Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

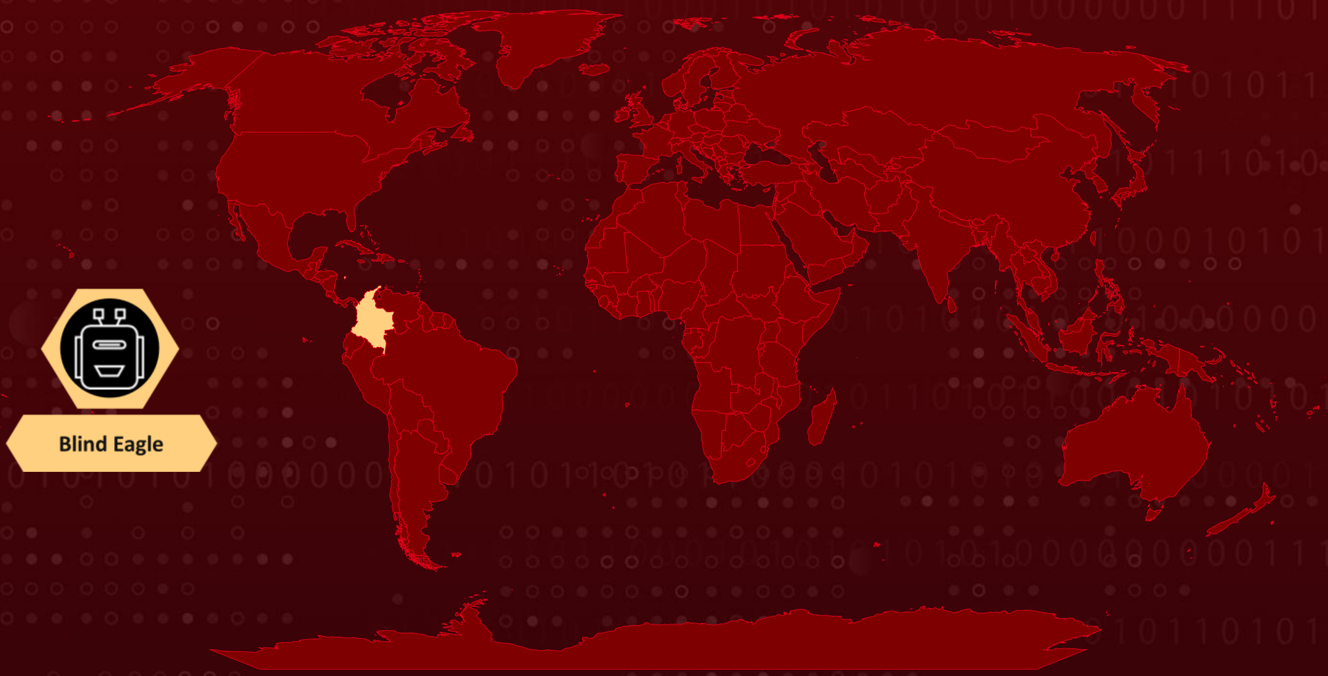
Blind Eagle’s Cyber Reign: Striking Before You Can Blink

Date of Publication	Admiralty Code	TA Number
March 12, 2025	A1	TA2025075

Summary

Attack Commenced: November 2024
Threat Actor: Blind Eagle (aka APT-C-36, AguilaCiega, APT-Q-98)
Malware: PureCrypter RAT, Remcos RAT
Targeted Country: Colombia
Targeted Industries: Government, Judicial Institutions, Private Organizations, Financial, Critical Infrastructure
Affected Product: Microsoft Windows
Attack: Blind Eagle, a cunning cybercriminal group, is making waves with its latest attack spree, slipping past defenses using a newly patched Windows flaw (CVE-2024-43451). With over 1,600 victims already caught in its web, the group isn't just exploiting vulnerabilities. It is also studying security fixes and striking before defenses are in place. Blind Eagle proves that cyber threats are evolving faster than ever, leaving organizations scrambling to keep up.

Attack Regions



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

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1 Blind Eagle, also known as APT-C-36, is a cyber threat group operating at the intersection of espionage and cybercrime. Since November 2024, the group has orchestrated a series of sophisticated campaigns targeting Colombian institutions and government entities. One particularly damaging wave struck on December 19, 2024, compromising more than 1,600 victims.

#2 This latest operation stands out for its innovative tactics, including the exploitation of a recently patched Microsoft Windows vulnerability CVE-2024-43451, the use of a nascent packer-as-a-service (PaaS) called HeartCrypt, and the distribution of malware via Bitbucket and GitHub, moving beyond conventional platforms like Google Drive and Dropbox.

#3 Their attack strategy is CVE-2024-43451, a vulnerability that exposes a user's NTLMv2 hash, enabling attackers to authenticate through pass-the-hash or relay attacks. Remarkably, the exploit can be triggered by seemingly harmless actions right-clicking, deleting, or dragging a file.

