Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

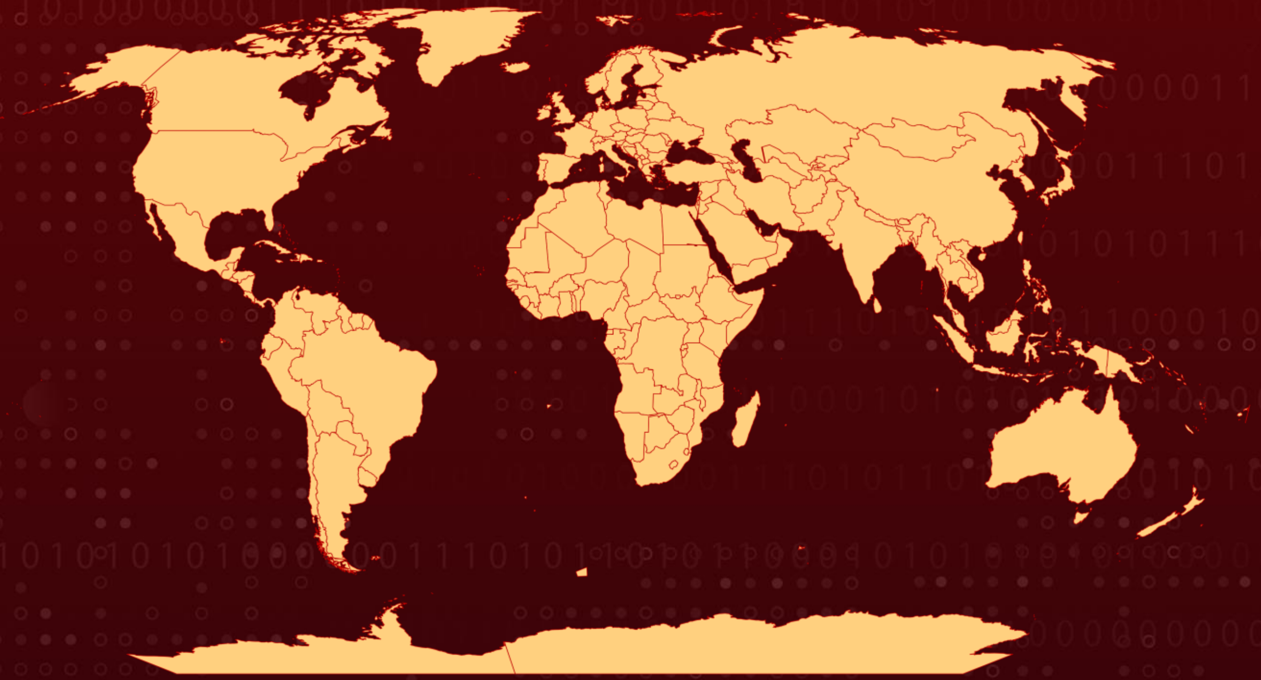
Advanced BlackCat Ransomware Using Triple Extortion Tactics and Signed Kernel Driver

Date of Publication	Admiralty Code	TA Number
May 23, 2023	A1	TA2023241

Summary

First Appearance: February 2023
Malware: BlackCat Ransomware (aka ALPHV, AlphaV, AlphaVM, ALPHV-ng, or Noberus)
Targeted Countries: Worldwide
Ransom Demands: $1.5 million - $3 million
Affected Platforms: Windows, Linux, and VMware ESXi
Attack: The BlackCat ransomware operation is a highly sophisticated and customizable threat targeting corporate environments, featuring advanced encryption, spreading capabilities, and triple extortion tactics. It utilizes a signed kernel driver for defense evasion recently.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

ALPHV ransomware, also known as BlackCat, is a sophisticated ransomware operation that emerged recently. It is considered one of the most advanced ransomware variants of the year, with a wide range of customizable features for targeting corporate environments. The ransomware is written in Rust, a programming language known for its high performance and memory safety.

#2

ALPHV BlackCat operates as a ransomware-as-a-service (RaaS) where affiliates are recruited to carry out corporate breaches and encrypt devices. Affiliates receive varying revenue shares based on the size of the ransom payment they generate. The ransomware offers multiple encryption modes and algorithms, allowing for flexibility and optimization in the encryption process.

#3

The ransomware is designed to be command-line driven, highly configurable, and capable of performing various actions such as spreading between computers, killing virtual machines, wiping ESXi snapshots, and more. It also has the ability to encrypt files on different operating systems, including Windows, ESXi, Debian, Ubuntu, and ReadyNAS/Synology.

#4

ALPHV BlackCat incorporates a cross-platform approach, ensuring that files can be decrypted even when mounted on different operating systems. The ransomware is known to demand ransoms ranging from $400,000 to $3 million, payable in Bitcoin or Monero. Additionally, it employs a triple-extortion tactic by stealing data before encrypting devices and threatening to publish the data if the ransom is not paid.

#5

One notable feature of ALPHV BlackCat is the use of signed kernel drivers for defense evasion. These drivers are employed to gain privileged-level access and impair security measures on targeted systems. The ransomware operators use different methods to sign their malicious kernel drivers, including abusing Microsoft signing portals or utilizing stolen or leaked cross-signing certificates.

