Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

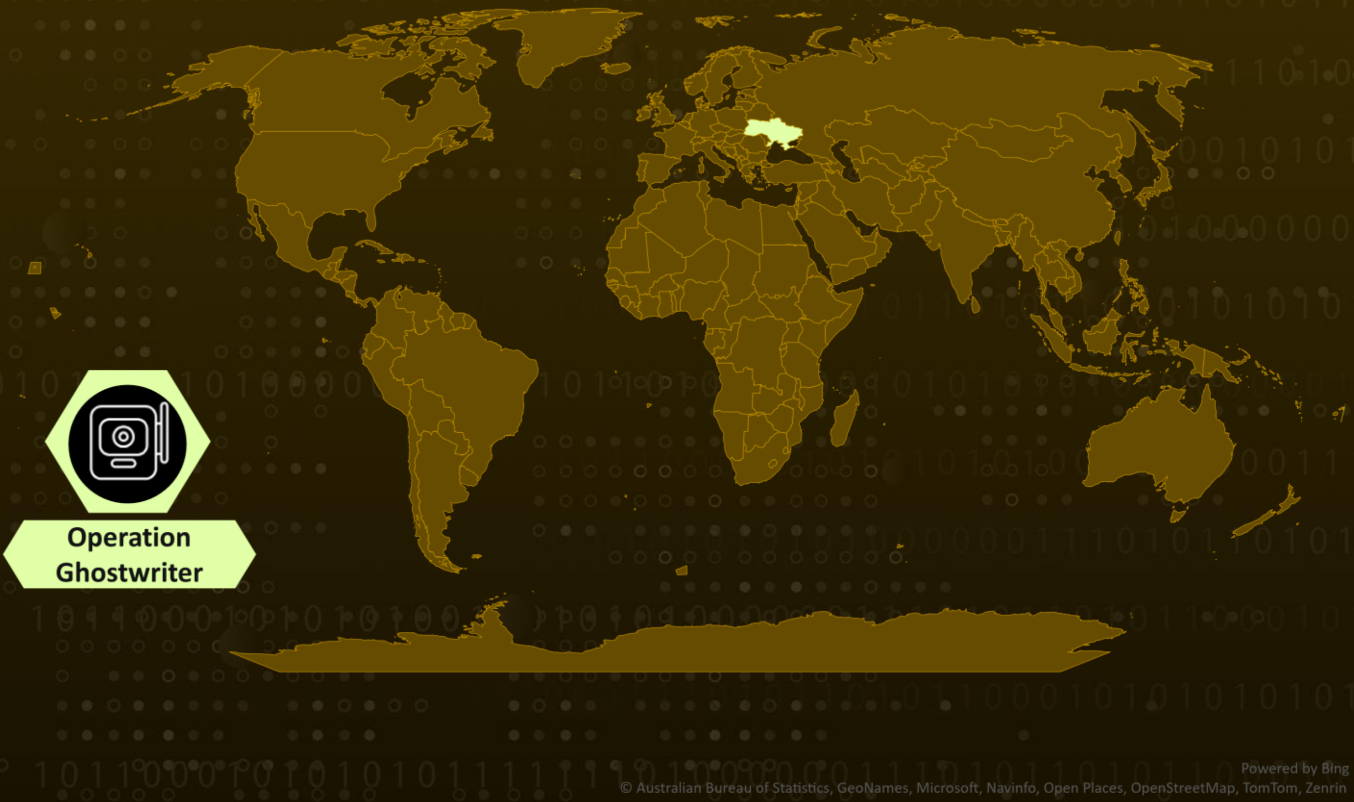
Attacker Employs Multi-Stage Malware Strategy to Target Ukraine

Date of Publication	Last Update Date	Admiralty Code	TA Number
June 06, 2024	June 07, 2024	A1	TA2024218

Summary

Discovered: June 2024
Attack Region: Ukraine
Affected Platform: Microsoft Windows
Affected Industry: Defense
Actor: Operation Ghostwriter (aka UAC-0057, UNC1151, TA445, UAC-0051, PUSHCHA, DEV-0257, Storm-0257)
Attack: A new sophisticated cyber attack has been detected targeting Ukraine, the threat actor Operation Ghostwriter is aiming to deploy Cobalt Strike and take control of compromised hosts. The attack chain begins with a Microsoft Excel file containing an embedded VBA macro that initiates the infection. The attacker employs a multi-stage malware strategy to deliver the infamous 'Cobalt Strike' payload and establish communication with a command-and-control (C2) server.

Attack Regions


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

Attack Details

#1 A complex cyberattack has been uncovered, involving an Excel file embedded with a VBA macro intended to deploy a DLL file. The threat actor Operation Ghostwriter employs a multi-stage malware strategy to deliver the "Cobalt Strike" payload and establish communication with a command-and-control (C2) server.

#2 The malicious Excel document, presented in Ukrainian, entices users to enable its VBA macros. Once enabled, the document displays sheets related to military budget allocations. The VBA macro deploys a HEX-encoded DLL downloader, creating a shortcut named "ACtIVePRObE" in "%APPDATA%\Microsoft". The macro then executes the DLL file using the "Shell" command, which in turn calls regsvr32 to execute the DLL file.

#3 The downloader, obfuscated using ConfuserEx, performs checks for specific process names to detect analysis tools or antivirus software. Upon detection, it terminates the program. The downloader constructs a web request to download the next stage payload from a specified URL, decrypts it, and saves the decoded data in the TEMP folder. After execution, the downloader deletes the decoded file and creates a new file for persistence, adding a registry value for auto-start.

