Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

FreeWorld Ransomware Targets MSSQL Servers Facing Siege

Date of Publication	Admiralty Code	TA Number
September 6, 2023	A1	TA2023355

Summary

Attack Began: August 2023
Campaign: DB#JAMMER
Malware: FreeWorld Ransomware
Attack Region: Worldwide
Attack: Adversaries are capitalizing on inadequately protected Microsoft SQL (MS SQL) servers in an operation known as DB#JAMMER, deploying both Cobalt Strike and a ransomware strain named FreeWorld, which appears to be a more recent iteration of the Mimic ransomware.

Attack Regions

Attack Details

#1 A cyberattack campaign, known as DB#JAMMER, has been discovered, targeting vulnerable Microsoft SQL Server (MSSQL) databases. The threat actors gained unauthorized access to the victim's host by employing brute-force techniques to breach an MSSQL login. Once authenticated, they swiftly initiated a comprehensive database enumeration, with a particular emphasis on extracting additional login credentials.

#2 They exploited the xp_cmdshell configuration option to execute shell commands and conduct reconnaissance activities. This multifaceted attack strategy ultimately facilitated the delivery of FreeWorld ransomware and Cobalt Strike payloads. Consequently, they established persistent access on the host, connecting to a remote SMB share for file transfers, including malicious tools like Cobalt Strike.

#3 This served as a gateway for deploying AnyDesk software, which facilitated the distribution of the FreeWorld ransomware. In some cases, the attackers also attempted to establish RDP persistence through Ngrok. FreeWorld ransomware exhibits characteristics reminiscent of the **Mimic ransomware** variant, particularly in its utilization of a legitimate application called Everything.exe to query and identify target files for encryption.

#4 Upon execution, the ransomware encrypts the victim's host, appending the '.FreeWorldEncryption' extension to the compromised files. Subsequently, it generates a text file named 'FreeWorld-Contact.txt,' containing instructions on how to remit the ransom.

#5 Worldwide, there are a staggering 422.3k MS SQL servers, with the greatest concentration found in China, the United States, Korea, and India. Alarmingly, there has been a remarkable 174% surge in ransomware incidents targeting vulnerable SQL servers on a global scale.

Recommendations

Enhance MSSQL Server Security: Implement multi-factor authentication (MFA) and robust password policies to mitigate brute-force attacks, especially in regions with a high concentration of MS SQL servers like China, the United States, Korea, and India. In MSSQL environments, restrict the usage of the xp_cmdshell stored procedure.

Monitoring and Access Control: Implement monitoring and detection systems to identify unauthorized access and suspicious activities, such as brute-force attempts and unusual queries. Ensure that access privileges are limited to essential personnel and that permissions are regularly updated. Restrict service exposure to only allow application servers access to the database, avoiding any unnecessary external exposure.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0008** Lateral Movement	**TA0010** Exfiltration	**TA0011** Command and Control
TA0040 Impact	**T1110** Brute Force	**T1046** Network Service Discovery	**T1112** Modify Registry
T1562.001 Disable or Modify Tools	**T1098** Account Manipulation	**T1505.001** SQL Stored Procedures	**T1003** OS Credential Dumping
T1110.001 Password Guessing	**T1021.001** Remote Desktop Protocol	**T1105** Ingress Tool Transfer	**T1572** Protocol Tunneling
T1573.001 Symmetric Cryptography	**T1219** Remote Access Software	**T1567** Exfiltration Over Web Service	**T1486** Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8937a510446ed36717bb8180e5e4665c0c5d5bc160046a31b28417c86fb1ba0f, 9d576cd022301e7b0c07f8640bdeb55e76fa2eb38f23e4b9e49e2cdba5f8422d, 867143a1c945e7006740422972f670055e83cc0a99b3fa71b14deababca927fe,

