Aug 09 2023

NETMANAGEIT

Intelligence Report MAR-10454006.r4.v2 SEASPY and WHIRLPOOL Backdoors

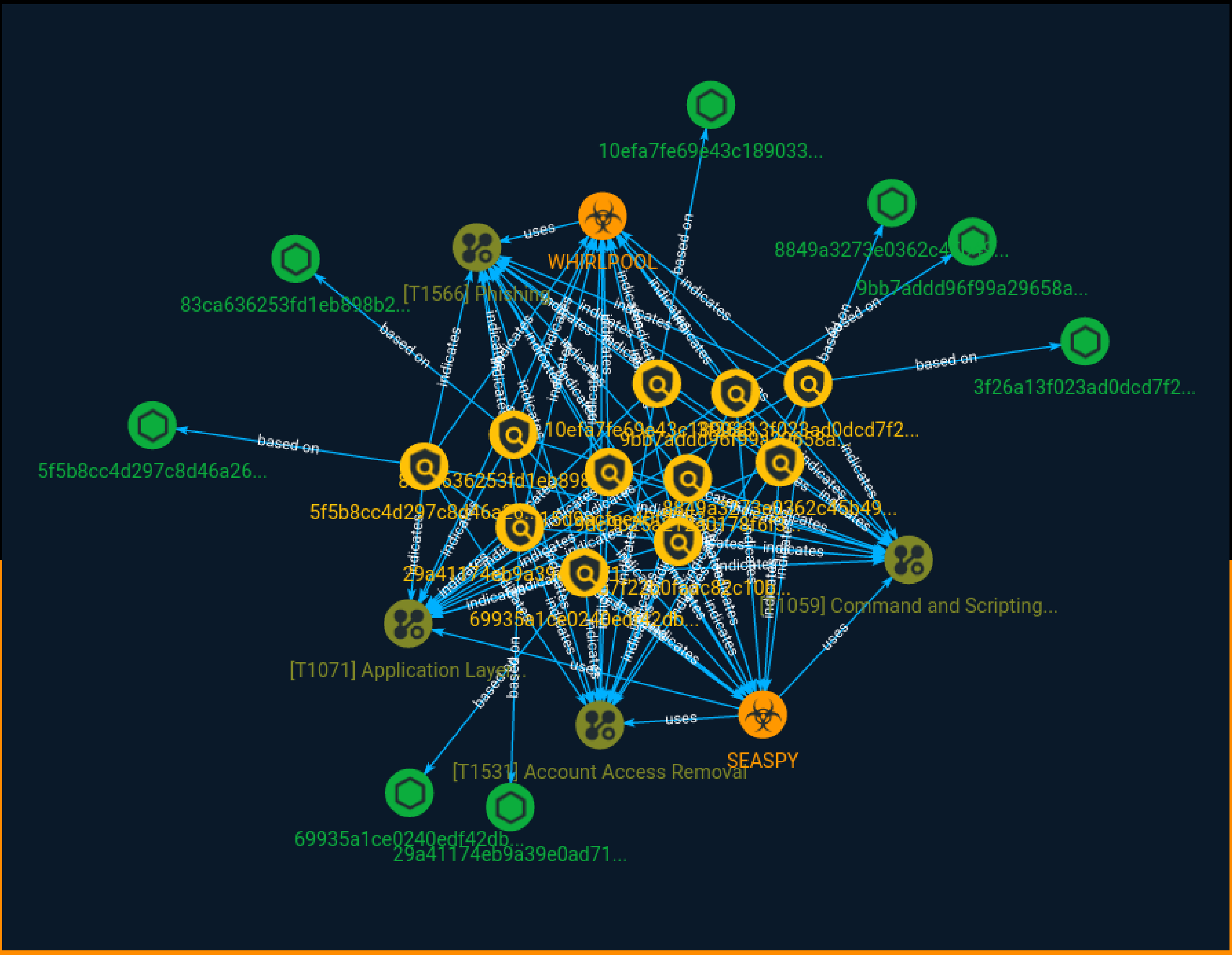

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4
- Malware 10
- Attack-Pattern 11

Observables

- StixFile 14

External References

- External References 15

Overview

Description

CISA obtained four malware samples - including SEASPY and WHIRLPOOL backdoors. The device was compromised 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).

