National Cyber Security Centre
a part of GCHQ

COLDSTEEL

Malware Analysis Report

Version 1.1

A fully featured Windows remote access tool.

31 January 2023

National Cyber Security Centre
a part of GCHQ

COLDSTEEL

A fully featured Windows remote access tool.

Executive summary

- COLDSTEEL provides interactive desktop & command line invocation, functionality including the ability to copy files, take screenshots and simulate user input.
- COLDSTEEL persists as a Windows service.
- COLDSTEEL communicates with the C2 server using a raw TCP connection.

Introduction

This report covers technical analysis of the COLDSTEEL malware previously reported on by Ahnlab[1] and Fortinet[2]. One of the samples described in this report was identified on a UK network in 2022, many similar samples have also been identified in public malware repositories.

COLDSTEEL is a Windows Remote Access Tool providing interactive desktop & command line invocation capabilities. Several variants have been identified, most expose similar functionality to one-another. Many of the variants may be easily distinguished by an ID string such as `MileStone2016`, `MileStone2017` or `FBI20111024` used in their network communications. These names will be used throughout this report to draw distinction between the variants but should not be taken as a comment on the age of the samples. In the same way, the `FBI20111024` variant name should not be taken as an indicator of attribution. This report will focus on the more recently observed `MileStone` variants and draw comparisons to an `FBI20111024` sample. Other variants have also been observed but for brevity these are not included in this report.

COLDSTEEL is routinely obfuscated using the Themida packer[3]. More details about this are available in Defence evasion (Themida).

1 https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=29904&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

2 https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits

3 https://www.oreans.com/Themida.php

National Cyber Security Centre
a part of GCHQ

Malware details

Metadata

Filename	newdev.dll
Description	Themida-protected MileStone2017 variant of COLDSTEEL seen on a UK victim.
Size	2,558,703 bytes
MD5	ca1575ce6131735f7e8e1309b657a626
SHA-1	54153b749c06dbf2d7d2eaea2bbebf00f6d0b54b
SHA-256	968d26244b3243a25c66170900b815123469822385cab610267c3a65e755d1ba
Compile time	05 Jul 2017, 13:09:02 UTC

Filename	newdev.dll
Description	MileStone2017 variant of COLDSTEEL.
Size	24,064 bytes
MD5	8f57ce99d53addabec1d964cd34c96f4
SHA-1	b4a9ab6e040c88630ea46a2ae4ff41a558366122
SHA-256	e92d4e58dfae7c1aadeef42056d5e2e5002814ee3b9b5ab1a48229bf00f3ade6
Compile time	05 Jul 2017 13:09:02 UTC

Filename	newdev.dll
Description	Themida-protected MileStone2017 variant of COLDSTEEL. Uses a unique IP, different service name and unique Themida version.
Size	2,411,520 bytes
MD5	53fa0c94678fabf711802009452b521b
SHA-1	9ec69a042106fc9d27a27197d3b680b468bca9a0
SHA-256	7ce2909bf205c1a574ac3dcac5891e31aa59dd4cad6c41d7159ad017c837903c
Compile time	Wed, 05 Jul 2017 13:09:02 GMT UTC

Filename	newdev.dll
Description	MileStone2016 variant of COLDSTEEL with different service properties.
Size	26,624 bytes
MD5	bb40bbbd3b69e0eb802c42d2506b6754
SHA-1	bf80e329cba134ccd96f9572d2c0bf250515c26e
SHA-256	a9fa8e8609872cdcea241e3aab726b02b124c82de4c77ad3c3722d7c6b93b9b5
Compile time	Sat, 16 Jul 2016 07:34:43 UTC

Filename	newdev.dll
Description	MileStone2016 variant of COLDSTEEL.
Size	26,576 bytes
MD5	c5cf6e70d5a5c489aa1c0326799dbe90
SHA-1	a94ed3d673261d62f2959979272d8c8d17e6e7f3
SHA-256	14930488158df5fca4cba80b1089f41dc296e19bebf41e2ff6e5b32770ac0f1e
Compile time	17 Jul 2016 07:04:17 UTC

