Shikitega - New stealthy malware targeting Linux

cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux

1. AT&T Cybersecurity
2. Blog

September 6, 2022 | Ofer Caspi

Executive summary

AT&T Alien Labs has discovered a new malware targeting endpoints and IoT devices that are running Linux operating systems. Shikitega is delivered in a multistage infection chain where each module responds to a part of the payload and downloads and executes the next one. An attacker can gain full control of the system, in addition to the cryptocurrency miner that will be executed and set to persist.

Key takeaways:

- The malware downloads and executes the Metasploit's “Mettle” meterpreter to maximize its control on infected machines.
- Shikitega exploits system vulnerabilities to gain high privileges, persist and execute crypto miner.
- The malware uses a polymorphic encoder to make it more difficult to detect by anti-virus engines.
- Shikitega abuse legitimate cloud services to store some of its command and control servers (C&C).

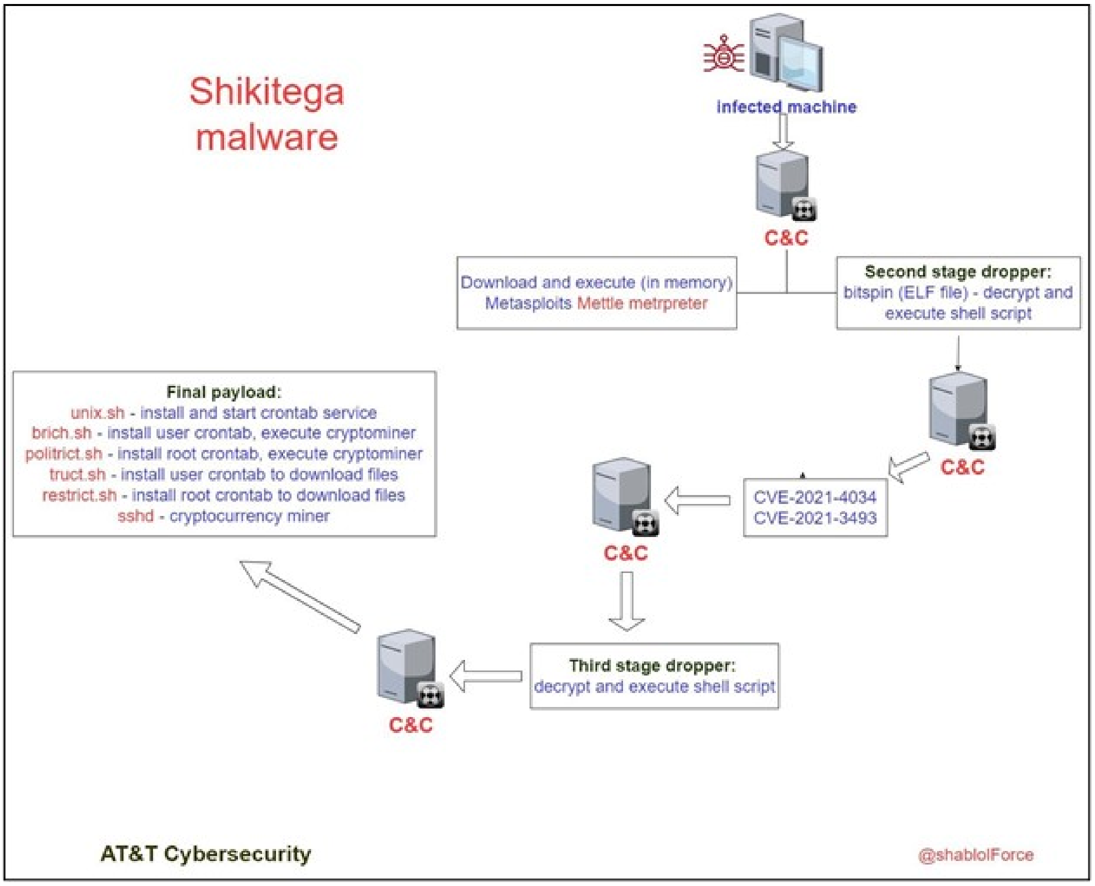

Figure 1. Shikitega operation process.

Background

With a rise of nearly 650% in malware and ransomware for Linux this year, reaching an all-time high in the first half year of 2022, threat actors find servers, endpoints and IoT devices based on Linux operating systems more and more valuable and find new ways to deliver their malicious payloads. New malwares like BotenaGo and EnemyBot are examples of how malware writers rapidly incorporate recently discovered vulnerabilities to find new victims and increase their reach.

