Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

Google Threat Intelligence Group ⋮⋮ 10/28/2024

In September 2024, Google Threat Intelligence Group (consisting of Google's Threat Analysis Group (TAG) and Mandiant) discovered UNC5812, a suspected Russian hybrid espionage and influence operation, delivering Windows and Android malware using a Telegram persona named "Civil Defense". "Civil Defense" claims to be a provider of free software programs designed to enable potential conscripts to view and share crowdsourced locations of Ukrainian military recruiters. If installed with Google Play Protect disabled, these programs deliver an operating system-specific commodity malware variant to the victim alongside a decoy mapping application we track as SUNSPINNER. In addition to using its Telegram channel and website for malware delivery, UNC5812 is also actively engaged in influence activity, delivering narratives and soliciting content intended to undermine support for Ukraine's mobilization efforts.

Figure 1: UNC5812's "Civil Defense" persona

Targeting Users on Telegram

UNC5812's malware delivery operations are conducted both via an actor-controlled Telegram channel `@civildefense_com_ua` and website hosted at `civildefense[.]com.ua`. The associated website was registered in April 2024, but the Telegram channel was not created until early September 2024, which we judge to be when UNC5812's campaign became fully operational. To drive potential victims towards these actor-controlled resources, we assess that UNC5812 is likely purchasing promoted posts in legitimate, established Ukrainian-language Telegram channels.

- On September 18th 2024, a legitimate channel with over 80,000 subscribers dedicated to missile alerts was observed promoting the "Civil Defense" Telegram channel and website to its subscribers.
- An additional Ukrainian-language news channel promoting Civil Defense's posts as recently as October 8th, indicating the campaign is probably still actively seeking new Ukrainian-language communities for targeted engagement.
- Channels where "Civil Defense" posts have been promoted advertise the ability to reach out to their administrations for sponsorship opportunities. We suspect this is the likely vector that UNC5812 is using to approach the respective legitimate channels to increase the operation's reach.

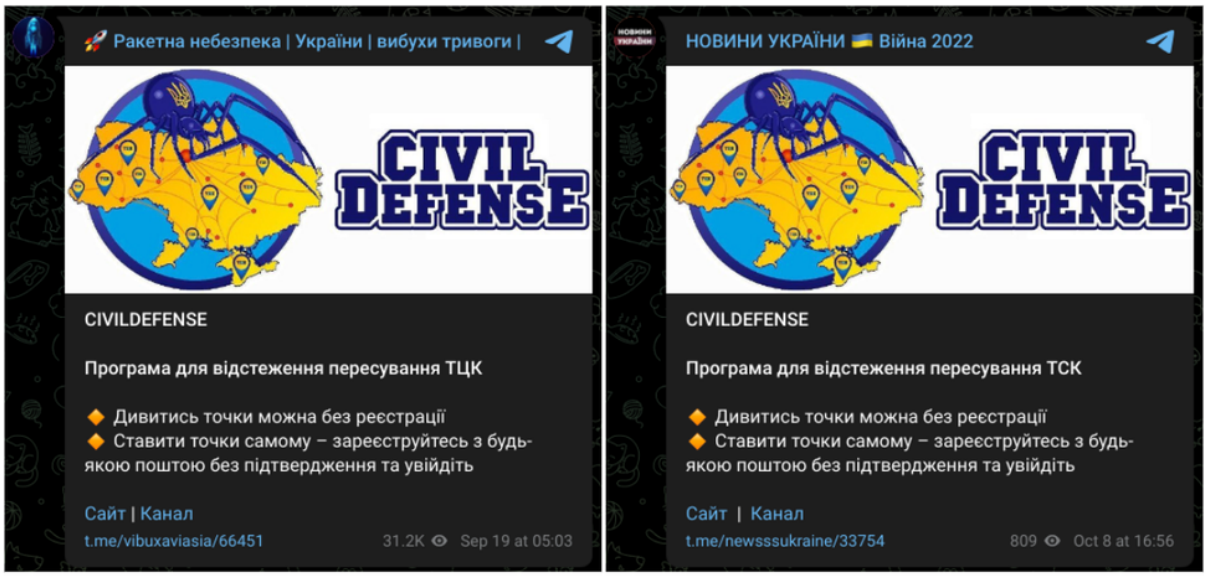

Figure 2: Civil Defense promoted in Ukrainian-language missile alert and news communities

The ultimate aim of the campaign is to have victims navigate to the UNC5812-controlled "Civil Defense" website, which advertises several different software programs for different operating systems. When installed, these programs result in the download of various commodity malware families.

