Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

CarnavalHeist: New Banking Trojan Targets Brazilian Users

Date of Publication	Admiralty Code	TA Number
June 6, 2024	A2	TA2024217

Summary

Attack Began: February 2024
Targeted Countries: Brazil
Malware: CarnavalHeist Banking Trojan
Targeted Industries: Banking, Finance
Affected Platform: Windows
Attack: CarnavalHeist is a new banking trojan targeting Brazilian users and has been active since February 2024. This malware stands out for using a Python-based loader and targets banking desktop applications, stealing credentials through overlay attacks and keylogging.

Attack Regions

Attack Details

#1 An active campaign targets Brazilian users with a new banking trojan called "CarnavalHeist." This trojan shares many tactics with other Brazilian banking trojans but stands out for its use of a Python-based loader in the DLL injection process and its specific targeting of banking desktop applications. CarnavalHeist primarily targets Brazilian users, evident from the use of Portuguese in the infection chain and Brazilian financial institutions' names embedded in the malware.

#2 CarnavalHeist's infection begins with spam emails containing financial themes that lure users into downloading malicious payloads via URLs. These payloads involve a multi-stage infection process using LNK files or MSI installers, which eventually lead to the execution of a Python script that injects a malicious DLL. This malware uses overlay attacks and input capture techniques like keylogging and screen capture to steal banking credentials.

#3 Researchers attribute the development and operation of CarnavalHeist to Brazilian actors, identified through operational mistakes during domain registration. The actors behind CarnavalHeist used GitHub accounts and exposed personal information in WHOIS records, leading to their identification.

#4 CarnavalHeist has been in development since at least late 2023, with significant activity starting in February 2024, and remains active to date. The actors behind CarnavalHeist display low-to-moderate sophistication, but shows potential for future development improvements.

Recommendations

Deploy Strong Email Filtering Systems: Implement robust email filtering solutions to detect and prevent the dissemination of harmful attachments, particularly those originating from suspicious or unknown sources. This can significantly reduce the likelihood of initial infection through phishing emails.

Exercise Caution with Email Attachments and Links: Encourage users to exercise caution when interacting with email attachments or links, especially those from unfamiliar senders or containing unexpected content. Verify the sender's identity before opening attachments, and report suspicious emails to the IT security team.

Network Segmentation: Segment networks to limit the spread of malware infections. Restrict access to sensitive systems and data, and implement firewalls and access controls to prevent lateral movement by attackers.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0040 Impact
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
T1547.001 Registry Run Keys / Startup Folder	T1055.001 Dynamic-link Library Injection	T1027.010 Command Obfuscation	T1027.012 LNK Icon Smuggling
T1027.009 Embedded Payloads	T1036.008 Masquerade File Type	T1056.001 Keylogging	T1056.002 GUI Input Capture
T1010 Application Window Discovery	T1082 System Information Discovery	T1570 Lateral Tool Transfer	T1113 Screen Capture
T1125 Video Capture	T1102 Web Service	T1102.002 Bidirectional Communication	T1104 Multi-Stage Channels
T1105 Ingress Tool Transfer	T1568.002 Domain Generation Algorithms	T1571 Non-Standard Port	T1020 Automated Exfiltration

T1567 Exfiltration Over Web Service	T1584 Compromise Infrastructure	T1036 Masquerading	T1056 Input Capture
T1566 Phishing	T1027 Obfuscated Files or Information	T1059 Command and Scripting Interpreter	T1547 Boot or Logon Autostart Execution
T1566.001 Spearphishing Attachment	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.006 Python
T1055 Process Injection			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	104[.]41[.]51[.]80, 191[.]239[.]116[.]217, 191[.]239[.]123[.]241, 191[.]233[.]241[.]96, 191[.]234[.]212[.]140, 191[.]235[.]233[.]246, 4[.]203[.]105[.]118, 191[.]233[.]248[.]170
URL	hxxps[://]is[.]gd/38qeon?0177551.5510, hxxps[://]is[.]gd/ROnj3W?0808482.5176, hxxps[://]notafiscaleletronica[.]nf-e[.]pro/danfe/?notafiscal=00510242.500611, hxxps[://]nota-fiscal[.]nfe-digital[.]top/nota-estadual/?notafiscal=00792011.977347, hxxps[://]nfe-visualizer[.]app[.]br/notas/?notafiscal=000851113082.35493424000, hxxp[://]adobe-acrobat-visualizer[.]brazilsouth[.]cloudapp[.]azure[.]com/Documentos, hxxps[://]104[.]41[.]51[.]80@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]239[.]116[.]217@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]239[.]123[.]241@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]233[.]241[.]96@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]234[.]212[.]140@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]235[.]233[.]246@80/Documentos/files/a3[.]cmd, hxxp:[//]191[.]235[.]87[.]229/Documentos/dc/c[.]cmd,

