The Importance of Patching: An Analysis of the Exploitation of N-Day Vulnerabilities | Fortinet Blog

Published: 2024-02-07 · Archived: 2026-04-02 10:58:54 UTC

Affected Platforms: FortiGate
Impacted Users: Government, service provider, consultancy, manufacturing, and large critical infrastructure organizations
Impact: Data loss and OS and file corruption
Severity Level: High

Executive Summary

The following supplementary research provides an analysis of the exploitation of resolved N-Day Fortinet vulnerabilities. "N-Day vulnerabilities" refer to known vulnerabilities for which a patch or fix is available but for which organizations have not yet resolved via patching.

Fortinet continues to monitor ongoing activity by threat actors targeting known, unpatched vulnerabilities, specifically:

- December 2022 - FG-IR-22-398 / CVE-2022-42475
- June 2023 - FG-IR-23-097 / CVE-2023-27997

Fortinet continues to urge all customers to take immediate action to review the guidance, assess whether affected, and if appropriate, upgrade their FortiGate devices as advised, and follow Fortinet's public advisories.

Fortinet diligently balances our commitment to the security of our customers and our culture of researcher collaboration and transparency.

In our ongoing communications and work with our customers and third-party public and private partners, we have been able to collect malware samples and, in some cases, related network traffic specific to these vulnerabilities and collaborate with these organizations to share our analysis and advised recommended actions with our customers and the global cyber ecosystem.

We are sharing this analysis to help customers make informed risk-based decisions and for other threat research and security organizations to help the industry collaborate on identifying this actor(s)'s activity and aid in detecting and preventing further activity.

This report was timed to coincide with the report on Volt Typhoon activity from CISA.

N-Day Abuse

The term "zero-day vulnerability" refers to a software vulnerability exploited by attackers before the software vendor becomes aware of it and releases a fix or patch. In contrast, and specific to this analysis, "N-Day vulnerabilities" refer to known vulnerabilities for which a patch or fix is available but for which organizations have not yet taken appropriate measures to apply the patch, leaving their systems exposed to potential exploitation.

Fortinet diligently monitors the abuse of N-Day vulnerabilities where patches have been released, but organizations have not yet upgraded.

FortiOS - heap-based buffer overflow in sslvpnd
December 2022 - FG-IR-22-398 / CVE-2022-42475

FortiOS & FortiProxy - Heap buffer overflow in sslvpn pre-authentication
June 2023 - FG-IR-23-097 / CVE-2023-27997

The best defense against any N-Day vulnerability is following good cyber hygiene, including remediation guidance and timely patching. As previously detailed, these vulnerabilities are not trivial to exploit. The complexity of the exploit suggests an advanced actor, and the fact the attacks are highly targeted at governmental or strategic targets such as critical national infrastructure, manufacturing, and service providers in government-adjacent industries suggests nation-state capability.

In this write-up, we analyze recently observed malicious N-Day activity. The following research details our investigations into the malware and IoCs being observed, which may be useful for organizations tracking adversary activity.

Incident Analysis

Fortinet diligently balances our commitment to the security of our customers and our culture of researcher collaboration and transparency. We are sharing this information to support impacted organizations, and threat researchers and security organizations tracing these actors' activity.

The malware used in these incidents are commonly a variant of a Linux implant customized for FortiOS. The following information was gathered during our forensic filesystem and binary analysis of compromised appliances. However, not all incidents are identical, so we have broken them down into clusters.

Cluster 1

Target Industries: manufacturing, consulting, local government

ld.so.preload:

In this cluster, /etc/ld.so.preload contained the string /data2/libcrashpad.so. Files listed within ld.so.preload will be preloaded by any other binary on the system, which results in all FortiOS processes loading and executing the /data2/libcrashpad.so shared object file on start. Typically, malware will leverage this preloading mechanism to maintain persistence should a process be killed.

File Path	**/data2/libcrashpad.so**
Hashes:	**MD5**: e3bb54fb78b70d50746082d077cfccba **MD5:** 1f7c614bbb75fec9b94efb58404bdeca **MD5:** d590aa857efe4623c221a398e953c764 **MD5:** 5fe8e0625b272cf2bb75023c1ded7b44
File Type:	ASCII Text

libcrashpad.so:

libcrashpad.so executes /data2/tftpd under the following conditions:

1. /tmp/tftpd.lock is not present
2. The current process’s command name is ‘ripd’

/tmp/tftpd.lock will be created if libcrashpad.so executes.

File Path	**/data2/libcrashpad.so**
Hashes:	**MD5:** e9f64481280c964a6a5dbf551e9cf6f0 / **SHA256:** 7075c5595ac2b34c8f5cf99aeeae0a99b10df100cfb5362f9a2a033ce4451a0e **MD5:** 9db3c6c29b4028ccd63ee38b62620df7 / **SHA256:** 9af6b6b1ce11ab62a95f3990cdf9b0f3d4bc722f662d80116bcdabdd302f4aee **MD5:** aa53393374e3ec355c0071adeba535eb / **SHA256:** ef7f71ea1c7f35c8a28fc2e98fa9e59b8e2d0f0bea84a527cf2c20ccc4f8b816 **MD5:** 604d909d4d8d69c07e3474ceaf379f20 / **SHA256:** ddc68e6647f9abcf23206d2fbcbccb4459d7f545abfc9b2e12ebba2e5a29bcd1 **MD5:** 78310bad651eff14e5ecefe674630e75 / **SHA256:**

	1103c2cd47fd62d2c9353edb5c2dce23173c15770594237b84e01635723b0eec **MD5:** 5b2882b0a4de3210e1bfa5db1ed63713 / **SHA256:** **MD5:** dbe0d8d612ad89229cd6175e37157f3c / **SHA256:**
File Type:	ELF 64-bit LSB shared object, x86-64, dynamically linked

tftpd:

This is the primary executable responsible for dropping additional malware files and other malicious features. The tftpd binary performs the following actions:

1. Establish malware persistence for /data2/libcrashpad.so by creating the file /data/etc/ld.so.preload containing a file path to libcrashpad.so.
2. Perform timestomping on files to evade detection and as an anti-forensics technique:
    a. For files /bin/smit, /bin/toybox, /data/etc/ld.so.preload, /data2/libcrashpad.so, and /data2/tftpd - their access time and modification time are set based on the corresponding values of /bin/init.
    b. For file /lib/libaprhelper.so – its access time and modification time are set based on the corresponding values of /lib/libc.so.6.
3. Enumerate all running processes and check the presence of the sslvpnd process. Once identified, it drops /lib/libaprhelper.so and injects it into the sslvpnd process. tftpd receives data from the sslvpnd process via the file system socket /tmp/clientsDownload.sock. It may attempt to retrieve data, such as the address of the peer connected to the socket, from sslvpnd connections via the hooked accept and accept4 syscalls.
4. Drop /bin/smit binary. It then deletes the existing FortiOS symbolic link of /bin/smit, which was originally directed to /bin/init file.
5. Drop /bin/toybox binary. Following this, it deletes an existing FortiOS symbolic link of /bin/sh, which was originally directed to the /bin/sysctl file. It then copies the binary /bin/toybox to be the new /bin/sh. It sometimes creates a new folder, /usr/bin.
6. Additional routines are present that may allow stored credentials to be decrypted from the configuration (see Mitigations section for more details)

