The Russian Shadow in Eastern Europe: A Month Later

Introduction

The Gamaredon attacks against Ukraine doesn't seem to have stopped. After a month since our last report we spotted a new suspicious email potentially linked to the Gamaredon group. The group was first discovered by Symantec and TrendMicro in 2015 but evidence of its activities has been dated back to 2013. During recent times, Gamaredon is targeting the Ukrainian military and law enforcement sectors too, as officially stated by the CERT-UA.

Cybaze-Yoroi ZLAB team dissected the artifact recovered from their latest attack to figure out evolution or changes in the threat actor TTPs.

Technical Analysis

The infection chain is composed by different stages of password protected SFX (self extracting archive), each containing vbs or batch scripts.

At the final stage of this malicious chain, we found a customized version of UltraVNC, a well known off-the-shelf tool for remote administration, modified by the Group and configured to connect to their command and control infrastructure. Despite its apparent triviality, the Matryoshka of SFX archives reached a low detection rate, making it effective.

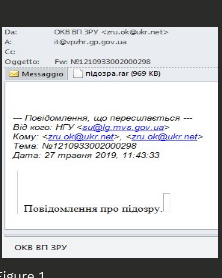
Figure 1. Malicious e-mail

Stage 1

Hash	5555a3292bc6b6e7cb61bc8748b21c475b560635d8b0cc9686b319736c1d828e
Threat	Gamaredon Pteranodon implant
Brief Description	SFX file
Ssdeep	24576:PXwOrRsTyuURQFsVhIe74lpyevrM4vZxn6k1gQ Guo:PgwRAyuURQ2/1YpyeT7ok8

Table 1. Information about initial SFX file

The mail attachment is a RAR archive containing a folder named "*suspected*" in Ukrainan and a single suspicious file with ".scr" extension. At first glance, it is possible to notice the PowerPoint icon associated to the file, normally not belonging to .scr files.

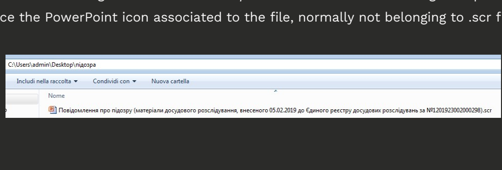
Figure 2. Content of malicious e-mail


Figure 3. Low AV detection of SFX malware

The file has a very low detection rate on VirusTotal platform: only four AV engines are able to identify it as malicious and only on engine understands it may be associated to the Gamaredon implant.

After a quick analysis, the real nature of the .scr file emerges: it is a Self Extracting Archive containing all the files in Figure 4.

They are extracted into *%TEMP%\7ZipSfx.000* and the first command to be executed is *15003.cmd* , which firstly checks for the presence of malware analysis tools. If it detects the presence of Wireshark or Procexp tools, it kill itself. Otherwise, it copies:

- the "11439" file in *%USERNAME%\winupd.exe*
- the "28509" file in "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\winupd.lnk" pointing to the previous executable and granting persistence to machine reboot
- the "20261" file in "%TEMP%\7ZipSfx.000\Document.docx"

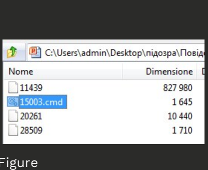
Figure 4. Content of SFX

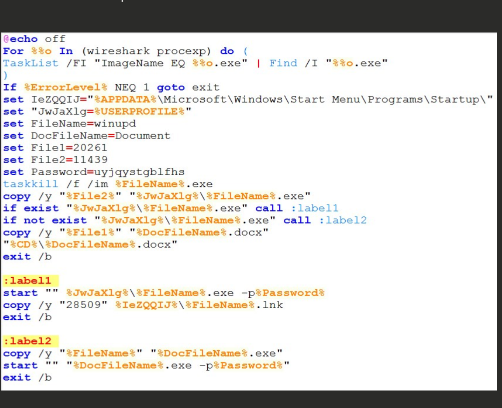

Figure 5. Script content in "*15003.cmd*" file

At the same time, the extracted document will be shown in order to divert the user attention and to continue the infection unnoticed. This document, written in Ukraine language, contains information about a criminal charge.

