



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:



First time CIA.gov was defaced in 1996

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

Now this is a little test of system virus spawning in security chamber to make all ps die instantly...

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

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...



WHAT PEOPLE HEAR:








SOMEONE HACKED INTO THE COMPUTERS OF THE **CIA!!**



WHAT COMPUTER EXPERTS HEAR:

SOMEONE TORE DOWN A POSTER HUNG UP BY THE **CIA!!**



-  Infecting URL.RS.TC.bb1fAUzi
19:33:43 United States → Belgium
-  Infecting URL.RS.TC.bb1fAUzi
19:33:43 United States → Belgium
-  Infecting URL.RS.TC.e742VdYj
19:33:43 NY, United States → Belgium
-  Web Client Enforcement Violation
19:33:42 WA, United States → Austria
-  Web Client Enforcement Violation
19:33:42 WA, United States → Austria
-  Web Server Enforcement Violation
19:33:42 TX, United States → MN, United S...
-  Infecting URL.RS.TC.fc43Phzz
19:33:42 United States → India






LIVE CYBER THREAT MAP



DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>




TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

-  Mongolia
-  Ethiopia
-  Nepal
-  Macao
-  Vietnam




TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

-  Education
-  Government
-  Healthcare

TOP MALWARE TYPES

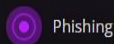
Malware types with the highest global impact in the last day.

-  Smishing
-  Adware
-  Mobile

Everyone is Getting Hacked, All the Time



Malware



Phishing



Exploit

threatmap.checkpoint.com



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:

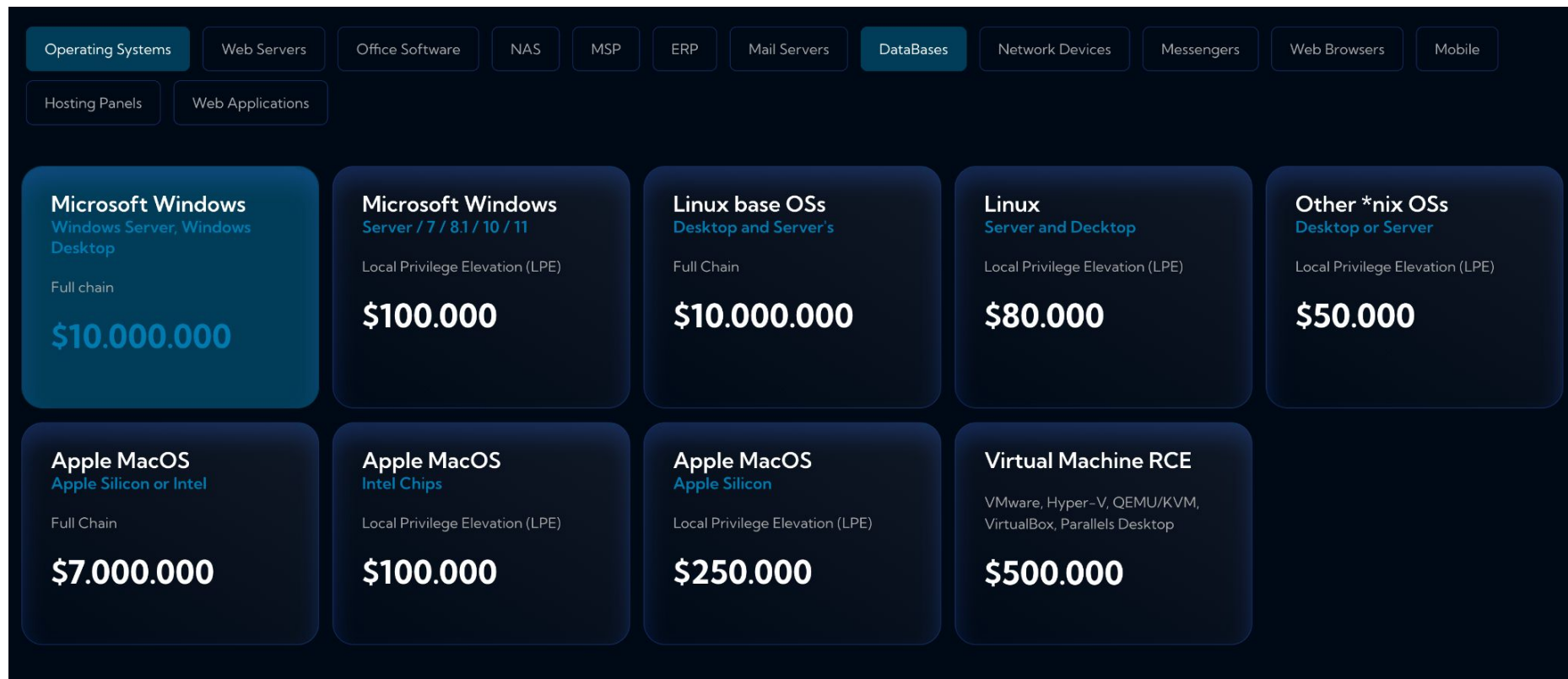
Email: [REDACTED] - Name: [REDACTED] - ScreenName: [REDACTED] - Followers: [REDACTED] - Created At: [REDACTED]

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



ZERODIUM Payouts for Mobiles*

Up to \$2,500,000											1.001 Android FCP Zero Click Android
Up to \$2,000,000											1.002 iOS FCP Zero Click iOS
Up to \$1,500,000									2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS	
Up to \$1,000,000									2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android	
Up to \$500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS		
Up to \$200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS		
Up to \$100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	6.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS		

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

■ iOS
■ Android
■ Any OS

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”

PaX
(<http://pageexec.virtualave.net>)

