New Dora RAT Malware

Date: 04th June 2024 | Severity: High

Summary

The AhnLab Security Intelligence Center (ASEC) recently uncovered multiple attack cases by the Andariel APT group targeting educational, manufacturing, and construction sectors in Korea. These attacks use various malware such as keyloggers and infostealers to control infected systems and steal data from compromised systems. Attackers have developed new malware, like Dora RAT, to perform basic malicious functions.
The group uses vectors like spear phishing, watering hole attacks, and exploiting software flaws to gain access.

Attack Vectors

- Nestdoor is an RAT malware strain that has been found since at least May 2022. It can receive the threat actor's commands to control the infected system and has been discovered continuously in the Andariel group's attack cases. For the convince of classification, this post lists cases as Nestdoor based on their collected names.
- The malware strains classified as an "Unidentified RAT" are developed in C++ and can receive the threat actor's commands and carry out malicious behaviors such as file upload and download, reverse shell, and command execution. Its other characteristics include binary obfuscation to disrupt analysis and various features such as keylogging, clipboard logging, and proxy.
- Dora RAT is a relatively simple malware strain that supports reverse shell and file download/upload. The identified malware has two types: one operates as a standalone executable file, while the other runs by being injected into the explorer.exe process.
- Some of the other malware strains delivered in the attacks encompass a keylogger that's installed via a lean Nestdoor variant as well as a dedicated information stealer and a SOCKS5 proxy that exhibits overlaps with a similar proxy tool used by the Lazarus Group.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• a2aefb7ab6c644aa8eeb482e27b2dbc4 • e7fd7f48fbf5635a04e302af50dfb651 • 33b2b5b7c830c34c688cf6ced287e5be • 468c369893d6fc6614d24ea89e149e80 • 3ec2292dc5be0161d25f258f716d92e96c591ab084548679dd7b169f80b2e967 • c419f17b54d5b1dd356af3703e1c31064720521337abed3ffecfed0884d1e235 • 0995f1f2e4bb43ef7e3dcd57c06154fc812394ac214861c5e30084a215018dbe • 42fd586328a0dfa54af5d94905b36eb6ab59a23f49e190468a8dc55380b559fa • 0dca85d00502ed5ddd1e3a1d4cb8a95e3d2e38df • 52c5c2ec17f22d079f36c06516eb6943e6defe58 • 36fb2e182ae4348715825cfbd09eb54de7557a84 • ef3b9d308f38924ebe3970f85c8466613381cd20 • 7416ea48102e2715c87edd49ddbd1526 • 4bc571925a80d4ae4aab1e8900bf753c • 468c369893d6fc6614d24ea89e149e80
Domain	• kmobile.bestunif[.]com
IP address	• 45.58.159[.]237 • 209.127.19[.]223 • 206.72.205[.]117 • 4.246.149[.]227

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Ensure all operating systems and software are up to date with the latest security patches.
- Employ reliable antivirus and antimalware software to detect and block known threats.
- Regularly update these tools to maintain the latest threat intelligence.
- Implement IDPS to detect and prevent unusual network activity, system behavior, or similar threats.
- Enable two-factor authentication (2FA) on your accounts adds an extra layer of security and can help prevent unauthorized access even if your login credentials have been stolen.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.rewterz.com/threat-advisory/andariel-apt-uses-new-dora-rat-to-target-south-korean-institutes-active-iocs
- https://thehackernews.com/2024/06/andariel-hackers-target-south-korean.html