Sep 09 2023

NETMANAGEIT

Intelligence Report

MAR-10454006.r5.v1 SUBMARINE, SKIPJACK, SEASPRAY, WHIRLPOOL, and SALTWATER Backdoors

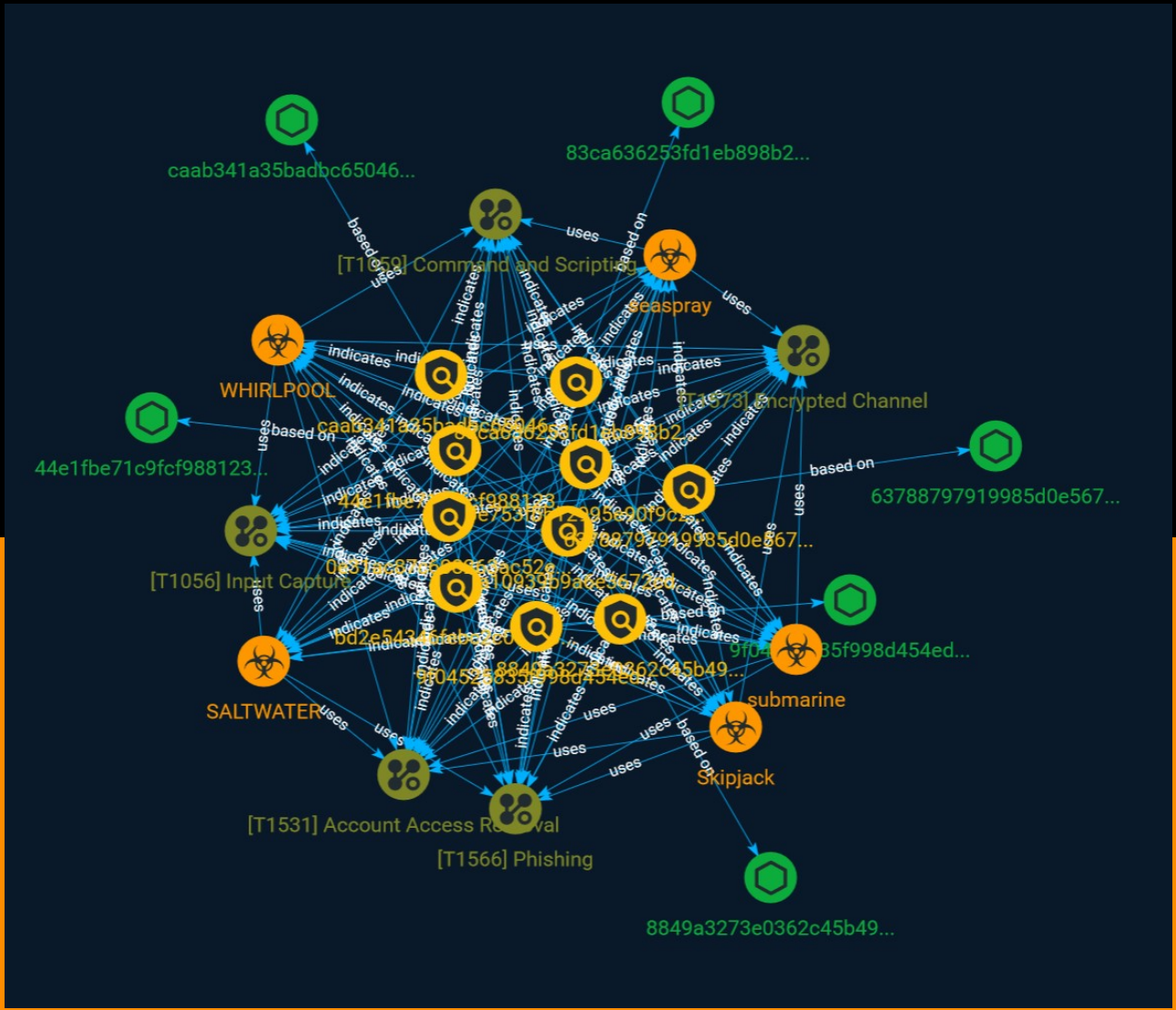

Table of contents

Overview

Entities

Observables

External References

Overview

Description

CISA obtained five malware samples - including artifacts related to SUBMARINE, SKIPJACK, SEASPRAY, WHIRLPOOL, and SALTWATER backdoors.

Confidence

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

15 / 100

Indicator

Name

948a10939b9a6e3672cd37cb062c57d2de0b20f2

Description

Detects SALTWATER samples

Pattern Type

yara

Pattern

rule CISA_10454006_13 : SALTWATER backdoor exploit_kit communicates_with_c2 determines_c2_server hides_executing_code exploitation { meta: author = "CISA Code & Media Analysis" incident = "10454006" date = "2023-08-10" last_modified = "20230905_1500" actor = "n/a" family = "SALTWATER" capabilities = "communicates-with-c2 determines-c2-server hides-executing-code" malware_type = "backdoor exploit-kit" tool_type = "exploitation" description = "Detects SALTWATER samples" sha256 = "caab341a35badbc65046bd02efa9ad2fe2671eb80ece0f2fa9cf70f5d7f4bedc" strings: $s1 = { 70 74 68 72 65 61 64 5f 63 72 65 61 74 65 } $s2 = { 67 65 74 68 6f 73 74 62 79 6e 61 6d 65 } $s3 = { 54 72 61 6d 70 6f 6c 69 6e 65 } $s4 = { 64 73 65 6c 64 73 } $s5 = { 25 30 38 78 20 28 25 30 32 64 29 20 25 2d 32 34 73 20 25 73 25 73 25 73 0a } $s6 = { 45 6e 74 65 72 20 6f 75 73 63 64 6f 6f 65 7c 70 72 65 64 61 72 65 28 25 70 2c 20 25 70 2c 20 25 70 29 } $s7 = { 45 6e 74 65 72 20 61 75 74 63 63 6f 6f 71 38 63 72 65 61 74 65 } $s8 = { 74 6e 6f 72 6f 74 65 63 74 6a 73 65 6d 6f 72 79 } $s9 = { 56 55 43 4f 4d 49 53 53 } $s10 = { 56 43 4f 4d 49 53 53 } $s11 = { 55 43 4f 4d 49 53 44 } $s12 = { 41 45 53 4b 45 59 47 45 4e 41 53 53 49 53 54 } $s13 = { 46 55 43 4f 4d 50 50 } $s14 = { 55 43 4f 4d 49 53 53 } condition: uint16(0) == 0x457f and filesize < 1800KB and 8 of them }