Shikitega uses an infection chain in multiple layers, where the first one contains only a few hundred bytes, and each module is responsible for a specific task, from downloading and executing Metasploit meterpreter, exploiting Linux vulnerabilities, setting persistence in the infected machine to downloading and executing a cryptominer.

Analysis

The main dropper of the malware is a very small ELF file, where its total size is around only 370 bytes, while its actual code size is around 300 bytes. (figure 2)

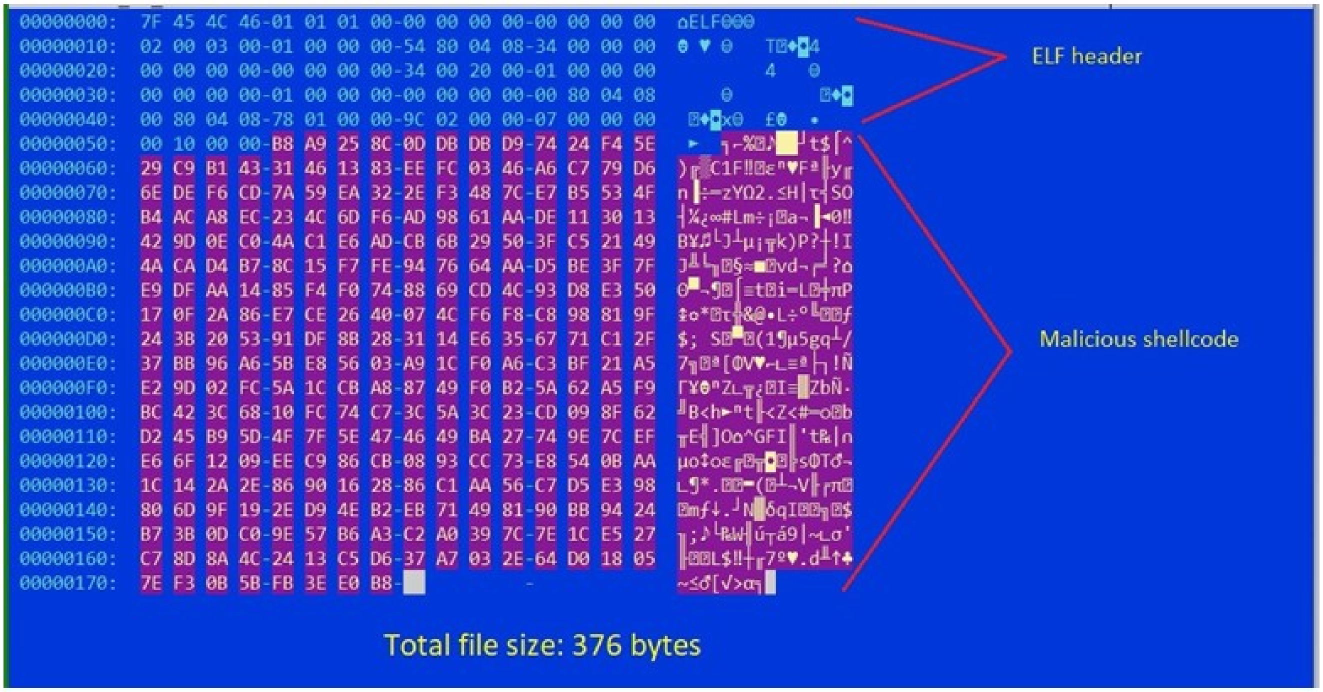

Figure 2. Malicious ELF file with a total of only 376 bytes.

The malware uses the “Shikata Ga Nai” polymorphic XOR additive feedback encoder, which is one of the most popular encoders used in Metasploit. Using the encoder, the malware runs through several decode loops, where one loop decodes the next layer, until the final shellcode payload is decoded and executed. The encoder stud is generated based on dynamic instruction substitution and dynamic block ordering. In addition, registers are selected dynamically. Below we can see how the encoder decrypts the first two loops: (figures 3 and 4)

