Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

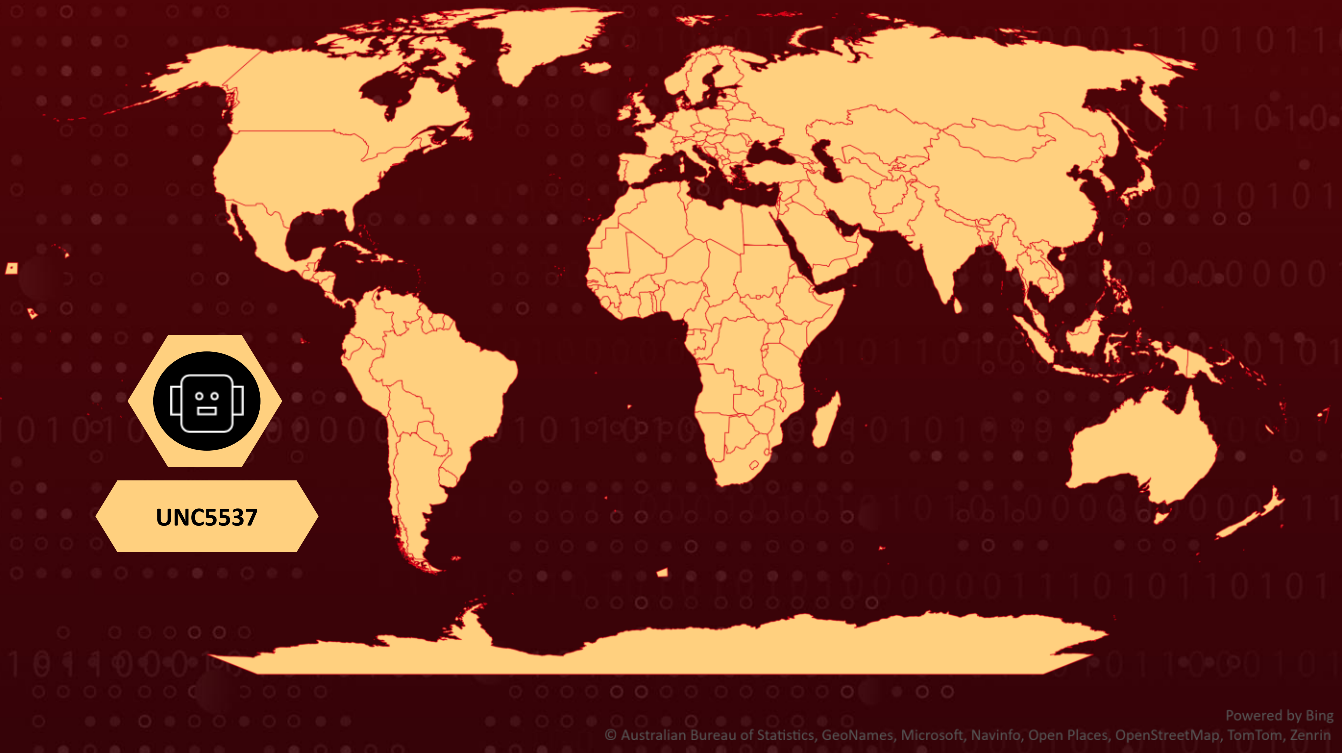
UNC5537 Targeting Snowflake Users for Data Theft and Extortion

Date of Publication	Last updated date	Admiralty Code	TA Number
May 31, 2024	June 11, 2024	A2	TA2024213

Summary

First Seen: May 2024
Targeted Regions: Worldwide
Threat Actor: UNC5537
Malware: Rapeflake (aka FROSTBITE)
Attack: UNC5537, a threat actor, targets Snowflake instances, focusing on data theft and extortion, exploiting weak authentication and VPN IPs. Snowflake customers should heed recent communications, as over 1,500 organizations are targeted. Proactive threat hunting and robust security measures are essential to safeguard against UNC5537's sophisticated attacks.

Attack Regions


UNC5537
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A threat actor named UNC5537 has been actively targeting organizations that use Snowflake instances, focusing on data theft and extortion. This cyber campaign exploits stolen customer credentials to gain unauthorized access to sensitive data stored in Snowflake environments. The attacks are particularly successful in systems that lack two-factor authentication (2FA), making it easier for the threat actor to breach security.

