Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

ProxyShellMiner Exploits Windows Exchange Server Vulnerabilities for Cryptocurrency Mining

Date of Publication	Admiralty Code	TA Number
February 17, 2023	A1	TA2023087

Summary

First Seen: May 2021
Affected Product: Microsoft Exchange Server
Attack: ProxyShellMiner exploits Windows Exchange servers' vulnerabilities, which are used to gain unauthorized access and compromise an organization, leading to the installation of cryptocurrency miners.

CVEs

CVE	NAME	PATCH
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	✓
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	✓

Attack Details

#1

The ProxyShellMiner malware exploits the ProxyShell vulnerabilities in Windows Exchange servers to gain access and compromise an organization, with the aim of installing crypto miners. The attackers use the domain controller's NETLOGON folder to ensure the malware executes throughout the domain, with the help of legitimate, compromised mail servers acting as Command and Control (C2) servers. The mining of cryptocurrency can cause various negative effects, such as system performance degradation, power consumption, equipment overheating, and even service disruption.

#2

The CVE-2021-34473 vulnerability allows attackers to bypass authentication and gain permissions through specially crafted URLs, while the CVE-2021-34523 and CVE-2021-31207 vulnerabilities are combined to allow unauthorized remote code execution. Once the Exchange mailbox server is compromised, the attacker can modify the ACL settings in the domain, assign Dcsync ACL to a user, and export the hash in the domain to take over the domain controller and control the entire intranet. Ultimately, the mining Trojan horse is delivered again through the domain controller and added to the scheduled task for mining.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0011** Command and Control
T1104 Multi-Stage Channels	**T1055** Process Injection	**T1562** Impair Defenses	**T1053** Scheduled Task/Job
T1027 Obfuscated Files or Information	**T1059** Command and Scripting Interpreter		

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	mail.shaferglazer[.]com mail.ghmproperties[.]com mail.itseasy[.]com mail.techniservinc[.]com
SHA256	936d851d95e621dfb220bed06011e6fac0019dba7f2e601f47764301f5ce60e9, 93430f789cc8397d6476597c54665caf3e2eaedbf90b3faa96bda207bfef0d80, b3bb2131d7f2bfe9243462330662c17001644298bcba42f59ee3fd305af02b80, e86d39fb3a97910aa31fea95f82b2b3d567074639312862b4eba3e1f5525e7a7, 0045babd9555de9612982b6bad2da3303a5f920e4c4d983741de0e5c52633adc, 00d196f4ffe017676a060bd91b261765f26cf1c217d263dd5aaeea14fff076ef, 262e03bdd3e341a211fc60d3864e5397856b273a3b9ea02e4d24227af8bd8366, 28c83220eafe0b20bcab2e6da10d060f64029d93072ec7b05c5a58b539bdd7cb, 2bb26e1ad01d13c2c7675b8c5bae9aaa4eae12ebcc613a6f18f2d6f49654765e, 464915467e993d199b24bbe371a746c67aa0fcdc6519c81cf8d7d02be753d072, 470ed37e23d6727632762ba9abe504e4ade0f497b5b4b92f95e54824a75c715f,