TYPE	VALUE
SHA256	80bf2731a81c113432f061b397d70cac72d907c39102513abe0f2bae079373e4, 75975b0c890f804dab19f68d7072f8c04c5fe5162d2a4199448fc0e1ad03690b, c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e, 4c83e46a29106afbaf5279029d102b489d958781764289b61ab5b618a4307405, 0a2cfffb353b1f14dd696f8e86ea453c49fa3eb35f16e87ff13ecdf875206897, 74cc7b9f881ca76ca5b7f7d1760e069731c0e438837e66e78aee0812122cb32d, 947afaa9cd9c97cabd531541107d9c16885c18df1ad56d97612ddbc628113ab5, 95a73b9fda6a1669e6467dcf3e0d92f964ede58789c65082e0b75adf8d774d66, a3d865789d2bae26726b6169c4639161137aef72044a1c01647c521f09df2e16, e93f3c72a0d605ef0d81e2421cca19534147dba0dded2ee29048b7c2eb11b20a, cc54096fb8867ff6a4f5a5c7bb8cc795881375031eed2c93e815ec49db6f4bff, 68ed5f4b4eabd66190ae39b45fff0856fba4b3918b44a6d831a5b9120b48a1e9, 42396ce27e22be8c2f0620ee61611d7f86dfe9543d2f2e2af3ef5e85613cee32, f9f6c453da12c8ff16415c9b696c2e7df95a46e9b07455cd129ce586b954870d, 569e3b6eac58c4e694a000eb534b1f33508a8b5de8a7ad3749c24727cc878f4d, 8937a510446ed36717bb8180e5e4665c0c5d5bc160046a31b28417c86fb1ba0f, 2d27f57b4f193a563443acc7fe0cbf611f4ff0f1171fcbdf16c3ecef8f9dbedb, 2b68fe68104359e1bc044db33b4e88b913e4f5be69da9fd6e87ea59a50311e6e, 11259f77f4e477cd066008fbfc7c31d5bbdc9ef708c4b255791ee380999a725c, bd1c3303d13cadf8bbd6200597e9d365ec3c05f1f48052cd47dcd69e77c94378, cd5a2ec1a95d754ee5189bfee6e1f61c76a0a5ee8173da273e02f24a62faccfa, bec3f75f638025a5fe3b8d278856fd273999c49ae7543c109205879b59afc4c3, 2ac044936a922455c80e93f76cc3e2ce539fdab1af65c0703b57177feb5326a6,

TYPE	VALUE
SHA256	fbc9ba3ba7387c38eb9832213b2d87cf5f9fc2ba557e6fdf23556665ca3ef44a, 08f827a63228d7bcd0d02dd131c1ae29bc1d9c3619be67ea99d8a62440be57ab
Domain	gelsd[.]com
IPv4	45.148.122[.]63

References

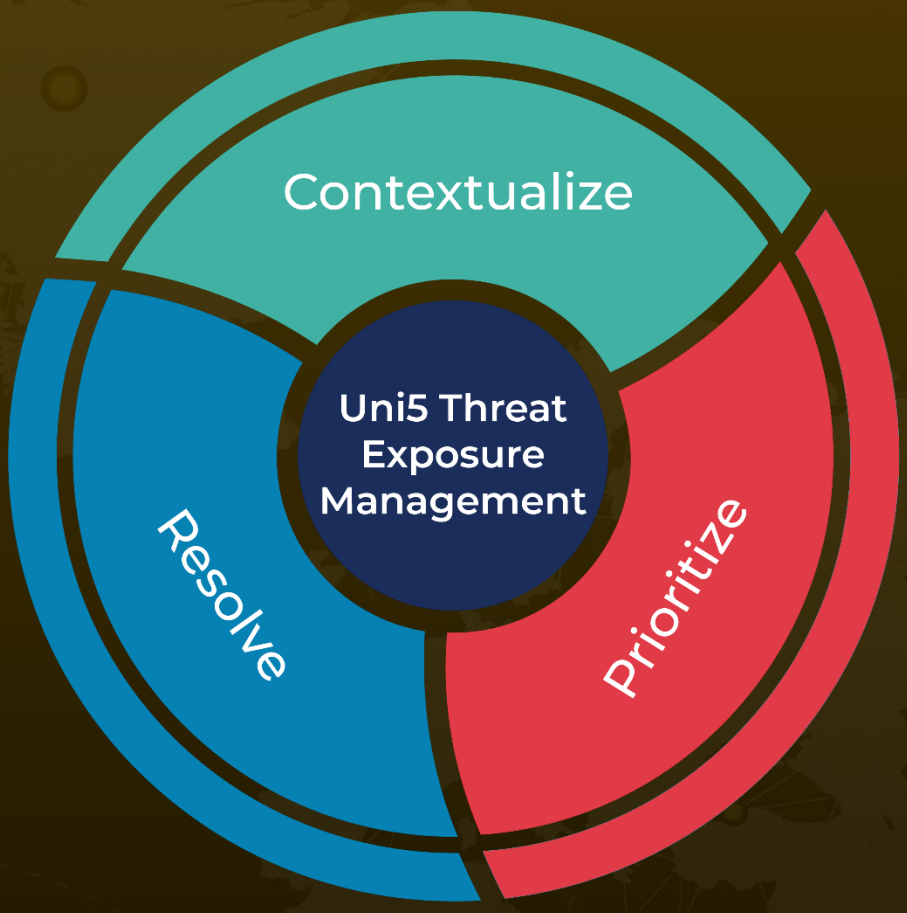
https://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/

https://www.hivepro.com/new-ransomware-mimic-emerges-in-the-wild-abusing-legitimate-tool-for-faster-encryption/

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

September 6, 2023 . 6:00 AM

More at www.hivepro.com