Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

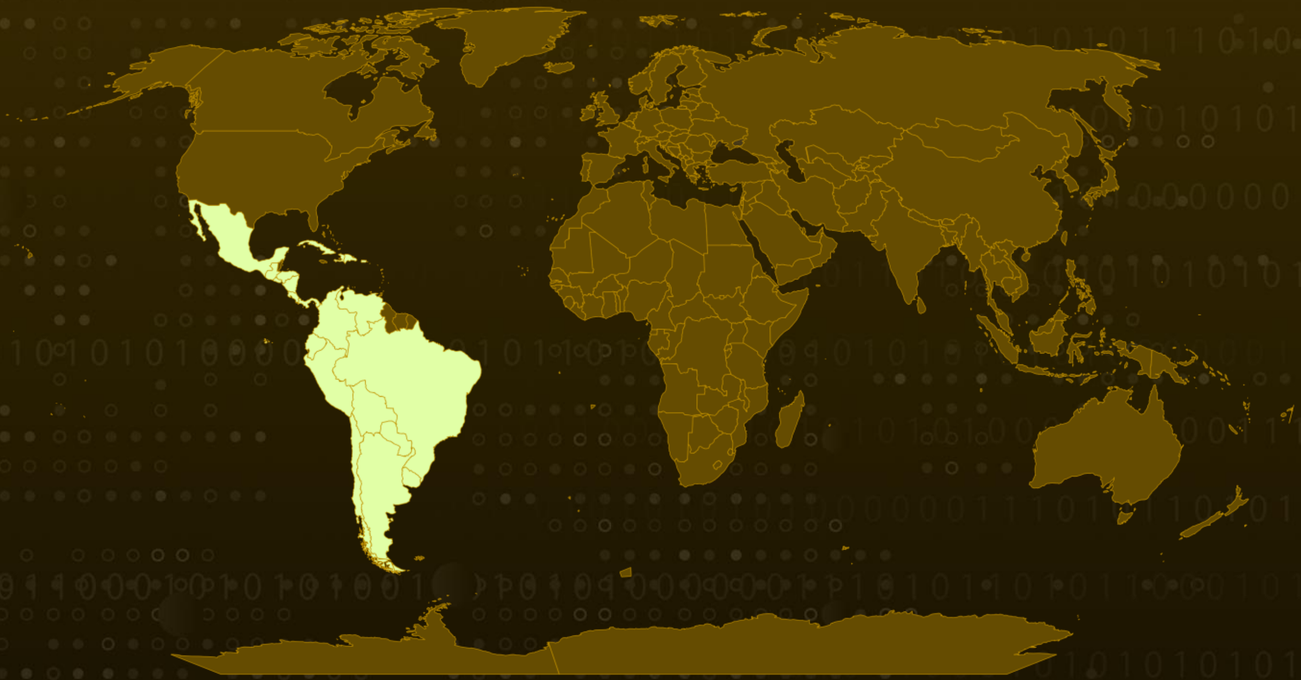
JanelaRAT Strikes at Latin American Financial Sector

Date of Publication	Admiralty Code	TA Number
August 17, 2023	A1	TA2023335

Summary

Attack Began: June 2023
Malware: JanelaRAT, BX RAT
Attack Region: LATAM region
Affected Platforms: Windows
Targeted Industry: Financial, Cryptocurrency
Attack: JanelaRAT, a financial malware, is directed towards users in Latin America (LATAM) with the ability to seize sensitive data. This malicious software primarily focuses on gathering financial and cryptocurrency information from banks and financial entities within the LATAM region.

Attack Regions



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

Attack Details

#1

JanelaRAT, a type of financial malware, focuses on users within Latin America (LATAM) to extract sensitive data. This malicious software places a primary emphasis on gathering financial and cryptocurrency details from financial institutions and banks across the LATAM region. The attack sequence commences with the transmission of a VBScript enclosed within ZIP archives.

