Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

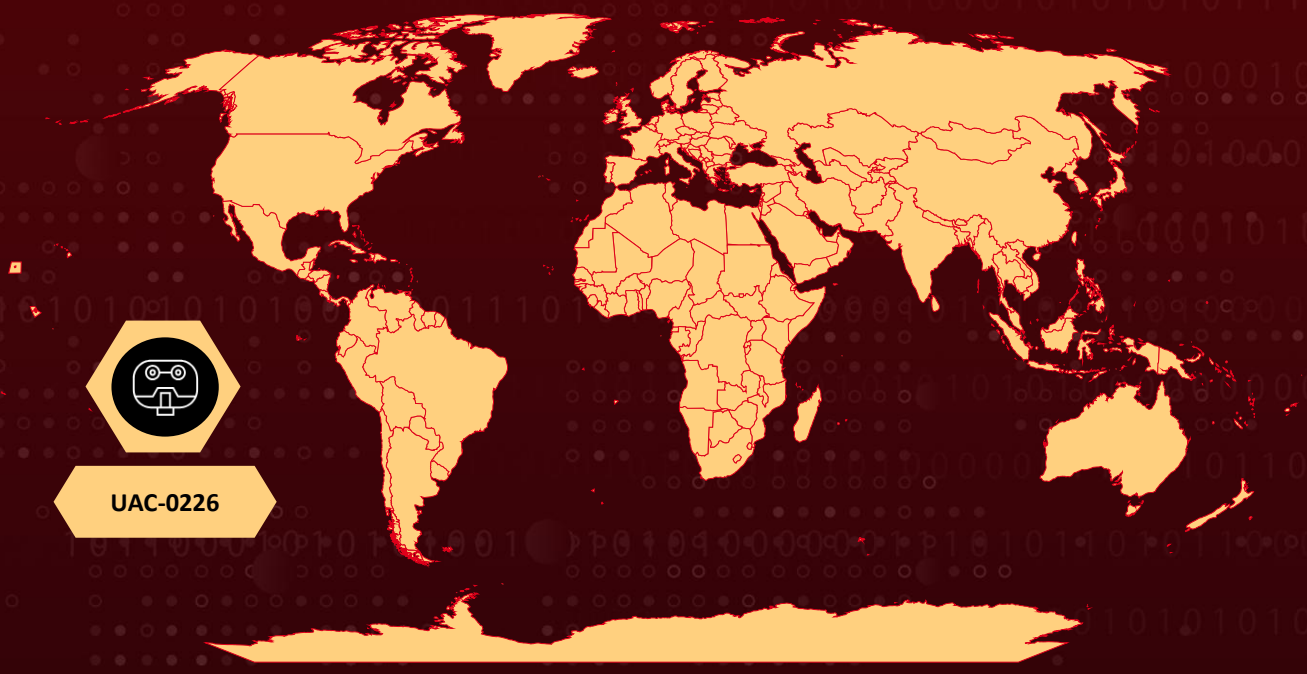
UAC-0226: Targeted Cyber-Espionage Against Ukrainian Innovation Hubs

Date of Publication	Admiralty Code	TA Number
April 9, 2025	A1	TA2025108

Summary

Attack Commenced: February 2025
Targeted Country: Ukraine
Malware: GIFTEDCROOK
Targeted Platform: Windows
Targeted Industries: Military, Law Enforcement Agencies, Government
Threat Actor: UAC-0226
Attack: The UAC-0226 cyber-espionage campaign targets Ukrainian military and government entities using phishing emails with malicious Excel attachments. Once opened, these deploy the GIFTEDCROOK malware, which steals browser data and exfiltrates it via Telegram. The attack aims to compromise national security and disrupt critical operations, highlighting the urgent need for strong cybersecurity practices.

Attack Regions



Attack Details

#1 The UAC-0226 cyber espionage attack targets Ukrainian military innovation centers, armed forces, law enforcement agencies, and local government entities particularly those near the eastern border. The primary objective of this campaign is to conduct espionage by stealing sensitive data, compromising national security, and disrupting institutional operations.

#2 The threat actors behind UAC-0226 are using phishing emails as their initial attack vector. These emails contain Microsoft Excel attachments with titles related to defense and technological innovation, likely intended to attract the attention of targeted users. Once opened, the attachments execute embedded Base64-encoded scripts designed to bypass user suspicion and deliver a secondary payload without triggering immediate alarms.