Name

bd2e54346febc2c0eb5044203e51f8fd8bec7af7

Description

Detects perl script linked to SKIPJACK backdoor samples

Pattern Type

yara

Pattern

rule CISA_10454006_11 : trojan { meta: author = "CISA Code & Media Analysis" incident = "10454006" date = "2023-07-20" last_modified = "20230726_1700" actor = "n/a" family = "n/a" Capabilities = "n/a" Malware_Type = "trojan" Tool_Type = "unknown" description = "Detects perl script linked to SKIPJACK backdoor samples" SHA256 = "63788797919985d0e567cf9133ad2ab7a1c415e81598dc07c0bfa3a1566aeb90" strings: $s1 = { 2f 65 74 63 2f 66 73 74 61 62 2e 6d 61 69 6e } $s2 = { 28 3c 46 53 54 41 42 3e 29 } $s3 = { 6d 79 20 28 24 70 61 72 74 69 74 69 6f 6e 2c 20 24 66 73 5f 74 79 70 65 29 } $s4 = { 70 72 69 6e 74 20 24 66 73 5f 74 79 70 65 } $s5 = { 70 72 69 6e 74 20 24 70 61 72 74 69 74 69 6f 6e } condition: all of them }

Name

44e1fbe71c9fcf9881230cb924987e0e615a7504c3c04d44ae157f07405e3598

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44e1fbe71c9fcf9881230cb924987e0e615a7504c3c04d44ae157f07405e3598']

Name

63788797919985d0e567cf9133ad2ab7a1c415e81598dc07c0bfa3a1566aeb90

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '63788797919985d0e567cf9133ad2ab7a1c415e81598dc07c0bfa3a1566aeb90']

Name

0e31ac87c608263ac52e4009e10c6c1b5b8c33ea

Description

Detects SEASPRAY samples

Pattern Type

yara

Pattern

rule CISA_10454006_12 : SEASPRAY trojan evades_av { meta: author = "CISA Code & Media Analysis" incident = "10454006" date = "2023-08-23" last_modified = "20230905_1500" actor = "n/a" family = "SEASPRAY" capabilities = "evades-av" malware_type = "trojan" tool_type = "unknown" description = "Detects SEASPRAY samples" sha256 = "44e1fbe71c9fcf9881230cb924987e0e615a7504c3c04d44ae157f07405e3598" strings: $s1 = { 6f 73 2e 65 78 65 63 75 74 65 28 27 73 61 73 6c 61 75 74 63 68 64 27 } $s2 = { 73 65 6e 64 65 72 } $s3 = { 73 74 72 69 6e 67 2e 66 69 6e 64 } $s4 = { 73 74 72 69 6e 67 2e 6c 6f 77 65 72 } $s5 = { 62 6c 6f 63 6b 2f 61 63 63 65 70 74 } $s6 = { 72 65 74 75 72 6e 20 41 63 74 69 6f 6e 2e 6e 65 77 7b } $s7 = { 4c 69 73 74 65 6e 65 72 2e 6e 65 77 7b } condition: filesize < 10KB and all of them }

Name

0e753fbb12995e90f9c2717ace07bc15398d45f1

Description

Detects malicious Linux WHIRLPOOL samples

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

9f04525835f998d454ed68cfc7fcb6b0907f2130ae6c6ab7495d41aa36ad8ccf

Description

is__elf SHA256 of 436587bad5e061a7e594f9971d89c468

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f04525835f998d454ed68cfc7fcb6b0907f2130ae6c6ab7495d41aa36ad8ccf']

Name

caab341a35badbc65046bd02efa9ad2fe2671eb80ece0f2fa9cf70f5d7f4bedc

Description

is__elf SHA256 of 4ec4ceda84c580054f191caa09916c68

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'caab341a35badbc65046bd02efa9ad2fe2671eb80ece0f2fa9cf70f5d7f4bedc']

Name

83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c

Description

is__elf SHA256 of 85c5b6c408e4bdb87da6764a75008adf

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c']
Name
8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347
Description
is__elf SHA256 of 177add288b289d43236d2dba33e65956
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347']

Malware

Name
submarine
Name
SALTWATER
Name
seaspray
Name
Skipjack
Name
WHIRLPOOL

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

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Encrypted Channel

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

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)

StixFile

Value
63788797919985d0e567cf9133ad2ab7a1c415e81598dc07c0bfa3a1566aeb90
44e1fbe71c9fcf9881230cb924987e0e615a7504c3c04d44ae157f07405e3598
caab341a35badbc65046bd02efa9ad2fe2671eb80ece0f2fa9cf70f5d7f4bedc
9f04525835f998d454ed68cfc7fcb6b0907f2130ae6c6ab7495d41aa36ad8ccf
83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c
8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347

External References

- https://otx.alienvault.com/pulse/64fb9629c647d5fde828ddc1
- https://www.cisa.gov/news-events/analysis-reports/ar23-250a-0