File Path	**/data2/tftpd**
Hashes:	**MD5:** cf3e6cb8ada288aa2d1bc39d1ce2ad54 **SHA256:** a322034e610aa07632ade4323d37d55c5c613b155ef51b05ab83de4159c231b2 **MD5:** 0909a8ee77fbd40ab461df20600ddae0 **SHA256:** ba0b6b0c6b628dffcf0f34fa78fb61acb6c1b457f7b5addadbe4dba575bac5bd **MD5:** 953813bb2137e351709d98a91336eb25 **SHA256:** 65a9314fc3fac8cc238534d81c12e2080820f86a58299113c164aea4cd18f11c **MD5:** b11faf42afeca35920a248001b90e997 **SHA256:**
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) dynamically linked, stripped

Libaprhelper.so:

Libaprhelper.so is dropped by tftpd and injected into the sslvpnd process. Libaprhelper.so hooks the system calls accept and accept4 in the process' Procedure Linkage Table. The accept hook function first calls the true accept syscall. It then receives 48 bytes from the socket, which accepts the connection. Eight bytes located at offset 15 from the received data are compared with the byte sequence DA F3 64 13 C2 8D 63 C3. If the pattern matches, the socket may be shared with the tftpd process via the file system socket /tmp/clientsDownload.sock.

File Path	**/lib/libaprhelper.so**
Hashes:	**MD5:** 9e898f389003f9141831856f021fda3a **SHA256:** 5bfe16360fb42fa50a56fe8b1140bec202e9345965ddb456a8311b2583d2fe48 **MD5:** 176220a8ac6f344aaf620efab5c6f276 **SHA256:** 7a86b793612a6b6a3f27d7c24eec4c75202915c7c2c36b786c39ef95628b1286 **MD5**: 2349d1d1acb69e91aea5be7767254f81 **SHA256:** 1209b5ff4755e689e260e680caf33b52ecd3fa8a1bb20ff06d7770828490baee **MD5:** 9d7b6fc9a0702381062726f634d0df0f **SHA256:** 43c1905b2078a8de9d0fa42e16465692066825e3dcb42a17cbf40b77736527c2 **MD5:** e7ab34f7df83ce3ed6bf287332f7ce73 **SHA256:** 80d03d5d35a7b9bde7e5e60f0df3baa0c51cbbd9214d875cd1967f589b9df183 **MD5:** 8b2c08f4e558626f34494b171e21f644 **SHA256:** a667edc691e9950ec0bc92e9f2cdcb7e99a0862860638640404 35f26537f9d9b **MD5:** 9d2bc4e59357b56199b709a599600fa7 **SHA256:** **MD5:** b32ad75ce0494586a8b278c0413c0406 **SHA256:**
File Type:	ELF 64-bit LSB shared object x86-64, version 1 (SYSV) dynamically linked, stripped

smit:

On a clean FortiOS system, /bin/smit is a symbolic link to /bin/init. The standalone malicious smit binary retains the normal FortiOS function to hide its presence by forking a child process to execute /bin/init with the arguments provided to /bin/smit. It performs the following malicious actions after the child process terminates:

1. Establish malware persistence for /data2/libcrashpad.so by creating the file /data/etc/ld.so.preload containing a file path to libcrashpad.so
2. Perform timestomping on /data/etc/ld.so.preload. The access time and modification time are set based on the corresponding values of /bin/init.

File Path	**/bin/smit**
Hashes:	**MD5:** 08039b1cbdf880a3d86f8646bb286709 **SHA256:** 2b1aa340384b5e889008839bc961fcb438379cc2de8be880664ae41fd9e77084 **MD5:** 2fc1aa1ab1ecde77eb6724f7385d5749 **SHA256:** 46ac81f19c996d9a2e257ef584455a721aad15f1cdeb597e8f853e288b3e9070 **MD5:** cf49feb43667819b880422efbe89fd01 **SHA256:** 6a92e750eb4e84be875158e6ecb11ac3e4716c04ff32d29206bf7b1a4ec46edc
File Type:	ELF 64-bit LSB shared object x86-64, version 1 (SYSV) dynamically linked, stripped

toybox:

A toybox binary was dropped by tftpd. tftpd then created a new symbolic link, linking /bin/sh to /bin/toybox.

Toybox is a static binary package containing functions such as insmod, iotop, lsmod, lsusb, makedev, mkdir, mkfifo, nc, netcat, pivot_root, route, wget, ftpget, shred, and other utilities. These binaries can modify system and network settings,

which can help accomplish further actions, such as exfiltration, pivoting to other devices, and getting more system information. This toybox might provide convenience to the attacker for their lateral movement.

File Path	**/bin/toybox**
Hashes:	**MD5:** d0a31975a436d0fe3b4f990c5003ca59 **SHA256:**
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) statically linked, stripped

Cluster 2

Target Industries: Internet Service Provider

/data/etc/ld.so.preload:

Files listed within ld.so.preload will be preloaded by any other binary on the system. In these cases, /data/etc/ld.so.preload contains the string /data2/flatkc_info, which results in flatkc_info being executed whenever other binaries are run.

File Path	**/data/etc/ld.so.preload**
Hashes:	**MD5:** 2495159a80aafcdb80bcf8d913d4db80 **SHA256:** **MD5:** b62871b520bd304086da76c729fa5cf7 **SHA256:**
File Type:	ASCII Text

/data2/flatkc_info:

Executes /data2/new_alert_info.

File Path	**/data2/flatkc_info**
Hashes:	**MD5:** 5d898fdbe0080f5c4437d834e8c23498 **SHA256:** 1029ff063f739ebbf8add74313f2cc454f5d14655327d1a1c190b115549173ed
File Type:	ELF 64-bit LSB shared object executable x86-64, version 1 (SYSV) dynamically linked, stripped

/data2/new_alert_info:

New_alert_info creates and executes the files /bin/smit, /bin/httpsclid, and /bin/httpsng. Upon rebooting, these three files in the bin directory will not persist. New_alert_info, however, provides a persistence mechanism for smit, httpsclid, and httpsng. The files are embedded within new_alert_info and not downloaded from an external source.

New_alert_info also reinforces persistence for flatkc_info by creating the file /data/etc/ld.so.preload and adding the string /data/etc/flatkc_info to it.

This malware bears similarities to Rekoobe Malware, which is commonly used by APT31.

