Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

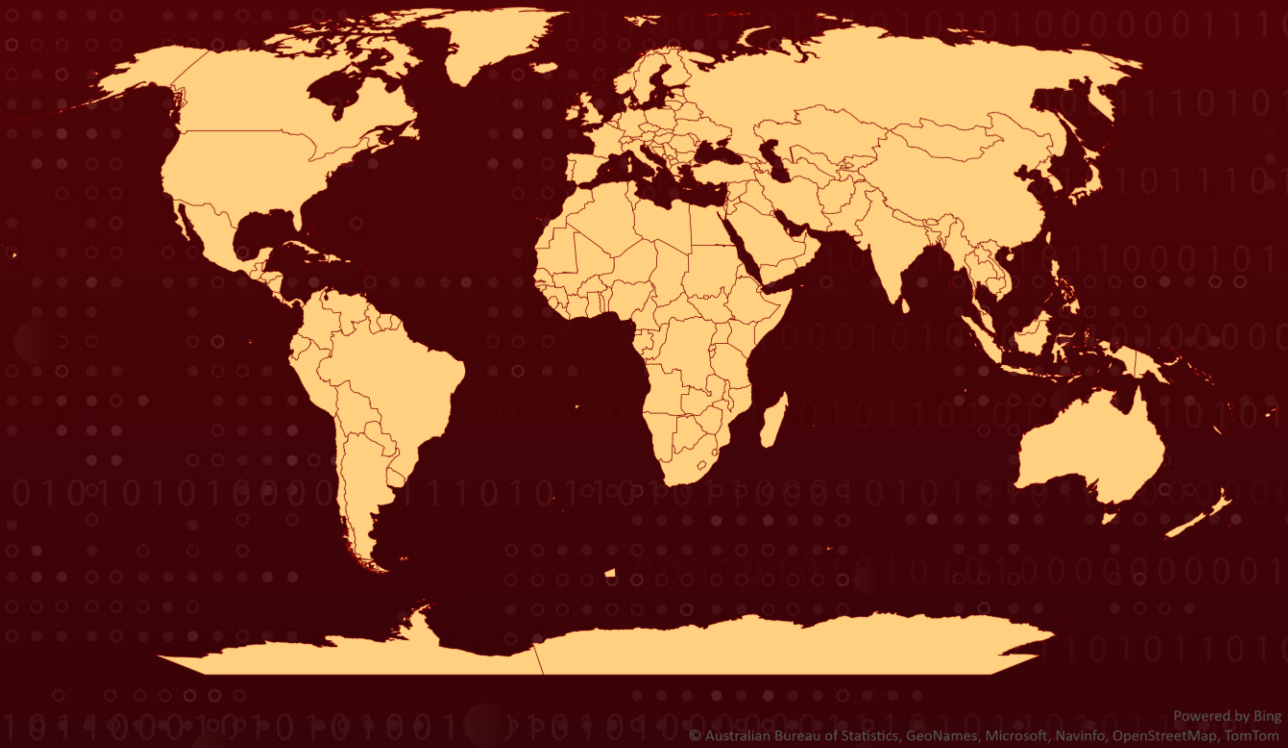
HardBit Ransomware: A Threatening Cyber Attack Targeting Organizations with New Version 2.0

Date of Publication	Admiralty Code	TA Number
February 22, 2023	A1	TA2023097

Summary

First Appearance: October 2022
Target Countries: Worldwide
Malware: HardBit Ransomware
Affected Platform: Windows
Attack: HardBit is a ransomware group that targets organizations and demands cryptocurrency payments for decrypting data. Recently, they have employed a new extortion tactic of demanding to know the victim's cyber insurance coverage in order to extort millions of dollars in ransom.

Attack Regions


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

Attack Details

#1

HardBit is a ransomware strain that focuses on extorting cryptocurrency payments from organizations in exchange for data decryption. It first emerged in October 2022, and a newer version, HardBit 2.0, surfaced at the end of November of the same year. To negotiate ransom demands, the group behind HardBit urges victims to reach out to them via email or the Tox instant messaging platform. More recently, the group has adopted a new tactic demanding to be informed of the victim's cyber insurance coverage to increase their ransom demands, potentially extorting millions of dollars from the victim.

#2

HardBit gathers information about the victim host via web-based enterprise management and Windows Management Instrumentation (WMI) functions to evade analysis in the victim's sandbox environment. Additionally, HardBit performs a number of pre-encryption steps to lower the security posture of the victim host, including deleting the Volume Shadow Copy Service (VSS), deleting the Windows backup utility catalog and shadow copies, editing the boot configuration, disabling many Windows Defender Antivirus features, terminating services, and establishing persistence.

