Sep 07 2023

NETMANAGEIT

Intelligence Report

Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475

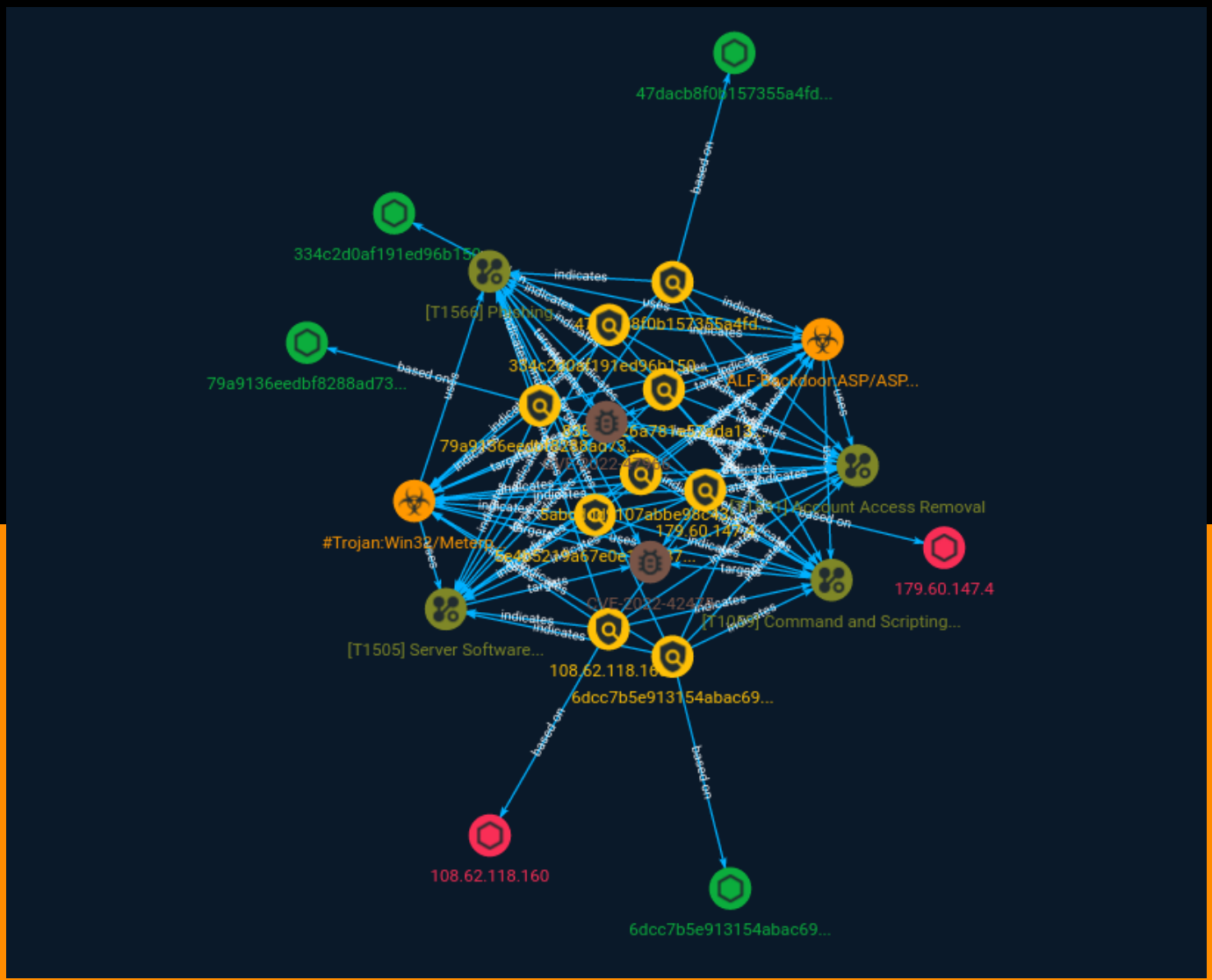

Table of contents

Overview

Entities

Observables

External References

Overview

Description

CISA and co-sealers are releasing this joint Cybersecurity Advisory (CSA) to provide network defenders with tactics, techniques, and procedures (TTPs), IOCs, and methods to detect and protect against similar exploitation.