#2

Within the ZIP archive, two components are included, which are responsible for executing subsequent stages of the infection chain and achieving DLL side-loading. To evade analysis and detection, JanelaRAT employs string encryption and is capable of transitioning into an inactive state as required. Moreover, it constitutes a notably modified iteration of BX RAT, which was first identified in 2014.

#3

One of the innovative inclusions in this trojan is its ability to capture Windows titles and transmit them to threat actors, subsequent to registering the newly compromised host with the command-and-control (C2) server. Further capabilities of JanelaRAT encompass tracking mouse inputs, recording keystrokes, capturing screenshots, and collating system metadata for transmission via C2.

#4

The developer of JanelaRAT is fluent in Portuguese, as evidenced by the extensive language utilization in malware strings, metadata, and decrypted strings. By employing an adaptive strategy that involves dynamic socket configuration and exploits DLL side-loading from reputable sources, JanelaRAT presents a significant and noteworthy threat.

Recommendations

Employ behavior-based analysis tools that can detect abnormal activity on endpoints. JanelaRAT may exhibit unusual behaviors, such as logging keystrokes or capturing screenshots. Behavior analysis can help catch such activities. Additionally, it is recommended to exercise caution when engaging with links and attachments from sources that are unfamiliar or untrusted.

Employ network monitoring tools to detect unusual patterns of data traffic or behavior that might indicate a JanelaRAT infection. Look for irregular connections to external servers, particularly command-and-control servers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0043 Reconnaissance
T1587 Develop Capabilities	T1608 Stage Capabilities	T1587.001 Malware	T1608.001 Upload Malware
T1059.005 Visual Basic	T1059 Command and Scripting Interpreter	T1547.001 Registry Run Keys / Startup Folder	T1574.002 DLL Side-Loading
T1027.002 Software Packing	T1140 Deobfuscate/Decode Files or Information	T1497.003 Time-Based Evasion	T1132.001 Standard Encoding
T1573.001 Symmetric Cryptography	T1095 Non-Application Layer Protocol	T1041 Exfiltration Over C2 Channel	T1573 Encrypted Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://zimbawhite.is-certified[.]com:3001/clientes/6, hxxp://zimbawhite[.]is-certified[.]com:3001/clientes/[1-44], hxxp://45[.]42[.]160[.]55/
MD5	c18edb805748b4bd5013ccb47f061c2a, 7e4592e02951be844a2ee603d75070a6, 526a0b2d142567d8078e24ab0758fad7, e841f4691e5107fe360b1528384a96f0, c39f75423862c1525f089a5e966b9d04,

TYPE	VALUE
MD5	c18edb805748b4bd5013ccb47f061c2a, 72c02b3181c763d0e67f060e91635a97, 897e8483b673db70fdc5d3d111600cac, c2f4cb0da89b4ea86ab5369a942428eb, e56d8632db98b07d2b49423f7dd64b42, 8b83e6b2d891cdf9250e9afd17081eab, 999a9af2cd20a8c4bcf652e3523aafa3, 51268b9681df47022c44af43f9d57255, 24c6bff8ebfd532f91ebe06dc13637cb, 1b72c12db8a37103a37cab5b3b14398c, 397e407e63128e71089971e3b35dd253, 172ca00d32a201f5e917bc4d73f720a1, 505fab6d83ef86a4b12b5808047fa7f1, 3870e4a4d86a34424ea47bdaa722cd89, 44d9f29a81a2f2df83b6000165e8a06f, f71471d7e94ef739a8ee44125023b750, ec60bc4522fa58bfe9592abde33948a7, 81618be603bca301ac156ed169444569, ba2bd2d31cf591480b69e106b0e77b5c, e2d7101f405ed88aba89bf39d56ee7a8, 84919bf0583c0e6c04e606f34a1d56f3, 48c189e5dfe28b9d2b32fd813a991adb, e684e872213432320c78f56c72c88a8e, c86fdacd8af28cb08ef406bc6d4fc5a7, d057c499f440b77cfcad8d859d389915, 36a8a7407f084b4ae461b6bb4dd0b65c, 900445a57f462d0df130c3612e6caed7, 691cc21dae6e320564f74d6372e94286, b1e1134c82fdfe28394893008947457 4, 0cf2707ce1dccd6054813cb9207bf3d4, d1684fa84602a2d560b47dfe0f0779b4, 2cbee69042a4d85ecfe6e55639b1b42a, da48cd57e4b45cba63716bc2d53c4c76, b2aaee6945f75caa1c44bca3e2812993, e166bd80341871c9d752537f80584334, 3bbfc1f2e20ba8209d057c215303b2bf, 4d62fc39e2586da78b65fff6dc844670, aa3162289e7e848b7aeb19c8b85131fd, 1fc6298c88b3ea2030cc0382369d0bb9, 42eb945b1b881b2319a74af06b1037db, 8ca3dd771adbba82d28ce7ba4a0b8c97, 4a1465999cdd9ee687b72289df05eaa9, 5335caa5d199eac6f67b2e911b6b1e37, e2f9e1dfb24c9deb7f4a3c0c5c1fd016,