The Guaranteed End of Arbitrary
Code Execution

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

📅 Posted on October 3, 2025 • ⌚ 6 minutes • 📖 1072 words

Table of contents



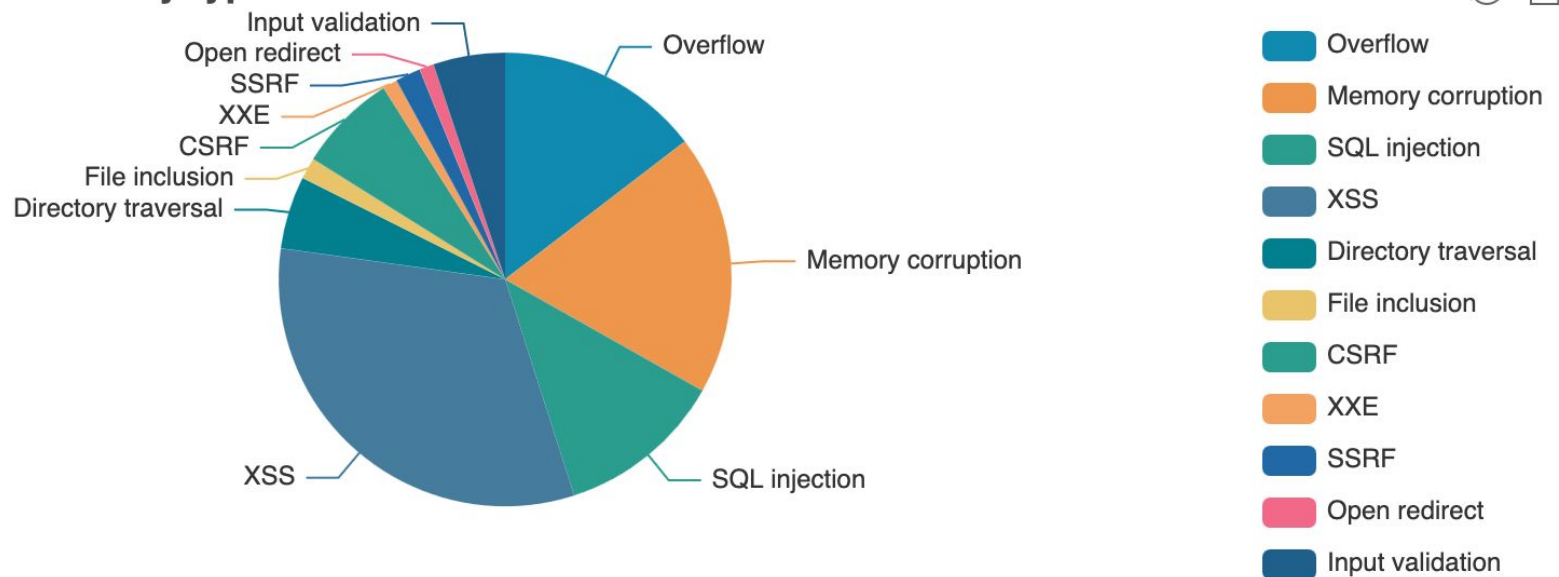
Vulnerabilities per product - as of 2026

	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

Vulnerabilities by type



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

<https://owasp.org/Top10/>



TOP10

A horizontal bar with a blue-to-dark-blue gradient, positioned below the "TOP10" text.

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

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)
- Hackerone
 - <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

Oday "In the Wild"