TYPE	VALUE
SHA256	dbf4ecc7c3d14ac20504ba717825d94be0eb836e346736ea828ba07c6ce670f3, efc5f0b30288af8e822aaa39573c356f4566224df13342eab537071ef88a1687, f302f60bb67a868a0755c347a37872fb606cf8980339c1c633fafb8887893642, fb01a223346337859da55a22f11db796eddf462e553324aae07157dbeee73dde, 858b2388ccc40e9492c300863218f4c812effbba9957a75b1bdb3a857866f4a7, 386fddb95863142e049deaeb50ca031b296ef16929e97986a6e3208496067d12, e965e0aa86506949bd1a2df7fb0302c97124cb67eade4c9057a66e9c00ca1c36, d519e08310bd660302ca1cc6ef84eb8d226b727cae134765c285be5fd6a026d3, 221befc820f3dd4bad7644a91474f152af2a254134cbe2b6c5d82e5799e54489, 221befc820f3dd4bad7644a91474f152af2a254134cbe2b6c5d82e5799e54489, 189ab9a1c8dd4ee739de12596214093a2cd2d302663879848f18d5d472e95022, dc8aff8bc675dcfc5988caf198a2460bee232f153a0ff76fe46095c5abe6e57b, 4897b8e3e9a40b8a95ec4b03674906f44383f4fa564784e6aab4e4dd7112d0db, f17fac8576e1214976b6390daf795d61c4455c4e573a66adc3b255ff02f3b724, 714f20fdf035c83919501653160d465d36a90a5af63dd8a614d00241c55e3e71, 79a3550f3519b1c8237901eea12b1a2b7ac758784af61d2da9f453ce2a985745, 77ceaa18a65df2fc19763495d8bb811938a4c3c79d1cd788e464acb9bf7dd323, d4b1bbc543bbb1b3394de4588362bfa57df84cc658b190cf67e5f10f06cdec4b, 795315c89332e0743d7864a0d20f0e3befc06fa04279e3a424a32d334eb9a512, 4fd5c775940aafd9f93dc2830b326defdeaa76dab66702be84c58924d93936da, 8b01557e339623d45116e87c9f0d112f22eab8ca06b34229e2bd37057742b980, 61dbfa414eac7acaeaba373801f7f6edb58b8ee6d209a2a4453686c557e02ad1, 83a91514dd87b264443ffc515ae2719e60b8bb0452cf1a53b463f016bcdb03bb,

TYPE	VALUE
SHA256	c13cf4bb0d025f9d74889215a8071fc6460a6fd339fe48d1b426be4dfecd1833, f356b4824a51e13618ceba2ab522132b5959e2c49d2f57867f63e49b98417b9a, b0bf535d5d3e08c51e6dc7967ceca7a533beddb465cb9b5440f412e47e1ad7de, 05885bc5d29c90c9e49fe2c4cadabb1a713fdd3ac0a4a49a9b0cf50e76d95692, a98d334ea0f9dc39f6c48fbeacaedaaf35e2619efaa045cdbcfd4e233de0775c, c29d5af9cb1656fc2a1d0a376c343b08f58a73c2721ec9613140dbd4e31c1975, dfd7cb555b67866f201d1d7ed37da76c1bdd9df5979b4f0b22b2cf45d648479d, 0107ed0325f626d76c46bc437d3cebd66c3ad41ffc649738a078b62b7b2855ff, ff2b5c12f248f783b1b8a9e85daa2d0f912c23d1b6eb9d08d4f27ed3a848ac73, b48a57e15701460c876d8773a02d74a236040543dc84435bb144bda7fc55756a, 62d198f9d1753c5b1ec4c6d197f0628857c7e2e05a570009e78b17a1cd4bfc77, 76fdd0f432520008155c50ba35063264dee842acc25ad85462c1f4b1d8ba5b3e, 1f1a3a5659071ce2b852d2473d42f840fb1f6e929ee92d2442f4bfa674caf22a, 5ee0ae90aab227a4081ab7947f59966405c1feb3b3293fc4d4935d3ff8ce8e84, 21e3e8526394d1c8bd8b86ee7d4b9332edf5e512a852ff5c55ccb4074ed2f40c, 8bc2f75f48a94fd4308608f0c9a74cbfb7686eeea9148932ea596acc1cd1d3e9, 6588d928a8088f94f60d2ea9f7ba0be20b489e188d64572a7b8cf195668aea5f, 271a916063d57a1fca1a61ba4cf294bdeb3664a2859c2438b065af3d35163f2d, db7103f16832321fb888abc21ab3466dd4baece803fdd54d2edfb5b901ffeeab, e5aac8e5308a97f3c02c38f272c1f42fec19e045ded9395fe8632a0cc37f0ca6, c0c749bc5aff378870ca117b5290a2a7e0dffc21df5a332ca92524368caa3ef1, 85df166268dddf4fb4fedad86f13b0229dddd4dd87d9de3355c08c23974cd74a, 8633106081c9246e83ed899d645adc7dc94464c46014cde26b66e9ec190f1cb9,

