Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

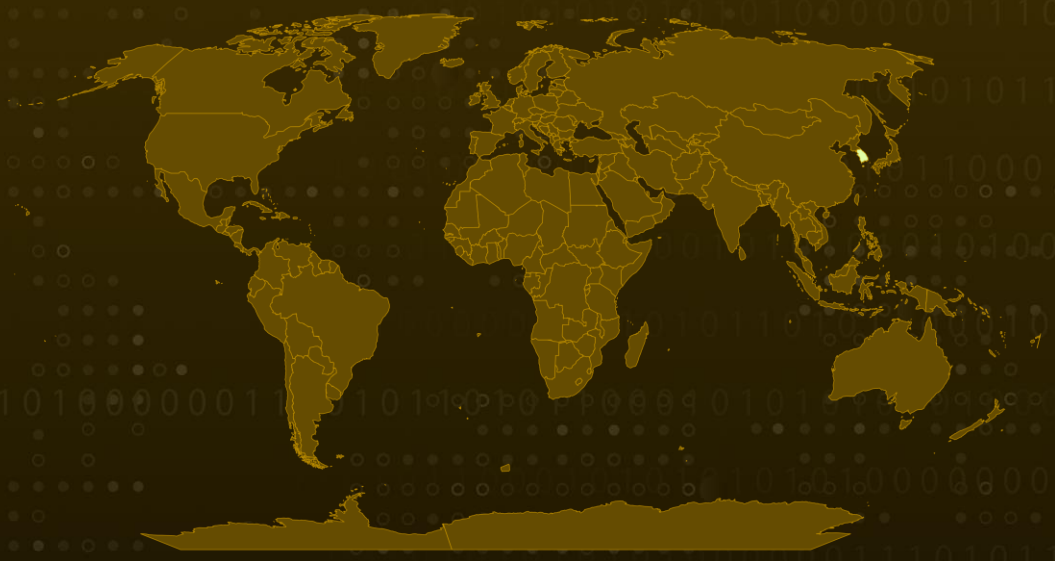
New BlackBit Ransomware Targets South Korea

Date of Publication	Admiralty Code	TA Number
May 5, 2023	A1	TA2023213

Summary

Attack Began: September 2022
Attack Country: South Korea
Malware: BlackBit
Attack: The BlackBit ransomware, a variant of LokiLocker with cosmetic changes, checks keyboard layout, establishes persistence, removes backups, disables defenses, and presents payment information through various methods, making it a sophisticated strain that could cause immense financial and data losses if not detected and mitigated.

Attack Regions



Attack Details

#1

A new variant of ransomware, BlackBit, that is being distributed in Korea. The ransomware is a copy of the LokiLocker with some cosmetic changes, such as icons, name, and color scheme. It operates on the Ransomware-as-a-Service (RaaS) model and has several capabilities, including establishing persistence, defense evasion, and impairing recovery.

#2

When executed, the ransomware first checks the keyboard layout of the victim's system using a killswitch. If the system language is determined to be Persian, the ransomware terminates itself. If not, it proceeds with further operations. The ransomware creates a mutex object and locks it to ensure that only one instance of the ransomware is running at any given time. It then establishes persistence on the infected system by copying itself to various locations, including the startup folder, and creates a Task Scheduler entry for the file.

#3

After establishing persistence, the ransomware executes commands to remove all backups from the infected system, including deleting shadow copies and disabling recovery mode. It then disables Windows Defender and the system's firewall. The ransomware incorporates three methods for presenting payment information to the victim, including dropping ransom notes, displaying pop-ups when the victim tries to open encrypted files, and presenting an HTA page via mshta.exe.

Recommendations

Employ strict access control measures: To prevent the BlackBit from gaining unauthorized access to critical systems and sensitive information, implement strict access control measures such as multi-factor authentication, strong password policies, and role-based access control.

Use threat intelligence: Keep up-to-date with the latest threat intelligence to identify potential attacks and respond quickly to any suspicious activity. Use this information to monitor for activity associated with BlackBit.

