Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Mimic's Successor Elpaco Ransomware Enhances Customization Features

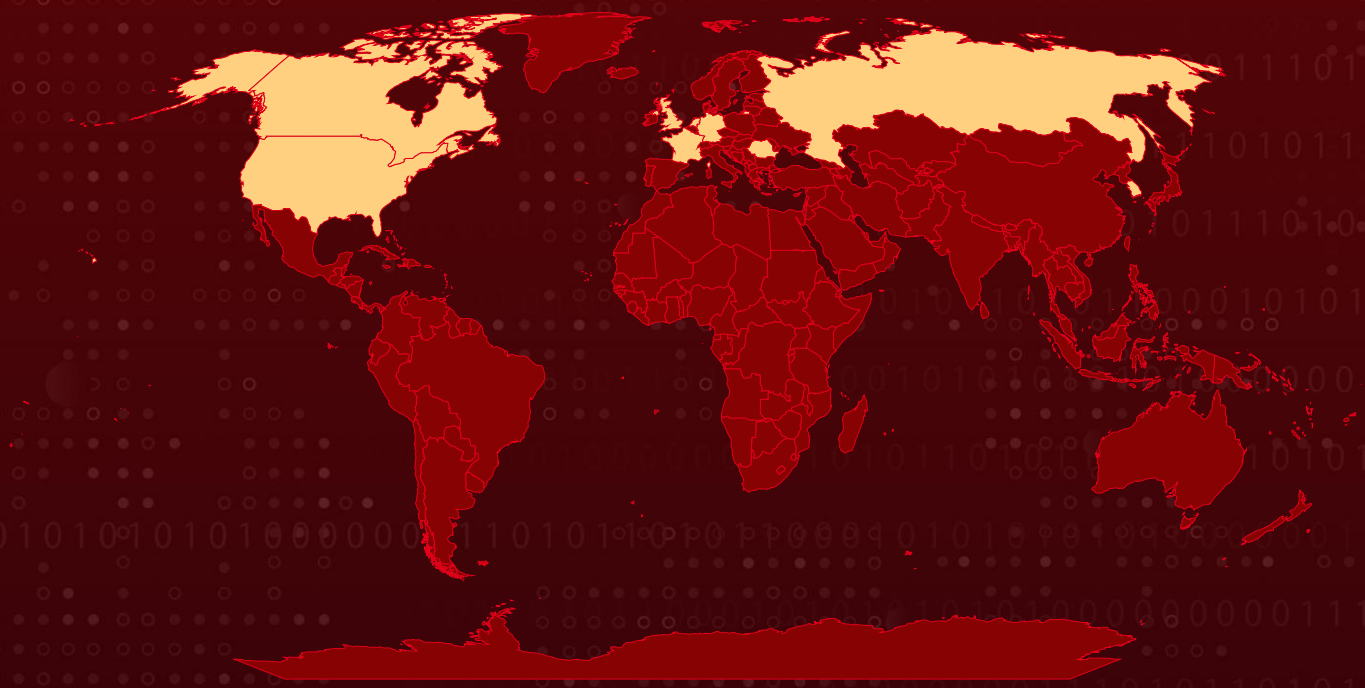
Date of Publication	Admiralty Code	TA Number
December 6, 2024	A1	TA2024453

Summary

Active Since: August 2023
Malware: Elpaco ransomware (aka ELPACO-team)
Targeted Countries: United States, Russia, Netherlands, Germany, France, Canada, Romania, South Korea, United Kingdom

Attack: Elpaco ransomware, an advanced variant of the notorious Mimic ransomware, is renowned for its highly sophisticated customization features and stealthy attack strategies. This cyber threat targets organizations in the United States, Russia, the Netherlands, Germany, and France, leveraging brute-force attacks on RDP servers and exploiting the critical Zerologon vulnerability (CVE-2020-1472) to achieve privilege escalation, making it a formidable adversary in the ransomware landscape.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-1472	ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓

Attack Details

#1 The Elpaco ransomware also referred to as the ELPACO-team, is an advanced variant of Mimic ransomware, notable for its enhanced customization features. Its predecessor, Mimic, experienced significant activity surges in January and September 2024.

#2 Elpaco operators typically infiltrate victims' servers through brute-force attacks on RDP credentials. Once access is obtained, the attackers deploy the ransomware and exploit the CVE-2020-1472 vulnerability, commonly known as Zerologon, to escalate privileges.

#3 Elpaco primarily targets organizations in the United States, Russia, the Netherlands, Germany, and France. It is a 32-bit Windows executable developed using Microsoft Visual C++, featuring an overlay section with a 7zSFX self-extracting archive.

#4 The ransomware encrypts files using the ChaCha20 stream cipher, with the encryption key secured via RSA-4096 asymmetric encryption. This dual-layered encryption method makes decryption infeasible without the private key. To further evade detection and hinder forensic analysis, Elpaco executes a self-deletion mechanism after encrypting files.

#5 While Mimic ransomware leverages "Everything APIs" to optimize file targeting and encryption efficiency, Elpaco distinguishes itself by implementing advanced stealth tactics. These include renaming processes and disabling system recovery options.

#6 Additionally, Elpaco employs tools like PowerShell to disable virtual machines and overwrites critical system files to maintain persistence. Unlike Mimic, which focuses on modular attacks derived from Conti's leaked source code, Elpaco expands its capabilities to thoroughly disrupt system restoration processes.