#3

Finally, the HardBit ransomware payload is automatically executed whenever the system is rebooted. Organizations should continue to follow general counter-ransomware advice to limit exposure to risk, reduce the incentive for these groups to operate, and avoid ransom payments.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the ’Potential MITRE ATT&CK TTPs’ & ‘Indicators of Compromise (IoC)’ on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0007 Discovery	TA0040 Impact
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	T1204 User Execution
T1059 Command and Scripting Interpreter	T1588 Obtain Capabilities	T1562 Impair Defenses	T1027 Obfuscated Files or Information
T1588.006 Vulnerabilities	T1047 Windows Management Instrumentation	T1012 Query Registry	T1586 Compromise Accounts
T1490 Inhibit System Recovery	T1070 Indicator Removal	T1070.004 File Deletion	T1204.002 Malicious File
T1140 Deobfuscate/Decode Files or Information	T1012 Query Registry	T1005 Data from Local System	T1529 System Shutdown/Reboot

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 b565a7b25dc4227872fe972ceee9ff8fce91eb10b373ebc9401f4f32348244ef 422e0e4e01c826c8a9f31cb3a3b37ba29fb4b4b8c4841e16194258435056d8a3 a0138b24593483f50ae7656985b6d6cfe77f7676ba374026199ad49ad26f2992 cb239d641cfa610b1eaf0ecd0f48c42dd147f547b888e4505297c4e9521d8afe fafbe16c5646bf1776dd3ef62ba905b9b2cb0ee51043859a2f3cdda7dfe20d4c

TYPE	VALUE
Email ID	alexgod5566@xyzmailpro[.]com filetest@decoymail[.]net filetest@onionmail[.]org godgood55@tutanota[.]com

References

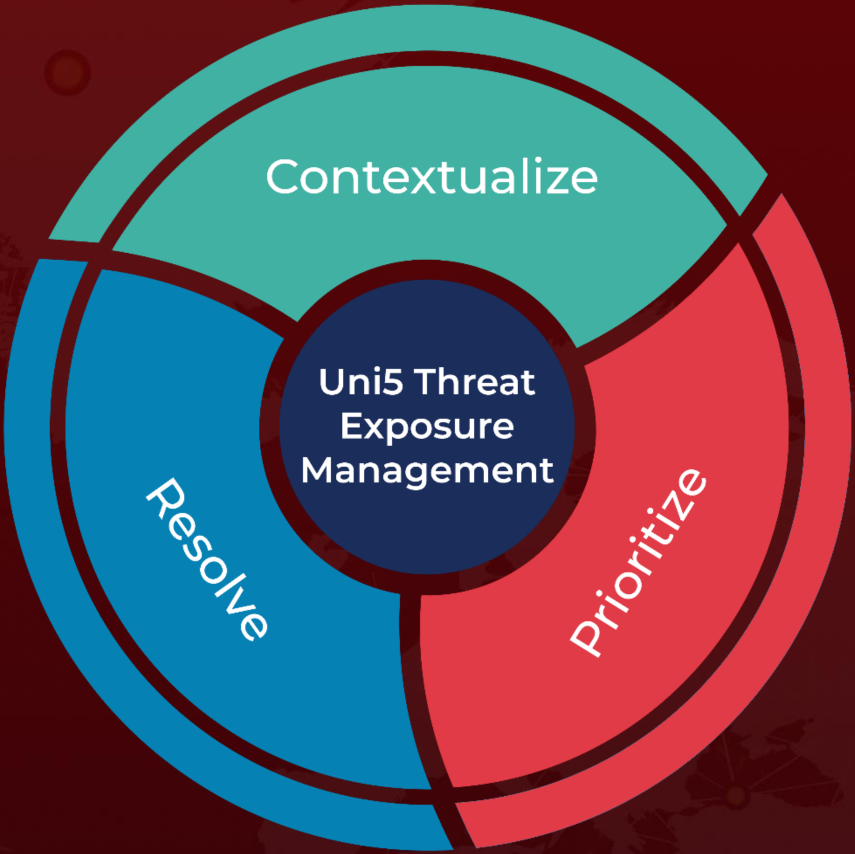
https://www.varonis.com/blog/hardbit-2.0-ransomware

https://www.bankinfosecurity.com/new-hardbit-20-ransomware-tactics-target-insurance-coverage-a-21286

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

February 22, 2023 • 11:00 PM

More at www.hivepro.com