Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

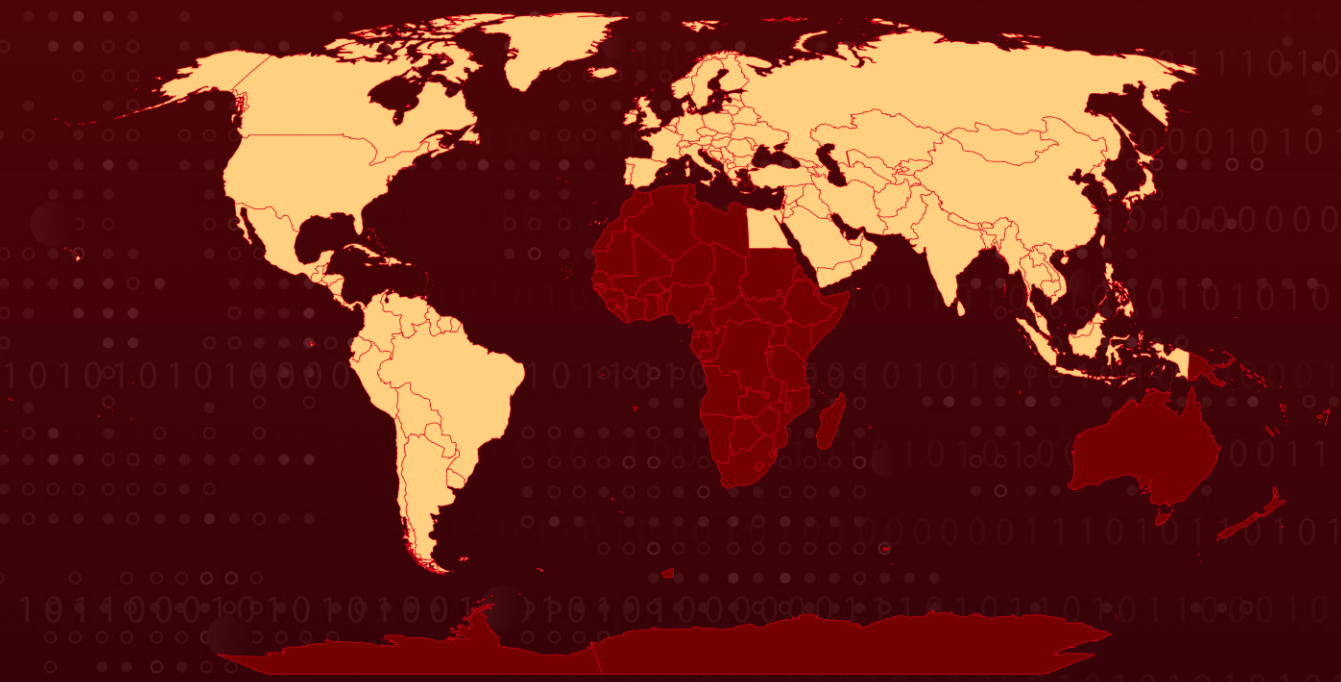
Abyss Locker's Substantial Threat Explored

Date of Publication	Admiralty Code	TA Number
February 27, 2024	A1	TA2024077

Summary

First Seen: July 2023
Malware: Abyss Locker ransomware (aka AbyssLocker)
Attack Region: Europe, North America, South America, and Asia
Targeted Industries: Horticulture, Management Consulting, Architecture, Automotive, Technology, Healthcare, Financial, Manufacturing
Affected Platforms: Windows, Linux
Attack: Abyss Locker ransomware surfaced in July 2023, deriving from the HelloKitty ransomware source code, indicating a lineage predating its official release. Similar to other ransomware variants, Abyss Locker infiltrates corporate networks, exfiltrates data for extortion, and encrypts devices, posing a considerable threat to both Linux and Windows systems.

Attack Regions



Attack Details

#1 The Abyss Locker, active since July 2023, has its origins in the HelloKitty ransomware source code, implying a lineage preceding its official release. Similar to other ransomware entities, Abyss Locker threat actors infiltrate corporate networks, pilfer data for extortion, and encrypt devices within the network.

#2 Notably, the ransomware possesses the capability to eliminate Volume Shadow Copies and system backups, presenting a significant threat to both Linux and Windows systems. The initial approach employed by Abyss Locker ransomware shows variability, with affiliated threat actors observed in the past using SSH brute force attacks to gain entry to exposed servers.

#3 In the Linux domain, Abyss Locker payloads are derived from the Babuk codebase, demonstrating analogous functionality. Geographically, the ransomware targets various regions, with a primary focus on the United States, particularly affecting sectors such as healthcare, manufacturing, and technology. The Windows version of Abyss Locker encrypts files on compromised machines, adding a ".abyss" extension to the encrypted files and leaving a ransom note labeled "WhatHappened.txt."

#4 In contrast, the Linux version appends a ".crypt" extension to encrypted files and generates ransom notes with a ".README_TO_RESTORE" extension. Notably, as of now, the Abyss Locker ransomware threat actor does not appear to maintain a TOR site that exposes victims' names or allows others to view stolen data.