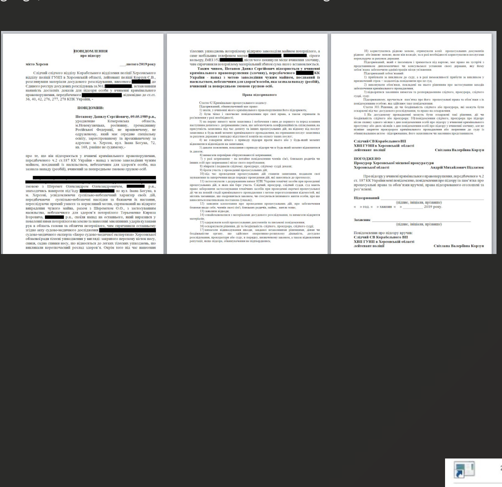
Figure 6. Fake document to divert attention on malware execution

Instead, exploring the LNK file is possible to see it's able to start the "*winupd.exe*" file, with a particular parameter: %USERPROFILE%\winupd.exe -puyjqystgblfhs. This behavior indicates the "winupd.exe" executable is another Self Extracting Archive, but this time it is password protected.

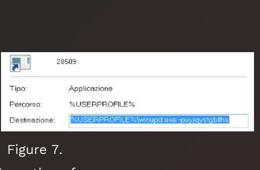
Figure 7. Execution of "*winupd.exe*" (SFX) and relative password (uyjqystgblfhs)

Stage 2

Hash	fd59b1a991df0a9abf75470aad6e2fcd67c070bfccde9b4304301bc4992f678e
Threat	Gamaredon Pteranodon implant
Brief Description	SFX file
Ssdeep	24576:bGKUQ8Lj7S6Jr1ye4SM4vzxn3k1jQ GujR:biJr1yeNxJkro

Table 2. Information about second SFX file

When launched, it extracts its content in "%TEMP%\RarSFX0\", then executes the "setup.vbs" script, which contains only two code lines. So, the execution flow moves on "1106.cmd".

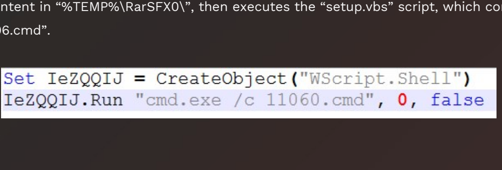

Figure 8. Content of "*setup.vbs*" script

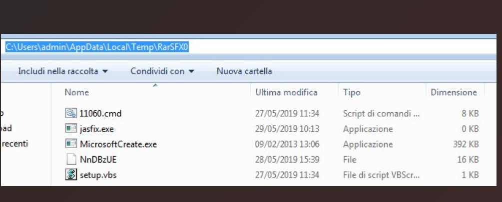
Figure 9. Content of "%APPDATA%\Local\Temp\RarSFX0" after "*winupd.exe*" (SFX) extraction

The source code of "1106.cmd" is full of junk instructions. However, in the end it performs a simple action: it writes a new VBS script in *%APPDATA%\Microsoft\SystemCertificates\My\Certificates* . This script tries to download another malicious file from "*http://bitvers.ddns[.net/{USERNAME}/{DATE}/index.html*". Performing many researches abot this server we noticed the continuously modification of associated records. Indeed, the attacker has changed many time the domain names in the latest period. Moreover, querying the services behind the latest associated DNS record the host responds with "403 Forbidden" message too, indicating the infrastructure may still be operative.

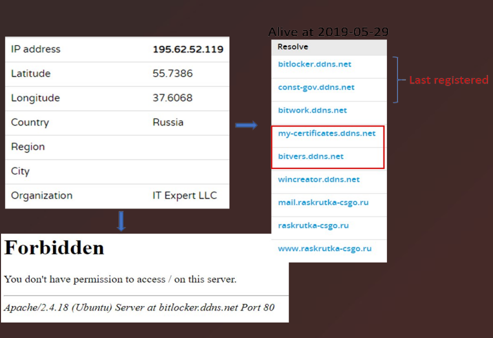

Figure 10. Information about C2 and relative DNS

The scripts creates a new scheduled task in order to periodically execute (every 20 mins) the previous VBS script.

Also, it collects all the information about the victim's system using the legit *systeminfo* Microsoft tool and sends them to the remote server through a POST request using the "MicrosoftCreate.exe" file, which actually is the legit "wget" utility. The response body will contain a new executable file, named "jasfix.exe", representing the new stage.


Figure 11. POST request sent to C2 with victim machine information

Stage 3

Hash	c479d82a010884a8fde0d9dcfdf92ba9b5f4125fac1d26a2e36549d8b6b4d205
Threat	Gamaredon Pteranodon implant
Brief Description	SFX file
Ssdeep	24576:Gfxwgmyg5EOJ+IlpBz2GAROm560XVEC1Ng MdfaQbhUfElg+m:GJpgldPzeRBJVEC1CMd

Table 3. Information about third SFX file

After few researches, we were able to retrieve the "jasfix.exe" file, the next stage of the infection chain. After downloading it, we notice that it is another SFX archive other files.

