Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

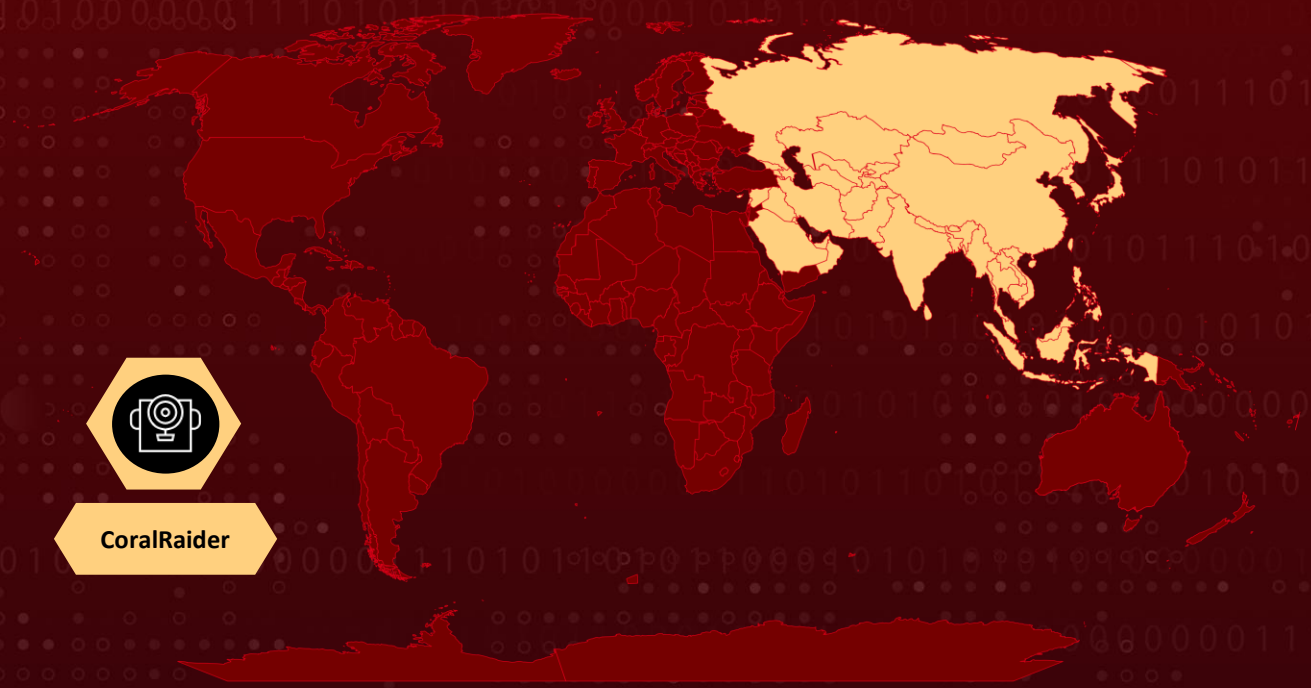
CoralRaider Targeting Social Media Accounts Across Asia for Financial Gain

Date of Publication	Admiralty code	TA Number
April 5, 2023	A1	TA2024131

Summary

First Appearance: 2023
Actor Name: CoralRaider
Target Region: Asia
Target: Social media accounts (personal and business), financial information, credentials
Affected Platform: Windows
Malware: RotBot, XClient stealer

Actor Map



Actor Details

#1 A new threat actor named "CoralRaider," believed to originate from Vietnam and driven by financial motives. Operating since at least 2023, CoralRaider targets victims primarily in Asian countries, focusing on stealing credentials, financial data, and social media accounts, including business and advertisement accounts.

#2 The actor employs various payloads, including RotBot (a customized QuasarRAT variant) and XClient stealer. They utilize the dead drop technique, utilizing legitimate services to host C2 configuration files and uncommon Living-off-the-Land Binaries (LoLBins).

#3 Analysis of CoralRaider's desktop images revealed clues such as device IDs and IP addresses linked to Vietnam. Furthermore, examination of their OneDrive folders and PDB strings indicated a Vietnamese origin, strengthening this assessment.

#4 The campaign involves distributing malicious Windows shortcut files targeting victims in multiple Asian countries. Upon execution, these files download and execute an HTA file, initiating a series of PowerShell scripts leading to the deployment of RotBot and subsequently XClient stealer.

#5 RotBot, disguised as a Printer Subsystem application, conducts evasion checks and reconnaissance on victim machines. It configures internet proxies and creates mutex markers.

#6 XClient stealer, a .Net executable, evades detection and steals a wide array of victim data, including social media credentials, browser information, and financial details. It also targets platforms like Facebook, Instagram, YouTube, TikTok, Telegram, and Discord. The XClient stealer exfiltrates stolen data to the actor's Telegram C2 channel.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
CoralRaider	Vietnam **MOTIVE** Financial gain	Asia	-

Recommendations

Email Filtering and Security: Implement robust email filtering solutions capable of detecting and blocking phishing emails before they reach users' inboxes. Utilize advanced threat protection features to identify malicious attachments, URLs, and spoofed sender addresses commonly used by CoralRaider.

Multi-Factor Authentication (MFA): Enforce MFA across all corporate accounts, especially for critical systems and applications like Office 365. MFA can significantly reduce the risk of unauthorized access, even if credentials are compromised through phishing attacks.