#3 This secondary payload is a custom malware named GIFTEDCROOK, developed in C/C++. Once deployed, the malware focuses on extracting sensitive data, particularly from widely used web browsers such as Google Chrome, Microsoft Edge, and Mozilla Firefox. It harvests login credentials, cookies, and browsing history, which can be used for further infiltration or intelligence gathering.

#4 Uniquely, the malware uses PowerShell commands to send the stolen data directly to a Telegram bot, leveraging the popular messaging app as a covert exfiltration channel. The ongoing nature of the attack underscores the importance of robust cybersecurity hygiene, especially in sectors that handle sensitive or strategic information.

Recommendations

Strengthen Email Security: Implement advanced email filtering solutions to detect and block phishing emails and malicious attachments. Enable attachment sandboxing to safely analyze suspicious files before they reach end users. Educate personnel, especially in defense and government sectors, to recognize and report phishing attempts.

Monitor and Audit System Activity: Regularly review email and web server logs for unusual behavior, such as unexpected file downloads or outbound PowerShell commands. Deploy endpoint detection and response (EDR) tools to detect anomalies, malware activity, and lateral movement.

Harden System Configurations: Disable or restrict the use of PowerShell where not required, and enforce logging for PowerShell execution. Apply the principle of least privilege across all user accounts to limit the impact of potential breaches. Ensure macros in Office documents are disabled by default and only enabled for verified documents.

Network and Endpoint Monitoring: Monitor endpoint behavior for signs of script execution and abnormal PowerShell usage. Use behavioral analysis tools to detect malware like GIFTEDCROOK that may bypass traditional signature-based defenses. Implement network traffic monitoring to detect exfiltration patterns, especially connections to Telegram APIs or suspicious PowerShell activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0010 Exfiltration	TA0002 Execution	TA0007 Discovery
TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control	TA0003 Persistence
TA0005 Defense Evasion	T1566.001 Spearphishing Attachment	T1059.001 PowerShell	T1204 User Execution
T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information	T1082 System Information Discovery	T1204.002 Malicious File
T1140 Deobfuscate/Decode Files or Information	T1555 Credentials from Password Stores	T1539 Steal Web Session Cookie	T1041 Exfiltration Over C2 Channel
T1567.002 Exfiltration to Cloud Storage	T1567 Exfiltration Over Web Service	T1555.003 Credentials from Web Browsers	T1566 Phishing

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	037e2ca3c97e1a5645cdc45fb0d98064, 0a178f76c48c038e8bad03a62b52cfc9, 100cd9d907e986ba8d5fc6d0488557d9, 1b71d870f34587e0a2717f9925086eab, 333b09f8865aae5d257b6f11f2fe5d08, 3394fc2ba0a976818691751aa7f86d05, 4a2ec9f72b910c0a8e3efc4c334f5bad, 671b42e854ae2ee3341456fbec7c7787, 8b694068e5088e0c32739956e28b077e, 966373dbe28f4111f6ce47038fb343da, 9c03d0da190d1046583ba9fa83a8bcd3, 9f6c82c240ba5ef6bb85d28c0cdf7f7f, b3831f0bace886aaba81873edc20aba4, b63b783a9aca15726babd599d2963869, cffdd24742610fe5710dbc9ebd258c64, d280a258704bf9155bceaf4f731988ea, daffbfd71f8595ab6d6b8c94cc81a778, e5f4188682e40e79800ccd165289c844, f62ea2cbd220596072010e91dd65b673
IPv4	149[.]102[.]246[.]110, 37[.]120[.]239[.]187, 89[.]44[.]9[.]186
URLs	http[://]37[.]120[.]239[.]187:6501, http[://]89[.]44[.]9[.]186:3240
SHA256	0a4777725673f9f7114ddceddd80e5a72ad3a4d20fd2014d4c60e2cc1a6cefc2, 24a60e50ed8469fc31afa9abfc361291f72922430cf062bf9c4ac7e6d84b5fad, 2930ad9be3fec3ede8f49cecd33505132200d9c0ce67221d0b786739f42db18a, 40e68d7240e692ef3301cfaa92a04e0af65f2d725cbfa6711c3154b627fec0f1, 530185fac69e756fb62f23e21e7c0b0828a964b91bbf40f1d04fc2136c1b6dd1, 58b38775f655498b134ce8cd52ab0aba05b710f7611e41cbdffdc3597c5d5f3d, 78ea83bfbca85a39e59fa35c8f704873f3fdad3a5278430e75286247530042b8,