File Path	**/data2/new_alert_info**
Hashes:	**MD5:** 210fcaa8bf95c3c861ee49cca59a7a3d **SHA256:** 64932db564f8cd3a58f3d019d1967b981fdcf3c59f7f5ff6bb3bdf8ec736c31a **MD5:** a5d4b0228beca0f5360049490882683f **SHA256:** 3b897cf3ef1af97d19d8cc7680235f75ee5cbd431d2f93e7e6ac17f003dd812d **MD5:** a1192fca2299c57b122e1ffbadecef37 **SHA256:** 05ac806a539c0054bbb8774bac63ac75dcbd8c709932ec21b8c5b67693272e3b
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) statically linked, stripped

httpsclid:

Httpsclid contains an embedded ELF file. It writes the file to the device as /tmp/busybox.

A local socket /tmp/ClientSessionData is created for inter-process communication. Httpsclid can perform various actions based on what is transmitted through the socket. 1. Exit program, 2. Data exfiltration, 3. Download/write files, 4. Remote shell. This file also has the additional capability to query AD Servers via LDAP to identify all active user accounts and query VMWare NSX SecurityTag APIs to mirror switch traffic.

File Path	**/bin/httpsclid**
Hashes:	**MD5:** 944a31cf9936920a3fb947cb29171631 **SHA256:** 7ff5e0c2ecd6397dcbc013d4c343007f9ebb4099aabda9a7745ab1dd1b215c91 **MD5:** d84a95d19f19eeee2415f41c2c181db8 **SHA256:** 5089f545aa94d273d18150102dc65c3a08b4335d6f171d9b3f655599d8589b0e **MD5:** 4c375c7ac9ee2f8a04c920381683e811 **SHA256:** 7edd6af205e748d13641bf3d3209bc69ab062b71db06700277b337f3b026700e **MD5:** 60057a831f3498751e37413c45c29c4a **SHA256:**
File Type:	ELF 64-bit LSB executable x86-64 version 1 (SYSV) statically linked, stripped

This malware also bears similarities to Rekoobe Malware, commonly used by APT31.

/bin/httpsng:

Httpsng masquerades itself by running with the process name [ata/0]. It may introduce additional malware to the system. /bin/httpsng contains code to use "/tmp/busybox tar -xvf" to unpack /tmp/tarlog.tar. However, the origin of /tmp/tarlog.tar is unknown and was not found in any systems.

Httpsng receives an IP address via an ICMP request and establishes back a connection to that IP address. It can perform various actions based on what is transmitted through the connection. 1. Exit program, 2. Data exfiltration, 3. Download/write files, 4. Remote shell

File Path	**/bin/httpsng**

Hashes:	**MD5:** 7454bb4b3dfe4f4386980b63f119c208 **SHA256:** 1b7af533f32a1c0bb62420be787d9e02c8a71bca77f2b0857dd20599f8833853 **MD5:** f5caae23ace1ee0b48d02427b08f0bad **SHA256:** 534632ae386cf4d2190ef03be08a96f25fb3a9537d1c380141d36d797b983705
File Type:	ELF 64-bit LSB executable x86-64 version 1 (SYSV) statically linked, stripped

/bin/smit:

Establishes persistence for /data2/flatkc_info by creating the file /data/etc/ld.so.preload containing the file path to flatkc_info.

File Path	**/bin/smit**
Hashes:	**MD5:** fc78c1800fbe25e57a7333ca51e183b6 **SHA256:** b8bd746e4713e101266d74bbe8cfbf064b5979adb8df68076d295df9e0a215d0 **MD5:** 247139079d8a1c2534ef0d2b726d8ebb **SHA256:** 4860b98219177aacb786b1a2d5c68e999c0c8cf6c6400c7fe773fb18f44c78be **MD5:** 823ae2645869e4fc9ebcb046aa760440 **SHA256:**
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) dynamically linked, stripped

busybox:

A legitimate busybox binary.

File Path	**/tmp/busybox & httpsng**
Hashes:	**MD5:** ebce43017d2cb316ea45e08374de7315 **SHA256:** 6e123e7f3202a8c1e9b1f94d8941580a25135382b99e8d3e34fb858bba311348
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) statically linked, stripped

Cluster 3

Target Industries: manufacturing, consulting

ld.so.preload:

Files listed within ld.so.preload will be preloaded by any other binary on the system. In these cases, /data/etc/ld.so.preload contains the string /data2/libunwind.1.so, which results in libunwind.1.so being executed whenever other binaries are run.

File Path	**/tmp/busybox & httpsng**

Hashes:	**MD5:** 8644b8b1cec97b2f43c89526c3b8aaae **SHA256:**
File Type:	ASCII Text

libunwind.1.so:

Libunwind.1.so executes /data2/httpdng under the following conditions:

1. /tmp/httpdng.lock is not present
2. The current process' command name is 'ripd'

/tmp/httpdng.lock will be created if libunwind.1.so executes /data2/httpdng.

File Path	**/data2/libunwind.1.so**
Hashes:	**MD5:** e9c2a3efaa97462168790b2fe234a7ba **SHA256:** 5700a8d9f00ebeb52536d16701522ecf6a07deb660e442cd67acdfb768e17c39
File Type:	ELF 64-bit LSB shared object x86-64, version 1 (SYSV) dynamically linked, stripped

httpdng:

Httpdng establishes persistence for /data2/libunwind.1.so by leveraging the file /data/etc/ld.so.preload. It is also responsible for dropping files in non-persistent directories (directories in which added files are deleted on reboot). /bin/toybox, /bin/smit,/data2/libunwind.1.so, /tmp/.ptyagent, and /data/etc/ld.so.preload are created by httpdng. Apart from /tmp/.ptyagent, the access and modify timestamps of these files are changed to match those of /bin/init.

Httpdng may create the file /lib/libaprsd.so. Its access and timestamps are modified to match those of /lib/libc.so.6. The malware may attempt to load this shared object into the sslvpnd process. Httpdng receives data from the process that has loaded /lib/libaprsd.so via a file system socket, /tmp/clientsDownload.sock. It may attempt to retrieve data from connections via the hooked accept and accept4 syscalls.

File Path	**/data2/httpdng**
Hashes:	**MD5:** f84a5eff50af2a7bfae49345b3b3ce1e **SHA256:** 662dd91647c45df0625c011565a60f18e0de47b9e57653763868205f4026593f **MD5:** 7aaaf17e4e3638d2f93b1cf5a1579ac6 **SHA256:** 0088cfd5b4b7195edab836236ba0c6a0c2aded3e4b8a842f11ee4e9c5e4ae3c1 **MD5**: e1aff3203fd38fc4790157d908ef742a **SHA256:** **MD5:** f66c0c328d40cffdb0d8dfa0444fe923 **SHA256:**
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) dynamically linked, stripped

libaprsd.so:

Libaprsd.so hooks the system calls accept and accept4 in the process' Procedure Linkage Table. The accept hook function first calls the true accept syscall. It then receives 48 bytes from the socket, which accepts the connection. Eight bytes located

at offset 15 from the received data are compared with the byte sequence DA F3 64 13 C3 84 C2 80. If the pattern matches, the socket may be shared with the httpdng process via the file system socket /tmp/clientsDownload.sock.