#4 The "ResetEngine.dll" file is responsible for decrypting and injecting the final payload, utilizing tactics to evade detection in sandboxes. It inspects running processes and implements anti-debugging measures. The final payload is decrypted and injected into itself using various APIs. The attack aims to deploy Cobalt Strike on targeted endpoints, particularly in Ukraine's geopolitical landscape.

#5 This sophisticated malware attack employs multi-stage tactics to evade detection and ensure operational stability. The attacker incorporates location-based checks during payload downloads to conceal suspicious activities. Users must exercise caution when handling files from suspicious sources, given the critical role of office documents in such attacks.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**T1059** Command and Scripting Interpreter	**T1059.005** Visual Basic
T1574 Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1497** Virtualization/Sandbox Evasion	**T1055** Process Injection
T1027 Obfuscated Files or Information	**T1027.013** Encrypted/Encoded File	**T1211** Exploitation for Defense Evasion	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1518** Software Discovery	**T1518.001** Security Software Discovery	**T1566** Phishing

T1480 Execution Guardrails	**T1070** Indicator Removal	**T1070.004** File Deletion	**T1203** Exploitation for Client Execution
T1218 System Binary Proxy Execution	**T1218.010** Regsvr32	**T1218.011** Rundll32	**T1140** Deobfuscate/Decode Files or Information
T1057 Process Discovery	**T1071** Application Layer Protocol	**T1105** Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	goudieelectric[.]shop, simonandschuster[.]shop, thevegan8[.]shop
SHA256	88c97af92688d03601e4687b290d4d7f9f29492612e29f714f26a9278c6eda5b, 815c1571356cf328a18e0b1f3779d52e5ba11e5e4aac2d216b79bb387963c2be, 9649d58a220ed2b4474a37d6eac5f055e696769f87baf58b1d3d0b5da69cbce5, af8104e567c6d614547acb36322ad2ed6469537cd1d78ae1be65fbde1d578abc, de1bceb00c23e468f4f49a79ec69ec8ad3ed622a3ffc08f84c0481ad0f6f592b, 6f4642a203541426d504608eed7927718207f29be2922a4c9aa7e022f22e0deb, d90f6e12a917ba42f7604362fafc4e74ed3ce3ffca41ed5d3456de28b2d144bf, d9b16f077cd6e00137ba208031d22fd6423d0ef303883ad4b6f78638693f2044, 83545b07d74087acd8408d7810cafdb6c2200a72ae7dd990af40b082ad533368 9ac5fa37f5, cf3d0201f0e70a3e6527e58250ddcff77370262b8cb377e8c5995f, 08fa6aaf064470dbfac7894469457b2d78541adccba3f1bb278dd4c3f936131a
URL	hxxps[:]//goudieelectric[.]shop/cms/svg/6364[.]2809640e[.]chunk[.]svg

References

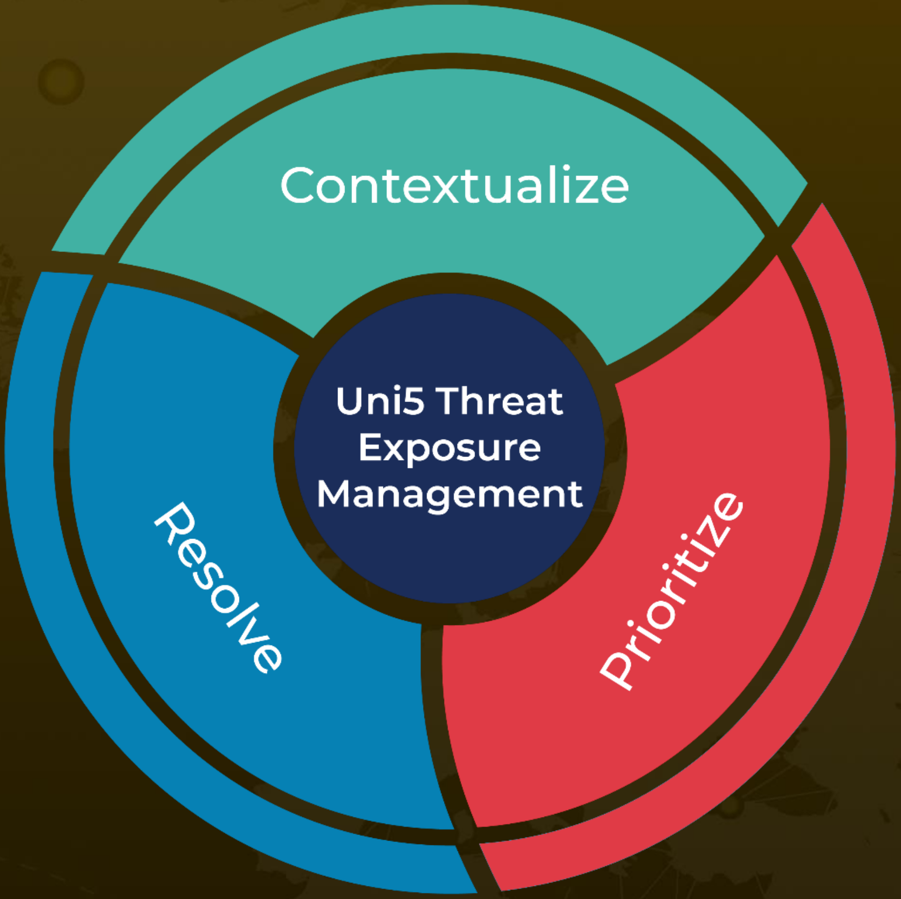
https://www.fortinet.com/blog/threat-research/menace-unleashed-excel-file-deploys-cobalt-strike-at-ukraine

https://cyble.com/blog/unc1151-strikes-again-unveiling-their-tactics-against-ukraines-ministry-of-defence/

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

June 06, 2024 • 6:50 AM

More at www.hivepro.com