Confidence

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

15 / 100

Indicator

Name

83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c

Description

is__elf SHA256 of 5ce46efc6b28bd94955138833dc97916957dbde1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c']

Name

6ec815d9acfee40f23b3f748b469754cd0669eee

Pattern Type

yara

Pattern

```
rule CISA_10454006_10 : trojan persists_after_system_reboot { meta: Author = "CISA Code &
Media Analysis" Incident = "10454006" Date = "2023-07-20" Last_Modified = "20230726_1700"
Actor = "n/a" Family = "n/a" Capabilities = "persists-after-system-reboot" Malware_Type =
"trojan" Tool_Type = "unknown" Description = "Detects script samples known to start
SEASPY after reboot" SHA256 =
"29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b" strings: $s1 = { 21
20 2d 64 20 24 7b 72 63 5f 62 61 73 65 7d 2f 72 63 24 7b 72 75 6e 6c 65 76 65 6c 7d 2e 64 } $s2 =
{ 52 75 6e 6e 69 6e 67 20 73 63 72 69 70 74 73 20 66 6f 72 20 72 75 6e 6c 65 76 65 6c 20 24 72 75
6e 6c 65 76 65 6c } $s3 = { 5b 20 2d 66 20 24 7b 70 72 65 76 5f 73 74 61 72 74 7d 20 5d 20 26 26
20 5b 20 21 20 2d 66 20 24 7b 73 74 6f 70 7d 20 5d 20 26 26 20 63 6f 6e 74 69 6e 75 65 } $s4 = {
24 7b 69 7d 20 73 74 61 72 74 20 3e 3e 2f 72 6f 6f 74 2f 62 6f 6f 74 2e 6c 6f 67 20 32 3e 3e 2f 72
6f 6f 74 2f 62 6f 6f 74 2e 6c 6f 67 } $s5 = { 2f 73 62 69 6e 2f 42 61 72 72 61 63 75 64 61 4d 61 69
6c 53 65 72 76 69 63 65 20 65 74 68 30 } condition: all of them }
```

Name

9bb7addd96f99a29658aca9800b66046823c5ef0755e29012983db6f06a999cf

Description

stack_string SHA256 of 191e16b564c66b3db67f837e1dc5eac98ff9b9ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9bb7addd96f99a29658aca9800b66046823c5ef0755e29012983db6f06a999cf']

Name

478b7f22b0faac82c10b733dbb71fa12c5e9fbad

Pattern Type

yara

Pattern

rule CISA_10452108_02 : WHIRLPOOL backdoor communicates_with_c2 installs_other_components { meta: Author = "CISA Code & Media Analysis" Incident = "10452108" Date = "2023-06-20" Last_Modified = "20230804_1730" Actor = "n/a" Family = "WHIRLPOOL" Capabilities = "communicates-with-c2 installs-other-components" Malware_Type = "backdoor" Tool_Type = "unknown" Description = "Detects malicious Linux WHIRLPOOL samples" SHA256_1 = "83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c" SHA256_2 = "8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347" strings: $s0 = { 65 72 72 6f 72 20 2d 31 20 65 78 69 74 } $s1 = { 63 72 65 61 74 65 20 73 6f 63 6b 65 74 20 65 72 72 6f 72 3a 20 25 73 28 65 72 72 6f 72 3a 20 25 64 29 } $s2 = { c7 00 20 32 3e 26 66 c7 40 04 31 00 } $a3 = { 70 6c 61 69 6e 5f 63 6f 6e 6e 65 63 74 } $a4 = { 63 6f 6e 6e 65 63 74 20 65 72 72 6f 72 3a 20 25 73 28 65 72 72 6f 72 3a 20 25 64 29 } $a5 = { 73 73 6c 5f 63 6f 6e 6e 65 63 74 } condition: uint32(0) == 0x464c457f and 4 of them }

