Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

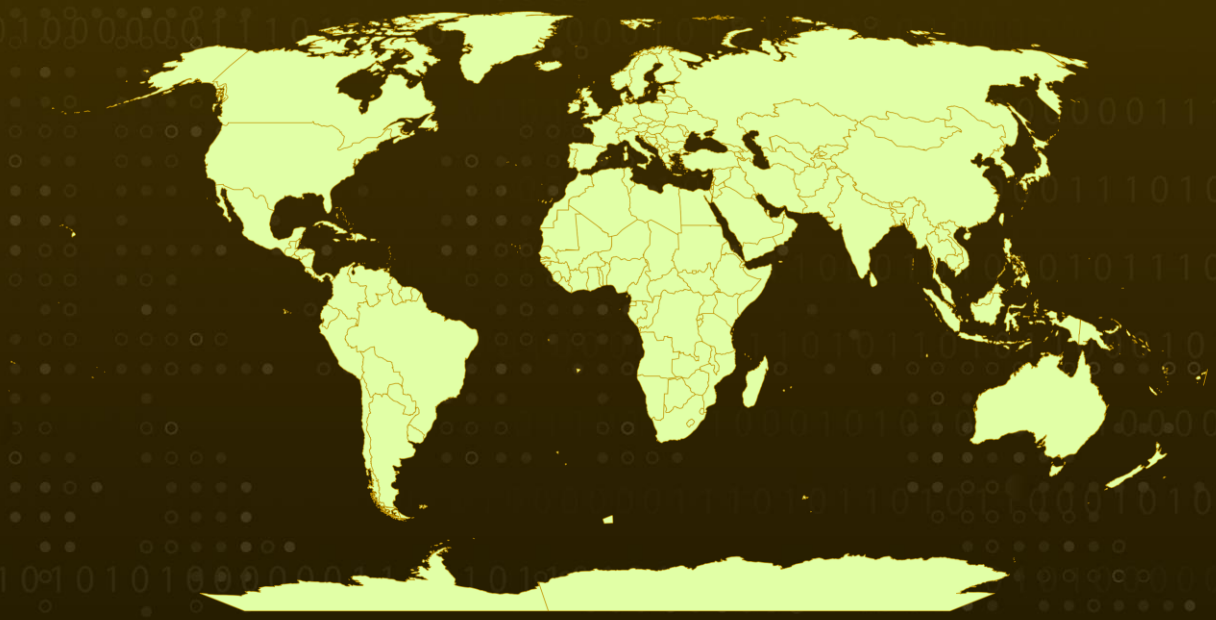
From Brute-Force to BlueSky Ransomware

Date of Publication	Admiralty Code	TA Number
December 6, 2023	A1	TA2023490

Summary

Attack Commenced: December 2022
Malware: BlueSky Ransomware, Tor2Mine
Attack Region: Worldwide
Attack: A focused campaign directed at publicly accessible MSSQL servers unfolded, entailing malicious actors' utilization of Cobalt Strike and Tor2Mine. After gaining successful network access, the adversaries deployed the BlueSky ransomware across the entire network.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF and NG	✗	✓	✓

Attack Details

#1 During December 2022, a series of orchestrated activities were directed towards publicly accessible MSSQL servers. Malicious actors then utilized Cobalt Strike and Tor2Mine to execute post-exploitation maneuvers. Subsequently, upon gaining network access, they propagated the **BlueSky ransomware** across the entire network.

#2 The initial breach was facilitated through a brute-force attack targeting the MS SQL 'sa' (System Administrator) account on a server exposed to the internet. After successfully acquiring the password, the adversaries enabled users with sysadmin privileges to execute shell commands on the host. Subsequently, a Cobalt Strike beacon and a PowerShell script were deployed, establishing a connection to a Tor2Mine stager server.

#3 This sequence was followed by the execution of a PowerShell script designed to perform various operations, including assessing the privileges of the active user, disabling antivirus solutions, and deploying a miner payload named java.exe. Depending on the user's privileges, the script also created scheduled tasks and Windows services to ensure persistence on the host.

#4 The PowerShell scripts involved in this incident, as well as the infrastructure for the Tor2Mine server, were later identified in May 2023 in conjunction with the exploitation of the **PaperCut NG CVE-2023-27350**.

Recommendations

Enhance MSSQL Server Security: Strengthen authentication mechanisms to mitigate brute-force attacks. Enforce robust password policies, particularly for critical accounts like the System Administrator account. Regularly audit and update security configurations for publicly accessible MSSQL servers.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Implement Network Security Measures: Employ intrusion detection and prevention systems to identify and thwart malicious activities. Monitor network traffic for unusual patterns, especially after successful login attempts, to detect potential unauthorized access.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1078 Valid Accounts	T1059.003 Windows Command Shell	T1059.001 PowerShell	T1569.002 Service Execution
T1053.005 Scheduled Task	T1543.003 Windows Service	T1055 Process Injection	T1562.001 Disable or Modify Tools
T1112 Modify Registry	T1027 Obfuscated Files or Information	T1036.004 Masquerade Task or Service	T1110 Brute Force
T1003.001 LSASS Memory	T1033 System Owner/User Discovery	T1135 Network Share Discovery	T1021.002 SMB/Windows Admin Shares
T1071.001 Web Protocols	T1486 Data Encrypted for Impact		

Indicators of Compromise (IOCs)

