# IcedID Malware and Nexus Malware

***C-Suite level threat review by applicable business area addressing active threats.***

Outsourcing expertise is one-way malicious actors optimize operations and increase the number of successful cyberattacks. This report illustrates two outsourcing examples, initial access brokers and malware-as-a-service (MaaS). Initial access brokers, as the name indicates, sell threat actors access into organizations. IcedID malware is utilized by many initial access brokers. Nexus malware is an example of MaaS. MaaS is a type of service where threat actors develop and maintain malware which is then leased to other threat actors for exploitation.

## IcedID Malware:

IcedID malware (also known as BokBot) first emerged in 2017 as a modular banking trojan, stealing users' financial information to commit bank fraud. Recent updates to the malware have shifted the focus away from bank fraud to payload delivery. The malware is mainly utilized by adversaries targeting banks, but with the recent updates it could be useful to threat actors targeting a range of industries.

## Nexus Malware:

Nexus malware is an Android banking Trojan that first emerged in June 2022. It is thought to be an updated version of Sova, an Android banking trojan discovered in mid-2021. Nexus malware targets banks and cryptocurrency services worldwide. Its primary objective is to steal banking and financial information from its victim's infected devices. Nexus malware is leased to threat actors for $3000 a month.

### IcedID Malware

Threat Level: Medium

**Attack:**

The original IcedID variant is delivered via a phishing email with a malicious attachment and uses a man-in-the-browser attack (MITRE T1185) to steal financial information. If the user opens the attachment (MITRE T1204.002), IcedID is installed, exfiltrates system information, and requests to download the bot from the command-and-control (C2) server (MITRE T1071.001). The C2 server will verify system information (ex: it is not a sandbox environment) and send the IcedID bot payload. Proofpoint recently identified additional variants, Forked IcedID and Lite IcedID, without the banking fraud functionality. The Lite IcedID variant differs the most as it is instead used as a second-stage payload to machines infected with Emotet (another malware), suggesting a possible link between Emotet and IcedID developers.

**Remediation:**

- It is recommended to conduct regularly phishing simulations to train users to identify and report phishing emails. Users that fail could then undergo additional training and be retested.
- Acquire an email security solution.
- Consider email authentication mechanisms such as SPF and DKIM to reduce spoofing.

### Nexus Malware

Threat Level: Medium

**Attack:**

Nexus malware takes over the user accounts by performing overlay attacks and logging keystrokes to steal user credentials. When a user of a targeted banking or cryptocurrency application uses a compromised android device, Nexus redirects them to a page that looks like the genuine application login page (MITRE T1056) and steals their credentials using an embedded keylogger (MITRE T1056.001). Nexus malware can also gain access to online accounts by intercepting SMS messages containing two-factor authentication codes (MITRE T1111). It was found to be stealing seeds and balance information from cryptocurrency wallets, cookies (MITRE T1359) from targeted websites, and two-factor codes of Google's Authenticator app using Android's "Accessibility services" features.

**Remediation:**

- Download and install antivirus and internet security software package on your connected devices.
- Enforce multifactor authentication (MFA) with strong passwords and enable biometric security features.
- Provide training to the users to not click on any links received via SMS or emails and to be mindful of giving permissions to apps installed on your mobile device.

## IcedID Malware Details:

- **An in-depth analysis of the new variants:** https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid
- **Consolidated analysis of the new variants:** https://www.csoonline.com/article/3691897/researchers-warn-of-two-new-variants-of-potent-icedid-malware-loader.html

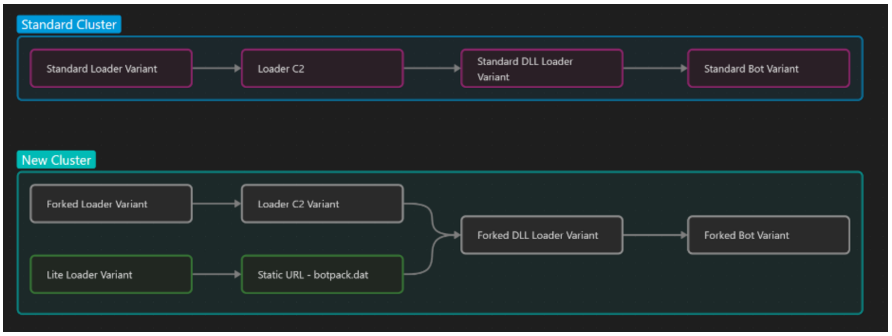
## Nexus Malware Details:

- **An in-dept analysis of the malware:** https://blog.cyble.com/2023/03/09/nexus-the-latest-android-banking-trojan-with-sova-connections/
- **Consolidated analysis of the new variants:** https://www.csoonline.com/article/3691652/android-based-banking-trojan-nexus-now-available-as-malware-as-a-service.html

## How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity

**Overview of the IcedID Variants**




Source: https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid

ABOUT K LOGIX
Cybersecurity Advisory and Consulting Services
Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.