CISA Releases Malware Analysis Reports on Barracuda Backdoors | CISA

Published: 2023-09-07 · Archived: 2026-04-05 22:44:24 UTC

Updated September 7, 2023

CISA has published an additional malware analysis report associated with malicious Barracuda activity. The report provides analysis on the following malware samples:

- SUBMARINE – SUBMARINE is a backdoor that exploits a vulnerability on the target environment where the base64 string within the file name will be executed on the Linux shell. Note: Also see description and additional MAR below.
- SKIPJACK – SKIPJACK is a backdoor that enumerates file system information.
- SEASPRAY – SEASPRAY is a backdoor that registers an event handler for all incoming email attachments and is a launcher for WHIRLPOOL.
- WHIRLPOOL – WHIRLPOOL is a backdoor that can connect to a remote address then create a new process. Note: Also see description and additional MAR below.
- SALTWATER – SALTWATER is a backdoor that can perform DNS resolution and establish communications, over the network, using a TLS version 1 connection. The malware can execute any shell command with the same privileges as its calling process.

For more information, including indicators of compromise and YARA rules for detection, see the following malware analysis report:

- SUBMARINE, SKIPJACK, SEASPRAY, WHIRLPOOL, and SALTWATER Backdoors MAR-10454006.r5.v1.CLEAR

End of September 7, 2023 update

Updated August 18, 2023

CISA has published an additional malware analysis report associated with malicious Barracuda activity. The report provides analysis on the following malware sample:

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

For more information, including indicators of compromise and YARA rules for detection, see the following malware analysis report:

- WHIRLPOOL Backdoor MAR-10459736.r1.v1.CLEAR

End of August 18, 2023 update

Updated August 9, 2023

CISA has published an additional malware analysis report associated with malicious Barracuda activity. The report provides analysis on four malware samples, including:

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

For more information, including indicators of compromise and YARA rules for detection, see the following malware analysis report:

- SEASPY and WHIRLPOOL Backdoors MAR-10454006.r4.v2.CLEAR

End of August 9, 2023 update

CISA has published three malware analysis reports on malware variants associated with exploitation of CVE-2023-2868. CVE-2023-2868 is a remote command injection vulnerability affecting Barracuda Email Security Gateway (ESG) Appliance, versions 5.1.3.001-9.2.0.006. It was exploited as a zero day as early as October 2022 to gain access to ESG appliances. According to industry reporting, the actors exploited the vulnerability to gain initial access to victim systems and then implanted backdoors to establish and maintain persistence.

CISA analyzed backdoor malware variants obtained from an organization that had been compromised by threat actors exploiting the vulnerability.

- **Barracuda Exploit Payload and Backdoor** – The payload exploits CVE-2023-2868, leading to dropping and execution of a reverse shell backdoor on ESG appliance. The reverse shell establishes communication with the threat actor's command and control (C2) server, from where it downloads the SEASPY backdoor to the ESG appliance. The actors delivered the payload to the victim via a phishing email with a malicious attachment.
- **SEASPY** – SEASPY is a persistent and passive backdoor that masquerades as a legitimate Barracuda service. SEASPY monitors traffic from the actor's C2 server. When the right packet sequence is captured, it establishes a Transmission Control Protocol (TCP) reverse shell to the C2 server. The shell allows the threat actors to execute arbitrary commands on the ESG appliance.
- **SUBMARINE** – SUBMARINE is a novel persistent backdoor executed with root privileges that lives in a Structured Query Language (SQL) database on the ESG appliance. SUBMARINE comprises multiple artifacts—including a SQL trigger, shell scripts, and a loaded library for a Linux daemon—that together enable execution with root privileges, persistence, command and control, and cleanup. CISA also analyzed artifacts related to SUBMARINE that contained the contents of the compromised SQL database. This malware poses a severe threat for lateral movement.

For more information, including indicators of compromise and YARA rules for detection, on the exploit payload, SEASPY, and SUBMARINE backdoor, see the following Malware Analysis Reports:

- Exploit Payload Backdoor MAR-10454006-r3.v1.CLEAR
- SEASPY Backdoor MAR-10454006-r2.v1.CLEAR
- SUBMARINE Backdoor MAR-10454006-r1.v2.CLEAR

For more information on CVE-2023-2868 see, Barracuda's page Barracuda Email Security Gateway Appliance (ESG) Vulnerability and Mandiant's blogpost Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor.

To report suspicious or criminal activity related to information found in these malware analysis reports, contact CISA's 24/7 Operations Center at Report@cisa.gov or 1-844-Say-CISA (1-844-729-2472).
