Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

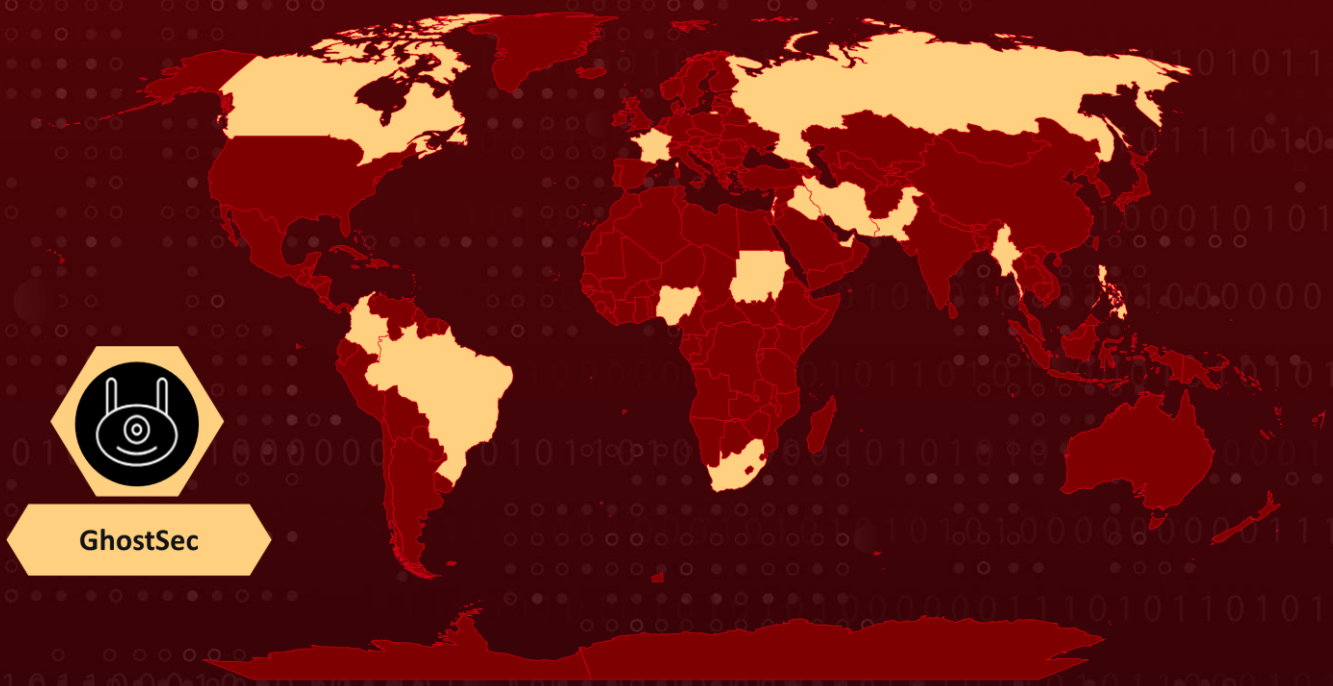
GhostSec Pioneering the Hacktivist Front with GhostLocker

Date of Publication	Admiralty Code	TA Number
November 17, 2023	A1	TA2023465

Summary

Active Since: May 2022
Threat Actor: GhostSec (aka Ghost Security)
Malware: GhostLocker
Attack Region: Russia, Israel, Columbia, Iran, South Africa, Nigeria, Pakistan, Iraq, United Arab Emirates, Lebanon, France, Brazil, Sudan, Myanmar, Nicaragua, Philippines, Canada
Targeted Industries: Telecommunications Companies, Surveillance Systems, and Internet Of Things (IoT) Devices.
Attack: GhostSec, a hacktivist coalition stemming from the Anonymous group and part of 'The Five Families,' has introduced GhostLocker, an advanced Ransomware-as-a-Service (RaaS) framework.

