Information Disclosure	Windows NTFS Information Disclosure Vulneral	???	2025-03-11	https://msrc.micr	???	???	Anonymous
13	CVE-2025-22225	VMWare	VMware ESXi	Memory Corruption	OOB VMware ESXi	???	2025-03-04	https://support.b	???	???	Microsoft Threat

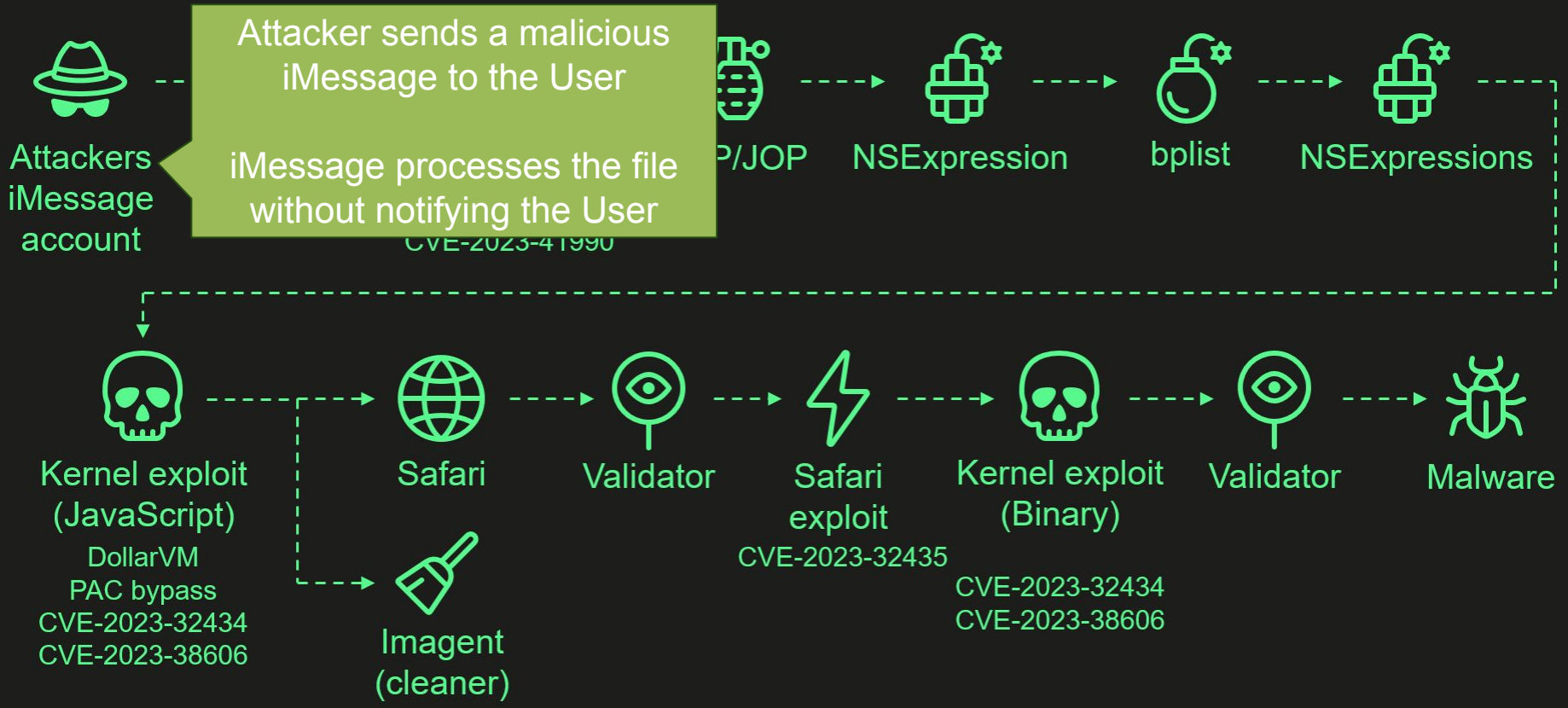
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



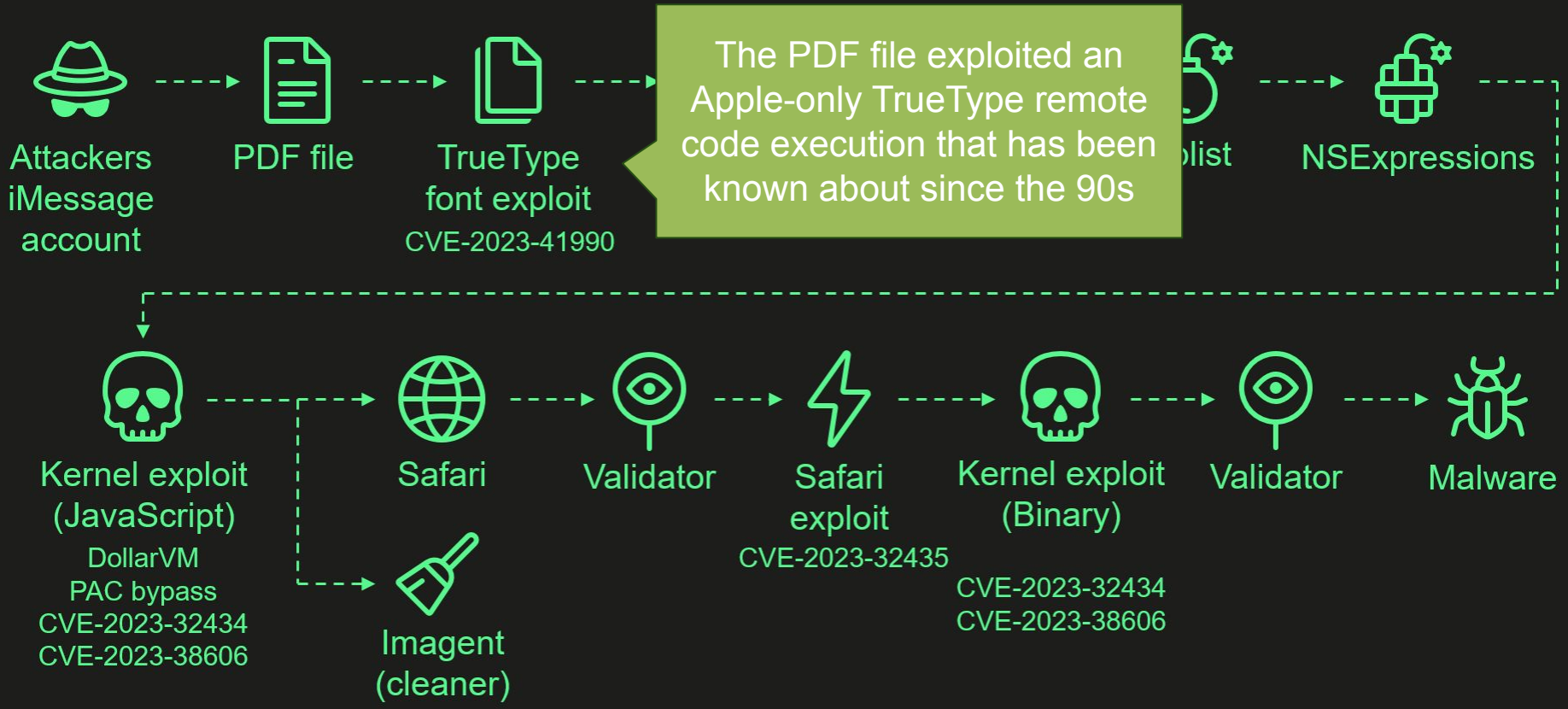
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