File

Edit

View

Insert

Format

Data

Tools

Extensions

Help

Q

Menus

100%

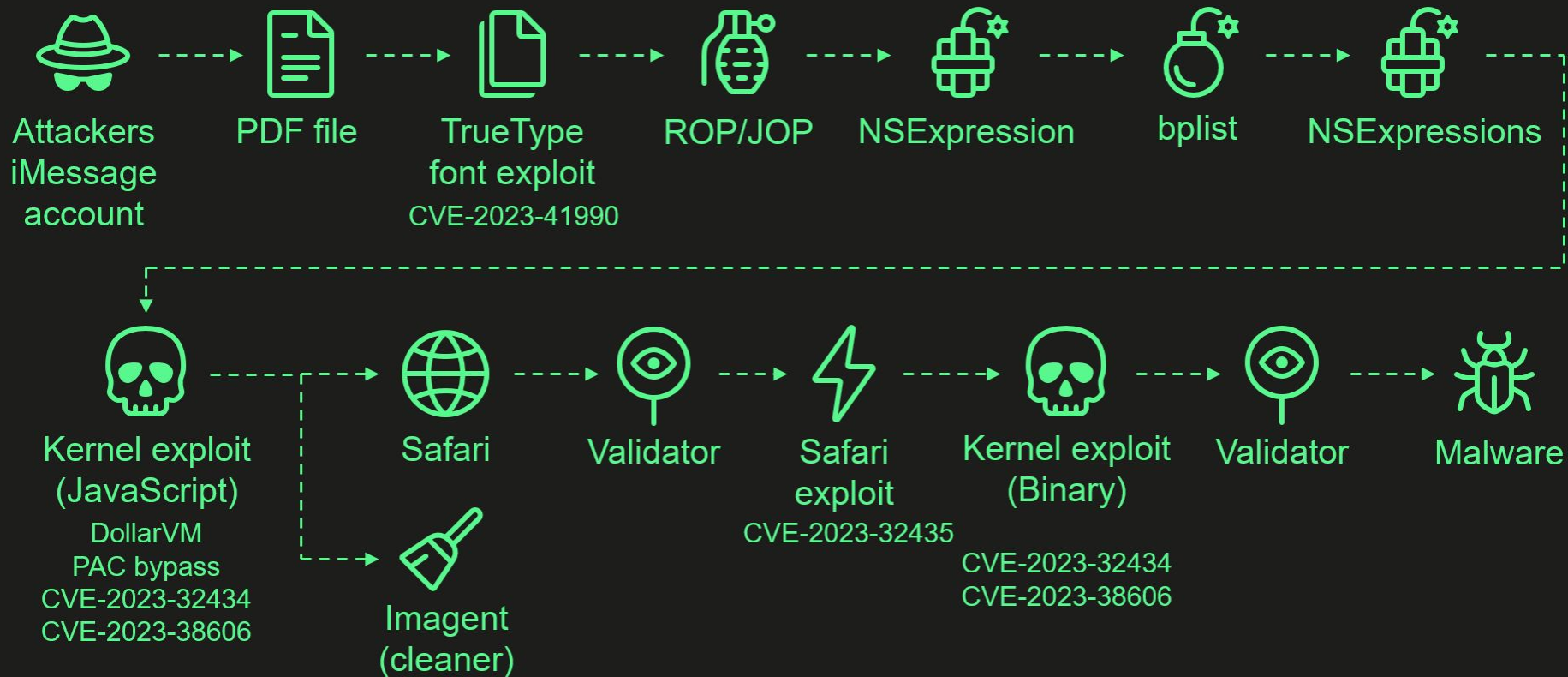
View only

D15

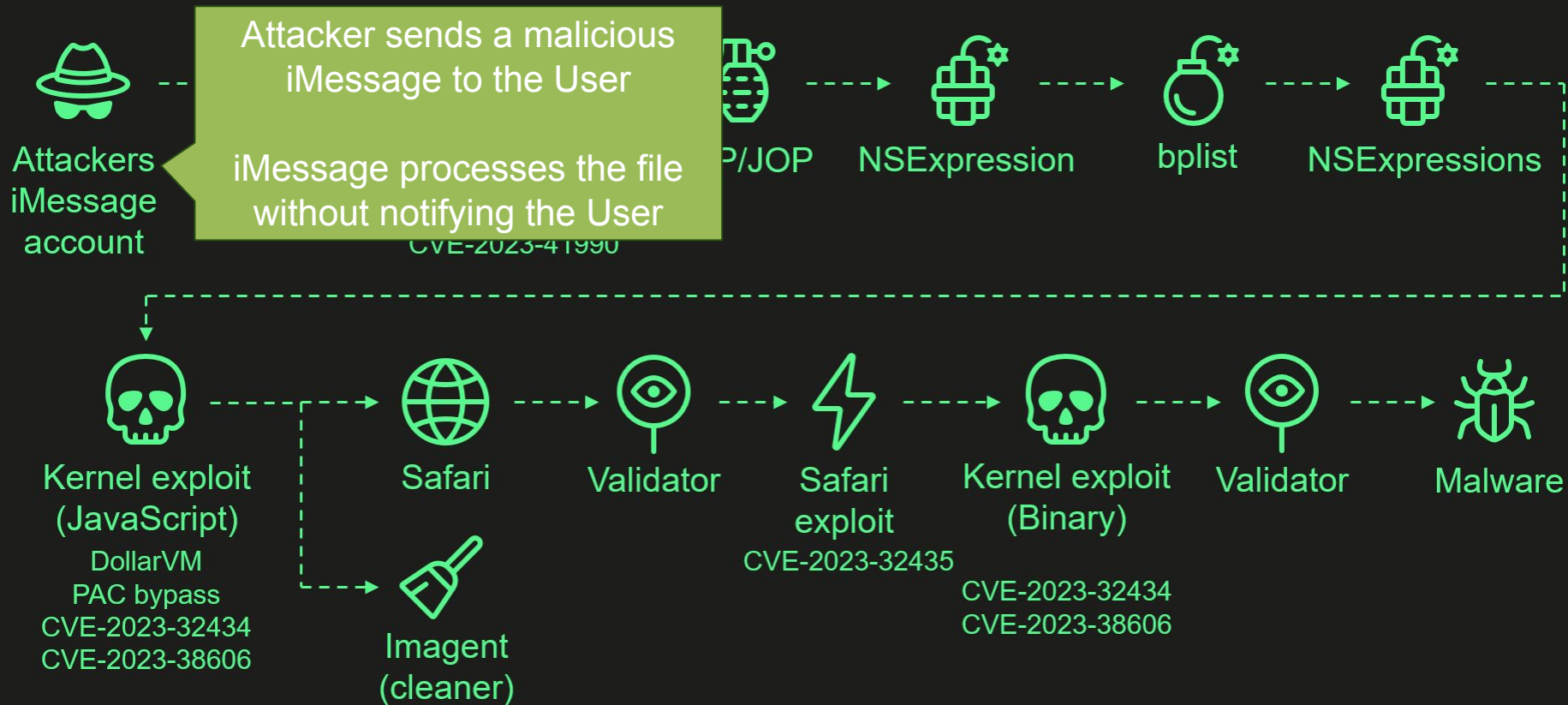
Logic Error

	A	B	C	D	E	F	G	H	I	J	K
1	CVE	Vendor	Product	Type	Description	Date Discovers	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 h	???	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 Vulne	???	2025-02-11	https://msrc.micr	???	???	???
5	CVE-2025-21418	Microsoft	Windows	Memory Corruption	Windows AncillaryFunction 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 Featu	???	2025-03-11	https://msrc.micr	???	???	Aliakbar Zahra
8	CVE-2025-24993	Microsoft	Windows	Memory Corruption	Windows NTFS Remote Code Execution Vulne	???	2025-03-11	https://msrc.micr	???	???	Anonymous
9	CVE-2025-24985	Microsoft	Windows	Memory Corruption	Windows Fast FAT File System Driver Remote	1	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 Juracko w
11	CVE-2025-24984	Microsoft	Windows	Information Disclosure	Windows NTFS Information Disclosure Vulne	???	2025-03-11	https://msrc.micr	???	???	Anonymous
12	CVE-2025-24991	Microsoft	Windows	Information Disclosure	Windows NTFS Information Disclosure Vulne	???	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

