Analysing a 10-Year-Old SNOWBALL

By Dominik Reichel

Published: 2017-09-06 · Archived: 2026-04-06 00:35:28 UTC

Much has been written about the malware toolkit dubbed Animal Farm which is made up of several implants known as Babar, Bunny, NBot, Dino, Casper and Tafacalou. Some of these tools have been used in past attacks against organizations, companies and individuals.

One of the first tools believed to be used by this adversary to target a potential victim is Babar, also known as SNOWBALL. Previous samples of SNOWBALL date back to 2011. However, Palo Alto Networks Unit 42 has identified a much older version. This version of the malware dates back to 2007 according to its compilation time stamp which we believe is valid.

We discovered this sample by coincidence while searching for another unrelated malware in a large malware repository. While looking at the strings and the structure, we could make a connection to previously published documents and decided to do a deeper analysis.

Why analyse malware from the past?

Analysing historical malware samples helps us learn about its set of features and technical capabilities. This helps us compare a tool used by one adversary to that used by similarly adversaries at that time.

This earlier sample of Babar uses many features not present in later versions. The sample also uses a compromised third party website as a C2 server like later versions. We also found a simple bug and a design flaw in the code you wouldn't expect from malware developed by mature actors.

Detailed technical breakdown

The Loader

The PE sample comes in form of a loader which has a compilation time stamp of 11/09/2007 11:37:36 PM. The loader contains a resource named **MYRES** (Figure 1) where the payload DLL is stored.