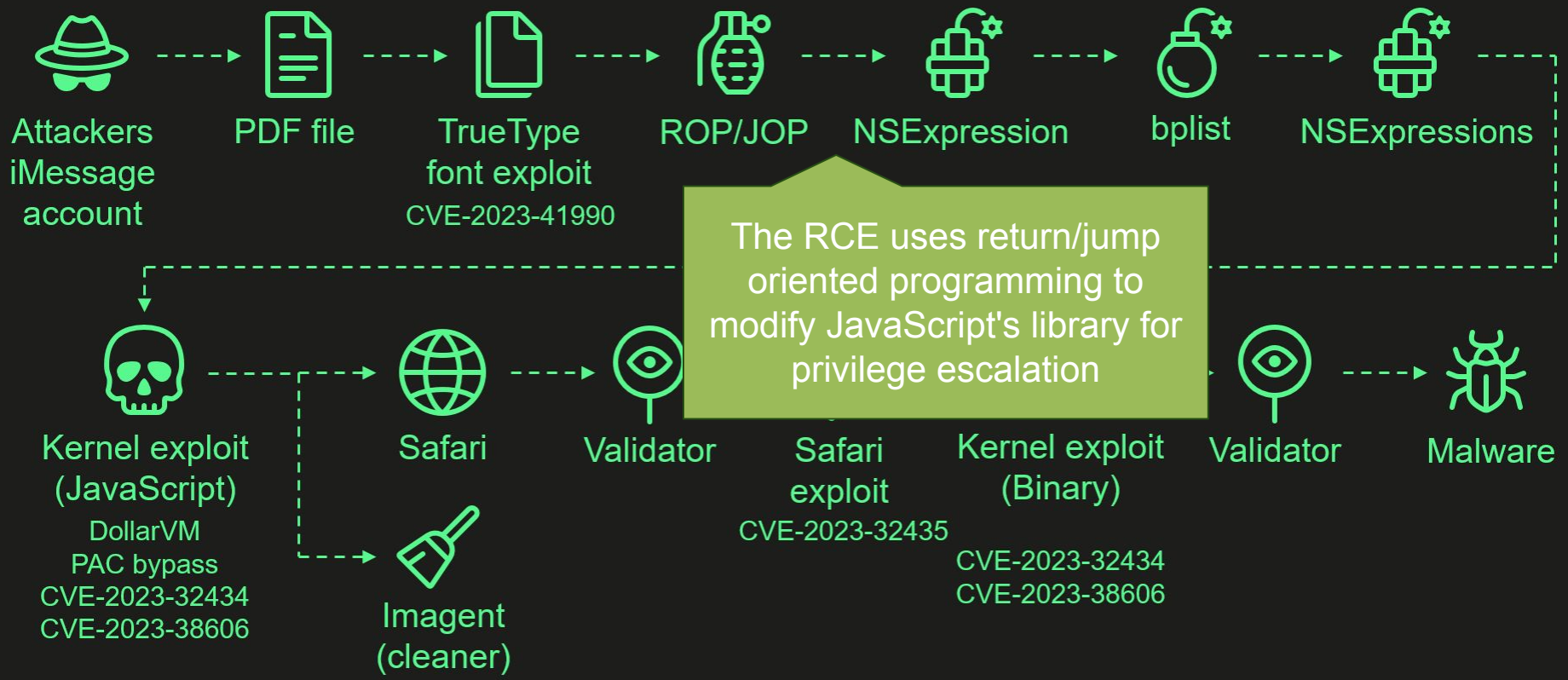
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



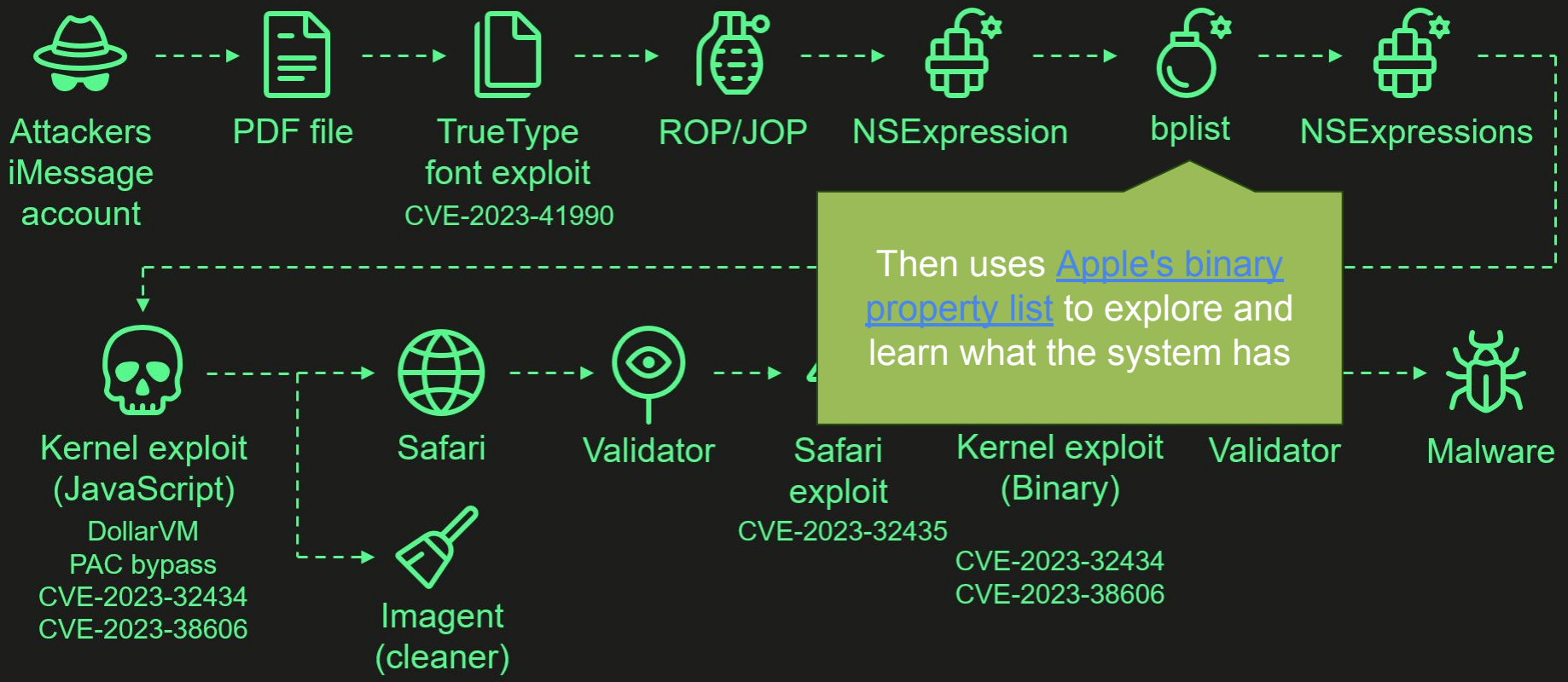
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



