Evolution of sophisticated spyware: from Agent.BTZ to ComRAT

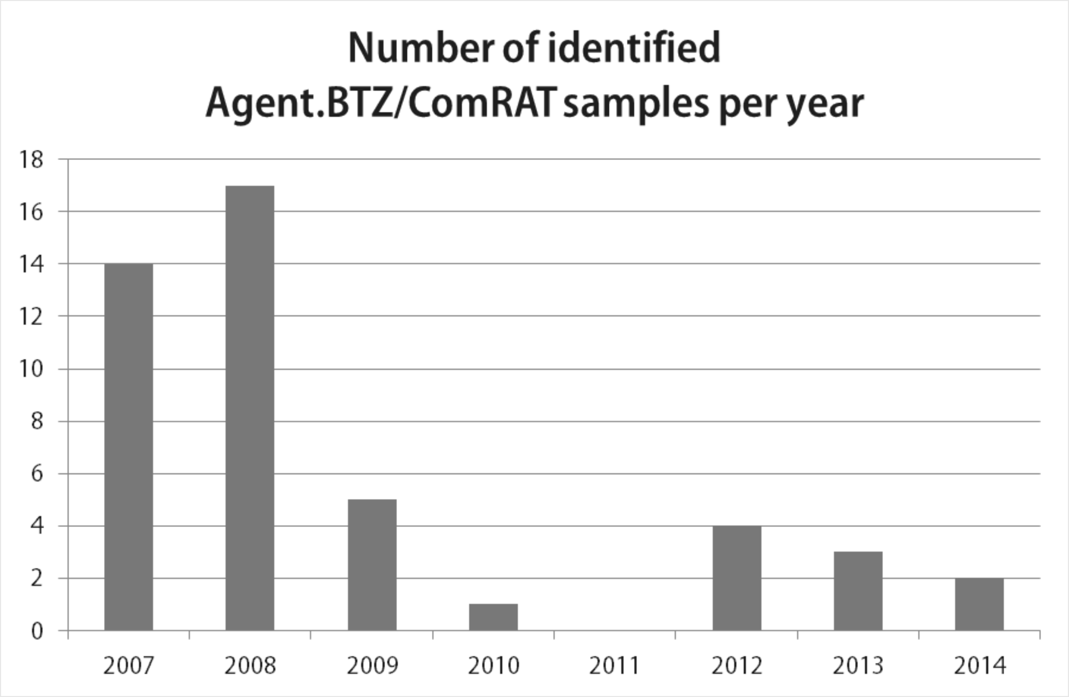
In November 2014, the experts of the G DATA SecurityLabs published an article about ComRAT, the Agent.BTZ successor. We explained that this case is linked to the Uroburos rootkit. We assume that the actor behind these campaigns uses several different malware strains is order to compromise the targeted infrastructure: Uroburos, a rootkit; Agent.BTZ/ComRAT, remote administration tools or Linux malware and maybe even more.

We decided to have an even closer look at Agent.BTZ and ComRAT and therefore analyzed the evolution of this RAT, covering seven years of development. Here is a table with the minimal information about 46 different samples:

MD5	Version	Compilation Date
b41fbdd02e4d54b4bc28eda99a8c1502	Ch 1.0	Wed Jun 13 07:31:32 2007 UTC
93827a6c77e84ffdd9c793d485d3df6e	Ch 1.0	Wed Jun 13 07:31:32 2007 UTC
3e9c7ef54ea3d55d5b53abab4c3e2385	Ch 1.0	Wed Jun 13 07:31:32 2007 UTC
b9ed8876ef5a05ba364a9cdbdf4f184d	Ch 1.0	Tue Jun 19 12:41:21 2007 UTC
d8f98f64687b05a62c81ce9e52dd808d	Ch 1.1	Tue Jun 26 08:46:11 2007 UTC
2cf64ff9dad8d64ee9322e390d4f7283	Ch 1.1	Tue Jun 26 08:46:11 2007 UTC
24e679155697bd31b34036a44d4346a7	Ch 1.2wcc	Tue Jul 24 12:57:37 2007 UTC
53b8b9f779b1d1d298884d1c21313ab3	Ch 1.2wcc	Tue Jul 24 12:57:37 2007 UTC
69ae46fedf3c18ff36fc850e0baa9365	Ch 1.2wcc	Tue Jul 24 12:57:37 2007 UTC
e05511a84eb345954b94f1e05c78bf22	Ch 1.2	Thu Jul 26 07:20:17 2007 UTC
f93ce76f6580d68a95260198b2d6feaa	Ch 1.3	Mon Dec 3 14:15:58 2007 UTC
db5d1583704b0fb6d1cff0b62a512a7d	Ch 1.4	Tue Dec 11 17:36:03 2007 UTC
2b348c225985679f62e50b28bdb74ac9	Ch 1.4	Tue Dec 11 17:36:03 2007 UTC
af3f0efbd69905123f7df958cc88dff9	Ch 1.4	Tue Dec 11 17:36:03 2007 UTC
e825c4961293ad45883cd52f38695283	Ch 1.5	Thu Mar 27 14:58:15 2008 UTC
2a67b53b7ef7b70763658ca7f60e7005	Ch 1.5	Thu Mar 27 14:58:15 2008 UTC
bbf569176ec7ec611d8a000b50cdb754	Ch 1.5	Thu Mar 27 14:58:15 2008 UTC
e5c76e67128e48cb0f003c2beee47d1f	Ch 1.5	Thu Mar 27 14:58:15 2008 UTC
8e5da63369d20e1d2c530bf806996285	Ch 2.02	Mon May 5 11:27:48 2008 UTC
78d3f074b70788897ae7e20e5137bf47	Ch 2.03	Mon May 12 11:52:31 2008 UTC
986f263ca2c529d5d28bce3c62f858ea	Ch 2.03	Thu May 22 10:24:55 2008 UTC
4f732099caf5d21729572cec229f7614	Ch 2.04	Mon Jun 9 17:23:56 2008 UTC
5336c24a3399f522f8e19d9c54a069c6	Ch 2.04	Mon Jun 9 17:23:56 2008 UTC
dc1c54751f94b6fdf0b6ecdd64e67701	Ch 2.04	Mon Jun 9 17:23:56 2008 UTC
40335fca60acd05f1428b13a9a3c1228	Ch 2.04	Mon Jun 9 17:23:56 2008 UTC
72663ee9d3efaff959bff4ce25bd37a6	Ch 2.04	Mon Jun 9 17:23:56 2008 UTC

5ef72904221aa4090a262a24714054f0	Ch 2.04	Mon Jun 9 17:23:56 2008 UTC
331eca9c7d9fd9cbe7cd192af09880a3	Ch 2.05	Thu Nov 6 13:21:45 2008 UTC
db1156b072d58acdac1aeab9af2160a2	Ch 2.05	Thu Nov 6 13:21:45 2008 UTC
74dbea70bfb15db31bb9f757ed4bb1a0	Ch 2.07	Mon Dec 29 11:37:17 2008 UTC
eb928bca5675722c7e9e2b09eec1158a	Ch 2.07	Mon Dec 29 11:37:17 2008 UTC
162f415abad9708aa61db8e03bcf2f3c	Ch 2.11	Mon Sep 14 13:22:57 2009 UTC
448524fd62dec1151c75b55b86587784	Ch 2.11	Mon Sep 14 15:28:07 2009 UTC
29bb70a40689e9e665d15716519bacfd	Ch 2.12	Tue Sep 29 10:28:40 2009 UTC
38d6719d6a266c6cefb8626c57378927	Ch 2.13	Mon Dec 7 14:25:12 2009 UTC
02eda1effde92bdf8462abcf40c4f776	Ch 2.13	Mon Dec 7 14:27:53 2009 UTC
5121ce1f96d74076df1c39748e019f42	Ch 2.14.1	Wed Feb 17 15:14:20 2010 UTC
28dc1ca683d6a14d0d1794a68c477604	Ch 3.00	Tue Jan 31 16:12:25 2012 UTC
40bd7846553550f38e458b8493824cb4	Ch 3.00	Tue Feb 14 10:28:06 2012 UTC
ba0c777317461ed57a85ffae277044dc	Ch 3.02	Wed Apr 4 16:23:44 2012 UTC
b86137fa5a232c614ec5405be4d13b37	Ch 3.10	Tue Dec 18 08:22:43 2012 UTC
7872c1d88fe21d8a85f160a6666c76e8	Ch 3.20	Fri Jun 28 12:16:40 2013 UTC
83a48760e92bf30961b4a943d3095b0a	Ch 3.20	Fri Jun 28 12:16:58 2013 UTC
3d65c18d09f47547f85c631ebeeda482	Ch 3.20	Mon Jun 24 10:51:01 2013 UTC
ec7e3cfaeaac0401316d66e964be684e	Ch 3.25	Thu Feb 6 12:37:44 2014 UTC
b407b6e5b4046da226d6e189a67f62ca	Ch 3.26	Thu Jan 3 18:03:46 2013 UTC