Recommendations

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Regular Patching and Updates: Keep operating systems, third-party applications, and security software updated to patch vulnerabilities, including high-risk exploits like Zerologon (CVE-2020-1472).

Enforce Application Whitelisting: Implement strict application whitelisting policies to prevent unauthorized or malicious executables from running within your environment.

Monitor Network Traffic: Track network activity for anomalies such as excessive data transfers to unfamiliar IP addresses or unusual RDP usage patterns.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Regularly Test Backup Restores: Conduct frequent tests to verify the integrity of backup data and ensure that restoration processes work as intended. This practice helps identify any issues before an actual data recovery scenario arises.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0040 Impact

T1135 Network Share Discovery	**T1059.003** Windows Command Shell	**T1059.001** PowerShell	**T1486** Data Encrypted for Impact
T1489 Service Stop	**T1490** Inhibit System Recovery	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control
T1036 Masquerading	**T1112** Modify Registry	**T1562** Impair Defenses	**T1562.004** Disable or Modify System Firewall
T1055 Process Injection	**T1564** Hide Artifacts	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder
T1566 Phishing	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1203** Exploitation for Client Execution
T1204 User Execution	**T1204.002** Malicious File	**T1070** Indicator Removal	**T1070.004** File Deletion
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1016** System Network Configuration Discovery	**T1005** Data from Local System

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	33eeeb25f834e0b180f960ecb9518ea0, b951e50264f9c5244592dfb0a859ec41, b93eb0a48c91a53bda6a1a074a4b431e, c44487ce1827ce26ac4699432d15b42a, 3b03324537327811bbbaff4aafa4d75b, 245fb739c4cb3c944c11ef43cddd8d57, ac34ba84a5054cd701efad5dd14645c9, 0bf7c0d8e3e02a6b879efab5deab013c, 742c2400f2de964d0cce4a8dabadd708, 51014c0c06acdd80f9ae4469e7d30a9e, 1b37dc212e98a04576aac40d7ce7d06a, 26f59bb93f02d5a65538981bbc2da9cc,

TYPE	VALUE
MD5	03a63c096b9757439264b57e4fdf49d1, 57850a4490a6afd1ef682eb93ea45e65, fade75edbf62291fbb99c937afc9792c, 803df907d936e08fbbd06020c411be93
SHA1	61f73e692e9549ad8bc9b965e25d2da683d56dc1, 8af05099986d0b105d8e38f305efe9098a9fbda6
SHA256	9f6a696876fee8b811db8889bf4933262f4472ad41daea215d2e39bd537cf32f, e160d7d21c917344f010e58dcfc1e19bec6297c294647a06ce60efc7420d3b13

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

References

https://securelist.com/elpaco-ransomware-a-mimic-variant/114635/

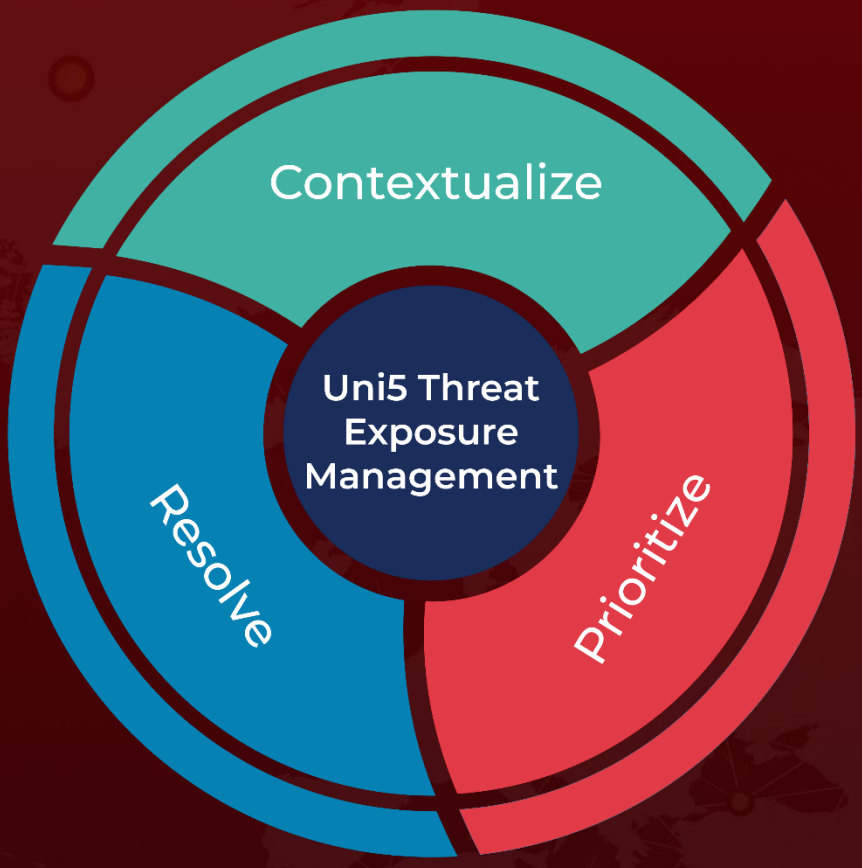
https://www.cyfirma.com/research/elpaco-team-ransomware-a-new-variant-of-the-mimic-ransomware-family/

https://hivepro.com/threat-advisory/new-ransomware-mimic-emerges-in-the-wild-abusing-legitimate-tool-for-faster-encryption/

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

December 6, 2024 . 4:00 AM

More at www.hivepro.com