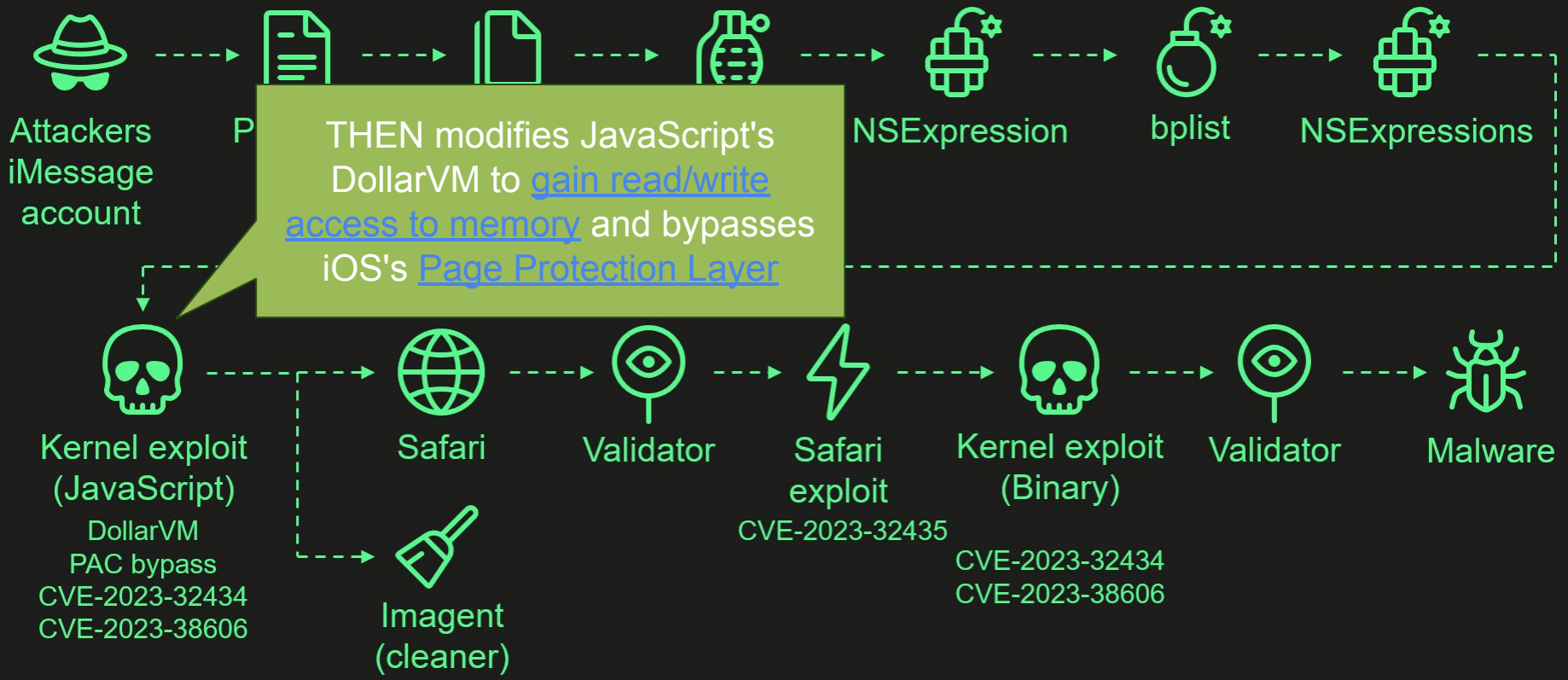
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



