ANALYSIS REPORT

10454006.r2.v1 NUMBER

Malware Analysis Report

2023-07-27 DATE

Notification

Summary

Description

CISA obtained two SEASPY malware samples. The malware was used 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.

For information about related malware, specifically information on the initial exploit payload and other backdoors, see CISA Alert: CISA Releases Malware Analysis Reports on Barracuda Backdoors.

Submitted Files (2)

3e21e547cf94cb07c010fe82d6965e5bd52dbdd9255b4dd164f64addfaa87abb (BarracudaMailService.1)

69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192 (6931018-BarracudaMailService.2)

Findings

69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192

Tags

trojan

Details

Name	6931018-BarracudaMailService.2
Size	2924089 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.26, BuildID[sha1]=495062eaa63784dad0a098d58892f58deb47ea66, with debug_info, not stripped
MD5	5d6cba7909980a7b424b133fbac634ac
SHA1	d114a707fc6abbd8060f821893a9ee64dc3b2714
SHA256	69935a1ce0240edf42dbe24535577140601bcf3226fa01e4481682f6de22d192
SHA512	ef966e1d679daa44ee4c86848b71a0be27a79c8824eba8e74c866322e59a8bdce66b32f3d4417256af351f87dd149a73ed7e8e40df5794c5273cf029d04b6f25
ssdeep	49152:laMq45lHsbhe9YBU80A3hvJeD7ANjQ4maMTFhmwzHPm0WhphC:oqJh4YWkLeDKOhmwa0WhphC
Entropy	6.165718

Antivirus

ESET	a variant of Linux/SeaSpy.A trojan
McAfee	Linux/Seaspy!5D6CBA790998

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. The sample 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) Command-and-Control (C2) through Transmission Control Protocol (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 "oXmp". Note: This hard-coded string may change for other SEASPY variants. When the right sequence of packet 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—

Screenshots

```
{
  undefined4 *puVar1;
  size_t sVar2;

  if (param_1 < 2) {
    puts("usage: ./BarracudaMailService <Network-Interface>. e.g.: ./BarracudaMailService eth0"
  }
  else {
    sVar2 = strlen(param_2[1]);
    memcpy(CDR_INTERFACE,param_2[1],sVar2);
    sVar2 = strlen(*param_2);
    memset(*param_2,0,sVar2);
    puVar1 = (undefined4 *)*param_2;
    *puVar1 = 0x69706361;
    *(undefined2 *)(puVar1 + 1) = 100;
    sVar2 = strlen(param_2[1]);
    memset(param_2[1],0,sVar2);
    start_pcap_listener(1);
  }
  return 0;
}
```

Figure 1. - This is disassembler output showing how the malware checks the parameters that the malware was executed with.

3e21e547cf94cb07c010fe82d6965e5bd52dbdd9255b4dd164f64addfaa87abb

Tags

trojan

Details

Name	BarracudaMailService.1
Size	2924089 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.26, BuildID[sha1]=41942e680be29136ce7f1cdc9a15fd43968b0db0, with debug_info, not stripped
MD5	32ffe48d1a8ced49c53033eb65eff6f3
SHA1	2c7ad0e7897f348bec2e32f2af4282bd65916f8d
SHA256	3e21e547cf94cb07c010fe82d6965e5bd52dbdd9255b4dd164f64addfaa87abb
SHA512	12fd230c78c9e14b1bbb7f3c6776a14710693fa4224b4376775f118fc35584a5946a57dda43db20bd9ffc2950f4e62e8c206506744bca5fe39e6cb9a1a91b981
ssdeep	49152:bgt0bmh2EXaRuFmK3cnlBceICm4ewQ/MTs/dgPm0WhphC:Ma0gug7bceI4ih/dp0WhphC
Entropy	6.165197

Antivirus

ESET	a variant of Linux/SeaSpy.A trojan
McAfee	Linux/Seaspy!32FFE48D1A8C

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 sample has the sample malicious capabilities as BarracudaMailService.2 (5d6cba7909980a7b424b133fbac634ac). The only difference between the binaries is located in the function named "start_pcap_listener". In the function "start_pcap_listener" both binaries call a function named "reverse shell" to start the reverse shell functionality of the malware. The difference is that BarracudaMailService.1 (32ffe48d1a8ced49c53033eb65eff6f3) jumps directly to the set of instructions that start the reverse shell, as opposed to BarracudaMailService.2 (5d6cba7909980a7b424b133fbac634ac), which contains an extra set of instructions before jumping to the instructions that start the reverse shell.

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.