ANALYSIS REPORT

10454006.r4.v2 NUMBER

Malware Analysis Report

2023-08-08 DATE

Notification

Summary

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).

SEASPY is a persistent and passive backdoor that masquerades as a legitimate Barracuda service “BarracudaMailService” that allows the threat actors to execute arbitrary commands on the ESG appliance.

WHIRLPOOL is a backdoor that establishes a Transport Layer Security (TLS) reverse shell to the Command-and-Control (C2) server.

For information about related malware, specifically information on the initial exploit payload, a second SEASPY backdoor variant, and the SUBMARINE backdoor, see CISA Alert: CISA Releases Malware Analysis Reports on Barracuda Backdoors.

Submitted Files (4)

29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b (QuoVadis_Root_CA_1_G3.pem)

3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115 (BarracudaMailService.old)

83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c (rverify)

9bb7addd96f99a29658aca9800b66046823c5ef0755e29012983db6f06a999cf (resize_reisertab)

Findings

3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115

Tags

trojan

Details

Name	BarracudaMailService.old
Size	2924217 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.26, BuildID[sha1]=598b486976708dc59ecf3fdec8727b82df63b7de, with debug_info, not stripped
MD5	4ca4f582418b2cc0626700511a6315c0

SHA1	0ea36676bd7169bcbf432f721c4edb5fde0a46a9
SHA256	3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115
SHA512	71e0aaaf8981782ccb09331548d2458671d1dd65433052e44583ece98fffda9b6f0a3805d6d9c653dd0e1378602a7c1a3b0482a563b6644af49c908876ec1a3b
ssdeep	49152:X7PdfV6LWGqla76yHbSgfrNr1glmyifFTZwwP80WhpKG:zdfBlm6cbxr1pDw30WhpKG
Entropy	6.167504

Antivirus

AhnLab	HackTool/Linux.Reverseshell
Antiy	Trojan/Win32.Casdet
Bitdefender	Trojan.Linux.Generic.298175
Emsisoft	Trojan.Linux.Generic.298175 (B)
ESET	Linux/SeaSpy.A trojan
McAfee	ELF/Barracuda.a
Quick Heal	ELF.Barracuda.47823.GC
Sophos	Linux/Agnt-BS
Varist	E64/SeaSpy.A

YARA Rules

```
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*))
}
```

ssdeep Matches

No matches found.

Relationships

3f26a13f02...	Related_To	29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b

Description

This artifact is a 64-bit Executable and Linkable Format (ELF) file that has been identified as a "SEASPY" malware variant installed as a system service. The malware is a persistent backdoor that masquerades as a legitimate Barracuda Networks service. The malware is designed to listen to commands received from the Threat Actor's (TA's) C2 through TCP packets. When executed, the malware uses libpcap sniffer to monitor traffic for a magic packet on TCP port 25 (Simple Mail Transfer Protocol (SMTP)) and TCP port 587. It checks the network packet captured for a hard-coded string "oXmp". When the right sequence of packets is captured, it establishes a TCP reverse shell to the TA's C2 server for further exploitation. This allows the TA to execute arbitrary commands on the compromised system.

The malware is based on an open-source backdoor program named "cd00r" and it is executed using the parameter below:

--Begin argument--
Usage: "./BarracudaMailService <Network-Interface>"
Sample: "./<malware> eth0"
--End argument--

29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b

Details

Name	QuoVadis_Root_CA_1_G3.pem
Size	2698 bytes
Type	POSIX shell script, ASCII text executable
MD5	2d841cb153bebcfdee5c54472b017af2
SHA1	7a791d4d7e55d7a2fdc08ac0f22ab7ae068fdf26
SHA256	29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b
SHA512	021c28dfd1a4136a6aa80fb86546655f4b0b8a9c528af157edc556074922553d58fa793b061a18316783b8b74eb38d3e08c5ece4eecc8fa4953ac0a556595cca
ssdeep	48:2LrIlobkq9g03Xxk7OnoDzHyvIoXirAAAt6KWejvPqRvOojmJL0pNZiWtDjE5:2Lzbhg0nusoH2IoXirArMgqVmJL0pNZw
Entropy	5.234290

Antivirus

No matches found.

YARA Rules

```
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
}
```

ssdeep Matches

No matches found.

Relationships

29a41174eb...	Related_To	3f26a13f023ad0dcd7f2aa4e7771bba74910ee 227b4b36ff72edc5f07336f115

Description

This artifact is an initialization script. Upon its execution it sets terminal settings to default using the 'stty sane' command. It then runs through the process of setting a runlevel variable and stops other services that were started by a previous runlevel. It also kills any services that are running on the current runlevel. Next, the script will start its associated services at the current runlevel. After logging functionalities are started, the script will then check if the runlevel is 3, which will result in the terminal screen being cleared using /usr/bin/clear. Finally, the script contains the command “/sbin/BarracudaMailService eth0” at the end. BarracudaMailService will be started automatically when the initialization script is run on the network interface eth0. BarracudaMailService is a known name for the SEASPY backdoor.