#4 While Blind Eagle's malicious payload does not directly exploit this flaw, it mimics the vulnerability's behavior by initiating an unusual WebDAV request when the file is interacted with, signaling the attacker that it has been accessed. A second WebDAV request follows once the user clicks the file to retrieve and execute the next-stage payload.

#5 Microsoft disclosed this vulnerability on November 12, 2024, and within just ***six days***, Blind Eagle had weaponized it into a functioning attack chain. Instead of relying solely on custom-built malware, Blind Eagle incorporates widely available underground cybercrime tools, a trend that continues with its latest tactics.

#6 To shield its payloads from detection, the group employs HeartCrypt, a packer-as-a-service that obfuscates malware using a .NET-based Remote Access Trojan (RAT) believed to be a variant of PureCrypter. Ultimately, the infection culminates in the deployment of Remcos RAT, a powerful tool that grants attackers full control over compromised systems.

#7 Blind Eagle's rapid adaptation underscores a troubling shift in the modern cyber landscape. Rather than waiting for undiscovered zero-day vulnerabilities, threat actors are now closely tracking security patches, swiftly repurposing or mimicking exploit behaviors before organizations can fully implement defenses.

Recommendations

Strengthen Patch Management: Apply security updates immediately upon release, especially for critical vulnerabilities like CVE-2024-43451. Monitor patch releases closely and prioritize fixes for vulnerabilities actively exploited in the wild.

Strengthen Authentication and Identity Security: Enforce Multi-Factor Authentication (MFA) to mitigate NTLMv2 hash relay attacks. Disable NTLM authentication wherever possible, replacing it with more secure alternatives like Kerberos. Implement password hashing policies and use strong, unique passwords to reduce the risk of pass-the-hash attacks.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration
T1587 Develop Capabilities	T1587.004 Exploits	T1588 Obtain Capabilities	T1588.001 Malware
T1059 Command and Scripting Interpreter	T1204 User Execution	T1204.002 Malicious File	T1543 Create or Modify System Process
T1546 Event Triggered Execution	T1055 Process Injection	T1070 Indicator Removal	T1027 Obfuscated Files or Information

T1027.002 Software Packing	**T1083** File and Directory Discovery	**T1057** Process Discovery	**T1082** System Information Discovery
T1105 Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1140** Deobfuscate/Decode Files or Information	**T1573** Encrypted Channel
T1550.002 Pass the Hash			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	177[.]255[.]85[.]101, 181[.]131[.]217[.]244, 62[.]60[.]226[.]64
Hostname	amuntgroupfree[.]ip-ddns[.]com, servicioseguroenlineabb[.]com, 17dic[.]ydns[.]eu, 21ene[.]ip-ddns[.]com, comina998[.]ddns-ip[.]net, donato[.]con-ip[.]com, elyeso[.]ip-ddns[.]com, newstaticfreepoint24[.]ddns-ip[.]net, republicadominica2025[.]ip-ddns[.]com, elyeso[.]ip-ddns[.]com[:]30204
URLs	drive[.]usercontent[.]google[.]com/download?id=1CZcgN1kxz9kSNgscR9qgiOAERo-w-rTa&export=download, drive[.]usercontent[.]google[.]com/download?id=1PZ2Ndi-GT-oQHlobFIdDJoSDSXkJvECV&export=download, drive[.]usercontent[.]google[.]com/download?id=1R9MR64hy-dQelTZMPtsrSXLWObFt7mf2&export=download, raw[.]githubusercontent[.]com/Oscarito20222/file/refs/heads/main/redtube[.]exe, 62[.]60[.]226[.]64/file/1374_2790[.]exe, 62[.]60[.]226[.]64/file/3819_5987[.]exe, 62[.]60[.]226[.]64/file/4025_3980[.]exe, 62[.]60[.]226[.]64/file/9451_1380[.]exe
MD5	16010d959e14338201481f8fb25f881c, 6f21738f94daf7b7a839d072852460e8, 7163fe5f3a7bcfdeec9a07137838012a, d630835afafe3493e8d120210d56ce95