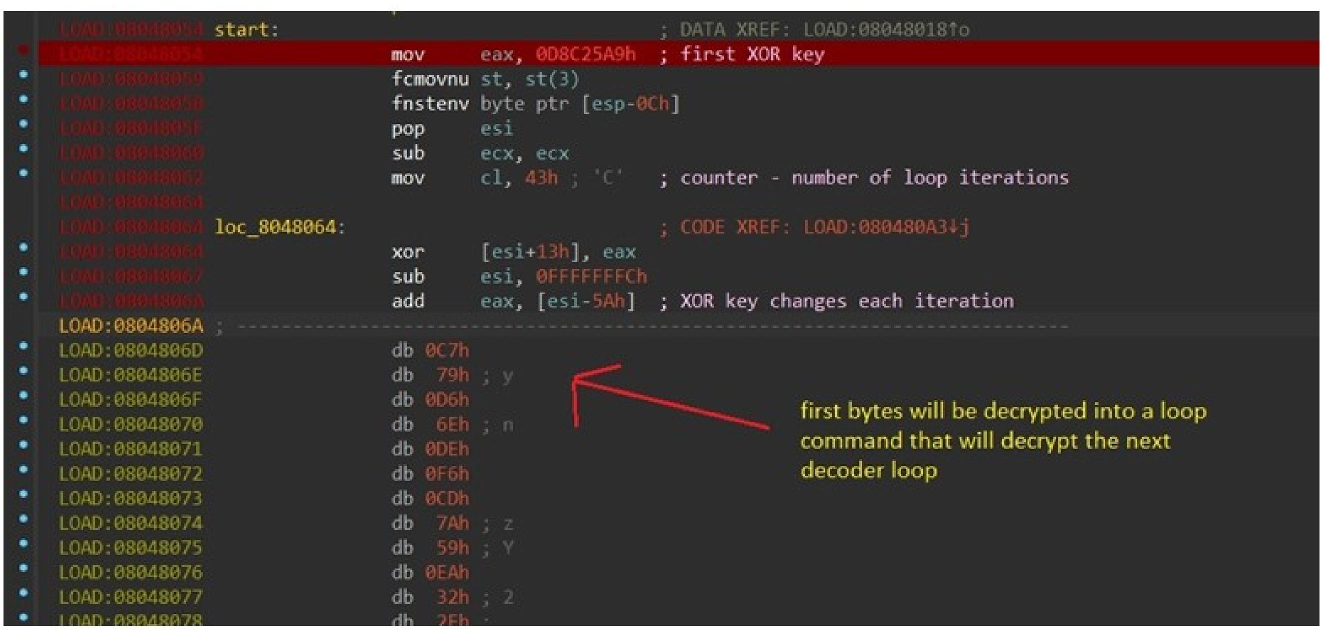

Figure 3. First “Shikata Ga Nai” decryption loop.

