Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

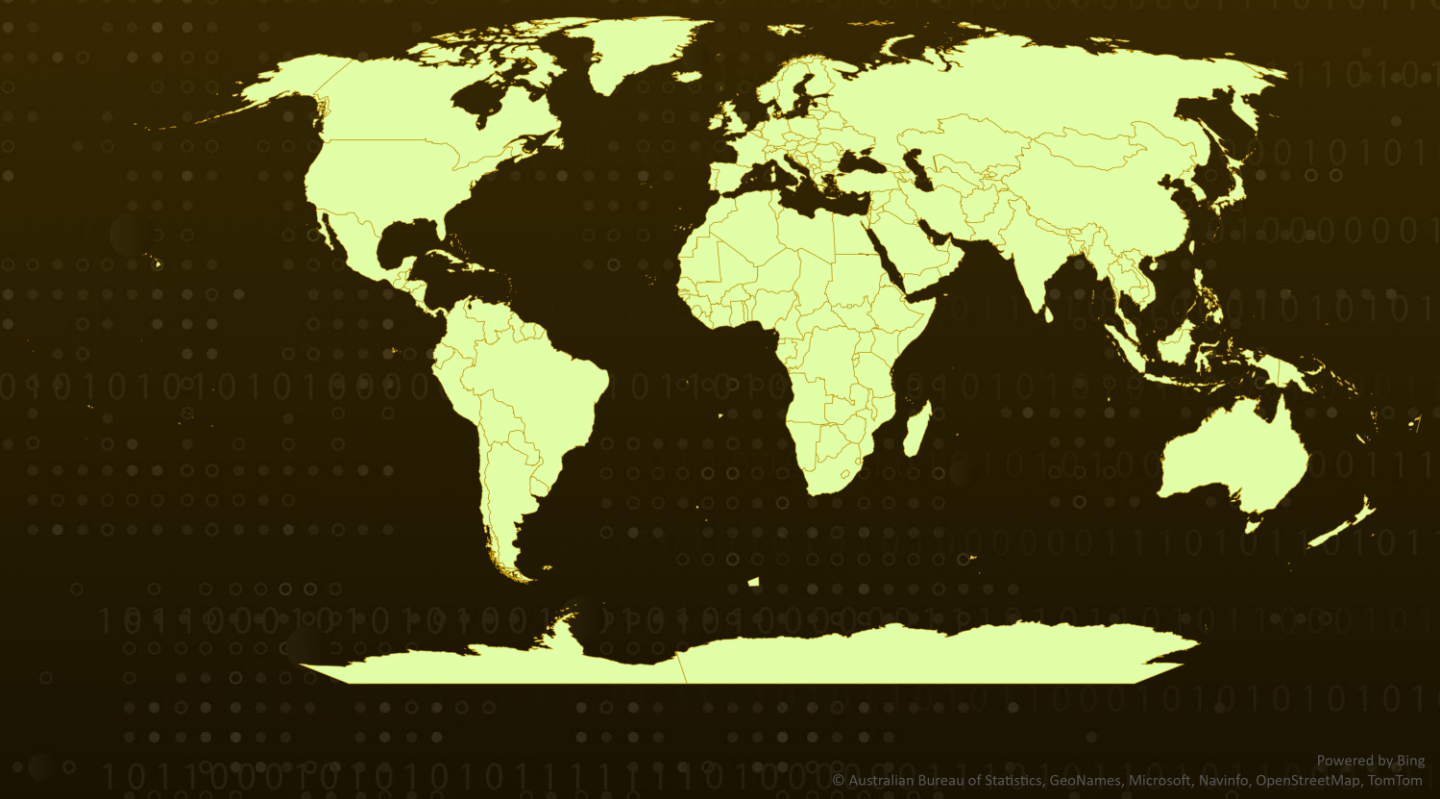
CLOUD#REVERSER: From Cloud Storage to Command and Control

Date of Publication	Admiralty Code	TA Number
May 22, 2024	A1	TA2024200

Summary

Campaign: CLOUD#REVERSER
Attack Region: Worldwide
Attack: CLOUD#REVERSER is a campaign that leverages popular cloud storage services such as Google Drive and Dropbox to conduct malicious operations by threat actors. This strategy exemplifies a recurring tactic in which threat actors successfully infiltrate and maintain a foothold on compromised systems.

