Analysis Report (TLP:WHITE)
Analysis of a PlugX variant (PlugX version 7.0)

Conducted by CIRCL - Computer Incident Response Center Luxembourg
Team CIRCL

March 29, 2013

Document version: 1.0

CIRCL
Computer Incident
Response Center
Luxembourg

Contents

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

1 Scope of work

This report is the analysis of a Remote Access Tool (RAT) which we call a variant of Plugx[1]. Plugx is an interesting piece of malware for several reasons:

- It demonstrates the attack principle of the fastest/cheapest path of attack[2] by abusing perfectly valid signed binaries to perform the attack
- It features ways to defeat other protection mechanisms like UAC[3]
- In contrast to many other pieces of malware, the author[4] shows the ability to write good code, especially doing logging the right way to improve the piece of software
- It appears to be modularized and easily extensible

2 Analyzed samples

- Sample A - Stage 1 of Malware
  - Description
    - Hash found in a malware database
  - Original filename
    - update.exe
  - Hashes
    - MD5: f1f48360f95e1b43e9fba0fec5a2afb8
    - SHA1: 70ceb467db7b0161d22e4545479f747417b9705a
    - SHA-256: 2bc5ce39dd9afe2157448d3f6d8cb9c549ed39543d159616e38480b9e6c11c49
  - Filetype
    - PE32 executable (GUI) Intel 80386, for MS Windows, RAR self-extracting archive
  - Filesize
    - 370702 Bytes (326KB)
  - Compile time
    - Sat Jun 9 15:19:49 2012
- Sample B - Valid, signed McAfee binary
  - Description
    - File dropped by Sample A
  - Original filename
    - mcvsmap.exe
  - Hashes

[1] Known variant names: Gulpix, Korplug

[2] `http://satoss.uni.lu/seminars/srm/pdfs/2012-Alexandre-Dulaunoy.pdf`

[3] `http://msdn.microsoft.com/en-us/library/windows/desktop/bb756996.aspx`

[4] For better readability we do not distinguish between a single author or a group of authors. Hence the expression is a synonym for "the authors"

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

    * MD5: 4e1e0b8b0673937415599bf2f24c44ad
    * SHA1: 9224de3af2a246011c6294f64f27206d165317ba
    * SHA-256: ae16e10e621d6610a3f7f2c7122f9d1263700ba02d1b90e42798decb2fe84096
  - Filetype
    * PE32 executable (GUI) Intel 80386, for MS Windows
  - Filesize
    * 262672 Bytes (257K)
  - Compile time
    * Fri May 8 17:59:52 2009
  - Authenticode[5] verification

```
Verified: Signed
Signers:
  McAfee, Inc.
  VeriSign Class 3 Code Signing 2004 CA
  Class 3 Public Primary Certification Authority
Signing date: 5:24 PM 5/8/2009
Publisher: McAfee, Inc.
Description: McAfee VirusMap Reporting module
Product: McAfee VirusScan API
Version: 13,11,0,0
File version: 13,11,102,0
Strong Name: Unsigned
Original Name: McVsMap.EXE
Internal Name: McVsMap
Copyright: Copyright  2008 McAfee, Inc.
Comments: n/a
MD5: 4e1e0b8b0673937415599bf2f24c44ad
SHA1: 9224de3af2a246011c6294f64f27206d165317ba
SHA256: ae16e10e621d6610a3f7f2c7122f9d1263700ba02d1b90e42798decb2fe84096
```

- Sample C - DLL to be loaded by Sample B, loads Sample D
  - Description
    * File dropped by Sample A
  - Original filename
    * McUtil.DLL
  - Hashes
    * MD5: ad4a646b38a482cc07d5b09b4fffd3b3
    * SHA1: ae0f9bf2740d00c5d485827eb32aca33feaa3a90
    * SHA-256: 0a99238e1ebebc47d7a89b2ccddfae537479f7f77322b5d4941315d3f7e5ca48
  - Filetype
    * PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
  - Filesize
    * 49152 Bytes (48K)

[5] http://msdn.microsoft.com/en-us/library/ms537359%28v=vs.85%29.aspx

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

  - Compile time
    * Wed Mar 13 02:52:28 2013

- Sample D - Malicious payload to be loaded by Sample C
  - Description
    * File dropped by Sample A
  - Original filename
    * McUtil.DLL.PPT
  - Hashes
    * MD5: 545bb4365a9b7cdb6d22844ebeedda93
    * SHA1: a267f1183b4ff843d68a63264846abf78cc71d1f
    * SHA-256: d4fe890a08d4dd44b58a3b85b2a7e89536338099c1c42a9b7e85f4007b0a37b7
  - Filetype
    * pure code (IA32) without headers
  - Filesize
    * 124820 Bytes (122K)
  - Compile time
    * unknown (pure code)

- Sample E - Stage 2 of Malware
  - Description
    * Extracted malware from memory
  - Original filename
    * dump00C60000.bin
  - Hashes
    * MD5: 65ceb039e7b4731a165cfee081e220af
    * SHA1: b49766187971e3070644a9de2054bc93241b2263
    * SHA-256: deeac56026f3804968348c8afa5b7aba10900aeabee05751c0fcac2b88cff71e
  - Filetype
    * PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
  - Filesize
    * 176128 Bytes (172K)
  - Compile time
    * Mon Nov 26 04:46:01 2012

