Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

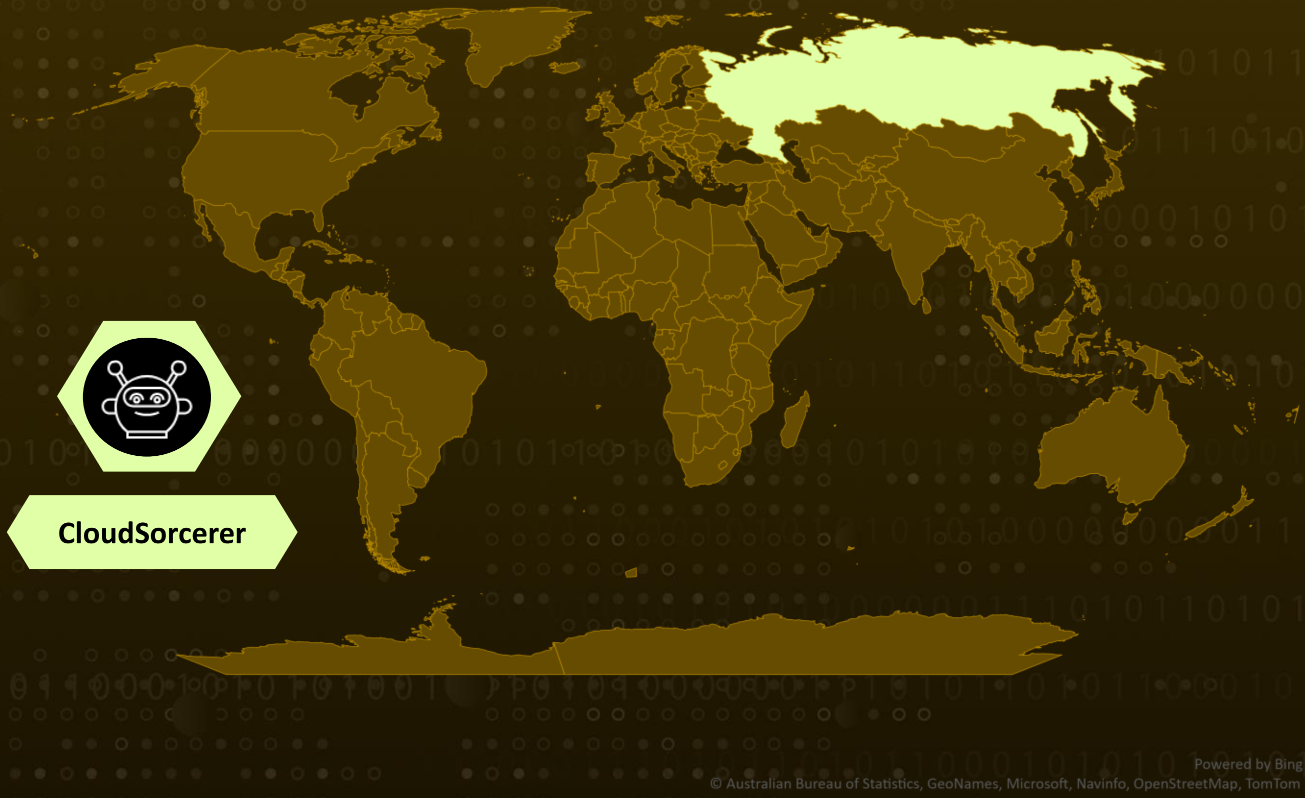
CloudSorcerer APT: A Stealthy Cloud Threat Targeting Russia

Date of Publication	Admiralty Code	TA Number
July 9, 2024	A1	TA2024264

Summary

Attack Began: May 2024
Actor Name: CloudSorcerer
Target Region: Russia
Target Sector: Government

Actor Map


CloudSorcerer
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

#1 CloudSorcerer is a newly discovered advanced persistent threat (APT) group that has been targeting Russian government entities since May 2024. This sophisticated cyberespionage group uses custom malware to leverage public cloud services for command and control (C2) operations and data exfiltration.

#2 The CloudSorcerer malware is a Windows backdoor that exhibits different behaviors depending on the process it is executed in. If executed from the "mspaint.exe" process, it functions as a backdoor, collecting system information and executing arbitrary code. If executed from the "msiexec.exe" process, it initiates C2 communication to receive further commands.

#3 For other processes, the malware attempts to inject shellcode into the "msiexec.exe", "mspaint.exe", or "explorer.exe" processes before terminating the initial process. The shellcode used by CloudSorcerer for process injection performs standard functionality, such as parsing the Process Environment Block (PEB) to identify Windows API offsets and mapping the malware code into the memory of the target processes.

#4 A key innovation of CloudSorcerer is its strategic use of public cloud platforms such as Microsoft Graph, Yandex Cloud, and Dropbox for conducting C2 operations. By leveraging API calls and authentication tokens, the group ensures secure and resilient communication channels, enhancing operational stealth and survivability.

#5 The CloudSorcerer backdoor supports a range of malicious commands, including executing shell commands, copying, moving, renaming, or deleting files, receiving and injecting shellcode into remote processes, mapping PE files into remote processes, creating new processes or services, and adding or removing network users.

