Jul 31 2023

NETMANAGEIT

Intelligence Report

MAR-10454006-r1.v2

SUBMARINE Backdoor

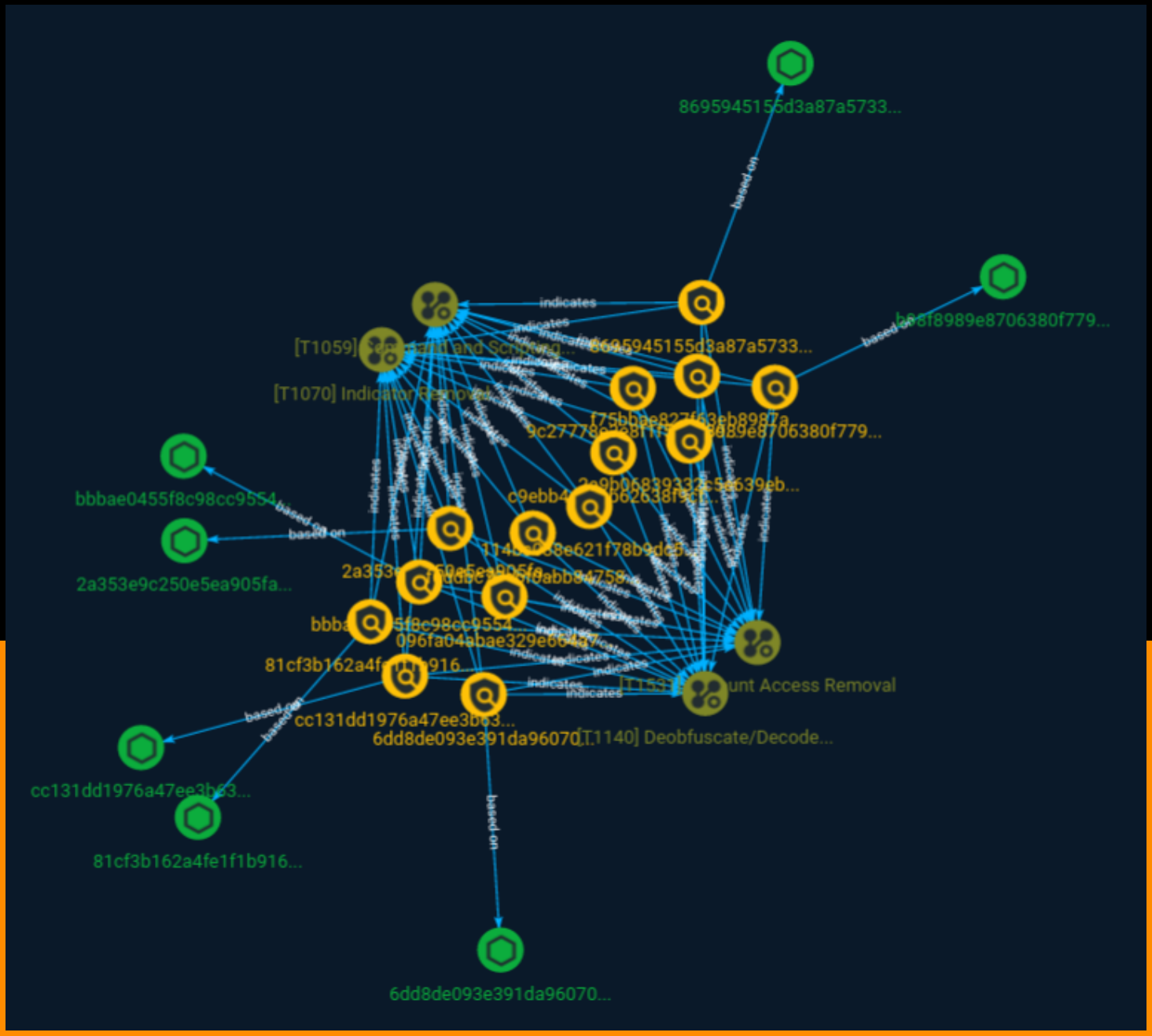

Table of contents

Overview

Entities

Observables

External References

Overview

Description

CISA obtained seven malware samples related to a novel backdoor CISA has named SUBMARINE. The malware was used by threat actors exploiting CVE-2023-2868, a former zero-day vulnerability affecting certain versions 5.1.3.001 - 9.2.0.006 of Barracuda Email Security Gateway (ESG).

