New Bandook RAT Variant Resurfaces, Targeting Windows Machines

Date: 8th January 2024 | Severity: Medium

Summary

New Bandook RAT Variant Resurfaces, Targeting Windows Machines. A new variant of a remote access trojan called Bandook has been observed being propagated via phishing attacks with an aim to infiltrate Windows machines, underscoring the continuous evolution of the malware.

Attack Vectors

- The starting point of the latest attack sequence is an injector component that's designed to decrypt and load the payload into msinfo32.exe, a legitimate Windows binary that gathers system information to diagnose computer issues.
- Fortinet FortiGuard Labs, which identified the activity in October 2023, said the malware is distributed via a PDF file that embeds a link to a password-protected .7z archive
- The malware, besides making Windows Registry changes to establish persistence on the compromised host, establishes contact with a command-and-control (C2) server to retrieve additional payloads and instructions

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	5b49b856ed078c80306a6f190c445138 695ebe3e45a89552d7dabbc2b972ed66 89df83ffca7aae77fe72522173ec71ac cc9283299523aed18b5c82c22b0b9f27 d3577d76430cf9910df854e066331f56 33c172779ac7117e30d37a6fe26361b2175cae03 89f1e932cc37e4515433696e3963bb3163cc4927 90e8f60e0b1f19da57011fba19c04fab0614e757 b9d9d73c162969ef56931cc26928f67dfaae1523 efbeec9846500b7d54d7fbc51de78b92976d1bbc 2e7998a8df9491dad978dee76c63cb1493945b9cf198d856a395ba0fae5c265a 3169171e671315e18949b2ff334db83f81a3962b8389253561c813f01974670b 430b9e91a0936978757eb8c493d06cbd2869f4e332ae00be0b759f2f229ca8ce 8904ce99827280e447cb19cf226f814b24b0b4eec18dd758e7fb93476b7bf8b8 cd78f0f4869d986cf129a6c108264a3517dbcf16ecfc7c88ff3654a6c9be2bca d3e7b5be903eb9a596b9b2b78e5dd28390c6aadb8bdd4ea1ba3d896d99fa0057 e87c338d926cc32c966fce2e968cf6a20c088dc6aedf0467224725ce36c9a525
Ip address	45.67.34.219 77.91.100.237

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit IP address to network team to block in all firewall perimeters.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

Reference Links

https://thehackernews.com/2024/01/new-bandook-rat-variant-resurfaces.html
https://otx.alienvault.com/pulse/65981831fc1332aa2f30e6d3/