- For Windows users, the website delivers a downloader tracked publicly as Pronsis Loader that is written in PHP that is compiled into Java Virtual machine (JVM) bytecode using the open source JPHP project. When executed, Prosnis Loader initiates a convoluted malware delivery chain, ultimately delivering SUNSPINNER and a commodity information stealer commonly known as PURESTEALER.
- For Android users, the malicious APK file attempts to install a variant of the commercially available Android backdoor CRAXSRAT. Different versions of this payload were observed, including a variant containing SUNSPINNER in addition to the CRAXSRAT payload.
- While the Civil Defense website also advertises support for macOS and iPhones, only Windows and Android payloads were available at the time of analysis.

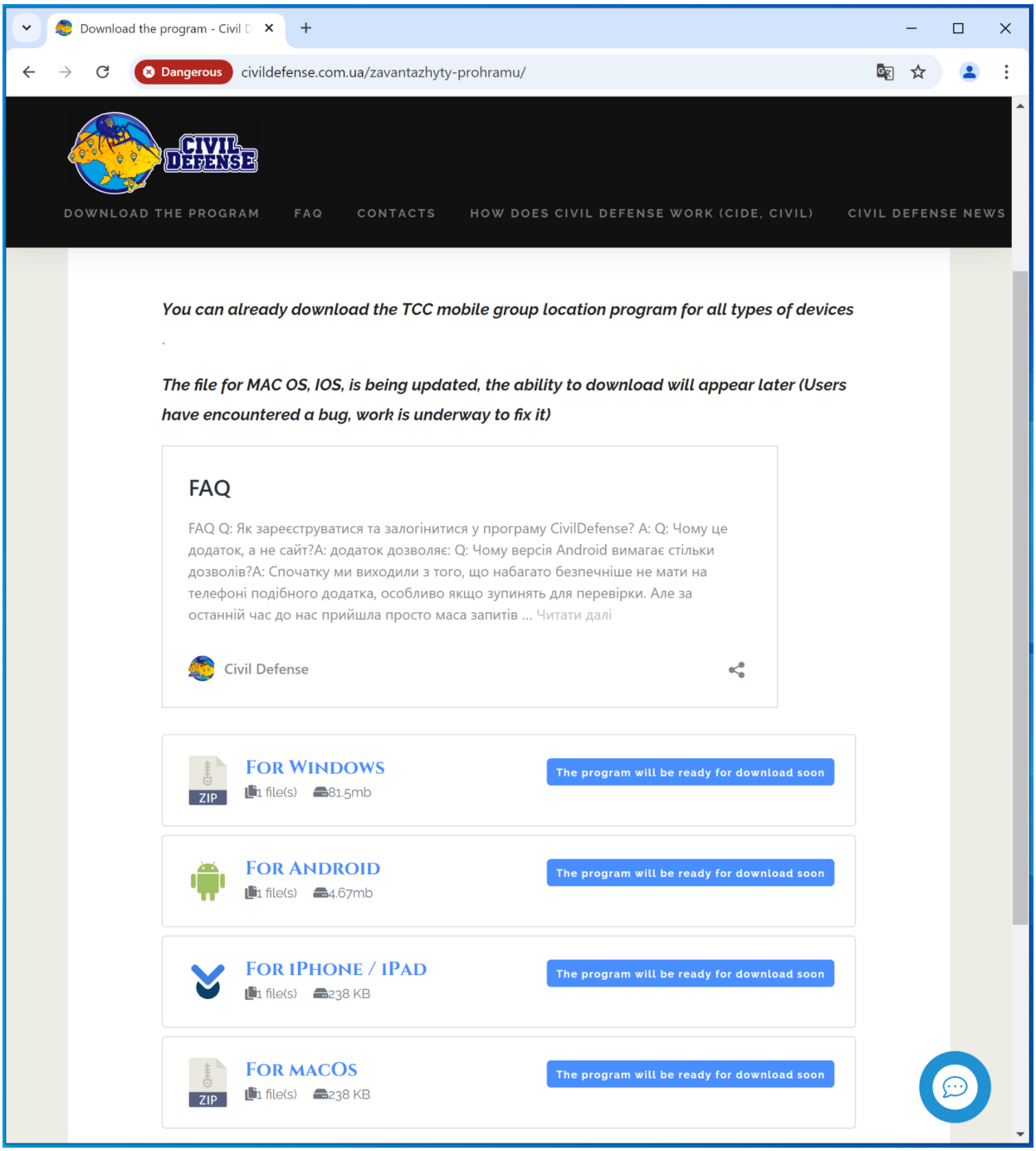

Figure 3: Download page, translated from Ukrainian

Notably, the Civil Defense website also contains an unconventional form of social engineering designed to preempt user suspicions about APK delivery outside of the App Store and justify the extensive permissions required for the CRAXSRAT installation.

- The website's FAQ contains a strained justification for the Android application being hosted outside the App Store, suggesting it is an effort to "protect the anonymity and security" of its users, and directing them to a set of accompanying video instructions.