National Cyber Security Centre
a part of GCHQ

Filename	newdev.dll
Description	FBI20111024 variant of COLDSTEEL.
Size	66,392 bytes
MD5	25d2eeb36e729679e5e6c647a306850f
SHA-1	3c365d907dc9f06d19dd192e92ebeeefb8e8c964
SHA-256	50838e12e58a2d96b1a2ebdb53a25151cc22cbd458dba49fcb355ccfc82e0e63
Compile time	04 May 2011 10:48:19 UTC

National Cyber Security Centre
a part of GCHQ

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	COLDSTEEL can run arbitrary commands using `cmd.exe`.
	T1569.002	System Services: Service Execution	COLDSTEEL executes malicious code as a Windows service.
Persistence	T1543.003	Create or Modify System Process: Windows Service	COLDSTEEL creates an autostart service to persist after a system reboot.
Initial Access	T1190	Exploit Public-Facing Application	COLDSTEEL is believed to have been deployed following exploitation of Log4j.
Defense Evasion	T1027.002	Obfuscated Files or Information: Software Packing	`MileStone2017` variants of COLDSTEEL have been observed to be packed using Themida as described in Defence Evasion (Themida).
	T1112	Modify Registry	COLDSTEEL modifies registry keys directly to add a description to its service.
	T1070.004	Indicator Removal: File Deletion	COLDSTEEL has the ability to delete files from the infected machine.
	T1134.002	Access Token Manipulation: Create Process with Token	The `MileStone2016` variant of COLDSTEEL has the ability to create a process as the user named `ANONYMOUS`.
Discovery	T1082	System Information Discovery	COLDSTEEL collects a range of system information from the infected machine.
	T1083	File and Directory Discovery	COLDSTEEL has commands to enumerate the filesystem.
	T1057	Process Discovery	`FBI20111024` variants of COLDSTEEL have the ability to collect process information.
Command and Control	T1095	Non-Application Layer Protocol	COLDSTEEL communicates over TCP sockets, using a custom message format.

Functionality

Overview

COLDSTEEL sets up persistence using a Windows service as described in Functionality (Persistence), while running as this service COLDSTEEL performs a basic system survey, the information is then beaconed out to the C2 server over raw TCP. Additional tasking can then be received from the C2 server which COLDSTEEL performs, sending results back to the C2 server.

Persistence

COLDSTEEL maintains persistence using a Windows service. The observed variations in service properties defined by the actor are shown in the following Tables.

Name	Description
Name	Name
Binary Path Name	`C:\Windows\System32\svchost.exe -k alg`
Display Name	Disp
Description	Desc
Service DLL	`C:\Users\<user>\AppData\Roaming\newdev.dll`

Table 1: shows an example of the service created by a `MileStone2016` variant of COLDSTEEL

Name	Description
Name	msupdate
Binary Path Name	`C:\Windows\System32\svchost.exe -k msupdate`
Display Name	Microsoft Update
Description	Enables the download and installation of Windows updates. If this service is disabled, this computer will not be able to use the Automatic Updates feature or the Windows Update Web site.
Service DLL	`C:\Users\<user>\AppData\Roaming\newdev.dll`

Table 2: shows an example of the service created by a `MileStone2017` variant of COLDSTEEL

Name	Description
Name	msupdate2
Binary Path Name	`C:\Windows\System32\svchost.exe -k msupdate2`
Display Name	Microsoft update
Description	Enables the download and installation of Windows updates. If this service is disabled, this computer will not be able to use the Automatic Updates feature or the Windows Update Web site.
Service DLL	`C:\Users\<user>\AppData\Roaming\newdev.dll`

Table 3: shows an example of the service created by a `MileStone2017` variant of COLDSTEEL

It should be noted that loading the DLL as a Service invokes the `ServiceMain` export.