TYPE	VALUE
SHA256	e3c87972e925ec4e4e9cc2cd77092e80a9b5e20741232e3202fbdf5b0df7a5c0, b19428c70c927eca3e3a0453cba41a5862c5a9bb82a2b94f2c70cfb834f201d9, 05e19a3047c52ecade2a7cabc47a1f8ad721cc56521aa17b24d5a458b6f5150a, d573b805aa549991ad7f39b98367c813c932a645141c4a0375998c1041be17ab, b1ea1863d5a3811547170cc37fb979c14415528fd17062109b0f5da077c89171, 74cc2967fca79283e1cf9441f470518f397fc792606582ec804ac846f0178b42, 5ec41eaf2aa08b6c8f7122c0b4fc789d858f1702e2eafa249aef1a55464dd286, 5e777165a9e654f2bff64df071b275b825c436b1d230124d97a2baf00bc94fca, 5c5c2c6a6774fdd462f731f4b67e26b3d81de309a3eb3864895cf6181c28b2ab, 45c3b528baae7e912dc40f0fa616c4ba79fcaec531f9816ee4f35de3a960abbc, 9bdbeb586de734672d31ce6a489b3cf1f0946667824ae03be0a8a7e39207a301, a2ecdf7b5db735476495d1e6f7781c099c977b3dbce571f22cd0c121d436254d, a6f33a412556758c4471658b1949eb58fce742456472ac4726d8069d08385013, b1dea969973202397d2d0e68e7cb5cb719015b974e81c2dd3294ff67297c7019

Patch Link

https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-may-11-2021-kb5003435-028bd051-b2f1-4310-8f35-c41c9ce5a2f1

https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-april-13-2021-kb5001779-8e08f3b3-fc7b-466c-bbb7-5d5aa16ef064

References

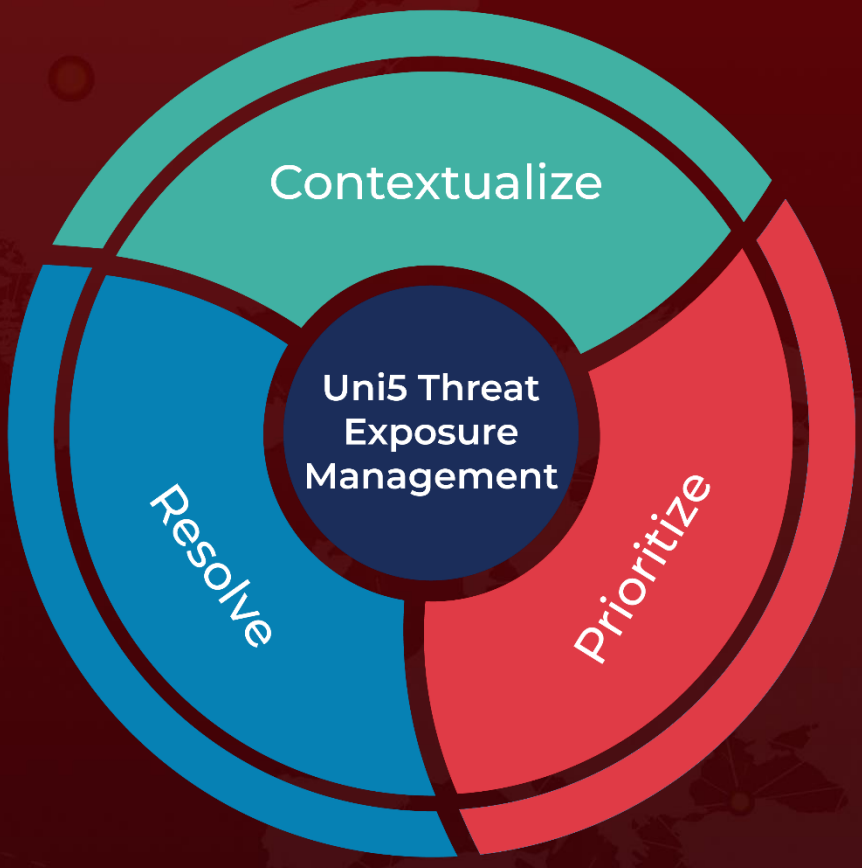
https://blog.morphisec.com/proxyshellminer-campaign

https://www.bilibili.com/read/cv17634838?from=articleDetail

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

February 17, 2023 • 12:30 AM

More at www.hivepro.com