Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

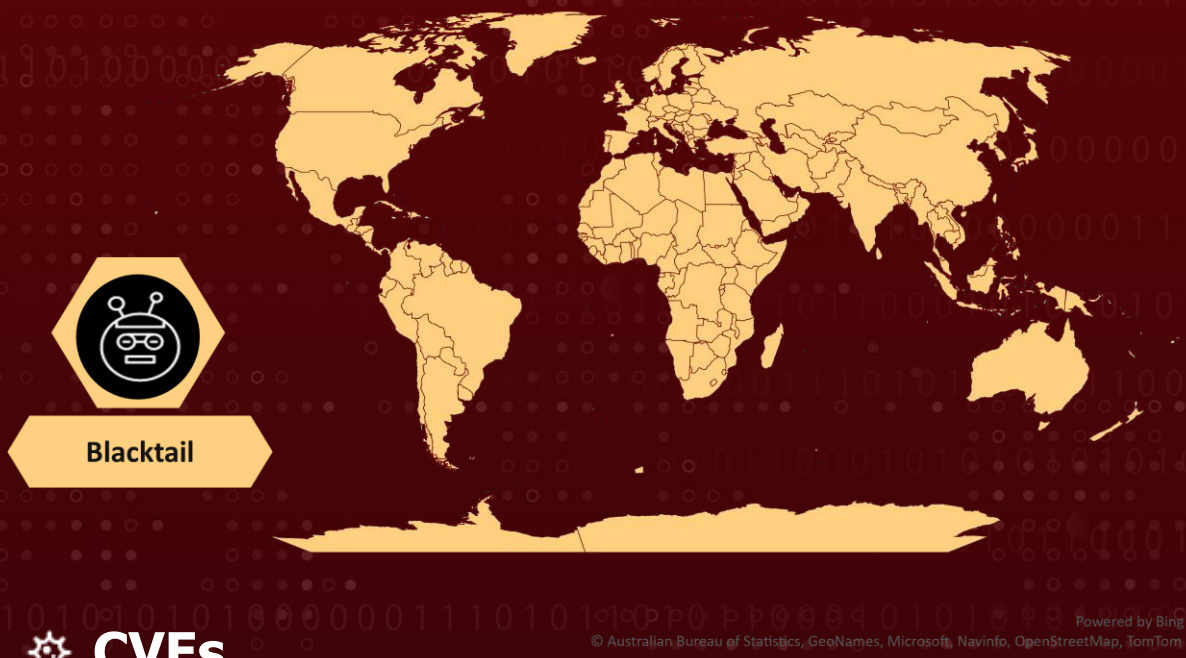
Buhti Ransomware Operation Repurposes Leaked Encryptors

Date of Publication	Admiralty Code	TA Number
May 29, 2023	A1	TA2023248

Summary

First seen: February 2023
Actor: Blacktail
Attack Region: Worldwide
Malware: Buhti Ransomware
Affected Platforms: Windows and Linux systems.
Attack: Buhti ransomware, linked to Blacktail threat actors, employs leaked code of LockBit and Babuk variants. By exploiting vulnerabilities like PaperCut NG, they exfiltrate data and distribute ransomware. The addition of a custom Golang exfiltration tool heightens the evolving threat.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF and NG	✗	✓	✓
CVE-2022-47986	IBM Aspera Faspex Code Execution Vulnerability	IBM Aspera Faspex	✗	✓	✓

Attack Details

#1

Buhti, a relatively new ransomware operation, has emerged in cybersecurity. Interestingly, instead of developing its own malicious payload, Buhti has chosen to utilize variants of the leaked LockBit and Babuk ransomware families to target both Windows and Linux systems. It came to the public's attention in February 2023 and is now associated with a threat actor group known as Blacktail.

#2

Although Blacktail does not develop its own ransomware, they have created a customized data exfiltration utility, which is essentially a slightly modified version of the leaked LockBit 3.0 (also known as LockBit Black) ransomware. Additionally, it is worth noting that Blacktail employs at least one piece of custom malware—a data-exfiltration tool coded in Golang. The Blacktail group demonstrates a swift response to exploiting recently disclosed vulnerabilities. Their attacks specifically focused on a recently discovered vulnerability in PaperCut NG and MF (CVE-2023-27350).

