Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

True Face of Civil Defense: Russian Espionage Group Targets Ukraine

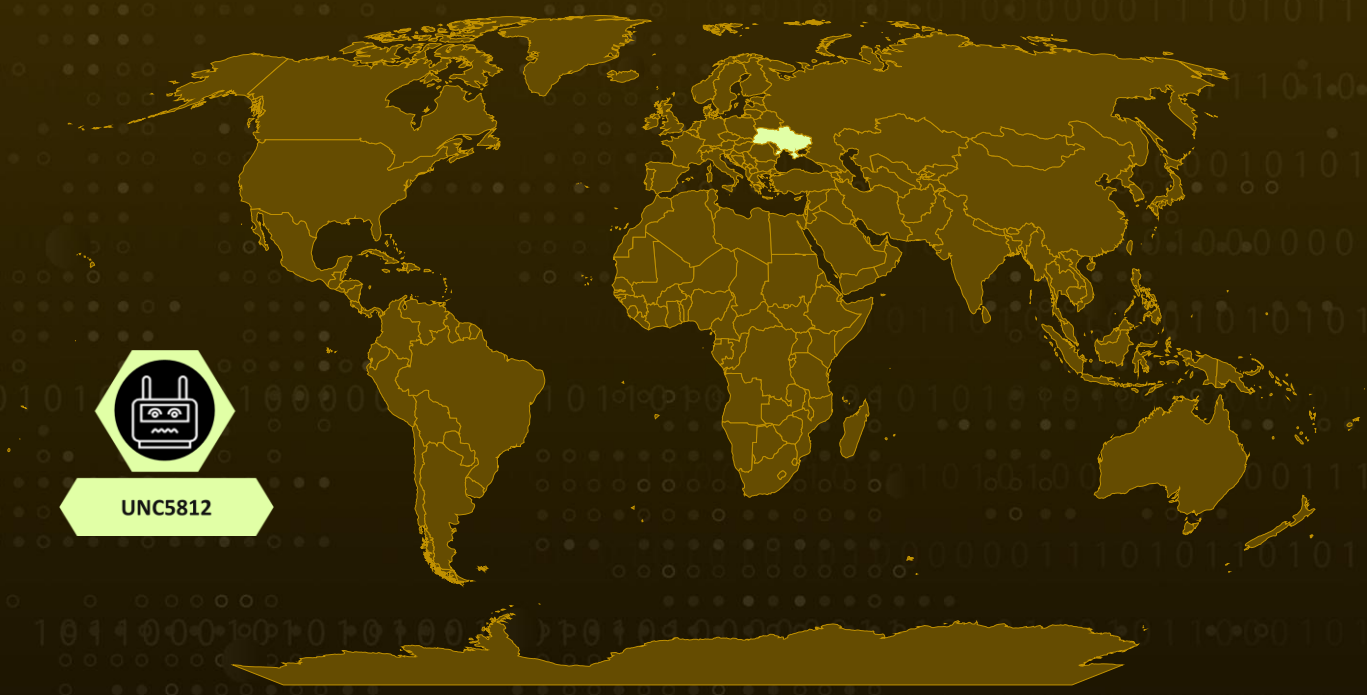
Date of Publication	Admiralty Code	TA Number
October 30, 2024	A1	TA2024417

Summary

Attack Commenced: April 2024
Threat Actor: UNC5812
Malware: Pronsis Loader, SUNSPINNER, PURESTEALER
Affected Platforms: Windows and Android
Targeted Country: Ukraine
Targeted Industry: Military

Attack: UNC5812, suspected to be a Russian-led hybrid operation, has initiated a complex campaign leveraging its "Civil Defense" Telegram profile to deploy malware targeting the Ukrainian military. Through a website and a Telegram channel with over 80,000 followers, "Civil Defense" promotes free software it claims assists conscripts in tracking Ukrainian military recruiters.