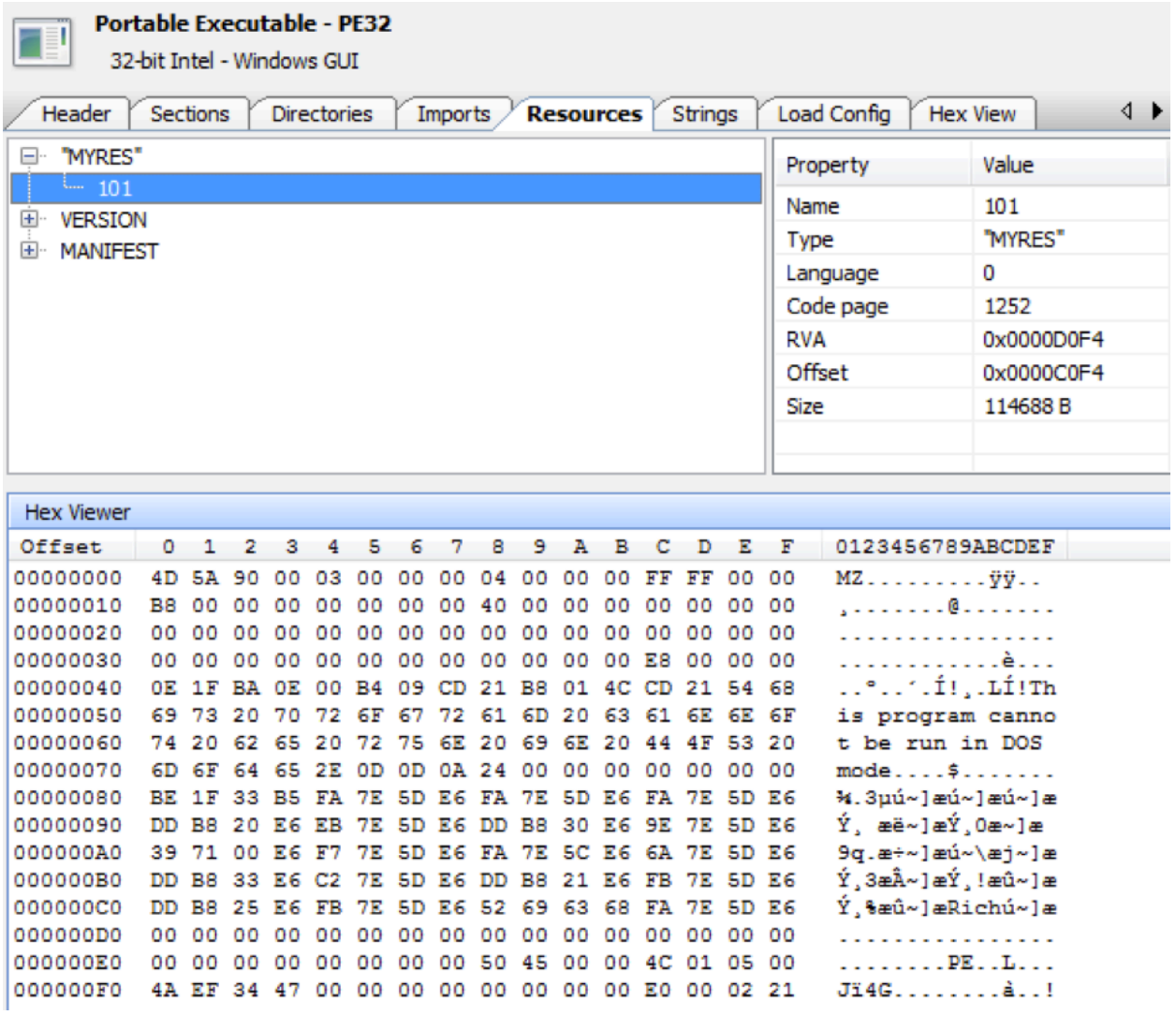

Figure 1. PE resource named MYRES with main payload DLL

The version info resource language ID is 1036 which stands for French.

The following clear text strings can be found in the loader:

1	HTTP\SHELL\open\command
2	SOFTWARE\Clients\StartMenuInternet
3	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\
4	%APPDATA%
5	event.log
6	Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
7	%ALLUSERSPROFILE%
8	%ALLUSERSPROFILE%
9	%APPDATA%

10	%APPDATA%
11	AppData
12	SeDebugPrivilege
13	MYRES
14	Software\Microsoft\Windows\ShellNoRoam\MUICache\
15	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\
16	\Microsoft\wmimgnt.dll
17	\Microsoft\wmimgnt.exe
18	ExitProcess
19	KERNEL32.DLL
20	%ProgramFiles%
21	\Internet Explorer\iexplore.exe -embedding
22	iexplore.exe
23	-embedding

At the beginning, it changes the error mode of the process to handle the following errors:

- SEM_NOOPENFILEERRORBOX
- SEM_NOGPFAULTERRORBOX
- SEM_FAILCRITICALERRORS

For this, it sets up an exception handler with the address to ExitProcess(). Thus, if any of the errors occur the malware just exits.

Next, it tries to gain debug privileges and checks if the major OS version is >= Windows Vista and the platform ID is VER_PLATFORM_WIN32_NT. If so, if tries to create a file named event.log in the %ALLUSERSPROFILE% folder. However, the authors forget to append the character "\" before appending the hardcoded string "event.log". This results in the creation of the following file:

1	C:\ProgramDataevent.log

If the call to CreateFile() fails, it tries to delete this file.

Next, it tries to get the local AppData folder path first by querying the %APPDATA% environment variable and if that fails, it looks in the shell folders in the registry. This data is then used to create the following file paths with the hardcoded file names:

1	C:\Users_username_\AppData\Roaming\Microsoft\wmimgnt.dll

```
2  C:\Users\_username_\AppData\Roaming\Microsoft\wmimgnt.exe
```

The malware also tries to delete any traces it was executed by deleting the corresponding entries in the following registry keys:

```
1  HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache\
2  HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
```

After this, the malware checks if its main module is already present on a victim's system by trying to open the file:

```
1  C:\Users\_username_\AppData\Roaming\Microsoft\wmimgnt.dll
```

If the file is present, the malware checks if the module file name of the process is as follows and exits otherwise:

```
1  C:\Users\_username_\AppData\Roaming\Microsoft\wmimgnt.exe
```

If it matches the malware creates a temporary file in the local user's temp folder and copies the resource named MYRES into it. This file is the payload DLL which then gets moved as wmimgnt.dll to the AppData folder. The file attributes are changed to hidden and the file time is changed to make it look like an old file. The same procedure is done with the initial file which gets copied as wmimngt.exe into the AppData folder.