Screenshots

```
    check_script_status

    case ${runlevel} in
        0|6)
            ${i} stop >/dev/null 2>/dev/null # Don't log shutdown for now >>/root/boot.log 2>>/root/boot.log
            ;;
        sysinit) ${i} start
            ;;
        *)
            ${i} start >>/root/boot.log 2>>/root/boot.log
            ;;
    esac
    error_value=${?}

    if [ "${error_value}" != "0" ]; then
        print_error_msg
    fi
done
if [ "$runlevel" = "3" ] && [ -x "/usr/bin/clear" ]; then
    /usr/bin/clear
fi
# End $rc_base/init.d/rc
/sbin/BarracudaMailService eth0
```

Figure 1. - At the end of the script the string "/sbin/BarracudaMailService eth0" is specified.

9bb7addd96f99a29658aca9800b66046823c5ef0755e29012983db6f06a999cf

Tags

trojan

Details

Name	resize_reisertab
Size	2549176 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, for GNU/Linux 2.6.26, BuildID[sha1]=c971d01d9faa9d7fd94aef13b24e0b5d3d149a7c, stripped
MD5	45b79949276c9cb9cf5dc72597dc1006
SHA1	191e16b564c66b3db67f837e1dc5eac98ff9b9ef

SHA256	9bb7addd96f99a29658aca9800b66046823c5ef0755e29012983db6f06a999cf
SHA512	0f4307b5f48c193c1036b56b3cf569f79cb8fc2306f8f796d5548bcd5a96fc52127d2186d980c71d5917eb6d6026e92405a3cd453011503515e2e4f3311201c3
ssdeep	49152:4TnrmLlCGFyVfj+QCH2qirsZZrnYgBbfhceT+c02:KnrXxj317rs/NocJ
Entropy	6.227206

Antivirus

AhnLab	Trojan/Linux.SeaSpy.2549176
Antiy	Trojan/Linux.SeaSpy.a
Bitdefender	Trojan.Linux.Generic.298117
Emsisoft	Trojan.Linux.Generic.298117 (B)
ESET	a variant of Linux/SeaSpy.A trojan
IKARUS	Trojan.Linux.Seaspy
Varist	E64/SeaSpy.A

YARA Rules

```
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*))
}
```

ssdeep Matches

No matches found.

Description

This artifact is a 64-bit ELF file that has been identified as a "SEASPY" malware variant installed as a system service. This variant

of SEASPY has had its symbols stripped. The malware is a persistent backdoor that masquerades as a legitimate Barracuda Networks service. The malware is designed to listen to commands received from the TA's C2 through TCP packets.

When executed, the malware uses libpcap sniffer to monitor traffic for a magic packet on TCP port 25 (SMTP) and TCP port 587. It checks the network packet captured for a hard-coded string "TfuZ". When the right sequence of packets is captured this SEASPY variant launches an authentication sequence prior to launching the reverse shell. Once the TA authenticates, the malware starts a reverse shell on the infected system. This allows the TA to execute arbitrary commands on the compromised system.

The malware is based on an open-source backdoor program named "cd00r" and it is executed using the parameter below:

--Begin argument--
Usage: "./BarracudaMailService <Network-Interface>"
Sample: "./<malware> eth0"
--End argument--

83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c

Tags

trojan

Details

Name	rverify
Size	2646516 bytes
Type	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.32, BuildID[sha1]=fb2cdec59a77c255bd422c92e5de2d0f3f19bd6c, with debug_info, not stripped
MD5	85c5b6c408e4bdb87da6764a75008adf
SHA1	5ce46efc6b28bd94955138833dc97916957dbde1
SHA256	83ca636253fd1eb898b244855838e2281f257bbe8ead428b69528fc50b60ae9c
SHA512	4aef99afc89062387b4987d49e5128ae37a3c25b59f05ccf324e593c67a8f5bd96e1f883d77225dbd0cc9456d736c90dd890bbead6082a14ae9f06abf07f87d8
ssdeep	49152:FKuknP+5ada3TUFChbGh7eMKPEGqnVoqqEoLC+2U:tkP+M834FChbGh7rE2+2U
Entropy	6.540106

Antivirus

Adaware	Unavailable (production)
AhnLab	Trojan/Linux.Whirpool.2646516
Antiy	Trojan/Linux.Agent.wl
Avira	LINUX/Agent.shpuf
Bitdefender	Trojan.Linux.Generic.298125
Emsisoft	Trojan.Linux.Generic.298125 (B)
ESET	a variant of Linux/WhirlPool.A trojan
IKARUS	Trojan.Linux.Agent
McAfee	Trojan-FVEB!85C5B6C408E4
Sophos	Linux/Agnt-BS
Varist	E32/Agent.HC

YARA Rules

```
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
}
```

ssdeep Matches

No matches found.

Description

This artifact is a 32-bit ELF file that has been identified as a malware variant named "WHIRLPOOL". The malware takes two arguments (C2 IP and port number) from a module to establish a Transport Layer Security (TLS) reverse shell. The module that passes the arguments was not available for analysis.

Relationship Summary

3f26a13f02...	Related_To	29a41174eb9a39e0ad712ed5063c561e9c2e1db1f8f6b04b2ca369a6efc3ac9b
29a41174eb...	Related_To	3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115

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.