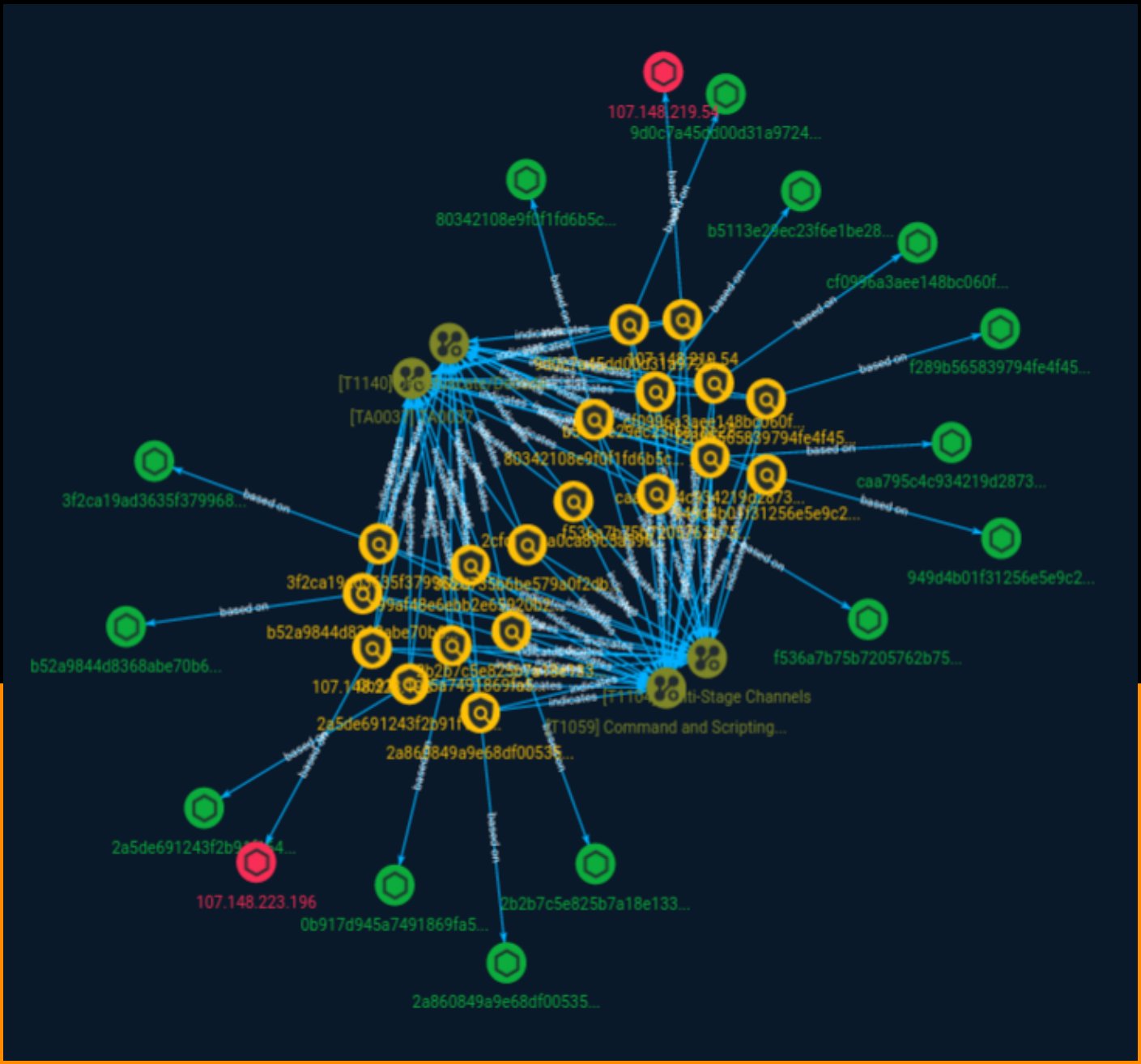
Jul 31 2023

NETMANAGEIT

# Intelligence Report

# MAR-10454006-r3.v1

# Exploit Payload Backdoor



# Table of contents

## Overview



## Entities



## Observables



## External References

# Overview

## 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.

## Confidence

*This value represents the confidence in the correctness of the data contained within this report.*

15 / 100

# Indicator

| Name |
| --- |
| 0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6'] |
| **Name** |
| b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = 'b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2'] |
| **Name** |