#6 While CloudSorcerer shares some operational similarities with previously identified APT groups like CloudWizard, its distinct malware code and operational methodologies suggest it represents a new and evolving threat actor. This group's sophisticated use of cloud infrastructure and intricate malware capabilities highlight the ongoing challenge posed by advanced cyberespionage tactics in today's interconnected digital landscape.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
CloudSorcerer	Unknown	Russia	Government
	MOTIVE		
	Information theft and espionage		

Recommendations

Implement Cloud Access Security Broker (CASB) Solutions: Deploy CASB solutions to monitor and control user access to cloud services, detect anomalies, and prevent unauthorized data exfiltration. CASB tools can help identify and block suspicious cloud service usage patterns associated with CloudSorcerer's C2 infrastructure.

Enhance Cloud Security Posture Management (CSPM): Regularly assess the security configuration of cloud environments and address misconfigurations that could be exploited by threat actors. Ensure that cloud service authentication and authorization mechanisms are properly configured to prevent unauthorized access.

Implement Endpoint Detection and Response (EDR): Deploy EDR solutions on endpoints to detect and respond to advanced threats like CloudSorcerer. EDR tools can help identify and block suspicious process behavior, such as the dynamic malware execution and shellcode injection techniques used by CloudSorcerer.

Enforce Least Privilege Access: Implement the principle of least privilege for user accounts and service accounts in cloud environments. Restrict access to cloud services and resources based on the minimum required permissions to limit the potential impact of a successful compromise.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	**TA0011** Command and Control	**TA0009** Collection	**TA0002** Execution
TA0003 Persistence	**TA0005** Defense Evasion	**TA0010** Exfiltration	**T1059** Command and Scripting Interpreter
T1059.009 Cloud API	**T1559** Inter-Process Communication	**T1053** Scheduled Task/Job	**T1047** Windows Management Instrumentation
T1543 Create or Modify System Process	**T1140** Deobfuscate/Decode Files or Information	**T1112** Modify Registry	**T1083** File and Directory Discovery
T1046 Network Service Discovery	**T1057** Process Discovery	**T1012** Query Registry	**T1082** System Information Discovery
T1005 Data from Local System	**T1102** Web Service	**T1568** Dynamic Resolution	**T1567** Exfiltration Over Web Service
T1537 Transfer Data to Cloud Account			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://github[.]com/alinaegorovaMygit, hxxps://my.mail[.]ru/yandex.ru/alinaegorova2154/photo/1
MD5	F701fc79578a12513c369d4e36c57224
SHA1	f1a93d185d7cd060e63d16c50e51f4921dd43723
SHA256	e4b2d8890f0e7259ee29c7ac98a3e9a5ae71327aaac658f84072770cf8ef02de

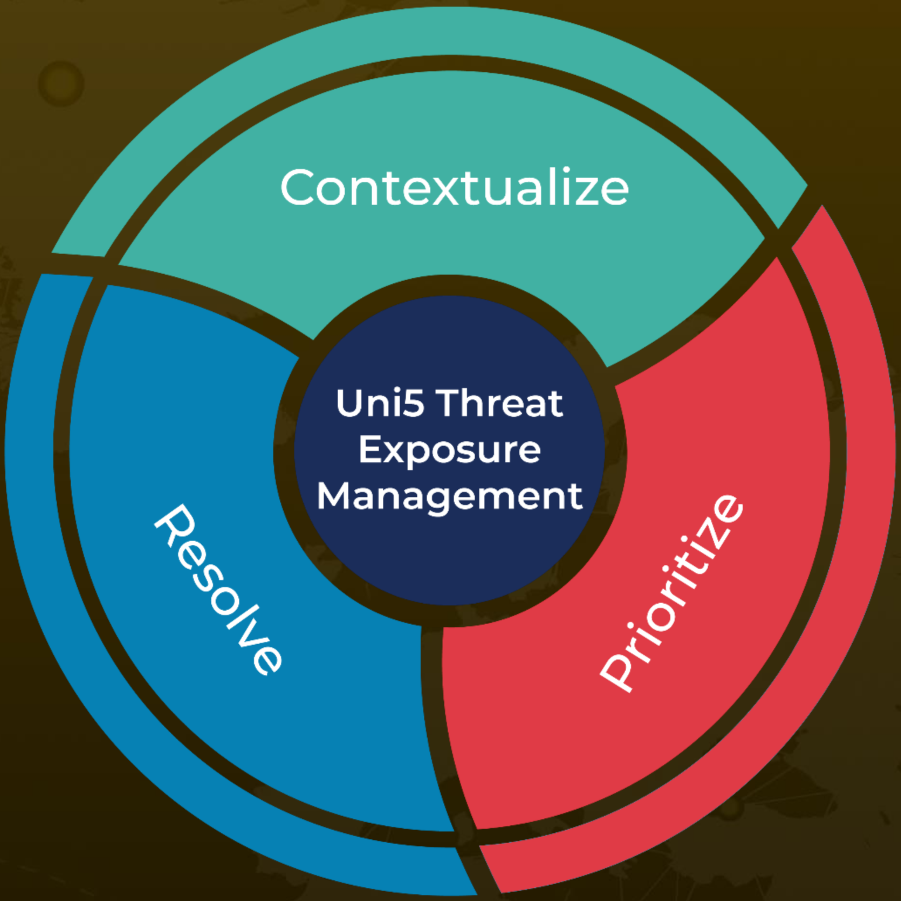
References

https://securelist.com/cloudsorcerer-new-apt-cloud-actor/113056/

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 9, 2024 • 6:00 AM

More at www.hivepro.com