Buhti Ransomware Gang Switches Tactics, Utilizes Leaked LockBit and Babuk Code - RedPacket Security

By April 1, 2026

Published: 2023-05-25 · Archived: 2026-04-05 15:15:07 UTC

The threat actors behind the nascent **Buhti** ransomware have eschewed their custom payload in favor of leaked LockBit and Babuk ransomware families to strike Windows and Linux systems.

“While the group doesn’t develop its own ransomware, it does utilize what appears to be one custom-developed tool, an information stealer designed to search for and archive specified file types,” Symantec said in a report shared with The Hacker News.

The cybersecurity firm is tracking the cybercrime group under the name **Blacktail**. Buhti was first highlighted by Palo Alto Networks Unit 42 in February 2023, describing it as a Golang ransomware targeting the Linux platform.

Later that same month, Bitdefender revealed the use of a Windows variant that was deployed against Zoho ManageEngine products that were vulnerable to critical remote code execution flaws (CVE-2022-47966).

The operators have since been observed swiftly exploiting other severe bugs impacting IBM’s Aspera Faspex file exchange application (CVE-2022-47986) and PaperCut (CVE-2023-27350) to drop the ransomware.

The latest findings from Symantec show that Blacktail’s modus operandi might be changing, what with the actor leveraging modified versions of the leaked LockBit 3.0 and Babuk ransomware source code to target Windows and Linux, respectively.

Both Babuk and LockBit have had its ransomware source code published online in September 2021 and September 2022, spawning multiple imitators.

One notable cybercrime group that's already using the LockBit ransomware builder is the Bl00dy Ransomware Gang, which was recently spotlighted by U.S. government agencies as exploiting vulnerable PaperCut servers in attacks against the education sector in the country.

Despite the rebranding changes, Blacktail has been observed utilizing a custom data exfiltration utility written in Go that's designed to steal files with specific extensions in the form of a ZIP archive prior to encryption.

"While the reuse of leaked payloads is often the hallmark of a less-skilled ransomware operation, Blacktail's general competence in carrying out attacks, coupled with its ability to recognize the utility of newly discovered vulnerabilities, suggests that it is not to be underestimated," Symantec said.

Ransomware continues to pose a persistent threat for enterprises. Fortinet FortiGuard Labs, earlier this month, detailed a Go-based ransomware family called Maori that's specifically designed to run on Linux systems.

While the use of Go and Rust signals an interest on part of threat actors to develop "adaptive" cross-platform ransomware and maximize the attack surface, it's also a sign of an ever-evolving cybercrime ecosystem where new techniques are adopted on a continual basis.

"Major ransomware gangs are borrowing capabilities from either leaked code or code purchased from other cybercriminals, which may improve the functionality of their own malware," Kaspersky noted in its ransomware trends report for 2023.

Indeed, according to Cyble, a new ransomware family dubbed Obsidian ORB takes a leaf out of Chaos, which has also been the foundation for other ransomware strains like BlackSnake and Onyx.

What makes the ransomware stand out is that it employs a rather distinctive ransom payment method, demanding that victims pay the ransom through gift cards as opposed to cryptocurrency payments.

"This approach is effective and convenient for threat actors (TAs) as they can modify and customize the code to their preferences," the cybersecurity firm said.

Source: https://www.redpacketsecurity.com/buhti-ransomware-gang-switches-tactics-utilizes-leaked-lockbit-and-babuk-code/