TYPE	VALUE
File Names	del.ps1, checking.ps1, Invoke-PowerDump.ps1
IPv4	5.188.86[.]237

TYPE	VALUE
URLs	hxxp://0x53611451/win/clocal, hxxp://qlqd5zqefmkcr34a[.]onion[.]sh/win/checking[.]hta, hxxps://asq[.]d6shiiwz[.]pw/win/hssl/d6[.]hta, hxxp://83[.]97[.]20[.]81/win/checking[.]hta, hxxp://83[.]97[.]20[.]81/win/update[.]hta, hxxps://asd[.]s7610rir[.]pw/win/checking[.]hta, hxxps://asq[.]r77vh0[.]pw/win/hssl/r7[.]hta, hxxp://asq[.]r77vh0[.]pw/win/checking[.]hta, hxxp://5[.]188[.]86[.]237/vmware[.]exe
MD5	9e88c287eb376f3c319a5cb13f980d36, 7b68bc3dd393c2e5273f180e361f178a, 0c0195c48b6b8582fa6f6373032118da, bfd36fd6a20ccd39f5c3bb64a5c5dd8b, 08bdf000031bbad1a836381f73adace5, 42a80cc2333b612b63a859f17474c9af
SHA1	501af977080d56a55ff0aeba66b58e7f3d1404ea, 07610f11d3b8ccb7b60cc8ad033dda6c7d3940c4, d25340ae8e92a6d29f599fef426a2bc1b5217299, e938646862477e598fcda20d0b7551863f8b651c, 3dff4ae3c421c9143978f8fc9499dca4aed0eac5, e7be97fb2200eb99805e39513304739a7a28b17e
SHA256	74b6d14e35ff51fe47e169e76b4732b9f157cd7e537a2ca587c58dbdb15c624f, d4f4069b1c40a5b27ba0bc15c09dceb7035d054a022bb5d558850edfba0b9534, 11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5, 35b95496b243541d5ad3667f4aabe2ed00066ba8b69b82f10dd1186872ce4be2, f955eeb3a464685eaac96744964134e49e849a03fc910454faaff2109c378b0b, 3b463c94b52414cfaad61ecdac64ca84eaea1ab4be69f75834aaa7701ab5e7d0

Patch Link

https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

References

https://thedfirreport.com/2023/12/04/sql-brute-force-leads-to-bluesky-ransomware/

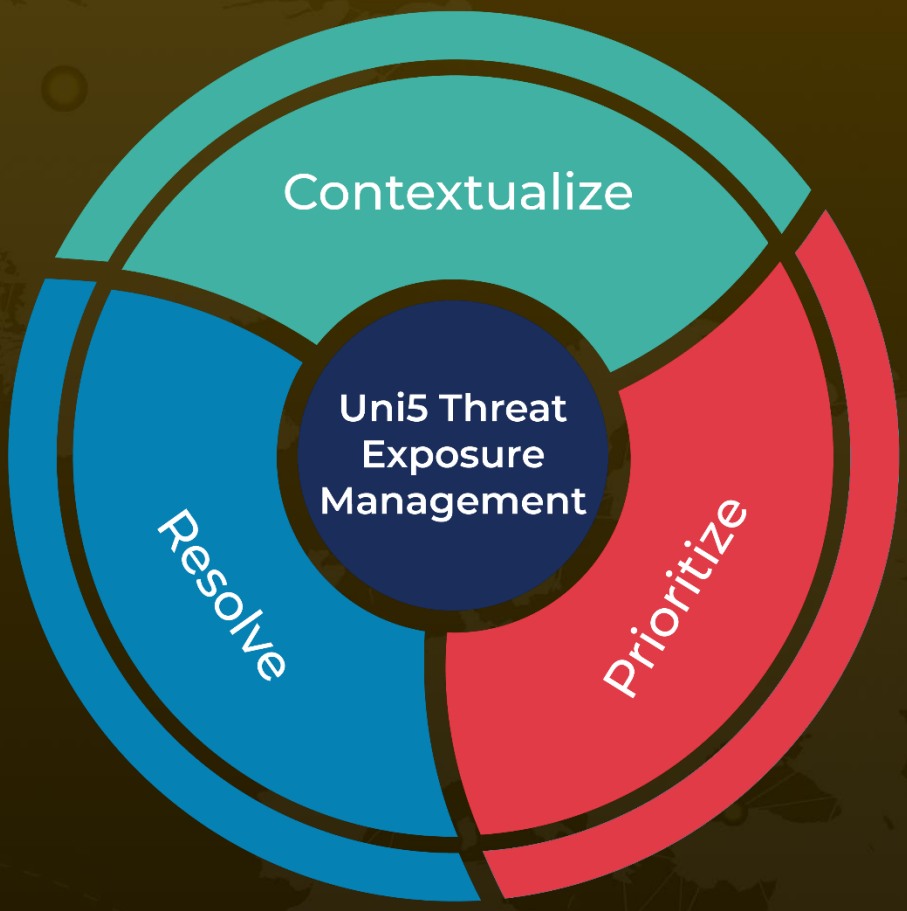
https://www.hivepro.com/threat-advisory/bluesky-ransomware-incorporates-multithreading-to-expedite-encryption/

https://www.hivepro.com/threat-advisory/critical-papercut-security-vulnerabilities-actively-exploited-in-the-wild/

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

December 6, 2023 . 5:00 AM

More at www.hivepro.com