- The Ukrainian-language video instructions then guide victims on how to disable Google Play Protect, the service used to check applications for harmful functionality when they are installed on Android devices, as well as to manually enable all permissions once the malware is successfully installed.

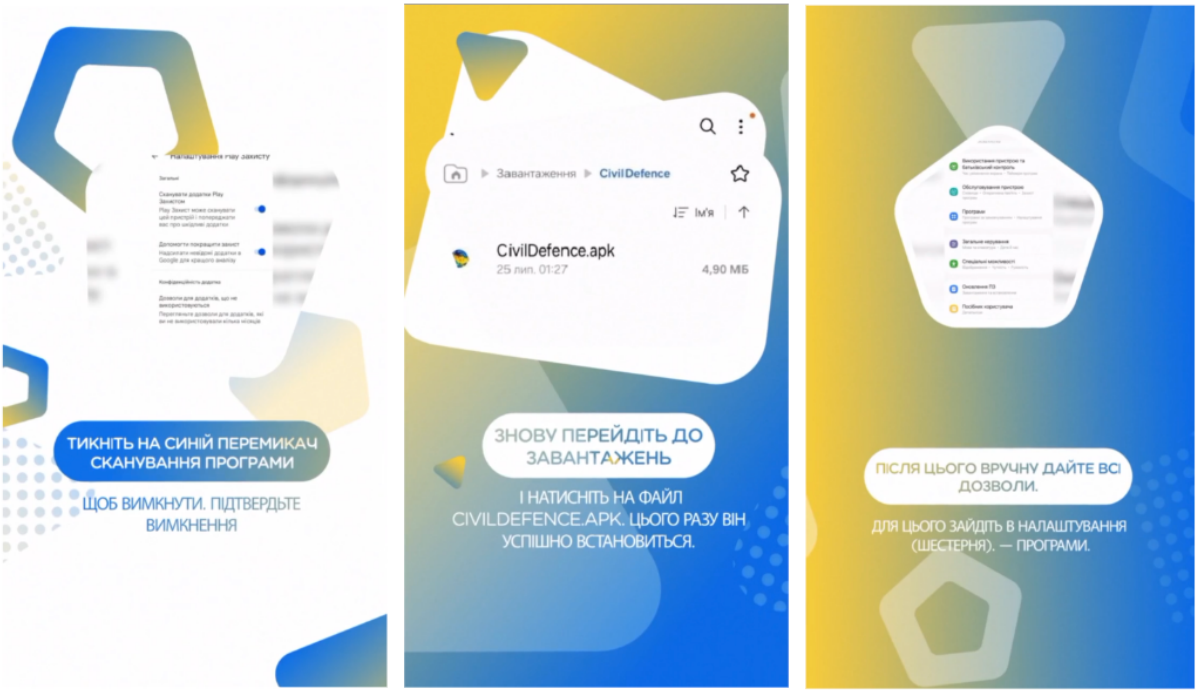

Figure 4: Screenshots of video instructions to turn off Google Play Protect and manually enable CRAXSRAT permissions

Anti-Mobilization Influence Operation

In parallel to its efforts to deliver malware and gain access to the devices of potential military recruits, UNC5812 is also engaged in influence activity to undermine Ukraine's wider mobilization and military recruitment efforts. The group's Telegram channel is actively used to solicit visitors and subscribers to upload videos of "unfair actions from territorial recruitment centers," content that we judge likely to be intended for follow-on exposure to reinforce UNC5812's anti-mobilization narratives and discredit the Ukrainian military. Clicking on the "Send Material" (Ukrainian: Надіслати матеріал) button opens a chat thread with an attacker-controlled `https://t[.]me/UAcivildefenseUA` account.