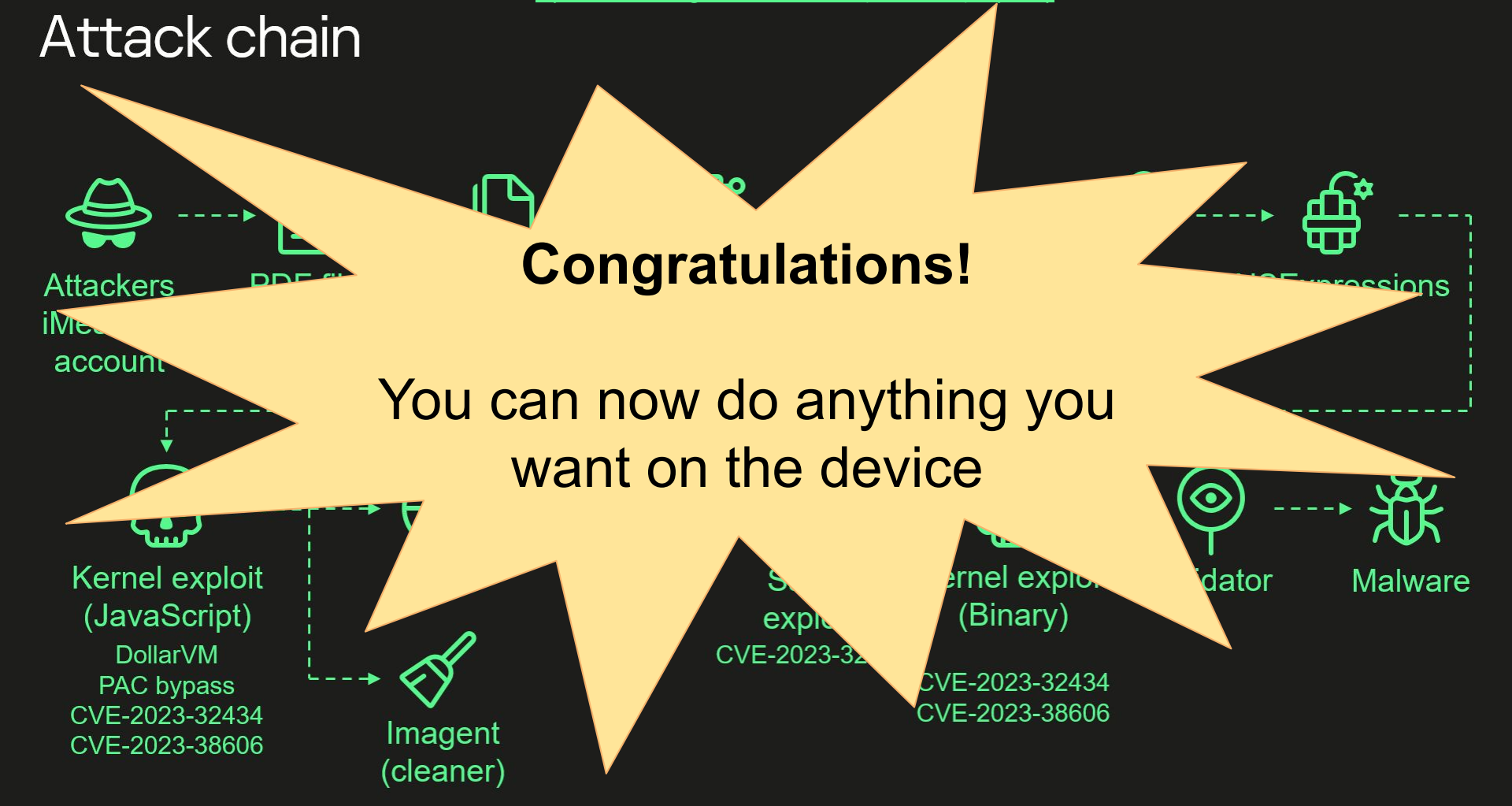
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



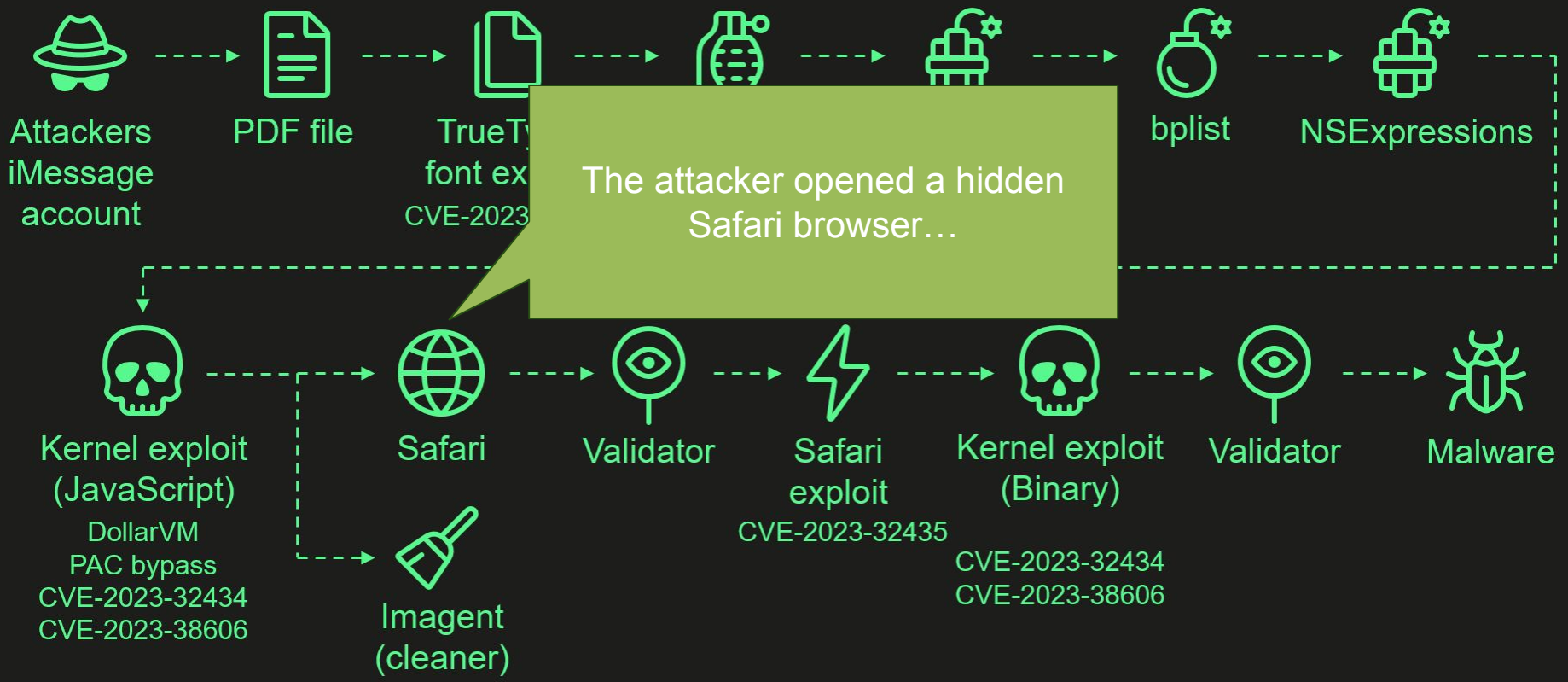
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



