Buhti: New Ransomware Operation Relies on Repurposed Payloads

By About the Author

Archived: 2026-04-05 13:58:18 UTC

A relatively new ransomware operation calling itself Buhti appears to be eschewing developing its own payload and is instead utilizing variants of the leaked LockBit and Babuk ransomware families to attack 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.

Buhti, which first came to public attention in February 2023, was initially reported to be attacking Linux computers. However, Symantec's Threat Hunter Team has also uncovered attempts to attack Windows computers on compromised networks.

The group appears to be quick to exploit recently disclosed vulnerabilities, with one recent attack exploiting the recently patched PaperCut vulnerability. Since Buhti hasn't been linked to any known cyber-crime group, Symantec has assigned the actor name Blacktail to its operators.

LockBit rebrand

A recent Buhti attack saw the attackers attempt to deploy a ransomware payload against Windows computers on the targeted network. Analysis of the payload revealed that it was a minimally modified version of the leaked LockBit 3.0 (aka LockBit Black) ransomware.

Encrypted files are appended with a .buthi extension. The ransom note can be seen in Figure 1.

The ransomware includes a feature that drops a LockBit-branded .bmp file (Figure 2) and makes it the Windows wallpaper, but this functionality was disabled by the attackers.

The ransomware also has the capability to send system information about the infected computer to a command-and-control (C&C) server, but this functionality is also disabled and no C&C server is specified.

LockBit 3.0 was developed for the Syrphid cyber-crime group (aka Bitwise Spider), which is the operator of the LockBit ransomware. The builder for the ransomware was leaked in September 2022, allegedly by a disgruntled developer.

Babuk repurposed

While Buhti came to public attention for targeting Linux machines with a payload written in Golang, analysis by Symantec of multiple Linux payloads found that they were all variants of the leaked Babuk ransomware.

Babuk was one of the first ransomware actors to target ESXi systems with a Linux payload. Babuk's source code was leaked in 2021 and since then has been adopted and reused by multiple ransomware operations.

The ransom note dropped by Linux variants was identical to that of the Windows payload; with only the payment address differing.

Exfiltration tool

Blacktail does appear to use at least one piece of custom malware, a data-exfiltration tool (SHA256: 9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd).

Written in Golang, it is designed to steal the following file types: .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, .yaml. Copied files are placed into a .zip archive, which is created using an open source utility called zip.

The tool can be configured via command-line arguments to specify both the directory to search for files of interest in and the name of the output archive. The -o argument in the command line specifies the archive to be created. The -d argument specifies the directory to search for files of interest in. For example:

CSIDL_WINDOWS\temp\xhfw.exe -o CSIDL_WINDOWS\temp\output.zip -d CSIDL_PROFILE

Vulnerability exploitation

Recent Buhti attacks exploited a recently discovered vulnerability in PaperCut NG and MF (CVE-2023-27350). The exploit allows an attacker to bypass authentication and remotely execute code. The vulnerability was disclosed and patched by PaperCut on March 15, 2023, and in recent weeks multiple threat actors have begun utilizing the exploit against unpatched systems.

The attackers exploited the vulnerability in order to install Cobalt Strike, Meterpreter, Sliver, AnyDesk, and ConnectWise. The tools were leveraged to steal data from, and deliver the ransomware payload to, multiple computers on the targeted network.

Blacktail appears quick to utilise new exploits. In February, they were reported to be exploiting a vulnerability in IBM's Aspera Faspex file-exchange application (CVE-2022-47986).

Dangerous adversary

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.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7 - Buhti (Windows)

eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c - Buhti (Linux)

e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206 - Buhti (Linux)

d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6 - Buhti (Linux)

d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65 - Buhti (Linux)

8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441 - Buhti (Linux)

898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a - Buhti (Linux)

515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855 - Buhti (Linux)

4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880 - Buhti (Linux)

22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe - Buhti (Linux)

18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef - Buhti (Linux)

01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4 - Buhti (Linux)

7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c - Buhti (Linux)

287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52 - Buhti (Linux)

32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c - Cobalt Strike Beacon

5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72 - Cobalt Strike Beacon

d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb - Cobalt Strike Beacon

de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72 - Cobalt Strike Beacon

65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b - Meterpreter

8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334 - Meterpreter

8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2 - Meterpreter

97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a – Meterpreter

c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351 - Meterpreter

9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf - Possible Meterpreter

9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd - Exfiltration tool

ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937 - Possible exfiltration tool

bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24 - Sliver

91.215.85[.]183

81.161.229[.]120