#2 Moreover, UNC5537 uses commercial VPN IPs to obscure their origins and activities, complicating efforts to trace and mitigate these attacks. One of the key tools used by UNC5537 is an attack tool named "rapeflake." Although detailed information about this tool remains unknown, its identification points to the sophistication and targeted nature of the attacks.

#3 In addition to data theft, UNC5537 engages in extortion tactics, further pressuring organizations by publicly posting stolen data on hacker forums. This strategy not only threatens the confidentiality of the affected organizations but also their reputations and operational integrity. The public exposure of stolen data amplifies the urgency for organizations to comply with the extortion demands, exacerbating the impact of the attacks.

#4 Snowflake, a widely adopted cloud-based data warehousing and analytics platform, serves over 9,437 global customers and holds a 21.51% market share. Its ability to manage and analyze vast amounts of data makes it a critical asset for many organizations, highlighting the importance of securing these environments against sophisticated threats like UNC5537.

#5 Investigations into these incidents are still ongoing, reports indicate that over 1500 organizations are currently targeted. There is speculation that ransomware groups may also be involved in this campaign. Meanwhile, Lockbit has seen a significant spike in activity in May with over 20+ victims reported in the past week alone. It is vital for all Snowflake customers to ensure their environments are secured against such threats. Immediate measures, particularly enabling 2FA and applying recent security updates, are essential to mitigating the risk of data theft and extortion.

Recommendations

Enforce Two-Factor Authentication (2FA): Ensure that 2FA is enabled and enforced across your organization. This additional layer of security helps prevent unauthorized access even if credentials are compromised. Make 2FA mandatory for all users to minimize the risk of breaches.

Implement Single Sign-On (SSO): Enforce Single Sign-On (SSO) to centralize and streamline authentication processes. SSO helps manage user access more effectively and can reduce the risk of password-related vulnerabilities. Verify that users cannot bypass SSO by using direct username/password authentication to Snowflake.

Blocking Unauthorized Data Exfiltration: To enhance data security and prevent unauthorized data exfiltration in Snowflake, it is crucial to control the use of the COPY INTO <location> command, which allows unloading data to external URLs. By default, Snowflake permits this functionality, posing a potential risk of data exfiltration. To mitigate this risk, you can configure Snowflake to block such actions by setting the PREVENT_UNLOAD_TO_INLINE_URL parameter to true.

Implement Endpoint Protection: Deploy comprehensive endpoint protection platforms (EPP) that include behavior analysis and real-time threat detection capabilities. Ensure all systems and software are kept up-to-date with the latest security patches.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, storing them securely offline. Test restoration processes to ensure backup integrity and availability. In case of ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0040** Impact	**TA0001** Initial Access	**TA0009** Collection
TA0007 Discovery	**TA0010** Exfiltration	**TA0006** Credential Access	**T1657** Financial Theft
T1619 Cloud Storage Object Discovery	**T1586.003** Cloud Accounts	**T1586** Compromise Accounts	**T1530** Data from Cloud Storage
T1486 Data Encrypted for Impact	**T1212** Exploitation for Credential Access	**T1621** Multi-Factor Authentication Request Generation	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	102[.]165[.]16[.]161, 104[.]129[.]24[.]115, 104[.]129[.]24[.]124, 104[.]223[.]91[.]28, 146[.]70[.]117[.]210, 146[.]70[.]117[.]56, 146[.]70[.]119[.]24, 146[.]70[.]124[.]216, 146[.]70[.]165[.]227, 146[.]70[.]166[.]176, 146[.]70[.]171[.]112, 146[.]70[.]171[.]99, 154[.]47[.]30[.]137, 154[.]47[.]30[.]150, 162[.]33[.]177[.]32, 169[.]150[.]201[.]25, 169[.]150[.]203[.]22, 169[.]150[.]223[.]208, 173[.]44[.]63[.]112, 176[.]123[.]3[.]132, 176[.]123[.]6[.]193, 176[.]220[.]186[.]152, 184[.]147[.]100[.]29, 185[.]156[.]46[.]144, 185[.]156[.]46[.]163, 185[.]204[.]1[.]178, 185[.]213[.]155[.]241, 185[.]248[.]85[.]14, 185[.]248[.]85[.]59, 192[.]252[.]212[.]60, 193[.]32[.]126[.]233, 194[.]230[.]144[.]126, 194[.]230[.]144[.]50, 194[.]230[.]145[.]67, 194[.]230[.]145[.]76, 194[.]230[.]147[.]127, 194[.]230[.]148[.]99, 194[.]230[.]158[.]107, 194[.]230[.]158[.]178, 194[.]230[.]160[.]237, 194[.]230[.]160[.]5, 198[.]44[.]129[.]82, 198[.]44[.]136[.]56, 198[.]44[.]136[.]82,

