Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

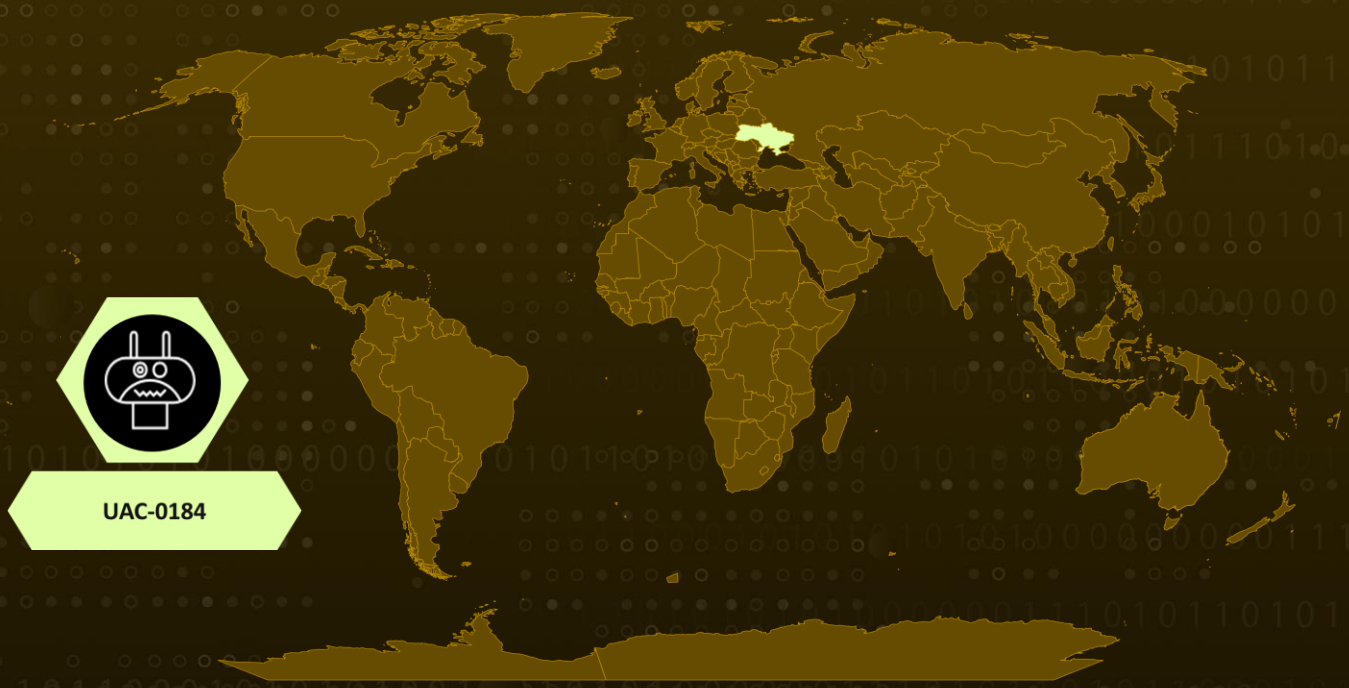
UAC-0184 Strikes Ukraine with XWorm RAT

Date of Publication	Admiralty Code	TA Number
June 26, 2024	A1	TA2024245

Summary

Threat Actor: UAC-0184
Malware: XWorm RAT
Attack Region: Ukraine
Attack: UAC-0184 has orchestrated an advanced malware campaign targeting Ukraine, deploying the Remote Access Trojan (RAT) XWorm. This attack, initiated by UAC-0148, utilizes email and spear-phishing techniques featuring ZIP attachments.

Attack Regions



Attack Details

#1 The threat actor known as UAC-0184 has launched a sophisticated malware campaign against Ukraine, deploying the Remote Access Trojan (RAT) known as XWorm. UAC-0148 initiated the attack via email and spear-phishing tactics, using enticing ZIP attachments.

#2 A PowerShell script is triggered upon executing the LNK shortcut, downloading an additional ZIP file and a decoy document. This ZIP file contains multiple components: a legitimate Python executable, a malicious Python DLL, and an encrypted payload binary.

#3 The infection strategy leverages DLL sideloading and Shadowloader to deploy the final payload, identified as the XWorm RAT. XWorm is classified as commodity malware, designed to be easily accessible to threat actors, including those with limited technical skills, who can purchase and utilize it for various cybercrimes.

#4 The objective of the UAC-0184 cybercriminals was cyber espionage, aiming to gain unauthorized access to victims' computers, remotely control infected systems, steal sensitive information, and execute commands.

Recommendations

Behavior-Based Detection: Use endpoint detection and response (EDR) solutions to detect unusual behaviors indicative of a RAT like XWorm, such as unauthorized access attempts or anomalous system activities.

Implement Application Whitelisting: Use whitelisting to ensure only approved and trusted applications and DLLs can execute on your systems. Regularly review and update the whitelist to include necessary software while excluding potentially harmful programs.