Thanks to the versioning, we can deduce that the compilation dates we saw and currently see actually seem to be legit – except for the last known version, in which the author modified the compilation date in order to make the analysis more complex. We can see that this malware was really active in 2007 and 2008. New versions declined in frequency in 2009 and only one new sample was identified in 2010. We did not encounter any new sample from 2011, but the malware appeared back in 2012, with a new major version.

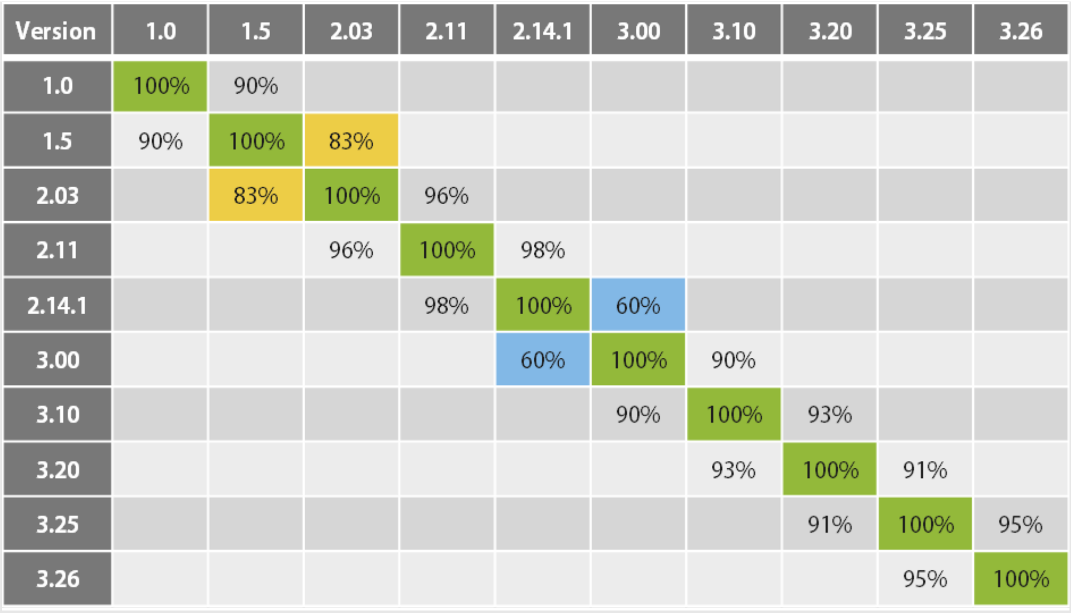


The RAT’s evolution described in ten steps

To describe the evolution of the development, we decided to compare ten major versions:

- Version Ch 1.0 (2007-06) to Ch 1.5 (2008-03)
- Version Ch 1.5 (2008-03) to Ch 2.03 (2008-05)
- Version Ch 2.03 (2008-05) to Ch 2.11 (2009-09)
- Version Ch 2.11 (2009-09) to Ch 2.14.1 (2010-02)
- Version Ch 2.14.1 (2010-02) to Ch 3.00 (2012-01)
- Version Ch 3.00 (2012-01) to Ch 3.10 (2012-12)
- Version Ch 3.10 (2012-12) to Ch 3.20 (2013-06)
- Version Ch 3.20 (2013-06) to Ch 3.25 (2014-02)
- Version Ch 3.25 (2014-02) to Ch 3.26 (2013-01; date has been modified)

The following chapter will present the main differences between the versions mentioned above. Here is the resemblance ratio for each version, comparing direct neighbor versions only, created using BinDiff:



Version	1.0	1.5	2.03	2.11	2.14.1	3.00	3.10	3.20	3.25	3.26
1.0	100%	90%								
1.5	90%	100%	83%							
2.03		83%	100%	96%						
2.11			96%	100%	98%					
2.14.1				98%	100%	60%				
3.00					60%	100%	90%			
3.10						90%	100%	93%		
3.20							93%	100%	91%	
3.25								91%	100%	95%
3.26									95%	100%

The biggest code update has occurred between version 2.14.1 and version 3.00. The gap matches the absence of samples during two years and this fundamental modification is what we call the death of Agent.BTZ and the birth of ComRAT.

Differences between version Ch 1.0 (2007-06) to Ch 1.5 (2008-03)

The analyzed samples are:

- Ch 1.0: b41fbdd02e4d54b4bc28eda99a8c1502
- Ch 1.5: bbf569176ec7ec611d8a000b50cdb754
- Code similarity: 90%

We did not identify strong modification between the two samples. However, we can notice the following:

- The configuration file (XML) in version 1.5 is stored in Unicode and not in ASCII anymore;
- The two versions implement a mechanism to infect new media connected to the infected system. The implementation is not exactly the same nor is the log of media infection;
- Version 1.5 creates a new event: “wowmgr_is_load”. This event has then been used for years.

Differences between version Ch 1.5 (2008-03) and Ch 2.03 (2008-05)

The analyzed samples are:

- Ch 1.5: bbf569176ec7ec611d8a000b50cdb754
- Ch 2.03: 78d3f074b70788897ae7e20e5137bf47
- Code similarity: 83%

In version 2.03 of Agent.BTZ, the authors changed the following:

- They added obfuscation in order to hide sensitive strings;
- The communication protocol was modified in order to include the flag “<CHCMD>”
- we assume that “CH” has the same meaning than “Ch” before the version number and “CMD” is the abbreviation for command;
- From now on, the malware supports “runas” in order to execute commands as administrator. This command was implemented by Microsoft in Windows Vista in 2007. We assume that the author implemented this feature because several targets switched to this version of Windows in 2008.

According to an article, version 1.5 was used against the US Pentagon. We assume that the string obfuscation was performed in order to bypass security measures being capable of detecting an intrusion.

Differences between version Ch 2.03 (2008-05) and Ch 2.11 (2009-09)

The analyzed samples are:

- Ch 2.03: 78d3f074b70788897ae7e20e5137bf47
- Ch 2.11: 162f415abad9708aa61db8e03bcf2f3c
- Code similarity: 96%

The codes of these two versions are extremely similar to each other, we can only notice small changes:

- The author changed the name of several registry keys (probably to avoid detection by well-known IOC);
- The name of two exported functions were modified, too: InstallM() becomes AddAtomT() and InstallS() becomes AddAtomS(),probably for the same reason than above.