Conduct regular security awareness training: Employees should be regularly trained on how to identify and respond to phishing attacks, social engineering tactics, and other common techniques used by threat actors like.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery	TA0040 Impact
T1059 Command and Scripting Interpreter	T1204 User Execution	T1047 Windows Management Instrumentation	T1564 Hide Artifacts
T1070 Indicator Removal	T1082 System Information Discovery	T1083 File and Directory Discovery	T1057 Process Discovery
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	90bae9356dc021172d0ff06603e7a4cf bf528ecf7601043fe7931ed1fdd1d081 9d898e39591f9a8b49fa27841acb7392 d37b49b0a53fd07895ca4dc956cbc459 8ead445620033ecee6c426cfbeac214b
SHA1	b04ccaa781be7521d50faa36db269f71ac56af58 2f052cc3e64870b8ac28efb2d79bc2b16dff3e8e e9b35995bf772cd11be13bc5c9ac93c846f00405 3cac81473dd91e7adf4516f1805bc5bdfeb562e4 7fd07c934ce9b7c4ad902408ed528acf4ce32ddb
SHA256	1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e603161e3f18db2f b8ffd72534056ea89bfd48cbe6efb0b4d627a6284a7b763fdb7dfd070c1049ba 43c6aef23a90c742274d6db2148a5cb5027c82e94ba2db4ae4b4184956e370b5 cd29a952a51204f2e8744271b822c277b63ad8a54e3a6422e342eb9c53df0bda b3324b629febeefb17201abb52bc66094b4ffb292f8aa3a549f39e7e11c63694

References

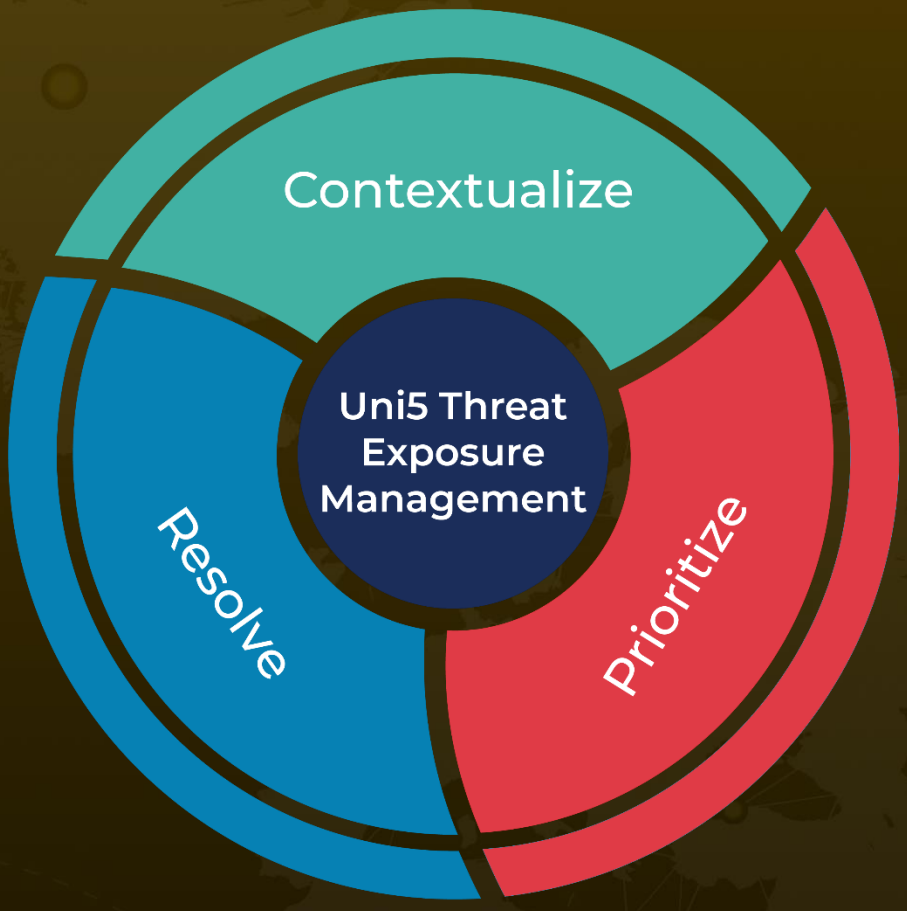
https://blog.cyble.com/2023/05/03/blackbit-ransomware-a-threat-from-the-shadows-of-lokilocker/

https://asec.ahnlab.com/en/51497/

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 5, 2023 • 5:15 AM

More at www.hivepro.com