Confidence

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

15 / 100

Indicator

Name
8695945155d3a87a5733d31bf0f4c897e133381175e1a3cdc8c73d9e38640239
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8695945155d3a87a5733d31bf0f4c897e133381175e1a3cdc8c73d9e38640239']
Name
cc131dd1976a47ee3b631a136c3224a138716e9053e04d8bea3ee2e2c5de451a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'cc131dd1976a47ee3b631a136c3224a138716e9053e04d8bea3ee2e2c5de451a']
Name

2a353e9c250e5ea905fa59d33faeaaa197d17b4a4785456133aab5dbc1d1d5d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2a353e9c250e5ea905fa59d33faeaaa197d17b4a4785456133aab5dbc1d1d5d5']

Name

bbbae0455f8c98cc955487125a791052353456c8f652ddee14f452415c0b235a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bbbae0455f8c98cc955487125a791052353456c8f652ddee14f452415c0b235a']

Name

f6ddbc70abf0abb8475846063b9d5124047adf3d

Pattern Type

yara

Pattern

rule CISA_10454006_04 : SUBMARINE trojan backdoor hides_artifacts hides_executing_code infects_files installs_other_components remote_access exploitation { meta: Author = "CISA

Code & Media Analysis" Incident = "10454006" Date = "2023-07-05" Last_Modified = "20230711_1500" Actor = "n/a" Family = "SUBMARINE" Capabilities = "hides-artifacts hides-executing-code infects-files installs-other-components" Malware_Type = "trojan backdoor" Tool_Type = "remote-access exploitation" Description = "Detects SUBMARINE launcher script samples" SHA256_1 = "b98f8989e8706380f779bfd464f3dea87c122651a7a6d06a994d9a4758e12e43" strings: $s1 = { 73 6c 65 65 70 } $s2 = { 7c 62 61 73 65 36 34 20 2d 64 } $s3 = { 4c 44 5f 50 52 45 4c 4f 41 44 } $s4 = { 2f 68 6f 6d 65 2f 70 72 6f 64 75 63 74 2f 63 6f 64 65 2f 66 69 72 6d 77 61 72 65 2f 63 75 72 72 65 6e 74 2f 73 62 69 6e 2f 73 6d 74 70 63 74 6c 20 72 65 73 74 61 72 74 } $s5 = { 65 63 68 6f 20 2d 6e 20 27 } $s6 = { 73 68 } $s7 = { 23 21 20 2f 62 69 6e 2f 73 68 } condition: filesize < 2KB and 6 of them }

Name

c9ebb4ccdcb62638f9cf4a452d8315eac21e17f0

Pattern Type

yara

Pattern

rule CISA_10454006_01 : SUBMARINE trojan backdoor remote_access_trojan remote_access information_gathering exploitation determines_c2_server controls_local_machine compromises_data_integrity { meta: Author = "CISA Code & Media Analysis" Incident = "10452108" Date = "2023-06-29" Last_Modified = "20230711_1500" Actor = "n/a" Family = "SUBMARINE" Capabilities = "determines-c2-server controls-local-machine compromises-data-integrity" Malware_Type = "trojan backdoor remote-access-trojan" Tool_Type = "remote-access information-gathering exploitation" Description = "Detects SUBMARINE Barracuda backdoor samples" SHA256_1 = "81cf3b162a4fe1f1b916021ec652ade4a14df808021eeb9f7c81c8d2326bddab" strings: $s1 = { 32 35 30 2d 6d 61 69 6c 32 2e 65 63 63 65 6e 74 72 69 63 2e 64 75 63 6b } $s2 = { 6f 70 65 6e 73 73 6c 20 61 65 73 2d 32 35 36 } $s3 = { 65 63 68 6f 20 2d 6e 20 27 25 73 27 20 7c 20 62 61 73 65 36 34 20 2d 64 } $s4 = { 2d 69 76 } $s5 = { 48 65 6c 6c 6f 20 25 73 20 5b 25 73 5d 2c 20 70 6c 65 61 73 65 64 20 74 6f 20 6d 65 65 74 20 79 6f 75 } $s6 = { e8 47 fa ff } $s7 = { 63 6f 6d 6d 61 6e 64 } $s8 = { 2d 69 76 20 36 39 38 32 32 62 36 63 } $s9 = { 73 65 6e 64 } $s10 = { 73 6f 63 6B 65 74 } $s11 = { 63 6f 6e 6e 65 63 74 } condition: filesize < 15KB and 8 of them }

