Mphasis
The Next Applied

JaskaGO Malware Attacking Windows and MacOS Operating Systems

Date: 27th December 2023 | Severity: High

Summary

JaskaGO, using the Go programming language, signifies a rise in malware trends. Go’s simplicity attracts authors, creating versatile threats.

Despite macOS’s perceived security, JaskaGO eliminates the myth, targeting both macOS and Windows users. It disguises itself as legit software on pirated pages, evolving and spreading since its first Mac-focused appearance in July 2023

Attack Vectors

The malware tricks users with a fake error box on startup, pretending to fail. It checks for virtual machines by examining system details like: -

- Processors
- Memory
- MAC addresses

we have mentioned all the stealers used: -

- Browser stealer
- Cryptocurrency stealer

JaskaGO is a cross-platform threat challenging macOS invulnerability, using anti-VM tactics for stealth, persistently embedding in systems, and transforming into a dangerous threat with stealer capabilities.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	7bc872896748f346fdb2426c774477c4f6dcedc9789a44bd9d3c889f778d5c4b f38a29d96eee9655b537fee8663d78b0c410521e1b88885650a695aad89dbe3f 6efa29a0f9d112cfbb982f7d9c0ddfe395b0b0edb885c2d5409b33ad60ce1435 f2809656e675e9025f4845016f539b88c6887fa247113ff60642bd802e8a15d2 85bffa4587801b863de62b8ab4b048714c5303a1129d621ce97750d2a9a989f9 37f07cc207160109b94693f6e095780bea23e163f788882cc0263cbddac37320 e347d1833f82dc88e28b1baaa2657fe7ecbfe41b265c769cce25f1c0e181d7e0 c714f3985668865594784dba3aeda1d961acc4ea7f59a178851e609966ca5fa6 9b23091e5e0bd973822da1ce9bf1f081987daa3ad8d2924ddc87eee6d1b4570d 1c0e66e2ea354c745aebda07c116f869c6f17d205940bf4f19e0fdf78d5dec26 e69017e410aa185b34e713b658a5aa64bff9992ec1dbd274327a5d4173f6e559 6cdda60ffbc0e767596eb27dc4597ad31b5f5b4ade066f727012de9e510fc186 44d2d0e47071b96a2bd160aeed12239d4114b7ec6c15fd451501c008d53783cf 8ad4f7e14b36ffa6eb7ab4834268a7c4651b1b44c2fc5b940246a7382897c98e 888623644d722f35e4dcc6df83693eab38c1af88ae03e68fd30a96d4f8cbcc01 3f139c3fcad8bd15a714a17d22895389b92852118687f62d7b4c9e57763a88670 60a5d189ccf3fc32a758f1e218f814f6ce81744 3c887ece654ea46b1778d3c7a8a6a7c7c7cfa61c c806c7006950dea6c20d3d2800fe46d9350266b6

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

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.

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://gbhackers.com/jaskago-malware-attacking-windows-and-macos/

https://otx.alienvault.com/pulse/6582b53bca0abfc9ad2fec28/