TYPE	VALUE
SHA1	07647f0eddf46d19e0864624b22236b2cdf561a1, 08daf84d9c2e9c51f64e076e7611601c29f68e90, 12eacb556eee889a16beb2fe9449748ebb4e33b0, 133bc4304057317b0b93f5ff44f20d153b985b50, 1b6fc5c2150d598472f892a88305545626d977bd, 1d1e007a9d8939bee7a0333522cc4f7480d448cc, 1fcc44d3b20381acce66f5634743917e8f22dae7, 220a606655d64d03762d319c5f5b80038e5bc13c, 29335b62acef53cb7076f81b8fa25e9baf6d9994, 3262538dbe881b34cfd71cedcb27e03688573f0e, 33ddaedc98991435f740f7a5a8a931a8cadd5391, 3bd90557615ef95e4244bdbaa8e0e7fd949cdd3a, 3d3248ad14dce8b6fcf416d56d8de52b07b549e7, 408d7ef19b151668e2445532e06c6b3a569ebf98, 44182ce5a8fadef41064d7c0266e8f99015262b0, 4b825dc642cb6eb9a060e54bf8d69288fbee4904, 4e3cb251fb98a47c2f5dec5f3722723990c17a49, 5d1edc470b4b33a31f982077e08b2e61f438feab, 62c86b52fabaaecc398b902965e58c4154edc427, 63a5c5307b93e0393aba14b42d7915ab7a2733ef, 67eb4f5d839ca89b28203a27ce3ca74029b93b7c, 758c73ab9706ae6977f9b4601c20b3667836d3ef, 83c851f265f6d7dc9436890009822f0c2d4ba50a, 9653938c6fd4b347209d87923f3617d70a3c12e2, a0338654304b6f824bdc39bbb482a0e114f8a3a1, a7b74e834eddb6eb9a23a268c7088b3aeba493d4, a84f5a384b090598cd29be6b2492cbb45c73c3ac, abf71fd332b760da29aa211f4aaa1661860a98c6, b7f7fe7ce6d5eb7453ca5edd616bc9f071cd3ea5, ba95ea1dcc744566a9552d9665feff035925a5c5, d119d827561c0796c50deb8cf69f324811479e88, d2279dc66302d8afad41c82ad81d0733e1f2273d, d645bd6c880358d2bb4dfd83252ebbb6156c6b5c, de2b332d06251e6449760ceead598a56da637daa, e0837aebd649dba01bc4d594ef21a8086edaaeeb, e9e56beee7cf526a4df97e35f2df9458cae0ec23, f03354f986a1398d1b471c0af75b404474cf94f7
SHA256	2cedf60566ee524440c85a8779d5e12a203d1dff140f4c3d32374b7eab547ef6, 5433726d3912a95552d16b72366eae777f5f34587e1bdaa0c518c5fcbc3d8506, 6587de22729bf3dd6f3632d67881fbc75275b9fd6d88597c7f04462ec1b2bcdf, 75fed14fd61067a1c0c2a10d0eefcc349308e1f4a1993a075a9f0c768affab13

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

References

https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/

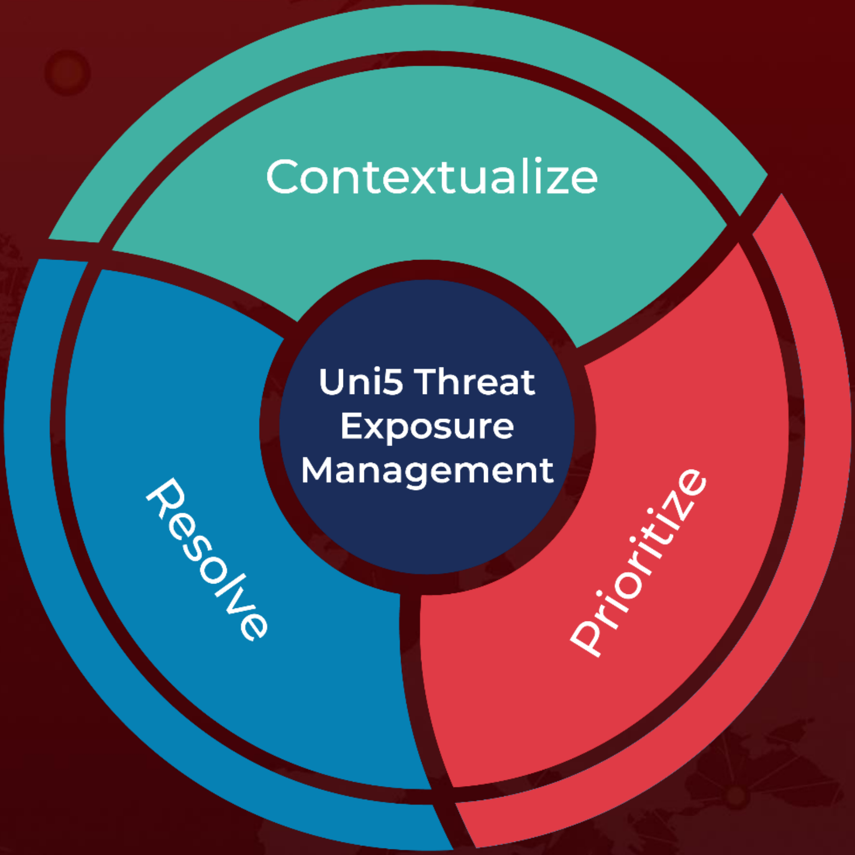
https://hivepro.com/threat-advisory/blind-eagle-blotchyquasar-malware-rattles-colombian-insurance-sector/

https://hivepro.com/threat-advisory/microsofts-november-patch-tuesday-addresses-active-zero-day-exploits/

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

March 12, 2025 • 5:00 AM

More at www.hivepro.com