UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0337

CISA UNCOVERS BACKDOOR IN ESG APPLIANCES

DATE ISSUED: 02nd August 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) has identified a new malware strain named Submarine (also referred to as DepthCharge by Mandiant) on the compromised Barracuda ESG (Email Security Gateway) appliances.

BREAKDOWN

Barracuda disclosed that the attackers took advantage of the CVE-2023-2868 remote command injection zero-day vulnerability to deploy newly discovered malware named Saltwater and SeaSpy. Additionally, they used a malicious tool called SeaSide to establish reverse shells, enabling them to gain convenient remote access to the compromised systems. However, CISA has discovered another new malware strain known as Submarine that lives in a Structured Query Language (SQL) database on the ESG appliance. The submarine is a multi-component backdoor that is utilized for evading detection, maintaining persistence, and harvesting data from the affected systems. A suspected pro-China hacker group (UNC4841) deployed the backdoor in a series of data-theft attacks detected in May. The threat actors responded to Barracuda's remediation efforts by employing this additional malware to maintain continuous access to customer ESG appliances.

REMEDIATION STEPS

- Barracuda recommends customers discontinue the use of the compromised ESG appliance and contact Barracuda support (support@barracuda.com) to obtain a new ESG virtual or hardware appliance.
- Implement Email Authentication Protocols: Utilize SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify sender authenticity and prevent email spoofing.
- Conduct Regular Security Audits: Perform regular security audits of email gateway configurations and policies to identify and address any vulnerabilities.

REFERENCES & RESOURCES

The Hacker News https://thehackernews.com/2023/07/hackers-deploy-submarine-backdoor-in.html

Bleeping Computer https://www.bleepingcomputer.com/news/security/cisa-new-submarine-malware-found-on-hacked-barracuda-esg-appliances/