TYPE	VALUE
IPv4	198[.]54[.]130[.]153, 198[.]54[.]131[.]152, 198[.]54[.]135[.]35, 198[.]54[.]135[.]67, 198[.]54[.]135[.]99, 204[.]152[.]216[.]105, 206[.]217[.]205[.]49, 206[.]217[.]206[.]108, 37[.]19[.]210[.]21, 37[.]19[.]210[.]34, 45[.]134[.]140[.]144, 45[.]134[.]142[.]200, 45[.]155[.]91[.]99, 45[.]27[.]26[.]205, 45[.]86[.]221[.]146, 5[.]47[.]87[.]202, 66[.]115[.]189[.]247, 66[.]63[.]167[.]147, 79[.]127[.]217[.]44, 87[.]249[.]134[.]11, 93[.]115[.]0[.]49, 96[.]44[.]191[.]140, 138[.]199[.]34[.]144, 198[.]44[.]136[.]35, 66[.]115[.]189[.]210, 206[.]217[.]206[.]88, 37[.]19[.]210[.]28, 146[.]70[.]225[.]67, 138[.]199[.]43[.]92, 149[.]102[.]246[.]3, 43[.]225[.]189[.]163, 185[.]201[.]188[.]34, 178[.]249[.]209[.]163, 199[.]116[.]118[.]210, 198[.]54[.]130[.]147, 156[.]59[.]50[.]195, 198[.]44[.]136[.]195, 198[.]44[.]129[.]67, 37[.]19[.]221[.]170, 96[.]44[.]189[.]99, 146[.]70[.]134[.]3, 66[.]115[.]189[.]200, 103[.]75[.]11[.]51, 69[.]4[.]234[.]118, 146[.]70[.]173[.]195, 138[.]199[.]60[.]29, 66[.]115[.]189[.]160,

TYPE	VALUE
IPv4	154[.]47[.]30[.]144, 178[.]249[.]211[.]80, 143[.]244[.]47[.]92, 146[.]70[.]132[.]227, 193[.]19[.]207[.]226, 46[.]19[.]136[.]227, 68[.]235[.]44[.]35, 103[.]136[.]147[.]4, 198[.]54[.]133[.]163, 169[.]150[.]203[.]16, 146[.]70[.]224[.]3, 87[.]249[.]134[.]15, 198[.]54[.]134[.]131, 142[.]147[.]89[.]226, 146[.]70[.]117[.]35, 193[.]19[.]207[.]196, 146[.]70[.]144[.]35, 146[.]70[.]173[.]131, 107[.]150[.]22[.]3, 169[.]150[.]201[.]29, 146[.]70[.]117[.]163, 146[.]70[.]138[.]195, 146[.]70[.]184[.]67, 104[.]129[.]57[.]67, 185[.]248[.]85[.]49, 146[.]70[.]168[.]67, 138[.]199[.]43[.]66, 79[.]127[.]217[.]35, 194[.]127[.]167[.]108, 194[.]36[.]25[.]49, 146[.]70[.]171[.]67, 138[.]199[.]60[.]3, 45[.]134[.]212[.]93, 146[.]70[.]187[.]67, 66[.]63[.]167[.]163, 154[.]47[.]29[.]3, 149[.]102[.]246[.]16, 198[.]44[.]129[.]99, 146[.]70[.]128[.]195, 185[.]65[.]134[.]191, 146[.]70[.]119[.]35, 87[.]249[.]134[.]28, 149[.]102[.]240[.]67, 103[.]75[.]11[.]67, 69[.]4[.]234[.]124, 169[.]150[.]196[.]3, 169[.]150[.]201[.]3, 185[.]188[.]61[.]196,