- Sample F - UAC circumvention
  - Description
    * File temporarily created on filesystem
  - Original filename

    * UAC.TMP
  - Hashes
    * MD5: 52df5c2c07433e2a8f054c2347acb3b4
    * SHA1: 8051474c1fc0d8f404a42ea32eca1699e54f02e1
    * SHA-256: dc09091e5d0ce03c6144748f17bd636f2f0b2ca56f88b550c1d48860596dbdb1
  - Filetype
    * PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
  - Filesize
    * 2560 Bytes (2.5K)
  - Compile time
    * Thu Mar 29 08:03:43 2012

2.1 Limitations

This work has been done with utmost care, following best practices in software reversing, forensic investigations and/or information gathering. However, the work is only covering small aspects (based on the indicators given, lacking full context) and not an exhaustive analysis, and hence the report is as-is, not giving any guarantees of completeness or claiming absolute accuracy. This work is provided for information only.

2.2 Sharing

The document is classified as TLP:WHITE, CIRCL authorizes everyone to share this analysis report as-is without modification.

3 Executive summary

The analyzed malicious software is an exhaustive Remote Access Tool (RAT) that defeats several protection methods of modern Windows operating systems, including execution of signed code and defeating UAC in Windows 7. It comes with a multitude of functionalities that are well implemented.

4 Analysis

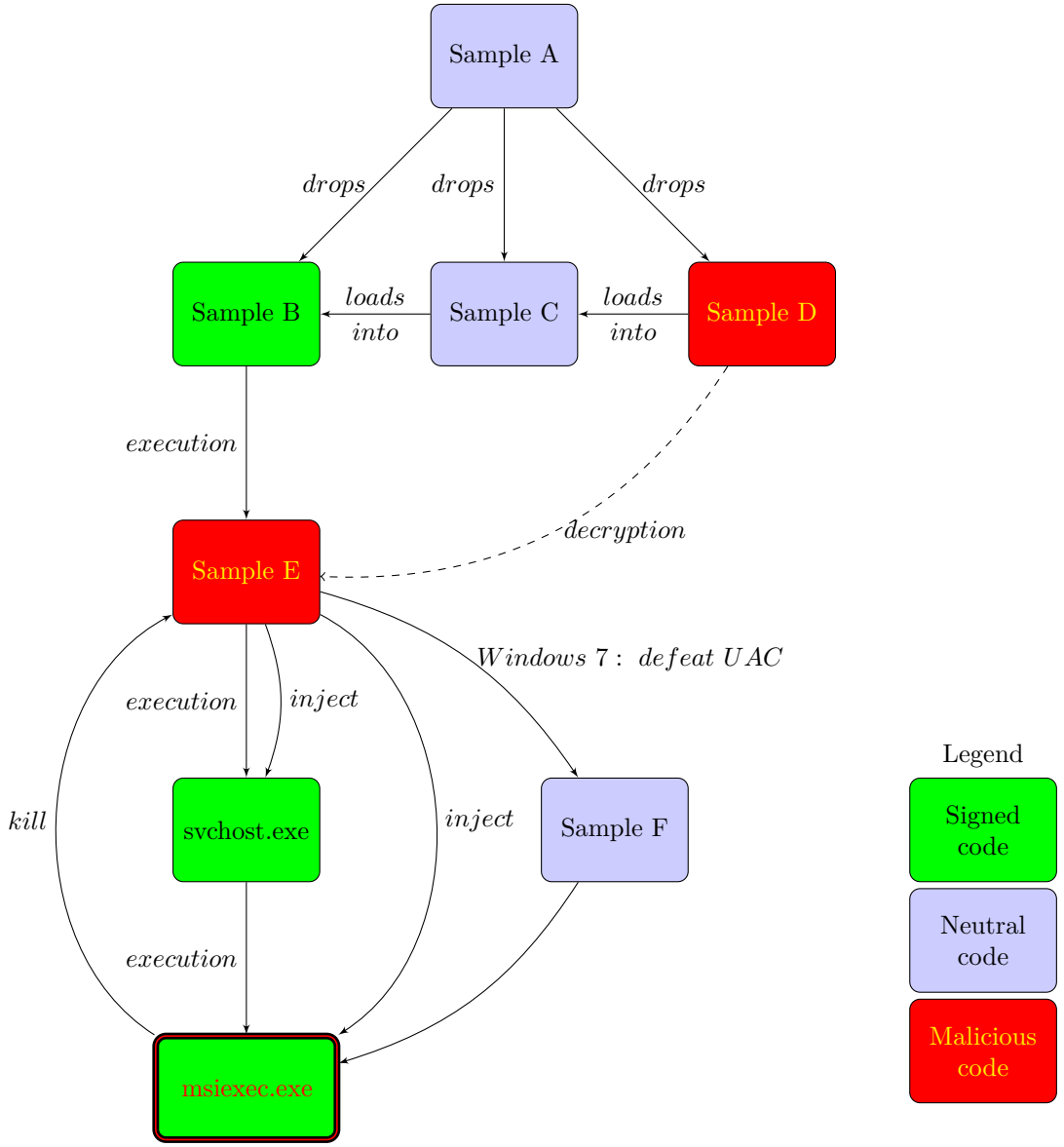
4.1 Techniques used

The analysis has been done using a mixed-approach of dynamic analysis and static analysis in order to overcome some of the obfuscation and encryptions used by the malware. Some of the techniques might have also an impact on the interpretation of the malware. Unfortunately, when we started this investigation, the IP address is no longer accepting connections on the given ports when tested on 2013-03-26. An interaction following the protocol of this malware is therefore no longer possible.

