Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

GhostSec and Stormous Join Forces for a Ransomware Blitz

Date of Publication
March 7, 2024

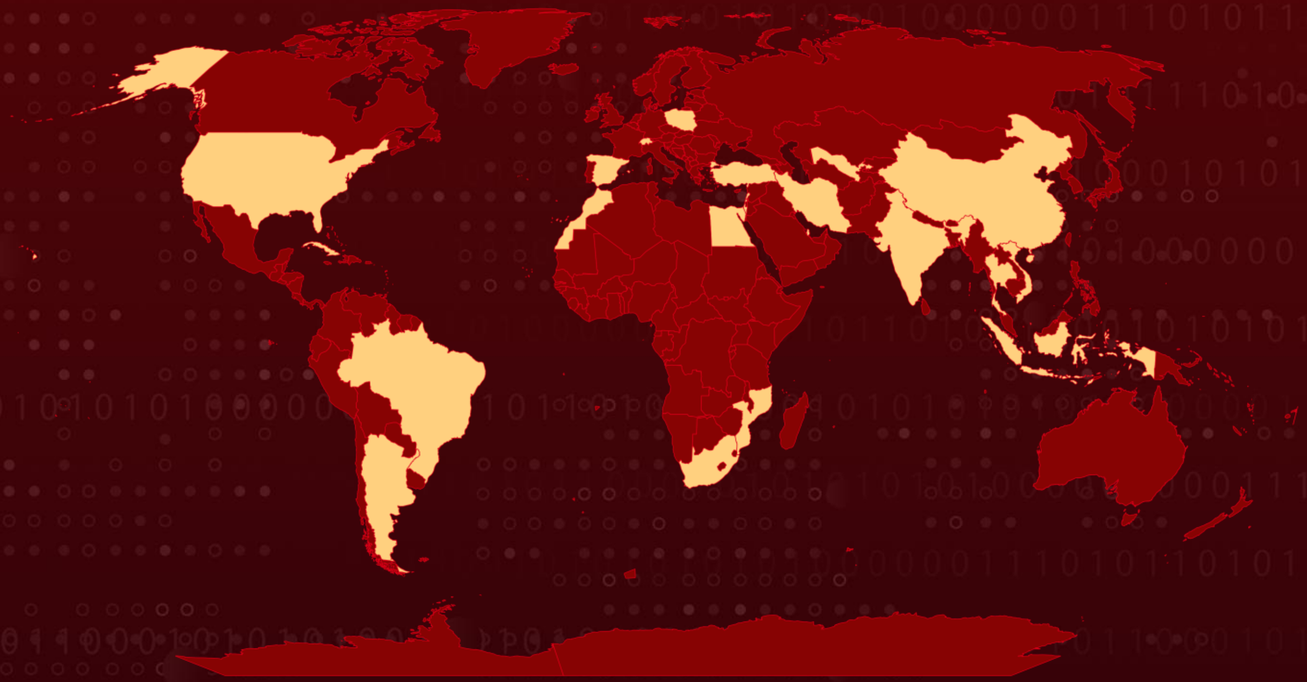
Admiralty Code
A1

TA Number
TA2024090

Summary

Active Since: February 2024
Malware: GhostLocker, Stormous, GhostPresser
Attack Region: Argentina, Brazil, China, Cuba, Egypt, India, Indonesia, Iran, Israel, Lebanon, Morocco, Mozambique, Poland, Qatar, South Africa, Spain, Switzerland, Thailand, Turkey, United States, Uzbekistan, Vietnam
Targeted Industries: Pharmaceutical, Media, Airline, Internet Services, Energy, Retail, Consulting, Semiconductors Equipment, Hospitality, Construction, Engineering, Technology, Education, Manufacturing, Government, Transport, Real Estate, Telecommunication
Attack: The GhostSec and Stormous ransomware factions have launched a sophisticated campaign. Introducing the GhostLocker 2.0 ransomware and the STMX_GhostLocker ransomware-as-a-service (RaaS) initiative, these groups employ double extortion tactics, posing a significant threat to businesses primarily in the Middle East.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The GhostSec and Stormous ransomware factions have collaboratively initiated a sophisticated ransomware campaign, strategically targeting various organizations. Concurrently, GhostLocker and Stormous ransomware have launched a new ransomware-as-a-service (RaaS) initiative named STMX_GhostLocker, catering to affiliates with diverse options.

#2 These ransomware groups are engaging in double extortion tactics, menacing businesses across various sectors in predominantly Middle Eastern countries. GhostSec, a self-proclaimed modern-day Five Families group aligning itself with ThreatSec, Stormous, Blackforums, and SiegedSec, disseminates its motives via Telegram channels. The group's objectives seem predominantly profit-oriented rather than geared towards kinetic sabotage.

#3 The recently introduced RaaS program, STMX_GhostLocker, offers three service categories for affiliates: paid, free, and an option for individuals desiring to sell or publish data on their blogs. In November 2023, GhostSec unveiled an enhanced iteration of their GhostLocker ransomware, GhostLocker 2.0 (also known as GhostLocker V2), coded in Go.

