Hive Pro

# THREAT ADVISORY

| Russian threat actor UAC-0056 targets European countries | TA2022064 |
|---|---|
| **Threat Level** RED | **Publish Date –** Mar 18, 2022 |

The Governmental Computer Emergency Response Team of Ukraine (CERT-UA) has released an alert about a Russian threat actor UAC-0056 (SaintBear, UNC2589, TA471) delivering malwares using email attachments. UNC2589 is a cyber espionage cluster that has been active since early 2021 and has used a constant set of tactics, techniques, and procedures (TTPs). Its primary emphasis has been on Ukraine and Georgia, although spear phishing have also been found targeting foreign ministries in Western Europe and North America, as well as pharmaceutical businesses and financial sector entities.

The first spear phishing campaign was carried out using spear phishing emails in which the actors have included links to Zip archives containing malicious shortcuts (LNK), as well as attachments in the form of PDF documents, Word documents, JavaScript files, and Control Panel File (CPL) executables. Even Word documents connected to emails have utilized a number of tactics to implant payloads into the machine, including malicious macros, embedded JavaScript, and the exploitation of CVE-2017-11882.The email had a Word document with a malicious JavaScript code attached that would download and install a payload known as SaintBot (a downloader) and OutSteel (a document stealer).

The threat actor was also seen implementing previously unknown collection of activities which revolves around a Python-compiled virus that poses as Ukrainian language translation software, which further deployes Cobalt Strike beacon , GrimPlant, and GraphSteel malware.

The Mitre TTPs used by UAC-0056 are:
TA0001 - Initial Access
TA0003 - Persistence
TA0005 - Defense Evasion
TA0002 - Execution
TA0011 - Command and Control
T1566: Phishing
T1566.001: Phishing: Spearphishing Attachment
T1105: Ingress Tool Transfer
T1112: Modify Registry
T1137.001: Office Application Startup: Office Template Macros
T1203: Exploitation for Client Execution

## Actor Details

| Name | Origin | Target Locations | Target sectors | Motive |
|---|---|---|---|---|
| UAC-0056 (SaintBear, UNC2589, TA471) | Russia | Ukraine, Georgia, North America | Financial Services, Energy, Government, Transportation, Media | Information theft |

Hive Pro

# THREAT ADVISORY

## Vulnerability Details

| CVE ID | Affected Products | Affected CPE | Vulnerability Name | CWE ID |
|---|---|---|---|---|
| CVE-2017-11882 | Microsoft Office 2007, 2010, 2013, 2016 | cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*:* | Microsoft Office Memory Corruption Vulnerability | CWE-119 |

## Indicators of Compromise (IoCs)

| Type | Value |
|---|---|
| MD5 | 12ed130045b2e731bc66c9261c88efaa,<br>22c1d43016cb2b8b9e5e5e9895526354,<br>0e3c3fe6167485807c4d36a904dfcae1,<br>259f06fcdb971f606d239b3178110981,<br>ccc3750d9270d1e8c95649d91f94033b,<br>5fa2c64ed3e9944030b6fd9f3d3d7102,<br>57a10dad336f1a6cb206dca7ddd3fcaf,<br>ab2a92e0fc5a6f63336e442f34089f16,<br>af9a60ea728985f492119ebf713e0716,<br>247165c7d96bf443b6a7360a44b7dcfb,<br>Cd8915c63f3134425aa7c851f5f1e645,<br>ca9290709843584aecbd6564fb978bd6,<br>cf204319f7397a6a31ecf76c9531a549,<br>b8b7a10dcc0dad157191620b5d4e5312,<br>2fdf9f3a25e039a41e743e19550d4040,<br>aa5e8268e741346c76ebfd1f27941a14,<br>9ad4a2dfd4cb49ef55f2acd320659b83,<br>15c525b74b7251cfa1f7c471975f3f95,<br>c8bf23864162121290151757 0e96fae7,<br>4f11abdb96be36e3806bada5b8b2b8f8,<br>9ea3aaaeb15a074cd617ee1dfdda2c26<br>1b161170a6b025b3f44746e20afd130f |
| URLs | hxxps://forkscenter[.]fr/BitdefenderWindowsUpdatePackage.exe,<br>91.242.229[.]35:443/l,<br>hxxps://forkscenter[.]fr/Sdghrt_umrj6/wisw.exe,<br>hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949948174636830761/one.exe,<br>hxxps://cdn.discordapp[.]com/attachments/947916997713358890/949978571680673802/cesdf.exe,<br>hxxps://nirsoft[.]me/s/2MYmbwpSJLZRAtXRgNTAUjJSH6SSoicLPIrQl/field-keywords/,<br>hxxps://nirsoft[.]me/nEDFzTtoCbUfp9BtSZlaq6ql8v6yYb/avp/amznussraps/,<br>hxxp://45[.]84.0.116:443/i,<br>hxxp://45[.]84.0.116:443/m,<br>hxxp://45[.]84.0.116:443/p,<br>ws://45[.]84.0.116:443/c,<br>forkscenter[.]fr,<br>nirsoft[.]me, |

| Type | Value |
| --- | --- |
| URLs | hxxps://cdn.discordapp[.]com/attachments/932413459872747544/938291977735266344/putty.exe<br>hxxps://cdn.discordapp[.]com/attachments/932413459872747544/938317934026170408/puttyjejfrwu.exe,<br>hxxp://185.244.41[.]109:8080/upld/,<br>hxxp://eumr[.]site/load74h74830.exe,<br>eumr[.]site,<br>mariaparsons10811@gmail[.]com, |
| IPs | 45 [.] 84.0.116,<br>156 [.] 146.50.5,<br>185.244.41[.]109 |
| SHA-1 | 3eec65c8ac25682d9e7d293ca9033c8a841f4958,<br>d77421caae67f4955529f91f229b31317dff0a95,<br>ef5400f6dbf32bae79edb16c8f73a59999e605c7,<br>3847ca79b3fd52b105c5e43b7fc080aac7c5d909 |

## Patch

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

## References

https://cert.gov.ua/article/18419
https://cert.gov.ua/article/37704