TYPE	VALUE
MD5	3ec6342286d5b699bc1fb2ef6598f906, 3cbe59c309f803fffdadcc69d3578a53, 4c9c287103defb55b9e89278800e4025, 7548edc03021561c4d7a1b386aaa7696, 596de51352cbeb0d26d861e991889578, 18ed52de642d3f3aab7c271804bd005a, 5a5106ee07d277b373d13c9f3160fea0, 7b70c957449ab51f8d561582f229d5cf, 0898c4c1cb698cd29707db44352ab868, 5f628223fa083e4598badfe7efae5269, 304202cbc70412e76a216257ff4d2085, 398d0268535cba57fa3b33159bbe04f3, e6c501b52165cd278724ea229e44a8b9, c625443768b40cfbc93e28b92e874740, c5f2d6d3d3ac3521d2b2f7fa90d3ee5e, b036f1351ed5af87005978c7b6036d3d, 3a336c5c7bd08587ad1709294d044e41, fc79aa5093f55dfa18a20f538c5e475e, 4b142b23110fbb7b98ad49c051d7a1af, 76887ccf6de5b5f8d70cd6d91450b131, 6364aa555ae8fd0ba5a8d97a2ffa314a, f4a42ef33e3a3a41b4e7ee0cd3173fb6
SHA1	37df375be813d91e11795a75872479c1a656e951, Be7e5282efe58018b462a5ba0a78a7f01108460d
SHA256	0c873439bc0af08fdf0c335c5a94752413fd096c0c2f1138f17e786bc5ce59c3, c6b3f1648f7137df91606f6aaaa6d25d672e18c8adcb178c6d8cdcf3148a3c81
Domains	cnt-blackrock[.]geekgalaxy[.]com, aigodmoney009[.]access[.]ly, freelascdmx979[.]couchpotatofries[.]org, 439mdxmex[.]damnserver[.]com, 897midasgold[.]ddns[.]me, disrupmoney979[.]ditchyourip[.]com, kakarotomx[.]dnsfor[.]me, skigoldmex[.]dvrcam[.]info, i89bydzi[.]dynns[.]com, infintymexbrock[.]geekgalaxy[.]com, brockmex57[.]golffan[.]us, j1d3c3mex[.]homesecuritypc[.]com, myfunbmdablo99[.]hosthampster[.]com, irocketxmtm[.]hopto[.]me, hotdiamond777[.]loginto[.]me, imrpc7987bm[.]mmafan[.]biz,