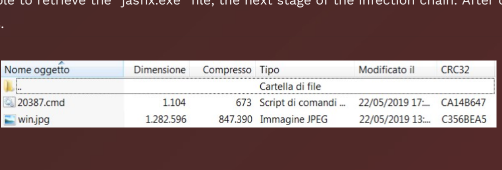
Figure 12. Content of "*jasfix.exe*" (SFX) downloaded from the C2

The first file to be executed is "20387.cmd" that renames the *win.jpg* into *win.exe* , another password protected SFX.

Stage 4

Hash	28eff088a729874a611ca4781a45b070b46302e494bc0dd53cbaf598da9a6773
Threat	Gamaredon Pteranodon implant
Brief Description	SFX file
Ssdeep	24576:9GKUQ8vCTAaaJVssTk3OwO+vl+3yt6Xf IAR:9vaJes2Ocl7t9S

Table 4. Information about fourth SFX file

This latest SFX archive follows the typical pattern of the Gamaredon archives Matryoshka, where the "*.cmd*" file is in designed to decrypt and run next stage. This time using the string "*gblfhs*" as password.

Figure 13. Script to rename "win.jpg" into "win.exe", decrypt and run next stage

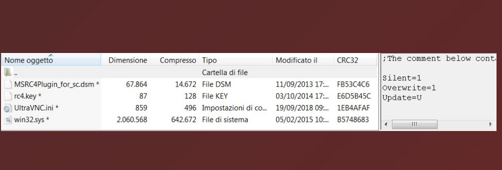
Figure 14. Content of "win.exe" (last SFX of infection)

However, the file named "*win32.sys*" is particularly interesting: it actually is a PE32 executable file. Exploring the "*.rsrc*" section of the PE32 executable, we noticed different "*.class*" files. Two of them are named "*VncCanvas*" and "*VncViewer*". These files are part of a legit Remote Administration Tool (RAT) named UltraVNC, available at this link.

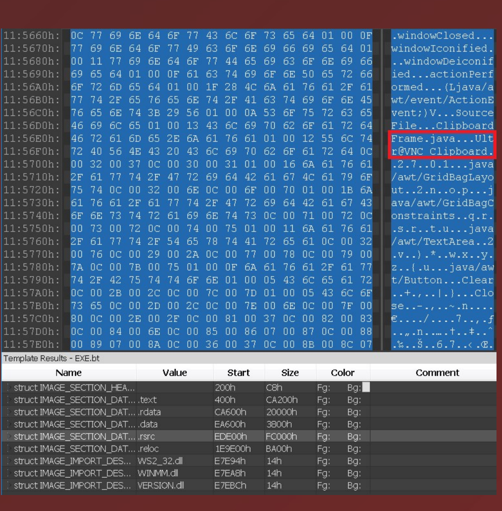
Figure 15. Content of "win32.sys"

The "*win.exe*" SFX archive contains other interesting files too: one of them is an "*.ini*" configuration file containing all the parameters and the password used by the UltraVNC tool.

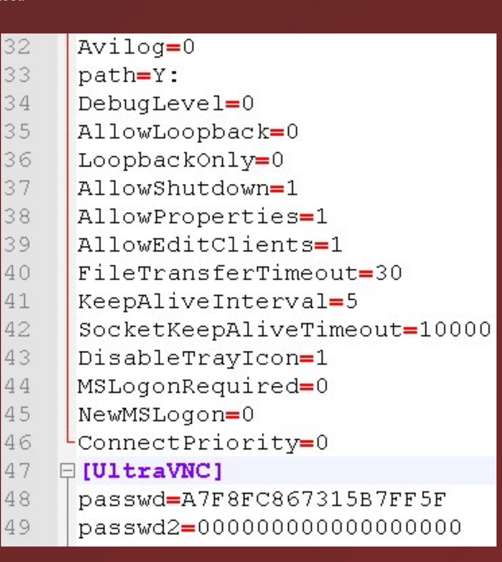

Figure 16. Configuration file used by "win32.sys" (Custom ultraVNC)

Finally, the RAT tries to establish a connection to the "*torrent-vnc[.ddns[.net*" domain, headed to an endpoint reachable on 195.88.208.51, a VPS hosted by the Russian provider IPServer.