Attack Regions



Attack Details

#1 UNC5812, considered a Russian-led hybrid operation blending espionage with influence tactics, uses a Telegram account, "Civil Defense," to distribute malware. This campaign targets the Ukrainian military, deploying malware for Windows and Android devices while also claiming compatibility with macOS and iOS.

#2 The "Civil Defense" operation established an online presence with its website, civildefense[.]com[.]ua, registered on April 24, 2024, and a Telegram channel, civildefense_com_ua, activated on September 10, 2024. With over 80,000 followers, this channel shares missile alerts and directs users to "Civil Defense" resources, fostering engagement across its platforms.

#3 Presenting itself as a provider of free software for potential conscripts, "Civil Defense" claims to offer tools for tracking locations and sharing information about Ukrainian military recruiters. If Google Play Protect is disabled, these applications install a commodity malware variant alongside a decoy mapping app known as SUNSPINNER.

#4 In addition to malware deployment, UNC5812 is active in influence operations, spreading propaganda and seeking user-generated content aimed at undermining support for Ukraine's mobilization efforts.For Windows users, a ZIP download extracts a PHP-based malware loader named Pronsis, which installs both SUNSPINNER and PURESTEALER.

#5 PURESTEALER is an information-stealing malware available commercially from the "Pure Coder Team" at prices ranging from $150 per month to $699 for a lifetime license. On Android, users are targeted with a malicious APK file that installs a variant of the CRAXSRAT backdoor, another widely available commercial tool.

Recommendations

Implement Real-Time Threat Monitoring: Develop a real-time threat monitoring system that can automatically block or alert users about potentially harmful applications, especially those downloaded from third-party sources. This system should leverage data from Safe Browsing and Google Play Protect to provide comprehensive protection.

Increase Transparency and User Control: Provide users with more transparent information about how their data is being protected and give them more control over app permissions. This empowerment can reduce the likelihood of users disabling critical security features.

Analyze Traffic to Malicious IPs: Use network monitoring to detect traffic to malicious domains and IPs linked to known malware servers. Look for connections attempting to contact command-and-control (C2) servers associated with malware like Pronsis Loader, SUNSPINNER, and PURESTEALER.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
TA0042 Resource Development	**T1071.001** Web Protocols	**T1053** Scheduled Task/Job	**T1562.001** Disable or Modify Tools
T1562 Impair Defenses	**T1083** File and Directory Discovery	**T1119** Automated Collection	**T1203** Exploitation for Client Execution
T1041 Exfiltration Over C2 Channel	**T1036** Masquerading	**T1105** Ingress Tool Transfer	**T1083** File and Directory Discovery
T1204.002 Malicious File	**T1587.001** Malware	**T1071** Application Layer Protocol	**T1588.001** Malware
T1587 Develop Capabilities	**T1588** Obtain Capabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
Telegram channel	[@]civildefense_com_ua
Domains	civildefense[.]com[.]ua, h315225216[.]nichost[.]ru, fu-laravel[.]onrender[.]com, nichost[.]ru
URLs	hxxps[:]//t[.]me/UACivildefenseUA, hxxp[:]//t[.]me/civildefense_com_ua, hxxp[:]//h315225216[.]nichost[.]ru/itmo2020/Student/map_markers/mainurl[.]json, hxxps[:]//fu-laravel[.]onrender[.]com/api/markers, hxxp[:]//185[.]169[.]107[.]44/cd/CivilDefenseFluxxer[.]zip, hxxp[:]//185[.]169[.]107[.]44/cd/civildefensestarter[.]zip, hxxp[:]//185[.]169[.]107[.]44/source/cityproductpro[.]zip, hxxp[:]//185[.]169[.]107[.]44/source/storescientificpro[.]exe, hxxp[:]//206[.]71[.]149[.]194/cd/cddldurl[.]txt, hxxp[:]//206[.]71[.]149[.]194/cd/pdldurl[.]txt, hxxp[:]//h315225216[.]nichost[.]ru/itmo2020/Student/map_markers/CivilDefense[.]apk, hxxps[:]//civildefense[.]com[.]ua/civildefense/CivilDefensse[.]apk
MD5	4ca65a7efe2e4502e2031548ae588cb8, 7ef871a86d076dac67c2036d1bb24c39, d36d303d2954cb4309d34c613747ce58, b3cf993d918c2c61c7138b4b8a98b6bf, 31cdae71f21e1fad7581b5f305a9d185, aab597cdc5bc02f6c9d0d36ddeb7e624, e98ee33466a270edc47fdd9faf67d82e, 0385d669af51031ffb20b61c1d33d606, 2035ed9c36a8d70be88de57155b6cb75, 2762571c8a849f5f41d2eb22613eca49, 4f42d37074e4ac5e6d3cb605430e122b, 77fd3f271bf41e61581cc08c9eb15dfd, 836fe8d7e680032fa36fbcf85f52fd49, 97a339136b5fddcbeec07f093d33557e, c7f6ddb7c196249be8933a215e657057, d5a83b5bdd8010bc3f4629763ed15173, e2241a2341eb89aafee9c721ca20fd3f, f10ccc45ee7d5d261545b64c63288265, f960434d421036c88268ebaac46391b1,