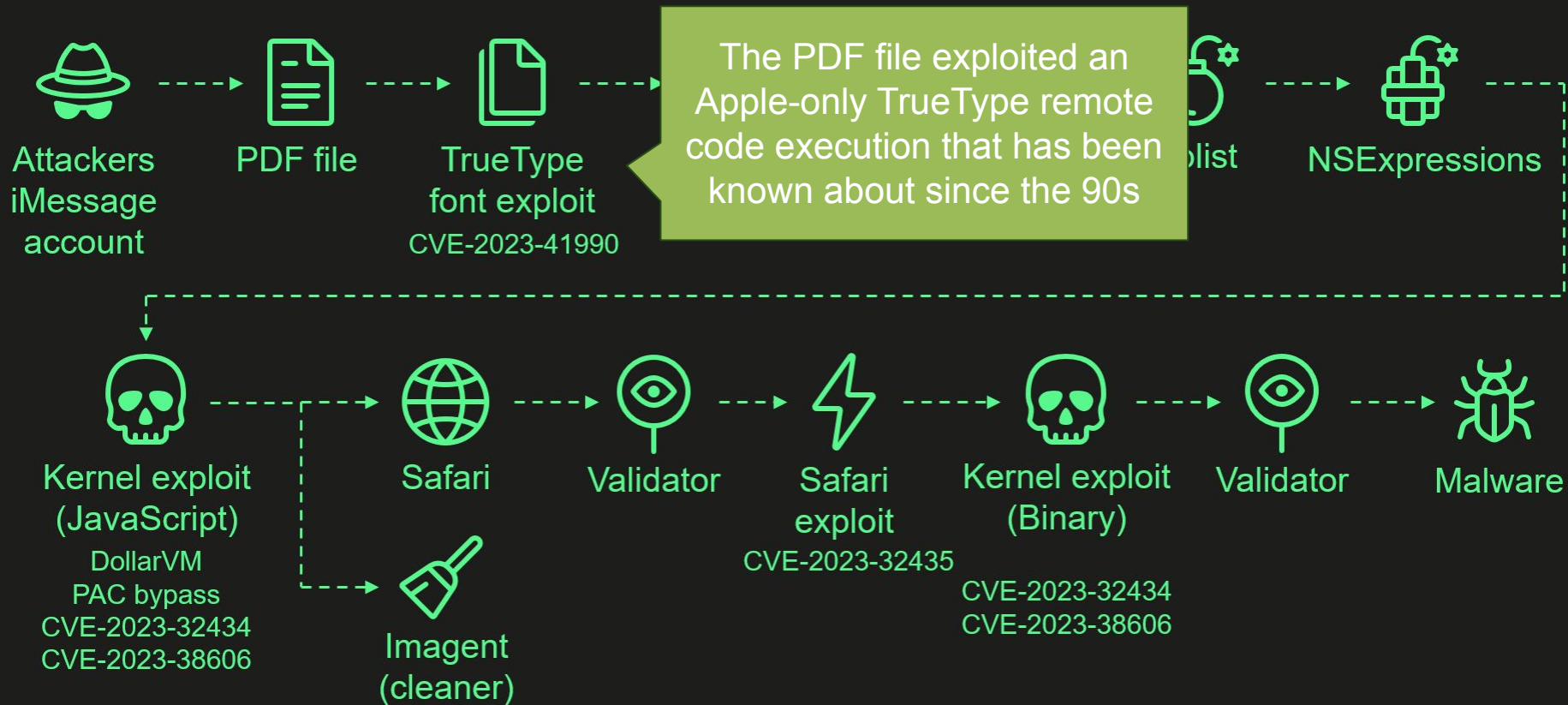
Attack chain



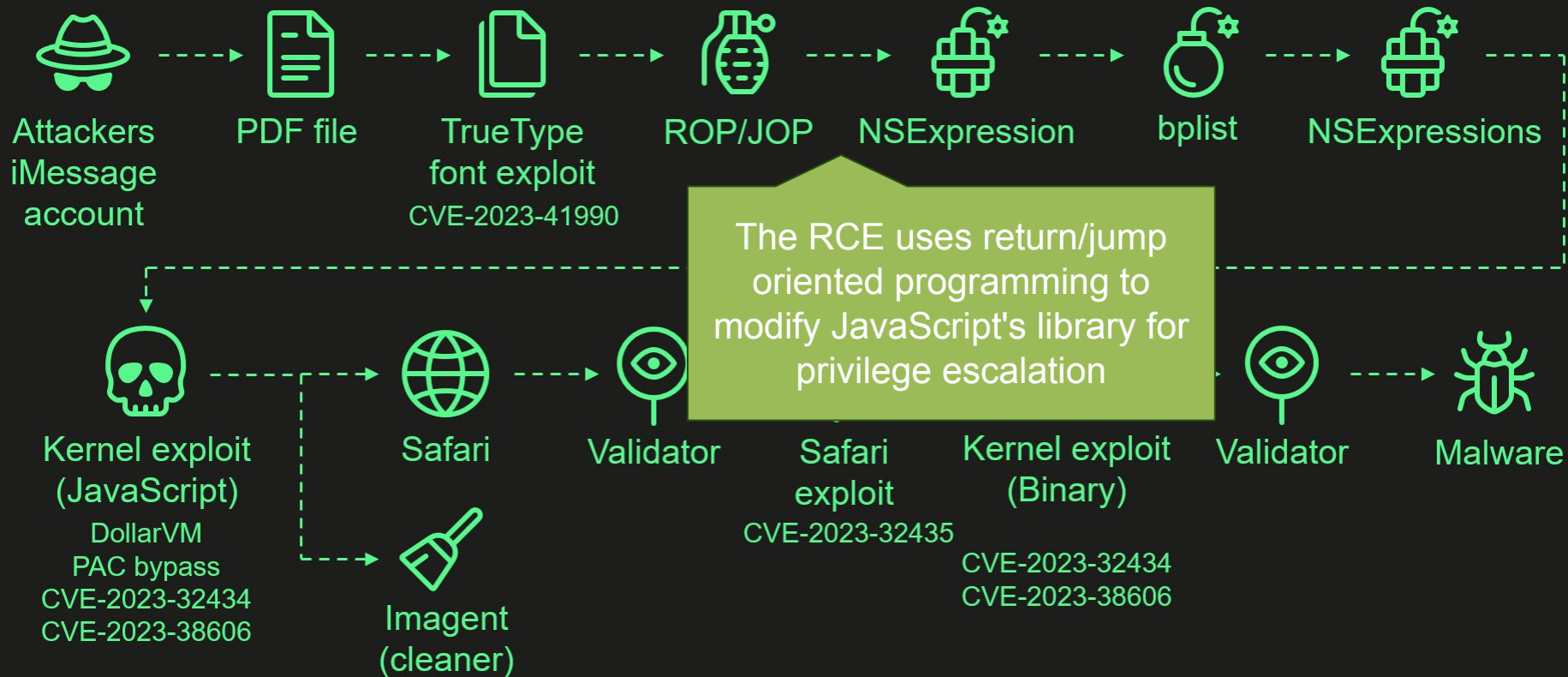
Attack chain



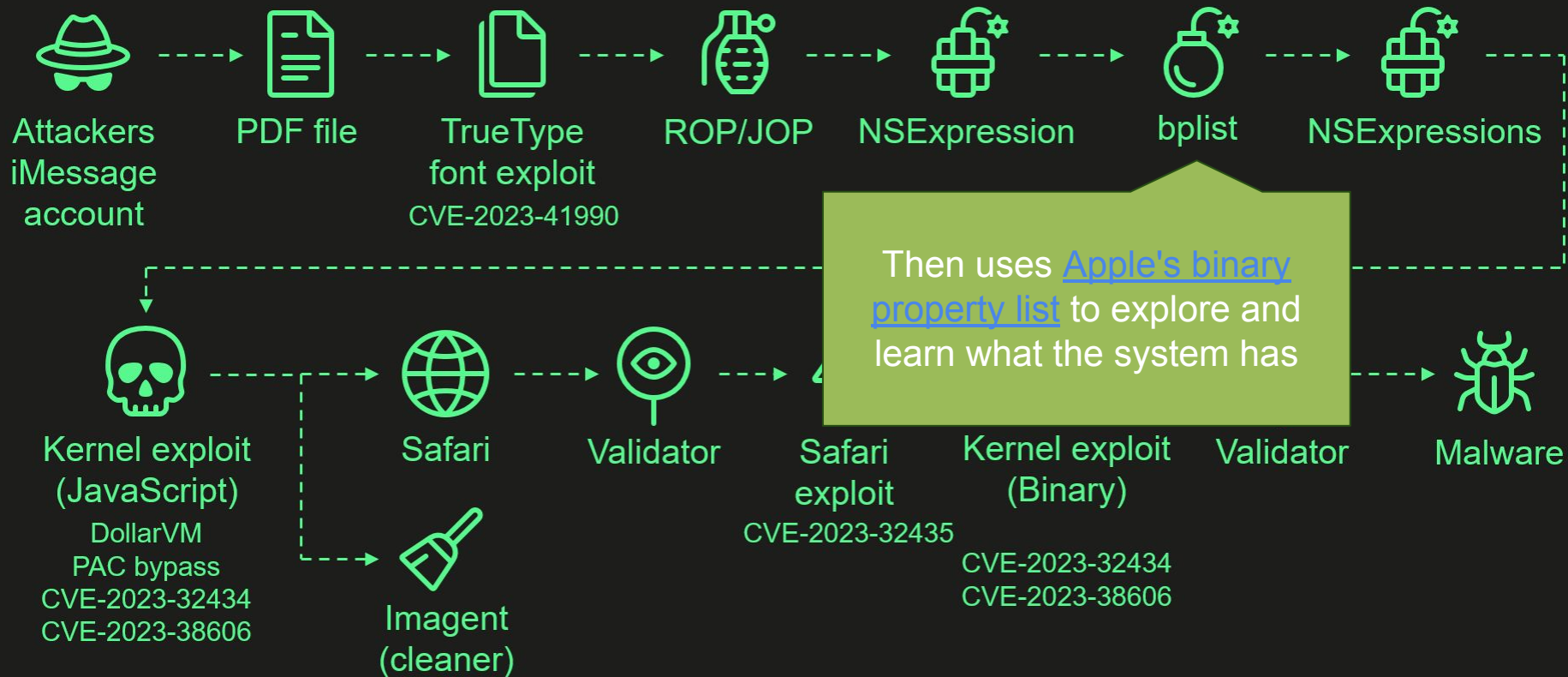
Attack chain



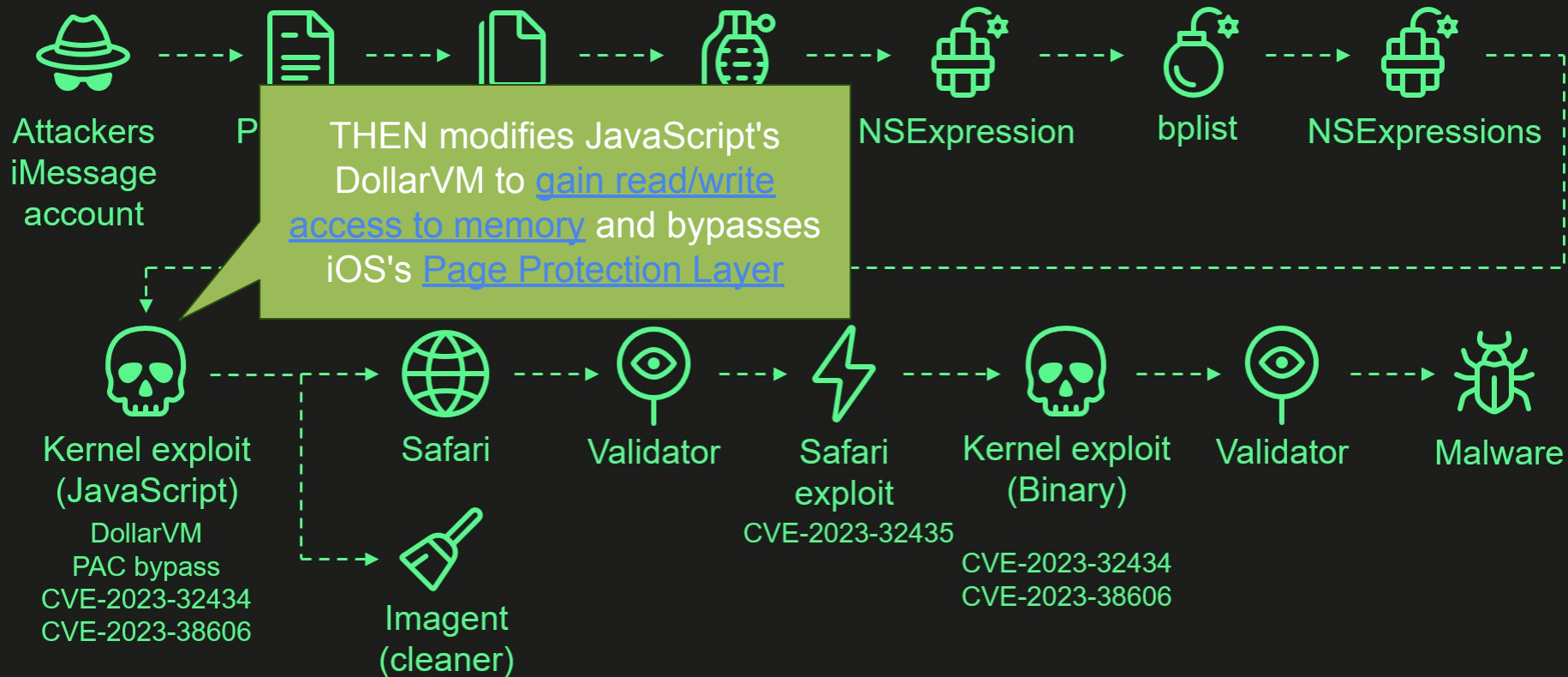
Attack chain



Attack chain

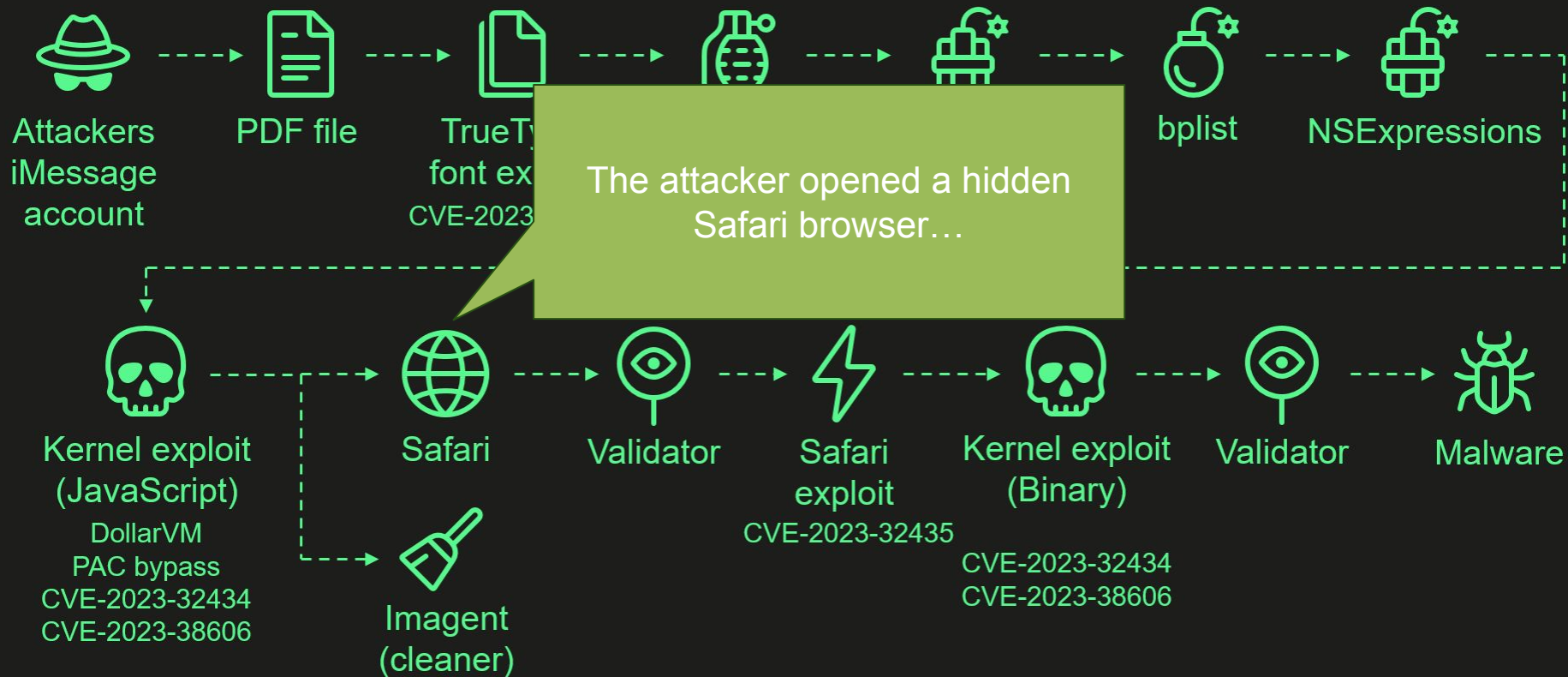


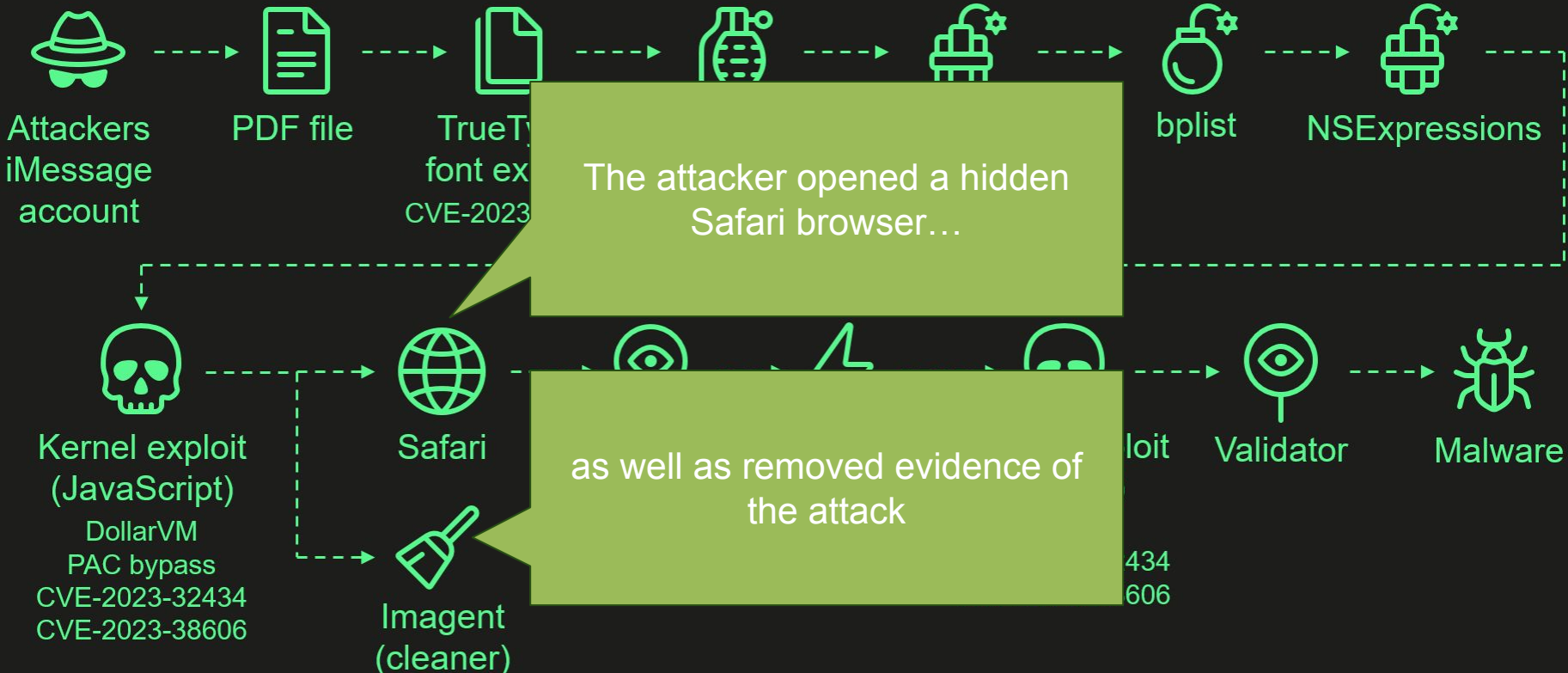
Attack chain



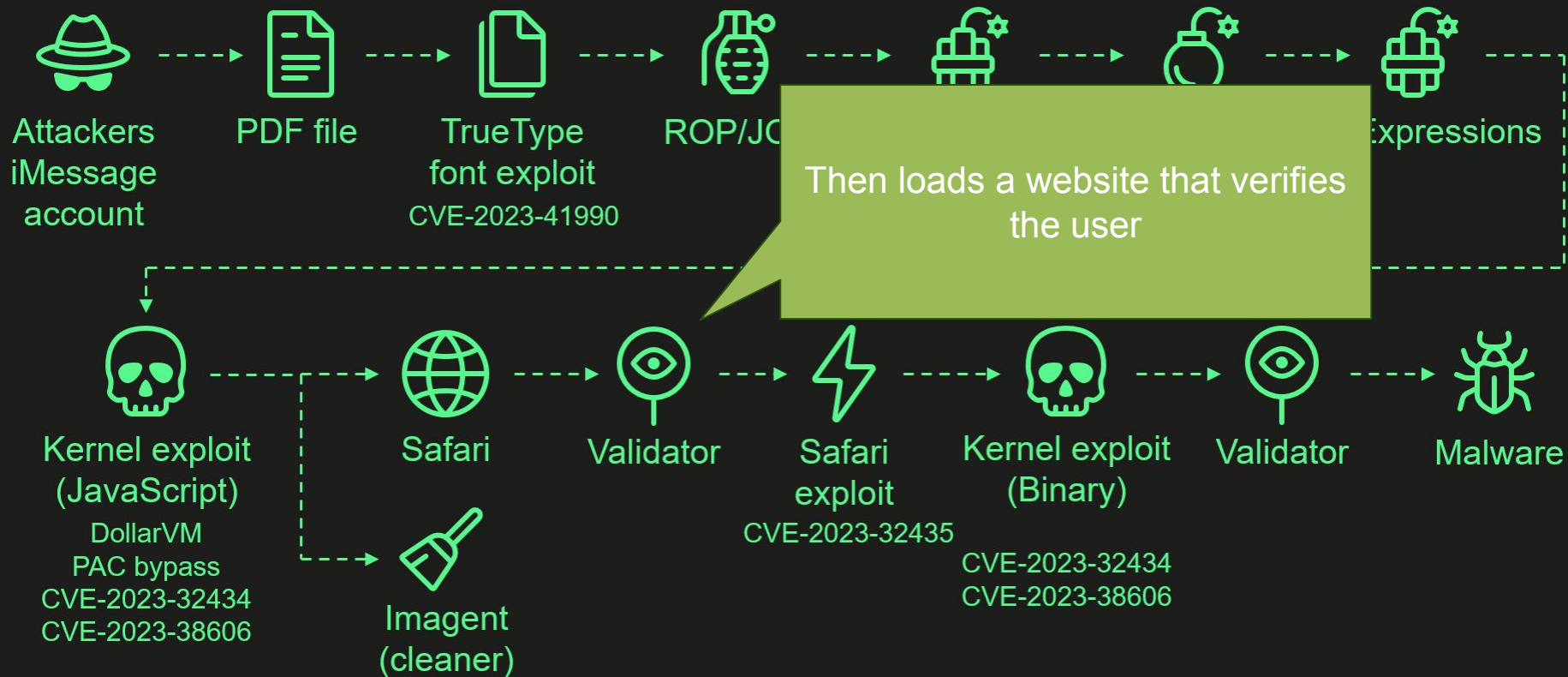


Attack chain