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

4.2 Execution process

4.2.1 Diagram



4.2.2 Explanation

Sample A is a self-extracting archive which contains three files, Sample B, Sample C and Sample D. It is assumed that Sample A is a part of another attack vector, like PDF or Office document attacks where the user just opens a crafted document which exploits the document reader, drops and opens both a readable document and a malicious file like Sample A.

```
1 Type = Rar
2 Solid = -
```


CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
Blocks = 3
Multivolume = -
Volumes = 1

    Date        Time     Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2009-05-14  00:56:12 ....A       262672       119784  mcvsmap.exe
2013-03-13  09:52:28 ....A        49152        20285  McUtil.DLL
2013-03-13  14:56:12 ....A       124820       124820  McUtil.DLL.PPT
------------------- ----- ------------ ------------  ------------------------
                             436644       264889  3 files, 0 folders
```

Executing the self-extracting archive extracts the files and runs mcvsmap.exe (Sample B). Sample B is a valid signed file that the author of the malware took from a software bundle from McAfee. Sample B, when executed, attempts to load a file McUtil.DLL from the same directory, which usually is another component of McAfee. The malware author instead bundled the valid McAfee file Sample B with a custom DLL (Sample C). Since the file will be loaded without hesitation (there are no protection mechanisms implemented; neither does McAfee check if the imported file meets any conditions nor is any protection implemented for loading unsigned libraries in signed code), the signed Sample B jumps into the beginning of the code section of Sample C (via Push/Return):

```
.text:0040465E add     esp, 0Ch
.text:00404661 lea     eax, [ebp+88h+LibFileName]      ; McUtil.dll
.text:00404664 push    eax                             ; lpLibFileName
.text:00404665 call    ds:LoadLibraryA
.text:0040466B push    0FFFFFFFFh
.text:00404670 push    offset start_of_mciutil_dll
.text:00404675 retn
.text:00404676 ; ---------------------------------------------------------------------------
```

At the target location the following code is executed:

```
read_execute_file()
{
  NumberOfBytesRead = GetModuleFileNameW(hModule, &filename, 0x2000u);
  lstrcatW(&filename, L".PPT");
  hFile_mcutil.dll.ppt = CreateFileW(&filename, GENERIC_READ, 1u, 0, OPEN_EXISTING, 0,
      0);
  if ( hFile_mcutil.dll.ppt == -1 )
  {
    result = GetLastError();
  }
  else
  {
    buffer = VirtualAlloc(0, 0x100000u, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    if ( buffer && ReadFile(hFile_mcutil.dll.ppt, buffer, 0x100000u, &NumberOfBytesRead
        , 0) )
    {
      CloseHandle(hFile_mcutil.dll.ppt);
      buffer();
      Sleep(0xFFFFFFFF);
      Sleep(0xFFFFFFFF);
      Sleep(0xFFFFFFFF);
      result = 0;
    }
    else
    {
      result = GetLastError();
```


CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
25      }
26    }
27    return result;
28  }
```

The code retrieves the filename of itself (line 3), which is McUtil.DLL, and appends .PPT (line 4). A handle to the filename McUtil.DLL.PPT is created in line 5. In line 12 an exectuable memory region is created, which is filled with the content of the file McUtil.DLL.PPT (line 13). After closing the handle to the file (line 15), the memory region is called (line 16). The next screenshot shows that the memory contains only pure code without any overhead like MZ/PE headers. The entropy of this file is 7.997904 bits per byte:

```
00C40000 cmp     edx, 0CBE1F4B7h
00C40006 test    edx, 0FF2A2004h
00C4000C xor     esi, 0BBE5876Fh
00C40012 dec     edx
00C40013 xor     edx, 2EA8D3E3h
00C40019 cmp     edi, 45B286E4h
00C4001F and     esi, 0A05A96A4h
00C40025 inc     edx
00C40026 mov     edi, 2BFCC370h
00C4002B cmp     edi, 0A347050Bh
00C40031 cmp     esi, 3646EDD4h
00C40037 mov     edx, 9C72B29Ah
00C4003C call    $+5
00C40041 test    esi, 760A483Dh
00C40047 dec     esi
00C40048 and     edx, 0BB03BC9h
00C4004E or      edi, 0BE8D653Ah
00C40054 and     edi, 0CF84EF63h
00C4005A or      esi, 44A352FBh
00C40060 and     edx, 231692BEh
00C40066 and     edi, 92FA77C5h
00C4006C and     edi, 0C537FF3Bh
00C40072 pop     eax
00C40073 add     esi, 5F409FE1h
00C40079 dec     edi
00C4007A or      edx, 0F77945A9h
00C40080 cmp     edx, 64CCDD6Dh
00C40086 add     esi, 808BF208h
00C4008C cmp     edx, 6CD05232h
00C40092 dec     esi
00C40093 cmp     edx, 0F3F3B05Ah
00C40099 mov     edi, 49319D2Ah
00C4009E sub     edx, 0F80B7589h
00C400A4 cmp     esi, 0F5C87C7Ah
00C400AA add     edx, 0FC22F58Eh
```

