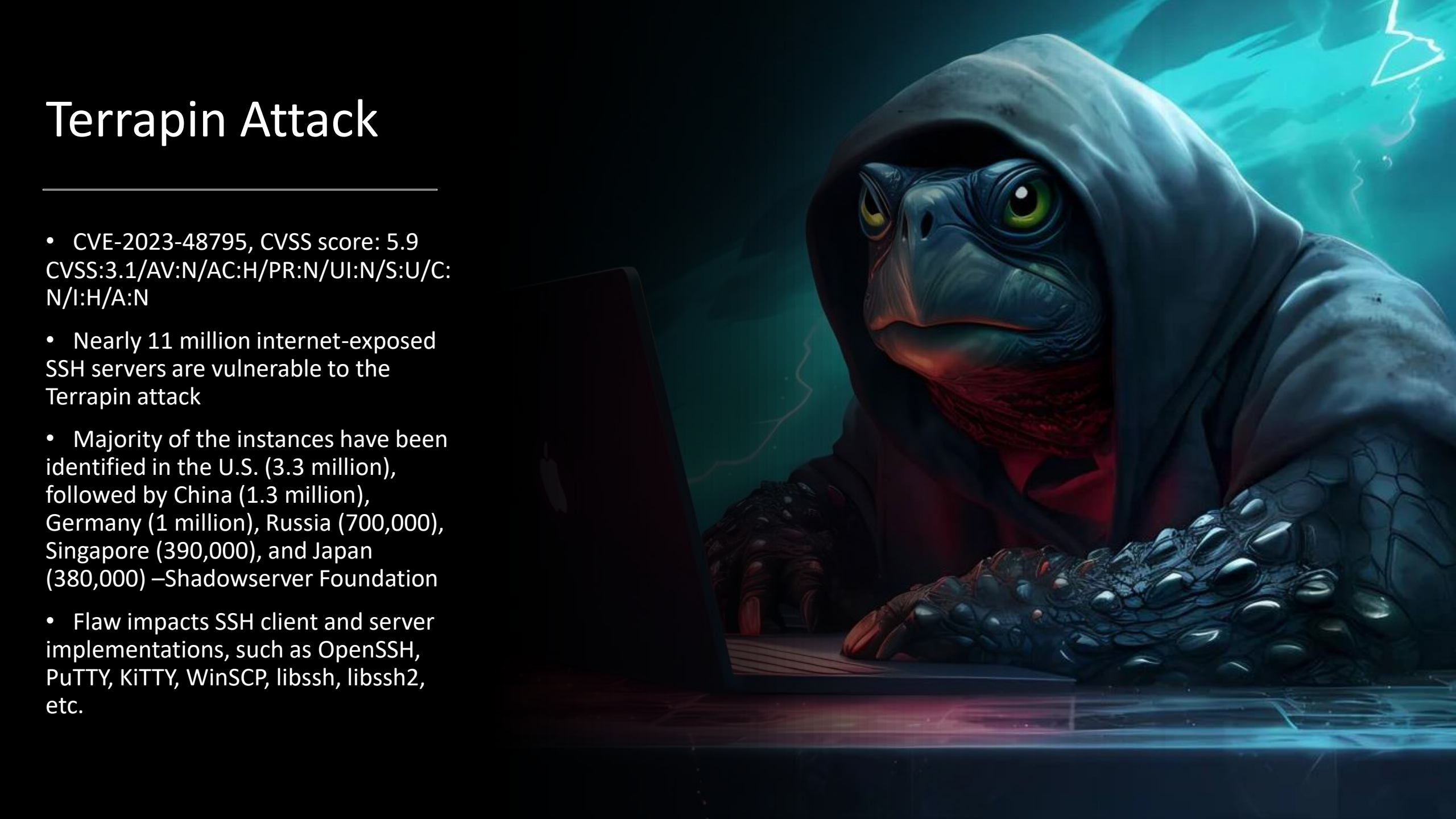
Cyber Minutes

"New Year, New Threats"

