Aug 21 2023

NETMANAGEIT

Intelligence Report

WHIRLPOOL Backdoor | CISA

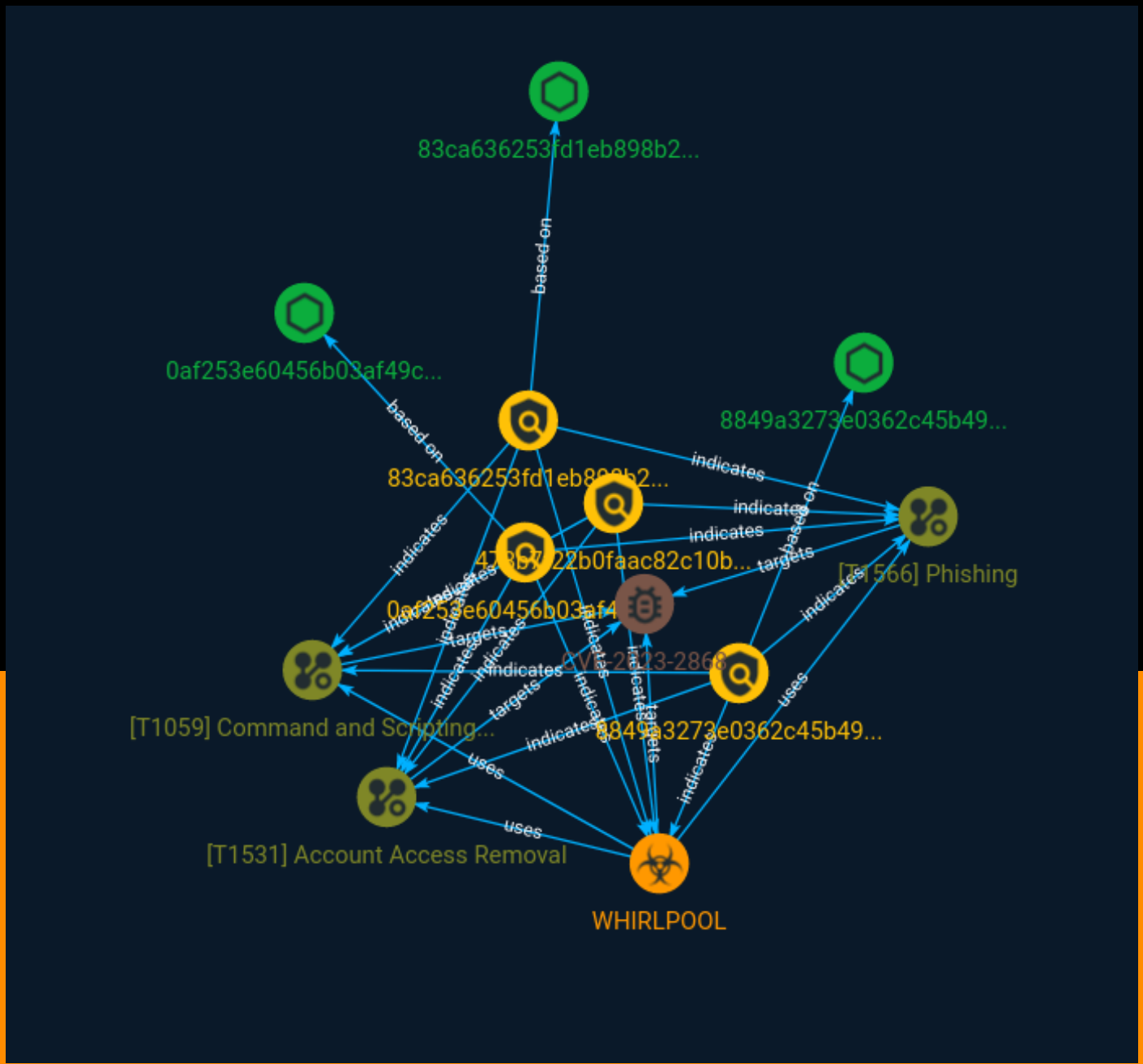

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The CISA cybersecurity and Infrastructure Security Agency (CISA) released an alert warning that a backdoor was being exploited to attack the US government's critical infrastructure, including the election and security of the United States.

Confidence

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

15 / 100

Indicator

Name

0af253e60456b03af49cc675f71d47b2dd9a48f50a927e43b9d8116985c06459

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0af253e60456b03af49cc675f71d47b2dd9a48f50a927e43b9d8116985c06459']

Name

83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c

Description

is__elf

Pattern Type

stix

Pattern

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

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

8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347

Description

is__elf

Pattern Type

stix

Pattern

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

Vulnerability

Name
CVE-2023-2868

Malware

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

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
0af253e60456b03af49cc675f71d47b2dd9a48f50a927e43b9d8116985c06459
83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c
8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347

External References

- https://otx.alienvault.com/pulse/64e377918085028l9a914e44
- https://www.cisa.gov/news-events/analysis-reports/ar23-230a