Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

CoralRaider’s Malware Campaign Distributing Stealers Via CDN Cache

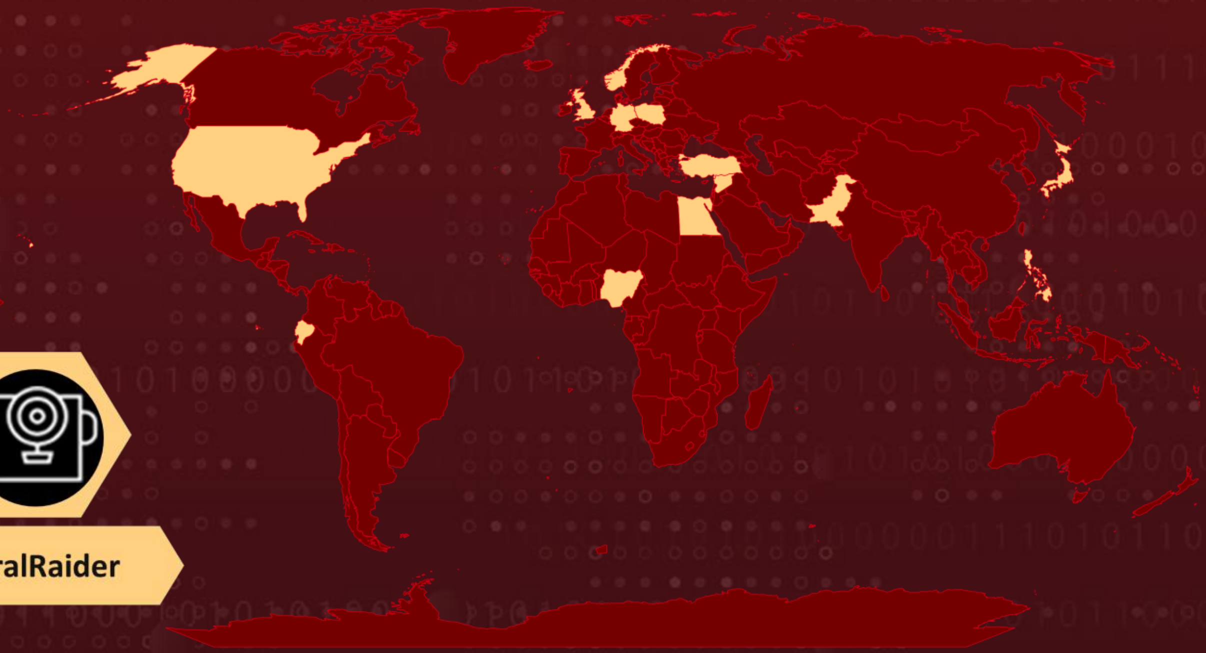
Date of Publication	Admiralty Code	TA Number
April 24, 2024	A1	TA2024161

Summary

Attack Began: February 2024
Attack Region: U.S., Nigeria, Pakistan, Ecuador, Germany, Egypt, the U.K., Poland, the Philippines, Norway, Japan, Syria and Turkey
Affected Industries: Computer service call center organizations and civil defense service organizations
Malware: Cryptbot, LummaC2 and Rhadamanthys
Actor: CoralRaider
Attack: A persistent malware campaign has been distributing three distinct stealers—CryptBot, LummaC2, and Rhadamanthys. This campaign utilizes Content Delivery Network (CDN) cache sites to host its malicious payload. CoralRaider, a financially motivated threat actor known for targeting social network accounts and credentials, is believed to be behind this campaign.

Attack Regions

CoralRaider



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

Attack Details

#1 An ongoing campaign involves a threat actor storing information-stealing malware in a content delivery network cache. This behavior has been attributed to a threat actor known as CoralRaider with a moderate degree of confidence. The hackers distribute information stealers such as LummaC2, Rhadamanthys, and Cryptbot.

#2 The infection chain begins when a victim opens a malicious shortcut file from a ZIP file, likely delivered via phishing emails. This Windows shortcut file contains an embedded PowerShell command that runs a malicious HTA file hosted on attacker-controlled CDN domains. The HTA file then executes an embedded JavaScript, which decodes and executes a PowerShell decrypter script. The PowerShell Loader script employs various techniques to evade detections and bypass UAC, ultimately downloading and executing payloads such as Cryptbot, LummaC2, or Rhadamanthys information stealer.

#3 The PowerShell loader script is a versatile tool that carries out multiple activities on a victim's machine. It drops a batch script into the victim's temporary folder, containing a PowerShell command to add the "ProgramData" folder to the Windows Defender exclusion list. This script is executed using a Living off the Land Binary (LoLBin) and a Programmatic Identifiers registry key, enabling it to bypass the victim's UAC.