The code, when executed, reveals the first hint about what we found:

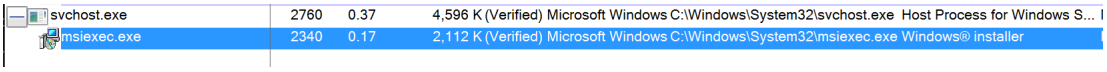
```
00C406A1 mov     [esi+10h], eax
00C406A4 mov     eax, [ebp+arg_10]
00C406A7 mov     [esi+14h], eax
00C406AA mov     eax, [ebp+arg_14]
00C406AD mov     [esi+18h], eax
00C406B0 mov     dword ptr [esi], 'PLUG'
00C406B6 mov     eax, [edi+28h]
00C406B9 add     eax, esi
00C406BB mov     [esi+1Ch], eax
```

It decompresses and decrypts itself, using the Microsoft API call RtlDecompressBuffer and the custom decryption routine:

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
1  int crypt(unsigned int a1, int a2, int a3, int a4)
2  {
3    if ( a4 > 0 )
4    {
5      v10 = a3 - a2;
6      do
7      {
8        a1 = a1 + (a1 >> 3) - 0x11111111;
9        a1 = a1 + (a1 >> 5) - 0x22222222;
10       a1 += 0x44444444 - (a1 << 9);
11       a1 += 0x33333333 - (a1 << 7);
12       v7 = *(v10 + a2++) ^ (a1 + a1 + a1 + a1);
13       v8 = a4-- == 1;
14       *(a2 - 1) = v7;
15     }
16     while ( !v8 );
17   }
18   return 0;
19 }
```

The decrypted and decompressed file is not written onto disk, it always remains in memory. Sample E is the extracted version of this memory segment. At this point it can be mentioned that neither the encrypted Sample D nor the decrypted memory segment Sample E are detected by Virus scanners.
After some initialisation work like adjusting tokens (SeDebugPrivilege, SeTcbPrivileg[6] , to act as part of the operating system), a new process is started, the original svchost.exe from Microsoft, and the code from Sample E is injected into the memory of that process. In a next step, svchost.exe is instructed to execute the original msiexec.exe from Microsoft, where also memory is injected like it has been done for svchost.exe. Special conditions apply when run under Window 7, which is protected by User Account Control (UAC). UAC is supposed to protect the user better from running malware by requesting the administator for approval before running a potentially dangerous application. In the environment of Windows 7, the malware drops temporarily file Sample F, which it uses to evade or defeat the UAC mechanism. After killing the parent processes, only two processes are left: svchost and msiexec. Both are verified binaries, none of the includes a malicious DLL.



Nevertheless, they both contain the malicious code. At this point in time the malware is already talking to the C&C, no user interaction was required, all standard security mechanisms were defeated.

4.3 Implemented commands

The analysis of Sample B revealed the commands as shown in the table below:

[6] http://technet.microsoft.com/en-us/library/bb457125.aspx

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

Table 1: Implemented commands

Source file	Internal command	subcommand	Description
XPlugOption.cpp	Option	0x2000	lock workstation
		0x2001	shutdown workstation (forced)
		0x2002	reboot workstation
		0x2003	shutdown workstation (graceful)
		0x2005	show messagebox
XPlugDisk.cpp	Disk	0x3000	enumerate drives
		0x3001	find file
		0x3002	find file recursively
		0x300A	create directory
		0x3004	read file
		0x3007	write file
		0x300D	file copy/rename/delete/move
		0x300C	create process on hidden desktop
		0x300E	get expanded environment string
XPlugScreen.cpp	Screen	0x4000	Remote Desktop capabilities
		0x4004	send mouse event
		0x4005	send keyboard event
		0x4006	send CTRL-Alt-Delete
		0x4100	take screenshot
XPlugProcess.cpp	Process	0x5000	create process
		0x5001	enumerate processes
		0x5002	kill process
XPlugService.cpp	Service	0x6000	query service config
		0x6001	change service config (forced)
		0x6002	start service
		0x6003	control service
		0x6004	delete service
XPlugShell.cpp	Shell	0x7002	start a cmd shell
XPlugTelnet.cpp	Telnet	0x7100	start telnet server
XPlugRegedit.cpp	RegEdit	0x9000	enumerate keys
		0x9001	create key
		0x9002	delete key
		0x9003	copy key
		0x9004	enumerate values
		0x9005	set value
		0x9006	delete value
		0x9007	get value
XPlugNethood.cpp	Nethood	0xA000	enumerate network resources
XPlugPortMap.cpp	Portmap	0xB000	starts port mapping
XPlugSQL.cpp	SQL	0xC000	get data source information
		0xC001	get driver description
		0xC002	execute statement
XPlugNetstat.cpp	Netstat	0xD000	get TCP table
		0xD001	get UDP table
		0xD002	set TCP entry
XPlugKeyLogger.cpp	Keylogger	0xE000	starts key logger thread

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

4.4 Command details

4.4.1 Option

XPlugOption implements commands to lock the workstation, shut it down or reboot it. In addition, XPlugOption can create a thread that calls MessageBoxW() in order to present a message box to the user.

4.4.2 Disk

XPlugDisk is used to enumerate connected disk drives and can be used to find and manipulate files and directories. In addition, XPlugDisk can be used to create a process, optionally on a hidden Windows desktop with the name "HH", as the code below illustrates:

```
1  if ( a1->hidden )
2   {
3     hDesktop = CreateDesktopW(L"HH", 0, 0, 0, 0x10000000u, 0);
4     if ( !hDesktop )
5       log("XPlugDisk.cpp", 665, 0);
6   }
7   hidden = a1->hidden;
8   StartupInfo.lpDesktop = (hidden != 0 ? L"HH" : 0);
9   StartupInfo.cb = 68;
10  StartupInfo.dwFlags = 1;
11  StartupInfo.wShowWindow = hidden == 0;
12  if ( CreateProcessW(0, &a1->commandline, 0, 0, 0, 0, 0, 0, &StartupInfo, &
        ProcessInformation) )
13  {
14  ...
15  }
```

4.4.3 Screen

XPlugScreen is not only taking screenshots, it is also implementing remote desktop capabilities. It is able to capture the screen (internal command: ScreenT1) and can send mouse and keyboard events (internal command: ScreenT2).

4.4.4 Process

XPlugProcess implements three commands and is able to enumerate, create and kill processes.

4.4.5 Service

In the module XPlugService commands are available related to Windows services. Code is implemented to query service configurations, change service configuration, start, control and delete services.

4.4.6 Shell

A remote shell for the attacker is created in the module XPlugShell, by creating an asynchronous set of pipes (\pipe\a and \pipe\b) for cmd.exe and the console attached to it (AttachConsole()).

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

4.4.7 Telnet

cmd.exe /Q is executed in the module XPlugTelnet in order to start a telnet server on the attacked machine.

4.4.8 RegEdit

XPlugRegedit implements a set of commands to process the Windows registry. It is able to enumerate, create, delete and copy keys. It is also able to enumerate, set, delete and get values from the registry.

4.4.9 Nethood

XPlugNethood is the module to enumerate network resources like network shares.

4.4.10 Portmap

XPlugPortMap indicates that it performs some port mapping, however, the code is not understood, yet.

4.4.11 SQL

XPlugSQL implements three functions to query SQL servers: a function to get data source information, a function to get the driver description and a function to execute SQL statements.

4.4.12 Netstat

XPlugNetstat gets the TCP and UDP connection table and is able to set TCP table entries.

4.4.13 Keylogger

The keylogger implemented in XPlugKeyLogger catches Window titles, date, time and logs entered keys into the file

```
1 C:\Documents and Settings\All Users\VirusMap\NvSmart.hlp
```

It has the format following the example below:

```
1 2013-03-26 09:40:57 | C:\Program Files\Mozilla Firefox\firefox.exe - Mozilla Firefox
2 www.google.com
3
4 2013-03-26 09:47:49 | C:\WINDOWS\system32\notepad.exe | Untitled - Notepad
5 This is not a password
6
7 2013-03-26 09:48:06 | C:\WINDOWS\Explorer.EXE | C:\Documents and Settings\All Users\
      VirusMap
```

4.5 Other notable commands and functions

4.5.1 log

This function is called almost everywhere when the author expects that a functions returns an error, at 1036 places. This is obviously done to ensure code quality.

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
write_log(LPCWSTR lpBuffer)
{
  ExpandEnvironmentStringsW(L"%ALLUSERSPROFILE%", &path_to_bug.log, 0x800u);
  // %ALLUSERSPROFILE%\SxS\bug.log
  lstrcatW(&path_to_bug.log, L"\\SxS");
  CreateDirectoryW(&path_to_bug.log, 0);
  SetFileAttributesW(&path_to_bug.log, 6u);
  lstrcatW(&path_to_bug.log, L"\\bug.log");
  result = CreateFileW(&path_to_bug.log, 0x40000000u, 1u, 0, 4u, 2u, 0);
  if ( result != -1 )
  {
    if ( SetFilePointer(result, 0, 0, 2u) != -1 )
    {
      GetLocalTime(&SystemTime);
      NumberOfBytesWritten = wsprintfW(
                               &Buffer,
                               L"%4.4d-%2.2d-%2.2d %2.2d:%2.2d:%2.2d: ",
                               SystemTime.wYear,
                               SystemTime.wMonth,
                               SystemTime.wDay,
                               SystemTime.wHour,
                               SystemTime.wMinute,
                               SystemTime.wSecond);
      if ( WriteFile(result, &Buffer, 2 * NumberOfBytesWritten, &NumberOfBytesWritten,
           0) )
      {
        len = lstrlenW(lpBuffer);
        WriteFile(result, lpBuffer, 2 * len, &len, 0);
      }
    }
    result = CloseHandle(result);
  }
  return result;
}
```

Example log file entries from file

```
%ALLUSERSPROFILE%\SxS\bug.log
```

```
2013-03-25 11:43:28: file: XSetting.h, line: 57, error: [1300]Not all privileges
    referenced are assigned to the caller.
2013-03-25 11:51:12: file: XInstallUAC.cpp, line: 162, error: [5]Access is denied.
2013-03-25 13:59:45: file: XRTL.cpp, line: 186, error: [1300]Not all privileges
    referenced are assigned to the caller.
2013-03-25 14:07:12: file: XRTL.cpp, line: 186, error: [123]The filename, directory
    name, or volume label syntax is incorrect.
2013-03-25 14:07:12: file: XSetting.h, line: 58, error: [3]The system cannot find the
    path specified.
2013-03-25 14:21:12: file: dllmain.cpp, line: 47, error: [1300]Not all privileges
    referenced are assigned to the caller.
2013-03-25 17:31:58: file: XInstall.cpp, line: 451, error: [5]Access is denied.
2013-03-25 17:37:00: file: XSoTcpHttp.cpp, line: 646, error: [12029]*
```

