Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

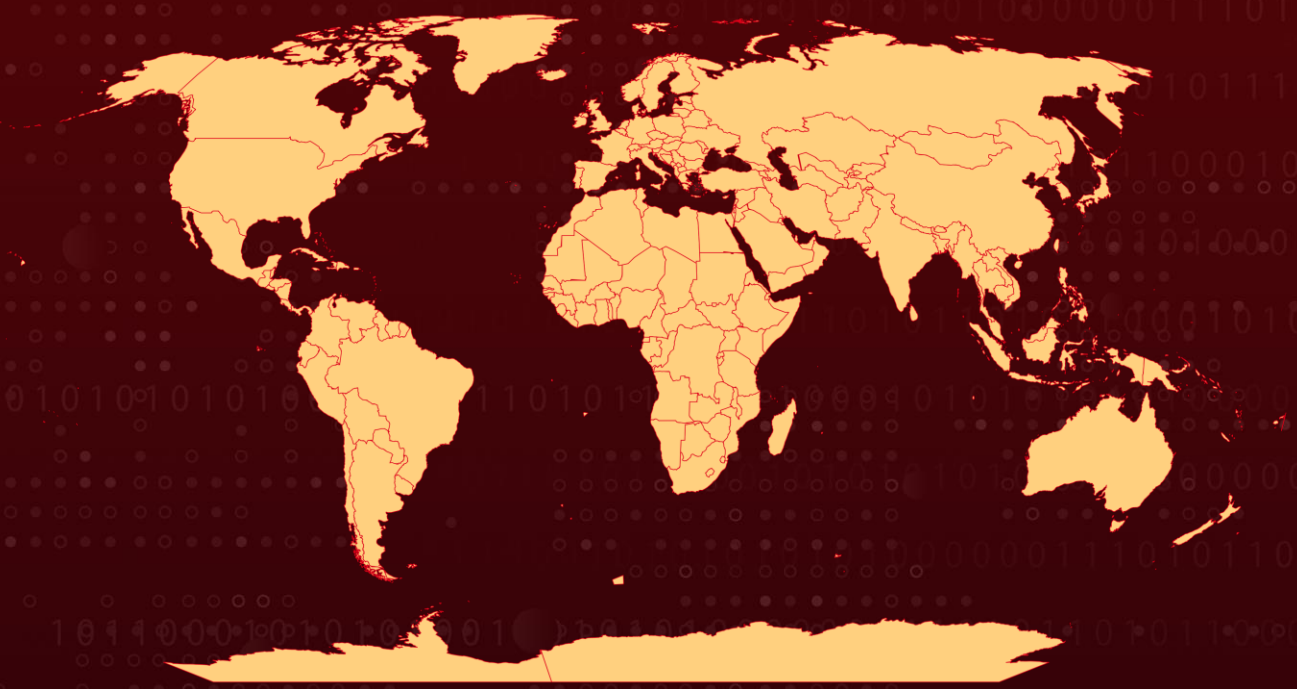
LostTrust Ransomware Unmasking the Gang Behind the Threat

Date of Publication	Admiralty Code	TA Number
October 9, 2023	A1	TA2023403

Summary

First Appearance: September 2023
Attack Region: Worldwide
Affected Platforms: Windows
Malware: LostTrust ransomware, SFile, Mindware, and MetaEncryptor
Attack: LostTrust ransomware, emerged in September 2023, is a multi-extortion threat related to SFile and Mindware, employing techniques reminiscent of MetaEncryptor, encrypting files and demanding ransoms. It presents a serious cybersecurity concern due to its similarities to other ransomware families.

Attack Regions



Attack Details

#1 The LostTrust ransomware operation, which emerged in September 2023, is a new multi-extortion threat. Analysis of LostTrust malware reveals it to be an evolution of SFile and Mindware, following similar operations and techniques as MetaEncryptor. The LostTrust ransom note attempts to portray the gang as offering a service while thinly veiling threats of data exposure if not paid. The gang claims to be specialists in network security.

#2 LostTrust ransomware terminates various services and processes on victim devices, including those associated with Microsoft Exchange, MSSQL, SharePoint, and more. It also attempts to remove Volume Shadow Copies and clear Windows Event Logs.