01-10-2024 | Jonathan Montoya

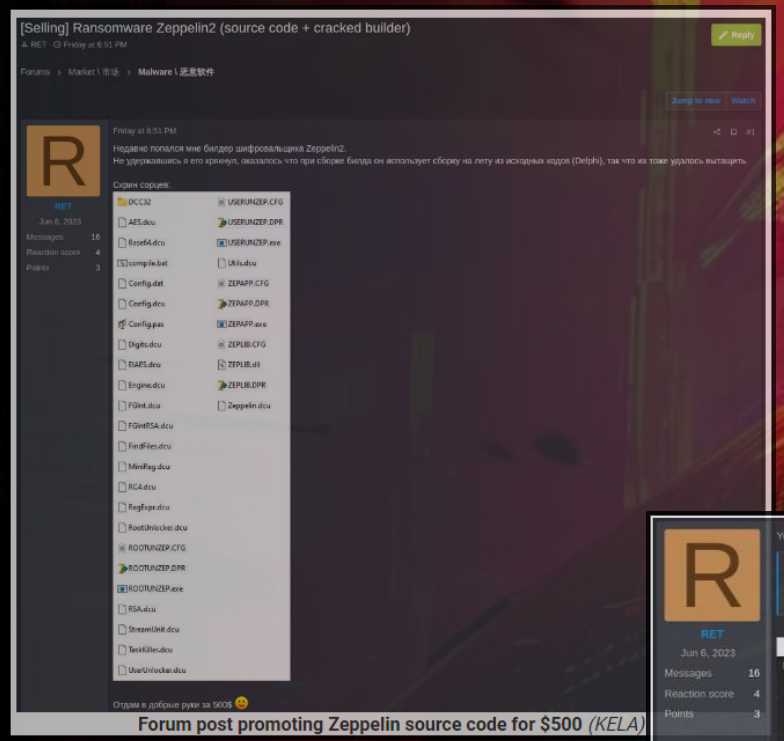
Terrapin Attack

- CVE-2023-48795, CVSS score: 5.9 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
- Nearly 11 million internet-exposed SSH servers are vulnerable to the Terrapin attack
- Majority of the instances have been identified in the U.S. (3.3 million), followed by China (1.3 million), Germany (1 million), Russia (700,000), Singapore (390,000), and Japan (380,000) –Shadowserver Foundation
- Flaw impacts SSH client and server implementations, such as OpenSSH, PuTTY, KiTTY, WinSCP, libssh, libssh2, etc.

