Hive Pro

Threat Level

Red

CISA: AA23-193A

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

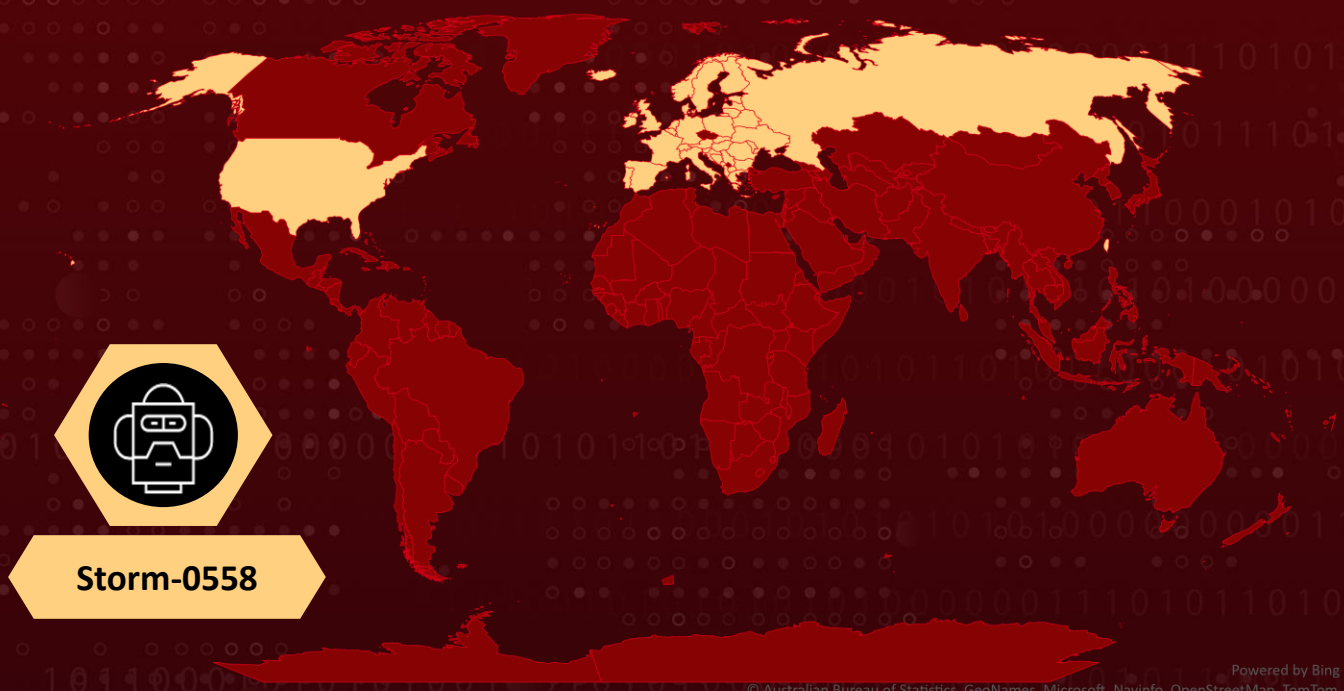
Storm-0558 Chinese Threat Actor Targets Email Accounts

Date of Publication	Admiralty code	TA Number
July 24, 2023	A1	TA2023310

Summary

First Appearance: August 2021
Actor Name: Storm-0558
Target Region: US, Europe, Taiwan, and Uyghur
Target Sectors: Government, Diplomatic entities, Media companies, Think tanks, and Telecommunications
Malware: Cigril

Actor Map



Actor Details

#1

Storm-0558 is a China-based threat actor with espionage objectives. Although some minimal overlaps with other Chinese groups were observed, Storm-0558 is considered to operate as its own distinct entity and has been observed engaging in unauthorized access to email data from approximately 25 organizations, including government agencies and consumer accounts in the public cloud.

#2

Historically, this actor has targeted US and European diplomatic, economic, and legislative governing bodies, as well as individuals connected to Taiwan and Uyghur geopolitical interests. The threat actor displays a keen interest in targeting media companies, think tanks, and telecommunications equipment and service providers.

#3

Storm-0558 frequently employs a widely used malware family 'Cigril'. This malicious software comes in various versions and is activated through dynamic-link library (DLL) search order hijacking.

#4

It employs various techniques to achieve its goals, including credential harvesting, phishing campaigns, and OAuth token attacks. Recently, the actor was found to have acquired an inactive Microsoft account (MSA) consumer signing key, using it to forge authentication tokens to gain access to email data.

#5

Storm-0558 operates with a high degree of technical tradecraft and employs a collection of PowerShell and Python scripts to perform REST API calls against the Outlook Web Access (OWA) Exchange Store service. These scripts allow the actor to download emails, attachments, and conversations, as well as access email folder information. The threat actor's infrastructure includes proxy servers and a web panel with specific SHA-1 hashes for authentication.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Storm-0558	China **MOTIVE** Information theft and espionage	US, Europe, Taiwan, and Uyghur	Government, Diplomatic entities, Media companies, Think tanks, and Telecommunications

Recommendations

Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.

Segregate Administrator and User Accounts: Separate administrator accounts from user accounts as per security best practices. Designate specific administrator accounts solely for administrative purposes to minimize potential exploitation of administrative privileges.