File Path	**/lib/libaprsd.so**
Hashes:	**MD5:** dc95090cca508d1196b972c385dc3405 **SHA256:** 89e049fd0df33da453fe04d9b2f9619b46dac0fceb7a8156560cce08fce3d8b7 **MD5:** 9d7a1a536eef0ff1e87ee1d78ac7bc69 **SHA256:** 1748035e9cb1932bbe6c3aa93c2ae044296e0f0774d0aa0d3eb688cdd2c0b2f2 **MD5:** 834e542076e7c37e848fb68b3671f7a1 **SHA256:** **MD5:** 62ef5ec4adbd655adcc418d7ba2262ac **SHA256:**
File Type:	ELF 64-bit LSB shared object x86-64, version 1 (SYSV) dynamically linked, stripped

smit:

Smit will establish malware persistence by creating the file /data/etc/ld.so.preload containing the string /data2/libunwind.1.so. This ensures /data2/libunwind.1.so will be executed regularly. The timestamps of /data/etc/ld.so.preload are modified by smit to mask its presence.

File Path	**/bin/smit**
Hashes:	**MD5:** bc1bd24e32fb6a778c1e79840e8ec78f **SHA256:** 51d0d5d83735a3a63a2405b4f9909676fc572827693f34b80799b0786a5f1677
File Type:	ELF 64-bit LSB executable ARM aarch64, version 1 (SYSV) dynamically linked, stripped

toybox:

Toybox binary dropped by httpdng. Toybox is a collection of Linux command line utilities.

File Path	**/bin/toybox**
Hashes:	**MD5:** d0a31975a436d0fe3b4f990c5003ca59 **SHA256:**
File Type:	ELF 64-bit LSB executable x86-64, version 1 (SYSV) statically linked, stripped

ptyagent:

Ptyagent may serve as a remote shell. It can create and listen to a network socket. It will also execute /bin/bash or /bin/sh, depending on what is present on the system.

File Path	**/tmp/.ptyagent**

Hashes:	**MD5:** 2d88911f67a2cce7fa97cdf0ae59a027 **SHA256:** 910e7fc043560fbc2757304503de38a8824238765b2d91d87b974fefa253e311
File Type:	ELF 32-bit LSB executable Intel 80386 version 1 (SYSV) statically linked, stripped

Cluster 4

libpe.so:

This is a file unpacker that unpacks an encoded file into multiple files. This file has the typical hallmark of malware by being able to delay startup by a random amount of time to avoid detection.

File Path	
Hashes:	**MD5:** 90235445d07be98cd0f820b5 **SHA256:** 50451bb5b6d68115695a6cb277839a6dd2bad8f70bdb8b79670b18dcde188965
File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, stripped

smartctl:

This file name is the same as the legitimate file /bin/smartctl. However, the purpose of this file is to execute shell commands from the FortiGate command line as it redirects its input to /bin/sh.

File Path	**/bin/smartctl**
Hashes:	**MD5:** 205a8c6049061930490b2482855babcd **SHA256:**
File Type:	ELF 32-bit LSB executable Intel 80386 version 1 (SYSV) statically linked, stripped

authd:

This binary provides a process injection feature into a running process and has an API hooking mechanism. We have seen malicious binaries that provide similar process injection capabilities. However, this binary seems a little more advanced as it includes a built-in API hooking mechanism.

File Path	**/bin/authd**
Hashes:	**MD5:** 9124ce75319514561156d2013fc9d3be **SHA256:** f40c04fb9e2d4157a0bc753925dbc5f757feb77cdd22f90fedf3cc5e095143bc
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux-x86-64.so.2

httpsd:

This binary has C2 communication capability and can read and write to a configuration.

File Path	**/bin/httpsd**
Hashes:	**MD5:** 218a3525ab8e46f7afe252d050a86907 **SHA256:** 3ed99aad5922744b6a75ea90ea6ece81ba0d8eb9935aec38b897e44ac3b36c35
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.32, stripped

This sample contained an interesting string that led one of our CERT partners to name this cluster COATHANGER

"She took his coat and hung it up."

This string is taken from the book Lamb to the Slaughter by Roald Dahl. A search for this string in Virus Total resulted in a single link to an innocuous PDF file containing the same string.

https://www.virustotal.com/gui/search/21ce19be794adbcff49c90cfff9eba5189ae0131ac69396ea5544822882b440b%255C/files

This was not overly unusual, given that the file appears to be a PDF copy of the book. However, the date of the upload was suspiciously recent for such an old book. Out of an abundance of caution, we analyzed the file, but it was found not to be malicious.

newcli:

It uses "authd" binary to inject /lib/preload.so file and replaces the reboot function with a malicious function.

File Path	**/bin/newcli**
Hashes:	**MD5:** ab89139e3d47fbaba2da33040da95200 **SHA256:** 2acc6a2a931db63fe3a875780f00192a60955c9794df68fe0ace0012d309b04f
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked

We have observed in other clusters an injector binary being used to inject into a process with pid=1.

preload.so:

Provides persistence and system functions. It can copy malicious files to memory and write them back to disk when the system reboots. It also provides a malicious function called newreboot.

This is somewhat similar to previous clusters due to the presence of a "reboot" export function/API hooking, but other features have not previously been observed.

File Path	**preload.so**
Hashes:	**MD5:** a62377c01935f366761846b5ceed5a49 **SHA256:** 1c437dc9e929669e5a65a1c70afb3107fba471afb9ad35e3848334c9332f2b59

File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked

sh:

This non-malicious busybox binary provides multiple tools, as seen in other campaigns.

File Path	**/bin/sh**
Hashes:	**MD5:** 991461b86aebecfd096dc11ff2a04b4b **SHA256:** dcd9a5af1c6297ed1a66c851efa305000335d8ade068ba515125a6612f1d5300
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

liblog.so:

This hook reads APIs and targets /dev/fgtlog to disable reading from /dev/fgtlog. We have not seen malware targeting /dev/fgtlog in previous clusters.

File Path	**/lib/liblog.so**
Hashes:	**MD5:** e24d14d3e6c6de0ed3db050dd5c935f0 **SHA256:** a79f80158ebbf9e34f6a7ec86b564de2fbee783fe6c1e20eefe2832226e2f827
File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, stripped

packfile:

This is a container file with malicious files in it that are unpacked as needed. This is unlike previous clusters.

File Path	**packfile**
Hashes:	**MD5:** 201ee76e996846d5ea3fc03bac3273dd **SHA256:** 4591b4fb1c93c27203b36c773597fd3f885338ad7641dcebf8ed2395acdf4a5f
File Type:	ELF 32-bit LSB executable Intel 80386 version 1 (SYSV) statically linked, stripped

Standalone Instances

Instance 1

Target industry: consultancy

ld.so.preload:

Files listed within ld.so.preload will be preloaded by any binary on the system. On this system, /data/etc/ld.so.preload contains the string /data2/lib/liblpmonitor.so, which results in liblpmonitor.so being loaded whenever other binaries are run. However, the file /data2/lib/liblpmonitor.so was not found on the disk at the time of our investigation.