Figure 17. C2 and relative port used by RAT

Conclusion

This recent attack campaign shows the Gamaredon operation are still ongoing and confirms the potential Russian interest about infiltrating the East European ecosystem, especially the Ukranian one. The techniques and the infection patterns the Group is using is extremely similar to the other attacks spotted in the past months of 2019, showing the Matryoshka structure to chain SFX archives, typical of their implant, but still effective and not easily detectable by several antivirus engines.

Also, digging into this infection chain, we noticed the come back of third party RATs as payload, a Gamaredon old habit that the usage of the custom-made Pterodo backdoor replaced few times ago.

Indicators of Compromise

Hashes

- 601d85c0236f8d3a82fecf353adb106fac23f1681ef866783ff6e634538c9ce0
- 566f495f334cbf4bf019d9ad58636ad0839eadce8d9e5e3fd78deececbcb6fdc
- 5555a3292bc6b6e7cb61bc8748b21c475b560635d8b0cc9686b319736c1d828e
- 3ed4ba91886309f8c25a9d2c052effab37193ffbb1dbbf29cbd1e9b7e9691514
- fd59b1a991df0a9abf75470aad6e2fcd67c070bfccde9b4304301bc4992f678e
- f53bb852e0721e623f55a63e325db1c13c4eddad2a8d6743f358430dfcbe9c23
- b511e05100b3a4f3515c5526d2dc3c873f66384225c174c65931744d9e682dc0
- 45a4db08585ae8148fc1f23644b04e431e2b945f285797e235002f2a41c04462
- ddd5b5ca4c0816d9983cb200a55a345a5dbe005e38642d088f05bb137174828a
- a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf599 (WGET)
- 774925ca3134dabfa57c548c11080fc383c9ed89af8cdc11e6caab5a25fc9564
- c479d82a010884a8fde0d9dcfdf92ba9b5f4125fac1d26a2e36549d8b6b4d205
- 57b094d0ad345a2654843bed9fdcd2af3f1d9f5d567919f5cb78d9e547093f23
- 28eff088a729874a611ca4781a45b070b46302e494bc0dd53cbaf598da9a6773
- d8a01f69840c07ace6ae33e2f76e832c22d4513c07e252b6730b6de51c2e4385
- 99c9440a84cdc428ce140de901452eb334faec49f1f6258acdde1ddcbb34376e
- ef0f0e80e5e1fae63b946f87d571fac8646e6ba90995536c08cd20d2e40da18e
- cedbbbc4deb6569c23aa20ac64ad1c2b2bef6f7b3405cef861f26a0b44d836d9

URL

- my-certificates[.ddns[.net
- bitvers[.ddns[.net
- torrent-vnc[.ddns[.net:5612

Components

- %TEMP%\RarSFX0\11060.cmd
- %TEMP%\RarSFX0\jasfix.exe
- %TEMP%\RarSFX0\MicrosoftCreate.exe
- %TEMP%\RarSFX0\NnDBzUE
- %TEMP%\RarSFX0\setup.vbs
- %TEMP%\7ZipSfx.000\11439
- %TEMP%\7ZipSfx.000\15003.cmd
- %TEMP%\7ZipSfx.000\20261
- %TEMP%\7ZipSfx.000\28509
- %TEMP%\7ZipSfx.000\Document.docx
- %USERNAME%\winupd.exe
- %APPDATA%\Microsoft\SystemCertificates\My\Certificates\{filename}.vbs
- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\winupd.lnk
- %TEMP%\RarSFX0\win\32.sys

IP

- 195.62.52.119

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
}

import "pe"
rule GamaredonPteranodon_SFX_intermediate_stage{
meta:
 description = "Yara Rule for Pteranodon implant Family Intermediate Stage"
 author = "Cybaze - Yoroi ZLab"
 last_updated = "2019-05-31"
 tlp = "white"
 category = "informational"
strings:
 $a1 = {56 8B F1 8D 46 04 50 FF}
 $a2 = {14 7A 19 5D 01 EB 18 02 85}
 $a3 = {0D 4D 38 B1 2D EE 1E 2B}
    $b1 = {34 9B 43 00 50 FF 15 30}
     $b2 = {AB B9 89 97 2F DD 7D 82}
     $b3 = {9D CA C6 91 EF}
     $c1 = {24 0C FF 15 34 9B 43 00}
     $c2 = {32 31 32 F0 32 2E 39}
     $c3 = {45 3B 4B 21 A7}

condition:
 pe.number_of_sections == 4 and all of ($a*) or
     pe.number_of_sections == 6 and all of ($b*) or
     pe.number_of_sections == 6 and all of ($c*)
}
```

Acknowledgement: special thanks to @JAMESWT_MHT for info and samples.