Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

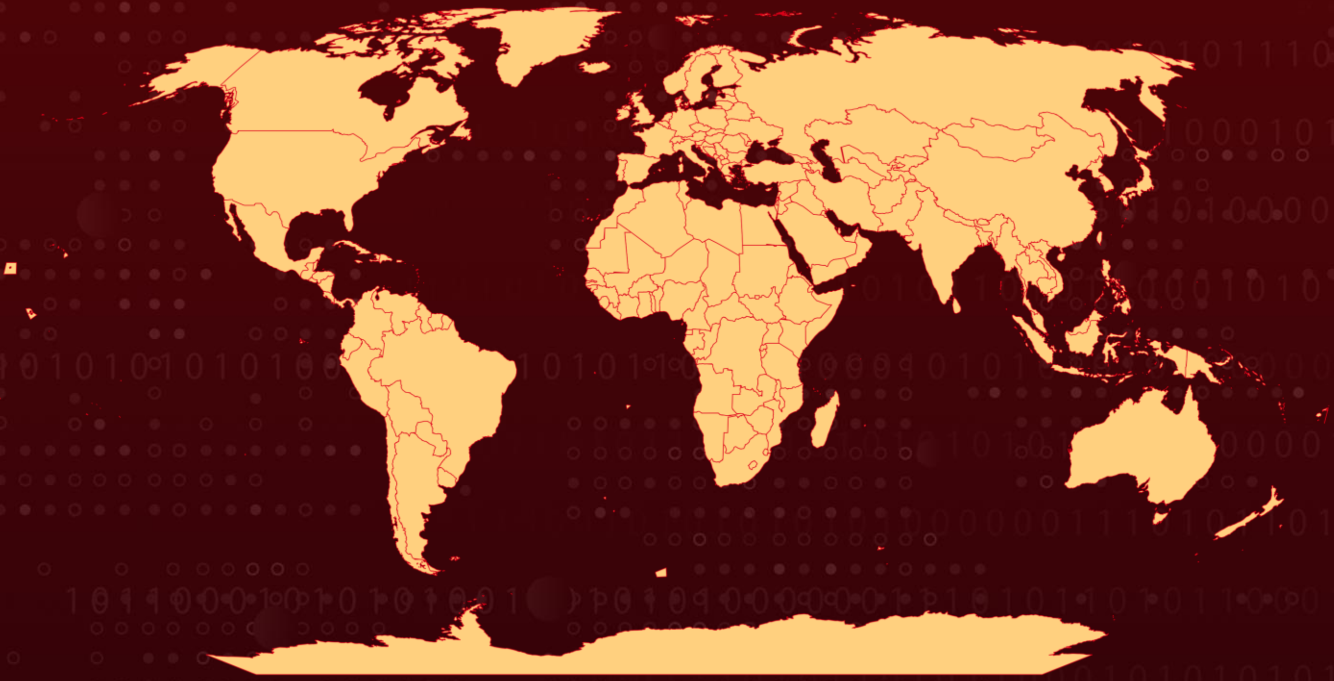
FAUST: A Phobos Ransomware Variant Launches Fileless Attack

Date of Publication	Admiralty Code	TA Number
January 30, 2024	A1	TA2024037

Summary

Attack Began: November 2023
Targeted Countries: Worldwide
Malware: FAUST ransomware, Phobos ransomware
Attack: FAUST ransomware, a variant of the Phobos family, exhibiting intricate deployment stages, from decoding Base64 data to injecting shellcode. Notably, it employs a fileless attack through an Office document with a VBA script, emphasizing the need for user caution with document files from untrusted sources.

Attack Regions



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

Attack Details

#1 The Phobos ransomware family, known for encrypting files on victims' computers, has recently been linked to a new variant called FAUST. This report from FortiGuard Labs details the attack flow of FAUST, starting with an Office document containing a VBA script. The script, when opened, triggers PowerShell to download malicious data from Gitea, leading to the deployment of the FAUST ransomware.

#2 The VBA script decodes Base64-encoded data and saves it as a clean XLSX file in the TEMP folder. The decoded data contains PowerShell commands to download additional malicious files from Gitea. The attacker then creates a new folder in the system, saves an executable named "AVG update.exe," and initiates a file encryption attack.

#3 The "AVG update.exe" serves as a downloader, employing techniques to evade detection and complicate analysis. It decodes its ".rdata" section, retrieves files from Gitea, and injects shellcode into a process named "SmartScreen Defender Windows.exe." The injected payload is part of the FAUST ransomware.

