National Cyber Security Centre
a part of GCHQ

Malware Tipper

Line Dancer

In-memory shellcode loader targeting Cisco Adaptive Security Appliance (ASA) devices.

Version 1

24 April 2024

Line Dancer

In-memory shellcode loader targeting Cisco Adaptive Security Appliance (ASA) devices.

Executive Summary

- This report covers Line Dancer, a shellcode loader identified being deployed to Cisco ASA devices during cyber-attacks observed in late 2023 and early 2024.
- This activity is tracked by Cisco Talos as the ArcaneDoor campaign.
- Line Dancer is distinct from Line Runner, a persistent Lua webshell discussed in a separate NCSC Malware Tipper.
- Line Dancer and Line Runner have been observed being deployed and in use together to achieve actor objectives on ASA devices.
- The shellcode loader was recovered from a 20KB region of memory marked as readable, writable, and executable residing outside of the text section of the `lina` process.
- To achieve execution, the pointer to the subroutine which handles parsing the `<host-scan-reply>` field in XML data from WebVPN traffic is overwritten to point to the shellcode loader.
- The shellcode loader will only load payloads prepended with a fixed 32-byte token, which is known to differ between victims.
- Shellcode payloads are base64-decoded, copied into the same 20KB region of memory as the loader and executed.
- It is advised to check for the presence of Line Dancer prior to checking for the presence of Line Runner, as a device reboot will remove traces of Line Dancer.
- NCSC would like to acknowledge the support from the Canadian Centre for Cybersecurity (CCCS) and the Australian Signal Directorate's Australian Cyber Security Centre (ACSC) on the malware investigation.

NCSC would like to thank Cisco for enabling the analysis in this report. If you discover the presence of Line Dancer on a Cisco ASA device, please contact Cisco prior to rebooting the device via the following link and report it to the respective cyber security centre or agency in your jurisdiction.

Introduction

This report covers analysis of a shellcode loader, named Line Dancer, recovered during forensic analysis of a Cisco ASA device.

Line Dancer was observed in use by the ArcaneDoor campaign discussed by Cisco Talos in this blog post.

Line Dancer has only been seen in memory and hence no file hash has been provided.

Functionality

Overview

Line Dancer is a small 64-bit shellcode loader which is the main component of a larger framework of functionality; it is used to run arbitrary shellcode payloads which it is sent via tasking. The payloads and their functionality are not covered here, but some of the functionality is outlined in the Cisco Talos blog. It was recovered from a 20KB region of memory marked as readable, writable, and executable outside of sections allocated to the `lina` process, it was not showing as file backed.

Analyst Comment: Due to the fact the 20KB region is outside of the `lina` text section it cannot be dumped with a `copy system:memory/text` CLI command.

Line Dancer itself is 192 (`0xC0`) bytes long and is aligned to a 16-byte boundary using `nop` instructions.

Line Dancer first checks whether the first 32-bytes of data - within the `host-scan-reply` XML field of a WebVPN HTTP(S) POST request - matches a custom, hardcoded authentication token. If they do not match, then execution is passed back to the legitimate `host-scan-reply` field parser. An example of this can be found in the Canadian Centre for Cybersecurity (CCCS) published advisory here.

If the token matches, then the data after the token has its length calculated and is placed into a dynamically allocated buffer.

Analyst Comment: The token for interacting with Line Dancer is victim specific.

This data is then base64-decoded and copied into a fixed memory address which is also within the 20KB region the shellcode loader is located in. The base64-decoded data is expected to be shellcode.

Analyst Comment: The fact the shellcode is always written to a fixed address means it overwrites previous payloads in place.

The shellcode payload is called, with execution returning to the legitimate `host-scan-reply` parser after it has been run.

Execution

The pointer to the function that parses the `host-scan-reply` data is overwritten with a pointer to the memory address where Line Dancer is located.

The pointer that is overwritten is in the data section of `lina`, not the text section which is distinct from directly hooking the function itself and will not show up as a modification to the text section.

Persistence

Line Dancer is not persistent, the actor achieves persistence on ASA devices via Line Runner. A link to the NCSC Malware Tipper on Line Runner can be found here.

It is currently unknown how the shellcode loader is placed into memory.

Detection

Split Lina

Lina is the binary that runs a lot of the functionality of the ASA device. It should have multiple memory regions allocated to it. The number of legitimate memory regions varies, depending on the version of the ASA. It has been observed being either 2 or 5. The number of memory regions in itself is not an indicator of compromise.

An observed Line Dancer payload changes the memory protections of a region of lina, this results in the text section being split and causing multiple

executable memory regions for lina. This is suspicious, especially if one is of size `0x1000`. This is a strong indicator of compromise for Line Dancer.

The command "`show memory region | Include lina`" can be run in enable mode to produce output for analysis.

Example output of non-compromised device:

```
5574dd45b000-5574e202a000 r-xp 00000000 00:02 5494 /asa/bin/lina
5574e2229000-5574e351e000 rw-p 049b9000 00:02 5494 /asa/bin/lina
```

Example output of a compromised device:

Note the presence of more than one region with an executable (x) flag, with one region having a size of `0x1000`. This is the difference in size between the first two hexadecimal numbers on each line of the command output (see line two in the command output):

```
558246778000-558248d87000 r-xp 00000000 00:02 5494 /asa/bin/lina
558248d87000-558248d88000 r-xp 0260f000 00:02 5494 /asa/bin/lina
558248d88000-55824b131000 r-xp 02610000 00:02 5494 /asa/bin/lina
55824b331000-55824c618000 rw-p 049b9000 00:02 5494 /asa/bin/lina
```

Yara

```
rule Line_Dancer {
    meta:
        author = "NCSC"
        description = "Targets code sections of Line Dancer, a
shellcode loader targeting Cisco ASA devices."
    strings:
        $ = {48 8D 5E 20 48 8D 3D BB FF FF FF BA 20 00 00 00}
        $ = {4C 89 EE 44 89 F2 48 8D 3D 9A 27 00 00}
        $ = {41 FF D7 41 5F 41 5E 41 5D 41 5C 5B 5D 48 C7 C0 01
00 00 00 5F}
    condition:
        all of them
}
```

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.