Name

096fa04abae329e664a7b1d239fe09d063d70dab

Pattern Type

yara

Pattern

rule CISA_10454006_07 : SUBMARINE trojan dropper exploit_kit evades_av hides_executing_code hides_artifacts exploitation { meta: Author = "CISA Code & Media Analysis" Incident = "10454006" Date = "2023-07-11" Last_Modified = "20230711_1830" Actor = "n/a" Family = "SUBMARINE" Capabilities = "evades-av hides-executing-code hides-artifacts" Malware_Type = "trojan dropper exploit-kit" Tool_Type = "exploitation" Description = "Detects ESG FileName exploit samples" SHA256 = "8695945155d3a87a5733d31bf0f4c897e133381175e1a3cdc8c73d9e38640239" strings: $s1 = { 7c 20 62 61 73 65 36 34 20 2d 64 20 7c 20 73 68 } $s2 = { 65 63 68 6f 20 2d 6e } $s3 = { 59 32 46 30 49 43 39 32 59 58 49 76 64 47 31 77 4c 33 49 67 66 43 42 69 59 58 4e 6c 4e 6a 51 67 4c 57 51 67 4c 57 6b 67 66 43 42 30 59 58 49 67 } condition: filesize < 1KB and all of them }

Name

9c27778e3e8f1f51076c0481effc1d5a2dd5adbd

Pattern Type

yara

Pattern

rule CISA_10454006_03 : SUBMARINE trojan backdoor loader rootkit virus controls_local_machine hides_artifacts infects_files installs_other_components remote_access exploitation information_gathering { meta: Author = "CISA Code & Media Analysis" Incident = "10454006" Date = "2023-07-03" Last_Modified = "20230711_1500" Actor = "n/a" Family = "SUBMARINE" Capabilities = "controls-local-machine hides-artifacts infects-files installs-other-components" Malware_Type = "trojan backdoor loader rootkit virus" Tool_Type = "remote-access exploitation information-gathering" Description = "Detects SUBMARINE launcher script samples" SHA256_1 = "bbbae0455f8c98cc955487125a791052353456c8f652ddee14f452415c0b235a" strings: $s1 = { 73

65 64 20 2d 69 } $s2 = { 4c 44 5f 50 52 45 4c 4f 41 44 3d } $s3 = { 6c 69 62 75 74 69 6c 2e 73 6f } $s4 = { 2f 73 62 69 6e 2f 73 6d 74 70 63 74 6c } $s5 = { 2f 62 6f 6f 74 2f 6f 73 5f 74 6f 6f 6c 73 } $s6 = { 72 6d 20 2d 72 66 } $s7 = { 62 61 73 65 36 34 20 2d 64 } $s8 = { 7c 73 68 } $s9 = { 72 65 73 74 61 72 74 } $s10 = { 2f 64 65 76 2f 6e 75 6c 6c } $s11 = { 23 21 20 2f 62 69 6e 2f 73 68 } $s12 = { 62 61 73 65 36 34 } condition: filesize < 2KB and all of them }

Name

b98f8989e8706380f779bfd464f3dea87c122651a7a6d06a994d9a4758e12e43

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b98f8989e8706380f779bfd464f3dea87c122651a7a6d06a994d9a4758e12e43']

Name

6dd8de093e391da96070a978209ebdf9d807e05c89dba13971be5aea2e1251d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6dd8de093e391da96070a978209ebdf9d807e05c89dba13971be5aea2e1251d0']

Name

f75bbae827f63eb8987ab0aaebc8d1f92557895c

Pattern Type

yara

Pattern

rule CISA_10454006_06 : SUBMARINE trojan backdoor cleans_traces_of_infection hides_artifacts installs_other_components { meta: Author = "CISA Code & Media Analysis" Incident = "10454006" Date = "2023-07-11" Last_Modified = "20230727_1200" Actor = "n/a" Family = "SUBMARINE" Capabilities = "cleans-traces-of-infection hides-artifacts installs-other-components" Malware_Type = "trojan backdoor" Tool_Type = "unknown" Description = "Detects SUBMARINE SQL trigger samples" SHA256_1 = "2a353e9c250e5ea905fa59d33faeaaa197d17b4a4785456133aab5dbc1d1d5d5" strings: $s1 = { 54 52 49 47 47 45 52 } $s2 = { 43 52 45 41 54 45 } $s3 = { 53 45 4c 45 43 54 20 22 65 63 68 6f 20 2d 6e } $s4 = { 62 61 73 65 36 34 20 2d 64 20 7c 20 73 68 } $s5 = { 72 6f 6f 74 } $s6 = { 53 45 54 } $s7 = { 45 4e 44 20 49 46 3b } $s8 = { 48 34 73 49 41 41 41 41 41 41 41 41 2b 30 61 43 33 42 55 } $s9 = { 2f 76 61 72 2f 74 6d 70 2f 72 } $s10 = { 2f 72 6f 6f 74 2f 6d 61 63 68 69 6e 65 } condition: filesize < 250KB and all of them }