Defence evasion

Themida

Themida is a software packer designed to frustrate reverse engineering & scanning. Variants of COLDSTEEL have been observed using Themida version 3.0.5 and 3.1.1. This is likely an attempt to hinder detection and analysis.

Themida is typically applied to the `MileStone2017` variants however some samples have been observed without it.

It should be noted that Themida is used to protect executables after compilation. Themida randomises certain aspects of the packing process, applying Themida to the same executable file multiple times results in different output files each iteration. By default, Themida does not modify an executable's compile time.

Impersonation

COLDSTEEL imitates legitimate sounding Windows service names like msupdate, this is believed to be to try and avoid drawing suspicion.

The `MileStone2016` variant of COLDSTEEL can also create a new administrator account `ANONYMOUS` with the password `MileSt0ne2@16`, a new instance of COLDSTEEL is created, and the user account deleted. In the `FBI20111024` variant the username is `_DomainUser_` and corresponding password is `Dom4!nUserP4ss.` This is likely to be to blend in logs or to hide the account used in the initial compromise.

Variant comparison

Observed COLDSTEEL variants differ in functionality as detailed below:

Property	FBI20111024	MileStone2016	MileStone2017
Windows 10 support	In the basic system survey there is no support for Windows 10 and a small memory leak occurs if run.	In the basic system survey there is no support for Windows 10 and a small memory leak occurs if run.	In the basic system survey Windows 10 is a recognised operating system.
Communication obfuscation	Communications are obfuscated as described in the Communication (overview) section.	Communications are obfuscated as described in the Communication (overview) section.	None present.
Uninstall	Has support to remove the service and modify registry keys by creating a new process using `WinExec`.	Some samples have support to remove the service and modify registry keys by creating a new process with `CreateProcessA`.	None present.
Beacon 3rd argument	Uninitialized memory.	Next item on the stack.	Null bytes.
Command differences	Observed to run under `_DomainUser_` account, additional clean-up command and process commands.	Observed to run under `Anonymous` account, possesses an additional clean-up command.	Contains a subset of `MileStone2016` sample's commands.
Themida	Not present.	Not present.	Typically present.

Communications

Overview

COLDSTEEL communicates using TCP to exfiltrate data and receive additional tasking. The port varies between samples, `443`, `8843` and `8888` having been observed. It should be noted that despite being on port 443 the traffic is not HTTPS, this traffic is not encrypted.

Communication with the C2 server is initiated by COLDSTEEL creating a socket over which it sends an initial beacon containing information about the victim machine. Tasking is returned by the C2 server, which is then carried out by COLDSTEEL and the result sent to the C2 server.

Communications from COLDSTEEL are sent in two parts the first is a message header consisting of a command ID, length of the following message and then an unused parameter, these are all little endian encoded. Then an optional second message that corresponds to the command itself matching the length specified previously in the first message. COLDSTEEL also expects to receive communications from the C2 in this format. For readability the two messages have been combined throughout this section.

The variants of COLDSTEEL except `MileStone2017` obfuscate the content of its communications by XORing each content byte with a hardcoded key byte, and then adding the hardcoded key byte to the result. This is only applied to message contents, not the message header. Communications from the C2 are not obfuscated in this way.

Exfiltration

Beacon format

MileStone2017

An example of the initial beacon sent from a `MileStone2017` variant of COLDSTEEL can be seen below:

COLDSTEEL MileStone2017 example beacon

```
0x0000  00 00 00 11 98 01 00 00 00 00 00 00 00 00 00 00  ....˜...........
0x0010  44 45 53 4B 54 4F 50 2D 52 42 4D 48 52 54 36 00  DESKTOP-RBMHRT6.
0x0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0050  75 73 65 72 5F 75 73 65 72 00 00 00 00 00 00 00  user_user.......
0x0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0090  32 30 34 36 4D 42 00 00 00 00 00 00 00 00 00 00  2046MB..........
0x00A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00B0  57 69 6E 20 31 30 20 53 50 30 00 00 00 00 00 00  Win 10 SP0......
0x00C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00F0  4D 69 6C 65 53 74 6F 6E 65 32 30 31 37 00 00 00  MileStone2017...
0x0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0110  01 00 00 00 04 00 00 00 34 00 00 00 16 00 00 00  ........4.......
0x0120  00 00 00 00 04 00 00 00 31 37 32 2E 33 30 2E 30  ........172.30.0
0x0130  2E 31 34 3A 38 38 38 38 00 00 00 00 00 00 00 00  .14:8888........
0x0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x01A0  00 00 00 00 00 00 00 00                          ........
```