Thereafter, the malware checks again the major OS version and platform ID like previously and opens the following registry key to get the default internet browser:

```
1  HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet
```

The malware authors assumed the browser string always ends with a ".exe" extension and calculate the string in the following manner:

```
1  RegOpenKeyExA(HKEY_CURRENT_USER, "SOFTWARE\\Clients\\StartMenuInternet", 0, 1u, phkResult);
2  RegQueryValueExA(phkResult, 0, 0, Type, Data, &amp;amp;cbData);
3  ...
4  v3 = strstr((const char *)Data, ".exe");
5  ...
6  v4 = v3[-v1] - (char *)Data + 4;
7  memcpy(a1, Data[v1], v4);
```

The calculation of the string length in v4 only works if the default browser is for example Internet Explorer or Firefox, as these browsers have an .exe extension in the registry key:

```
1  IEXPLORE.EXE
2  FIREFOX.EXE
```

While a browser like Chrome uses the following string:

```
1  Google Chrome
```

In this case, the string length gets wrongly calculated and the subsequent call to memcpy() fails with an error so the exception handler kicks in to terminate the process. However, as Chrome was first released in 2008 and the malware was coded earlier, this can't be considered as a bug.

After retrieving the string of the default browser from registry, it builds the following string to get the application path of it:

```
1  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths
```

If this was successful it searches for the string "iexplore.exe" in the path and appends the string " -embedding" to it. If it failed, the malware retrieves the ProgramFiles path via the environment variable "%ProgramFiles%" and appends the string "\Internet Explorer\iexplore.exe -embedding".

The command line argument "-embedding" does the following according to Microsoft:

```
1  Starts Windows Internet Explorer through OLE embedding (such as the WebBrowser Control).
```

At last, it creates a suspended process of Internet Explorer and injects the payload DLL via the infamous CreateRemoteThread() method.

The Payload DLL

This sample has a compilation time stamp of 11/09/2007 11:37:46 PM (10 seconds after the loader.) It contains an encrypted resource named **XML** which contains configuration data. The encryption algorithm RC4 is used with the key **+37:*$pK#s**. Both the version info and the XML resource language IDs have again the value 1036 (French).

Decrypted configuration data:

```
1  <HOST>cpcc-rdc.org</HOST>
2  <URL>/wp-pagin/outbase.php</URL>
3  <PORT>80</PORT>
4  <MIN>3000</MIN>
```

```
5   <MAX>4000</MAX>
6   <PREFIX>=#-+ApAcHe_ToMcAt+-#=</PREFIX>
7   <ENCODE>1</ENCODE>
8   <PASSWORD>TargetRenegade</PASSWORD>
9   <CONFIG_KEY>SOFTWARE\Microsoft\MSRPC</CONFIG_KEY>
10  <RUN_KEY>Windows Management Infrastructure (WMI)</RUN_KEY>
```

As can be seen, a third-party website was compromised as C2 server to host a script named outbase.php. The domain (cpcc-rdc.org) is the official site of Permanent Council of Accounting of the Democratic Republic of the Congo. The script is not online anymore as the attack was most likely carried many years ago.

