Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

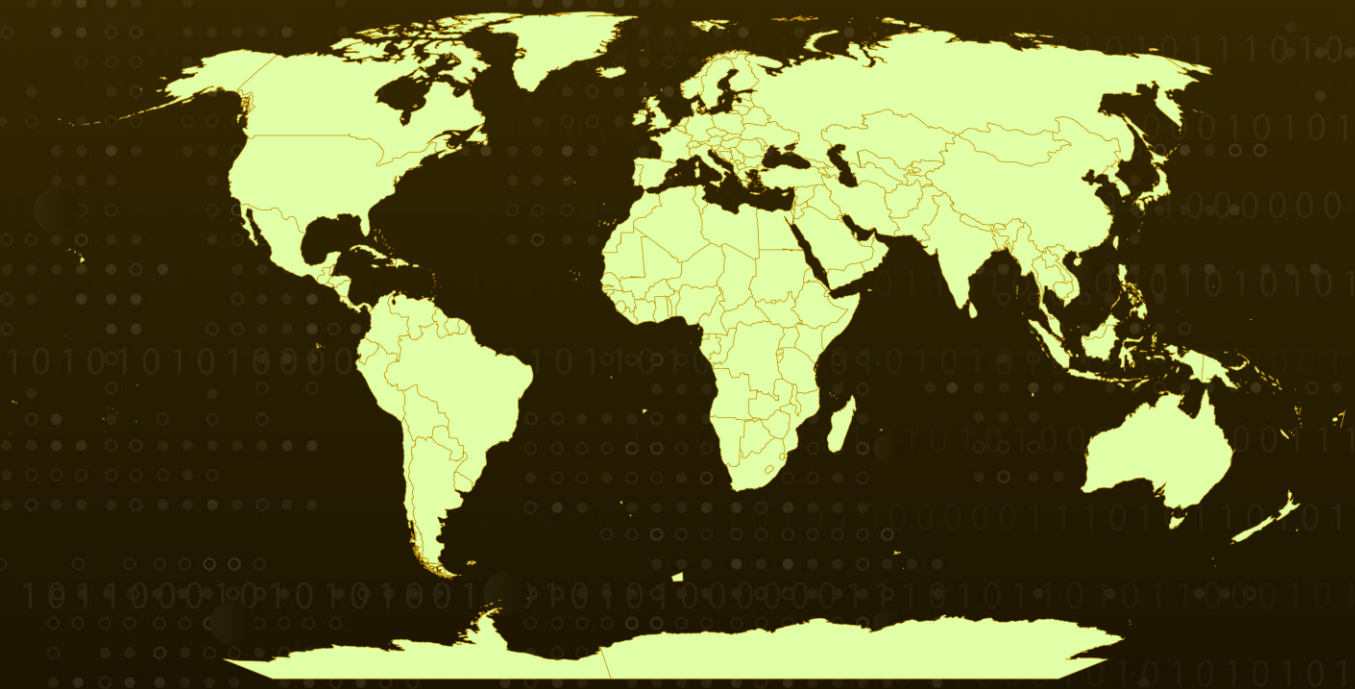
TargetCompany Ransomware's FUD Obfuscation Maneuvers

Date of Publication	Admiralty Code	TA Number
August 8, 2023	A1	TA2023324

Summary

First Seen: June 2021
Malware: TargetCompany Ransomware (aka Mallox, Fargo, and Tohnichi), Remcos RAT
Attack Region: Worldwide
Attack: The TargetCompany ransomware employs a combination of its proprietary variant and the BatCloak obfuscator engine, acclaimed for its full undetectability (FUD) capabilities. Accompanying this fusion is the Remcos RAT, which operates as a loader. This meticulously orchestrated amalgamation of malevolent tools is designed to strategically breach vulnerable systems.

Attack Regions



Attack Details

#1 The TargetCompany ransomware also recognized as Mallox, Fargo, and Tohnichi, can be traced back to approximately mid-June 2021. In its most recent string of attacks, the ransomware has employed a blend of its proprietary ransomware strain along with two established malicious software products the Remcos RAT and an iteration of the BatCloak obfuscator engine, renowned for its complete undetectability (FUD) capabilities. This integration is strategically aimed at infiltrating vulnerable systems.

#2 The latest version of this ransomware initiates its assault by exploiting vulnerabilities in SQL servers, thereby ensuring the persistent deployment of its initial stage. The operational procedure encompasses a diverse range of tactics aimed at establishing persistence. These tactics involve the manipulation of URLs and relevant pathways until a successful vector is discovered for executing the Remcos RAT.

#3 The utilization of FUD represents a strategic obfuscation method employed by attackers, automatically scrambling the ransomware's code to evade signature-based detection mechanisms. Consequently, this enhances the probability of operational success. The TargetCompany ransomware employs a FUD approach reminiscent of BatCloak's methodology.

#4 This involves utilizing a batch file as an outer layer, which is subsequently decoded and loaded through PowerShell, thereby facilitating the execution of Living Off the Land Binaries (LOLBins). In a subsequent phase of the attack, the group leverages the hacking tool Metasploit. This tool is introduced prior to the final sequence of the Remcos RAT's activities, serving as a means to load the TargetCompany ransomware, concealed within the FUD packer.

Recommendations

A substantial number of TargetCompany's victims continue to possess vulnerable SQL Servers that are being targeted for unauthorized access. To counteract this, it is imperative to gain insight into their patching deficiencies and thoroughly assess all potential attack vectors to safeguard their systems from susceptibility to misuse and exploitation.