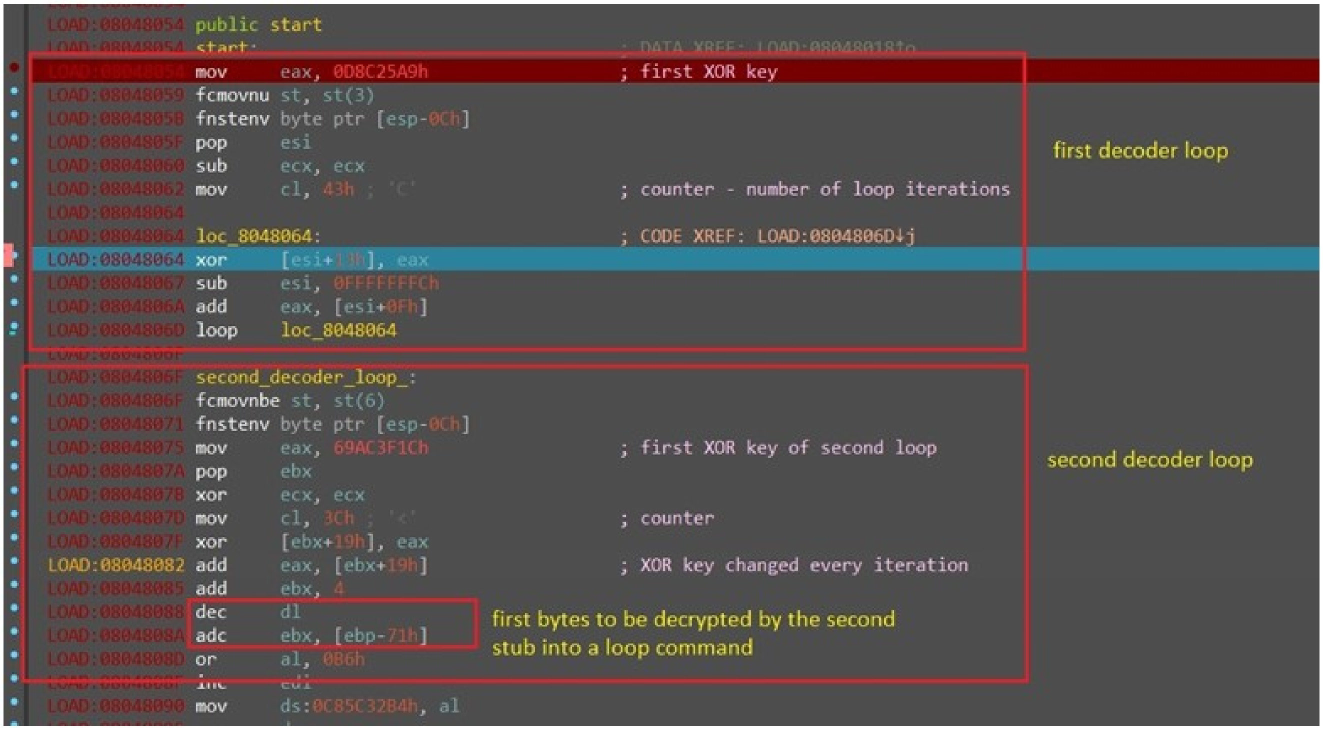

Figure 4. Second “Shikata Ga Nai” decryption loop created by the first one.

After several decryption loops, the final payload shellcode will be decrypted and executed. As the malware does not use any imports, it uses ‘int 0x80’ to execute the appropriate syscall. As the main dropper code is very small, the malware will download and execute additional commands from its command and control by calling 102 syscall (sys_socketcall). (Figure 5)

Figure 5. Calling system functions using interrupts

The C&C will respond with additional shell commands to execute, as seen in the packet capture in figure 6. The first bytes marked in blue are the shell commands that the malware will execute.