#4 After downloading the payload onto the victim's machine, the PowerShell loader executes a function. It then updates the previously dropped batch file with new instructions. These instructions are designed to run the downloaded payload information stealer using the Windows "start" command. This ensures that the information stealer is executed and begins its malicious activities on the victim's system.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0010 Exfiltration	TA0011 Command and Control
T1218 System Binary Proxy Execution	T1218.005 Mshta	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1059.006 Python	T1059.007 JavaScript	T1204 User Execution	T1204.002 Malicious File
T1104 Multi-Stage Channels	T1566 Phishing	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link
T1112 Modify Registry	T1083 File and Directory Discovery	T1140 Deobfuscate/Decode Files or Information	T1041 Exfiltration Over C2 Channel
T1055 Process Injection	T1036 Masquerading	T1027 Obfuscated Files or Information	T1608 Stage Capabilities
T1608.001 Upload Malware	T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control	T1555 Credentials from Password Stores
T1217 Browser Information Discovery	T1105 Ingress Tool Transfer		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	150dd450f343c7b1e3b2715eae3ed470c1c1fadf91f2048516315f1500a58ffa, 74ea6e91c00baad0b77575740eb7f0fb5ad1d05ddea8227dc1aa477e179e62df, 3ae459746637e6f5536f3ba4158c822031578335505a512df3c31728cac8f627, 88528be553f2a6f72e2ae0243ea907d5dcdcd7c8777831b4c3ab2a67128bc9b9, fd53383d85b39e68d817e39030aa2184764ab4de2d478b7e33afc39dd9661e96, e68c9aedfd080fe8e54b005482fcedb16f97caa6f7dcfb932c83b29597c6d957, 8c732ec41550851cc933e635708820ec9202fddc69232ca4ed625d420aec3d86, 1942c417f2b71068fb4c1abb31bc77426bbe3513334cdaceaff3603955830e21, 5ad73cf7e08b8c7bab0d96ba92607b8c9b22b61354052cf59df93b782b6e039b, a1f16ab97b9516e85c202ff00bd77b0b5e0e4ed29bfad28797fbbd0f25a8e0ae, 963ffc17565079705c924b8ab86d1c7018f5edc50ce8e810df3eebead4e14e7f, 3b54d05ec98321980c1d71b89c42ff77a42f121e37f6ea54a6368a58ce1b1ad3, 934dc78ab89dd466b1a140954c6528b6a8591ca09a023616405cf71faf69f010, 305bf697e89e6eef59b0beef2b273a1daad174ebec238a67a6e80c5df5fffaf8, 31b4fd83c16bf7266c82a623998b0d7b54bb084b24a5cb71a2b5e9b17bb633dc, 5dc77655bddf8881b533e4db732dcf7ac5ebf3adad4be77ff226909a49bfc89b, 2ad94e492bc18e11f513a29968054e1a37df504ac577fd645e781e654f2730c9, 02e03904d09ccece4f71e34a4a6d0f1181471c4d17208ee6cfe940e11e185018, eef156d681c4921cbed720e6de257a69ad6a187e814037257977958eb0c7604e, 6089c53ef2b0100fd91554c2a56aafaeea86b08c5ad0459fd66bd05a6602a3ee, 7db78346dde71258ae1307b542d162a030c71031eebd0ed80816112d82c008f0,

TYPE	VALUE
SHA256	7f19557ee3024c59668e5bd1c96a8124b0a201a9fd656bd072332b400c413405, b6dbee1b6e444216668c44e41a84ca91cbd966e9035621423ecc12db52a36e01, b3e694ce12e6f67db5db56177abfddebbc29f558618987e014f47a46996a8ced, 1397268735c5c6e88d8bc717ac27f8810225b554ed2f0d76a3e0048b0933af18, 958508a626b94d5e2e00ab0b94cb75dca58091cce708d312ee1a1c0688ef067c, 51c1eccc1b95ecbeaebc4853606c02808fce208ff1f76f0c7aa11ad7fbb4b763, 3c075a2bcd06e103e6ec3a1b74ceaaf600d3a9e179e2719795377f71c4f8f9c8, 3ac52be2039a73df64e36672f3f0c748de10f6a8bed4b23642dd8da256137681, aea7c613ac659a083c35afd8e20f19a2c3583f81597dec48cbc886292cfcc975, a04c6804b63220a9cb1ea6c5f2990e6a810d7b4b7225e0fc5aa7ed7e2bac3c99, 7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8, a28152ed5039484e858d3c7d4bac03c6ad66fbaffb0e8ea3dfa8def95e115181, b796cc4a54ee27601c1ed3a0016caa6f58206f4f280391f67820b8b019602add, 5cb65b469023dcc77ede21c66a753fa9cbe67597aae142958fce4936ce3974aa
IPv4	185[.]23[.]108[.]220
URL	kzeight8ht[.]top/upload[.]php, kbeight8sb[.]top/upload[.]php, kbeight8vs[.]top/upload[.]php, kbeight8ht[.]top/upload[.]php, kbeight8pn[.]top/upload[.]php, dbeight8pt[.]top/zip[.]php, kveight8sb[.]top/zip[.]php, peasanthovecapspll[.]shop/api, claimconcessionrebe[.]shop/api, culturesketchfinanciall[.]shop/api, gemcreedarticulateod[.]shop/api, liabilityarrangemenyit[.]shop/api, modestessayevenmilwek[.]shop/api, secretionsuitcasenioise[.]shop/api, sofahuntingslidedine[.]shop/api,

TYPE	VALUE
URL	triangleseasonbenchwj[.]shop/api, techsheck.b-cdn[.]net/Zen90, zexodown-2.b-cdn[.]net/Peta12, denv-2.b-cdn[.]net/FebL5, metrodown-2.b-cdn[.]net/MebL1, metrodown-2.b-cdn[.]net/SAq2, denv-2.b-cdn[.]net/FebL4, download-main5.b-cdn[.]net/BSR_v7IDcc, metrodown-3.b-cdn[.]net/MebL1, dashdisk-2.b-cdn[.]net/XFeb18

References

https://blog.talosintelligence.com/suspected-coralraider-continues-to-expand-victimology-using-three-information-stealers/

https://www.hivepro.com/threat-advisory/coralraider-targeting-social-media-accounts-across-asia-for-financial-gain/

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.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

April 24, 2024 • 7:30 AM

More at www.hivepro.com