File Path	**/data/etc/ld.so.preload**
Hashes:	**MD5:** 0ef308bacbbc932fa24f10ae2b83a984 **SHA256:**
File Type:	ASCII Text

ptyagent

This file is based on Chisel, an open-source traffic tunneling tool that can tunnel TCP and UDP connections over HTTP and establish a reverse shell. This tooling has been observed to be used by multiple APTs, including the Lorenz Ransomware group and UNC757.

File Path	**/tmp/.ptyagent**
Hashes:	**MD5:** ca5184d43691ee8d8619377e600fa117 **SHA256:** 70372f95fa5cf917639007ae25a67a53d0297b67792b00bbea63ce0b170f95b8
File Type:	Known malware - Linux/Chisel.D!tr

Instance 2

Target industry: service provider

ld.so.preload:

Files listed within ld.so.preload will be preloaded by any other binary on the system. On this system, /data/etc/ld.so.preload contains the string /data2/liblink.so.1, which results in all the FortiOS processes loading and executing liblink.so.1. ld.so.preload also acts as a persistence mechanism.

File Path	**/data/etc/ld.so.preload**
Hashes:	**MD5:** ee50b080c6209e63a85c60cd3cee52b4 **SHA256:**
File Type:	ASCII Text

liblink.so.1:

liblink.so.1 performs a check to determine if the file /tmp/fortlinkd.lock exists. If the file is present, it proceeds. It also ensures that only one instance of liblink.so.1 performs malicious activities by verifying it is running under the ripd process. This check allows it to prevent multiple instances from engaging in malicious actions. Next, it executes the /data2/fortlinkd binary and creates the

file /tmp/fortlinkd.lock to prevent further executions of /data2/fortlinkd.

File Path	**/data2/liblink.so.1**
Hashes:	**MD5:** 031e21168d7e783d26998e63217a365c **SHA256:** dfafeb3efaba2c8e5d80ec7a37c00805895df1a47333515082da54e49a388a59
File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, stripped

fortlinkd:

The fortlinkd process attaches itself to the /bin/init process (pid=1) and reads the memory of /bin/init into a virtual address space. It continues this process until it locates the string /bin/smit and potentially attempts to modify the memory of the /bin/init process. It then deletes the original /bin/smit binary and replaces it with a new malicious binary as /bin/smit.

To provide full permissions, fortlinkd employs chmod on the malicious /bin/smit. If the /bin/fgfm file exists, it is removed, and a new malware file is dropped in its place as /bin/fgfm. The /data2/fortlinkd then executes the newly dropped fgfm binary, followed by the creation of /data2/liblink.so.1 and /data/etc/ld.so.preload files.

File Path	**/data2/fortlinkd**
Hashes:	**MD5:** d97bae365bd4c3fbf2eb834d678dbd11 **SHA256:** bfc20c8e21fa4674492576961baedae90f7794a8534d2ad3ef4e230de2fb38ab
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

smit:

smit checks for the presence of /data/etc/ld.so.preload file, which is used as a persistence mechanism. It creates a child process that executes /bin/init with smit as its argument.

File Path	**/bin/smit**
Hashes:	**MD5:** 823ae2645869e4fc9ebcb046aa760440 **SHA256:**
File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked

fgfm:

Fgfm binary masquerades itself by running with the process name [ata/0]. The malware may be able to download additional payloads, including the file /tmp/tmplog.tar. The file gets unpacked using /tmp/busybox tar -xvf. Fgfm can delete files on the system, establish a connection, and perform various actions based on what is transmitted through the connection.

1. Exit program
2. Data exfiltration
3. Download/write files
4. Remote shell

File Path	**/bin/fgfm**
Hashes:	**MD5:** 83d5c75bf1d2090a6cceaf2a80d906da **SHA256:**
File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked

Instance 3

Target industry: service provider

ld.so.preload:

Files listed within ld.so.preload will be preloaded by any binary on the system. On this FortiGate, /data/etc/ld.so.preload contains the string "/data/lib/libav.so", which results in /data/lib/libav.so being loaded whenever other binaries are executed.

File Path	**/data/etc/ld.so.preload**
Hashes:	**MD5:** 0d4b4c13a6ef8266ed5ef464c6883bf1 **SHA256:**
File Type:	ASCII Text

libav.so:

libav.so executes /data2/.vile/ketg under the following conditions:

- The current process' command line contains 'usbmuxd'
- /tmp/logx file is not present

The file /tmp/logx will be created if it doesn't exist. It is an empty file used as a mark of the execution. Libav.so also attempts to find the kernel symbol "fos_process_appraise" by iterating all kernel symbols using /proc/kallsyms and seems to change a few bytes in the device's physical

memory by accessing /dev/mem file to modify/bypass security features.

File Path	**/data/lib/libav.so.new/libav.so**
Hashes:	**MD5:** 30009c9052e588b93fb12e918bbcecfb **SHA256:** 6584f614fb0ef864cd5aa5b6ec1b42299f2b639a23e4b1e853caf3b2f2254b14
File Type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, stripped

ketg:

This is the primary executable for dropping additional malware files and other important malicious features. The ketg binary has the following capabilities:

1. Establish persistence: It checks for the existence of the file /data2/.vile/ldzvg and copies it as a persistence file /data/etc/ld.so.preload that contains the path to /data/lib/libav.so. It also changes the file permission and sets it to "r-

xr-xr-x.”

2. File creation:
    1. It checks for the existence of file /data2/.vile/libsef.so and copies this shared object as /data/lib/libav.so.new. It also changes the file permission and sets it to “r-xr-xr-x.”
    2. It checks for the existence of file /data2/.vile/569851 and copies this shared object as /SYSV64564856.
    3. It checks for the existence of file /data2/.vile/libsef.so and copies this shared object again in place of the legitimate AV Engine file /data/lib/libav.so. It also changes the file permission and sets it to “r-xr-xr-x.”
3. Process injection: It executes the binary /data2/.vile/ith with arguments to inject the shared object file /SYSV64564856 into the /bin/init process (pid=1). After successful injection, it deletes /SYSV64564856.

File Path	**/data2/.vile/ketg**
Hashes:	**MD5:** e9ae2188d7a46fdac30b192b7405cba2 **SHA256:** 8f380a844011daa8854798bf31981b660bf752e95c2e41ae50c0306275b5c0ed
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

SYSV64564856:

The shared object /SYSV64564856 is injected into the main /bin/init process with the help of a malicious /data2/.vile/ith binary. This shared object has API hooking ability and tries to hook the reboot function of FortiOS to execute the /data2/.vile/ketg binary before calling the original reboot function.