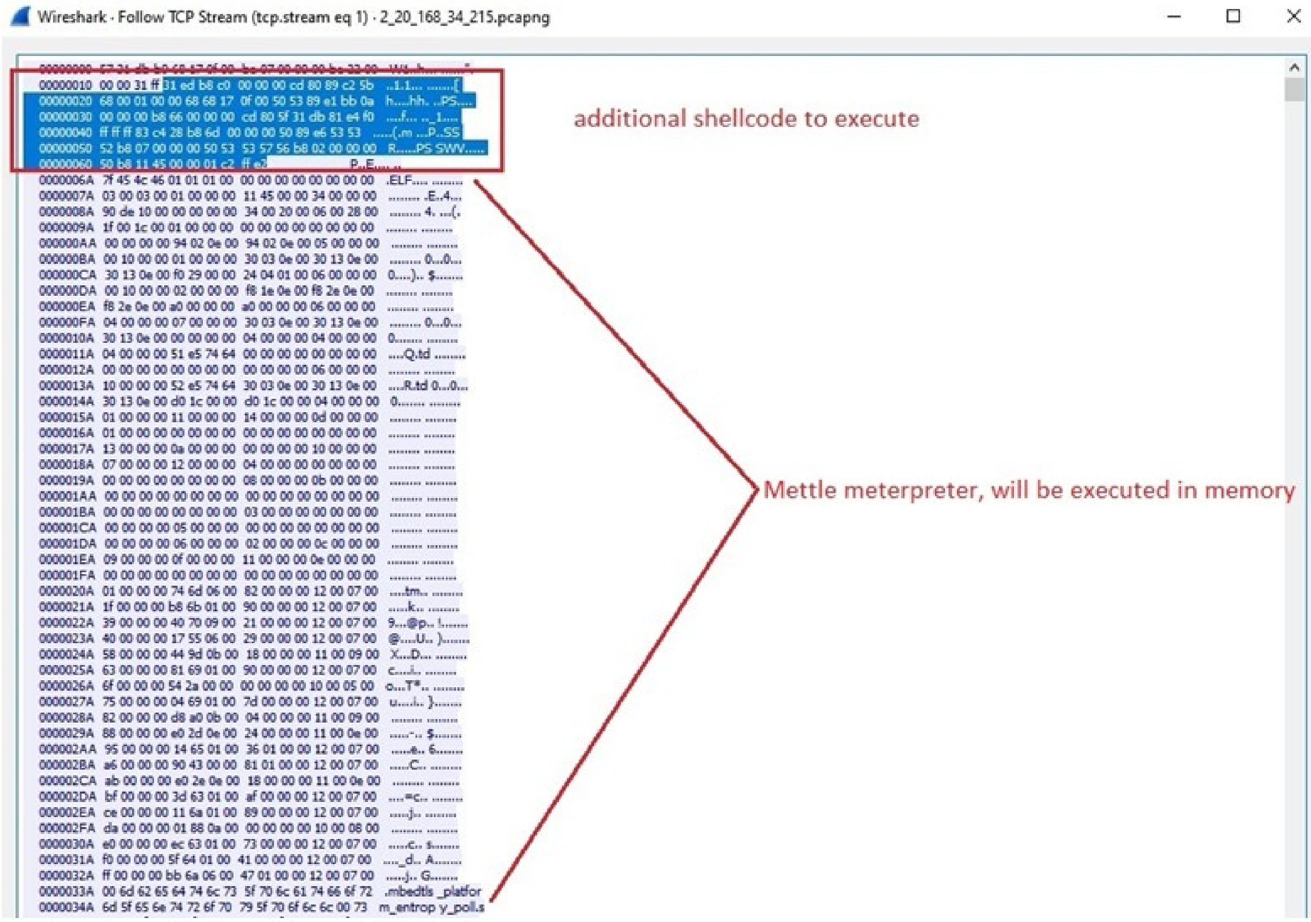

Figure 6. Additional commands received from C&C.

The received command will download additional files from the server that won't be stored in the hard drive, but rather will be executed from memory only. (Figure 7)

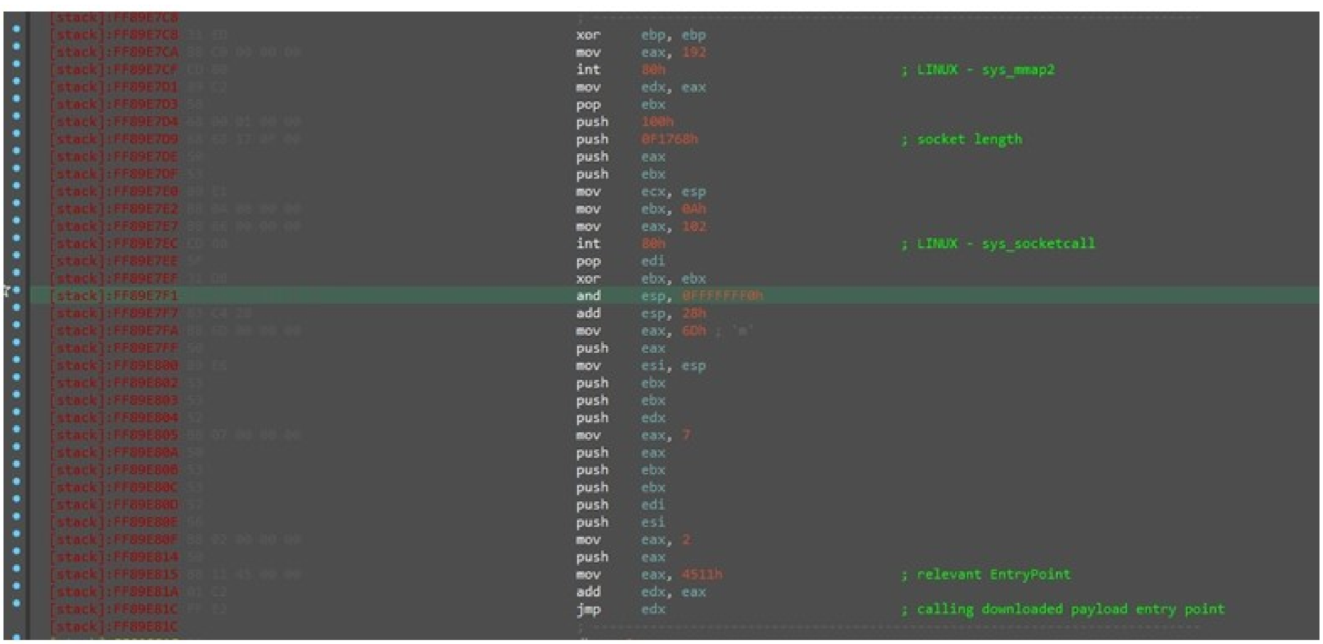

Figure 7. Executes additional shell code received from C&C.

In other malware versions, it will use the “execve” syscall to execute ‘/bin/sh’ with command received from the C&C. (figure 8)

Figure 8. Executing shell commands by using syscall_execve.

The malware downloads and executes ‘Mettle’, a Metasploit meterpreter that allows the attacker to use a wide range of attacks from webcam control, sniffer, multiple reverse shells (tcp/http..), process control, execute shell commands and more.

In addition the malware will use wget to download and execute the next stage dropper.