Recommendations

Maintain up-to-date systems and security measures: Keep all software, applications, and operating systems patched and updated with the latest security fixes. Deploy reputable antivirus and anti-malware solutions to detect and prevent ALPHV BlackCat ransomware infections.

Regularly back up critical data and test restoration: Conduct regular backups of important data and verify the integrity of backups by testing the restoration process. Store backups offline or in a separate and secure network to prevent them from being compromised in case of a ransomware attack.

Implement strong access controls and user awareness: Enforce strong password policies and encourage the use of multi-factor authentication (MFA). Educate employees about phishing attacks, safe browsing practices, and the importance of not opening suspicious email attachments or clicking on unknown links.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	**TA0002** Execution	**TA0008** Lateral Movement	**TA0004** Privilege Escalation
TA0011 Command and Control	**TA0042** Resource Development	**TA0005** Defense Evasion	**TA0040** Impact
TA0001 Initial Access	**TA0006** Credential Access	**T1569** System Services	**T1027** Obfuscated Files or Information
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1110** Brute Force	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools	**T1562.009** Safe Mode Boot	**T1489** Service Stop	**T1057** Process Discovery
T1649 Steal or Forge Authentication Certificates	**T1588.003** Code Signing Certificates	**T1529** System Shutdown/Reboot	**T1566** Phishing

T1588 Obtain Capabilities	**T1564** Hide Artifacts	**T1486** Data Encrypted for Impact	**T1210** Exploitation of Remote Services
T1078 Valid Accounts	**T1505** Server Software Component	**T1021** Remote Services	**T1068** Exploitation for Privilege Escalation
T1040 Network Sniffing	**T1041** Exfiltration Over C2 Channel	**T1046** Network Service Scanning	**T1047** Windows Management Instrumentation
T1106 Native API	**T1119** Automated Collection	**T1553** Subvert Trust Controls	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677 c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497
MD5	909f3fc221acbe999483c87d9ead024a a837302307dace2a00d07202b661bce2
SHA1	17bd8fda268cbb009508c014b7c0ff9d8284f850 78cd4dfb251b21b53592322570cc32c6678aa468 c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91 91568d7a82cc7677f6b13f11bea5c40cf12d281b 0bec69c1b22603e9a385495fbe94700ac36b28e5 5ed22c0033aed380aa154e672e8db3a2d4c195c4 cb25a5125fb353496b59b910263209f273f3552d 994e3f5dd082f5d82f9cc84108a60d359910ba79 f6793243ad20359d8be40d3accac168a15a327fb b2f955b3e6107f831ebe67997f8586d4fe9f3e98

References

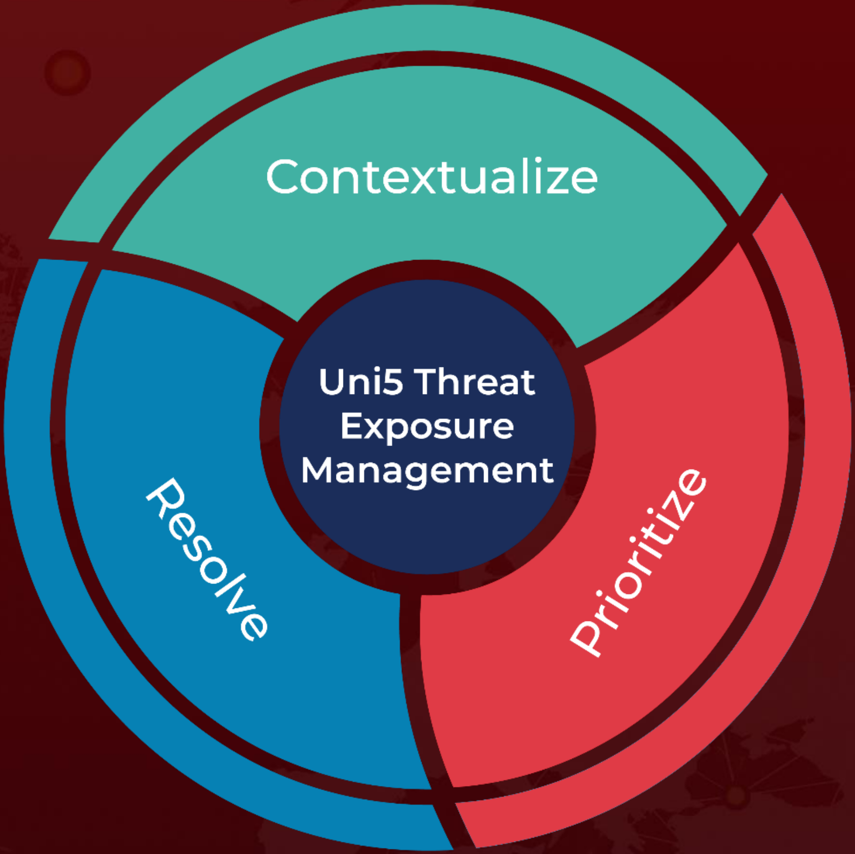
https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver/indicators-blackcat-ransomware-deploys-new-signed-kernel-driver.txt

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 23, 2023 • 6:30 AM

More at www.hivepro.com