#3 The ransomware encrypts files with a ".losttrustencoded" extension and leaves a ransom note named "!!LostTrustEncoded.txt" in each folder containing encrypted files.

#4 Similarities to Mindware and SFile are evident, with LostTrust being an extension of this lineage. It uses similar encryption processes, exclusion patterns, and even shares victim blog site formatting with MetaEncryptor. As of the analysis, 53 victims are listed on the LostTrust blog, with 13 on the MetaEncryptor blog.

#5 Ransom note construction in LostTrust is similar to that of Mindware, with references and functions related to encryption staging also present. Debug paths and string artifacts are consistent across these families.

Recommendations

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Regular Software Updates: Ensure that all operating systems, software applications, and security solutions are kept up-to-date with the latest patches and updates. This helps eliminate vulnerabilities that adversaries can exploit.

Endpoint Security: Use robust endpoint protection solutions that include antivirus, anti-malware, and behavior-based detection to safeguard individual devices from malware and other threats.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0009 Collection	TA0010 Exfiltration	TA0002 Execution
TA0040 Impact	T1218 System Binary Proxy Execution	T1202 Indirect Command Execution	T1485 Data Destruction
T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1486 Data Encrypted for Impact	T1562.002 Disable Windows Event Logging
T1070 Indicator Removal	T1070.001 Clear Windows Event Logs	T1562 Impair Defenses	T1562.001 Disable or Modify Tools

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	a67686b5ce1d970a7920b47097d20dee927f0a4d, 28f73b38ace67b48e525d165e7a16f3b51cec0c0, ae974e5c37936ac8f25cfea0225850be61666874, f91d3c1c2b85727bd4d1b249cd93a30897c44caa, bdb0c0282b303843e971fbcd6d2888d834da204c, 5ffac9dff916d69cd66e91ec6228d8d92c5e6b37, 6960beedbf4c927b75747ba08fe4e2fa418d4d9b, e04760f670fab000c5ff01da39d4f4994011e581, 665572b84702c4c77f59868c5fe4d0b621f2e62a, 8c507d26c2fec90707320ffb721ae626139bbf11, 46ca0c5ad4911d125a245adb059dc0103f93019d, e9b52a4934b4a7194bcbbe27ddc5b723113f11fe, 09170b8fd03258b0deaa7b881c46180818b88381, 9bc1972a75bb88501d92901efc9970824e6ee3f5, 0f20e5ccdbbed4cc3668577286ca66039c410f95, 14e4557ea8d69d289c2432066d860b60a6698548

TYPE	VALUE
SHA256	feddee093d72838ac1f13ea9bbfc0473e2f3df1495432d6f95d6fe8ddf7ff09b, 8396728b5267a9ff823db2ab600e3ef1d131fc36596d24747ac494e8cdfe877c, c306254b44d825e008babbafbe7b07e20de638045f1089f2405bf24e7ce9c0dc, 81828762ebe7ea99b672c8ac07dc3c311487a5a246db494c7643915f6c673562, 4576fd0e13e13c9d490bd84ff83d2f3b602272cdea5f6c54c74f75d067ac5505, 26b7c7079cfea22cd9335b788db32453a727c81aec313a3637391a9763434f0a, 97d679f364b1d0c6e3896574f1338801a0d707c137e4d220d2c974ae40fbe708, 92c24d0c2075133e91f1be803c00478c733ee5be5610564efc48dd160cf2c632, d1a0a2dc26603b2e764ee9ab90f3f55a2f11a43e402dd72f4a32a19b0ac414b5, 00309d22ab53011bd74f4b20e144aa00bf8bb243799a2b48f9f515971c3c5a92, 32c818f61944d9f44605c17ca8ba3ff4bd3b2799ed31222975b3c812f9d1126c, e82606b7c179cd39d0e68d9f61723c4b2c909c44e2630c69d7038cd0f1bcb595, 451c4ff0a4313c98b519179eb276914d18d01eb1d6b1a28d6af15fda1693ec34