Differences between version Ch 2.11 (2009-09) and Ch 2.14.1 (2010-02)

The analyzed samples are:

- Ch 2.11: 162f415abad9708aa61db8e03bcf2f3c
- Ch 2.14.1: 5121ce1f96d74076df1c39748e019f42
- Code similarity: 98%

These codes are really similar to each other, too. We can notice only two changes:

- The author patched several bugs;
- Four new exports appear: DllCanUnLoadNow(), DllGetClassObject(), DllRegisterServer(), DllUnregisterServer().

The four exported libraries show that the malware has started to support the OLE Component Object

Model (COM). This version is the first version able to be registered as a COM object. Three of the four functions are empty. The fourth one executes the malware.

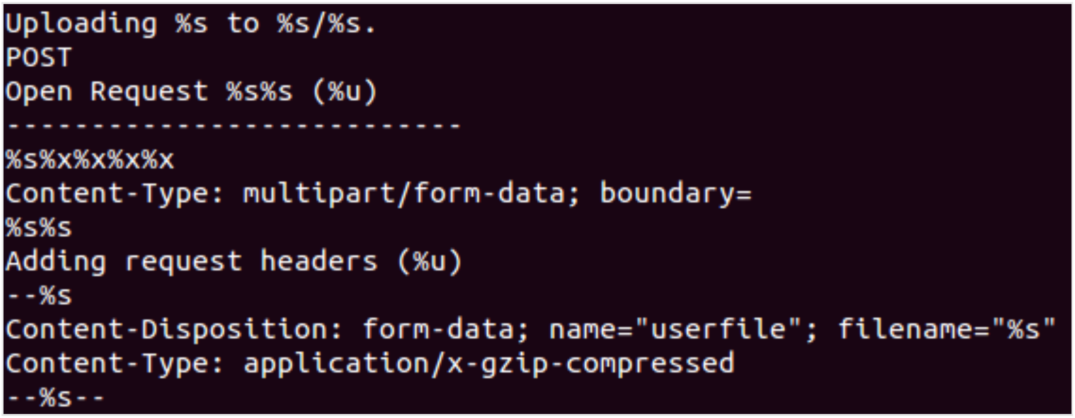
Differences between version 2.14.1 (2010-02) and Ch 3.00 (2012-01)

The analyzed samples are:

- Ch 2.14.1: 5121ce1f96d74076df1c39748e019f42
- Ch 3.00: 28dc1ca683d6a14d0d1794a68c477604
- Code similarity: 60%

These codes really differ from each other, even if some parts of version 2.14.1 were retained. Moreover, the developers changed the compiler; they switched from Visual Studio 6.0 to Visual Studio 9.0/10.0 , which is a strong indicator for the huge differences.Version 3.00 is what the G DATA SecurityLabs experts call ComRAT. We can say that version 2.14.1 is the last version of Agent.BTZ. Here are the main differences between Agent.BTZ and ComRAT:

- The new malware collects more information about the infected system (such as drive information, volume information…).
- The media stick infection mechanism has definitely been removed. We assume this happened due to the fact that Microsoft has disabled AutoRun for external media. For the attackers, this infection vector is not interesting anymore.
- The malware is injected into every process of the infected machine and the main payload is executed in “explorer.exe” as we explained in our article;
- The communication channel to the command and control is not the same anymore. In this new version, the malware uses POST requests with the following pattern:



```
Uploading %s to %s/%s.
POST
Open Request %s%s (%u)
---------------------------
%s%x%x%x%x
Content-Type: multipart/form-data; boundary=
%s%s
Adding request headers (%u)
--%s
Content-Disposition: form-data; name="userfile"; filename="%s"
Content-Type: application/x-gzip-compressed
--%s--
```

- As the malware is injected into every process of the infected system, it creates named pipe in order to handle inter-processes communication.

On several 3.00 samples, the author forgot to remove the compilation path, here are some examples:

- c:\projects\ChinckSkx64\Debug\Chinch.pdb
- c:\projects\ChinckSkx64\Release\libadcodec.pdb
- C:\projects\ChinckSkx64\x64\Release\libadcodec.pdb
- E:\old_comp_Chinch\Chinch\trunk\Debug\Chinch.pdb
- c:\projects\ChinchSk\Release\libadcodec.pdb

Thanks to these compilation paths, we assume that the original name of the RAT is "Chinch", which leads us to the assumption that the "CH" characters in the version name and in the flag "<CHCMD>" stands for "Chinch". In English, chinch is the word for a small North American bug, Blissus leucopterus. This word is derived from the Spanish word chinche, meaning pest.