Next stage dropper

The next downloaded and executed file is an additional small ELF file (around 1kb) encoded with the “Shikata Ga Nai” encoder. The malware decrypts a shell command that will be executed by calling syscall_execve with ‘/bin/sh” as a parameter with the decrypted shell. (Figure 9)

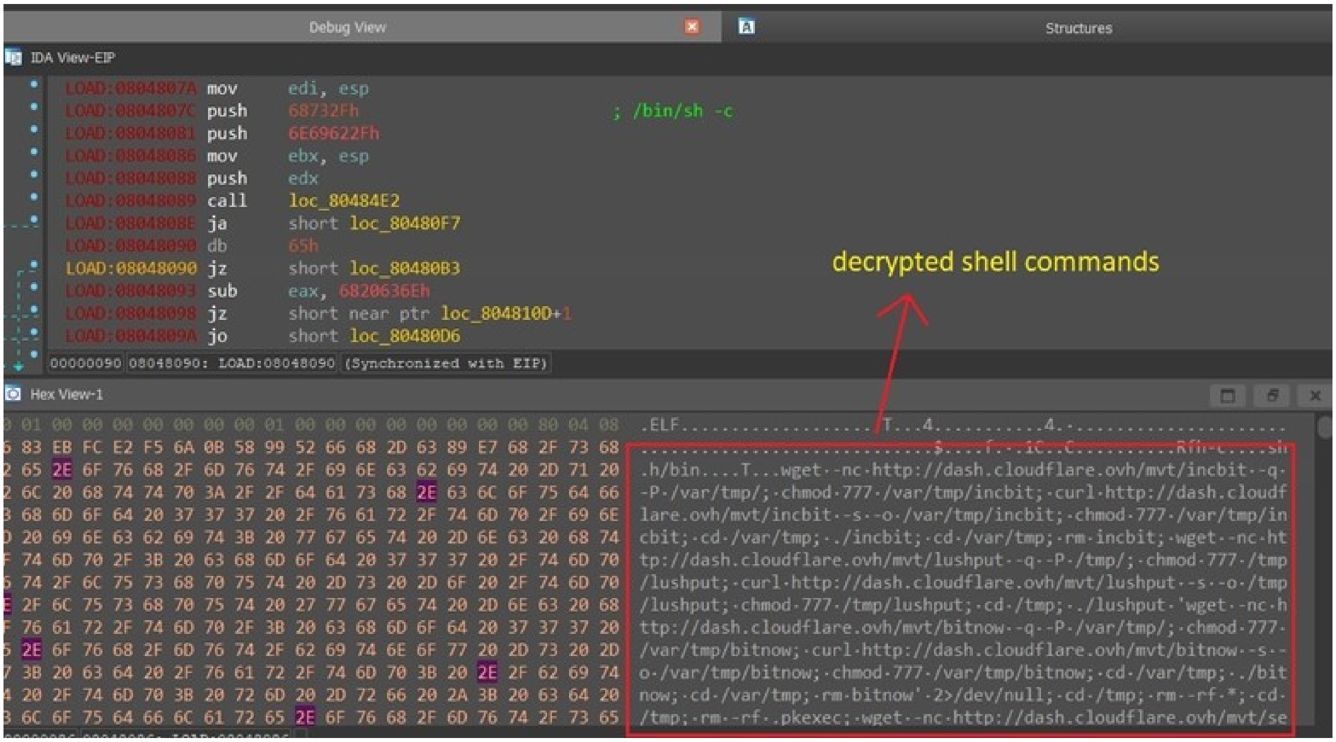

Figure 9. Second stage dropper decrypts and executes shell commands.

The executed shell command will download and execute additional files. To execute the next and last stage dropper, it will exploit two linux vulnerabilities to leverage privileges - CVE-2021-4034 and CVE-2021-3493 (figure 10 and 11).

Figure 10. Exploiting Linux vulnerability CVE-2021-3493.

Figure 11. Exploiting CVE-2021-4034 vulnerability.

The malware will leverage the exploit to download and execute the final stage with root privileges - persistence and cryptominer payload.

Persistence

To achieve persistence, the malware will download and execute a total of 5 shell scripts. It persists in the system by setting 4 crontabs, two for the current logged in user and the other two for the user root. It will first check if the crontab command exists on the machine, and if not, the malware will install it and start the crontab service.

To make sure only one instance is running, it will use the flock command with a lock file “/var/tmp/vm.lock”.

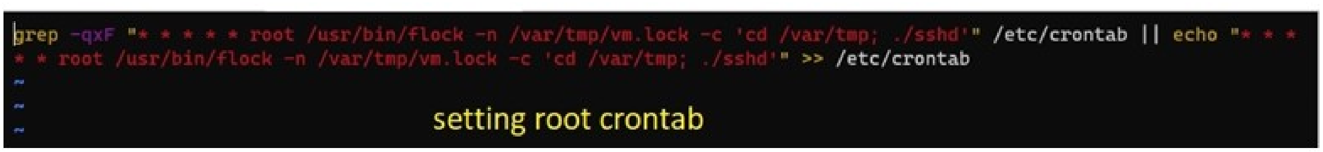

Figure 12. Adding root crontab to execute the final payload.