File Path	**/SYSV64564856**
Hashes:	**MD5:** 8771305a111e1b38ada954513af4507c **SHA256:**
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

ith:

This executable enables injecting a shared object into a running process. This binary performs process injection using Linux’s ptrace function. We observed that ith is executed by the ketg process using execve(“/data2/.ville/ith”, [1 –p 1 /SYSV64564856] [TERMINFO=/tmp/terminfo, TERM=vt220, and PWD=/, TZ=GMT]), thereby injecting malicious sharedobject into pid=1, which is the /bin/init process.

File Path	**/data2/.vile/ith**
Hashes:	**MD5:** 8d4c9b498da847c3690260bb28f046f9 **SHA256:** 75ce32c1e3ba902f7dcbf5bce63347448a94537682cebdde6d93efb2ede3f81c
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

/data2/.vile/dnpfmn:

This binary checks for the existence of the file /data2/.vile/lmcdle and executes the fmteld binary (which is very similar to the legitimate busybox binary), causing it to wait for 900 seconds and then kill all processes with the name lmcdle.

File Path	**/data2/.vile/dnpfmn**
Hashes:	**MD5:** 3977f8b8f5ec13604819f45282fd9b71 **SHA256:** adb1b6fc93a0225a203ec64a48470072b5d5c43d8f15860ee03f24673d9d97fe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

lmcdle:

This binary retrieves and stores kernel information and can communicate with the IP 146.185.214.63 on port 443, an IP in a Cloud Provider in Australia. This IP does not appear in any blocklist. After a connection is established, it sends some encoded data to this IP and can also receive responses from the server. At the time of investigation, the remote server did not respond with meaningful information.

File Path	**/data2/.vile/lmcdle**
Hashes:	**MD5:** 3fba828577e745c8a51d657cc393f461 **SHA256:** 20de58db0cfb04ce0abde662ca84b00ca7135bb546e2d32865046c3e4acc1b92
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

Fmteld and /data2/brodel:

Fmteld and brodel appear to be legitimate busybox binaries with no additional extensions.

File Path	**/data2/.vile/fmteld**
Hashes:	**MD5:** 46c59ceb4ded468d692a92e34df75988 **SHA256:**
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
File Path	**/data2/brodel**
Hashes:	**MD5:** 96e74f0f463eadeded69db5d0efde628 **SHA256:**
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

Malware Summary & Attribution

Clusters 1, 2, and 3

All three of the primary activity clusters contain similarities in techniques:

- In all cluster cases, persistence was achieved using the /bin/smit and /data/etc/ld.so.preload
- Clusters 1 and 3 use toybox as a multipurpose binary (cluster 2 uses a busybox).
- Clusters 1 and 3 target similar industries, unlike cluster 2.
- Clusters 2 and 3 use similar naming conventions for very different binaries (httpsng & httpdng).
- Cluster3 httpdng contains functionality similar to Cluster2 libcrashpad. It may be a different version of the malware.
- Use of /bin/smit and /data/etc/ld.so.preload appear in all the clusters, and this method was used on some single cases not listed in this document.
- One file, – /bin/smit, appeared to have been built from the same code and shared between clusters 1 and 2
- Cluster 2 malware bore many similarities to the Rekoobe Malware commonly used by APT31.

Due to the targeting of critical infrastructure organizations, living-off-the-land (LOTL) binaries, and the similarity of techniques employed, we believe Clusters 1 and 3 are from the same threat actor or group of actors and are related to Volt Typhoon (G1017). While using similar exploitation methods and the previously used Rekoobe Malware, the techniques used in Cluster 2 and targets are different enough to hypothesize this could be a separate but coordinating APT group.

Cluster 4

This cluster was only seen twice and does not have enough data points to make a clear attribution. There is an overlap in techniques similar to Clusters 1 and 3. Still, there are enough differences and regional targeting to assume this is a different APT potentially sharing tactics of a related actor. The techniques bear similar hallmarks of previously observed activities by APT15.

Instance 1

This individual instance does not show the hallmarks of the other cases. The use of Bash Scripts and off-the-shelf Chisel malware indicates a different actor, possibly UNC757, as described by CISA.

Instance 2

This individual instance bears the hallmark of the actor responsible for Cluster 1 and 3, based on atomic indicators. However, the evidence is weak.

Conclusion

Fortinet's culture of proactive, transparent, and responsible PSIRT disclosure is one of many ways we show up as a responsible member of a larger cybersecurity ecosystem and demonstrate our commitment to helping customers make informed risk-based decisions. Fortinet is sharing this follow-on research and related details to help the industry collaborate on identifying this actor(s)'s activity and aid in detecting and preventing further activity.

These attacks demonstrate the use of already resolved N-day vulnerabilities and subsequent LOTL techniques, which are highly indicative of the behavior employed by the cyber actor or group of actors known as Volt Typhoon, which has been using these methods to target critical infrastructure and potentially other adjacent actors. This report also further highlights the need for organizations to have a robust patch management program in place and to follow best practices to ensure a secure infrastructure.

Recommended actions

CISA has today provided additional guidance for securing your network against this activity in their white paper, *Identifying and Mitigating Living Off the Land Techniques* joint guidance**.**

This blog further highlights the need for organizations to follow good cyber hygiene, including industry guidance offered by the Network Resilience Coalition, of which Fortinet is a founding member. Fortinet strongly recommends the following activities:

- Monitor Fortinet Security Advisories and immediately patch affected systems.
    - If you suspect your device may have been compromised, please follow the recommended advice by performing a clean install of the latest patch version and audit your configuration for any unauthorized changes.

    - Fortinet has implemented additional measures to prevent the exploitation of unpatched systems in the wild. Fortinet has implemented hardware-based firmware and filesystem integrity checking, including virtual patching of the local management interface and real-time file system integrity checking, and continues to encourage customers to upgrade to the latest firmware version(s) to take advantage of these features.
    - Follow hardening recommendations, e.g., FortiOS 7.2.0 Hardening Guide
- Minimize the attack surface by disabling unused features and managing devices via an out-of-band method wherever possible.
- Maintain good cyber hygiene and follow vendor patching recommendations.

IOCs

As this is a post-compromise forensic static analysis on the malware samples, only file sample IoCs are included and not IP IoCs.