TYPE	VALUE
SHA1	eef25d4316a0c67ed00e3d40441fcab30ccd0a9d, d6de7db63cc8ed63610271f3310786b93852ece1, e2de9ca2575dfe6114e688c44647a58a1ec325c2, a8cf0215610317b68a71d7a6fed7d9e07241d373, 9ce3ab0bf4ee52e98fbd94787783ac6962e21304, 7f7e698b71c99ed266cf820de4d89582b0a22985, 03fe838f2c0e6dbe37e42995e369f8f0dc47574f, 3b83f2371c66380a11467313fb6df5ec7e647870, 55b8d067b2cf5f40e5d132633b8eb1a2ffb049b5, 62c06be3183c6c56bffb82fb53389792da304fd1, 70115281e9eb2945f3c3e1a83f21fb4e9f9aa140, 71059dddc2c963ea5f332d0b3b2255c151a8a44a, 89ee89b00cf83357160b8c3b9032070e1896848b, b8cabbf9b2b2cc44605ad187d34071928c40c6bb, d057d8bf464b2fd8503a869a3b12ee9628ce6816, d080e6a9baa0cabf1b48c616d9dd5e5f71f8a10b, e87a17bfe868be361ea87a8746b60915d780a146
SHA256	614e74654773e617475d519edd23380f531b60264fd7f8ed86aebf28efed4e39, 4c699f4ddb494bd442aa0cc3eceec77aa72fb41536eff8d09bd601e354130c3e, f2058183f59cba1aed685d44e5c5b9d56995cfa54b38e18889c059b2bde36b3a, d66075b2c70c3de22c9e774ad9e5f88d3d85708d1a5b17ccd4e76049c86b49b5, b4f7414f3c6de7cad88c4178ecfc8201d123fb6db9a5ecd8053f7750757d154e, aaa7979911d6b5665a4ff0a8a63cb06f3564c772c42914513bd5cbb6aa839d31, 3f298905573fd681f897012fdc7e6b26948fa0ad72e394c3cef996c21625f7db, 03aec4ba09a8695c59c2b38ea52e24106ed13d9e80fc0b5a6d736d852642db47, 1180b83620e60ad704a0d956f515f74813024ec701e738ecff18550da4a7b19a, 19a5700f61eb0f955ef93f0b0d4b71ca73d5beb14cc284a390e895cf82cc6054, 1b542b014b0964721d167e94d8fc6ee2324a06aae48de703b0b6f366068cd130, 2050328feb02e79f23375dcd90cf7abb27223211bcc7b8e31bc3adf37b82a3f6, 2b790db4560fd6b73a717314a01059d75180ee26dbe69ba09cad9529c779db31,