#3

This vulnerability allows attackers to bypass authentication and execute code remotely. Through this exploit, the attackers successfully deployed various tools like Cobalt Strike, Meterpreter, Sliver, AnyDesk, and ConnectWise. These tools were employed to steal data and distribute the Buhti ransomware payload across numerous computers in the targeted network. In February, Blacktail promptly leveraged new exploits, particularly those reported for a vulnerability found in IBM's Aspera Faspex file exchange application (CVE-2022-47986).

Recommendations

Ensure timely patching: Given the swift exploitation of recently disclosed vulnerabilities by threat actors like Blacktail, it is crucial to prioritize regular patching of systems and software. Timely patching can help prevent unauthorized access and remote code execution, mitigating the risk of ransomware attacks.

Implement multi-layered security measures: Organizations should adopt a multi-layered security approach to defend against evolving ransomware operations like Buhti. This includes a combination of robust endpoint protection, network segmentation, intrusion detection systems, and user awareness training to detect and prevent potential threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0009 Collection	TA0040 Impact	T1047 Windows Management Instrumentation	T1059 Command and Scripting Interpreter
T1129 Shared Modules	T1027 Obfuscated Files or Information	T1036 Masquerading	T1497 Virtualization/Sandbox Evasion
T1003 OS Credential Dumping	T1056 Input Capture	T1056.001 Keylogging	T1057 Process Discovery
T1082 System Information Discovery	T1083 File and Directory Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery
T1005 Data from Local System	T1185 Browser Session Hijacking	T1486 Data Encrypted for Impact	T1489 Service Stop

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	91.215.85[.]183 81.161.229[.]120
SHA256	063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7 eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206 d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6 d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65

TYPE	VALUE
SHA256	8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441 898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a 515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855 4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880 22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe 18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef 01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4 7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c 287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52 32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c 5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72 d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72 65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b 8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334 8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2 97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351 9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf 9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937 Bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24

Patch Links

https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

https://www.ibm.com/support/pages/node/6952319

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buhti-ransomware

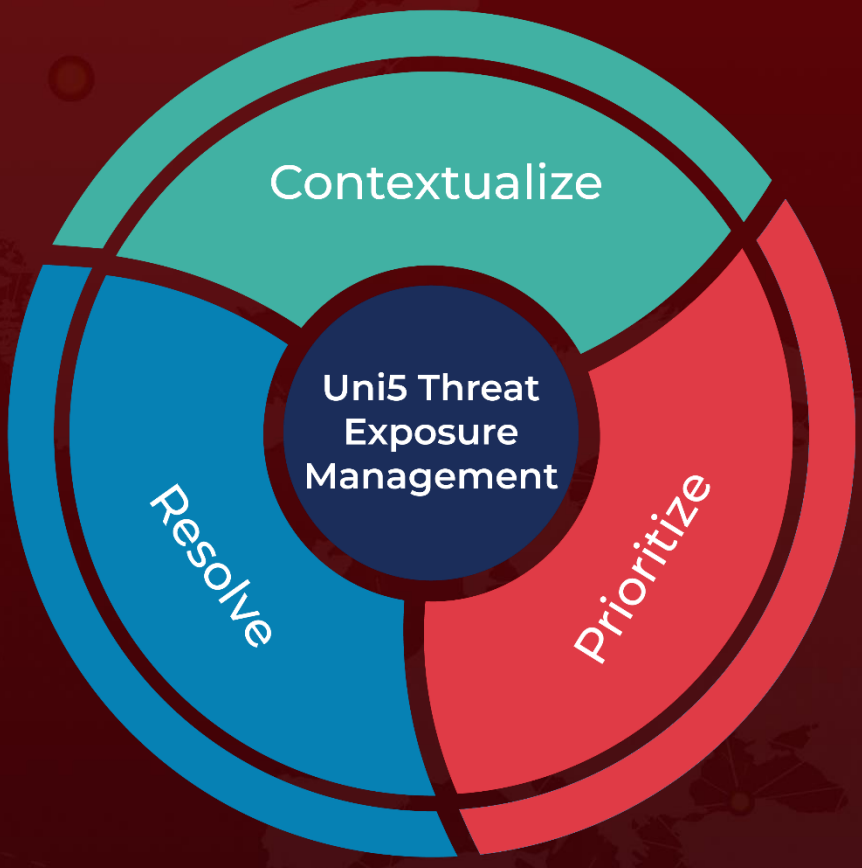
https://www.hivepro.com/critical-papercut-security-vulnerabilities-actively-exploited-in-the-wild/

https://www.hivepro.com/cisas-known-exploited-vulnerability-catalog-february-2023/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 29, 2023 • 5:55 AM

More at www.hivepro.com