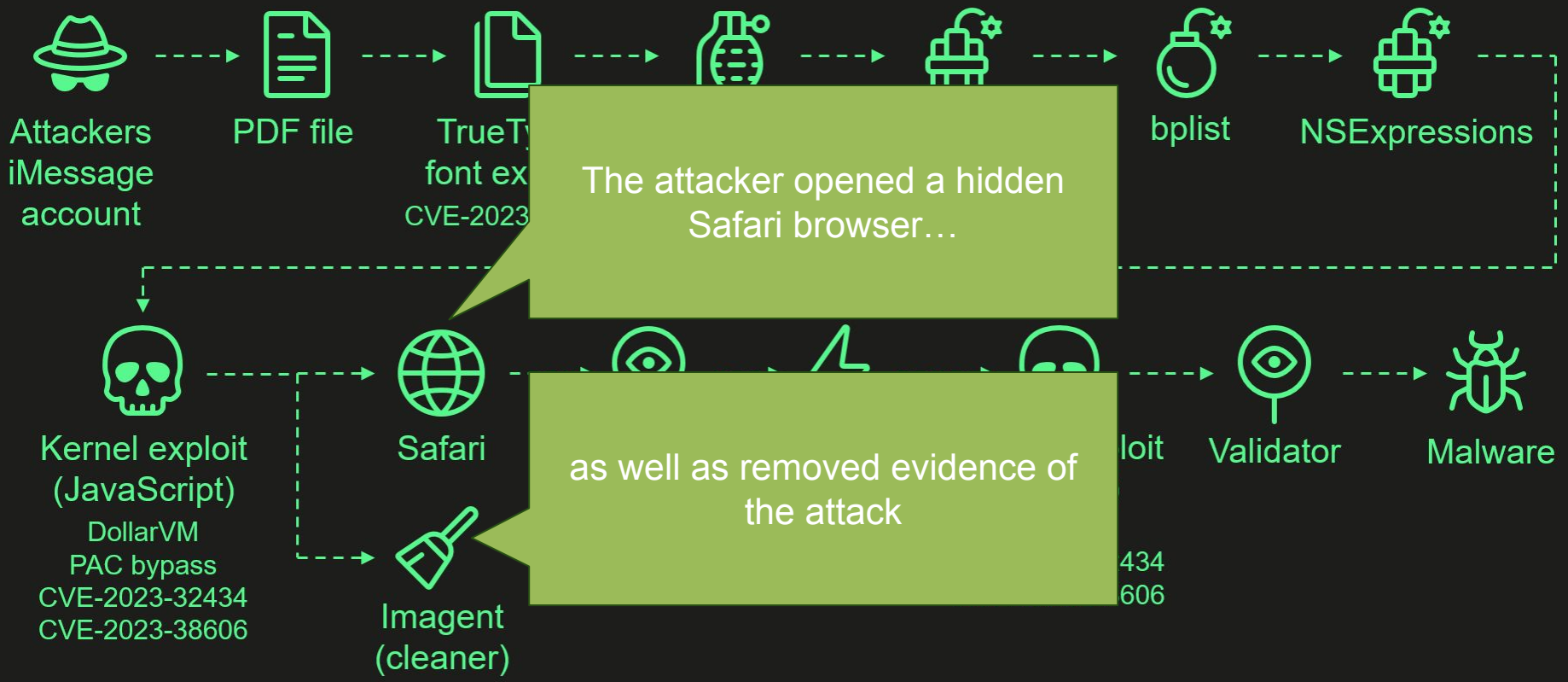
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



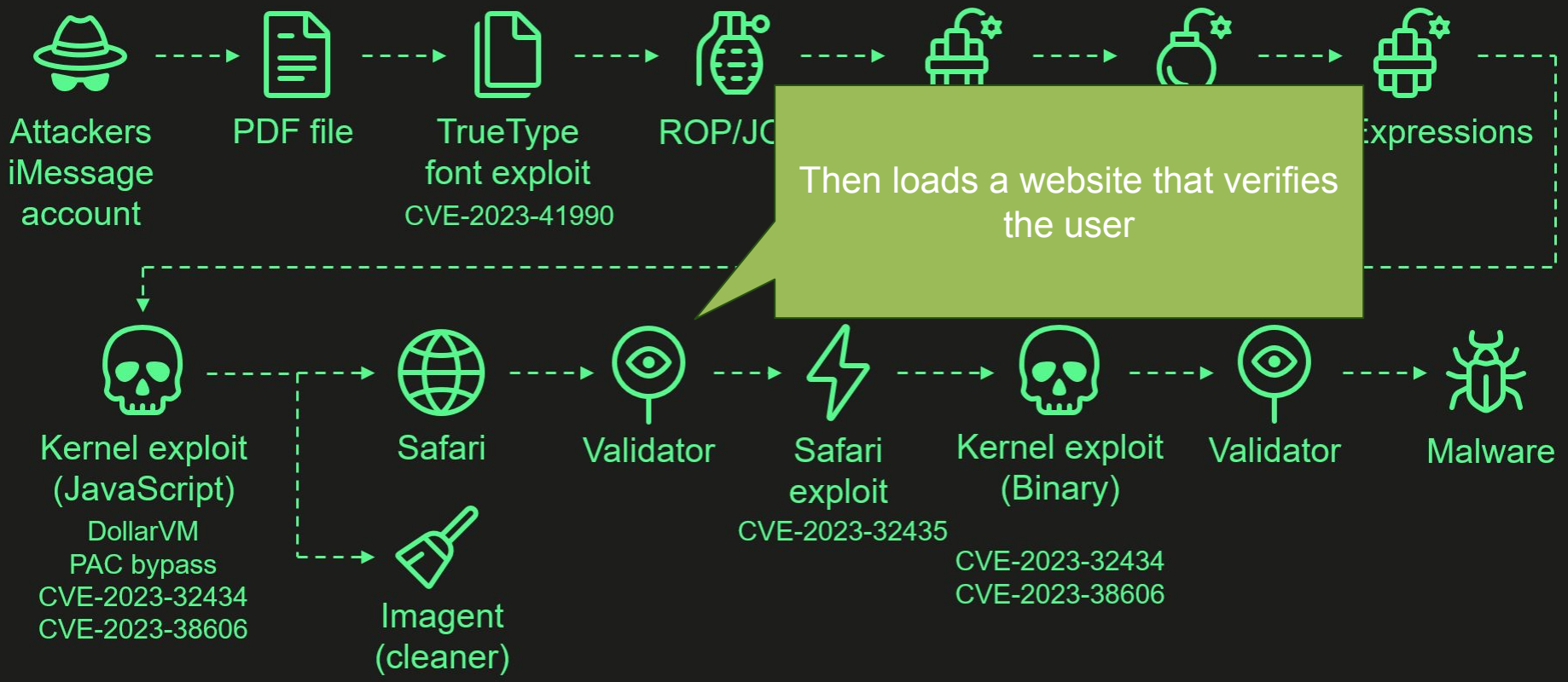
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