The following clear text strings can be found in the DLL:

```
1   reboot
2   shutdown
3   download
4   wget
5   fetch
6   wput
7   showconfig
8   timeout
9   timeout_main
10  timeout_safe
11  newurl_main
12  newurl_safe
13  movetosite
14  listprocess
15  killprocess
16  kitkit
17  uninstall
18  %s\%s
19  %d-%d
```

```
20  [+] Timeout set successfully
21  [-] Timeout error
22  [+] Timeout_main set successfully
23  [-] Timeout_main error
24  [+] Timeout_safe set successfully
25  [-] Timeout_safe error
26  ! EXECUTION TIME LIMIT EXCEEDED ! You maybe have to kill the process "%s" you launched (Use
    listprocess and killprocess...)
27  cmd.exe /C %s
28  command.com /c %s
29  [-] Unable to go to this unit
30  [-] Cannot reboot
31  [-] Cannot shutdown
32  [-] Download error
33  [%s] &gt; 500 Ko  =&gt;  use "big"
34  [-] Download error
35  Upload;%s;
36  [-] fetch error
37  [-] fetch error
38  [+] fetch seems to be OK
39  [-] fetch error
40  [+] Uninstalled
41  [-] Uninstall failed
42  data=
43  http://
44  [+] wput Ok
45  [-] wput error
46  http://
47  [+] wget Ok
48  [-] wget error
```

```
49  [+] movetosite "%s" Ok
50  [-] movetosite failed
51  [+] change main site url Ok
52  [-] change main site url failed
53  [+] change safe site url Ok
54  [-] change safe site url failed
55  Big in progress... Please wait before downloading the file.
56  [+] Big finished. You can now download the file
57  Multi-Part;%d;%s;
58  MULTI
59  [-] big error
60  [-] Can't list partitions
61    DRIVE_TYPE    LETTER   VOLUME_NAME
62  ----------------------------------------
63  Fixed
64  CDRom
65  Removable
66  NoRootDir
67  Remote
68  Ramdisk
69  Unknown
70  %12s      %s     %s
71            PROCESS NAME    PID
72  --------------------------------
73  %22s   %4d
74  [-] Unable to kill the process "%s" with the PID %d
75  [-] Unable to kill the process "%s" with the PID %d
76  [+] The process "%s" with the PID %d has been killed
77  [-] The process with the PID %d was not found
```

```
78  [-] killprocess error
79  ======= CURRENT PARAMS
80  [+] Url: http://%s%s
81  [+] Port: %d
82  [+] Timeout: %d-%d
83  ======= SAVED PARAMS
84  [Main Site]
85  [+] Url: http://%s%s
86  [+] Port: %d
87  [+] Timeout: %d-%d
88  [Safe Site]
89  [+] Url: http://%s%s
90  [+] Port: %d
91  [+] Timeout: %d-%d
92  bad allocation
93  %APPDATA%
94  event.log
95  Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
96  %ALLUSERSPROFILE%
97  %APPDATA%
98  AppData
99  MSFirstUpdate
100 %02d\%02d\%04d %02d:%02d:%02d
101 :strt
102 del /F /A "%s"
103 if EXIST "%s" GOTO strt
104 del /F /A "%s"
105 del /F /A %0
106 \Microsoft\wmimgnt.exe
```

