Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Lyrix Ransomware Turns Recovery Options Into Hollow Promises

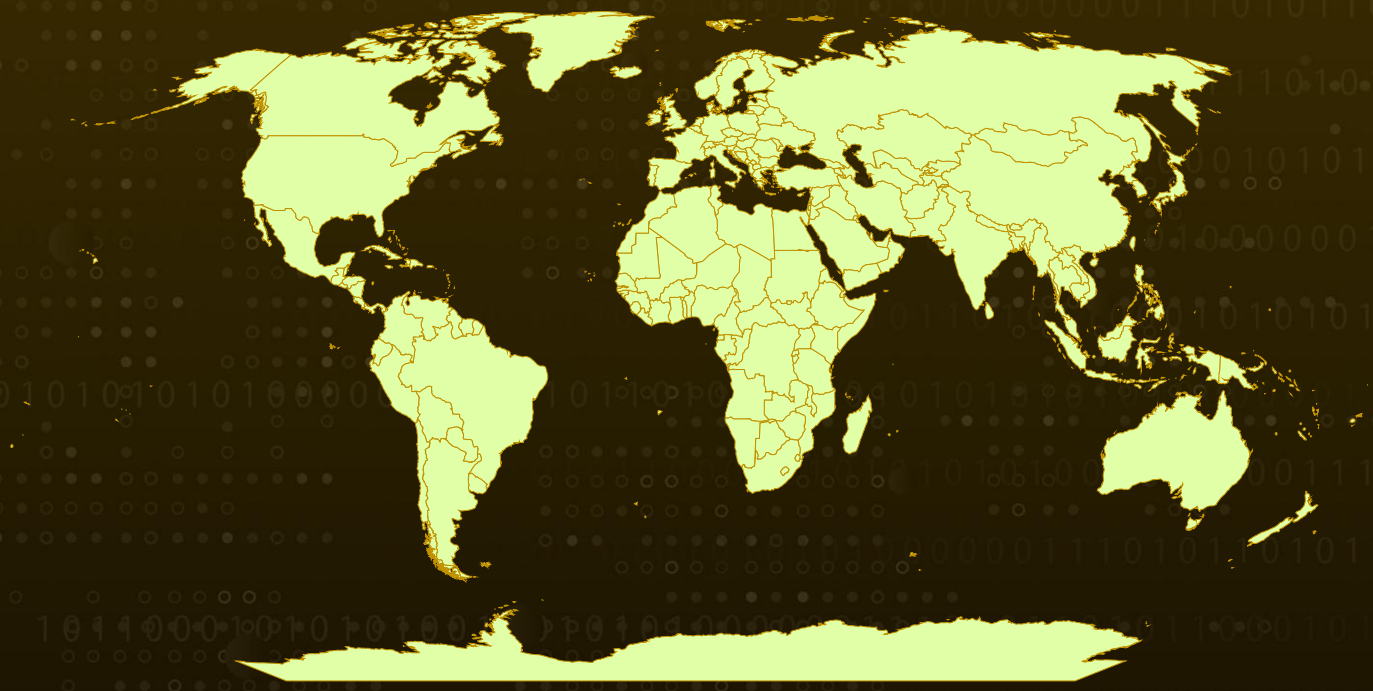
Date of Publication	Admiralty Code	TA Number
June 4, 2025	A1	TA2025171

Summary

First Appeared: April 20, 2025
Malware: Lyrix Ransomware
Targeted Region: Worldwide
Targeted Platform: Windows
Ransom: $50,000 to $2 million

Attack: In April 2025, a new ransomware strain named Lyrix surfaced, targeting Windows systems with sophisticated evasion techniques and disabling critical recovery mechanisms. By combining strong encryption, data theft, and the systematic dismantling of recovery options, Lyrix leaves victims with few choices, forcing them to risk permanent data loss.

Attack Regions



Attack Details

#1 In April 2025, a new ransomware strain named Lyrix was identified in the wild. Developed in Python and converted into a Windows executable using PyInstaller, Lyrix specifically targets Windows-based systems, employing robust encryption techniques and appending a unique file extension to every encrypted file it touches.

#2 From the moment it infects a system, Lyrix deploys a series of sophisticated evasion tactics. It leverages the Windows API function VirtualProtect to detect whether it's running inside a virtualized environment. To further complicate detection, it uses the Sleep function to delay its malicious activities, hoping to outlast automated sandbox analyses and avoid triggering security alerts.

#3 Once it establishes itself, Lyrix executes critical system commands designed to cripple recovery options. It begins by deleting all Volume Shadow Copies, the automatic backup snapshots Windows uses for system restores and file history recovery. As a precaution, it runs the wmic shadow copy delete command to ensure complete removal.

#4 The ransomware then modifies the system's boot configuration data (BCD), disabling error recovery messages and startup repair prompts. As a final blow, it deactivates the Windows Recovery Environment (WinRE), effectively locking users out of vital recovery tools during system boot. This layered sabotage ensures victims have virtually no options to restore their data without complying with the ransom demand.