Name

29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b']

Name

8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347']

Name

69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192']

Name

10efa7fe69e43c189033006010611e84394569571c4f08ea1735073d6433be81

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10efa7fe69e43c189033006010611e84394569571c4f08ea1735073d6433be81']

Name

9dc9b25a212a0178f6f3d7789f8be10f57bca164

Pattern Type

yara

Pattern

rule CISA_10452108_01 : SEASPY backdoor communicates_with_c2 installs_other_components { meta: Author = "CISA Code & Media Analysis" Incident = "10452108" Date = "2023-06-20" Last_Modified = "20230628_1000" Actor = "n/a" Family = "SEASPY" Capabilities = "communicates-with-c2 installs-other-components" Malware_Type = "backdoor" Tool_Type = "unknown" Description = "Detects malicious Linux SEASPY samples" SHA256_1 = "3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115" SHA256_2 = "69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192" SHA256_3 = "5f5b8cc4d297c8d46a26732ae47c6ac80338b7be97a078a8e1b6eefd1120a5e5" SHA256_4 = "10efa7fe69e43c189033006010611e84394569571c4f08ea1735073d6433be81" strings: $s0 = { 2e 2f 42 61 72 72 61 63 75 64 61 4d 61 69 6c 53 65 72 76 69 63 65 20 65 74 68 30 } $s1 = { 75 73 61 67 65 3a 20 2e 2f 42 61 72 72 61 63 75 64 61 4d 61 69 6C 53 65 72 76 69 63 65 20 3c 4e 65 74 77 6f 72 6b 2d 49 6e 74 65 72 66 61 63 65 } $s2 = { 65 6e 74 65 72 20 6f 70 65 6e 20 74 74 79 20 73 68 65 6c 6c } $s3 = { 25 64 00 4e 4f 20 70 6f 72 74 20 63 6f 64 65 } $s4 = { 70 63 61 70 5f 6c 6f 6f 6b 75 70 6e 65 74 3a 20 25 73 } $s5 = { 43 68 69 6c 64 20 70 72 6f 63 65 73 73 20 69 64 3a 25 64 } $s6 = { 5b 2a 5d 53 75 63 63 65 73 73 21 } $a7 = { bf 90 47 90 ec 18 fe e3 83 e2 a9 f7 8d 85 18 1d } $a8 = { 81 35 1e f0 94 ab 2a ba 5d f0 37 76 69 19 9f 1e } $a9 = { 6a 8e c7 89 ce c1 fe 64 78 a6 e1 c5 fe 03 d1 a7 } $a10 = { c2 ff d1 0d 24 23 ec c0 57 f9 8d 4b 05 34 41 b8 } condition: uint32(0) == 0x464c457f and (all of ($s*)) or (all of ($a*)) }

Name

5f5b8cc4d297c8d46a26732ae47c6ac80338b7be97a078a8e1b6eefd1120a5e5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f5b8cc4d297c8d46a26732ae47c6ac80338b7be97a078a8e1b6eefd1120a5e5']

Name

3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115

Description

stack_string SHA256 of 0ea36676bd7169bcbf432f721c4edb5fde0a46a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115']

Malware

Name
WHIRLPOOL

Name
SEASPY

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
Phishing

ID
T1566

Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

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

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

StixFile

Value
29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b
83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c
9bb7addd96f99a29658aca9800b66046823c5ef0755e29012983db6f06a999cf
69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192
8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347
3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115
5f5b8cc4d297c8d46a26732ae47c6ac80338b7be97a078a8e1b6eefd1120a5e5
10efa7fe69e43c189033006010611e84394569571c4f08ea1735073d6433be81

External References

- https://otx.alienvault.com/pulse/64d408a3c5e9f42a3dead3b6
- https://www.cisa.gov/news-events/analysis-reports/ar23-221a