Recommendations

Robust Backup and Recovery Planning: Implement frequent backups for all assets to ensure their complete safety. Utilize the 3-2-1-1 backup structure and employ specialized tools to enhance backup resilience and accessibility. Regularly test the backup and recovery procedures to validate their effectiveness.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0040** Impact
T1562 Impair Defenses	**T1059** Command and Scripting Interpreter	**T1486** Data Encrypted for Impact	**T1027** Obfuscated Files or Information
T1057 Process Discovery	**T1055** Process Injection	**T1041** Exfiltration Over C2 Channel	**T1036** Masquerading
T1070 Indicator Removal	**T1070.004** File Deletion	**T1490** Inhibit System Recovery	**T1082** System Information Discovery
T1083 File and Directory Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	72310e31280b7e90ebc9a32cb33674060a3587663c0334daef76c2ae2cc2a462, 3fd080ef4cc5fbf8bf0e8736af00af973d5e41c105b4cd69522a0a3c34c96b6d, 9243bdcbe30fbd430a841a623e9e1bcc894e4fdc136d46e702a94dad4b10dfdc, 0763e887924f6c7afad58e7675ecfe34ab615f4bd8f569759b1c33f0b6d08c64,

TYPE	VALUE
SHA256	dee2af08e1f5bb89e7bad79fae5c39c71ff089083d65da1c03c7a4c051fabae0, e6537d30d66727c5a306dc291f02ceb9d2b48bffe89dd5eff7aa2d22e28b6d7c, 1d04d9a8eeed0e1371afed06dcc7300c7b8ca341fe2d4d777191a26dabac3596, 1a31b8e23ccc7933c442d88523210c89cebd2c199d9ebb88b3d16eacbefe4120, 25ce2fec4cd164a93dee5d00ab547ebe47a4b713cced567ab9aca4a7080afcb7, b524773160f3cb3bfb96e7704ef31a986a179395d40a578edce8257862cafe5f, 362a16c5e86f13700bdf2d58f6c0ab26e289b6a5c10ad2769f3412ec0b2da711, e5417c7a24aa6f952170e9dfcfdf044c2a7259a03a7683c3ddb72512ad0cd5c7, 056220ff4204783d8cc8e596b3fc463a2e6b130db08ec923f17c9a78aa2032da, 877c8a1c391e21727b2cdb2f87c7b0b37fb7be1d8dd2d941f5c20b30eb65ee97, 2e42b9ded573e97c095e45dad0bdd2a2d6a0a99e4f7242695054217e2bba6829

Recent Breaches

https://www.vanwingerden.com/
https://www.mranet.org/
https://www.posen.com/
https://transaxle.com/
https://deltron.com/
https://vidalung.ai/
https://synergyfinancialgrp.com/
https://micrometals.com/

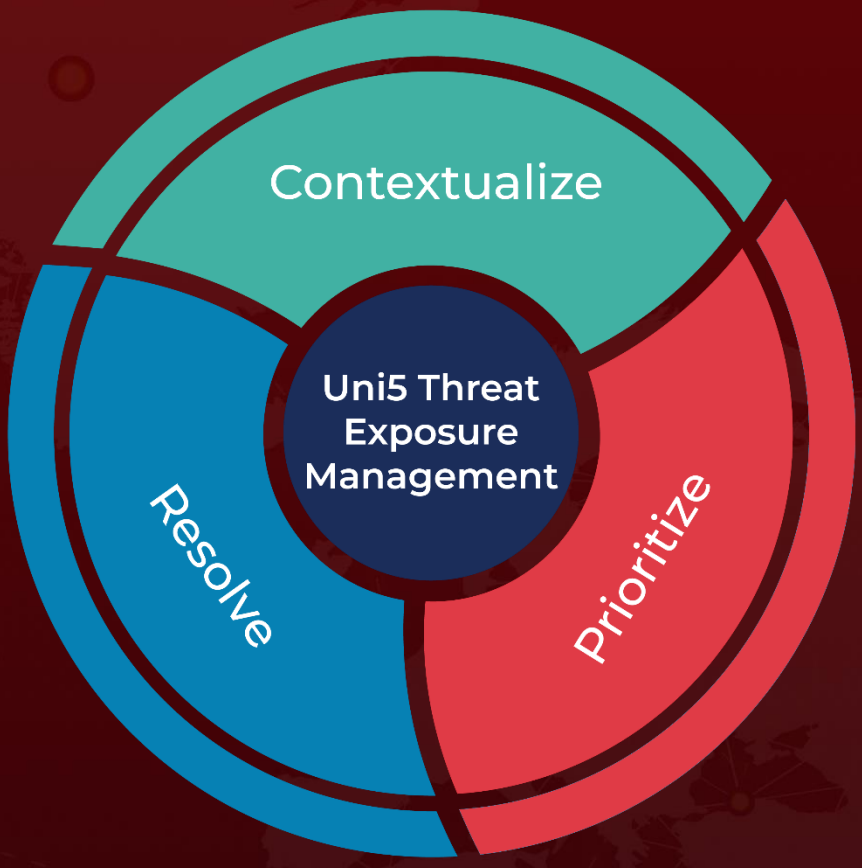
References

https://www.fortinet.com/blog/threat-research/ransomware-roundup-abyss-locker

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 27, 2024 • 4:40 AM

More at www.hivepro.com