Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

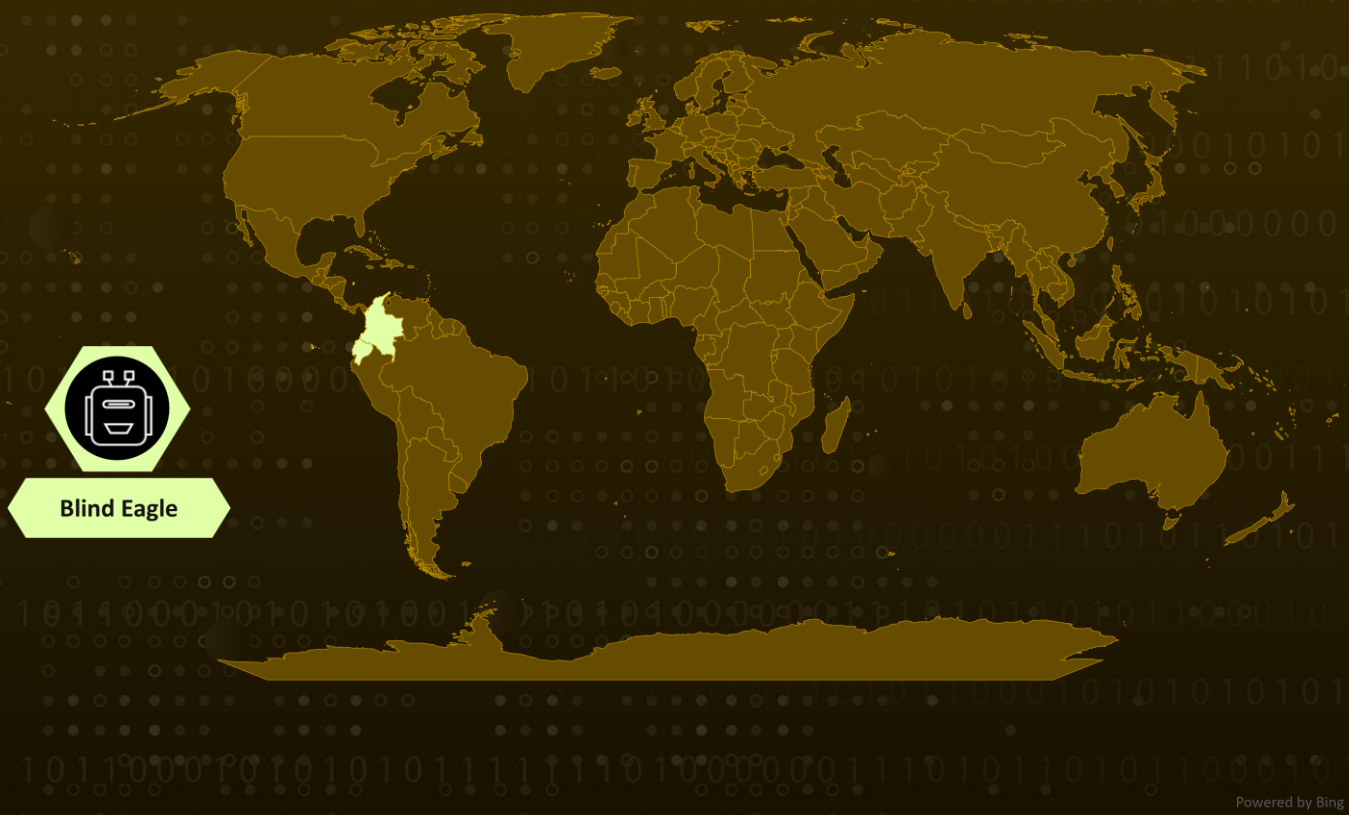
Blind Eagle's BlotchyQuasar Malware Rattles Colombian Insurance Sector

Date of Publication	Admiralty Code	TA Number
September 9, 2024	A1	TA2024345

Summary

Attack Began: June 2024
Threat Actor: Blind Eagle (aka AguilaCiega, APT-C-36, APT-Q-98)
Malware: BlotchyQuasar RAT
Targeted Region: Colombia, Ecuador
Targeted Industry: Insurance, Banking Services, Financial
Attack: Blind Eagle is a notorious cyber espionage group that targets Latin American organizations, particularly Colombia. The group is known for spear-phishing attacks, often impersonating government agencies like the Colombian National Tax and Customs Authority (DIAN) to trick victims into downloading BlotchyQuasar malware, a variant of QuasarRAT.

Attack Regions



Attack Details

#1 Blind Eagle, also known as APT-C-36, is a highly sophisticated threat actor group, notorious for targeting organizations across Latin America, especially in Colombia. Their primary attack vector involves spear-phishing campaigns, often masquerading as local government bodies, such as the Colombian National Tax and Customs Authority (DIAN). These phishing attempts typically create a sense of urgency by citing tax-related issues, prompting victims to download malicious files.

#2 In June 2024, Blind Eagle launched a campaign targeting the Colombian insurance sector with BlotchyQuasar malware, a variant of QuasarRAT. The attack begins with phishing emails containing either a PDF attachment or a link to a password-protected ZIP file hosted in a Google Drive folder. This folder belongs to a compromised account from a regional government organization in Colombia.

#3 The ZIP file carries the BlotchyQuasar malware, which is layered within multiple .NET executables designed to bypass detection using advanced obfuscation techniques. BlotchyQuasar enables keylogging, browser data theft, and surveillance of financial transactions, focusing on Colombian and Ecuadorian banking institutions. It communicates with command-and-control (C2) servers through dynamic DNS domains, often retrieving the C2 server location from encrypted data hosted on Pastebin.