Establish routine backups for all assets, ensuring they receive proper protection. Implement the 3-2-1-1 backup principle and deploy dedicated tools to guarantee backup integrity and availability.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0011 Command and Control	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1129 Shared Modules	T1055 Process Injection	T1006 Direct Volume Access	T1027 Obfuscated Files or Information
T1027.009 Embedded Payloads	T1036 Masquerading	T1070 Indicator Removal	T1070.006 Timestomp
T1140 Deobfuscate/Decode Files or Information	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1010 Application Window Discovery
T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1560 Archive Collected Data
T1071 Application Layer Protocol	T1571 Non-Standard Port	T1573 Encrypted Channel	T1518 Software Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	734803d815af2b27fbbb7b4516df3f6fb29ed76d1b16c661a38dbe860831b906, d59f6e95075026e755a415a5dd5fd4b617516c99d064b833e01c7e5d583cf2fd, 2aa688bebce1788d58ca8d42628b5642a4891adaf275b3ac246f7859f6280115, 26a674f981da653d72d139331e0a46e7dc09142ce2bc602655d6fbb37626c668, bcff44c6673ded04c8fb76b733837ce109ac6cbb0e4d1ba5b290f76632a4e718, 22816dc4dda6beec453e9a48520842b8409c54933cc81f1a338bc77199ab917e,

TYPE	VALUE
SHA256	52fe40246265e29ab791c26e57e568b18cbc4f57c3db5b12beb1415c416d64bb, 1ef8aebbb3816d7d534a581c1d1d8730a73355068e8b39587b2363ccbe692c08, 2efdffd1cf3adab21ff760f009d8893d8c4cbcf63b2c3bfcc1139457c9cd430b, 094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde, f0e68af393967d8a236461815dd601baf7ebced7b807c224bceb51d0e8bb4b87, 18c909a2b8c5e16821d6ef908f56881aa0ecceeaccb5fa1e54995935fcfd12f7, 08cfd5a321a47a55c5e8732e3d12bf937ca32426dcd668c7d620cfae48159348, e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173, e0d4dc05991211e86c920092966d7025f8e40b77a799428f8491c4f7fa6078a6, 12842d49038c066464ac723b9665ff93f634042646bdd6947b54042fd0e06342, bf28b8a8576beb4755ec6a9d93fc4539e40dee7197b6399dfad5224f5ee74b19, eb75b7d31a9bd3686fcb0088c6849724396871711013 68ebf9134a53abac3c20, 3c665d38c5ccb0b41983ad492b31c499b176219ca7a93494fd902f592cee2ff6, 777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899, 4b1949536f3f6140da0a9fc87eb0430b61206852145ada5cecbc279b242bce10
URLs	hxxp://80.66.75[.]37, hxxp://185.209.230[.]21:8080, hxxps[:]//whyers[.]io/QWEwqdsvsf/ap[.]php
IPv4	195.3.146[.]183, 80.66.75[.]116, 80.66.75[.]*

References

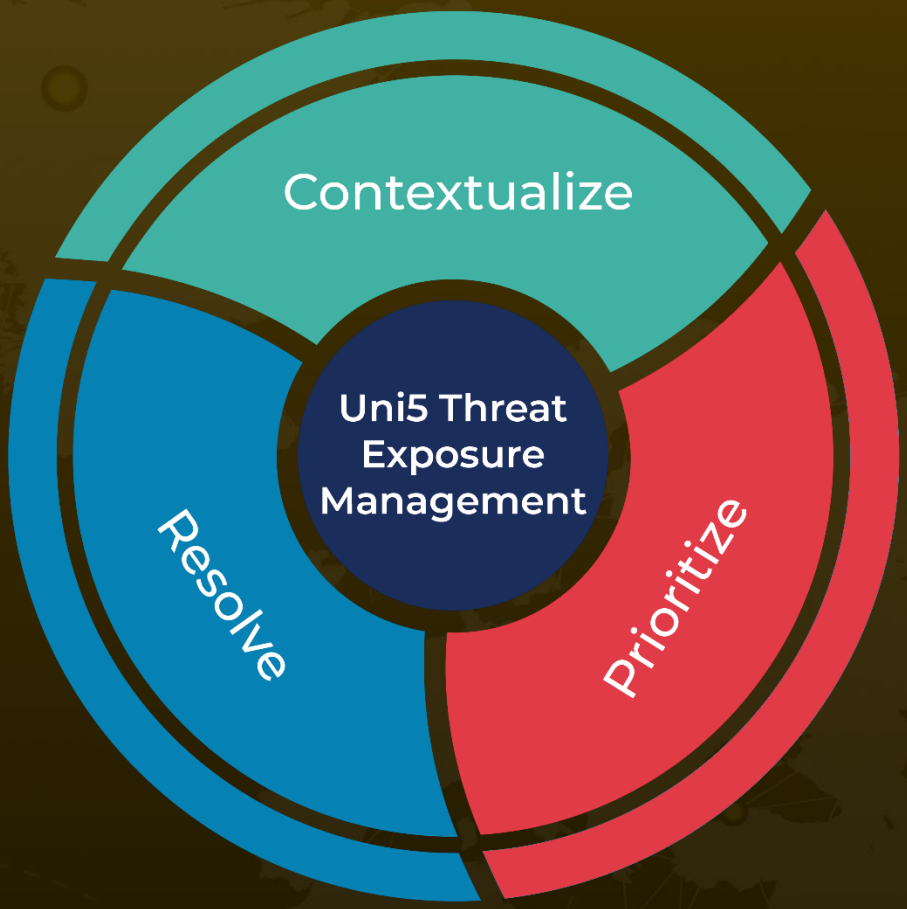
https://www.trendmicro.com/en_us/research/23/h/targetcompany-ransomware-abuses-fud-obfuscator-packers.html

https://www.hivepro.com/mallox-ransomware-is-ramping-up-its-operation/

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

August 8, 2023 . 5:30 AM

More at www.hivepro.com