The Uroburos case: new sophisticated RAT identified

In February 2014, the experts of the G DATA SecurityLabs published an analysis of Uroburos, the rootkit with Russian roots. We explained that a link exists between Uroburos and the Agent.BTZ malware, which was responsible for "the most significant breach of U.S. military computers ever." [1] Nine months later, after the buzz around Uroburos, aka Snake or Turla, we now identified a new generation of Agent.BTZ We dubbed it ComRAT and, by now, analyzed two versions of the threat (v3.25 and v3.26).

As reported earlier this year, Agent.BTZ used the same encoding key and the installation log file name as Uroburos. ComRAT, in its version 3.25, shows the same behavior. Furthermore, the attackers also shared a C&C domain. The latest version of ComRAT known to us (v3.26) uses a new key and does not create the installation log file, in order to complicate the analysis and to disguise the link between the two cases.

Another very interesting fact: the attackers use COM Object hijacking, the same persistence mechanism as COMpfun, which we described recently.

Taken everything into consideration, the indications we saw during our analyzes lead to the supposition that the group behind Agent.BTZ and Uroburos is still active and is pursuing the Agent.BTZ path once more to improve and change the RAT.

Dropper

The analyzed file is the latest version we identified: v3.26. The version identification is described in the chapter “Log files”. The major difference between this version and the older version(s) will be described there.

File installation

The first task of the malware is to install the file credprov.tlb in %APPDATA%\Microsoft\. This file is the main payload of the malware. The dropper executes the following command in order to install a second file:

rundll32.exe %APPDATA%\Microsoft\credprov.tlb,Install %APPDATA%\Microsoft\shdocvw.tlp

The second file is shdocw.tlp. The two files are Microsoft Windows dynamic libraries.

Persistence

To be started during the boot process of the infected machine, the malware creates the following registry key:

HKCU\Software\Classes\CLSID\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InprocServer32 = %APPDATA%\shdocvw.tlp

This registry key is used to associate the library shdocvw.tlp to the object 42aedc87-2188-41fd-b9a3-0c966feabec1 as previously explained in the article about COMpfun. The purpose is to load the library into each and every process executed on the infected system.

Dropper's log file

If the version of the malware is older than 3.26, the dropper creates an additional file called winview.ocx. We noticed that the file name is still the same as the file name used by Agent.BTZ in the past. The file is xored with the following obfuscation key (used by both, Uroburos and Agent.BTZ):
1dM3uu4j7Fw4sjnbcwlDqet4F7JyuUi4m5Imnxl1pzxI6as80cbLnmz54cs5Ldn4ri3do5L6gs923HL34x2f5cvd0fk6c1a0s

Here is the decoded log file content:

```
user1@gdata$ ./decode.py winview.ocx
Log begin: 06.11.2014 22:55:55
TVer=2.2
06.11.2014 22:55:55 TVer=2.3
06.11.2014 22:55:55 CFG: CFG_4
06.11.2014 22:55:55 User: user1
06.11.2014 22:55:55 Machine: x86
06.11.2014 22:55:55 Removing C:\Documents and Settings\user1\Application Data\\Microsoft\\shdocvw.tlb [2]
06.11.2014 22:55:55 Removing C:\Documents and Settings\user1\Application Data\\Microsoft\\oleaut32.dll [2]
06.11.2014 22:55:55 Removing C:\Documents and Settings\user1\Application Data\\Microsoft\\oleaut32.tlb [2]
06.11.2014 22:55:55 Removing C:\Documents and Settings\user1\Application Data\\Microsoft\\credprov.tlb [2]
06.11.2014 22:55:55 Removing C:\Documents and Settings\user1\Application Data\\Microsoft\\libadcodec.dll [2]
06.11.2014 22:55:55 Removing C:\Documents and Settings\user1\Application Data\\Microsoft\\libadcodec.tlb [2]
06.11.2014 22:55:55 Writing C:\Documents and Settings\user1\Application Data\\Microsoft\\shdocvw.tlb 51200B
Ok
06.11.2014 22:55:56 Writing C:\Documents and Settings\user1\Application Data\\Microsoft\\credprov.tlb
260096B Ok
06.11.2014 22:55:57 Exit code1 0
06.11.2014 22:55:57 Writing 3072B Ok
```

We can notice that the malware checks if an older version is installed on the system and if this is the case, the dropper removes the older version. In contrast to this, in our Uroburos analysis, we found out that Uroburos does not install itself in case a version of Agent.BTZ was found on a system.

Execution flow and features

During the startup of the infected machine, the shdocvw.tlp library is loaded into all processes. If the process is explorer.exe, this library will load the other library called credprov.tlb. This library is the real payload. Its features are common for a Remote Administration Tool (RAT):

- command execution;
- file download;
- file upload;
- information gathering.

ComRAT's communication to the command and control server is performed by the browser process and not by explorer.exe in order to avoid being blocked by a firewall on the system or any additional security products. The communication between the processes is performed by named pipe.