TYPE	VALUE
IPv4	87[.]249[.]134[.]2, 138[.]199[.]15[.]163, 45[.]134[.]213[.]195, 138[.]199[.]6[.]208, 169[.]150[.]227[.]223, 146[.]70[.]200[.]3, 149[.]88[.]22[.]156, 173[.]205[.]85[.]35, 206[.]217[.]206[.]48, 194[.]36[.]25[.]4, 154[.]47[.]16[.]48, 37[.]19[.]200[.]131, 146[.]70[.]166[.]131, 37[.]19[.]221[.]144, 149[.]88[.]20[.]207, 79[.]127[.]222[.]195, 194[.]127[.]167[.]88, 96[.]44[.]191[.]131, 69[.]4[.]234[.]119, 138[.]199[.]6[.]221, 146[.]70[.]128[.]227, 66[.]63[.]167[.]195, 169[.]150[.]196[.]16, 185[.]201[.]188[.]4, 173[.]44[.]63[.]67, 79[.]127[.]222[.]208, 198[.]54[.]134[.]99, 198[.]54[.]135[.]131, 138[.]199[.]43[.]79, 66[.]115[.]189[.]190, 149[.]88[.]20[.]194, 141[.]98[.]252[.]190, 129[.]227[.]46[.]163, 31[.]171[.]154[.]51, 79[.]127[.]217[.]48, 69[.]4[.]234[.]116, 206[.]217[.]206[.]68, 103[.]125[.]233[.]19, 146[.]70[.]188[.]131, 169[.]150[.]227[.]198, 129[.]227[.]46[.]131, 198[.]44[.]136[.]99, 149[.]88[.]22[.]130, 193[.]138[.]7[.]138, 146[.]70[.]168[.]195, 169[.]150[.]203[.]29, 206[.]217[.]205[.]118, 146[.]70[.]185[.]3, 146[.]70[.]124[.]131,

TYPE	VALUE
IPv4	194[.]127[.]199[.]32, 149[.]102[.]240[.]80, 143[.]244[.]47[.]79, 178[.]255[.]149[.]166, 188[.]241[.]176[.]195, 69[.]4[.]234[.]125, 138[.]199[.]21[.]240, 45[.]134[.]79[.]98, 178[.]249[.]209[.]176, 68[.]235[.]44[.]3, 198[.]54[.]133[.]131, 193[.]138[.]7[.]158, 154[.]47[.]30[.]131, 204[.]152[.]216[.]115, 206[.]217[.]205[.]125, 37[.]19[.]200[.]144, 146[.]70[.]171[.]131, 198[.]54[.]130[.]99, 149[.]22[.]81[.]208, 146[.]70[.]197[.]131, 198[.]54[.]131[.]131, 138[.]199[.]15[.]147, 185[.]248[.]85[.]34, 143[.]244[.]47[.]66, 92[.]60[.]40[.]225, 178[.]249[.]214[.]3, 146[.]70[.]133[.]3, 179[.]43[.]189[.]67, 69[.]4[.]234[.]120, 146[.]70[.]199[.]195, 185[.]156[.]46[.]157, 45[.]134[.]142[.]194, 68[.]235[.]44[.]195, 209[.]54[.]101[.]131, 104[.]129[.]41[.]195, 146[.]70[.]225[.]3, 206[.]217[.]205[.]126, 103[.]136[.]147[.]130, 194[.]110[.]115[.]3, 178[.]249[.]211[.]93, 185[.]188[.]61[.]226, 194[.]110[.]115[.]35, 146[.]70[.]198[.]195, 169[.]150[.]198[.]67, 103[.]108[.]229[.]67, 138[.]199[.]60[.]16, 96[.]44[.]191[.]147, 31[.]170[.]22[.]16,