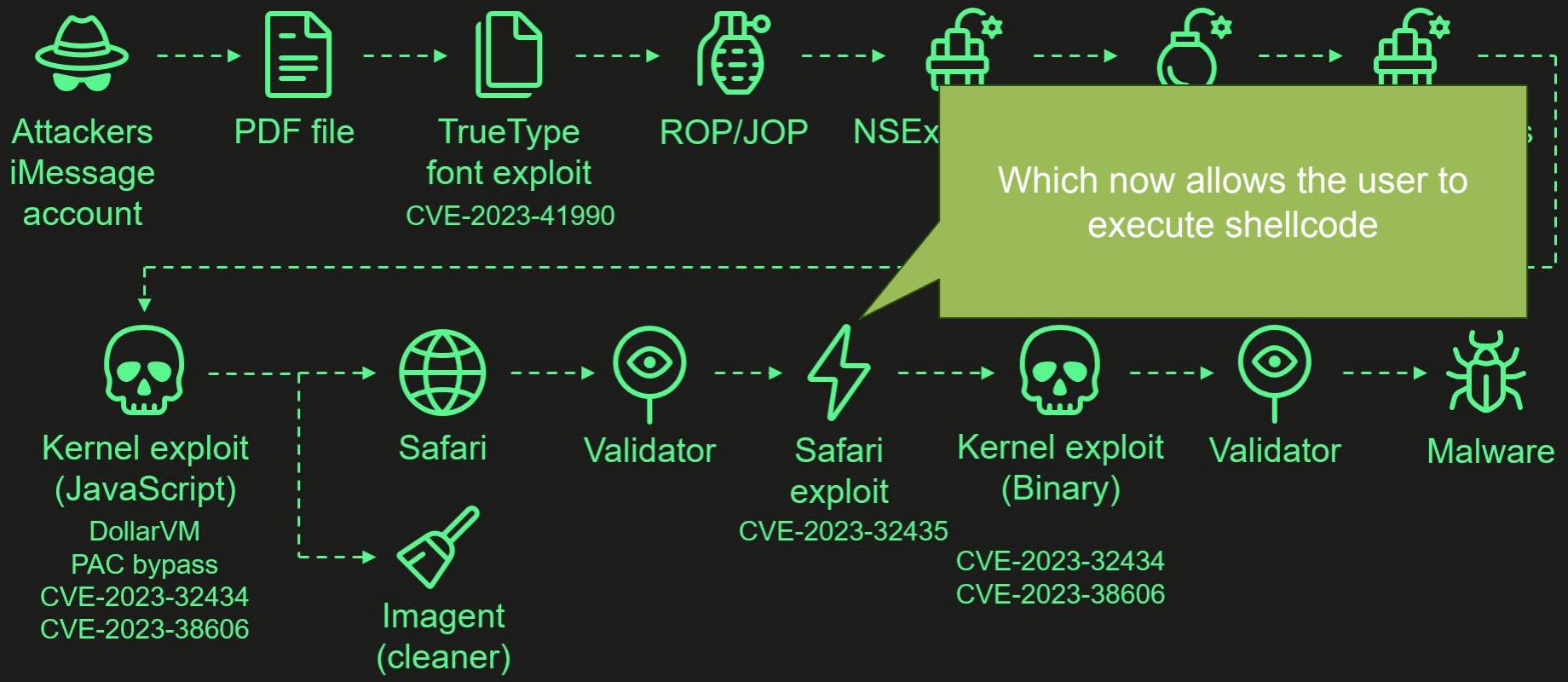
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



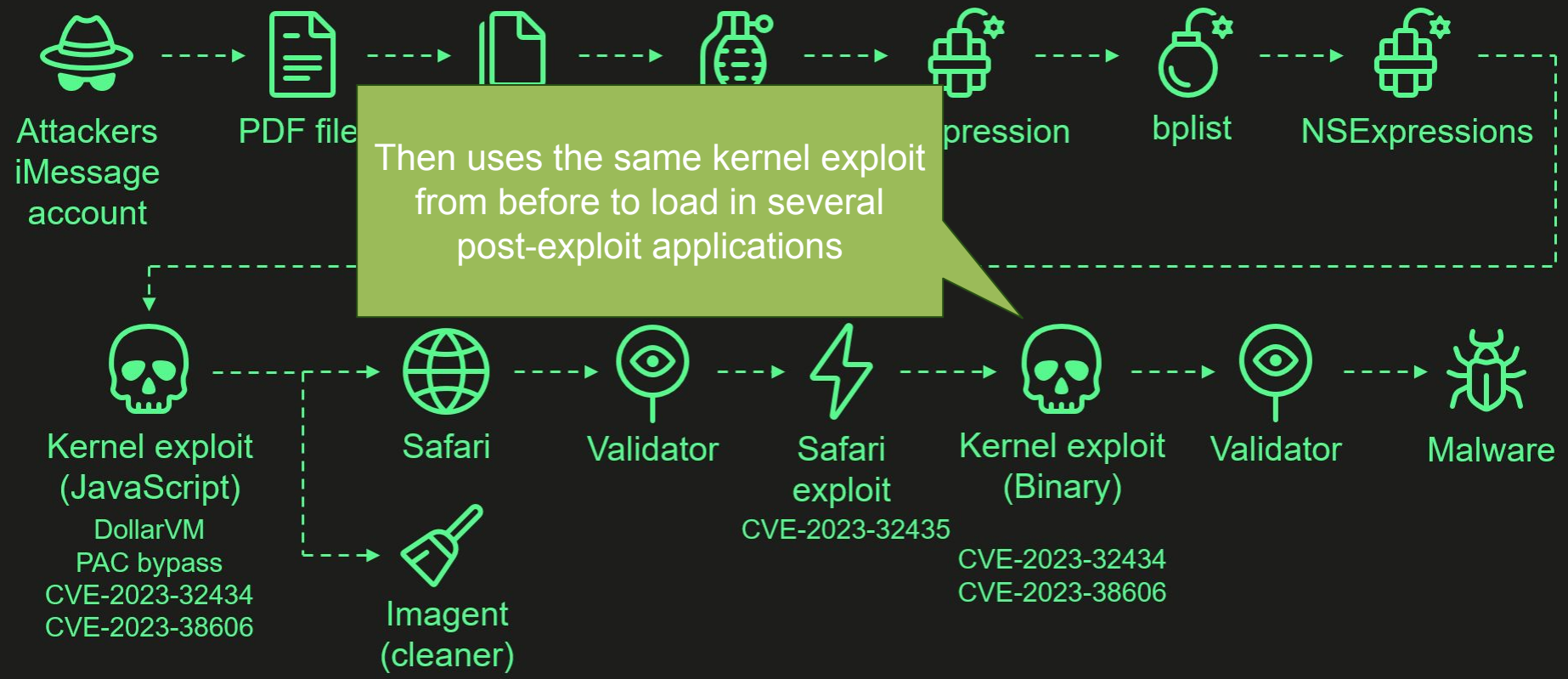
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