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1574 Hijack Execution Flow	T1547.001 Registry Run Keys / Startup Folder	T1574.002 DLL Side-Loading
T1055 Process Injection	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1057 Process Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer
T1059.005 Visual Basic	T1566 Phishing	T1566.001 Spearphishing Attachment	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	06adb754096f5853999038c000d8cdafa69bb1696b1011e781ab18bbea6107ce, 0d16de10ce708b990d1b0ae26ac12792c91864426c88a8c73a475f7f33db014b,

TYPE	VALUE
SHA256	17dc38bd4e01496a91d82e6de763df6fd94c00eb1e90e0cccd7f07f84b549f43, 38dea3732044129bd99314de582ba3d58a649c8967fe12b98cd867ca6e349ffe, 40fd3597c44d10e201304b80c20dd8f2a1ad1ee1032f90d83d7917e037a1d130, 444986ba74685fde34afbbf6a6963c5f35f12a1a65a705e5184c545a18c080c6, 7382cf09d04de58beeba4d71fec9777815924fe66849c89e4230b8f26bff2650, 7860a6e7264839c59506d5d69e40311e0c1e6af11b2351ccffe8d9b09acde9a3, 98fcabe279d4001b29949d980aa9ae8396b352ef7c4a90b9dbe07650a7d4b797, b1355a4eef0c265a9d918cec16f7299f4acc51daf8e3d59ef445cb46914f48ff, bf5a2450f5287f775c2427590c29c27e28e3662c2f68296c64cdacdb639f3b97, d815e32b7998d3927792e579d4ad8430792ca1043b3570f0ee73855529516d21, d938cb8accbc51046158350155f1af9248fc8459ef2b92be752b93dae77504a6, dd8377e9c3620d0732bedecd0d219f77f7bcffbc49470a9b7ff22db33fe4a185, dea780f228acbd536b5cbb35efe1a41d18771f6ed987c9d19b175de44f1d566c, e314b233b41a5688a4e43f876ccb10718351d3f396b4df623b4ebb0a093be7e0
URL	hxxp[:]//185[.]216[.]68[.]142[:]9000/hooks/xxx?id=%computername%, hxxp[:]//45[.]95[.]232[.]82/dfghujfdkg3fmsud/sud[.]exe, hxxp[:]//81[.]19[.]139[.]14/987yuhgzsd234dfwhjkaqppkg[.]zip, hxxp[:]//81[.]19[.]139[.]62/f8d79yuhjhlgdjlsjkf83da0pkg[.]zip, hxxp[:]//81[.]19[.]139[.]62/f8d79yuhjhlgdjlsjkf83da0sud/sud[.]exe, hxxp[:]//88[.]151[.]192[.]128/djfhu34u9983234s3fnvmxxzpkg[.]zip,

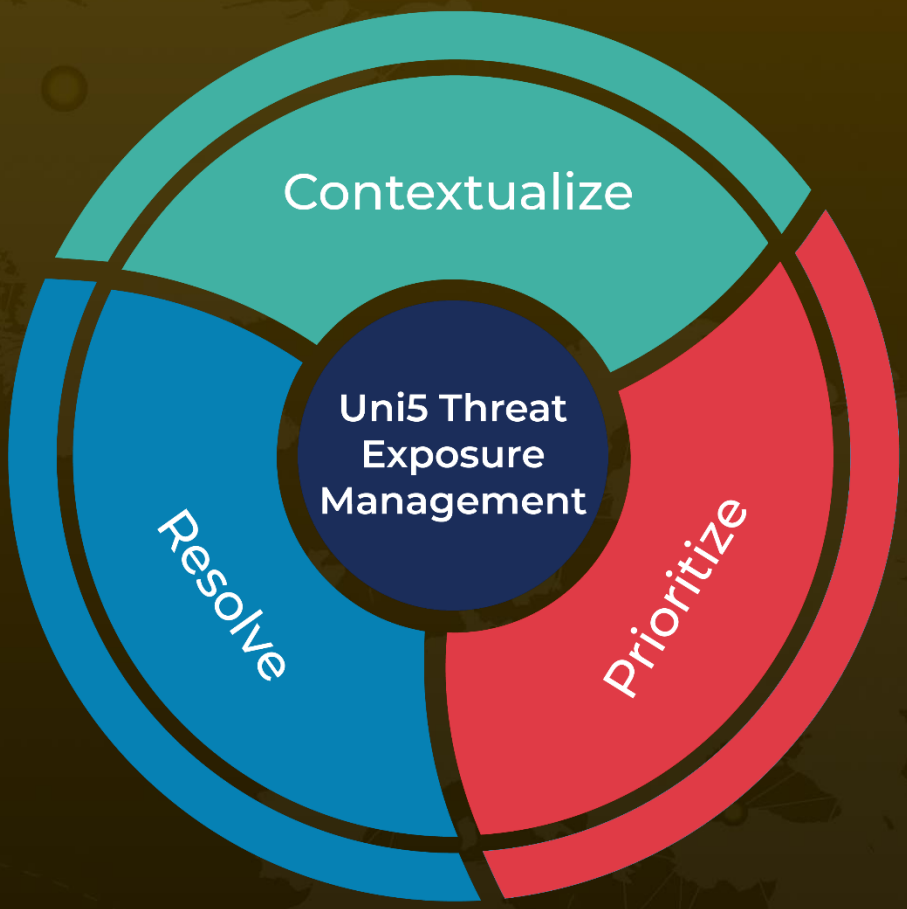
References

https://cyble.com/blog/uac-0184-abuses-python-in-dll-sideloading-for-xworm-distribution/

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 26, 2024 • 7:00 AM

More at www.hivepro.com