Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

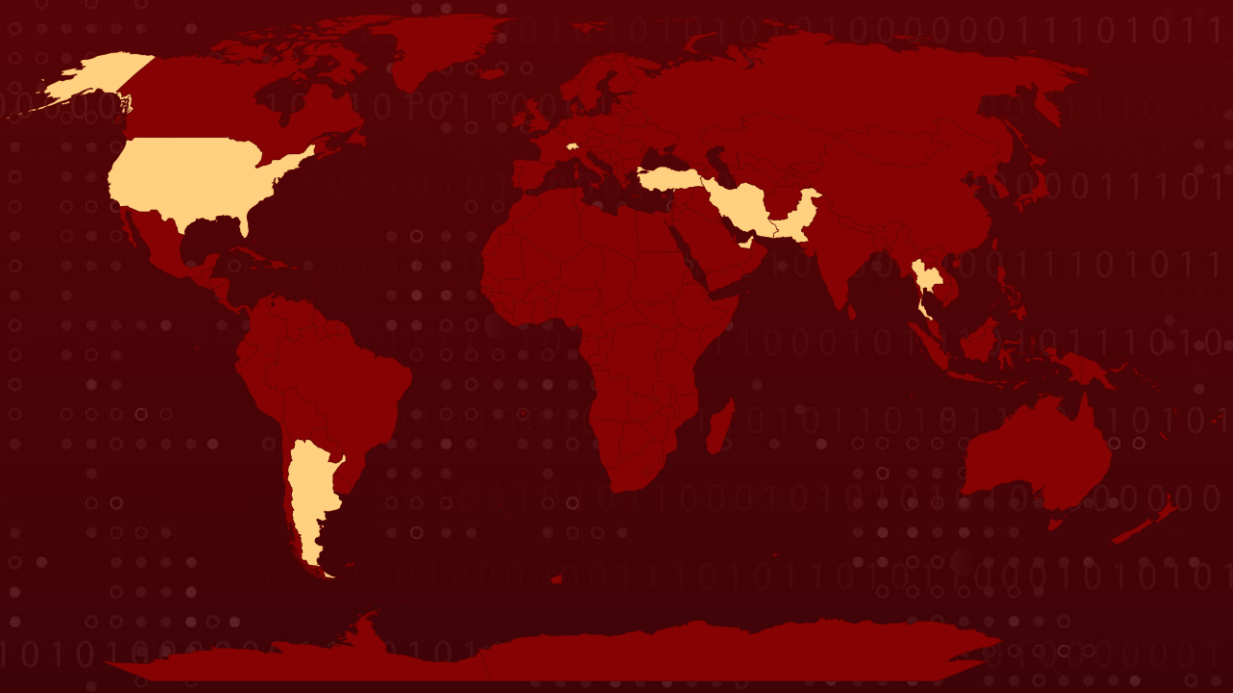
IceFire Ransomware Strikes Linux-Powered Enterprise Networks

Date of Publication	Admiralty Code	TA Number
March 14, 2023	A1	TA2023134

Summary

Attack began: March 2022
Malware: IceFire ransomware
Attack Region: Argentina, Iran, Pakistan, Switzerland, Thailand, Turkey, UAE, and USA.
Attack Sector: Technology, Media, and Entertainment sector, Internet Software & Services, Education.
Attack: A New Linux variant of IceFire ransomware is disseminated by exploiting the deserialization flaw in IBM Aspera Faspex, targeting networks of media/entertainment firms.

Attack Regions



CVEs

CVE	NAME	PATCH
CVE-2022-47986	Deserialization Vulnerability in IBM Aspera Faspex file-sharing software	✓

Attack Details

#1

The IceFire ransomware strain, previously identified on Windows systems, has now expanded its scope to target Linux enterprise networks of several media and entertainment industry organizations. The IceFire ransomware is being deployed by exploiting a deserialization vulnerability (CVE-2022-47986) in the IBM Aspera Faspex file-sharing software. Most of the attacks have been directed toward companies in Turkey, Iran, Pakistan, and the United Arab Emirates.

#2

The Linux variant of the IceFire ransomware is a 2.18 MB, 64-bit ELF binary created with gcc for AMD64 architecture. Once executed, files are encrypted and renamed with the ".ifire" extension appended to the original file name. The IceFire ransomware then deletes itself by removing the binary. The ransom message is deployed by the IceFire ransomware from an embedded resource in the malware and written to each directory targeted for file encryption.