Attack Regions



Attack Details

#1 The hacktivist syndicate known as GhostSec has unveiled an innovative Ransomware-as-a-Service (RaaS) framework called GhostLocker. GhostSec, a spin-off of the renowned Anonymous group, focuses its efforts on well-established telecommunications companies, surveillance systems, and Internet of Things (IoT) devices.

#2 GhostLocker is promoted as pioneering enterprise-grade locking software that prioritizes vital safety and efficacy. Initially priced at $999 for the first 15 affiliates, GhostSec plans to raise this fee to $4,999 in subsequent iterations. GhostSec is part of "The Five Families," a collective of five hacktivist groups, including ThreatSec, Stormous, Blackforums, and SiegedSec.

#3 GhostSec utilized Python in developing their encryptor, employing PyInstaller to package Python code into standalone executable applications compatible with various operating systems. The victim's information and encryption key are transmitted in plain text via the HTTP protocol. After the purported encryption process, GhostLocker drops a ransom note in an HTML file named "Imao."

#4 Recent versions of GhostLocker are compiled using Nuitka, a tool that translates Python programs into C binaries. The rise of Ransomware-as-a-Service (RaaS) models, exemplified by GhostLocker, highlights the increasing sophistication of cybercriminals.

Recommendations

Adopt Zero Trust Security Model: Embrace a Zero Trust security model, assuming that threats can originate from both external and internal sources. Verify and authenticate all users and devices attempting to access the network, regardless of their location or previous trust levels.

Implement Network Segmentation: Employ network segmentation strategies to isolate critical systems and sensitive data, reducing the potential impact of a ransomware attack. Limit lateral movement within the network to contain the spread of malware.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information	T1087.001 Local Account	T1659 Content Injection
T1543 Create or Modify System Process	T1560 Archive Collected Data	T1574 Hijack Execution Flow	T1057 Process Discovery
T1211 Exploitation for Defense Evasion	T1071.001 Web Protocols	T1059.006 Python	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778, ee227cdOef308287bc536a3955fd8138&16a0228ac42140e9M308ae6343a3f, Oe484560a909fc06b9987db73346eaoca6750d523f2334913c23e061695f5cc, abac31b5527803a89c941cf24280a9653oee898a7a338424bd3e9b15d792972, 663ac2d887df18e6da97dd358ebd2bca55404fd4a1C8CIC51215834fc6d11b33, 9b6be74c2c144f8bcb92c8350855d35C14bb7f2b727551C3dd5C8054c4136e3f, ee227cdOef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f, 0e484560a909fc06b9987db73346efaOca6750d5232334913c23e061695f5cc, abac31b5527803a89c941cf24280a9653cdee898a7a338424bd3e9b15d792972,

TYPE	VALUE
SHA256	663ac2d887df18e6da97dd358ebd2bca55404fd4a1c8c1c51215834fc6d11b33, Oe484560a909fc06b9987db73346efaOca6750d5232334913c23e061695f5cc, 15d874e24caf162bc58597ac5f22716694b5d43cf433bee6a78a0314280f2c80, 0e484560a909fc06b9987db73346efa0ca6750d523f2334913c23e061695f5cc, 4844f44c9de364377f574e4d6a8a77dc0b4d6a67f21ccbf693ac366e52eaa8cb, 65d3a922754af96d8d722859ac31f3de96522d50659c67607021f2ac728f9630, a98f8468d70426ba255469a92d983d653f937d954e936e0ff5d9a0f44f1bdf70, ee227cd0ef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f, 7d37eddf0b101ff2b633b2ffe33580bdb993a97fecc06874d7b5b07119b9ec99, 4c09a012efff318b01a72199051815c5a7b920634fb6c76082673681f54f2ec3
File Names	zncxtdvfxpndbwab.exe, wwndjlajmlkzqaqa.exe, xxmruwvcgorkidkg.exe, xxmruvwcgorkidkg.exe, 500.exe, XxWACzmWyB.exe, watchdog.exe
IPv4	195[.]2[.]79[.]117, 88[.]218[.]62[.]219
URLs	hxxp://88[.]218[.162[.]219/download hxxp://88[.]218[.161[.]141/incrementLaunches hxxp://88[.1218[.]61[.]141/add hxxp://88[.]218.62[.]219/download hxxp://88[.]218.62[.]219/ hxxps://88[.]218.62[.]219/download/ hxxp://88[.]218.62[.]219/downloadp hxxp://88[.]218.62[.]219/downloadastatus_codel hxxp://88[.]218.61[.]141/addaCrypticMastera__main__a__module__auserConfiga__qualname__uchrome.exeaproces hxxp://88[.]218.61[.]141/adda__main__a__module__auserConfiga__qualname__uchrome.exeaprocessesuC:/Users/%25