2cfdeac9a0ca89c5a5962824520485cfa44d6f12

**Pattern Type**

yara

**Pattern**

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*) }

**Name**

2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b']

**Name**

b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321']

**Name**

cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba']

**Name**

2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095']

**Name**

9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5']

**Name**

caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd']

**Name**

3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7']

**Name**

f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0

**Description**

SHA256 of dc5841d8ed9ab8a5f3496f2258eafb1e0cedf4d3

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0']

**Name**

80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043']

**Name**

2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7']

**Name**

949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788

**Description**

SHA256 of 1903a3553bcb291579206b39e7818c77e2c07054

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788']

**Name**

99af48e6ebb2e65920b293c78635c9d8085fc488

**Pattern Type**

yara

**Pattern**

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 }

**Name**

f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa']

**Name**

362d735b6be579a0f2dbcdb0b8fadc096696b609

**Pattern Type**

yara

**Pattern**

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 }

**Name**

107.148.223.196

**Description**

**ISP:** PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDAZ25kl/65CXE2WXB2k5TnAxK4CUjQ1lOY/YqTHkO9511m tZrbEI0wMactZJ8eH4w7i/MF8zn4CZIlyYWMOJKi5obIysCtozkO35HeRnJRAMIufl4GftzlH+xY hx6/ygJXod01Uqs8w83xpRYnxpNPhEUlEMQMY0JIkGwF3yt1/iGMWNtyBP0nXeCoXQoWG6fY0IN+JHCly4pRnxPVmnKwYoY6DsPyqMuZDIndhbYMm/Aitz84lEk85pE96nUPiIHLJfdJH/NqFmL9g+WHe7CYxfShx/0m2idxpibyKw43DVSwy5GsOMf/RmAvyWql8i4hAgudyKK8rsw9W/sskVqN Fingerprint: 3e:a3:bf:39:6f:3c:20:22:72:f5:f8:69:45:35:60:b1 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ```
---

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '107.148.223.196']

**Name**

107.148.219.54

**Description**

CC=US ASN=AS54600 PEGTECHINC

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '107.148.219.54']

# Attack-Pattern

| Name |
| --- |
| TA0037 |
| **ID** |
| TA0037 |
| **Name** |
| Multi-Stage Channels |
| **ID** |
| T1104 |
| **Description** |
| Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup |

first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

**Name**

Command and Scripting Interpreter

**ID**

T1059

**Description**

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

**Name**

Deobfuscate/Decode Files or Information

**ID**

T1140

## Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

# StixFile

| Value |
| --- |
| f536a7b75b7205762b75a037ebf6503029aab1a02afab14b2709797c32e7e0fa |
| 3f2ca19ad3635f379968b0302c7e42cf954f85ab61166c6f70acfebc72f38ab7 |
| cf0996a3aee148bc060f4726435dd0d7f1af79082277f407dfa07d81181322ba |
| 0b917d945a7491869fa5003f6b85c09f5f45795a7852a8b63ba1abdc9797d6a6 |
| 9d0c7a45dd00d31a9724fa9e96cb8ac99dd5a6502fe4515cedaabb2e58b1c5f5 |
| f289b565839794fe4f450ed0c9343b8fb699f97544d9af2a60851abc8b4656e0 |
| b52a9844d8368abe70b6ba0d8df84f88c8c0029dcbcf599665acd703b255d5d2 |
| b5113e29ec23f6e1be289b99dc7ac2af1c252b4b6ff6e977f7827ab7fd686321 |
| 949d4b01f31256e5e9c2b04e557dcca0a25fc2f6aa3618936befc7525e1df788 |
| 80342108e9f0f1fd6b5c44e88006cebe37e4eccb3a0f567636b22ad210c0a043 |
| 2b2b7c5e825b7a18e13319b4a1275a0dd0086abd58b2d45939269d5a613a41e7 |
| 2a5de691243f2b91f164c3021c157fbd783b4f3e7d5f5950182e52ec868cd40b |
| caa795c4c934219d287379b20c2912af0f815de95bb73e0f02f5fe6eb9aa50bd |

2a860849a9e68df0053556b85f20010a1384b4c87594ba4f9bb3e1b1d287b095

# IPv4-Addr

| Value |
| --- |
| 107.148.223.196 |
| 107.148.219.54 |

# External References

- https://otx.alienvault.com/pulse/64c80719b55c4fd963785a4a
- https://www.cisa.gov/news-events/analysis-reports/ar23-209c