Attack Regions



Attack Details

#1 A new, sophisticated campaign known as CLOUD#REVERSER exploits popular cloud storage services like Google Drive and Dropbox to facilitate malicious operations by threat actors.

#2 The attack begins when a user receives a phishing email containing a zip archive as an attachment. This archive includes an executable file disguised as a Microsoft Excel document. The filename employs the hidden right-to-left override (LTRO) Unicode character to reverse the order of the subsequent characters in the string, enhancing the deception.

#3 This executable is programmed to deploy eight payloads, one of which is a decoy Excel file. The threat actors succeed in infiltrating and persisting on compromised systems, camouflaging their activities within normal network traffic.

#4 The VBScript and PowerShell scripts utilized in the CLOUD#REVERSER campaign conduct command-and-control operations, leveraging Google Drive and Dropbox as platforms for managing file uploads and downloads.

#5 By embedding malicious scripts within ostensibly benign cloud platforms, the malware not only secures prolonged access to the targeted environments but also employs these platforms as channels for data exfiltration and command execution.

Recommendations

Beware of Double Extensions and Modified Icons: Users should be wary of files with double extensions, as they could be hiding malicious executables. Additionally, modified icons that resemble legitimate files, like Microsoft Excel, should be viewed with suspicion.

Monitor File Downloads and Script Activity: Implement monitoring systems to track file downloads, especially from external sources, and monitor script-related activities in commonly targeted directories, such as the "C:\ProgramData" directory.

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Enhance Endpoint Logging: Deploy robust endpoint logging capabilities, including additional process-level logging such as System Monitor (Sysmon) and PowerShell logging. This allows for better detection and analysis of malicious activities, particularly those involving encrypted channels through Dropbox and Google servers.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
TA0040 Impact	**T1560** Archive Collected Data	**T1539** Steal Web Session Cookie	**T1555** Credentials from Password Stores
T1555.003 Credentials from Web Browsers	**T1027** Obfuscated Files or Information	**T1027.010** Command Obfuscation	**T1070** Indicator Removal
T1070.004 File Deletion	**T1082** System Information Discovery	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1059.006 Python	**T1041** Exfiltration Over C2 Channel	**T1547.001** Registry Run Keys / Startup Folder	**T1547** Boot or Logon Autostart Execution
T1059 Command and Scripting Interpreter			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	91bd0f7e5af15248c1e3f2908891bbd9262753910fe4bbd61729f0c184287153, b89d6be0bcfb915492beb7ae726f815dcf289a284e650c200bda4faf5db60fa1, 4c37f3db024afd425301666e318c03e34f8813d21d90d95efb4018b3196d07b8, 5f0642383ca70a3fd2c4491b2826002763e90ca25a7413869fd824e7745d0465, 59c49f31b5f389c1c0109b0e603e2679c4f63c3f5c64432e820a50f50b80124f, 51d758fc04d05b997c651f658cdd30819ef5cf795d4498fad919e75a320e72ea, 4cb1e5ca257c709154b38704c34f4f0ade5305263fb21e6142c90c10a5764d52, 09fee43f923faaa30857a09c74d96fca9354653835165a01b274cad4c24460c7, 590353941bab80f38d77b2139bc7da6888b3dff9c8817c4b7e058f50173288bf, 9b9a3da9c602bf70a60cdb9b2bca6f4472222e8431b6b5ecf82b010fe274bba3, f96631cdffa6ae69e5432c38778f3b93e5335a935f62939cd0094e5ccb886460, 8955585100f75c59472e4c2c77fcddd7422400f745ae75132c81c6144aa86824, 7bb7ca87149b6407e1e7c11c1a528a2e2147d3096337e3da6f6be130f76ff6ac, beaa71057ad064e96fc9f8227a7c2a3b8d70d13e45d5908f25c066d937d5bd9d, f4275b0d3c4b6f3a165984b862f4890df14cc346013a22412f7288c9fdc65690
IPv4	159[.]100[.]13[.]216
File Names	KZAH.exe, RFQ-101432620247flxslx.exe, 4.exe, 20240416.xlsx, 3156.vbs, i4703.vbs, i6050.vbs, 68904.tmp, 97468.tmp,

