Carbanak Banking Malware Resurfaces with New Ransomware Tactics

By The Hacker News

Published: 2023-12-26 · Archived: 2026-04-05 16:41:32 UTC

The banking malware known as **Carbanak** has been observed being used in ransomware attacks with updated tactics.

"The malware has adapted to incorporate attack vendors and techniques to diversify its effectiveness," cybersecurity firm NCC Group said in an analysis of ransomware attacks that took place in November 2023.

"Carbanak returned last month through new distribution chains and has been distributed through compromised websites to impersonate various business-related software."

Some of the impersonated tools include popular business-related software such as HubSpot, Veeam, and Xero.

Carbanak, detected in the wild since at least 2014, is known for its data exfiltration and remote control features. Starting off as a banking malware, it has been put to use by the FIN7 cybercrime syndicate.

In the latest attack chain documented by NCC Group, the compromised websites are designed to host malicious installer files masquerading as legitimate utilities to trigger the deployment of Carbanak.

The development comes as 442 ransomware attacks were reported last month, up from 341 incidents in October 2023. A total of 4,276 cases have been reported so far this year, which is "less than 1000 incidents fewer than the total for 2021 and 2022 combined (5,198)."

The company's data shows that industrials (33%), consumer cyclicals (18%), and healthcare (11%) emerged as the top targeted sectors, with North America (50%), Europe (30%), and Asia (10%) accounting for most of the attacks.

As for the most commonly spotted ransomware families, LockBit, BlackCat, and Play contributed to 47% (or 206 attacks) of 442 attacks. With BlackCat dismantled by authorities this month, it remains to be seen what impact the move will have on the threat landscape for the near future.

"With one month of the year still to go, the total number of attacks has surpassed 4,000 which marks a huge increase from 2021 and 2022, so it will be interesting to see if ransomware levels continue to climb next year," Matt Hull, global head of threat intelligence at NCC Group, said.

The spike in ransomware attacks in November has also been corroborated by cyber insurance firm Corvus, which said it identified 484 new ransomware victims posted to leak sites.

"The ransomware ecosystem at large has successfully pivoted away from QBot," the company said. "Making software exploits and alternative malware families part of their repertoire is paying off for ransomware groups."

While the shift is the result of a law enforcement takedown of QBot's (aka QakBot) infrastructure, Microsoft, last week, disclosed details of a low-volume phishing campaign distributing the malware, underscoring the challenges in fully dismantling these groups.

The development comes as Kaspersky revealed Akira ransomware's security measures prevent its communication site from being analyzed by raising exceptions while attempting to access the site using a debugger in the web browser.

The Russian cybersecurity company further highlighted ransomware operators' exploitation of different security flaws in the Windows Common Log File System (CLFS) driver – CVE-2022-24521, CVE-2022-37969, CVE-2023-23376, CVE-2023-28252 (CVSS scores: 7.8) – for privilege escalation.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2023/12/carbanak-banking-malware-resurfaces.html