107	\Microsoft\wmimgnt.dll
108	wupdmgr.bat
109	Software\Microsoft\Windows\ShellNoRoam\MUICache
110	bad allocation
111	user=%s;%d;%s;
112	Default User ID
113	Identities
114	sCountry
115	Control Panel\International
116	User Agent
117	Software\Microsoft\Windows\CurrentVersion\Internet Settings
118	Software\Clients\StartMenuInternet
119	HTTP\SHELL\open\command
120	RegisteredOrganization
121	SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
122	RegisteredOwner
123	SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
124	CSDVersion
125	SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
126	CurrentVersion
127	SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
128	DefaultUserName
129	SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\Winlogon
130	USERNAME
131	Volatile Environment
132	DefaultDomainName
133	SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\Winlogon
134	USERDOMAIN
135	Volatile Environment

```
136 RegisteredOrganization
137 SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion
138 RegisteredOwner
139 SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion
140 CSDVersion
141 SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion
142 CurrentVersion
143 SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion
144 DefaultUserName
145 SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion\Winlogon
146 DefaultDomainName
147 SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion\Winlogon
148 Default
149 Login (owner): %s (%s)
150 Computer name: %s
151 Organization (country): %s (%s)
152 OS version (SP): %s (%s)
153 Default browser: %s
154 IE version: %s
155 Timeout: %d(min)
156 %d(max)
157 First launch: %s
158 Last launch : %02d\%02d\%04d %02d:%02d:%02d
159 bad allocation
160 \Microsoft\wmimgnt.exe
161 SeDebugPrivilege
162 ExitProcess
163 KERNEL32.DLL
164 RUN_KEY
```

```
CONFIG_KEY
bad allocation
after init
Before transform
After transform
bits: %d %d
buf: %x %x %x %x
bad allocation
Content-Type: application/x-www-form-urlencoded
bad allocation
msupdate32
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
+37:*$pK#s
&lt;%s&gt;%s
&lt;%s&gt;%d
PREFIX
ENCODE
PASSWORD
CONFIG_KEY
RUN_KEY
HOST_SAFE
URL_SAFE
PORT_SAFE
MIN_SAFE
MAX_SAFE
PREFIX
=#-+ApAcHe_ToMcAt+-#=
ENCODE
```

```
194 PASSWORD
195 TargetRenegade
196 RUN_KEY
197 Windows Management Infrastructure (WMI)
198 /outbase.php
199 127.0.0.1
200 URL_SAFE
201 /outbase.php
202 HOST_SAFE
203 127.0.0.1
204 PORT_SAFE
205 MIN_SAFE
206 MAX_SAFE
207
```

The sample only executes if the reason code why the DLL entry-point function was being called is **DLL_PROCESS_ATTACH**.

At first, the malware decrypts the XML configuration data to memory, searches for the XML tags **<RUN_KEY>** and <**CONFIG_KEY>** and extracts their content. With this data, it checks if the malware's persistency is already present in the registry Run key and creates it if it's not the case:

```
1 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
2 Value: Windows Management Infrastructure (WMI)
3 Value key: C:\Users\_username_\AppData\Roaming\Microsoft\wmimgnt.exe
```

Thereafter, it decrypts the data of the following XML tags and stores them in memory:

```
1 PREFIX
2 ENCODE
3 PASSWORD
4 RUN_KEY
5 URL
```

6	HOST
7	PORT
8	MIN
9	MAX

The implementation of this part of the code is somewhat flawed, since the malware contains the encrypted configuration data, but the same data (except for the C2 domain) is also present as clear text strings. If the decryption didn't work it uses the clear text strings.