Differences between version 3.00 (2012-01) and Ch 3.10 (2012-12)

The analyzed samples are:

- Ch 3.00: 28dc1ca683d6a14d0d1794a68c477604
- Ch 3.10: b86137fa5a232c614ec5405be4d13b37
- Code similarity: 90%

The codes are similar to each other, but the authors added several features:

- The malware generates more logs;
- The malware has a Mutex handle;
- The 3.10 version supports multiple command and control servers.

The last new feature is really interesting: if the compromised targets block a specific command and control server, the malware will continue to work, thanks to two alternative command and control servers.

Differences between version 3.10 (2012-12) and Ch 3.20 (2013-06)

The analyzed samples are:

- Ch 3.10: b86137fa5a232c614ec5405be4d13b37
- Ch 3.20: 7872c1d88fe21d8a85f160a6666c76e8
- Code similarity: 93%

The major new feature in the version is the new exports function called InstallW(). This exported function is used by the dropper to add persistence in the registry and to drop a second file (as explained in our previous article). Version 3.20 uses the following CLSID in order to hijack COM object: B196B286-BAB4-101A-B69C-00AA00341D07. This object is the IConnectionPoint interface. The CLSID was only used in this version. We assume that the performed COM object hijacking generates some trouble on the infected system, that's why the author changed related things in the next version. Furthermore, the CLSID was stored in plain text within the sample.

Differences between version Ch 3.20 (2013-06) and Ch 3.25 (2014-02)

The analyzed samples are:

- Ch 3.20: 7872c1d88fe21d8a85f160a6666c76e8
- Ch 3.25: ec7e3cfaeaac0401316d66e964be684e
- Code similarity: 91%

In the 3.25 version, the author switched to the CLSID: 42aedc87-2188-41fd-b9a3-0c966feabec1 as described in our article. Furthermore, the strings in the sample are obfuscated. The main new feature is the obfuscation – almost all strings are obfuscated and the XML pattern is not written in plain text anymore.

Differences between version Ch 3.25 (2014-02) and Ch 3.26 (2013-01; date has been modified)

The analyzed samples are:

- Ch 3.25: ec7e3cfaeaac0401316d66e964be684e
- Ch 3.26: b407b6e5b4046da226d6e189a67f62ca
- Code similarity: 95%

The version 3.26 is the latest known version. In this version:

- The authors removed the familiar XOR key used by Agent.BTZ and Uroburos. We assume that due to the G DATA publication in February 2014, the author decided to remove as many links as possible between Uroburos and Agent.BTZ/ComRAT/Chinch;
- The authors do not generate logs anymore;
- The compilation date has been modified, in order to make the analysis and timeline creation more complex.

Conclusion

This analysis shows us seven years of the evolution of a Remote Administration Tool, used by a group which targeted extremely sensitive entities, such as the US Pentagon in 2008 or the Belgium Ministry of Foreign Affairs in 2014 as well as the Finnish Ministry of Foreign Affairs.

Except for version 3.00, the modifications made are rather marginal. We can see that the authors adapted features to the Windows versions, patched bugs, added obfuscation etc... The biggest update was performed to version 3.00, after two years of silence. Visibly, this RAT was used alongside the Uroburos rootkit. Nevertheless, it is not entirely clear how and when the attackers choose to use the RAT or the rootkit or whether both are used in parallel.

Taking everything into consideration, G DATA SecurityLabs experts are sure that the group behind Uroburos/Agent.BTZ/ComRAT/Linux tool/... will remain an active player in the malware and APT field. The newest revelations made and connections drawn let us believe that there is even more to come.