Confidence

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

15 / 100

Indicator

Name

179.60.147.4

Description

ISP: Flyservers S.A. **OS:** Windows Server 2012 R2 ---------- Hostnames: ---------- Domains: ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: 18730 NetBIOS Domain Name: 18730 NetBIOS Computer Name: 18730 DNS Domain Name: 18730 FQDN: 18730 am Windows Server 2012R2 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 31 Aug 2023 19:10:39 GMT Connection: close Content-Length: 315 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.60.147.4']

Name

5e4b5219a67e0e1c3e874d3cf570b560bf4b9d27

Description

Detects OWA targeting ASPX Webshell samples

Pattern Type

yara

Pattern

rule CISA_10430311_03 : ASPX_WEBSHELL webshell { meta: author = "CISA Code & Media Analysis" incident = "10430311" date = "2023-03-21" last_modified = "20230404_1230" actor = "n/a" family = "ASPX Webshell" Capabilities = "n/a" Malware_Type = "webshell" Tool_Type = "n/a" description = "Detects OWA targeting ASPX Webshell samples" sha256_1 = "6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde" sha256_1 = "47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622" strings: $s1 = { 5a 30 32 6a 77 36 43 36 63 55 } $s2 = { 5a 38 49 30 32 38 33 6e 77 38 } $s3 = { 4f 57 41 77 65 62 63 6f 6e 66 69 67 } $s4 = { 54 55 43 53 4f 4e } $s5 = { 65 76 61 6c } condition: 3 of them }

Name

835b5926a781e57ada131f71abe15c7c1ae1b3f8

Description

Detects Fresh Meterpreter bianary samples

Pattern Type

yara

Pattern

rule CISA_10430311_02 : METERPRETER controls_local_machine compromises_data_integrity communicates_with_c2 keylogger exploit_kit remote_access_trojan back downloader screen_capture virus remote_access exploitation network_capture { meta: author = "CISA Code & Media Analysis" incident = "10430311" date = "2023-03-08" last_modified =

"20230405_1300" actor = "n/a" family = "METERPRETER" Capabilities = "controls-local-machine compromises-data-integrity communicates-with-c2" Malware_Type = "keylogger exploit-kit remote-access-trojan backdoor downloader screen-capture virus" Tool_Type = "remote-access exploitation network-capture" description = "Detects Fresh Meterpreter bianary samples" sha256_1 = "79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63" sha256_2 = "334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b" sha256_3 = "6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde" sha256_4 = "47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622" strings: $s0 = { 58 a4 53 e5 } $s1 = { 02 d9 c8 5f } $s2 = { 99 a5 74 61 } $s3 = { 4c 77 26 07 } $s4 = { 29 80 6b 00 } $s5 = { 50 41 59 4c 4f 41 44 3a } $s6 = { 48 83 ec 28 49 c7 c1 40 } condition: all of them }

Name

5abcddd9107abbe98c430447d9dd7af2805d9803

Description

Detects trojan downloader samples

Pattern Type

yara

Pattern

rule CISA_10430311_01 : METERPRETER trojan downloader { meta: author = "CISA Code & Media Analysis" incident = "10430311" date = "2023-03-03" last_modified = "20230404_1200" actor = "n/a" family = "METERPRETER" Capabilities = "n/a" Malware_Type = "trojan downloader" Tool_Type = "n/a" description = "Detects trojan downloader samples" sha256_1 = "334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b" strings: $s1 = { 49 be 77 73 32 5f 33 32 } $s2 = { 49 89 e6 48 81 ec a0 01 } $s3 = { 49 bc 02 00 e5 6b b3 3c 93 04 } $s4 = { 41 ba 4c 77 26 07 ff d5 } $s5 = { 41 ba ea 0f df e0 ff d5 } $s6 = { 41 ba 99 a5 74 61 ff d5 } $s7 = { 41 ba 02 d9 c8 5f ff d5 } $s8 = { 41 ba 58 a4 53 e5 ff d5 } condition: all of them }

Name

79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63']

Name

47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622']

Name

108.62.118.160

Description

CC=US ASN=AS30633 LEASEWEB-USA-WDC

Pattern Type

stix

Pattern

[ipv4-addr:value = '108.62.118.160']

Name

334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b']

Name

6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde']

Malware

Name
#Trojan:Win32/Meterpreter

Name
ALF:Backdoor:ASP/ASPXShell

Vulnerability

Name
CVE-2022-42475

Name
CVE-2022-47966

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

Server Software Component

ID

T1505

Description

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)

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
334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b
47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622
6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde
79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63

IPv4-Addr

Value
179.60.147.4
108.62.118.160

External References

- https://otx.alienvault.com/pulse/64fa236d0bd8437d7e733c34
- https://www.cisa.gov/news-events/analysis-reports/ar23-250a