#4 BlotchyQuasar's primary objective is to exfiltrate sensitive data by logging keystrokes and monitoring interactions with banking and financial platforms. Additionally, it can harvest credentials from various web browsers and FTP clients. The infrastructure supporting this campaign leverages compromised government accounts and VPNs, with C2 servers masked behind dynamic DNS domains. This ongoing operation represents a significant threat to organizations in Colombia, particularly those in the financial sector.

Recommendations

Implement Advanced Email Filtering: Use email filtering systems that block or flag suspicious attachments and links, especially from unknown senders. Advanced Threat Protection (ATP) solutions should be in place to detect spear-phishing attempts.

Network Segmentation: Segregate critical systems, such as financial and payment platforms, from the general network to limit lateral movement if a breach occurs.

Monitor VPN Traffic: Since the campaign uses VPNs and compromised government accounts, closely monitor VPN traffic for unusual behavior, especially from high-risk regions.

DNS Filtering and Blocking: Blind Eagle's C2 communication uses dynamic DNS domains. Employ DNS filtering tools to block known malicious domains and dynamically analyze DNS queries for signs of malware.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1056.002 GUI Input Capture	T1095 Non-Application Layer Protocol
T1583 Acquire Infrastructure	T1583.001 Domains	T1586 Compromise Accounts	T1586.002 Email Accounts
T1587 Develop Capabilities	T1587.001 Malware	T1608 Stage Capabilities	T1608.001 Upload Malware
T1566 Phishing	T1566.002 Spearphishing Link	T1204 User Execution	T1204.002 Malicious File
T1204.001 Malicious Link	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1053.005 Scheduled Task

T1562.001 Disable or Modify Tools	T1564.001 Hidden Files and Directories	T1027 Obfuscated Files or Information	T1027.003 Steganography
T1027.009 Embedded Payloads	T1027.013 Encrypted/Encoded File	T1553.005 Mark-of-the-Web Bypass	T1027.002 Software Packing
T1140 Deobfuscate/Decode Files or Information	T1056.001 Keylogging	T1056 Input Capture	T1539 Steal Web Session Cookie
T1041 Exfiltration Over C2 Channel	T1490 Inhibit System Recovery	T1036 Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	69[.]167[.]8[.]118
MD5	b83f6c57aa04dab955fadcef6e1f4139
SHA1	a68cac786b47575a0d747282ace9a4c75e73504d
SHA256	ec2dd6753e42f0e0b173a98f074aa41d2640390c163ae77999eb6c10ff7e2ebd
URL	hxxps[:]//pastebin[.]com/raw/XAfmb6xp
Domains	edificiobaldeares[.]linkpc[.]net, equipo[.]linkpc[.]net, perfect5[.]publicvm[.]com, perfect8.publicvm[.]com

References

https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar

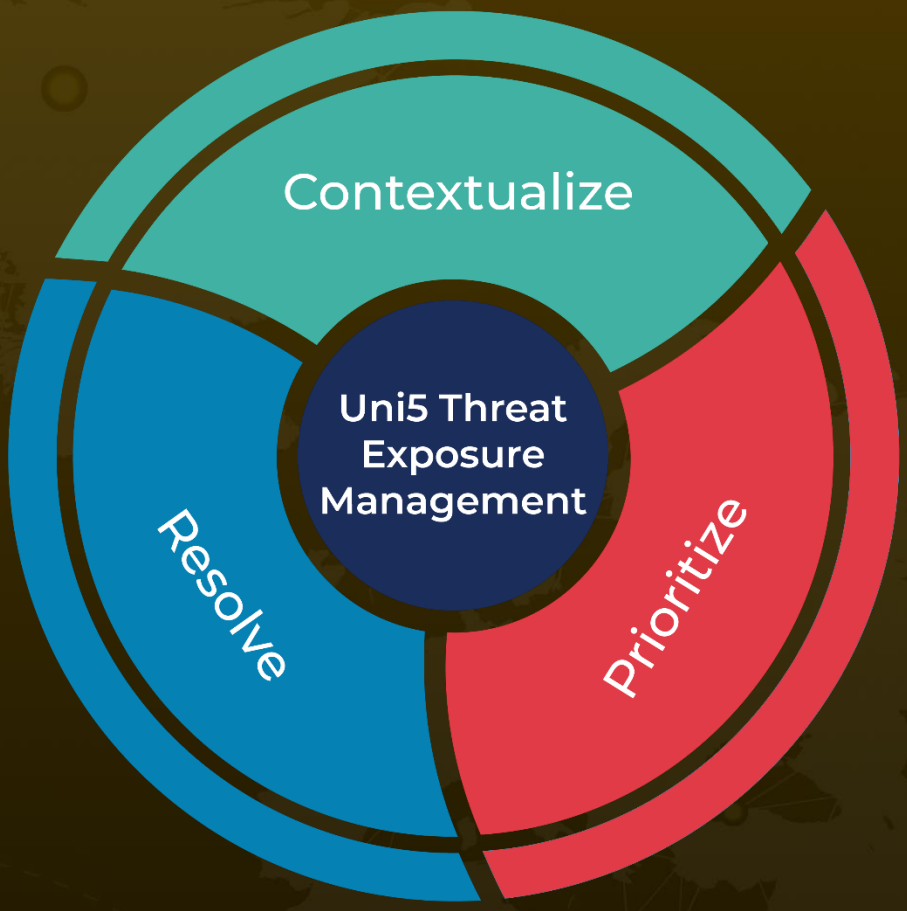
https://hivepro.com/threat-advisory/blind-eagle-hackers-resurfaced-with-a-formidable-infection-chain/

https://hivepro.com/threat-advisory/quasar-rat-utilizes-dll-side-loading-to-evade-detection/

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

September 9, 2024 • 5:30 AM

More at www.hivepro.com