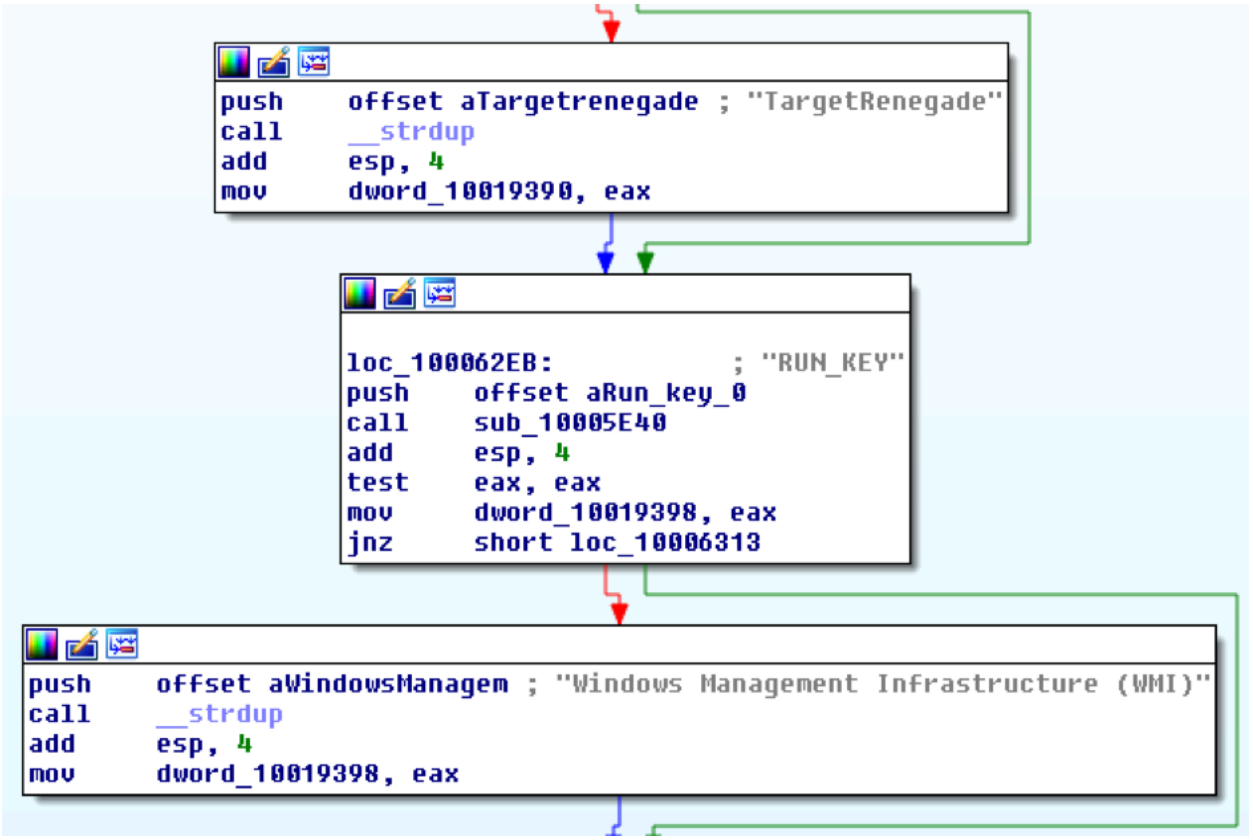

Figure 2. Clear text configuration data

It also creates the following new XML tags based on the old ones:

1	<MAX_SAFE>4800</MAX_SAFE>
2	<MIN_SAFE>3600</MIN_SAFE>
3	<PORT_SAFE>80</PORT_SAFE>
4	<URL_SAFE>/outbase.php</URL_SAFE>
5	<HOST_SAFE>127.0.0.1</HOST_SAFE>

All the XML tags are then RC4 encrypted with key **+37:*$pK#s** and stored in the following registry key:

```
1  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSRPC
2  Value: msupdate32
```

Then, it tries to get system information from the following registry keys:

```
1  HKEY_CURRENT_USER\Identities
2  Value: Default User ID
3  HKEY_CURRENT_USER\Control Panel\International
4  Value: sCountry
5  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
6  Value: User Agent
7  HKEY_CURRENT_USER\Software\Clients\StartMenuInternet
8  HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
9  Value: RegisteredOrganization
10 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
11 Value: RegisteredOwner
12 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
13 Value: CSDVersion
14 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion
15 Value: CurrentVersion
16 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\Winlogon
17 Value: DefaultUserName
18 HKEY_CURRENT_USER\Volatile Environment
19 Value: USERNAME
20 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\Winlogon
21 Value: DefaultDomainName
```

The malware also retrieves the current system time, encrypts it with RC4 and the same key and stores it in the following registry key:

```
1  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSRPC
```

2	Value: MSFirstUpdate
3	Value key: <RC4encrypteddatetime>

Then, it creates a string with the previously retrieved system information, the configuration data and the following string template:

1	Login (owner): %s (%s)
2	Computer name: %s
3	Organization (country): %s (%s)
4	OS version (SP): %s (%s)
5	Default browser: %s
6	IE version: %s
7	Timeout: %d(min) %d(max)
8	First launch: %s
9	Last launch : %02d\%02d\%04d %02d:%02d:%02d

Next, the MD5 hash of this string is calculated and encrypted with RC4 and the same key again. This encrypted string gets then stored in the following registry key:

1	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSRPC
2	Value: MSID
3	Value key: <MD5hashedandRC4encryptedsysteminformation>

To send victim information to the C2 server, it prepares a URL query string by entering the "INFO" branch. The other query branch named "CMD" is entered to send back the result of a command sent by the C2 server.

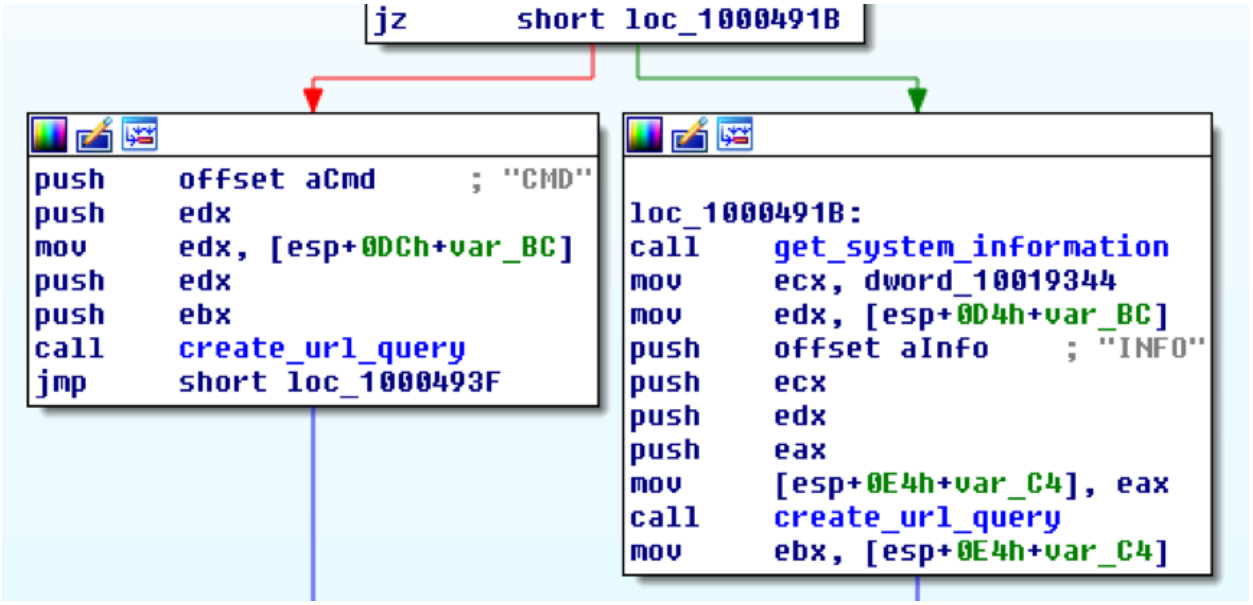

Figure 3. URL query string creation branches

At first, the checks if the <**ENCODE**> XML tag is set to 0x1 and if so it encrypts the previously created string with the victim's information with the password contained in the <**PASSWORD**> XML tag. It does this by bytewise adding 0x80 to the password string and then using an encoded byte to bytewise XOR the information string. The encrypted string gets then Base64 encoded and the characters "+", "/" and "=" URL encoded ("%2B", "%2F", "%3D"). The following string template is then used together with the encrypted data to form the final URL query string:

```
1 user=%s;%d;%s;
```