- The Civil Defense website is also interspersed with Ukrainian-language anti-mobilization imagery and content, including a dedicated news section to highlight purported cases of unjust mobilization practices.
- Anti-mobilization content cross-posted to the group's website and Telegram channel appears to be sourced from wider pro-Russian social media ecosystems. In at least one instance, a video shared by UNC5812 was shared a day later by the Russian Embassy on South Africa's X account.

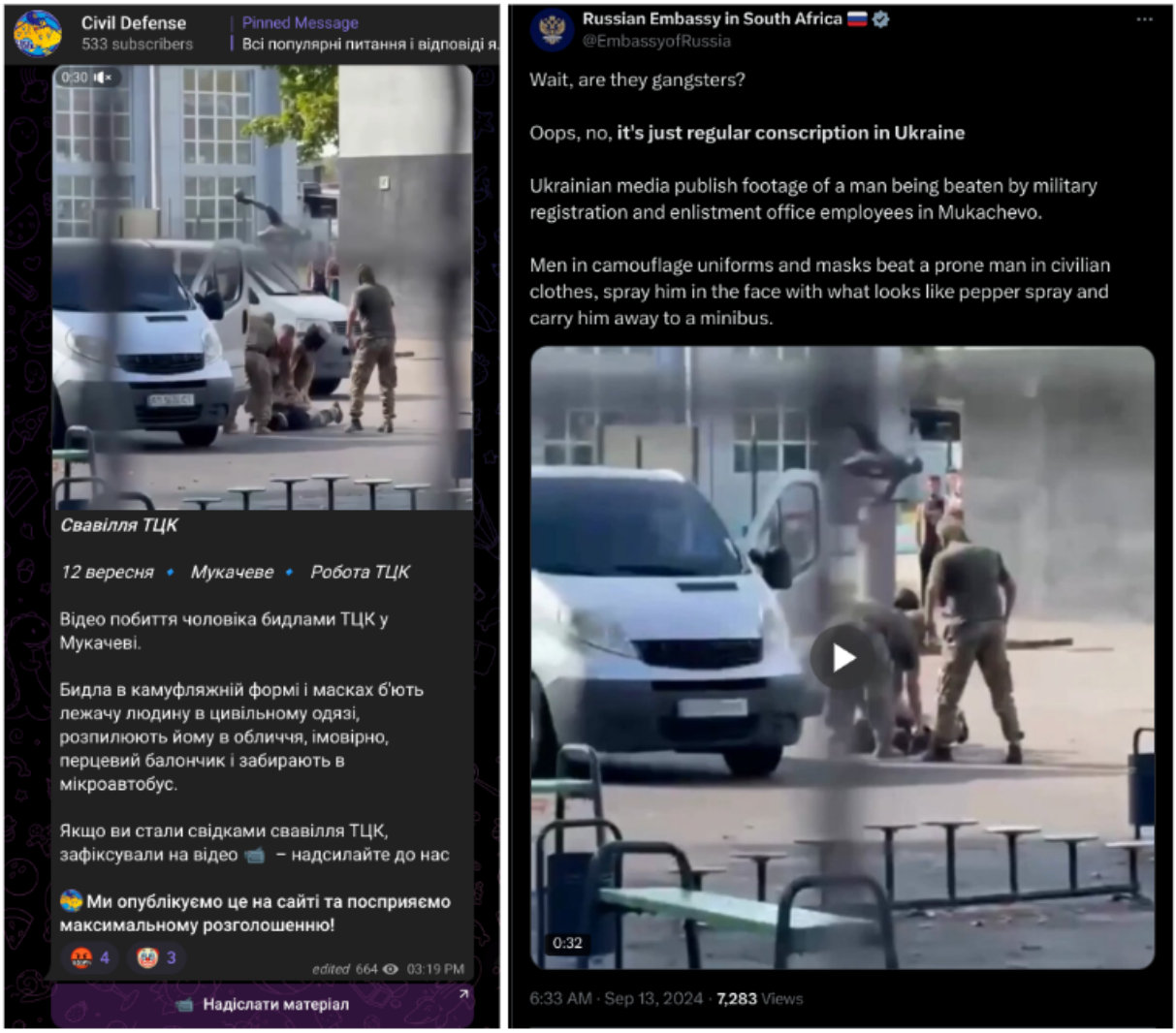

Figure 5: UNC5812's Telegram and a Russian government X account sharing the same video in close proximity, highlighting their shared focus on anti-mobilization narratives

