Vermin (UAC-0020) Hacking Collective Hits Ukrainian Government and Military with SPECTR Malware

By Andrii Bezverkhyi

Published: 2022-03-21 · Archived: 2026-04-02 11:57:42 UTC

This article covers the original investigation by CERT-UA: https://cert.gov.ua/article/37815.

On March 17, 2022, the government emergency response team of Ukraine CERT-UA revealed that the Ukrainian government infrastructure was hit by a massive spear-phishing campaign aimed at SPECTR malware delivery. The campaign was launched by Vermin (UAC-0020) hacking collective associated with the so-called Luhansk People's Republic (LPR), an unrecognized quasi-state located in the Donbas region of eastern Ukraine. Vermin cybercriminals are believed to be acting on behalf of the Moscow government and being an operational unit of the Russian cyber warfare against Ukraine.

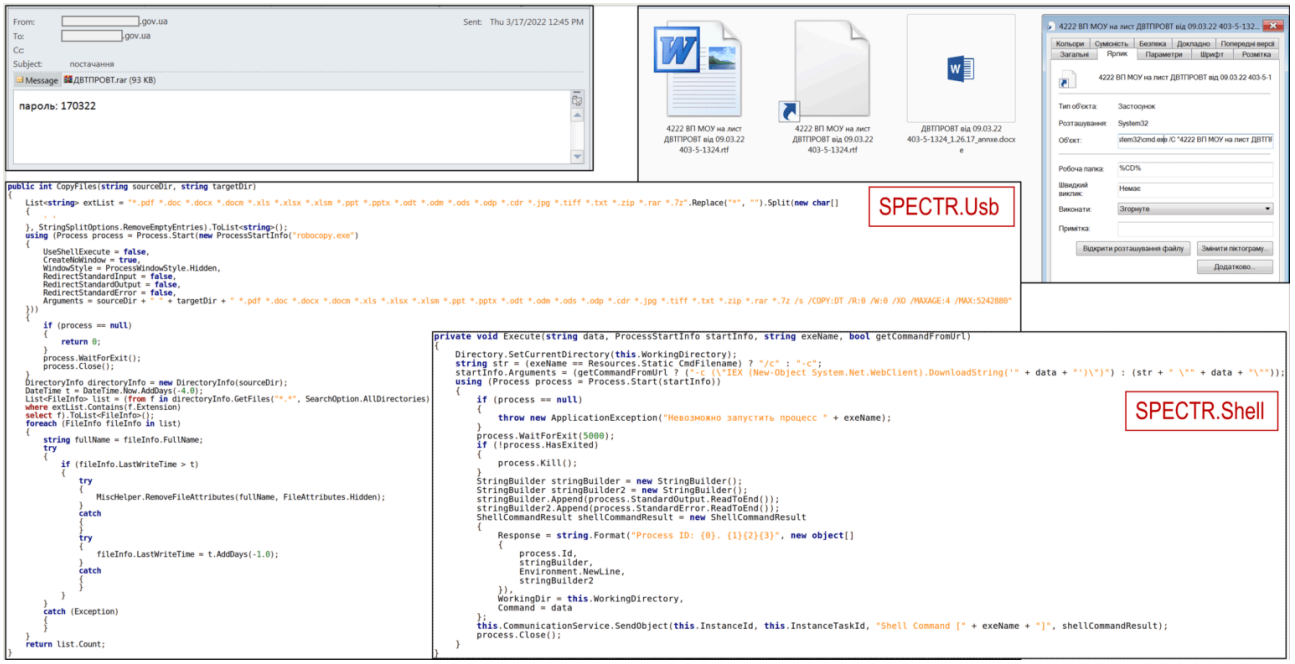
Vermin (UAC-0020): CERT-UA Research

According to the alert by CERT-UA, the LPR-affiliated Vermin collective (UAC-0020) disseminates malicious emails with the subject "supply" among the state bodies of Ukraine.

Such emails come with a password-protected RAR archive, dubbed *"ДВТПРОВТ.rar,"* which contains two malicious files. The files are *"4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-1324.rtf.lnk"* LNK-file and *"4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-1324.rtf"* EXE file. In case users open the LNK-file, the corresponding EXE-file is executed on the targeted system.

As a result of a cyber-attack, the compromised computer is exposed to harmful modular software dubbed SPECTR, which applies a set of malicious components SPECTR.Usb, SPECTR.Shell, SPECTR.Fs, SPECTR.Info, and SPECTR.Archiver to spread the infection further.