In addition an exception filter is installed to fetch the circumstances of otherwise not caught errors:

```
TopLevelExceptionFilter(struct_a1_30 *a1)
{
...
  if ( wsprintfA(
         &OutputString,
```


CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
6           "EName:%s,EAddr:0x%p,ECode:0x%p,EAX:%p,EBX:%p,ECX:%p,EDX:%p,ESI:%p,EDI:%p,EBP
                :%p,ESP:%p,EIP:%p\r\n",
7           &String1,
8           a1->ECode[3],
9           *a1->ECode,
10          v6->reg_eax,
11          v6->reg_ebx,
12          v6->reg_ecx,
13          v6->reg_edx,
14          v6->reg_esi,
15          v6->reg_edi,
16          v6->reg_ebp,
17          v6->reg_esp,
18          v6->reg_eip) >= 256 )
19      log("XException.cpp", 39, 0);
20    call_write_log(&OutputString);
21    call_OutputDebugStringA(&OutputString);
22  ...
23  }
```

4.6 Persistency

The three files Sample B, C and D are copied into the directory

```
1 C:\Documents and Settings\All Users\VirusMap
```

respectively in

```
1 C:\ProgramData\VirusMap (C:\Users\All Users\VirusMap)
```

After that, a new registry entry is set:

```
1 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

which calls mcvsmap.exe (Sample B) after login.

Another option is the installation as a service in

```
1 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VirusMap
```

The key "Imagepath" calls the same binary mcvsmap.exe (Sample B).

4.7 Control

The attacked computer uses TCP and UDP to connect to port 443 on help.yahoo-upgrade.com (122.199.194.197). Unfortunately, the machine at that IP address doesn't seem to reply to our requests anymore on 2013-03-26.
The Passive DNS showed some other associated domains and hostnames with this IP address:

```
1  help.yahoo-upgrade.com
2  support.yahoo-upgrade.com
3  update.ayuisyahooapis.com
4  support.ayuisyahooapis.com
5  update.trendmicrosoft.co.in
```

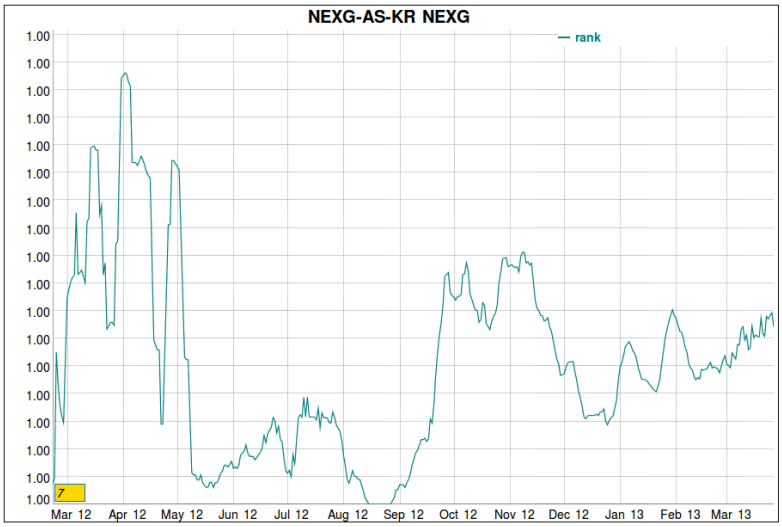
It's highly probable that theses hostnames were also used for other campaigns. You might use these as additional indicators for the detection of potential infections.

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

4.8 Network and domain information

4.8.1 Network

The IP address is located in the ASN 17877 and the ISP is not a known bulletproof hoster as you can see on its historical[7] BGP ranking evolution.




```
inetnum:        122.199.128.0 - 122.199.255.255
netname:        VAAN
descr:          NexG
descr:          5F SeoulAcademy B/D, 967-6 Daechi-Dong, Gangnam-Gu, 135-280
descr:          ************************************************
descr:          Allocated to KRNIC Member.
descr:          If you would like to find assignment
descr:          information in detail please refer to
descr:          the KRNIC Whois Database at:
descr:          "http://whois.nic.or.kr/english/index.html"
descr:          ************************************************
country:        KR
admin-c:        SL1625-AP
tech-c:         SL1625-AP
remarks:        www.nexg.net
status:         ALLOCATED PORTABLE
mnt-by:         MNT-KRNIC-AP
mnt-lower:      MNT-KRNIC-AP
changed:        hm-changed@apnic.net 20060606
source:         APNIC

person:         Sanguk Lee
nic-hdl:        SL1625-AP
e-mail:         ip@nexg.net
address:        5F SeoulAcademy B/D, 967-6 Daechi-Dong, Gangnam-Gu, 135-280
phone:          +82-2-538-7060
fax-no:         +82-2-571-8998
country:        KR
changed:        hostmaster@nida.or.kr 20050105
```