Centralize and Monitor Logs: Collect and store access and security logs from various cloud services, applications, and security solutions. Utilize a telemetry hosting solution, such as a SIEM, to centralize logs and enable continuous monitoring, auditing, alerting, and threat detection activities. Regularly review logs to identify suspicious behavior and potential threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0043 Reconnaissance
TA0010 Exfiltration	TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control
TA0004 Privilege Escalation	TA0006 Credential Access	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1589.001 Credentials	T1134.001 Token Impersonation/Theft	T1134 Access Token Manipulation	T1589 Gather Victim Identity Information
T1059.006 Python	T1505.003 Web Shell	T1505 Server Software Component	T1574.001 DLL Search Order Hijacking
T1574 Hijack Execution Flow	T1003.001 LSASS Memory	T1003 OS Credential Dumping	T1003.002 Security Account Manager

T1078 Valid Accounts	T1102 Web Service	T1567 Exfiltration Over Web Service	T1566 Phishing
T1090 Proxy	T1543.001 Launch Agent	T1543 Create or Modify System Process	T1106 Native API
T1190 Exploit Public-Facing Application			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	51.89.156[.]153, 176.31.90[.]129, 137.74.181[.]100, 193.36.119[.]45, 185.158.248[.]159, 131.153.78[.]188, 37.143.130[.]146, 146.70.157[.]45, 185.195.200[.]39, 185.38.142[.]229, 146.70.121[.]44, 31.42.177[.]181, 185.51.134[.]52, 173.44.226[.]70, 45.14.227[.]233, 185.236.231[.]109, 178.73.220[.]149, 45.14.227[.]212, 91.222.173[.]225, 146.70.35[.]168, 146.70.157[.]213, 31.42.177[.]201, 5.252.176[.]8, 80.85.158[.]215, 193.149.129[.]88, 5.252.178[.]68, 116.202.251[.]8, 185.158.248[.]93,

TYPE	VALUE
IPV4	20.108.240[.]252, 146.70.135[.]182, 195.26.87[.]219, 185.236.228[.]183, 85.239.63[.]160, 193.105.134[.]58, 146.0.74[.]16, 91.231.186[.]226, 91.222.174[.]41, 185.38.142[.]249, 195.26.87[.]219, 185.236.228[.]183, 85.239.63[.]160, 193.105.134[.]58, 146.0.74[.]16, 91.231.186[.]226, 91.222.174[.]41, 185.38.142[.]249, 51.89.156[.]153, 176.31.90[.]129, 137.74.181[.]100, 193.36.119[.]45, 185.158.248[.]159, 131.153.78[.]188, 37.143.130[.]146, 146.70.157[.]45, 185.195.200[.]39, 185.38.142[.]229, 146.70.121[.]44, 31.42.177[.]181, 185.51.134[.]52, 173.44.226[.]70, 45.14.227[.]233, 185.236.231[.]109, 178.73.220[.]149, 45.14.227[.]212, 91.222.173[.]225, 146.70.35[.]168, 146.70.157[.]213, 31.42.177[.]201, 5.252.176[.]8, 80.85.158[.]215, 193.149.129[.]88, 5.252.178[.]68, 116.202.251[.]8

TYPE	VALUE
SHA1	80d315c21fc13365bba5b4d56357136e84ecb2d4 , 931e27b6f1a99edb96860f840eb7ef201f6c68ec

References

https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

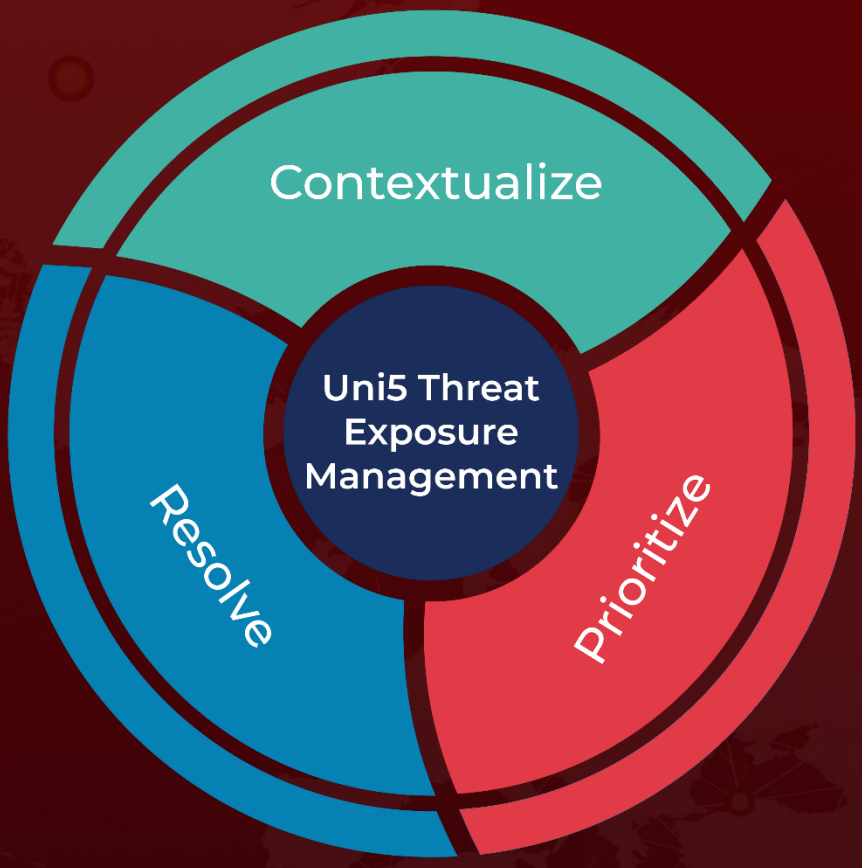
https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-193a

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

July 24, 2023. 5:30 AM

More at www.hivepro.com