#5 Encrypted files are renamed with an unusual extension: .02dq34jROu. Alongside the encrypted files, a ransom note titled README.txt is dropped into every affected folder. In this message, victims are informed that their data has been both encrypted and stolen.

#6 The attackers offer to decrypt two files free of charge as proof and demand a ransom payment to unlock the remaining data. The note also threatens to leak the stolen information if payment is not made, providing victims with a unique ID and contact instructions.

Recommendations

Deploy Distributed Ledger Technologies (DLT) for Data Integrity: Leverage blockchain or other Distributed Ledger Technologies (DLT) to create tamper-proof logs of critical system data. This ensures that even if ransomware compromises a system, the logs cannot be altered, offering valuable evidence for forensic investigations and providing a reliable method for restoring integrity.

Use Offline and Immutable Backups: Maintain regular backups of critical files, ideally in offline or immutable storage. Ensure these backups are tested for integrity and can be restored swiftly in case of an attack. Backup integrity checks should be performed frequently to ensure successful recovery when needed.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0040** Impact
T1059 Command and Scripting Interpreter	**T1129** Shared Modules	**T1542** Pre-OS Boot	**T1542.003** Bootkit
T1574 Hijack Execution Flow	**T1055** Process Injection	**T1014** Rootkit	**T1027** Obfuscated Files or Information
T1027.002 Software Packing	**T1036** Masquerading	**T1070.006** Timestomp	**T1202** Indirect Command Execution
T1497 Virtualization/Sandbox Evasion	**T1497.001** System Checks	**T1564** Hide Artifacts	**T1564.001** Hidden Files and Directories
T1564.003 Hidden Window	**T1057** Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1518.001 Security Software Discovery	**T1518** Software Discovery	**T1070.004** File Deletion	**T1070.001** Clear Windows Event Logs

T1486 Data Encrypted for Impact	**T1490** Inhibit System Recovery	**T1005** Data from Local System	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	d298fb4197d65eabf1ef427c2eb737f1, 72a8f2c6e5628f5e8e3c4dc7dcdb93cb
SHA256	fcfa43ecb55ba6a46d8351257a491025022f85e9ae9d5e93d945073f612c877b, 77706303f801496d82f83189beff412d83a362f017cadecc7a3e349a699ce458

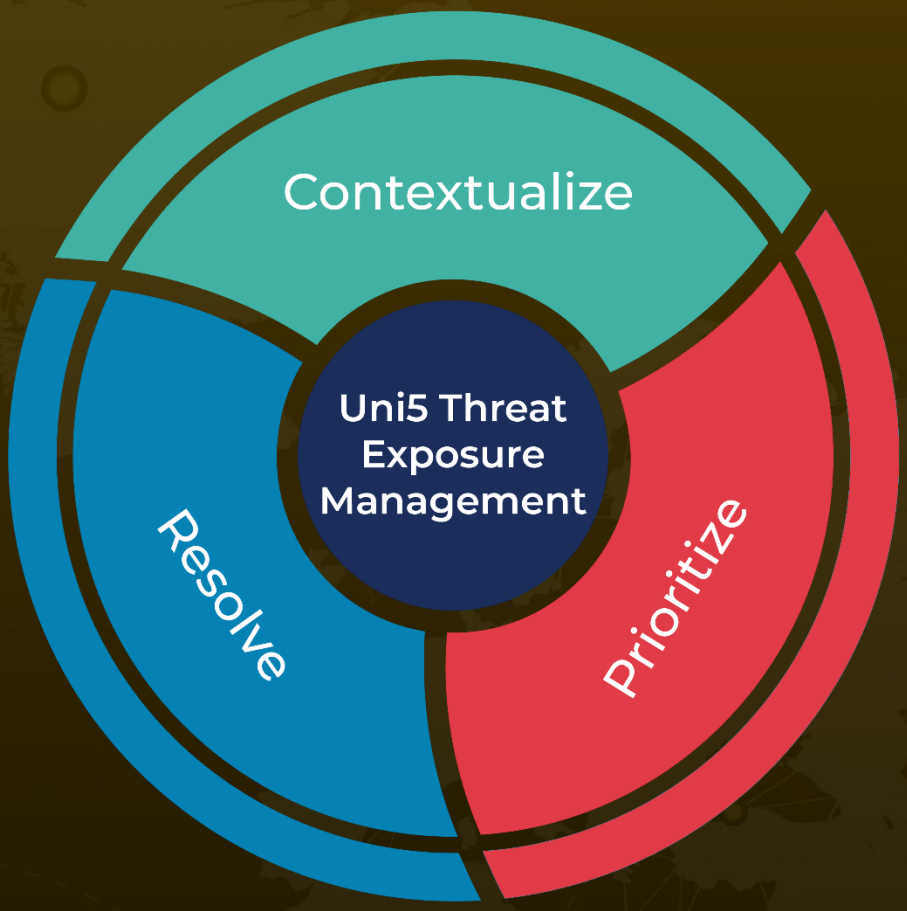
References

https://www.cyfirma.com/research/lyrix-ransomware/

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

June 4, 2025 • 5:30 AM

More at www.hivepro.com