Name

114bc038e621f78b9dc583d41e2cd4368568f069

Pattern Type

yara

Pattern

import "math" rule CISA_10454006_02 : SUBMARINE trojan backdoor exploitation hides_artifacts prevents_artifact_access { meta: Author = "CISA Code & Media Analysis" Incident = "10454006" Date = "2023-06-29" Last_Modified = "20230711_1500" Actor = "n/a" Family = "SUBMARINE" Capabilities = "hides-artifacts prevents-artifact-access" Malware_Type = "trojan backdoor" Tool_Type = "exploitation" Description = "Detects encoded GZIP archive samples" SHA256_1 = "6dd8de093e391da96070a978209ebdf9d807e05c89dba13971be5aea2e1251d0" strings: $s1 = { 48 34 73 49 41 41 41 41 41 41 41 41 2b 30 61 } $s2 = { 44 44 44 41 67 50 39 2f 2b 43 38 47 70 2f

36 63 41 46 41 41 41 41 3d 3d 0a} $s3 = { 37 56 4d 70 56 58 4f 37 2b 6d 4c 39 78 2b 50 59 } condition: filesize < 6KB and 3 of them and (math.entropy(0,filesize) > 5.8) }

Name

81cf3b162a4fe1f1b916021ec652ade4a14df808021eeb9f7c81c8d2326bddab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '81cf3b162a4fe1f1b916021ec652ade4a14df808021eeb9f7c81c8d2326bddab']

Name

2a9b06839332c5e639eb0e0ba7b17e81095e79cb

Pattern Type

yara

Pattern

rule CISA_10454006_05 : SUBMARINE trojan backdoor remote_access_trojan compromises_data_integrity cleans_traces_of_infection hides_artifacts installs_other_components remote_access exploitation { meta: Author = "CISA Code & Media Analysis" Incident = "10454006" Date = "2023-07-05" Last_Modified = "20230711_1500" Actor = "n/a" Family = "SUBMARINE" Capabilities = "compromises-data-integrity cleans-traces-of-infection hides-artifacts installs-other-components" Malware_Type = "trojan backdoor remote-access-trojan" Tool_Type = "remote-access exploitation" Description = "Detects SUBMARINE launcher script samples" SHA256_1 = "cc131dd1976a47ee3b631a136c3224a138716e9053e04d8bea3ee2e2c5de451a" strings: $s1 = { 4c 44 5f 50 52 45 4c 4f 41 44 } $s2 = { 23 21 20 2f 62 69 6e 2f 73 68 } $s3 = { 4c 44 5f 50 52 45 4c 4f 41 44 3d 2f 62 6f 6f 74 2f 6f 73 5f 74 6f 6f 6c 73 2f 6c 69 62 75 74 69 6c 2e 73 6f 20 65 78 65 63 } $s4 = { 3e 2f 64 65 76 2f 6e 75 6c 6c 20 32 3e 26 31 } $s5 = { 62 73 6d 74 70 64 20 63 6f 6e 74 72

```
6f 6c 20 73 63 72 69 70 74 } $s6 = { 42 53 4d 54 50 44 5f 50 49 44 } $s7 = { 2f 72 65 6c 6f 61 64
2f 72 65 73 74 61 72 74 } condition: filesize < 6KB and 6 of them }
```

Attack-Pattern

Name

Account Access Removal

ID

T1531

Description

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](https://attack.mitre.org/software/S0039) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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
2a353e9c250e5ea905fa59d33faeaaa197d17b4a4785456133aab5dbc1d1d5d5
b98f8989e8706380f779bfd464f3dea87c122651a7a6d06a994d9a4758e12e43
6dd8de093e391da96070a978209ebdf9d807e05c89dba13971be5aea2e1251d0
cc131dd1976a47ee3b631a136c3224a138716e9053e04d8bea3ee2e2c5de451a
8695945155d3a87a5733d31bf0f4c897e133381175e1a3cdc8c73d9e38640239
81cf3b162a4fe1f1b916021ec652ade4a14df808021eeb9f7c81c8d2326bddab
bbbae0455f8c98cc955487125a791052353456c8f652ddee14f452415c0b235a

External References

- https://otx.alienvault.com/pulse/64c7df893a87f081771bce7d
- https://www.cisa.gov/news-events/analysis-reports/ar23-209a