#4 FAUST, a Phobos variant, encrypts files on victims' computers, appending the ".faust" extension. It demands a ransom for decryption and adds persistence by modifying the registry. The ransomware has an exclusion list to avoid double-encrypting certain files. It also checks for the Mutex object to ensure only one process is running. The ransom note directs victims to contact the attackers via email or TOX message, Analysis of the TOX ID indicates ongoing selling activity associated with the ransomware.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Conduct Regular Data Backups and Test Restoration: Implement a robust data backup strategy that includes regular backups of critical data and systems. Ensure backups are stored offline or in a secure, isolated environment to prevent them from being compromised in the event of an attack. Regularly test the restoration process to verify the integrity and availability of backups.

Enhance Endpoint Security: Employ reputable antivirus and anti-malware solutions to detect and block known malware signatures. Regularly update and patch operating systems and software to address vulnerabilities that threat actors may exploit.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0005 Defense Evasion	TA0003 Persistence	TA0002 Execution
TA0040 Impact	T1059.005 Visual Basic	T1140 Deobfuscate/Decode Files or Information	T1486 Data Encrypted for Impact
T1059 Command and Scripting Interpreter	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1027 Obfuscated Files or Information
T1137 Office Application Startup	T1055 Process Injection	T1059.001 PowerShell	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	426284b7dedb929129687303f1bf7e4def607f404c93f7736d17241e43f0ab33, 50e2cb600471fc38c4245d596f92f5444e7e17cd21dd794ba7d547e0f2d9a9d5, a0a59d83fa8631d0b9de2f477350faa89499e96fd5ec07069e30992aaabe913a, ebe77c060f8155e01703cfc898685f548b6da12379e6aefb996dbcaac201587c, c10dc2f6694414b68c10139195d7db2bb655f3afdcc1ac6885ef41ef1f0078df

References

https://www.fortinet.com/blog/threat-research/phobos-ransomware-variant-launches-attack-faust

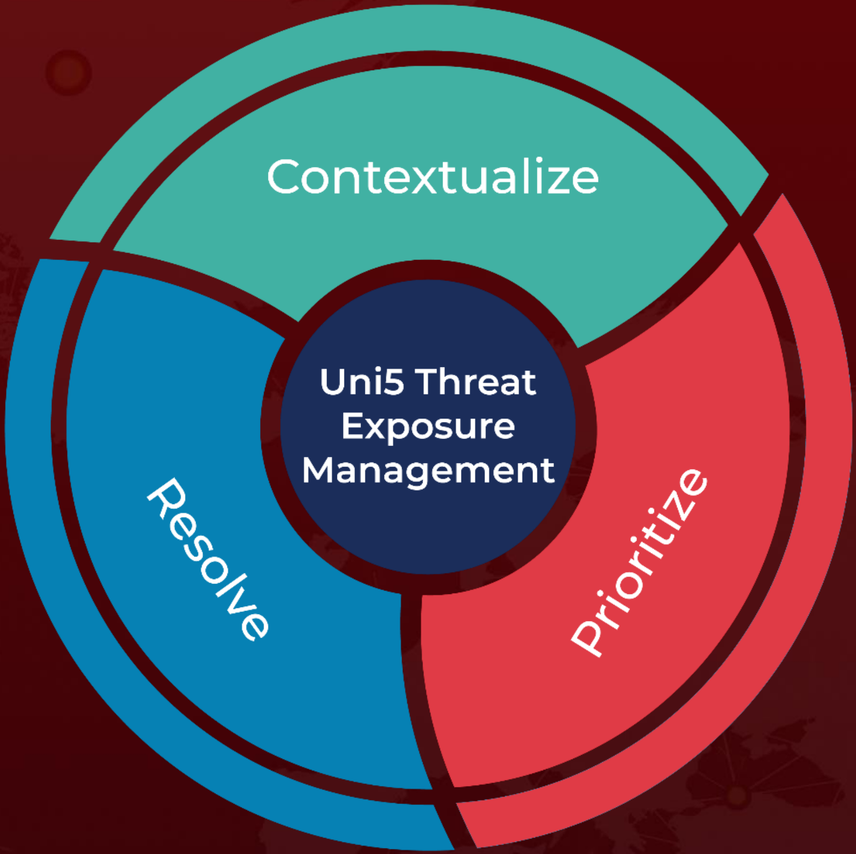
https://www.salvagedata.com/faust-ransomware/

https://www.hivepro.com/threat-advisory/in-depth-analysis-of-phobos-ransomware/

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

January 30, 2024 • 3:30 AM

More at www.hivepro.com