bscs23128-B - Info Sec
Khadijah Farooqi

Case Study # 1

0.1. An APT Group :
An APT group, or Advanced Persistent Threat group, is a team of skilled cyber attackers, often state-sponsored, that conducts long-term, targeted cyberattacks to gain unauthorized access to networks for espionage or sabotage.

1. APT Group :
BlueNoroff (a subgroup of Lazarus)

2. State Sponsored or Not :
it is a state sponsored and financially motivated on behalf of **North Korea**.

3. Major Attack:

- ***Rust Bucket Campaign***: In April 2023 it was discovered that they launched macOS-focused campaign targetting financial/crypto sectors.
  - **Malware/Tools** :
    - RustBucket: multi-stage macOS malware.
    - ObjCShellz: reverse shell for command execution.
  - **Targets**: macOS users in venture capital and crypto companies.
  - **Techniques**:
    - fake PDF viewer app that tricks people into installing it (social engineering).
    - step-by-step malware installation: first a small program (dropper) → then a bigger loader → finally the main backdoor.
    - works on both Intel and Apple Silicon Macs, so it can run on almost any modern Mac.
    - stays on the system by using startup programs (LaunchAgents), so it runs again even after restart.

4. Impact of attack:
it was a financial theft targeting crypto and fintech personnel

5. Threat Intelligence Feed:
https://blog.sekoia.io/bluenoroffs-rustbucket-campaign/

6. Indicators of Compromise :

- rustBucket used to deploy other malware through several infection chains that includes: LNK, MSI, OneNote and VHD files.
- initial intrusion vector included phishing emails, and linkedin profile.

sekoia.io identified this domain as sarahbeery.docsend[.]me
- in March 2023 they (sekoia.io) observed new files (MSI (a direction file about installation about a particular installer) file: 5c483473641807082e530744023044fd and One Note file: 4e05597d308d2368625dc19e86a9ca22) containing similar commands to those used in the VHD files reported by Kaspersky.

9. Active Bluenoroff C2 Servers:
104.156.149[.]130 (2023-04-18 - today)
104.255.172.52 (2023-03-18 - today)
104.234.147[.]28 (2023-01-21 - today)
104.168.138.7 (2023-03-17 - today)
104.168.167[.]88 (2022-10-17 - today)
155.138.159.45 (2022-09-20 - today)

10. Inactive Servers:
104.255.172[.]56 (2022-09-15 - 2023-04-11)
172.93.181[.]221 (2022-12-28 - 2023-03-06)
172.86.121[.]143 (2022-10-31 - 2022-12-21)
172.86.121[.]130 (2022-10-25 - 2023-01-24)
149.28.247[.]34 (2022-11-11 - 2022-11-11)
152.89.247[.]87 (2022-09-15 - 2022-10-24)
104.168.174[.]80 (2022-06-28 - 2022-09-16)
149.248.52[.]31 (2022-08-05 - 2022-08-31)
155.138.219[.]140 (2022-07-17 - 2022-08-16)

11. Category Of Malware:

- dropper
- remote access trojan (RAT)
- cross-platform deception components

12. Mistakes of Victim:

- trusting unknown “Internal PDF Viewer” installer without verifying the source.
- opening attachments and links from social channels (linkedin in this case) without validating the sender.
- macOS blind spots

13. Measures to reduce the impact:

- strong action from the OS to detect the malicious processes, in this case the child processes of PDF Viewer.
- awareness and training campaigns for the user of all platforms.
- application control (allowing only known apps to run on the pc).