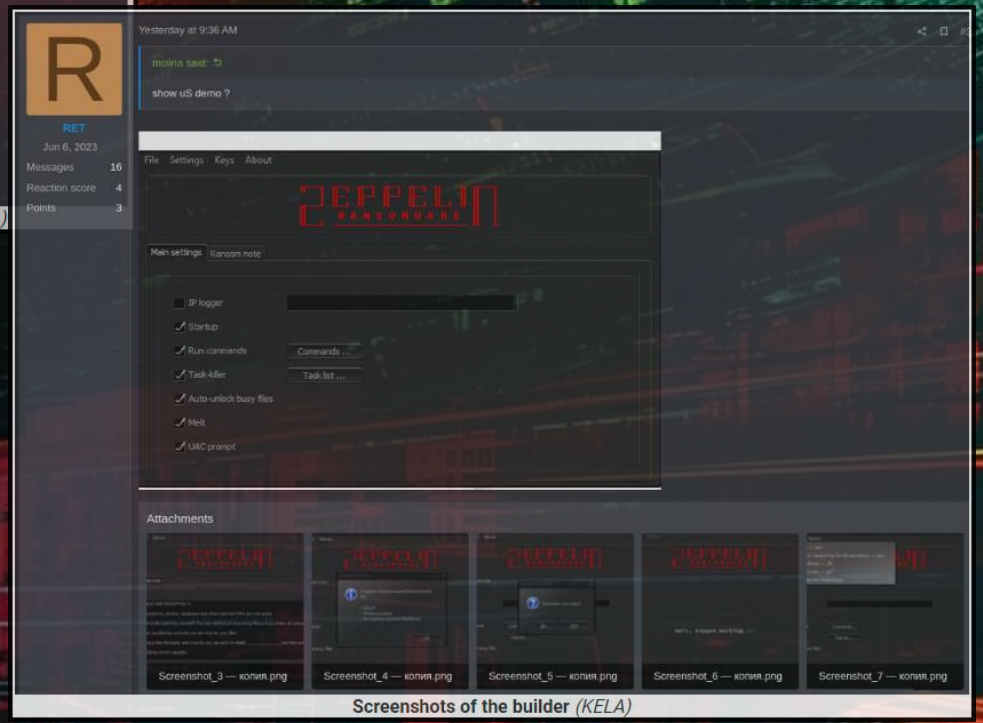


$500 Ransomware

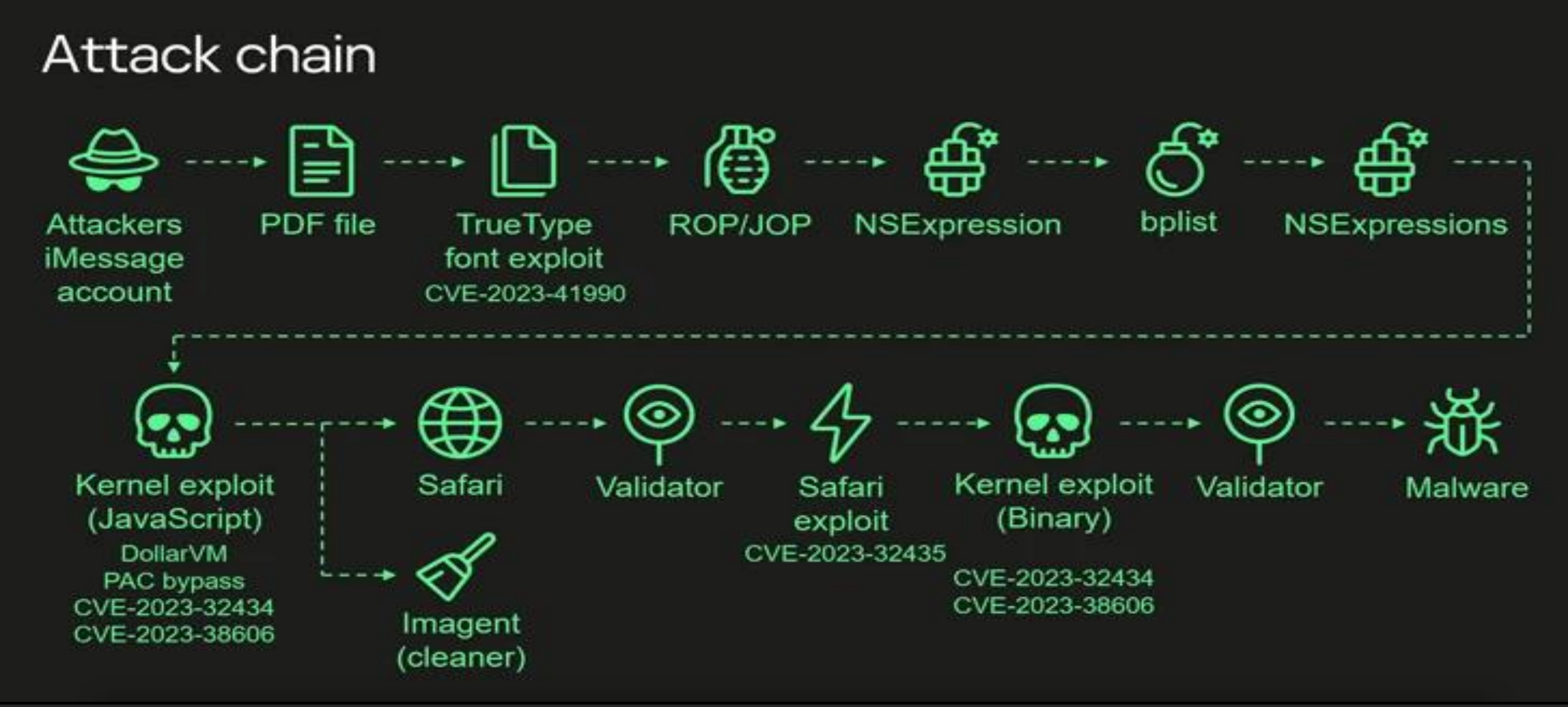
- The sale of the Zeppelin Ransomware builder source code and a cracked version for just $500 was announced on a crime forum
- This allows groups to start a RaaS easily and lowers the skill gap tremendously
- FBI issued warnings about Zeppelin Ransomware operators invoking new tactics of multi round encryption back in summer 2022
- Zeppelin RaaS discontinued in late 2022 following multiply flaws being found in the malware, allowing a decrypter to be built
- Seller has stated that these flaws are no longer present in the current version of the Ransomware



