Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Chinese Hacking Group Exploits Barracuda Zero-Day

Date of Publication	Admiralty Code	TA Number
August 30, 2023	A1	TA2023350

Summary

Attack Began: October 2022
Malware: DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE.
Threat Actor: UNC4841
Attack Region: Parts of Europe, Asia, South Africa, Australia, and the USA
Targeted Industry: Government, High-Tech, IT, Healthcare, Biotechnology, Telecommunication, Defense, Aerospace, Education, Consulting and Professional Services, Trade, Semiconductor, Energy, Non-Profit, Logistics, Manufacturing, Foreign Affairs
Attack: The Chinese-linked hacking group, tracked as UNC4841, has prominently directed its efforts towards infiltrating and compromising various entities in recent attacks. These offensives were particularly geared towards exploiting a zero-day vulnerability in the Barracuda Email Security Gateway (ESG), constituting a pivotal element of their comprehensive global espionage campaign.

Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-2868	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	Barracuda Networks Email Security Gateway (ESG) Appliance	✓	✓	✓

Attack Details

#1 The Chinese-associated hacking faction, tracked under the UNC4841, has demonstrated a notable inclination for targeting and infiltrating organizations in recent offensive operations. They have particularly focused on exploiting a vulnerability within the Barracuda Email Security Gateway (ESG). This calculated tactic is a significant component of a widespread global espionage campaign.

#2 UNC4841 stands as a well-endowed entity, employing an extensive array of malware and custom-crafted tools to orchestrate exfiltration from systems owned by prominent figures in governmental and high-tech spheres. Employing innovative tactics, UNC4841 introduced distinctive strains of malware tailored to sustain a presence within a select subset of high-priority targets.

#3 The modus operandi revolves around the exploitation of CVE-2023-2868 to deploy malicious software and execute post-exploitation actions. In specific instances, these breaches have triggered the deployment of supplementary malware varieties- namely, DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE—meticulously orchestrated to ensure persistence.

#4 SKIPJACK functions as a passive implant, creating a listener for specified email headers and subjects, deciphering and executing contents. Conversely, DEPTHCHARGE is preloaded into the Barracuda SMTP (BSMTP) daemon using environment variables, acquiring encrypted commands for execution. It also infiltrates configuration and system backups, automatically restoring itself during the backup restoration process. This allows it to maintain persistence even when new appliances are deployed.

#5 The third strain of malware, exclusively sent to selected targets, materializes as FOXTROT—an initiated C++ implant orchestrated via a C-based program named FOXGLOVE. Operating across TCP, FOXTROT possesses the capability to capture keystrokes, implement shell commands, transmit files, and establish a reverse shell.

Recommendations

Prioritize Patching CVE-2023-2868: Make certain that all Barracuda Email Security Gateway appliances receive timely updates containing the required security **patches** to address the vulnerability. Consistently monitor for updates and promptly apply them.

Network Segmentation and Isolation: Implementing robust network segmentation and isolating critical systems can minimize the lateral movement of malware within the network. This can help prevent the spread of malware strains like DEPTHCHARGE, which preloads into the Barracuda SMTP daemon.

Behavior-Based Intrusion Detection: Consider implementing behavior-based intrusion detection systems that can identify anomalous patterns and activities, even if they involve novel malware strains. This can provide an extra layer of defense against UNC4841's innovative tactics.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**T1543** Create or Modify System Process	**T1543.004** Launch Daemon	**T1574** Hijack Execution Flow
T1068 Exploitation for Privilege Escalation	**T1055** Process Injection	**T1211** Exploitation for Defense Evasion	**T1059** Command and Scripting Interpreter
T1212 Exploitation for Credential Access	**T1056** Input Capture	**T1056.001** Keylogging	**T1057** Process Discovery
T1082 System Information Discovery	**T1560** Archive Collected Data	**T1005** Data from Local System	**T1071** Application Layer Protocol
T1132 Data Encoding	**T1105** Ingress Tool Transfer	**T1588.006** Vulnerabilities	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	101[.]229[.]146[.]218, 103[.]146[.]179[.]101, 103[.]27[.]108[.]62, 103[.]77[.]192[.]13, 103[.]77[.]192[.]88, 103[.]93[.]78[.]142, 104[.]156[.]229[.]226, 104[.]223[.]20[.]222, 107[.]148[.]149[.]156, 107[.]148[.]219[.]227, 107[.]148[.]219[.]53, 107[.]148[.]219[.]54, 107[.]148[.]219[.]55, 107[.]148[.]223[.]196, 107[.]173[.]62[.]158, 113[.]52[.]106[.]3, 137[.]175[.]19[.]25, 137[.]175[.]28[.]251, 137[.]175[.]30[.]36, 137[.]175[.]30[.]86, 137[.]175[.]51[.]147, 137[.]175[.]53[.]17, 137[.]175[.]53[.]170, 137[.]175[.]53[.]218, 137[.]175[.]60[.]252, 137[.]175[.]60[.]253, 137[.]175[.]78[.]66, 139[.]84[.]227[.]9, 155[.]94[.]160[.]72, 155[.]94[.]160[.]95, 182[.]239[.]114[.]135, 182[.]239[.]114[.]254, 185[.]243[.]41[.]209, 192[.]74[.]226[.]142, 192[.]74[.]254[.]229, 195[.]234[.]82[.]132, 198[.]2[.]254[.]219, 198[.]2[.]254[.]220, 198[.]2[.]254[.]221, 198[.]2[.]254[.]222, 198[.]2[.]254[.]223,