TYPE	VALUE
Domains	dmrpc77bm[.]myactivedirectory[.]com, jxjmrpc797bm[.]mydissent[.]net, askmrpc747bm[.]mymediapc[.]net, myinfintyme09[.]geekgalaxy[.]com, infintymex747[.]geekgalaxy[.]com, infintymexb[.]geekgalaxy[.]com, jinfintymexbr[.]geekgalaxy[.]com, minfintymexbr[.]geekgalaxy[.]com, cinfintymex[.]geekgalaxy[.]com, 9mdxmex[.]damnserver[.]com, ikmidasgold[.]ddns[.]me, rexsrupmoney979[.]ditchyourip[.]com, kktkarotomx[.]dnsfor[.]me, megaskigoldmex[.]dvrcam[.]info, izt89bydzi[.]dynns[.]com, zeedinfintymexbrock[.]geekgalaxy[.]com
IPv4	191.96.224[.]215, 192.99.169[.]240, 191.96.79[.]24, 167.88.168[.]132, 102.165.46[.]28, 189.89.15[.]37

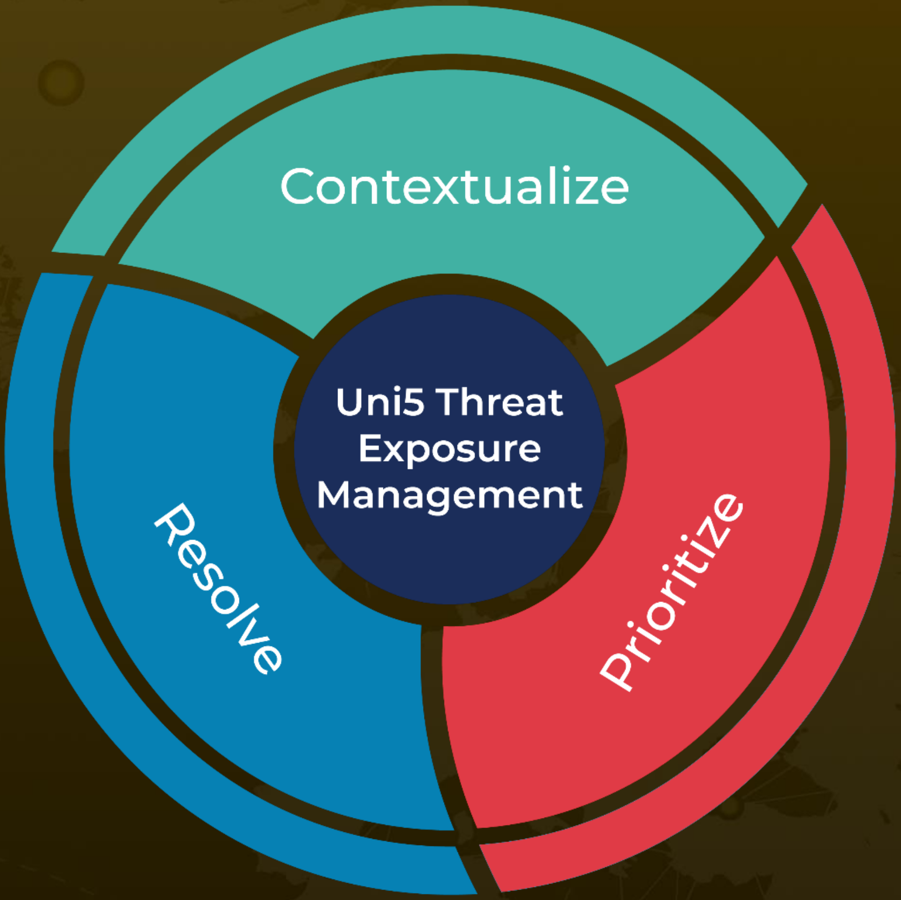
References

https://www.zscaler.com/blogs/security-research/janelarat-repurposed-bx-rat-variant-targeting-latam-fintech

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

August 17, 2023 • 7:30 AM

More at www.hivepro.com