[7] http://bgpranking.circl.lu/asn_details?asn=17877

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
mnt-by:         MNT-KRNIC-AP
source:         APNIC

inetnum:        122.199.128.0 - 122.199.255.255
netname:        VAAN-KR
descr:          NexG
country:        KR
admin-c:        LS151-KR
tech-c:         LS151-KR
status:         ALLOCATED PORTABLE
mnt-by:         MNT-KRNIC-AP
mnt-irt:        IRT-KRNIC-KR
remarks:        This information has been partially mirrored by APNIC from
remarks:        KRNIC. To obtain more specific information, please use the
remarks:        KRNIC whois server at whois.krnic.net.
changed:        hostmaster@nic.or.kr
source:         KRNIC
```

4.8.2 Domain

```
   Domain Name: YAHOO-UPGRADE.COM
     Registrar: JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD
     Whois Server: whois.55hl.com
     Referral URL: http://www.55hl.com
     Name Server: DNS5.4CUN.COM
     Name Server: DNS6.4CUN.COM
     Status: ok
     Updated Date: 08-aug-2012
     Creation Date: 18-jul-2011
     Expiration Date: 18-jul-2013

>>> Last update of whois database: Wed, 27 Mar 2013 22:36:13 UTC <<<

Domain Name: yahoo-upgrade.com

Registrant Contact:
yahoo
yahoo yahoo whiteyoo_123@yahoo.com
telephone: +48.56756756756
fax: +48.56732453453
yahoo yahoo yahoo 345345
CA

Administrative Contact:
yahoo yahoo whiteyoo_123@yahoo.com
telephone: +48.56756756756
fax: +48.56732453453
yahoo yahoo yahoo 345345
CA

Technical Contact:
yahoo yahoo whiteyoo_123@yahoo.com
telephone: +48.56756756756
fax: +48.56732453453
yahoo yahoo yahoo 345345
CA

Billing Contact:
yahoo yahoo whiteyoo_123@yahoo.com
telephone: +48.56756756756
```


CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
fax: +48.56732453453
yahoo yahoo yahoo 345345
CA
```

4.9 Current version and history of PlugX

A version string can be found in this binary:

```
d:\work\plug7.0(mcvsmap)(fking)j()\shellcode\shellcode\XPlug.h
```

This could mean PlugX, version 7.0 codename fking, build for mcvsmap. References can be found on the internet for previous versions of this malware family:

```
d:\work\plug4.0(nvsmart)(sxl)\shellcode\shellcode\XPlug.h
d:\work\plug3.1(icesword)\shellcode\shellcode\XPlug.h
d:\work\Plug3.0(Gf)UDP\Shell6\Release\Shell6.pdb
i:\work\plug2.0()\shellcode\shellcode\XPlug.h
```

A Appendix

A.1 Indicators of Compromise (IOC)

This section summarizes the known indicators of compromise. The list might not be exhaustive, but the existence of any or all of the following indicators might help to discover an infection.

A.1.1 Pipes

```
  \PIPE\a$PID
  \PIPE\b$PID
  \PIPE\RUN_AS_USER($PID)
```

(where $PID is the process ID of the active malicious process)

A.1.2 Files and directories

- Static files (dropped files)
  - update.exe

```
MD5:      f1f48360f95e1b43e9fba0fec5a2afb8
SHA1:     70ceb467db7b0161d22e4545479f747417b9705a
SHA-256:  2bc5ce39dd9afe2157448d3f6d8cb9c549ed39543d159616e38480b9e6c11c49
```

  - mcvsmap.exe

```
MD5:      4e1e0b8b0673937415599bf2f24c44ad
SHA1:     9224de3af2a246011c6294f64f27206d165317ba
SHA-256:  ae16e10e621d6610a3f7f2c7122f9d1263700ba02d1b90e42798decb2fe84096
```

  - McUtil.DLL

```
MD5:      ad4a646b38a482cc07d5b09b4fffd3b3
SHA1:     ae0f9bf2740d00c5d485827eb32aca33feaa3a90
SHA-256:  0a99238e1ebebc47d7a89b2ccddfae537479f7f77322b5d4941315d3f7e5ca48
```


CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

– McUtil.DLL.PPT

```
MD5:      545bb4365a9b7cdb6d22844ebeedda93
SHA1:     a267f1183b4ff843d68a63264846abf78cc71d1f
SHA-256:  d4fe890a08d4dd44b58a3b85b2a7e89536338099c1c42a9b7e85f4007b0a37b7
```

– UAC.TMP

```
MD5:      52df5c2c07433e2a8f054c2347acb3b4
SHA1:     8051474c1fc0d8f404a42ea32eca1699e54f02e1
SHA-256:  dc09091e5d0ce03c6144748f17bd636f2f0b2ca56f88b550c1d48860596dbdb1
```

Files and/or directories might be hidden and carry the system flag

```
C:\ProgramData\VirusMap (Windows 7)
C:\Users\All Users\VirusMap (Windows 7)
C:\Documents and Settings\All Users\VirusMap (Windows XP)
%ALLUSERSPROFILE%\SxS\bug.log
C:\Documents and Settings\All Users\VirusMap\NvSmart.hlp
```