TYPE	VALUE
URLs	hxxp://88[.]218.61[.]141/ hxxp://88[.]218.61[.]141/addp hxxp://88[.]218.61[.]141/incrementLaunchesT hxxp://88[.]218.61[.]141/incrementLaunches hxxp://88[.]218.61[.]141/add hxxp://195[.]2[.]79[.]117/

References

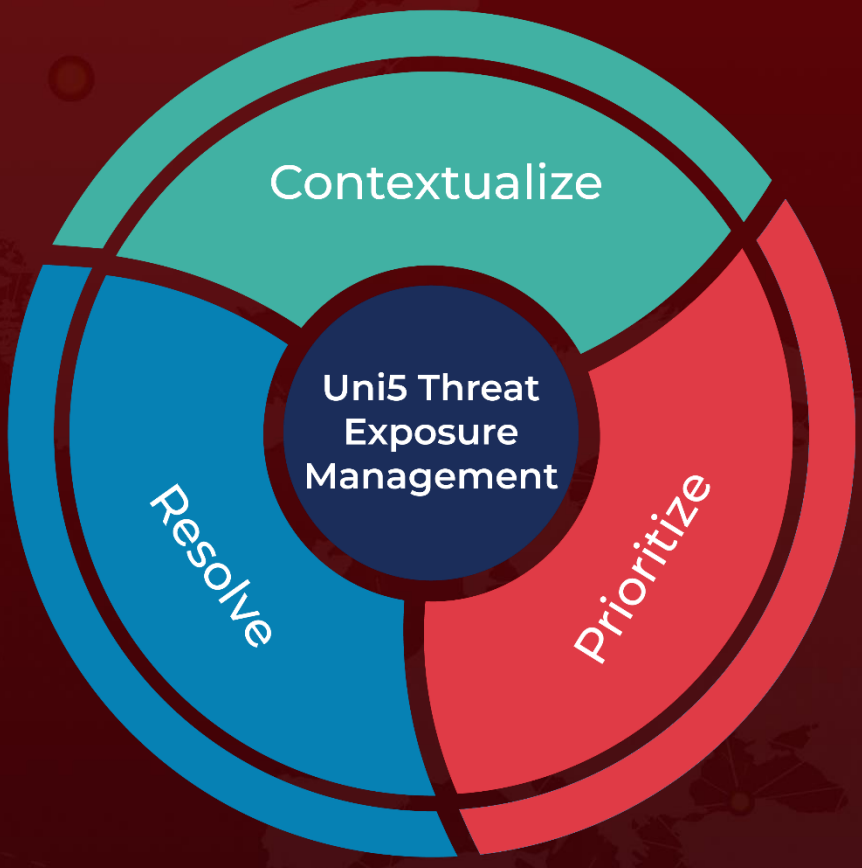
https://www.rapid7.com/blog/post/2023/11/08/ghostlocker-a-work-in-progress-raas/

https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec

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

November 17, 2023 . 4:30 AM

More at www.hivepro.com