TYPE	VALUE
IPv4	199[.]247[.]23[.]80, 213[.]156[.]153[.]34, 216[.]238[.]112[.]82, 23[.]224[.]42[.]29, 23[.]224[.]78[.]130, 23[.]224[.]78[.]131, 23[.]224[.]78[.]132, 23[.]224[.]78[.]133, 23[.]224[.]78[.]134, 37[.]9[.]35[.]217, 38[.]54[.]1[.]82, 38[.]54[.]113[.]205, 38[.]60[.]254[.]165, 45[.]148[.]16[.]42, 45[.]148[.]16[.]46, 45[.]154[.]253[.]153, 45[.]154[.]253[.]154, 45[.]63[.]76[.]67, 51[.]91[.]79[.]17, 52[.]23[.]241[.]105, 54[.]197[.]109[.]223, 64[.]176[.]4[.]234, 64[.]176[.]7[.]59
Domains	bestfindthetruth[.]com, fessionalwork[.]com, gesturefavour[.]com, goldenunder[.]com, singamofing[.]com, singnode[.]com, togetheroffway[.]com, troublendsef[.]com, mx01.bestfindthetruth[.]com, xxl17z.dnslog[.]cn
MD5	06528143748b54793b2a7561d96138c5, 4495cb72708f486b734de6b6c6402aba, 61514ac639721a51e98c47f2ac3afe81, f667939000c941e5b9dc91303c98b7fc, fe1e2d676c91f899b706682b70176983, 0d67f50a0bf7a3a017784146ac41ada0, 206b05ef55aff6fa453ba8e5f6c55167, 42722b7d04f58dcb8bd80fe41c7ea09e, 5392fb400bd671d4b185fb35a9b23fd3, 878cf1de91f3ae543fd290c31adcbda4, ac4fb6d0bfc871be6f68bfa647fc0125, 479315620c9a5a62a745ab586ba7b78c,

TYPE	VALUE
MD5	683acdb559bbc7fb64431d1f579a8104, ef00c92fa005c2f61ec23d5278a8fa25, ff4f425be50bacbb10f16287aaddb7e3, 94b6f76da938ef855a91011f16252d59, 32ffe48d1a8ced49c53033eb65eff6f3, 8406f74ac2c57807735a9b86f61da9f9, d81263e6872cc805e6cf4ca05d86df4e, da06e7c32f070a9bb96b720ef332b50b, c5c93ba36e079892c1123fe9dffd660f, 19e373b13297de1783cecf856dc48eb0, c56d7b86e59c5c737ee7537d7cf13df1, cb0f7f216e8965f40a724bc15db7510b, 881b7846f8384c12c7481b23011d8e45, f5ab04a920302931a8bd063f27b745cc, 0245e7f9105253ecb30de301842e28e4, 0c227990210e7e9d704c165abd76ebe2, 132a342273cd469a34938044e8f62482, 1bc5212a856f028747c062b66c3a722a, 2d841cb153bebcfdee5c54472b017af2, 2e30520f8536a27dd59eabbcb8e3532a, 349ca242bc6d2652d84146f5f91c3dbb, 3e3f72f99062255d6320d5e686f0e212, 4c1c2db989e0e881232c7748593d291e, 7d7fd05b262342a9e8237ce14ec41c3b, 8fc03800c1179a18fbd58d746596fa7d, a45ca19435c2976a29300128dc410fd4, ba7af4f98d85e5847c08cf6cefdf35dc, c528b6398c86f8bdcfa3f9de7837ebfe, c7a89a215e74104682880def469d4758, c979e8651c1f40d685be2f66e8c2c610, d1392095086c07bd8d2ef174cb5f6ca8, ad1dc51a66201689d442499f70b78dea, dde2d3347b76070fff14f6c0412f95ba, 858174c8f4a45e9564382d4480831c6b, 2ccb9759800154de817bf779a52d48f8, 177add288b289d43236d2dba33e65956, e52871d82de01b7e7f134c776703f696, 336c12441b7a678280562729c974a840, 5fdee67c82f5480edfa54afc5a9dc834, 407738e565b4e9dafb07b782ebcf46b0, 67a4556b021578e0a421fdc251f07e04, 694cdb49879f1321abb4605adf634935, 6f79ef58b354fd33824c96625590c244, 7ebd5f3e800dcd0510cfcbe2351d3838, d098fe9674b6b4cb540699c5eb452cb5,