Malware Analysis

UNC5812 operates two unique malware delivery chains for Windows and Android devices that are delivered from the group's website hosted at civildefense[.]com[.]ua. Common between these distinct delivery chains is the parallel delivery of a decoy mapping application tracked as SUNSPINNER, which displays to users a map that renders purported locations of Ukrainian military recruits from an actor-controlled command-and-control (C2) server.

SUNSPINNER

SUNSPINNER (MD5: 4ca65a7efe2e4502e2031548ae588cb8) is a decoy graphical user interface (GUI) application written using the Flutter framework and compiled for both Windows and Android environments. When executed, SUNSPINNER attempts to resolve a new "backend server" hostname from `http://h315225216.nichost[.]ru/itmo2020/Student/map_markers/mainurl.json`, followed by a request for map markers from `https://fu-laravel.onrender[.]com/api/markers` that are then rendered on the app's GUI.

Consistent with the functionality advertised on the Civil Defense website, SUNSPINNER is capable of displaying crowdsourced markers with the locations of the Ukrainian military recruiters, with an option for users to add their own markers. However, despite possessing the limited functionality required for users to register and add markers, the displayed map does not appear to have any genuine user inputs. All markers present in the JSON file pulled from SUNSPINNER's C2 infrastructure were added on the same day by the same user.