TYPE	VALUE
File Names	Tmp703.tmp, Tmp912.tmp, tmpdbx.ps1, zz.ps1

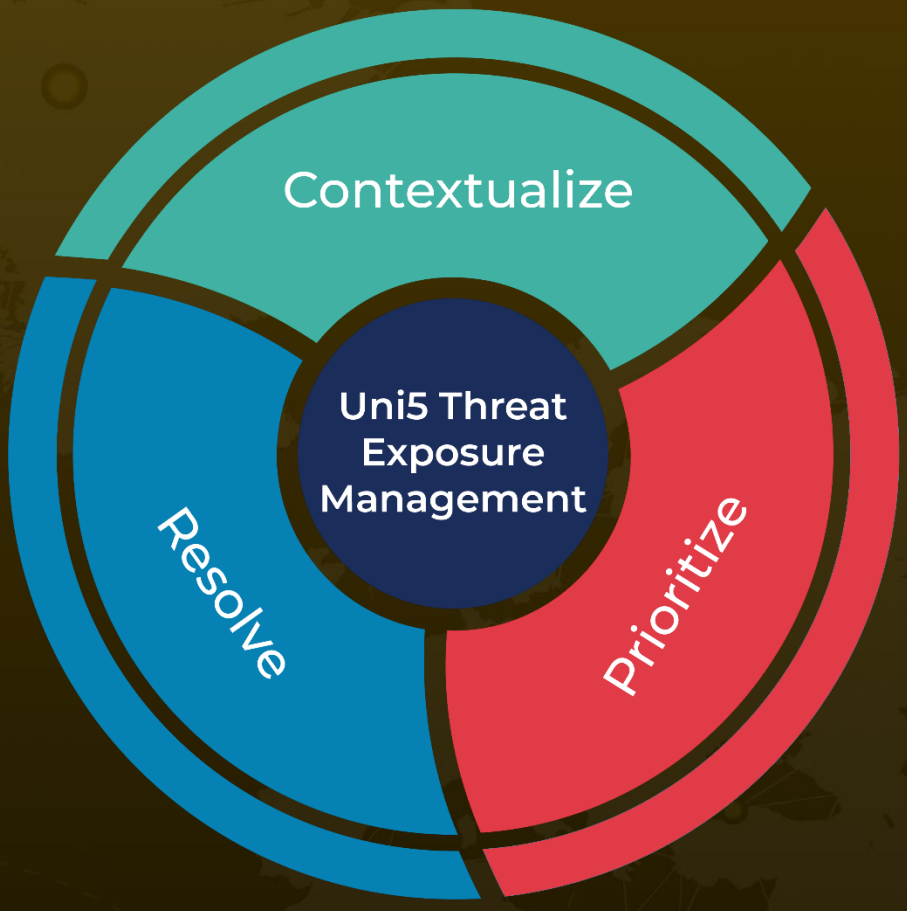
References

https://www.securonix.com/blog/analysis-and-detection-of-cloudreverser-an-attack-involving-threat-actors-compromising-systems-using-a-sophisticated-cloud-based-malware

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 22, 2024 • 6:00 AM

More at www.hivepro.com