Response ID	Message length (0x198) bytes	Null bytes
Computer name (Null padded to 0x40 bytes)	Username (Null padded to 0x40 bytes)	Physical memory (Null padded to 0x20 bytes)
Windows version (Null padded to 0x40 bytes)	Hardcoded ID (Null padded to 0x40 bytes)	Uptime: days, hours, minutes, seconds
Unused	Number of sessions	IP and port (Null padded to 0x80 bytes)

The username format consists of the username found using two different methods joined using an underscore. The username shown above is `user`.

Obfuscation

Other variants like `MileStone2016` perform a custom obfuscation routine to obfuscate the contents of network communications. An example of the obfuscated beacon can be seen below. The observed samples use a key of `0x1D` as shown below. To deobfuscate the content, each byte would have `0x1D` subtracted from it, then XORed with `0x1D`.

COLDSTEEL MileStone2016 example beacon

```
00 00 00 11 98 01 00 00 B6 01 00 B7 00 86 A6 02 76 75 6B 73 66 6F 6A 4D 6C
7C 6D 72 6C 66 48 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 85 8B 95 8C 5F 85 8B 95 8C 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 4C 4A 46 48 6D 7C
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 67 91 90 5A 47 5A 6B 6A 49 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 6D 91 8E 95 6B 86 8F 90 95 4C
4A 49 48 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 39 3A 3A
3A 35 3A 3A 3A 51 3A 3A 3A 35 3A 3A 3A 1E 3A 3A 3A 36 3A 3A 3A 49 41 4C 50
49 48 42 50 49 46 41 50 49 4B 4C 44 46 46 4B 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A 3A
```

Command ID	Message length (0x198) bytes	Next arguments on the stack
Computer name	Username	Physical memory
Windows version	Hardcode ID (MileStone2016)	Uptime: days, hours, minutes, seconds
Obfuscation key basis	Number of sessions	IP and port

It should be noted that the value of the Obfuscation key under the obfuscation is `0x1C` this is incremented to `0x1D` during the obfuscation routine, and it is that value is used.

Tasking example – File operations

After receiving the initial beacon, the C2 server can send tasking. For example, telling the malware to start a new thread for file operations:

COLDSTEEL C2 command to start file processing thread

```
00 00 00 21 00 00 00 00 B6 01 00 B7 00 86 A6 02
```

Command ID	Message length (0x0) bytes	Next argument on the stack

COLDSTEEL then creates a new thread for the file tasking commands and a new connection, over which it sends the following:

COLDSTEEL processing thread started response

```
01 00 00 11 00 00 00 00 00 00 00 00 00 00 00 00
```

Response ID	Message length (0x0) bytes	Unused

The C2 can then send commands related to the file system to the new connection:

COLDSTEEL C2 command to collect file properties

```
0x0000  03 00 00 21 22 00 00 00 00 00 00 00 00 32 00 10 43  ...!"........2..C
0x0010  3A 5C 55 73 65 72 73 5C 75 73 65 72 5C 44 65 73 6B  :\Users\user\Desk
0x0020  74 6F 70 5C 64 6F 77 6E 6C 6F 61 64 2E 74 78 74     top\download.txt
```

Command ID	Message length (0x22) bytes	Next argument on the stack
Command parameter		

COLDSTEEL will then send the results back to the C2:

COLDSTEEL file properties response exfil

0x0000	00 00 00 00 A4 00 00 00 00 00 00 00 00 00 00 00	....¤..........
0x0010	02 00 00 00 64 6F 77 6E 6C 6F 61 64 2E 74 78 74	....download.txt
0x0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0x0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0x0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0x0050	00 00 00 00 54 58 54 20 46 69 6C 65 20 00 00 00	....TXT File ...
0x0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0x0070	00 00 00 00 32 30 32 31 2D 30 38 2D 30 33 20 31	....2021-08-03 1
0x0080	35 3A 33 36 3A 33 38 20 00 00 00 00 00 00 00 00	5:36:38........
0x0090	00 00 00 00 00 31 2E 37 34 4D 42 00 00 00 00 00	....1.74MB......
0x00A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0x00B0	00 00 00 00	....

Command ID	Message length (0xA4) bytes	Null bytes
Object type (Directory = 1 File = 2)	Filename (Null padded to 0x40 bytes)	File type
File creation time	File size	

After this command has run, the file operation thread continues to run and can tasked with additional file command.

Command IDs

Command ID	Description
0x20000000	Uninstall. Terminates TCP session, then creates a new process using rundll32.exe calling one of its own exports to perform cleanup, removing the service. Not present in `MileStone2017` and some `MileStone2016` samples.
0x20000001	Terminates TCP session.
0x20000006	Simulate a Ctrl + Alt + Delete virtual key press.
0x20000011	Simulate a key press for any windows virtual key.
0x20000012	Simulate a key release for any windows virtual key.
0x20000013	Set cursor position.
0x20000014	Simulate left mouse down.
0x20000015	Simulate left mouse up.
0x20000016	Simulate left mouse double click (left mouse down, up, down, up).
0x20000017	Simulate right mouse down.
0x20000018	Simulate right mouse up.
0x20000019	Simulate right mouse double click (right mouse down, up, down, up).
0x21000000	Creation of thread that handles file operations.
0x21000002	Enumerates logical drives.
0x21000003	Get file properties.
0x21000004	Delete file.
0x21000005	Shell execute.
0x21000006	Copy file.
0x21000007	Move file.
0x21000008	Upload file to C2.
0x2100000A	Download file from C2.
0x21010000	Enumerates sessions.
0x22000001	Takes a screenshot and captures cursor position every 100 milliseconds.
0x23000000	Creates a new cmd.exe process which is communicated with using a new network connection to the C2 server. NB: In some examples cmd.exe is copied to a new file in the `C:\users\public\documents` named `dllhost.exe` and that is used instead.
0x23000004	Creates a new administrator account named `ANONYMOUS` with the password `MileSt0ne2@16`, a new instance of COLDSTEEL is executed under this user account, and the user account deleted. Alternative variants have also been seen with the username `_DomainUser_` and corresponding password `Dom4!nUserP4ss.` Not present in `MileStone2017`.
0x25000000	Creates a thread to deal with process operations. Only present in `FBI20111024` variant.
0x25000002	Performs a process listing. Only present in `FBI20111024` variant.

Command ID	Description
0x25000002	Terminate process. Only present in `FBI20111024` variant.

Response ID

COLDSTEEL uses hard coded values to indicate status. The following response codes have been observed.

Response ID	Description
0x00000000	Command ran successfully.
0x11000000	Initial beacon to C2 server.
0x11000001	File handling thread setup.
0x11000002	Remote desktop ready.
0x11000003	Reverse TCP shell is ready.
0x11000005	Thread for process interaction is running.
0x11000006	Thread for uploading file is running. Only present in `FBI20111024` variant.
0x11000007	Thread for downloading file is running.
0x11000009	Session enumeration command complete.

Conclusion

COLDSTEEL is a Remote Access Tool designed to support interactive desktop functionality & command-line access. The actor has taken some steps to hinder analysis & hide in plain sight. However, the consistent use of filename, service name and description aids detection.

The lack of support for Windows 10 version strings in `MileStone2016` and `FBI20111024` suggests that these may be older samples. If this is the case, the actor appears to have removed several pieces of functionality from COLDSTEEL, those primarily concerned with process enumeration & manipulation.