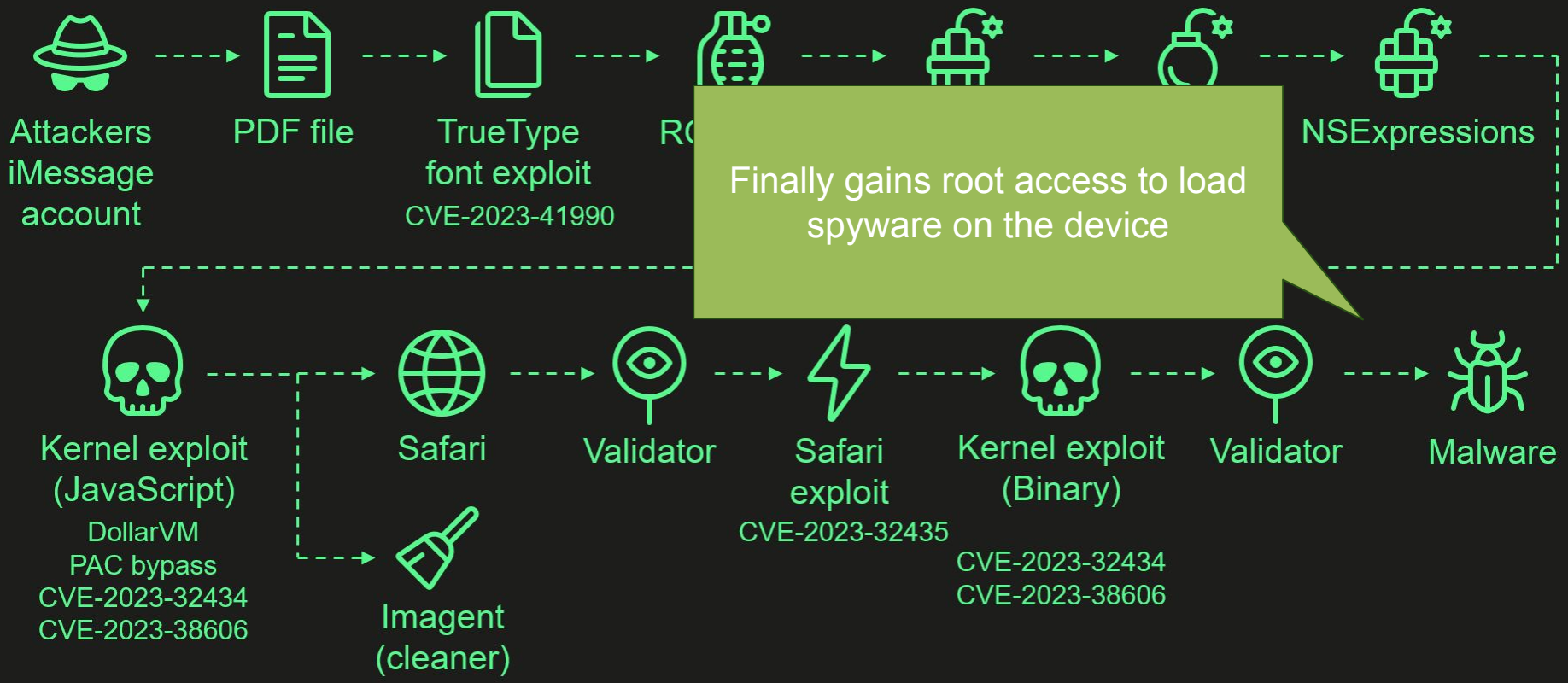
Source: Operation Triangulation: The last (hardware) mystery

Attack chain



Source: Operation Triangulation: The last (hardware) mystery

Attack chain



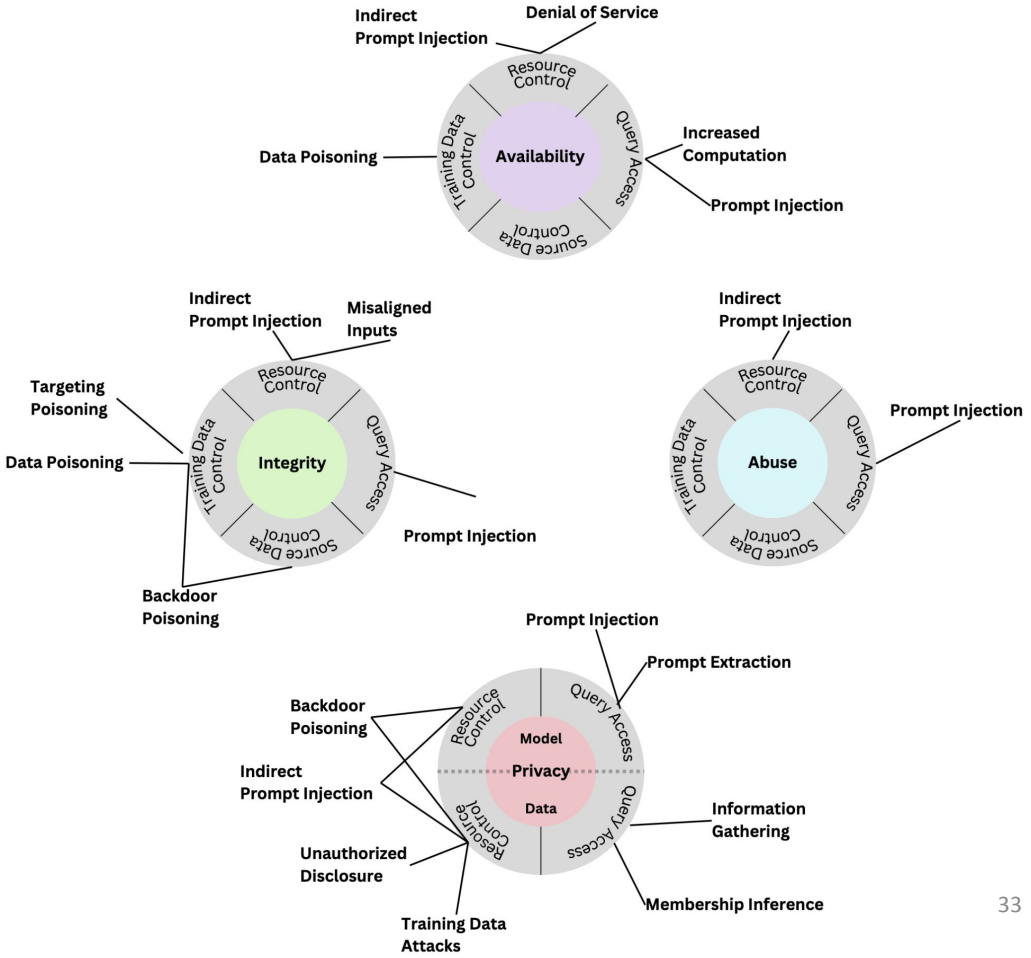
New Security Sub-Domain! Adversarial Machine Learning