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

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1053 Scheduled Task/Job	T1059 Command and Scripting Interpreter
T1129 Shared Modules	T1543 Create or Modify System Process	T1543.002 Systemd Service	T1546 Event Triggered Execution
T1546.004 Unix Shell Configuration Modification	T1547 Boot or Logon Autostart Execution	T1547.006 Kernel Modules and Extensions	T1036 Masquerading
T1070 Indicator Removal	T1070.004 File Deletion	T1222 File and Directory Permissions Modification	T1564 Hide Artifacts
T1564.001 Hidden Files and Directories	T1027 Obfuscated Files or Information	T1027.005 Indicator Removal from Tools	T1140 Deobfuscate/Decode Files or Information
T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1082 System Information Discovery	T1083 File and Directory Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1071 Application Layer Protocol	T1090 Proxy
T1095 Non-Application Layer Protocol	T1573 Encrypted Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	01de715b0f9e3725ef453d31acaaf598
SHA1	b676c38d5c309b64ab98c2cd82044891134a9973
SHA-256	e9cc7fdfa3cf40ff9c3db0248a79f4817b170f2660aa2b2ed6c551eae1c38e0b
URL	hxxp[://]159.65.217.216[:]8080/demo

Patch Links

https://exchange.xforce.ibmcloud.com/vulnerabilities/243512?_ga=2.34794403.3283 4304.1678795798-119972893.1678795798

Recent Breaches

https://novinparva.com/
https://www.wyden.io/
https://wxw.cat/
https://www.kodhosting.com/
https://guneshosting.com/
https://kru.ac.th/kru/intro/
https://37sur.com/
https://skifgroup.com/
https://cco1.com/
https://bestservers.pro/
https://directfn.net/
https://feesh.ch/

References

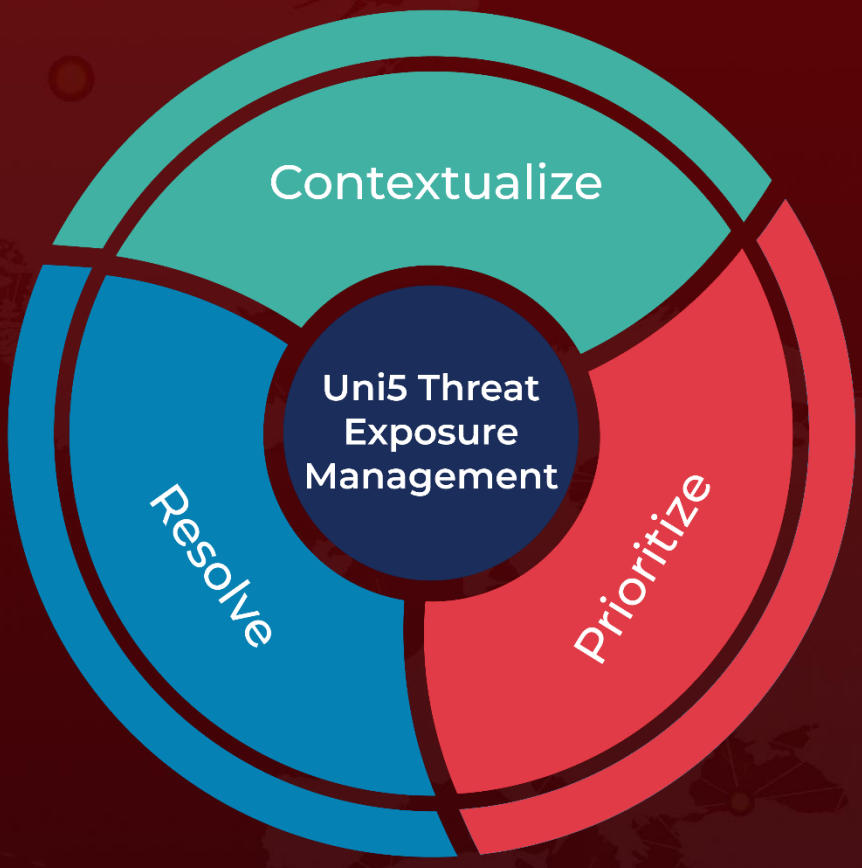
https://www.sentinelone.com/labs/icefire-ransomware-returns-now-targeting-linux-enterprise-networks/

https://www.bleepingcomputer.com/news/security/icefire-ransomware-now-encrypts-both-linux-and-windows-systems/

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

March 14, 2023 • 4:30 AM

More at www.hivepro.com