File	Hash	Detection
lamb_to_the_slaughter_story.pdf	**MD5:** a9fcd43714f33da1711dfb651fae5b17 **SHA1:** 34326088f095580209a74832fd68f8d1a91e7cc5 **SHA256:** 21ce19be794adbcff49c90cfff9eba5189ae0131ac69396ea5544822882b440b	N/A
ld.preeload	**MD5:** 2495159a80aafcdb80bcf8d913d4db80 **MD5:** b62871b520bd304086da76c729fa5cf7 **MD5:** e3bb54fb78b70d50746082d077cfccba **MD5:** 1f7c614bbb75fec9b94efb58404bdeca **MD5:** d590aa857efe4623c221a398e953c764 **MD5:** 5fe8e0625b272cf2bb75023c1ded7b44 **MD5:** 8644b8b1cec97b2f43c89526c3b8aaae **MD5:** 0ef308bacbbc932fa24f10ae2b83a984 **MD5:** 0d4b4c13a6ef8266ed5ef464c6883bf1 **MD5:** ee50b080c6209e63a85c60cd3cee52b4	N/A
/data2/flatkc_info	**MD5:** 5d898fdbe0080f5c4437d834e8c23498	ELF/Agen
data2/new_alert_info	**MD5:** 210fcaa8bf95c3c861ee49cca59a7a3d	ELF/Agen
	MD5: a5d4b0228beca0f5360049490882683f	ELF/Agen
	MD5: a1192fca2299c57b122e1ffbadecef37	ELF/Agen
/bin/httpsclid	**MD5:** 944a31cf9936920a3fb947cb29171631 **SHA256:** 7ff5e0c2ecd6397dcbc013d4c343007f9ebb4099aabda9a7745ab1dd1b215c91	ELF/Agen
	MD5: 60057a831f3498751e37413c45c29c4a	TBC
	MD5: d84a95d19f19eeee2415f41c2c181db8 **SHA256:** 5089f545aa94d273d18150102dc65c3a08b4335d6f171d9b3f655599d8589b0e	ELF/Agen

	MD5: 4c375c7ac9ee2f8a04c920381683e811 **SHA256:** 7edd6af205e748d13641bf3d3209bc69ab062b71db06700277b337f3b026700e	ELF/Agen
/bin/httpsng	**MD5:** 7454bb4b3dfe4f4386980b63f119c208 **SHA256:** 1b7af533f32a1c0bb62420be787d9e02c8a71bca77f2b0857dd20599f8833853	ELF/Agen
	MD5: f5caae23ace1ee0b48d02427b08f0bad **SHA256:** 534632ae386cf4d2190ef03be08a96f25fb3a9537d1c380141d36d797b983705	ELF/Agen
/bin/smit	**MD5:** fc78c1800fbe25e57a7333ca51e183b6 **SHA256:** b8bd746e4713e101266d74bbe8cfbf064b5979adb8df68076d295df9e0a215d0	ELF/Agen
	MD5: 247139079d8a1c2534ef0d2b726d8ebb **SHA256:** 4860b98219177aacb786b1a2d5c68e999c0c8cf6c6400c7fe773fb18f44c78be	ELF/Agen
	MD5: 2fc1aa1ab1ecde77eb6724f7385d5749 **SHA256:** 46ac81f19c996d9a2e257ef584455a721aad15f1cdeb597e8f853e288b3e9070	ELF/Agen
	MD5: 2fc1aa1ab1ecde77eb6724f7385d5749 **SHA256:** 46ac81f19c996d9a2e257ef584455a721aad15f1cdeb597e8f853e288b3e9070	ELF/Agen
	MD5: cf49feb43667819b880422efbe89fd01 **SHA256:** 6a92e750eb4e84be875158e6ecb11ac3e4716c04ff32d29206bf7b1a4ec46edc	ELF/Agen
	MD5: 08039b1cbdf880a3d86f8646bb286709 **SHA256:** 2b1aa340384b5e889008839bc961fcb438379cc2de8be880664ae41fd9e77084	ELF/Agen
	MD5: bc1bd24e32fb6a778c1e79840e8ec78f **SHA256:** 51d0d5d83735a3a63a2405b4f9909676fc572827693f34b80799b0786a5f1677	ELF/Agen
	MD5: 823ae2645869e4fc9ebcb046aa760440	TBC
/tmp/busybox	**MD5:** ebce43017d2cb316ea45e08374de7315	N/A
/data2/libcrashpad.so	**MD5:** e9f64481280c964a6a5dbf551e9cf6f0 **SHA256:** 7075c5595ac2b34c8f5cf99aeeae0a99b10df100cfb5362f9a2a033ce4451a0e	ELF/Agen
	MD5: 9db3c6c29b4028ccd63ee38b62620df7 **SHA256:** 9af6b6b1ce11ab62a95f3990cdf9b0f3d4bc722f662d80116bcdabdd302f4aee	ELF/Agen
	MD5: 5b2882b0a4de3210e1bfa5db1ed63713 **SHA256:** ef7f71ea1c7f35c8a28fc2e98fa9e59b8e2d0f0bea84a527cf2c20ccc4f8b816	ELF/Agen

	MD5: aa53393374e3ec355c0071adeba535eb **SHA256:**	ELF/Agen
	MD5: dbe0d8d612ad89229cd6175e37157f3c	TBC
	MD5: 604d909d4d8d69c07e3474ceaf379f20 **SHA256:** ddc68e6647f9abcf23206d2fbcbccb4459d7f545abfc9b2e12ebba2e5a29bcd1	ELF/Agen
	MD5: 78310bad651eff14e5ecefe674630e75 **SHA256:** 1103c2cd47fd62d2c9353edb5c2dce23173c15770594237b84e01635723b0eec	ELF/Agen
/data2/tftpd	**MD5:** cf3e6cb8ada288aa2d1bc39d1ce2ad54 **SHA256:** a322034e610aa07632ade4323d37d55c5c613b155ef51b05ab83de4159c231b2	ELF/Agen
	MD5: 0909a8ee77fbd40ab461df20600ddae0 **SHA256:** ba0b6b0c6b628dffcf0f34fa78fb61acb6c1b457f7b5addadbe4dba575bac5bd	ELF/Agen
	MD5: 953813bb2137e351709d98a91336eb25 **SHA256:** 65a9314fc3fac8cc238534d81c12e2080820f86a58299113c164aea4cd18f11c	ELF/Agen
	MD5: b11faf42afeca35920a248001b90e997	N/A
/lib/libaprhelper.so	**MD5:** 9e898f389003f9141831856f021fda3a **SHA256:** 80d03d5d35a7b9bde7e5e60f0df3baa0c51cbbd9214d875cd1967f589b9df183	ELF/Agen
	MD5: 9d2bc4e59357b56199b709a599600fa7	
	MD5: 176220a8ac6f344aaf620efab5c6f276 **SHA256:** 7a86b793612a6b6a3f27d7c24eec4c75202915c7c2c36b786c39ef95628b1286	ELF/Agen
	MD5: 2349d1d1acb69e91aea5be7767254f81 **SHA256:** 1209b5ff4755e689e260e680caf33b52ecd3fa8a1bb20ff06d7770828490baee	ELF/Agen
	MD5: 9d7b6fc9a0702381062726f634d0df0f **SHA256:** 43c1905b2078a8de9d0fa42e16465692066825e3dcb42a17cbf40b77736527c2	ELF/Agen
	MD5: b32ad75ce0494586a8b278c0413c0406	N/A
	MD5: e7ab34f7df83ce3ed6bf287332f7ce73 **SHA256:** 80d03d5d35a7b9bde7e5e60f0df3baa0c51cbbd9214d875cd1967f589b9df183	ELF/Agen
	MD5: 8b2c08f4e558626f34494b171e21f644 **SHA256:** a667edc691e9950ec0bc92e9f2cdcb7e99a086286063864040435f26537f9d9b	
/data2/libunwind.1.so	**MD5:** e9c2a3efaa97462168790b2fe234a7ba **SHA256:** 5700a8d9f00ebeb52536d16701522ecf6a07deb660e442cd67acdfb768e17c39	ELF/Agen