Recent Breaches

https://carnelutti.com/
https://foundationprosfl.com/
https://swanns.com/
https://gateseven.com/
https://asiavegetable.com/
https://doublevconstruction.com/
https://contrabandcontrol.com/
https://texaspatents.com/
https://iyseniorcare.com/
https://zoominfo.com/
https://ewbizservice.com/
https://gordonlawfirm.net/
https://nonprofitlight.com/
https://ambrosiniholding.com/
https://culluminc.com/
https://workplace.org/

https://looploc.com/
https://metoda.it/
https://carmocal.com/
https://johnsonboiler.com/
https://libertylines.com/
https://steuerberater-aschaffenburg.eu/
https://mackiegroup.com/
https://mtps.org/
https://gastrostatenisland.com/
https://jsmgroup.com/
https://keyconstruction.com/
https://encompolymers.com/
https://alexandercityal.gov/
https://gob.mx/
https://colorsdress.com/
https://spec-pro.com/
https://ananda.org/
https://jerseycollege.edu/
https://paradisecustomkitchens.com/
https://immanuelchristianschool.net/
https://spec-pro.com/
https://omniatel.it/
https://centraltrenching.com/
https://goldcoinrestaurant.com/
https://glassline.com/
https://sydgan.com/
https://bit.com.ar/
https://brownandstreza.com/
https://tormax.com/
https://fergusonwellman.com/
https://morgansd.org/
https://oasystechnologies.com/
https://mcsd.k12.ca.us/
https://hoosieruplands.org/
https://pnsa.ro/
https://arazozabrothers.com/
https://procab.se/
https://theaterleague.org/

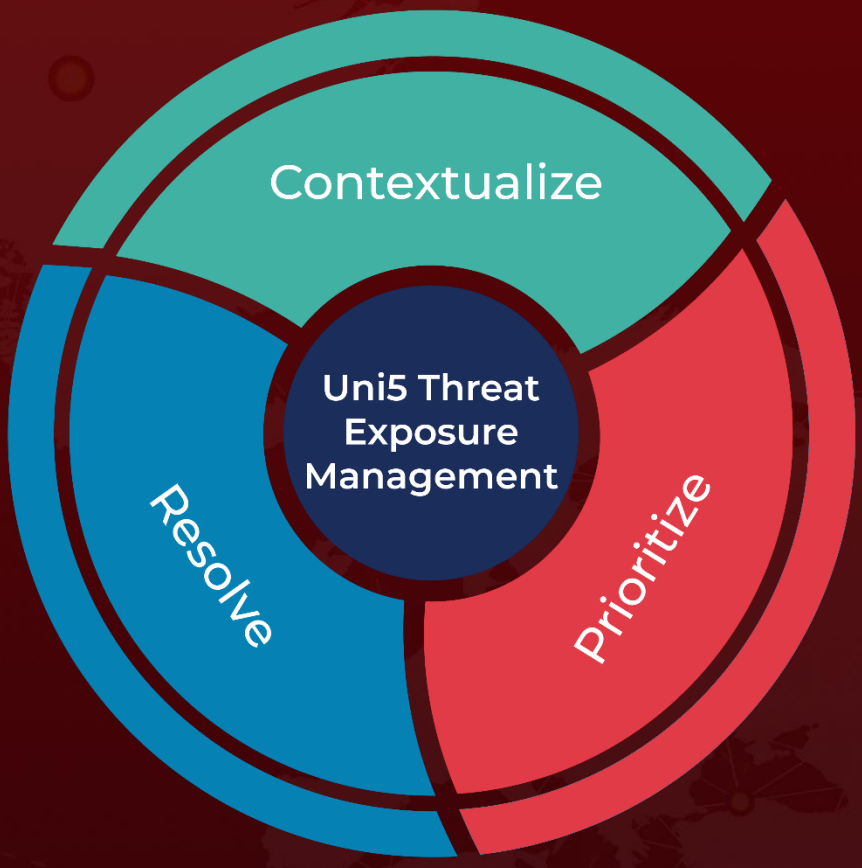
References

https://www.sentinelone.com/blog/losttrust-ransomware-latest-multi-extortion-threat-shares-traits-with-sfile-and-mindware/

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

October 9, 2023 . 7:30 AM

More at www.hivepro.com