Below is the list of downloaded and executed script to achieve persistence:

script name	details
unix.sh	Check if “crontab” commands exist in the system, if not install it and start the crontab service.
brict.sh	Adds crontab for current user to execute cryptominer.
politrict.sh	Adds root crontab to execute cryptominer.
truct.sh	Adds crontab for current user to download cryptominer and config from C&C.

script name	details
restrict.sh	Adds root crontab to download cryptominer and config from C&C.

As the malware persists with crontabs, it will delete all downloaded files from the system to hide its presence.

Cryptominer payload

The malware downloads and executes XMRig miner, a popular miner for the Monero cryptocurrency. It will also set a crontab to download and execute the crypto miner and config from the C&C as mentioned in the persistence part above.

Figure 13. XMRig miner is downloaded and executed on an infected machine.

Command and control

Shikitega uses cloud solutions to host some of its command and control servers (C&C) as shown by OTX in figure 14. As the malware in some cases contacts the command and control server using directly the IP without domain name, it's difficult to provide a complete list of indicators for detections since they are volatile and they will be used for legitimate purposes in a short period of time.

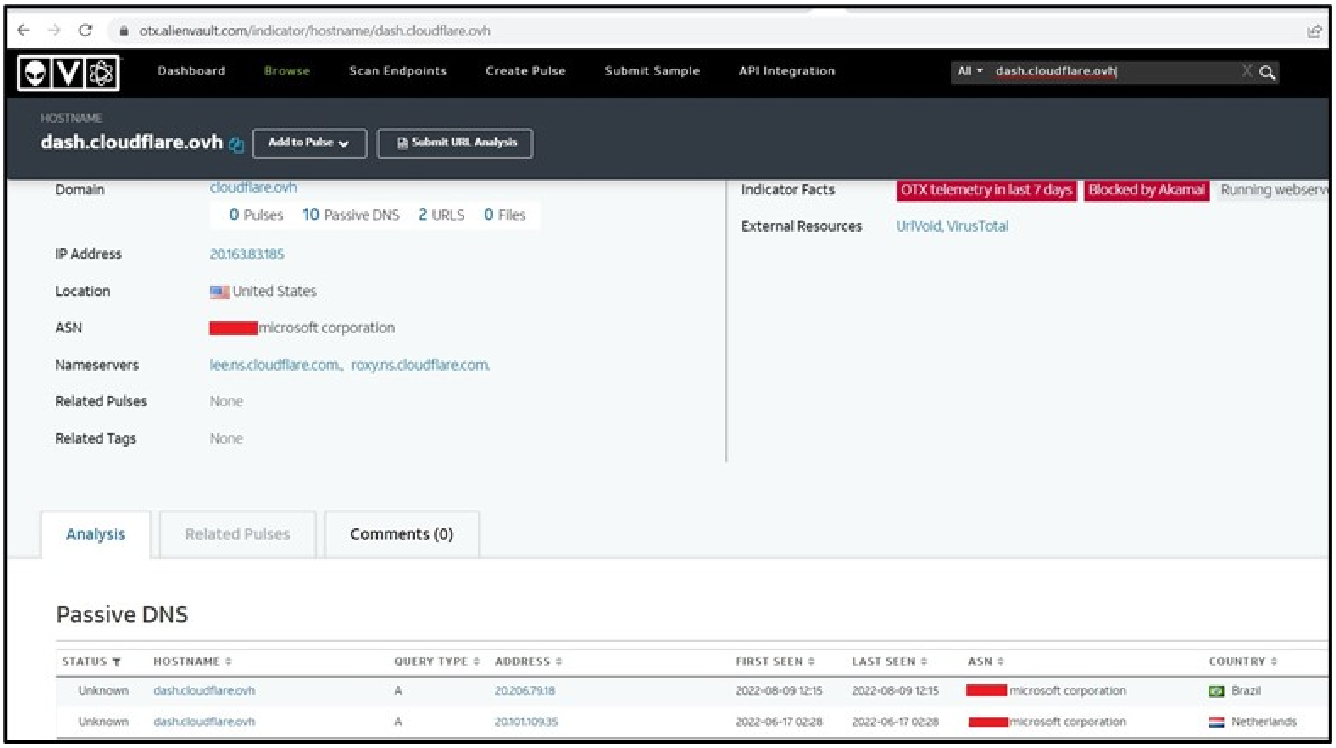

Figure 14. Command and control server hosted on a legitimate cloud hosting service.