/data2/httpdng	**MD5:** f84a5eff50af2a7bfae49345b3b3ce1e **SHA256:** 662dd91647c45df0625c011565a60f18e0de47b9e57653763868205f4026593f	ELF/Agen
	MD5: e1aff3203fd38fc4790157d908ef742a	
	MD5: f66c0c328d40cffdb0d8dfa0444fe923	
	MD5: 7aaaf17e4e3638d2f93b1cf5a1579ac6 **SHA256:** 0088cfd5b4b7195edab836236ba0c6a0c2aded3e4b8a842f11ee4e9c5e4ae3c1	ELF/Agen
/lib/libaprsd.so	**MD5:** dc95090cca508d1196b972c385dc3405 **SHA256:** 89e049fd0df33da453fe04d9b2f9619b46dac0fceb7a8156560cce08fce3d8b7	ELF/Agen
	MD5: 834e542076e7c37e848fb68b3671f7a1	
	MD5: 62ef5ec4adbd655adcc418d7ba2262ac	
	MD5: 9d7a1a536eef0ff1e87ee1d78ac7bc69 **SHA256:** 1748035e9cb1932bbe6c3aa93c2ae044296e0f0774d0aa0d3eb688cdd2c0b2f2	ELF/Agen
/bin/toybox	**MD5:** d0a31975a436d0fe3b4f990c5003ca59	Clean
/tmp/.ptyagent	**MD5:** 2d88911f67a2cce7fa97cdf0ae59a027 **SHA256:** 910e7fc043560fbc2757304503de38a8824238765b2d91d87b974fefa253e311	ELF/Agen
	MD5: ca5184d43691ee8d8619377e600fa117 **SHA256:** 70372f95fa5cf917639007ae25a67a53d0297b67792b00bbea63ce0b170f95b8	Linux/Chi
/data/lib/libav.so.new/libav.so	**MD5:** 30009c9052e588b93fb12e918bbcecfb **SHA256:** 6584f614fb0ef864cd5aa5b6ec1b42299f2b639a23e4b1e853caf3b2f2254b14	ELF/Agen
/data2/.vile/ketg	**MD5:** e9ae2188d7a46fdac30b192b7405cba2 **SHA256:** 8f380a844011daa8854798bf31981b660bf752e95c2e41ae50c0306275b5c0ed	Agent.CB
/SYSV64564856	**MD5:** 8771305a111e1b38ada954513af4507c **SHA256:** a25a7a7e3bcdc66545db1d62d3b09339ea7abef2a9731707f521a10338b5f563	ELF/Agen
/data2/.vile/ith	**MD5:** 8d4c9b498da847c3690260bb28f046f9 **SHA256:** 75ce32c1e3ba902f7dcbf5bce63347448a94537682cebdde6d93efb2ede3f81c	ELF/Agen
/data2/.vile/dnpfmn	**MD5:** 3977f8b8f5ec13604819f45282fd9b71 **SHA256:** adb1b6fc93a0225a203ec64a48470072b5d5c43d8f15860ee03f24673d9d97fe	ELF/Agen
/data2/.vile/lmcdle	**MD5:** 3fba828577e745c8a51d657cc393f461 **SHA256:** 20de58db0cfb04ce0abde662ca84b00ca7135bb546e2d32865046c3e4acc1b92	ELF/Agen
/data2/.vile/fmteld	**MD5:** 46c59ceb4ded468d692a92e34df75988	

/data2/brodel	**MD5:** 96e74f0f463eadeded69db5d0efde628	
/data2/liblink.so.1	**MD5:** 031e21168d7e783d26998e63217a365c **SHA256:** dfafeb3efaba2c8e5d80ec7a37c00805895df1a47333515082da54e49a388a59	ELF/Agen
/data2/fortlinkd:	**MD5:** d97bae365bd4c3fbf2eb834d678dbd11 **SHA256:** bfc20c8e21fa4674492576961baedae90f7794a8534d2ad3ef4e230de2fb38ab	ELF/Agen
/bin/fgfm	**MD5:** 83d5c75bf1d2090a6cceaf2a80d906da	
/data2/lib/* (Bash Scripts)	**MD5:** 33423931a013dfc4a41beb3c5faee2a8 **MD5:** 559b728ba316528a21b80e87447c2f47 **MD5:** 2d973c9863e70cd41578a4046990501a **MD5:** 93104b1c37cb4478df45b5ba8ea0ff62	N/A
Authd	**MD5:** 9124ce75319514561156d2013fc9d3be **SHA256:** f40c04fb9e2d4157a0bc753925dbc5f757feb77cdd22f90fedf3cc5e095143bc	ELF/Agen
Httpsd	**MD5:** 218a3525ab8e46f7afe252d050a86907 **SHA256:** 3ed99aad5922744b6a75ea90ea6ece81ba0d8eb9935aec38b897e44ac3b36c35	ELF/Agen
Liblog.so	**MD5:** e24d14d3e6c6de0ed3db050dd5c935f0 **SHA256:** a79f80158ebbf9e34f6a7ec86b564de2fbee783fe6c1e20eefe2832226e2f827	ELF/Agen
Libpe.so	**MD5:** 6c0adca790235445d07be98cd0f820b5 **SHA256:** 50451bb5b6d68115695a6cb277839a6dd2bad8f70bdb8b79670b18dcde188965	ELF/Agen
Newcli	**MD5:** ab89139e3d47fbaba2da33040da95200 **SHA256:** 2acc6a2a931db63fe3a875780f00192a60955c9794df68fe0ace0012d309b04f	ELF/Agen
Packfile	**MD5:** 201ee76e996846d5ea3fc03bac3273dd **SHA256:** 4591b4fb1c93c27203b36c773597fd3f885338ad7641dcebf8ed2395acdf4a5f	Data/Agen
Preload.so	**MD5:** a62377c01935f366761846b5ceed5a49 **SHA256:** 1c437dc9e929669e5a65a1c70afb3107fba471afb9ad35e3848334c9332f2b59	ELF/Agen
Sh	**MD5:** 991461b86aebecfd096dc11ff2a04b4b **SHA256:** dcd9a5af1c6297ed1a66c851efa305000335d8ade068ba515125a6612f1d5300	NA
Smartctl	**MD5:** 205a8c6049061930490b2482855babcd **SHA256:** 4519baebba73827e2b33f36f835d6cb704755abf1312d8d197be635f4d9ffade	NA

For details of the Fortinet PSIRT Policy and to report a vulnerability: https://www.fortiguard.com/psirt_policy.