#4 This iteration employs file encryption with the extension ".ghost," accompanied by a restructured ransom note compelling victims to establish contact within seven days to avert potential leakage of pilfered data. Upon initial execution, GhostLocker 2.0 establishes persistence by copying itself into the Windows Startup folder.

#5 GhostLocker RaaS equips affiliates with a ransomware builder, featuring configuration options such as persistence modes, target directories for encryption, and evasion techniques, encompassing process termination and execution of arbitrary commands to neutralize scheduled tasks or bypass User Account Controls.

#6 GhostSec's arsenal introduces two novel tools employed in compromising legitimate websites: the "GhostSec Deep Scan toolset" for recursive scanning of legitimate websites and a hack tool named GhostPresser, facilitating cross-site scripting (XSS) attacks.

Recommendations

Robust Backup Strategies: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

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

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0011 Command and Control	TA0040 Impact	T1204.002 Malicious File

T1129 Shared Modules	**T1059** Command and Scripting Interpreter	**T1057** Process Discovery	**T1083** File and Directory Discovery
T1569.002 Service Execution	**T1027** Obfuscated Files or Information	**T1070** Indicator Removal	**T1560** Archive Collected Data
T1041 Exfiltration Over C2 Channel	**T1036** Masquerading	**T1001** Data Obfuscation	**T1027.010** Command Obfuscation
T1486 Data Encrypted for Impact	**T1547.001** Registry Run Keys / Startup Folder	**T1071.001** Web Protocols	**T1059.006** Python

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282eb24b7c55f, 8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f443779e9, 36760e9bbfaf5a28ec7f85d13c7e8078a4ee4e5168b672639e97037d66eb1d17, 8fa28795e4cd95e6c78c4a1308ea80674102669f9980b2006599d82eff6237b3
IPv4	94[.]103[.]91[.]246
URLs	hxxp[://]94[.]103[.]91[.]246/incrementLaunch, hxxp[://]94[.]103[.]91[.]246/addInfection, hxxp[://]94[.]103[.]91[.]246/victimchat?id=[EncryptionID], hxxp[://]94[.]103[.]91[.]246/login?next=, hxxp[://]94[.]103[.]91[.]246/upload

References

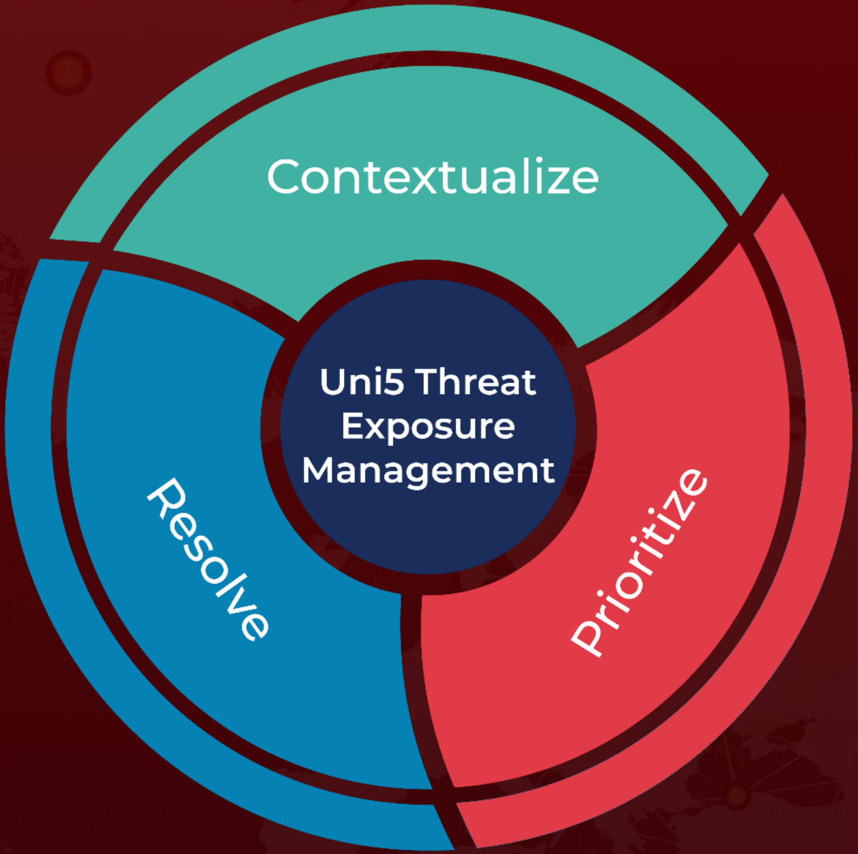
https://blog.talosintelligence.com/ghostsec-ghostlocker2-ransomware/

https://www.hivepro.com/threat-advisory/ghostsec-pioneering-the-hacktivist-front-with-ghostlocker/

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 7, 2024 • 7:00 AM

More at www.hivepro.com