TYPE	VALUE
MD5	03e07c538a5e0e7906af803a83c97a1e, 0dd78b785e7657999d05d52a64b4c4cf, 35a432e40da597c7ab63ff16b09d19d8, 806250c466824a027e3e85461dc672db, 830fca78440780aef448c862eee2a8ac, b354111afc9c6c26c1475e761d347144, b745626b36b841ed03eddfb08e6bb061, b860198feca7398bc79a8ec69afc65ed, c2e577c71d591999ad5c581e49343093, e68cd991777118d76e7bce163d8a2bc1, ed648c366b6e564fc636c072bbcac907, ff005f1ff98ec1cd678785baa0386bd1, a28de396aa91b7faca35e861b634c502, 1b1830abaf95bd5a44aa3873df901f28, 1fea55b7c9d13d822a64b2370d015da7, 3b93b524db66f8bb3df8279a141734bb

Patch Link

https://status.barracuda.com/incidents/34kx82j5n4q9

References

https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation

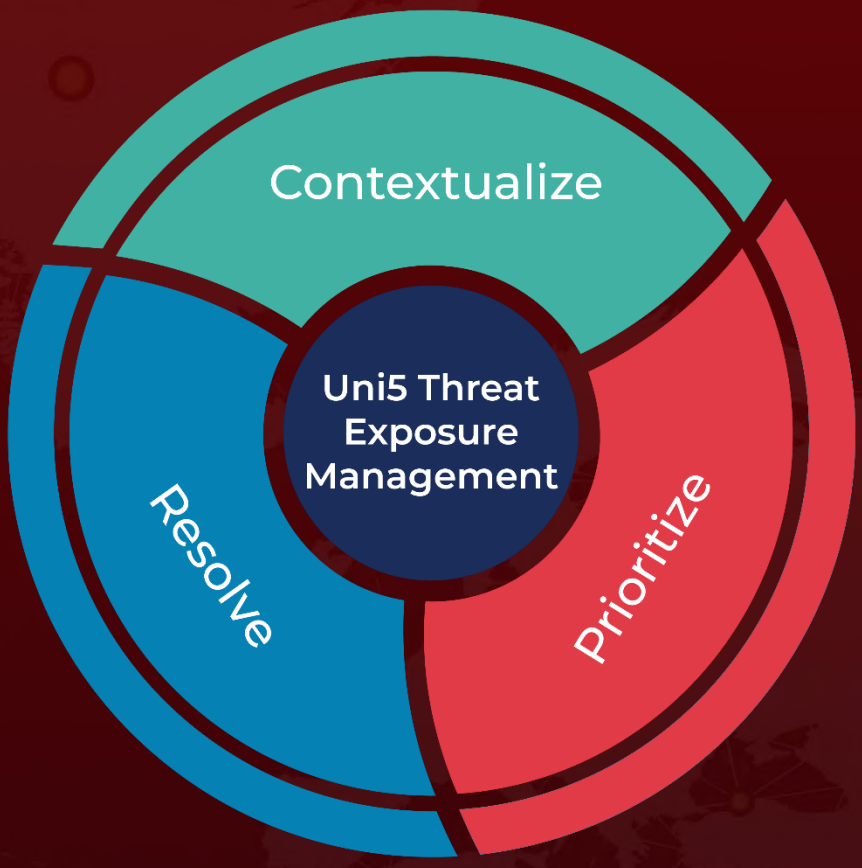
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

https://www.hivepro.com/a-zero-day-vulnerability-found-in-barracuda-email-security-gateway/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 30, 2023 • 10:00 PM

More at www.hivepro.com