TYPE	VALUE
SHA256	7ca3f2505e1778e6de3927571ba49d27b36447e6c28a60161d55fd2254966bce, 8427dc6e7da4c163d20c7f188232cf3f83c78ddb6fcad04cec84b33e0f9bdfc0, 8a638a788adb0edb6622b16fd8783bc225470f8ff94b1bba4a94b4d8c105acef, 92183f89b115881535b1bf1985f3ee4b4ebf077bec8cc4de0c6c6e266da0cb87, a02506468e632875a2c9c9c16e730b8bdc52f7450b28ee7bd8f5ac014b264e53, a2f651d39b8d97221ad36577e9b50beabdf0ad46aec0c29b6cff624e1e2ffd0c, c27cf714293c496c8fc05b330a57bcfcb6189267e2818062660de88b0f3a25cd, c8bb0dbc952c9dc2bbc550a300ed033ad5d2416390891ed1e800b08ad3ab5d3a, d7a66fd37e282d4722d53d31f7ba8ecdabc2e5f6910ba15290393d9a2f371997, e852d254395ef04308bcde37c3ee9725ab23ca82a202e7d69028c8bee0f0d05f, f8a31715840852e8ef04016b31f909123f2aa864f3850c45eb511fd1885b4037, ff1be55fb5bb3b37d2e54adfbe7f4fbba4caa049fad665c8619cf0666090748a

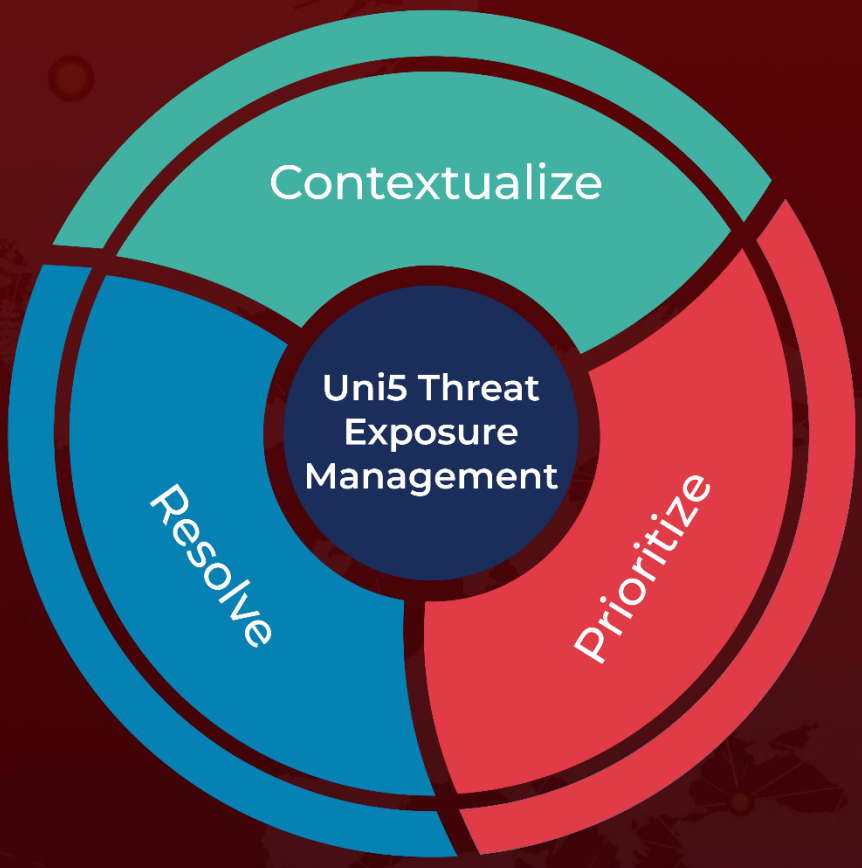
References

https://cert.gov.ua/article/6282946

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

April 9, 2025 • 9:40 PM

More at www.hivepro.com