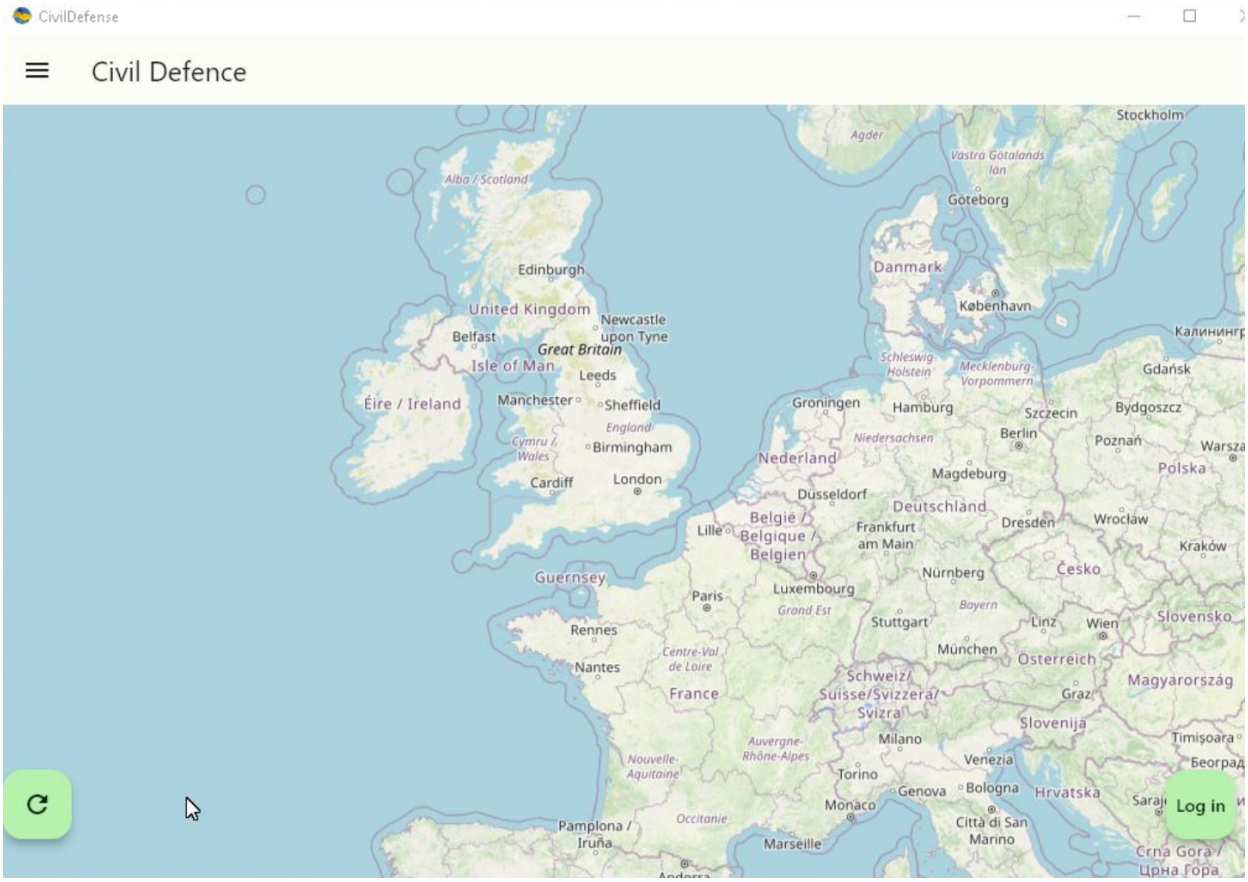

Figure 6: Decoy application for monitoring the locations of Ukrainian military recruitment staff

Windows — Pronsis Loader to PURESTEALER

The Windows payload downloaded from the Civil Defense website, `CivilDefense.exe` (MD5: 7ef871a86d076dac67c2036d1bb24c39), is a custom build of Pronsis Loader, a recently discovered commodity malware being operated primarily by financially motivated threat actors.

Pronsis Loader is used to retrieve both the decoy SUNSPINNER binary and a second-stage downloader "civildefensestarter.exe" (MD5: d36d303d2954cb4309d34c613747ce58), initiating a multi-stage delivery chain using a series self-extracting archives, which ultimately executes PURESTEALER on the victim device. The second-stage downloader is written in PHP and is compiled into Java Virtual machine (JVM) bytecode using the open-source JPHP project and then built as a Windows executable file. This file is automatically executed by the CivilDefense installer.

The final payload is PURESTEALER (MD5: b3cf993d918c2c61c7138b4b8a98b6bf), a heavily obfuscated commodity infostealer written in .NET that is designed to steal browser data, such as passwords and cookies, cryptocurrency wallets, and from various other applications such as messaging and email

clients. PURESTEALER is offered for sale by "Pure Coder Team" with prices ranging from $150 for a monthly subscription to $699 for a lifetime license.

Android — CraxsRAT

The Android Package (APK) file downloaded from the Civil Defense website "CivilDefensse.apk" (MD5: 31cdae71f21e1fad7581b5f305a9d185) is a variant of the commercially available Android backdoor CRAXSRAT. CRAXSRAT provides functionality typical of a standard Android backdoor, to include file management, SMS management, contact and credential harvesting, and a series of monitoring capabilities for location, audio, and keystrokes. Similar to PURESTEALER, it's also available for sale on underground forums.

The Android sample being distributed at the time of analysis only displayed a splash screen with the "Civil Defense" logo. However, an additional identified sample (MD5: aab597cdc5bc02f6c9d0d36ddeb7e624) was found to contain the same SUNSPINNER decoy application as in the Windows delivery chain. When opened, this version requests the Android REQUEST_INSTALL_PACKAGES permission from the user, which if granted, downloads the CRAXSRAT payload from `http://h315225216.nichost[.]ru/itmo2020/Student/map_markers/CivilDefense.apk`.

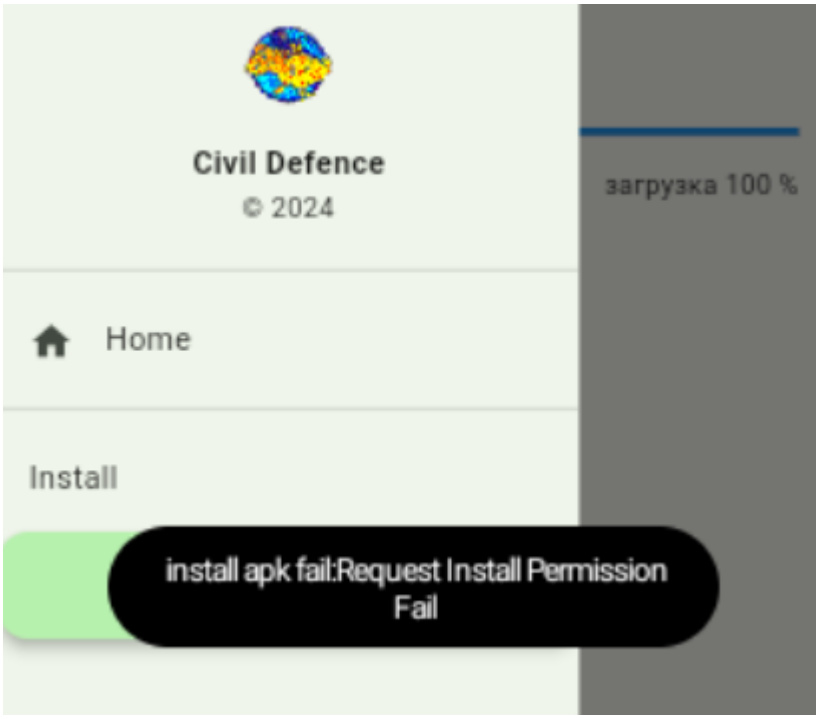

Figure 7: Error message displayed if the user doesn't grant `REQUEST_INSTALL_PACKAGES` permission

Protecting Our Users

As part of our efforts to combat serious threat actors, we use the results of our research to improve the safety and security of Google's products. Upon discovery, all identified websites, domains and files are added to Safe Browsing to protect users from further exploitation.

Google also continuously monitors for Android spyware, and we deploy and constantly update protections in Google Play Protect, which offers users protection in and outside of Google Play, checking

devices for potentially harmful apps regardless of the install source. Notably, UNC5812's Civil Defense website specifically included social engineering content and detailed video instructions on how the targeted user should turn off Google Play Protect and manually enable Android permissions required by CRAXSRAT in order to function. Safe Browsing also protects Chrome users on Android by showing them warnings before they visit dangerous sites. App scanning infrastructure protects Google Play and powers Verify Apps to additionally protect users who install apps from outside Google Play.

We have also shared our findings with Ukraine's national authorities who have taken action to disrupt the campaign's reach by blocking resolution of the actor-controlled "Civil Defense" website nationally.

Summary

UNC5812's hybrid espionage and information operation against potential Ukrainian military recruits is part of a wider spike in operational interest from Russian threat actors following changes made to Ukraine's national mobilization laws in 2024. In particular, we have seen the targeting of potential military recruits rise in prominence following the launch of Ukraine's national digital military ID used to manage the details of those liable for military service and boost recruitment. Consistent with research from EUvsDisinfo, we also continue to observe persistent efforts by pro-Russia influence actors to promote messaging undermining Ukraine's mobilization drive and sowing public distrust in the officials carrying it out.

From a tradecraft perspective, UNC5812's campaign is highly characteristic of the emphasis Russia places on achieving cognitive effect via its cyber capabilities, and highlights the prominent role that messaging apps continue to play in malware delivery and other cyber dimensions of Russia's war in Ukraine. We judge that as long as Telegram continues to be a critical source of information during the war, it is almost certain to remain a primary vector for cyber-enabled activity for a range of Russian-linked espionage and influence activity.

Indicators of Compromise

For a more comprehensive set of UNC5812 indicators of compromise, a Google Threat Intelligence Collection is available for registered users.

Indicators of Compromise	**Context**
civildefense[.]com[.]ua	UNC5812 landing page
t[.]me/civildefense_com_ua	UNC5812 Telegram channel
t[.]me/UAcivildefenseUA	UNC5812 Telegram account
e98ee33466a270edc47fdd9faf67d82e	SUNSPINNER decoy
h315225216.nichost[.]ru	Resolver used in SUNSPINNER decoy

fu-laravel.onrender[.]com	Hostname used in SUNSPINNER decoy
206.71.149[.]194	C2 used to resolve distribution URLs
185.169.107[.]44	Open directory used for malware distribution
d36d303d2954cb4309d34c613747ce58	Pronsis Loader dropper
b3cf993d918c2c61c7138b4b8a98b6bf	PURESTEALER
31cdae71f21e1fad7581b5f305a9d185	CRAXSRAT
aab597cdc5bc02f6c9d0d36ddeb7e624	CRAXSRAT w/ SUNSPINNER decoy