Forum post promoting Zeppelin source code for $500 *(KELA)*



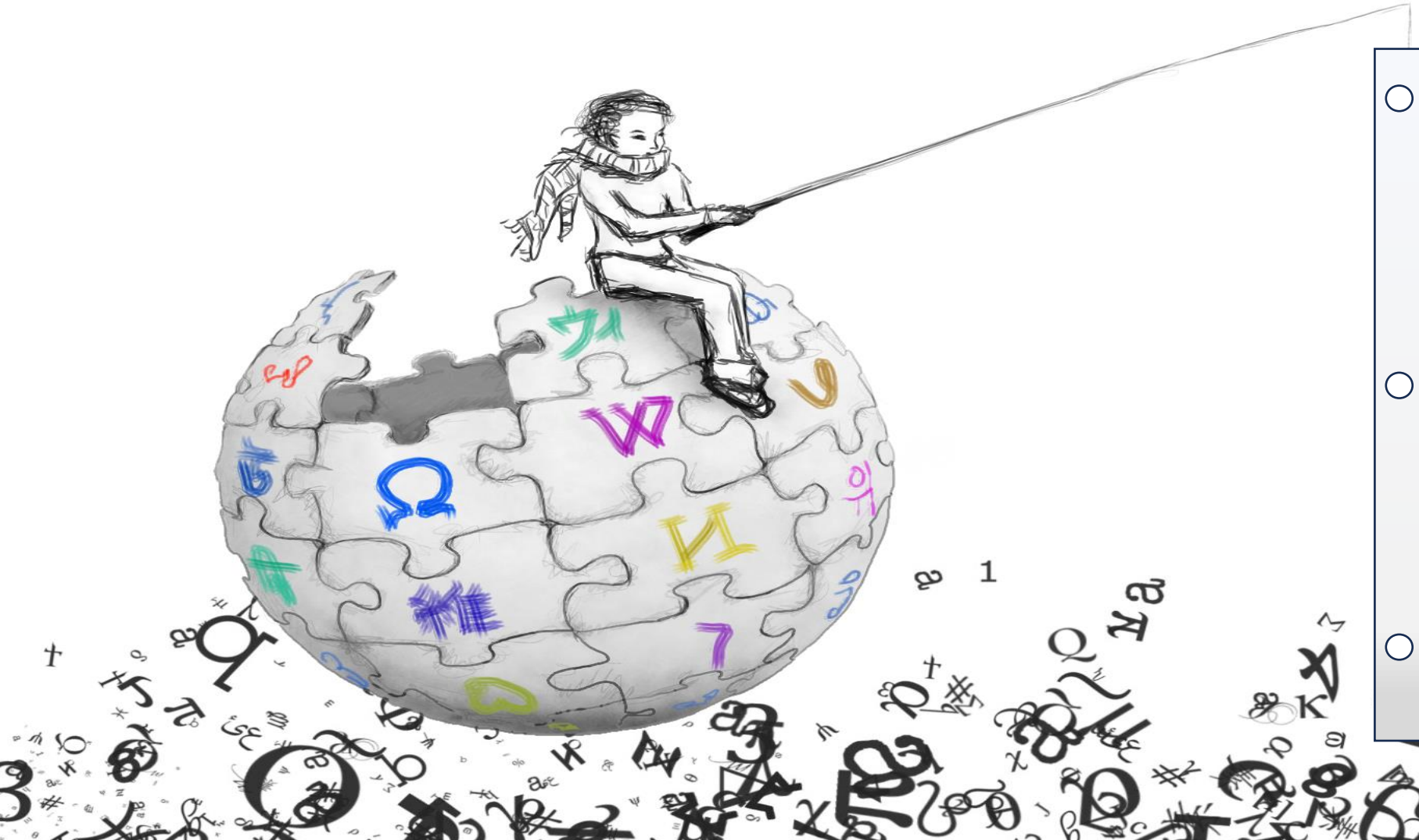
Screenshots of the builder *(KELA)*



“Operation Triangulation”

- This was campaign was discovered by cybersecurity firm Kaspersky at the beginning of 2023 after becoming a target of the attack
- The exploitation involves 4 zero-day flaws combined to “obtain an unprecedented level of access and backdoor target devices running up to iOS 16.2”
- This highly sophisticated hack has only been seen in malware like Pegasus spyware, which Apple released patches in Sept. 2023 to directly combat

Sources



- https://thehackernews.com/2024/01/spectralblur-new-macos-backdoor-threat.html
- https://www.bleepingcomputer.com/news/security/nearly-11-million-ssh-servers-vulnerable-to-new-terrapin-attacks/
- https://www.bleepingcomputer.com/news/security/zeppelin-ransomware-source-code-sold-for-500-on-hacking-forum/
- https://www.darkreading.com/cyberattacks-data-breaches/23andme-negligent-users-at-fault-breach-7m-records
- https://www.darkreading.com/cloud-security/attackers-abuse-google-oauth-endpoint-hijack-user-sessions
- https://thehackernews.com/2023/12/most-sophisticated-iphone-hack-ever.html