TYPE	VALUE
SHA256	2b8e532d8ac6332f0cb3a93f3da36f00f1b9d89e7e07c3da29fbe8bf98935102, 56a277f36545a8756a29cf6fc0da710e5843f46b7e61b3808ed66b03717e4ac3, 5be7a986f04f530d3ce26084e2fefb923c85ef16c883b466fa76f4063b29b783, a7de2e5e50e0d2dc512caffa7f248e516672a23c05c5301ccf7c27ab5d611b98, b590df549940efcf9e54489276afaf9e6bed2b5bba6fc36c3a959a3425aea5e0, c2b2be2496a9c566ec72fe24d2fc00d4cfe623198242560359c19ce09de64000, ce39b858c2056b37927526f21edf09c4885d9d5cab45f920491de9d8da5cc1bd, eef42383de210416f45e48dc35b74586a90bdcf4708f7afb818934bb72e9ea5e
File Name	CivilDefense.exe, civildefensestarter.exe, CivilDefensse.apk
IPv4	206[.]71[.]149[.]194, 185[.]169[.]107[.]44, 91[.]189[.]114[.]19,

References

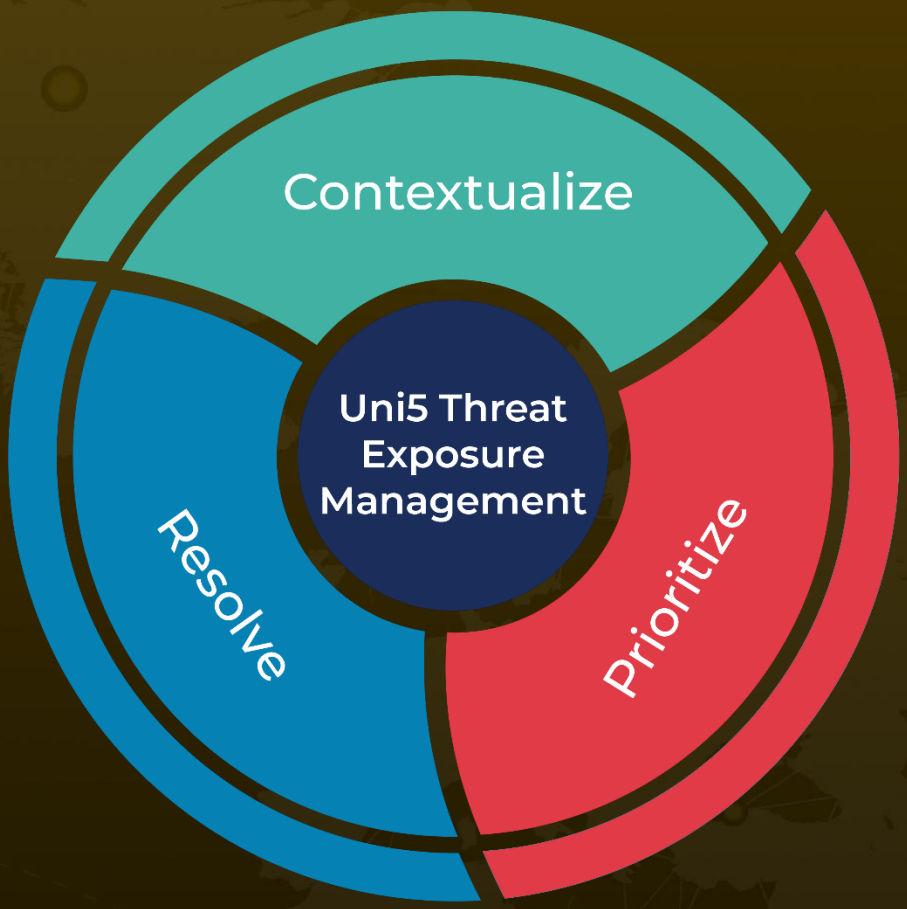
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives

https://hivepro.com/threat-advisory/errorfather-a-multi-stage-cerberus-attack-on-android/

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

October 30, 2024 . 7:30 AM

More at www.hivepro.com