Recommended actions

1. Keep software up to date with security updates.
2. Install Antivirus and/or EDR in all endpoints.
3. Use a backup system to backup server files.

Conclusion

Threat actors continue to search for ways to deliver malware in new ways to stay under the radar and avoid detection. Shiketega malware is delivered in a sophisticated way, it uses a polymorphic encoder, and it gradually delivers its payload where each step reveals only part of the total payload. In addition, the malware abuses known hosting services to host its command and control servers. Stay safe!

Associated Indicators (IOCs)

The following technical indicators are associated with the reported intelligence. A list of indicators is also available in the OTX Pulse. Please note, the pulse may include other activities related but out of the scope of the report.

TYPE	INDICATOR	DESCRIPTION
DOMAIN	dash[.]cloudflare.ovh	Command and control
DOMAIN	main[.]cloudfronts.net	Command and control

SHA256	b9db845097bbf1d2e3b2c0a4a7ca93b0dc80a8c9e8dbbc3d09ef77590c13d331	Malware hash
SHA256	0233dcf6417ab33b48e7b54878893800d268b9b6e5ca6ad852693174226e3bed	Malware hash
SHA256	f7f105c0c669771daa6b469de9f99596647759d9dd16d0620be90005992128eb	Malware hash
SHA256	8462d0d14c4186978715ad5fa90cbb679c8ff7995bcefa6f9e11b16e5ad63732	Malware hash
SHA256	d318e9f2086c3cf2a258e275f9c63929b4560744a504ced68622b2e0b3f56374	Malware hash
SHA256	fc97a8992fa2fe3fd98afddcd03f2fc8f1502dd679a32d1348a9ed5b208c4765	Malware hash
SHA256	e4a58509fea52a4917007b1cd1a87050b0109b50210c5d00e08ece1871af084d	Malware hash
SHA256	cbdd24ff70a363c1ec89708367e141ea2c141479cc4e3881dcd989eec859135d	Malware hash
SHA256	d5bd2b6b86ce14fbad5442a0211d4cb1d56b6c75f0b3d78ad8b8dd82483ff4f8	Malware hash
SHA256	29aafbfd93c96b37866a89841752f29b55badba386840355b682b1853efafcb8	Malware hash
SHA256	4ed78c4e90ca692f05189b80ce150f6337d237aaa846e0adf7d8097fcebacfe7	Malware hash
SHA256	130888cb6930500cf65fc43522e2836d21529cab9291c8073873ad7a90c1fbc5	Malware hash
SHA256	3ce8dfaedb3e87b2f0ad59e1c47b9b6791b99796d38edc3a72286f4b4e5dc098	Malware hash
SHA256	6b514e9a30cbb4d6691dd0ebdeec73762a488884eb0f67f8594e07d356e3d275	Malware hash
SHA256	7c70716a66db674e56f6e791fb73f6ce62ca1ddd8b8a51c74fc7a4ae6ad1b3ad	Malware hash
SHA256	2b305939d1069c7490b3539e2855ed7538c1a83eb2baca53e50e7ce1b3a165ab	Malware hash CVE-2021-3493
SHA256	4dcae1bddfc3e2cb98eae84e86fb58ec14ea6ef00778ac5974c4ec526d3da31f	Malware hash CVE-2021-4034
SHA256	e8e90f02705ecec9e73e3016b8b8fe915873ed0add87923bf4840831f807a4b4	Malware hash
SHA256	64a31abd82af27487985a0c0f47946295b125e6d128819d1cbd0f6b62a95d6c4	Malware shell script

SHA256	623e7ad399c10f0025fba333a170887d0107bead29b60b07f5e93d26c9124955	Malware shell script
SHA256	59f0b03a9ccf8402e6392e07af29e2cfa1f08c0fc862825408dea6d00e3d91af	Malware shell script
SHA256	9ca4fbfa2018fe334ca8f6519f1305c7fbe795af9eb62e9f58f09e858aab7338	Malware shell script
SHA256	05727581a43c61c5b71d959d0390d31985d7e3530c998194670a8d60e953e464	Malware shell script
SHA256	ea7d79f0ddb431684f63a901afc596af24898555200fc14cc2616e42ab95ea5d	Malware hash

Mapped to MITRE ATT&CK

The findings of this report are mapped to the following MITRE ATT&CK Matrix techniques:

- TA0002: Execution
  - T1059: Command and Scripting Interpreter
  - T1569: System Service
    - T1569.002: Service Execution
- TA0003: Persistence
  - T1543: Create or Modify System Process
- TA0005: Defense Evasion
  - T1027: Obfuscated Files or Information

Share this with others

Tags: malware research, otx, shikitega