TYPE	VALUE
IPv4	45[.]134[.]140[.]131, 169[.]150[.]196[.]29, 103[.]216[.]220[.]19, 173[.]205[.]93[.]3, 146[.]70[.]199[.]131, 103[.]214[.]20[.]131, 149[.]88[.]22[.]143, 149[.]40[.]50[.]113, 138[.]199[.]21[.]227, 138[.]199[.]6[.]195, 103[.]216[.]220[.]35, 198[.]44[.]136[.]67, 199[.]116[.]118[.]194, 146[.]70[.]129[.]131, 199[.]116[.]118[.]233, 146[.]70[.]184[.]3, 185[.]254[.]75[.]14, 38[.]240[.]225[.]69, 149[.]22[.]81[.]195, 43[.]225[.]189[.]132, 45[.]134[.]142[.]207, 146[.]70[.]196[.]195, 198[.]44[.]140[.]195, 206[.]217[.]205[.]119, 38[.]240[.]225[.]37, 169[.]150[.]227[.]211, 37[.]19[.]200[.]157, 146[.]70[.]132[.]195, 146[.]70[.]211[.]67, 206[.]217[.]206[.]28, 178[.]249[.]214[.]16, 149[.]88[.]22[.]169, 149[.]88[.]104[.]16, 194[.]36[.]25[.]34, 146[.]70[.]197[.]195, 45[.]134[.]212[.]80, 156[.]59[.]50[.]227, 104[.]223[.]91[.]19, 198[.]54[.]130[.]131, 185[.]248[.]85[.]19, 45[.]134[.]79[.]68, 45[.]134[.]142[.]220, 185[.]204[.]1[.]179, 146[.]70[.]129[.]99, 146[.]70[.]133[.]99, 69[.]4[.]234[.]122, 178[.]249[.]211[.]67, 198[.]54[.]131[.]163,

TYPE	VALUE
IPv4	198[.]44[.]129[.]35, 103[.]108[.]231[.]51, 146[.]70[.]165[.]3, 37[.]19[.]221[.]157, 92[.]60[.]40[.]210, 154[.]47[.]16[.]35, 194[.]127[.]199[.]3, 37[.]19[.]210[.]2, 103[.]108[.]231[.]67, 204[.]152[.]216[.]99, 176[.]123[.]7[.]143, 176[.]123[.]10[.]35, 195[.]160[.]223[.]23

References

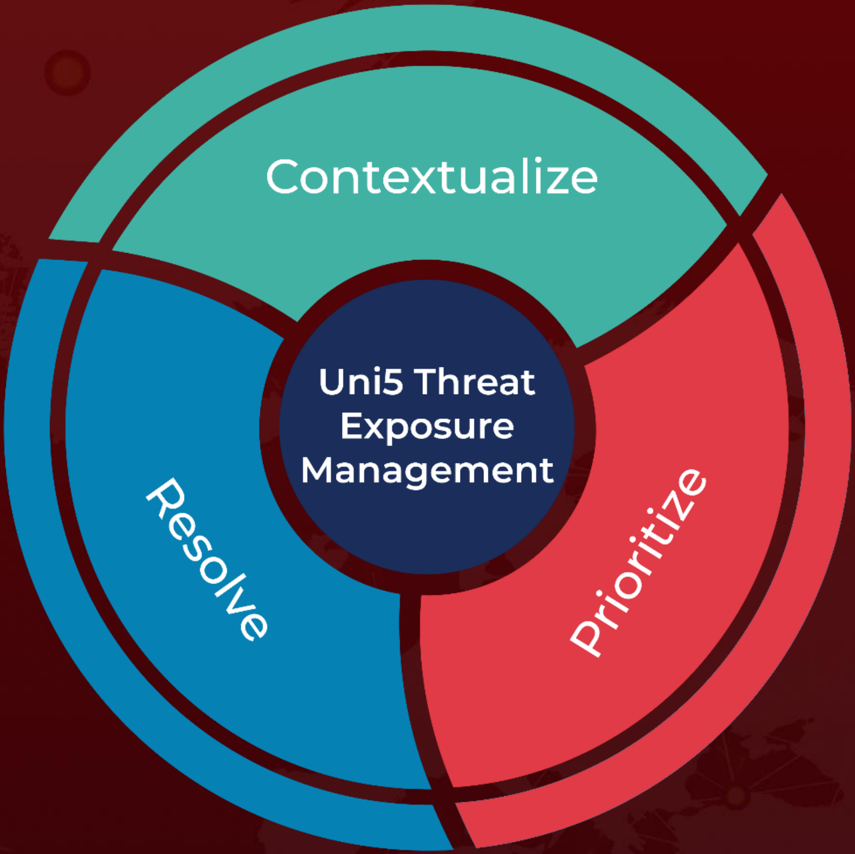
https://www.mitiga.io/blog/tactical-guide-to-threat-hunting-in-snowflake-environments

https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

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

May 31, 2024 • 5:30 AM

More at www.hivepro.com