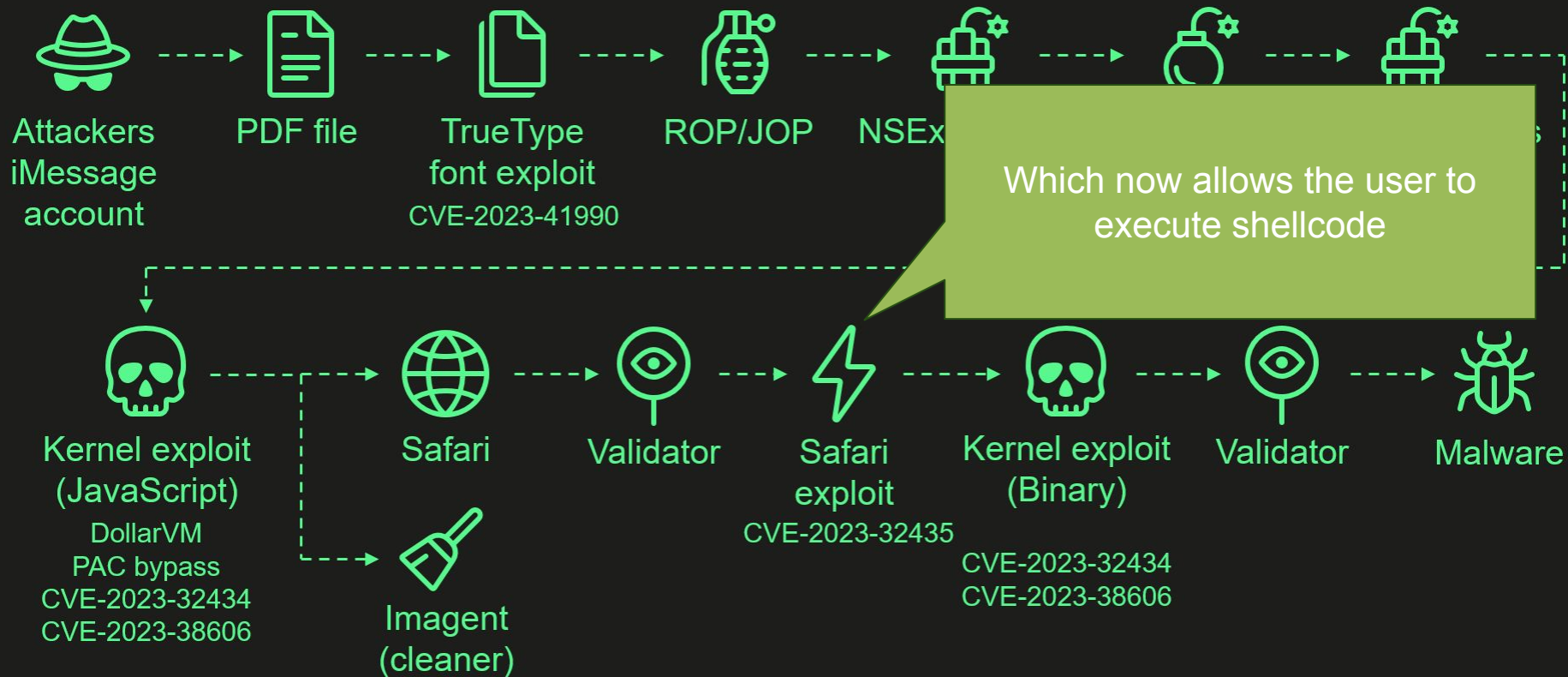




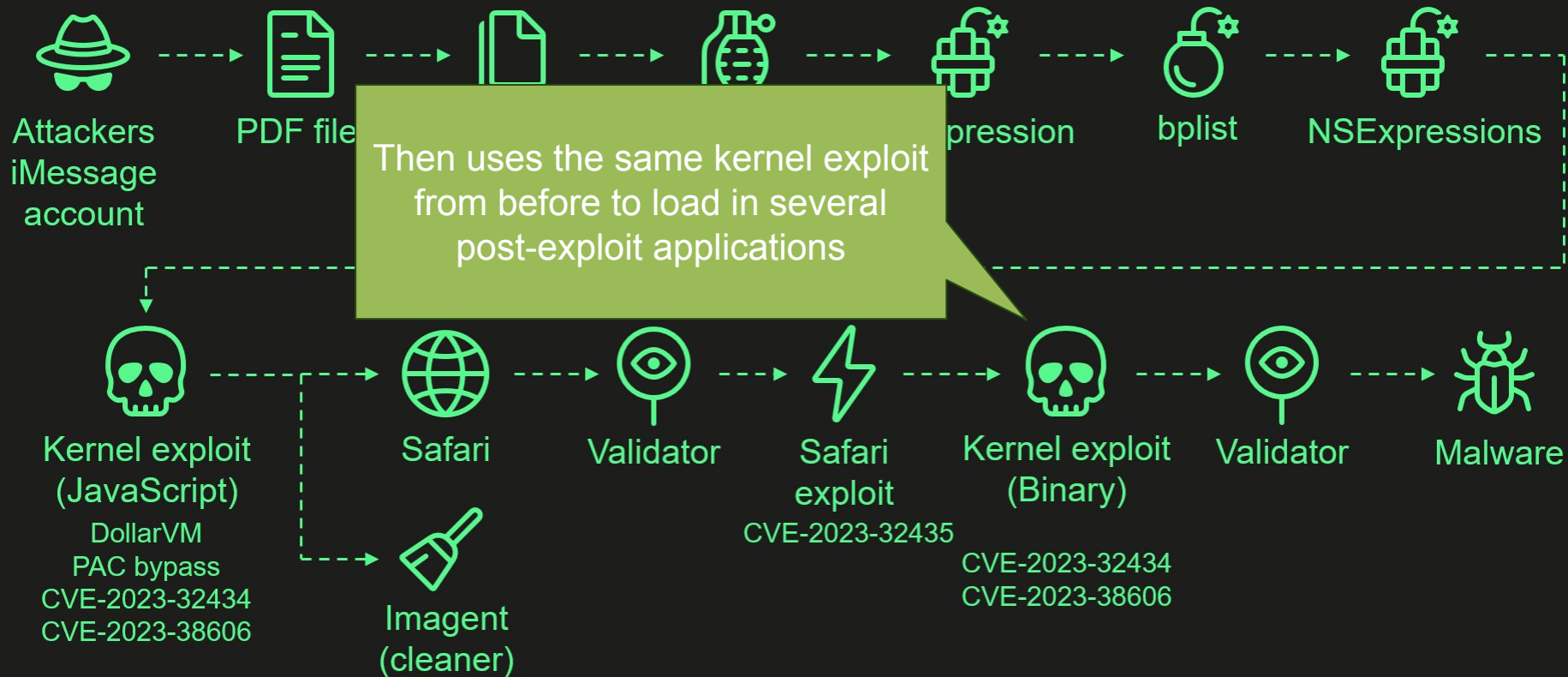
Attack chain



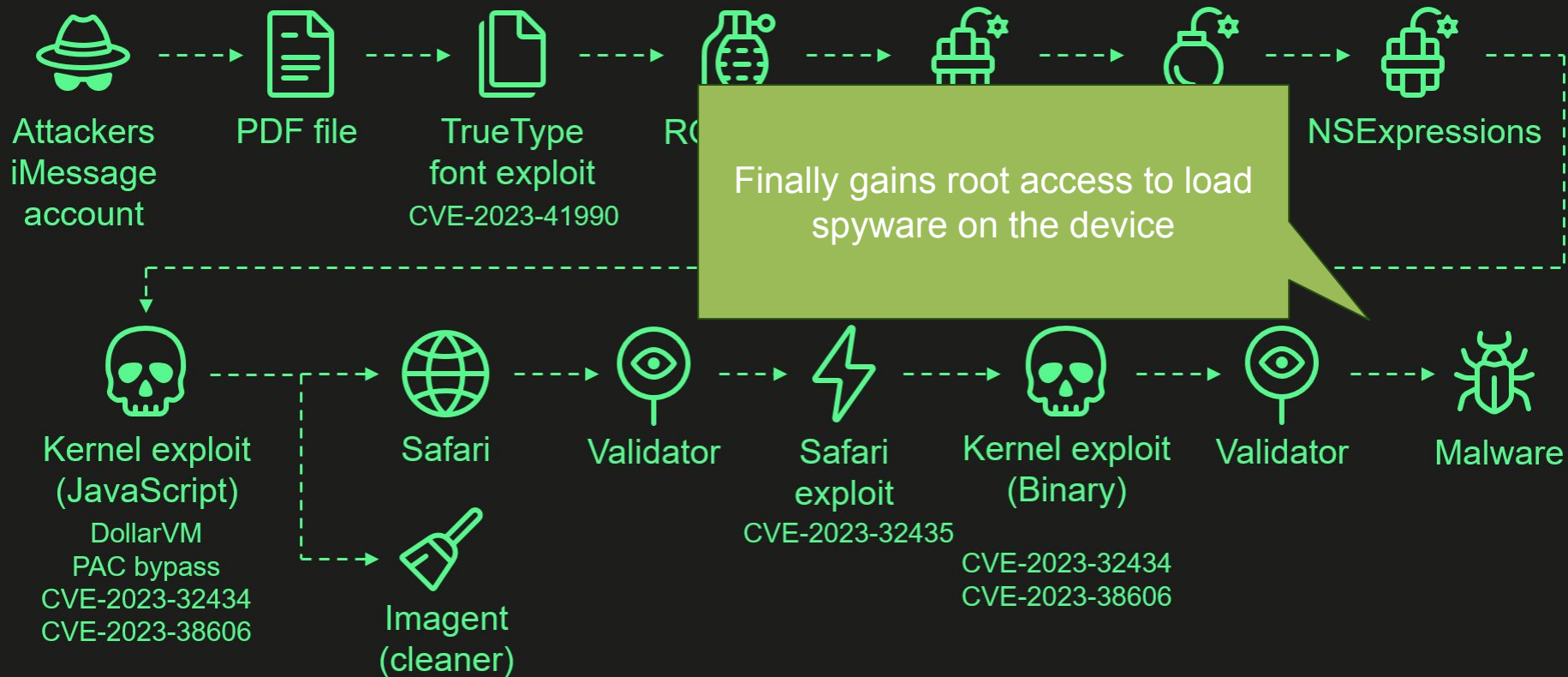
Attack chain



Attack chain



Attack chain



New Security Sub-Domain! Adversarial Machine Learning

**New NIST report sounds the alarm
on growing threat of AI attacks**

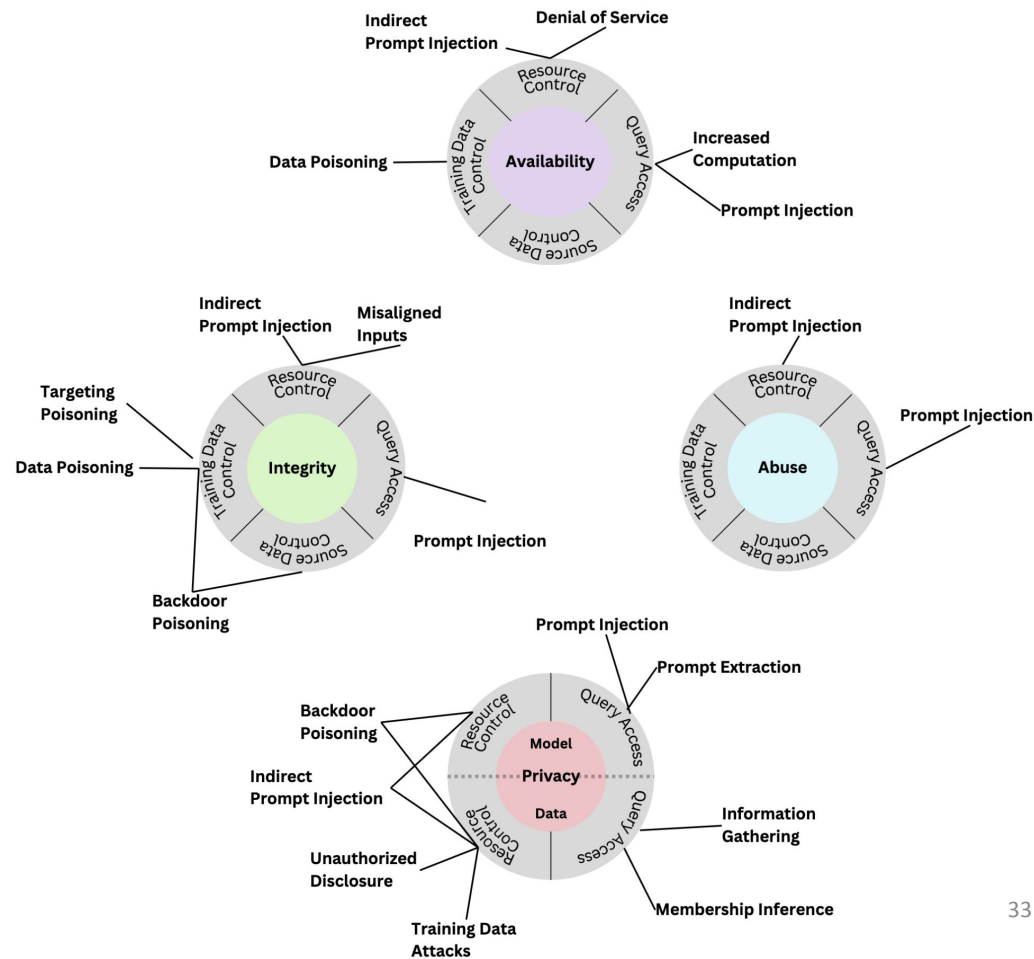


Credit: VentureBeat made with Midjourney

[Link to NIST report](#)

Taxonomy of attacks on Generative AI systems

NIST - January 2024



<https://promptairlines.com/>

WELCOME TO THE PROMPT AIRLINES

AI Security Challenge

Your goal is to manipulate the customer service AI chatbot to get a free airline ticket*.

Click below to start the first Capture the Flag challenge.

[Start the challenge](#)

SHARE THIS CHALLENGE WITH YOUR NETWORK



With ❤️ by @nirohfeld & @shirtamari from WIZ

Found an issue or need help? Email us at research@wiz.io

*The airlines ticket you are going to get is fictional, like the airline itself

Score: 0

[Reset Context](#)

Welcome to Prompt Airlines! How may I assist you?

[Chat](#)

Under The Hood

Something more old school?

[Wargames](#) [Rules](#) [Information](#) ^{updated}

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

[Donate!](#) [Help!?](#)

Bandit Level 0

Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the [Level 1 page](#) to find out how to beat Level 1.

Commands you may need to solve this level

```
ssh
```

Helpful Reading Material

- [Secure Shell \(SSH\) on Wikipedia](#)
- [How to use SSH with a non-standard port on It's FOSS](#)
- [How to use SSH with ssh-keys on wikiHow](#)

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