Notably, UA-CERT reports that the most recent Vermin attack leverages the same malicious infrastructure that was used by the threat group in July 2019. Moreover, the command-and-control (C&C) server equipment has been maintained by the Luhansk provider vServerCo (AS58271) for quite a long period.



Graphics provided by CERT-UA to illustrate the latest Vermin (UAC-0020) attack against Ukrainian state bodies

Global Indicators of Compromise (IOCs)

Files

baf502b4b823b6806cc91e2c1dd07613	ДВТПРОВТ.rar
993415425b61183dd3f900d9b81ac57f	4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-1324.rtf
1c2c41a5a5f89eccafea6e34183d5db9	4222 ВП МОУ на лист ДВТПРОВТ від 09.03.22 403-5-1324.rtf.lnk
d34dbbd28775b2c3a0b55d86d418f293	data.out
67274bdd5c9537affbd51567f4ba8d5f	license.dat (2022-02-25) (SPECTR.Installer)
75e1ce42e0892ed04a43e3b68afdbc07	conhost.exe
e08d7c4daa45beca5079870251e50236	PluginExec.exe (SPECTR.PluginLoader)
adebdc32ef35209fb142d44050928083	Spectator2.exe (SPECTR.Spectator2)
3ed8263abe009c19c4af8706d52060f8	Archiver.dll (2021-04-09) (SPECTR.Archiver)
f0197bbb56465b5e2f1f17876c0da5ba	ClientInfo.dll (SPECTR.Info)
d0632ef34514bbb0f675c59e6ecca717	FileSystem.dll (2021-04-09) (SPECTR.Fs)
00a54a6496734d87dab6685aa90588f8	FileTransfer.dll (2021-04-09) (SPECTR.Ft)
5db4313b8dbb9204f8f98f2c129fd734	Manager.dll (SPECTR.Mgr)
32343f2a6b8ac9b6587e2e07989362ab	Shell.dll (2021-04-09) (SPECTR.Shell)
ecc7bb2e4672b958bd82fe9ec9cfab14	Usb.dll (SPECTR.Usb)

Network Indicators

```
hxxp://176[.]119.2.212/web/t/data.out
hxxp://getmod[.]host/DSGb3Y3X
hxxp://getmod[.]host/ThlAHy3S
hxxp://getmod[.]host/OcthdaLm
```

```
getmod[.]host (2019-07-12)
syncapp[.]host (2019-07-12)
netbin[.]host (2019-07-12)
stormpredictor[.]host
meteolink[.]host
176[.]119.2.212
176[.]119.2.214
176[.]119.5.194
176[.]119.5.195
AS58271
```

Host Indicators

```
HKCU\Software\Google\Chrome\NativeMessagingHosts\com.microsoft.browsersec\EncodedProfile
HKCU\Software\Google\Chrome\NativeMessagingHosts\com.microsoft.browsercli\EncodedProfile
%APPDATA%\Microsoft\ExcelCnv\1033\license.dat
%APPDATA%\Microsoft\ExcelCnv\1033\conhost.exe
ESET_OPINIONS (network variable)
MSO (network variable)
MS Office Add-In Install Task (sheduled task)
```

To get actionable threat intelligence based on IOCs above, please refer to this Anomali ThreatStream link: https://ui.threatstream.com/tip/3754010.

Sigma Rules to Detect the Latest Vermin (UAC-0020) Attack Against Ukraine

To protect your organization's infrastructure against massive spear-phishing attacks and SPECTR malware infections linked to the malicious activity of Vermin (UAC-0020) threat actors, SOC Prime has released dedicated Sigma-based rules available in our Detection as Code platform. All detection content associated with the activity of these threat actors is tagged accordingly with *#UAC-0020*:

Full list of Sigma-based rules to detect the latest Vermin group's activity

SOC Prime platform offers a batch of IOC-based Sigma rules to detect the Vermin attack available for registry event, file event, image load, and other log sources. Also, the list of detections includes a set of Sigma behavior-based rules to boost your threat hunting capabilities and gain more insights into adversary behavior patterns.

MITRE ATT&CK® Context

To gain more insights into the context surrounding the latest spear-phishing campaign launched by Vermin hacking collective, all above mentioned Sigma-based detections are aligned with the MITRE ATT&CK framework addressing the following tactics and techniques:

Download JSON file for ATT&CK Navigator

The versions applicable for the file above are as follows:

- MITRE ATT&CK v10
- ATT&CK Navigator version: 4.5.5
- Layer File Format: 4.3
