New Hijack Loader Variant: Uses Process Hollowing, Has Enhanced Anti-Evasion Capabilities

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 20, 2024 /EINPresswire.com/ -- A new version of Hijack Loader, also known as IDAT Loader, has been discovered in the wild with updated anti-evasion capabilities, ANY.RUN reports.

Security researchers found that this new version decrypts and parses a PNG image to load its second stage payload, which features a modular architecture primarily aimed at injecting the main instrumentation module.

To enhance stealth, the malware employs various techniques, including avoiding inline API hooking, adding an exclusion for Windows Defender antivirus, bypassing User Account Control (UAC), and using process hollowing. In total, seven new modules were spotted by security researchers in March and April 2024.

Hijack Loader first appeared in September 2023 and has been growing in popularity, currently ranking as the 6th most detected malware in the ANY.RUN Trends Tracker. The loader is known to deliver various payloads, such as Amadey, Lumma Stealer, Meta Stealer, Racoon Stealer V2, Remcos RAT, and Rhadamanthys.

ANY.RUN sandbox can detect Hijack Loader using YARA rules. Analysis of a sample in ANY.RUN shows that it specifically targets 32-bit versions of Windows. The latest Hijack Loader IOCs, including IPs, hashes, and URLs, are available in ANY.RUN's Malware Trends Tracker for further analysis.

ANY.RUN helps over 400,000 cybersecurity professionals worldwide simplify malware analysis for threats targeting both Windows and Linux systems. The platform offers various advantages, including fast malware detection, real-time interaction with samples, and detailed behavior analysis.

Read more about the latest Hijack Loader discovery and how ANY.RUN can help with its analysis in the blog post.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
Twitter
YouTube