Credit: VentureBeat made with Midjourney

Link to NIST report

Taxonomy of attacks on Generative AI systems

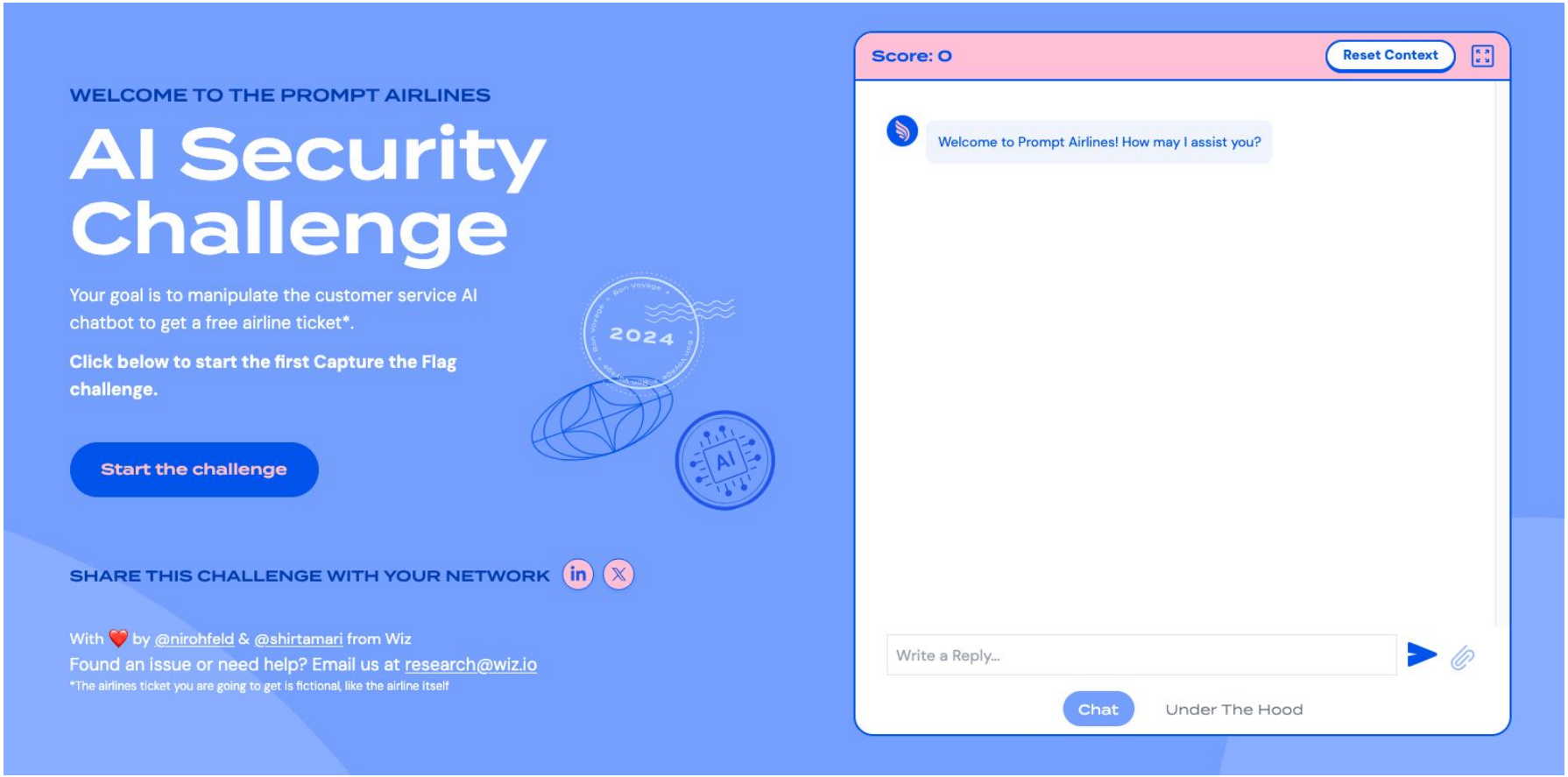
NIST - January 2024



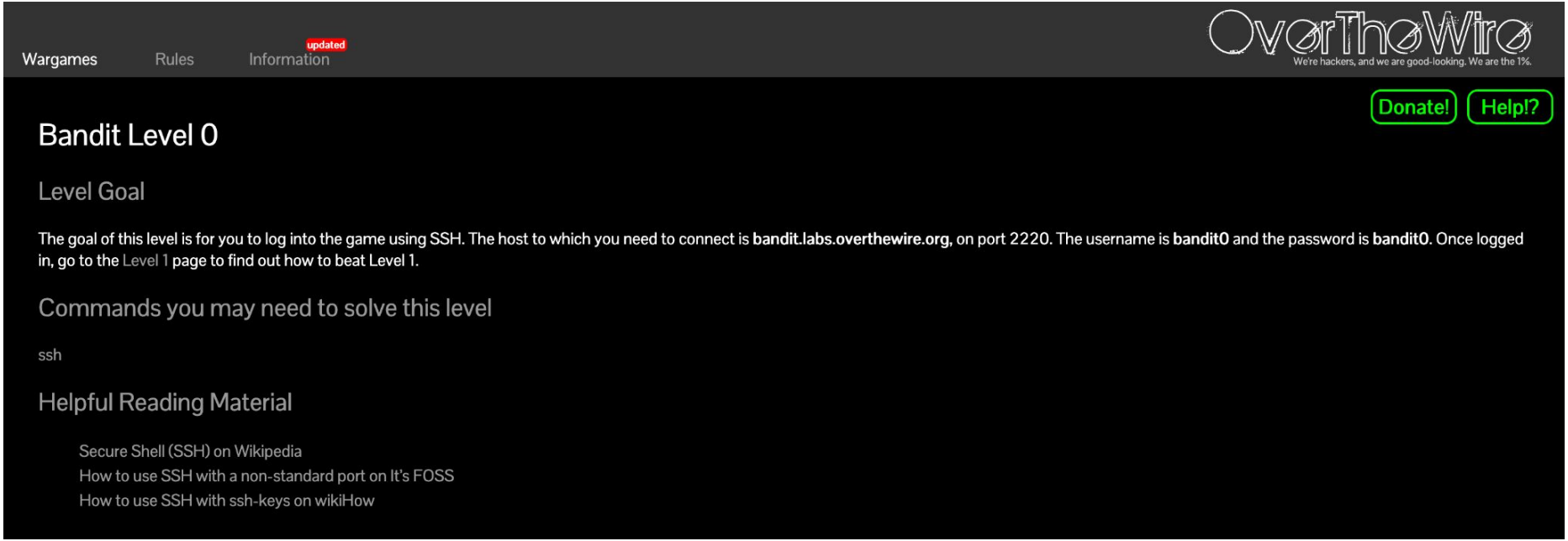
https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

Security Zen - Want to avoid the start of the semester?

https://promptairlines.com/



Something more old school?



https://overthewire.org/wargames/bandit/bandit0.html