Log files

Two log files are created during the malware execution: mskfp32.ocx and msvcrtd.tlb. If the malware version is older than 3.26, the xored key is the same as the dropper key. Concerning the version 3.26, the malware uses a new non-ASCII key. Here is an example of decoded log file for the version 3.26:

```
user1@gdata$ ./decode.py mskfp32.ocx
<?xml version="1.0" encoding="unicode"?>
<Ch>
<TVer>2.1</TVer>
<AppendLog>0</AppendLog>
<add key="Id" value="168466483094462" />
<add key="PVer" value="3.26" />
<add key="OSVer" value="512600 Service Pack 30" />
<add key="Machine" value="x86" />
<add key="CryptKeyType" value="3" />
<add key="CryptKeyId" value="0" />
<add ke="IsAdmin" value="1" />
<add key="Http idx1" value="4294967295" />
<add key="Http idx2" value="4294967295" />
<add key="Http timeout" value="60" />
<add key="Time" value="06:11:2014 15:54:34" />
<add key="Bias" value="-2" />
<add key="PcName" value="USER1-ABC1234" />
<add key="UserName" value="user1" />
<add key="WinDir" value="C:\\WINDOWS" />
<add key="TempDir" value="C:\\DOCUME~1\\user1\\LOCALE~1\\Temp\\" />
<add key="WorkDir" value="C:\\ Documents and Settings\user1\Application Data\\Microsoft\\" />'
</Ch>
```

We can identify the version of the malware thanks to the PVer flag. The command and control server information is stored in the registry, not in an XML, and encoded:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionMRU\IPlace

For example, in the analyzed sample the CC is: weather-online.hopto.org. This domain is far from unknown, as it has been mentioned in BAE System's Uroburos (aka Snake) analysis paper as C&C server domain for the Uroburos malware. Another connection between the cases.
If the malware version in lower than 3.26, the XML log file contains the command and control server information:

[...]
<add ke="IsAdmin" value="1" />
<add key="Http address" value="webonline.mefound.com" />
<add key="Http address" value="sportacademy.my03.com" />
<add key="Http address2" value="easport-news.publicvm.com" />
<add key="Http address2" value="new-book.linkpc.net" />
<add key="Http idx1" value="4294967295" />
[...]

Summary

Let us summarize the similarities and differences between Agent.BTZ, Uroburos and ComRAT as far as we can:
Similarities:
Before version 3.26:

- use of the same xor key
- use of the same file name for the log

On all versions:

- Some parts of the code are exactly the same (appears to be copy & paste)
  That is the reason why the sample is detected as Uroburos (aka Turla). The same code was used by Agent.BTZ and also the dll loaded into userland during the Uroburos analysis.
- Command and control server domains are shared between Uroburos and ComRAT.

Differences:

- In version 3.26, the author changed the key and remove the known file name
  This action can be an indication for the developer's effort to hide this connection
- The main difference is the design
  Agent.BTZ is a common RAT, a simple library executed on an infected machine. ComRAT is more complex and cleverer. The malware is loaded into each and every process of the infected machine and the main part (payload) of the malware is only executed in explorer.exe. Furthermore, the C&C communication blends into the usual browser traffic and the malware communicates to the browser by named pipe. It is by far a more complex userland design than Agent.BTZ.

These differences, mainly the more complex design, lead us to give this malware a new name.

The analyzed dropper of v3.25 has a compilation date of February 6th 2014. The more recent dropper of v3.26, which has all the mentioned changes implemented, reveals a compilation date of January 3rd 2013. We suspect that this date is spoofed in order to disguise that this is in fact a newer version.

Conclusion

This analysis shows that even after the Uroburos publication in February 2014, the group behind this piece of malware seems to be still active. In any case, the ComRAT developers implemented new mechanisms, changed keys, removed log files to hide their activities and tried to disguise the connections between the RAT ComRAT, the rootkit Uroburos and the RAT Agent.BTZ as much as possible. However, we can still follow the evolution of the malware by comparing the versions.

The persistence mechanism discovered in October 2014 makes it possible to intrude into a system in a really discreet manner and we estimate that other actors will use the same persistence mechanism in the near future.

We will definitely keep our ears and eyes open and continue analyzing.

IOC

MD5

51e7e58a1e654b6e586fe36e10c67a73 (dropper v3.25)
e6ce1f962a47479a86ff2e67129f4ecc (lib1, v3.25)
ec7e3cfaeaac0401316d66e964be684e (lib2, v3.25)
0ae421691579ff6b27f65f49e79e88f6 (dropper v3.26)
255118ac14a9e66124f7110acd16f2cd (lib1 v3.26)
b407b6e5b4046da226d6e189a67f62ca (lib2, v3.26)
8ebf7f768d7214f99905c99b6f8242dc (dropper, unknown version)
9d481769de63789d571805009cbf709a (dropper, unknown version)
83a48760e92bf30961b4a943d3095b0a (lib 64-Bit, unknown version)
ea23d67e41d1f0a7f7e7a8b59e7cb60f (lib 64-Bit; unknown version)

Paths

%APPDATA%\\Microsoft\\shdocvw.tlb
%APPDATA%\\Microsoft\\oleaut32.dll
%APPDATA%\\Microsoft\\oleaut32.tlb
%APPDATA%\\Microsoft\\credprov.tlb
%APPDATA%\\Microsoft\\libadcodec.dll
%APPDATA%\\Microsoft\\libadcodec.tlb

Registry

HKCU\Software\Classes\CLSID\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InprocServer32

Command and control

weather-online.hopto.org

webonline.mefound.com
sportacademy.my03.com
easport-news.publicvm.com
new-book.linkpc.net

Related articles:

October 30th 2014: COM Object hijacking: the discreet way of persistence
June 2nd 2014: Analysis of Uroburos, using WinDbg
May 13th 2014: Uroburos rootkit: Belgian Foreign Ministry stricken
March 3rd 2014: Uroburos - Deeper travel into kernel protection mitigation
February 28th 2014: Uroburos - highly complex espionage software with Russian roots

---

[1] www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain