Overview

SentinelOne has identified new malicious activity we assess to be closely associated with the UAC-0056 (SaintBear, UNC2589, TA471) alert, in which the threat actor was observed targeting Ukraine with Cobalt Strike, GrimPlant, and GraphSteel. This previously undiscovered set of activity centers around a Python-compiled binary that masquerades as Ukrainian language translation software, leading to the infection of GrimPlant, and GraphSteel.

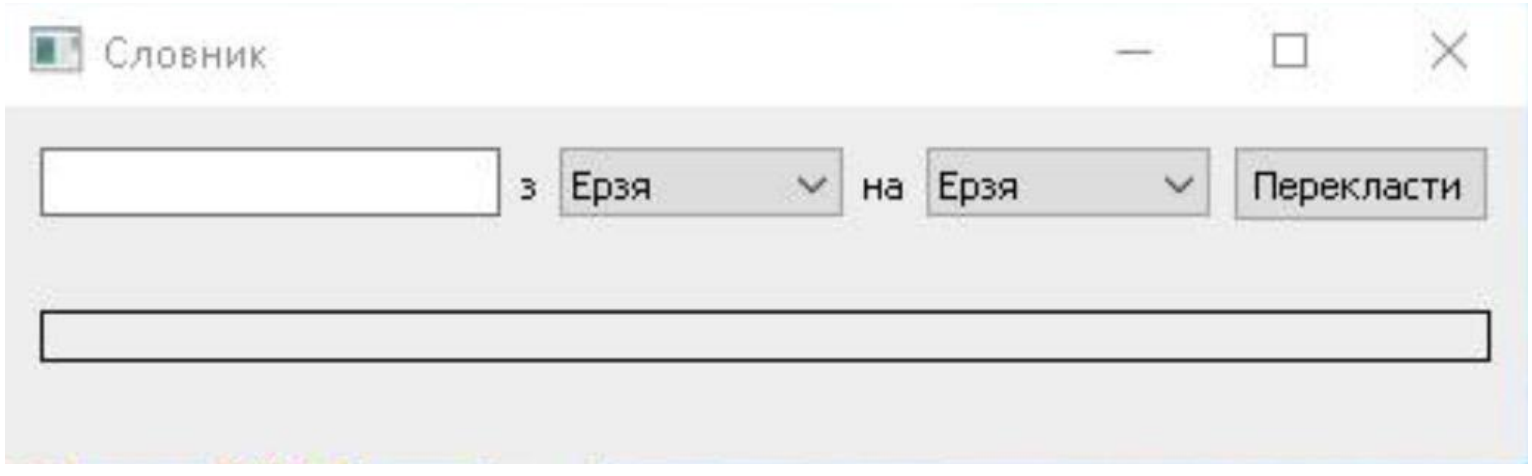
SentinelOne assesses UAC-0056's GrimPlant and GraphSteel activity began in early February 2022, while preparation for its use began at least as early as December 2021.

Dictionary Translator

SentinelOne has identified two files with names and paths correlating to the GraphSteel and GrimPlant malware referred to in the report by CERT-UA.

C:\Users\user\.java-sdk\microsoft-cortana.exe	d77421caae67f4955529f91f229b31317dff0a95
C:\Users\user\.java-sdk\oracle-java.exe	ef5400f6dbf32bae79edb16c8f73a59999e605c7

The two files identified are Go binaries dropped by the executable `2a60b4e1eb806f02031fe5f143c7e3b7` (dictionary-translator.exe). Dictionary-translator is a Python compiled binary that functions as a 45 MB translation application. Notably, this file was first uploaded to VirusTotal on February 11th 2022.



Translation Application

The Dictionary-translator binary is downloaded from the potentially actor-controlled domain: `hxxps://dictionary-translator[.]eu/program/dictionary-translator.exe`.

On launch, the translator application drops and executes four malicious files. These correlate to those described in the report by the Ukrainian CERT, three by name and path and one by functionality and path.

Matched File Path	UA-CERT Report Link (MD5)

\Users\user\AppData\Local\Temp\tmpj43i5czq.exe	15c525b74b7251cfa1f7c471975f3f95
\Users\user\.java-sdk\java-sdk.exe	c8bf23864162121290151757 0e96fae7
\Users\user\.java-sdk\microsoft-cortana.exe	9ea3aaaeb15a074cd617ee1dfdda2c26
\Users\user\.java-sdk\oracle-java.exe	4f11abdb96be36e3806bada5b8b2b8f8

Post-Compromise Activity

Upon execution, the GraphSteel variant of the malware will run a set of reconnaissance and credential harvesting commands, again similar to those described in the report.

netsh wlan show profiles [void][Windows.Security.Credentials.PasswordVault,Windows.Security.Credentials,ContentType=WindowsRuntime];$vault = New-Object Windows.Security.Credentials.PasswordVault;$vault.RetrieveAll() | % { $_.RetrievePassword();$_} | Select UserName, Resource, Password | Format-Table -HideTableHeaders reg query HKCU\Software\SimonTatham\Putty\Sessions

Additionally, the malware achieves persistence by setting the current user's registry `CurrentVersion\Run` value to execute the Go downloader at logon:

Key: HKU\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\Java-SDK Value: \Users\user\.java-sdk\java-sdk.exe -a FIAjtW4f+IgCUrs3hfj9Lg==

The variant discovered by SentinelOne attempts to connect to a different server using a similar pattern, attempting to establish a HTTP connection over port 443 to a single character letter URI: `hxxp://91.242.229.35:443/i`.

Clarification on Threat Actor UAC-0056

UAC-0056 has a history of public reporting but is most commonly known as UNC2589 (Mandiant) and TA471 (Proofpoint), among others. This actor is believed to be behind the WhisperGate activity in early January 2022 impacting government agencies in Ukraine. Based on our analysis, the actor was potentially building the infrastructure for the GrimPlant and GraphSteel campaign beginning in December 2021.

Timeline Demonstrating Known UAC-0056 Activity

Indicators of Compromise

IOC / SHA1	Description
dictionary-translator[.]eu	Dictionary-translator.exe Download Server
91.242.229[.]35:443/i	Go Downloader C2
3eec65c8ac25682d9e7d293ca9033c8a841f4958	Go Downloader
d77421caae67f4955529f91f229b31317dff0a95	GraphSteel Linked
ef5400f6dbf32bae79edb16c8f73a59999e605c7	GrimPlant Linked
3847ca79b3fd52b105c5e43b7fc080aac7c5d909	Dictionary-translator Program