Domain Monitoring and Defense: Regularly monitor domain registrations for any suspicious activity or unauthorized variations of legitimate domains. Consider implementing domain-based message authentication, reporting, and conformance (DMARC) policies to prevent email spoofing and domain impersonation.

Endpoint Protection: Deploy endpoint protection solutions that include anti-malware, firewall, and intrusion detection/prevention capabilities. These solutions can help detect and block malicious activities on endpoints, including the execution of malware like RotBot and XClient stealer.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1566 Phishing	T1204 User Execution	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1036 Masquerading	T1564 Hide Artifacts	T1555 Credentials from Password Stores	T1539 Steal Web Session Cookie
T1083 File and Directory Discovery	T1518 Software Discovery	T1113 Screen Capture	T1005 Data from Local System
T1071 Application Layer Protocol	T1090 Proxy	T1041 Exfiltration Over C2 Channel	T1137 Office Application Startup

Indicator of Compromise (IOCs)

TYPE	VALUE
IPv4	51[.]79[.]208[.]192, 199[.]34[.]27[.]196, 139[.]99[.]23[.]9, 14[.]225[.]210[.]98, 14[.]225[.]210[.]97, 14[.]225[.]210[.]209, 14[.]225[.]210[.]222
Domains	doc-0s-44-docstext[.]googleusercontent[.]com, doc-10-44-docstext[.]googleusercontent[.]com

TYPE	VALUE
SHA256	c29732d898dcf116f40eea3845d4e25a240e5840378985c7f192e0443a51a228, 2c4ed97859060ea6ac5a8c2f605debf98257a96f0f3d2ddfaeb066f59a86d4af, 075091793768885977c29a41a0ac591340ebafab26d2a65ce1dccb53997485a1, b2fd046022231171941 81c97ca8692a09f6f5cfdbc07c87560aaab821cd29536, 77acb85a28e79dc6479798c024282ddd54977dbff6ce40eb439b2a06ce9cb542, c84ff4fb6549c36ca0028e84ea8292ee3ae438254cddd63ef3d9ea769e0a1dfd, e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f, 0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0, 28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f, d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e, de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4, 020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34, 1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3, 93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1c, 4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643, 9bf684b010e4ec314d697acfac78c71ec24ba5f6e2c09b3be623ec62056aed02, 42654394f29f2e8db878fc4fd1c59e41afcd0add3b93f7d2f47ea3295b2bc643, 8d200892e4f1e68373e58e7cd7119fe26769fcf609636adc727df09f2377d1c2, a3299ecee7b3f06ca106f4c5b62bf1e0f28f227df71488583d2077c7e3ee01c2, 19055fb87b9a98a75544a533ec4f14f36a09a130219b8a33a13cb6073751ff39

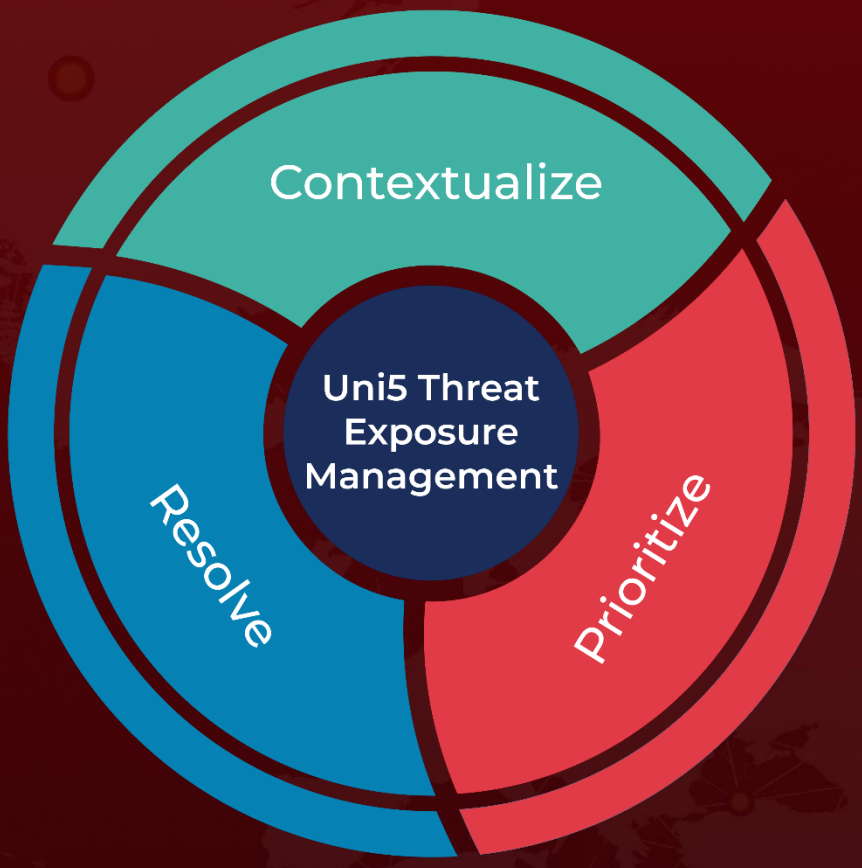
References

https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/

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

April 5, 2023 • 4:30 AM

More at www.hivepro.com