The first string is the previously calculated MD5 hash, the decimal number is made of a random number between 3000/3600 (XML tag) and 4000/4800 (XML tag). The last string is made of the hardcoded "INFO" string along with the Base64 encoded victim data. For example:

```
1 user=52ac9e4b389c5b2f8a63af4a126c1c80;3046;INFO;mI7BkjovU%2BoqZi4KTzd%2F0wdqqjJegip2KgYXN6N6inYqV..
```

To test if the computer is connected to the internet it uses InternetGetConnectedState() API function. Next, it enters either the "main" or the "safe" branch referring to the XML tags. The main branch is the usual execution path, while the safe branch only gets used for a specific malware command. If there is no internet connection it sleeps for a certain time, otherwise it contacts the C2 server present in the **<HOST>** XML tag together with the URL query string. The malware has the ability to send data with both HTTP request methods, GET and POST. However, this sample only uses the POST request method along with the following content type field:

```
1 Content-Type: application/x-www-form-urlencoded
```

After contacting the C2 server, the malware copies the response into memory and scans for the marker **=#-+ApAcHe_ToMcAt+-#=** taken from the **<PREFIX>** XML tag. If successful, the response gets Base64 decoded and decrypted with the same algorithm used to encrypt the victim information string. The PHP script **outbase.php** can respond with one of the commands listed below, which the malware then executes.

To process some commands, the malware creates an anonymous pipe and a hidden instance of cmd.exe or command.com, depending on the platform ID. The command line output gets redirected to the pipe, read into memory and later send back encrypted and encoded via the "CMD" URL query branch.

Possible malware commands:

1. pwd
Get current working directory

2. cd
change directory to delivered string

3. part
Get list and type of partitions

4. reboot
Reboot system

5. shutdown
Shutdown system

6. download
Download file < 512,000 bytes delivered in form of a URL ("500 Ko") to disk

7. big
Download file > 512,000 bytes delivered in form of a URL ("500 Ko") to disk

8. wget
Download file with predefined HTTP query string

9. fetch
Download file via URLDownloadToFile()

10. wput
Download data from internet via **download** command and sent data back via "data=" query

11. info
Send back victim system information (see above)

12. showconfig
Send back current config data with following string template:

1	======= CURRENT PARAMS
2	[+] Url: http://%s%s
3	[+] Port: %d
4	[+] Timeout: %d-%d
5	======= SAVED PARAMS
6	[Main Site]

7	[+] Url: http://%s%s
8	[+] Port: %d
9	[+] Timeout: %d-%d
10	[Safe Site]
11	[+] Url: http://%s%s
12	[+] Port: %d
13	[+] Timeout: %d-%d
14	
15	
16	

13. timeout
Change current timeout interval variables

14. timeout_main
Change timeout intervals in main XML configuration

15. timeout_safe
Change timeout intervals in safe XML configuration

16. newurl_main
Change host URL in main XML configuration

17. newurl_safe
Change host URL in safe XML configuration

18. movetosite
Change current host URL variable

19. listprocess
Get list of current processes with PID

20. killprocess
Terminate process delivered via string

21. kitkit
Terminate itself

22. uninstall
Delete malware files on disk and registry entries

Conclusion

This malware has a small set of features ranging from retrieving system information, to downloading files or killing processes on a victim's system. Technically, it is not outstanding and can be considered only average compared to alleged

state sponsored malware written at that time (e.g. Careto or Regin). The code and structure is similar to the Casper implant which is most likely based on this implant. The malware contains an obvious design flaw leaving the main part of the configuration data visible in clear text.

- AutoFocus customers can identify this, and other samples related to it using the Snowball
- WildFire and Traps properly classify Snowball samples as malicious.

Thanks to Esmid Idrizovic for his assistance in this analysis.

Indicators of Compromise:

Hashes (SHA-256)

Loader: c71b1a31bdf3a08fa99ed1f6a1c5ded61e66f3d41e4ed88a12430d1c14ed10ca
Payload DLL: a9220590d3c35fe22df9d38a066ca8d112b83764b39fea98b38761daa64c77b8