TYPE	VALUE
SHA256	c300749ea44f886be1887b3e19b946efbdbbc3e1bf3e416c78cfbff8d23bf70a, 1b4f44a00f61b3e0c8cd6c3125f03b6d4897d6ab90c8a6dc899ed96acee80dd6, 8424e76c9a4ee7a6d7498c2f6826fcde390616dc65032bebf6b2a6f8fbf4a535, d9877dc1ba0f977d100e687da59c216454d27e3988532652ac8f6331debbd071, 0d94547a0b8f9795e97e2a4a58b0ece65b4ea4b6e6019cbc96e1c79f373b4587, f848c0f66afc7b5a10f060c1db129529a974ae0ad71a767f7c7793351bb7ca04, e50bde1e319e699f587d3b5403c487e46deed61cc3f078fe951e7cb9f6896259, f00cb0603c055c85c7cdf9963d919d527b13013c182dc115ba733d28da57b1d9, 2c53b4dc15882cf22772994d8ed0947e4a8b70aef3a12ab190017b3317c167ea, a6d995d015c16985b456bcc5cd44377c3e5e5cf72b17771eadc51e1d02a3c6ef, 21e22c4736e7567b198b505ed303c3ca933e0c2d931b886756f6db18a9884a75, 2c1251ae1ec9d417bbbdd1f6ac99baa3f16a7639d0c12cb2883ef8c22c73e58e, 46e754727efdc2c891319d25a67ee999a4d8a0b21b0113db08eead42cf51b780, cd9f5773bd7672a3e09f2d05ef26775e8c7241879d5f4d13c5c5bc1704c49fa1, f2db799d892f2a7ac82bfa15826e74d778abdfa153ccafb9db1fdf56a0248a40, 5782b9bc96ce5ad011c122496ff0ff0dc08d6444c6d2e98606ada82130d5f21a, 19c02c5724622be4eedff95633f3fbaa604449aa50cc0761693bb8adb1e8cf97, 3b450994add1e3a206c56a7f8fd28e4132cffb27f3df345e07e8908d7989751f, 1e8fd8531a0851bb4d8fb6d8dd4b1a9509c8a971b11b7d95871d7b39004650ad, 8c31dcbef5c00fd98e426a1ae84163b807a2c5d1476b2d306c8f7e9d01d8df23, 2bcd8cc83cf31a77a556d5462a7e75c5e2120891414684a6e21612d61d734673,