Detection

Indicators of compromise

Type	Description	Values
IPv4	C2 infrastructure	192.95.36.61:443 103.224.80.76 138.128.98.106:8443 1.9.5.38:443
Path	Malicious DLL location.	`C:\Users\<user>\AppData\Roaming\newdev.dll`
Windows Service	Service used to maintain persistence	msupdate msupdate2 Name

User Account	Temporary user running a process.	Deleted user account, with orphaned process still running.
		`Anonymous`
		`_DomainUser_`

Rules and signatures

Description	Identifies the service created by COLDSTEEL.
Precision	No false positives have been identified during VT retrohunt queries.
Rule type	YARA

```
rule COLDSTEEL_service_strings
{
    meta:
        author = "NCSC"
        description = "Identifies the service created by COLDSTEEL."
        date = "2023-01-31"
        hash1 = "a94ed3d673261d62f2959979272d8c8d17e6e7f3"


    strings:
        $ = "msupdate"
        $ = "Microsoft Update"
        $ = "Enables the download and installation of Windows updates. If
this service is disabled, this computer will not be able to use the
Automatic Updates feature or the Windows Update Web site."

    condition:
        all of them
}
```

Description	Execution method used by COLDSTEEL.
Precision	No false positives have been identified during VT retrohunt queries.
Rule type	YARA

```
import "pe"
rule COLDSTEEL_rundll32_use_and_export_names
{
    meta:
        author = "NCSC"
        description = "Execution method used by COLDSTEEL."
        date = "2023-01-31"
        hash1 = "a94ed3d673261d62f2959979272d8c8d17e6e7f3"


    strings:
         $ = "rundll32.exe \"%s\",UpdateDriverForPlugAndPlayDevicesW"

    condition:
        all of them
        and pe.exports("UpdateDriverForPlugAndPlayDevicesW")
        and pe.exports("ServiceMain")
        and pe.exports("DiUninstallDevice")
}
```

National Cyber Security Centre
a part of GCHQ

Description	COLDSTEEL strings.
Precision	No false positives have been identified during VT retrohunt queries.
Rule type	YARA

```
rule COLDSTEEL_strings
{
    meta:
        author = "NCSC"
        description = "COLDSTEEL strings"
        date = "2023-01-31"
        hash1 = "a94ed3d673261d62f2959979272d8c8d17e6e7f3"


    strings:
        $ = "MileStone201"
        $ = "%SystemRoot%\\System32\\svchost.exe -k "
        $ = "%s SP%d"
        $ = "Win 2003"
        $ = "Win 98"
        $ = "RegSetValueEx(Svchost\\krnlsrvc)"
        $ = "RegOpenKeyEx(Svchost)"
        $ = "RegSetValueEx(ServiceDll)"

    condition:
        7 of them
}
```

National Cyber Security Centre
a part of GCHQ

Description	COLDSTEEL Themida import usage.
Precision	No false positives have been identified during VT retrohunt queries.
Rule type	YARA

```
import "pe"
rule COLDSTEEL_Themida_useage
{
    meta:
        author = "NCSC"
        description = "COLDSTEEL Themida import usage."
        date = "2023-01-31"
        hash1 = "9ec69a042106fc9d27a27197d3b680b468bca9a0"


    strings:
        $ = ".themida"
    condition:
        all of them
        and pe.exports("ServiceMain")
        and pe.imports("CloseServiceHandle", "ADVAPI32")
        and pe.imports("CreateEnvironmentBlock", "USERENV")
        and pe.imports("CreateWindowExA", "USER32")
        and pe.imports("SHGetFileInfoA", "SHELL32")
        and pe.imports("SelectObject", "GDI32")
        and pe.imports("WTSQuerySessionInformationA", "WTSAPI32")
        and pe.imports("strcspn", "MSVCRT")
}
```

National Cyber Security Centre
a part of GCHQ

Disclaimer

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.