A.1.3 Registry

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VirusMap and a key referencing Sample B
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run and a key referencing Sample B
```

A.1.4 Network (hostname and destination IP addresses)

```
help.yahoo-upgrade.com
122.199.194.197
```

A.2 References

- WHITE PAPER: PLUG X - PAYLOAD EXTRACTION
  - http://www.contextis.com/files/PlugX_-_Payload_Extraction_March_2013_1.pdf
  - Context Information Security - http://www.contextis.com/
  - Published 2013-03-22
- An Analysis of PlugX
  - http://lastline.com/blog.php
  - Lastline - http://www.lastline.com/
  - no publication date found
- PlugX is becoming mature
  - http://www.securelist.com/en/blog/208193974/PlugX_is_becoming_mature
  - Kaspersky Lab - http://www.kaspersky.com/

  - Published 2012-11-27

- Unplugging PlugX Capabilities
  - http://blog.trendmicro.com/trendlabs-security-intelligence/unplugging-plugx-capabilities
  - TrendMicro - http://www.trendmicro.eu/
  - Published 2012-09-17

- Tracking down the author of the PlugX RAT
  - http://labs.alienvault.com/labs/index.php/2012/tracking-down-the-author-of-the-plugx-ra
  - AlienVault - http://labs.alienvault.com
  - Published 2012-09-13

A.3 VirusTotal results

- Sample A

```
MicroWorld-eScan:       Trojan.Agent.AZDK
nProtect:               Trojan.Agent.AZDK
McAfee:                 RDN/Generic BackDoor!gq
Malwarebytes:           Trojan.Dropper.CH
Symantec:               WS.Reputation.1
Norman:                 Agent.APIJH
TrendMicro-HouseCall:   BKDR_POISON.PQ
Avast:                  Win32:Gulpix-B [Trj]
Kaspersky:              Backdoor.Win32.Gulpix.bo
BitDefender:            Trojan.Agent.AZDK
Agnitum:                Backdoor.Gulpix!EFaRR6zLtc4
ViRobot:                Backdoor.Win32.A.Gulpix.370702.B
Comodo:                 UnclassifiedMalware
F-Secure:               Trojan.Agent.AZDK
DrWeb:                  Trojan.Click2.52215
VIPRE:                  Trojan.Win32.Generic!BT
AntiVir:                TR/Agent.azdk.3
TrendMicro:             BKDR_POISON.PQ
McAfee-GW-Edition:      RDN/Generic BackDoor!gq
Sophos:                 Troj/Agent-AATT
Kingsoft:               Win32.Hack.Gulpix.(kcloud)
Microsoft:              Backdoor:Win32/Plugx.A
GData:                  Trojan.Agent.AZDK
AhnLab-V3:              Backdoor/Win32.Gulpix
Ikarus:                 Backdoor.Win32.Gulpix
Fortinet:               W32/Gulpix.BO!tr.bdr
AVG:                    Agent4.AKAP
Panda:                  Trj/CI.A
Scanned: 2013-03-21 04:01:12 - 45 scans - 28 detections (62.0%)
```

- Sample B (mcvsmap.exe)

```
Scanned: 2013-03-21 13:29:45 - 44 scans - 0 detections (0.0%)
```

- Sample C (McUtil.DLL)

CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu

```
MicroWorld-eScan:       Trojan.Agent.AZDK
nProtect:               Trojan.Agent.AZDK
McAfee:                 RDN/Generic BackDoor!gt
Malwarebytes:           Backdoor.Gulpix
Symantec:               WS.Reputation.1
Norman:                 Agent.APIJH
TrendMicro-HouseCall:   TROJ_GEN.RCBCRCJ
Avast:                  Win32:Gulpix-B [Trj]
Kaspersky:              Backdoor.Win32.Gulpix.bo
BitDefender:            Trojan.Agent.AZDK
Agnitum:                Backdoor.Gulpix!EFaRR6zLtc4
Comodo:                 UnclassifiedMalware
F-Secure:               Trojan.Agent.AZDK
DrWeb:                  Trojan.Click2.52215
VIPRE:                  Trojan.Win32.Generic!BT
AntiVir:                TR/Agent.azdk.2
TrendMicro:             TROJ_GEN.RCBCRCJ
McAfee-GW-Edition:      RDN/Generic BackDoor!gt
Sophos:                 Troj/Agent-AATT
Microsoft:              Backdoor:Win32/Plugx.A
GData:                  Trojan.Agent.AZDK
Commtouch:              W32/Backdoor.IYCB-5867
Ikarus:                 Backdoor.Win32.Gulpix
Fortinet:               W32/Gulpix.BO!tr.bdr
AVG:                    Agent4.AKAP
Panda:                  Trj/CI.A
Scanned: 2013-03-21 13:46:10 - 44 scans - 26 detections (59.0%)
```

- Sample D (McUtil.DLL.PPT)

```
Not uploaded to VirusTotal.
```

- Sample E

```
Not uploaded to VirusTotal.
```

- Sample F (UAC.TMP)

```
Panda:                  Suspicious file
Scanned: 2012-09-20 02:33:55 - 43 scans - 1 detections (2.0%)
```


CIRCL - Computer Incident Response Center Luxembourg
c/o smile - "security made in Lëtzebuerg" GIE
41, avenue de la gare, L-1611 Luxembourg
(+352) 247 88444 - info@circl.lu – www.circl.lu