New Buhti ransomware gang uses leaked Windows, Linux encryptors - RedPacket Security

By March 30, 2026

Published: 2023-05-26 · Archived: 2026-04-05 15:03:18 UTC


Hacker

A new ransomware operation named ‘Buhti’ uses the leaked code of the LockBit and Babuk ransomware families to target Windows and Linux systems, respectively.

While the threat actors behind Buhti, now tracked as ‘Blacktail,’ have not developed their own ransomware strain, they have created a custom data exfiltration utility that they use to blackmail victims, a tactic known as “double-extortion.”

Buhti was first spotted in the wild in February 2023 by Palo Alto Networks’ Unit 42 team, which identified it as a Go-based Linux-targeting ransomware.

A report published today by Symantec’s Threat Hunter team shows that Buhti also targets Windows, using a slightly modified LockBit 3.0 variant codenamed “LockBit Black.”

Ransomware recycling

Blacktail uses the Windows LockBit 3.0 builder that a disgruntled developer leaked on Twitter in September 2022.

Successful attacks change the wallpaper of the breached computers to tell victims to open the ransom note while all encrypted files receive the “.buthi” extension.


Buhti ransom note
Buhti ransom note *(Unit 42)*

For Linux attacks, Blacktail uses a payload based on the Babuk source code that a threat actor posted on a Russian-speaking hacking forum in September 2021.

Earlier this month, SentinelLabs and Cisco Talos highlighted cases of new ransomware operations using Babuk to attack Linux systems.

While malware reuse is generally considered a sign of less sophisticated actors, in this case, multiple ransomware groups gravitate towards Babuk due to its proven capability to compromise VMware ESXi and Linux systems, which are very profitable for cybercriminals.

Blacktail’s traits

Blacktail isn't merely a copycat that repurposes other hackers' tools with minimal modifications. Instead, the new group uses its own custom exfiltration tool and a distinct network infiltration strategy.

Symantec reports that Buhti attacks have been leveraging the recently disclosed PaperCut NG and MF RCE vulnerability that the LockBit and Clop gangs have also exploited.

The attackers rely on CVE-2023-27350 to install Cobalt Strike, Meterpreter, Sliver, AnyDesk, and ConnectWise on target computers, using them to steal credentials and move laterally into compromised networks, steal files, launch additional payloads, and more.

In February, the gang exploited CVE-2022-47986, a critical remote code execution flaw impacting the IBM Aspera Faspex file exchange product.

Buhti's exfiltration tool is a Go-based stealer that can receive command-line arguments that specify the targeted directories in the filesystem.

The tool targets the following file types for theft: pdf, php, png, ppt, psd, rar, raw, rtf, sql, svg, swf, tar, txt, wav, wma, wmv, xls, xml, yml, zip, aiff, aspx, docx, epub, json, mpeg, pptx, xlsx, and yaml.

The files are copied into a ZIP archive and later exfiltrated to Blacktail's servers.

Blacktail, and its ransomware operation Buhti, constitute a modern example of how easy it is for aspiring threat actors to spring into action using effective malware tools and cause significant damage to organizations.

Furthermore, the leaked LockBit and Babuk source code can be used by existing ransomware gangs who want to rebrand under a different name, leaving no connection to previous encryptors.

Kaspersky researcher Marc Rivero told BleepingComputer that they have witnessed hits on Czechia, China, United Kingdom, Ethiopia, United States, France, Belgium, India, Estonia, Germany, Spain, and Switzerland.

This means that Buthi is already a very active ransomware operation, and Blacktail remains a significant threat for organizations worldwide.

Blacktail's tactic of quickly adopting exploits for newly disclosed vulnerabilities makes them a potent threat that calls for increased vigilance and proactive defense strategies like timely patching.

Update 5/25 – Article updated to add extra info from Kaspersky

---

Original Source

To keep up to date follow us on the below channels.

Post navigation

Source: https://www.redpacketsecurity.com/new-buhti-ransomware-gang-uses-leaked-windows-linux-encryptors/