TYPE	VALUE
SHA256	c44df224b304a9d5d089be7d68d7e5cec4c76ec58fdc16c3f86b20a671b496cf4, b8b3963967232916cd721a22c80c11cd33057bd5629dcfa3f4b03d8a6dbf1403, 883c49b7c869019951eff94699480a7ecc97c9c45060a15797ecbd5fce060d26, e7aa64726783ec6f7249483e984ae20b31a091a488a3ed0f83c210702c506d20, b152346c2679392d7e15d1cc72a39a21d24e55360c4c1c845ef3524924e93fa9, 561e6a42e23d12abe6bba8c98f84c3ba7c45a5df840bfa6fd0dfea803c9b4b7e, 7e0051d9221c13a47245359a2cd2804b4d3d9302a321fc8085da1cf1a64bac91, 056b34444abe385addd08cc581a640b72d4f2cba05de2bfd0c897d5b273a7f28, ab3a284ae6e4e466a0715c162cfab85d75522bec48fa25947b16a0891ec2358a, 7232e3318fdc370e611b2bcbaaec3d58a0d687927714c24dc81fe60767d53a31, 3c89775ae7c35fe3d1ec7e75ac9d4a19959d082d31ab412af243125440ffea6c, aadbba21380dba5028a68b44c629988b0ca517f34c1adbd68f2edd604ea507fb, 278897ee9158f9843125bc2e26c14f96c4e79d5fc578b7e5973dc8dc919a3400, 049b7067ac87e44f464cb18e454d878ca6260b667a34f48ed0046c29b45bb149, 8573b7aa7ac688e2fb03845aa7903b5f58d880865e3b63c4884f8e29839a3754, f92af5e770018c9e1be5d934bb5699fcf4594d870988e7b18fb65501ef43f8f9, 3445066ae58aa68c09b2476e65f96f46d0a3ae0a09366d8f9e7e592ee3f2aa0c, d3a7f22886cd294549e5f93ec18ab04e085c397ef703f5543c3b967c1172bf41,

References

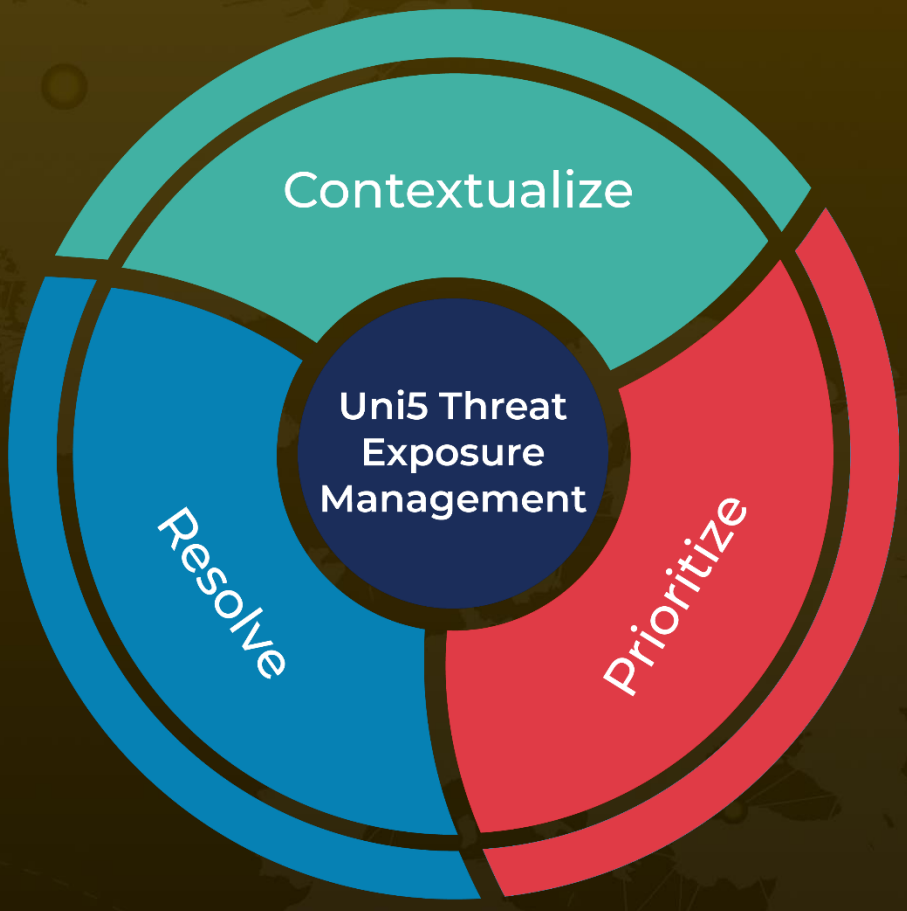
https://blog.talosintelligence.com/new-banking-trojan-carnavalheist-targets-brazil/

https://github.com/Cisco-Talos/IOCs/blob/main/2024/05/carnavalhiest.txt

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

June 6, 2024 • 5:30 AM

More at www.hivepro.com