# KPMG Cyber Threat Intelligence Platform

## Janela RAT – Advanced Multi-Stage Attack on LATAM FinTech

**TLP :** Clear

**KPMG. Make the Difference.**

**Janela RAT is a sophisticated Remote Access Trojan, first identified in mid-2023, and believed to be a modified variant of BX RAT. It spreads through malicious installation files disguised as legitimate software hosted on trusted platforms. Primarily targeting countries like Chile, Colombia, and Mexico, Janela RAT is used by financially motivated threat actors to infiltrate banking, fintech, and cryptocurrency sectors across Latin America.**

Janela RAT is delivered via malicious .MSI installers hosted on public GitLab repositories, disguised as legitimate software. Upon execution, the installer initiates a multi-stage infection process using orchestrating scripts written in Go, PowerShell, and batch. These scripts unpack a ZIP archive containing the RAT executable, a malicious Chromium-based browser extension, and supporting components. A batch or PowerShell script generates commands to launch the RAT executable using a hardcoded filename, initiating its core functionality. The Go-based unpacker extracts a password-protected ZIP file, decodes base64-encoded C2 domains and repository lists, and writes them into a config.json file for operational use. The scripts identify installed Chromium-based browsers and modify their launch parameters to silently install the malicious extension. The extension registers a native messaging host and uses its CollectRefresh function to gather system information, cookies, browsing history, installed extensions, and tab metadata, triggering RAT actions based on URL pattern matches. Janela RAT establishes encrypted WebSocket connections to base64-encoded domains and employs techniques such as encrypted communications, dynamic C2 rotation, idle-state behavior, and obfuscated binaries to maintain persistence and evade detection.

JanelaRAT's sophisticated use of obfuscation, and credential harvesting highlights the urgent need for enhanced defenses against evolving financial cyber threats.

### What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

### KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

| We offer a wide-range of services, including: |
|---|
| Strategic threat intelligence report |
| Machine ingestible threat intelligence feeds |
| Threat intelligence driven pre-emptive threat hunting exercise |
| Cyber Incident Response Services |

**KPMG in India Cyber Response Hotline: 1800 2020 502**

## KPMG in India contacts:


**Atul Gupta**
Partner
Head of Cyber Security
**T:** +91 98100 81050
**E:** atulgupta@kpmg.com

**B V, Raghavendra**
Partner
**T:** +91 98455 45202
**E:** raghavendrabv@kpmg.com

**Sony Anthony**
Partner
**T:** +91 98455 65222
**E:** santhony@kpmg.com

**Manish Tembhurkar**
Partner
**T:** +91 98181 99432
**E:** mtembhurkar@kpmg.com

**Rishabh Dangwal**
Director
**T:** +91 99994 30277
**E:** rishabhd@kpmg.com

kpmg.com/in


**Follow us on:**
**kpmg.com/in/socialmedia**

KPMG

# KPMG Cyber Threat Intelligence Platform

## Janela RAT – Advanced Multi-Stage Attack on LATAM FinTech

**TLP :** Clear

**KPMG. Make the Difference.**

### Indicators of Compromise: IP Addresses

| | |
|---|---|
| 191.96.79[.]24 | 191.96.224[.]215 |
| 189.89.15[.]37 | 192.99.169[.]240 |
| 102.165.46[.]28 | 167.88.168[.]132 |

### Indicators of Compromise: Domains

| | |
|---|---|
| w51w.worldassitencia[.]com | team000analytics.safepurelink[.]com |
| bulder.wordsuporttsk[.]com | |

### Indicators of Compromise: Hashes

| |
|---|
| 6550ea36af6d367e39b948835738f76d |
| e7a6f1889744468d72b8644529a6cbac |
| e2bf84693ebc12624d9be3f384b4e509 |
| b1c2a280a40a447aa28031e117902b12 |
| 18cdd3e64da55f495cf1d05c306cf176 |
| 8ea05d5b2b94f97dbe7ec483ce1077c9 |
| e89c194cf4530c001b14f9142262b410 |
| 6092804d3e3ff007705e6b5f612d59339c8df159 |
| 254cccfa8d1b29073c7a5c66e121f060333db400 |
| 31e778378306b9ce2c1cf2ddcecbfc7d42021763 |
| 6b06237e92984deb88583c909841dbfc54f57ca1 |
| b1258dad21ff1f06504e6cc2be41d6183d2c0e0c |
| ee0b392ce2df25630030cb10cb3d730d673a4b5a |
| 4adcdbf9933c47f478bda6058b5d5f237eb84b58 |
| 876cd37b9591d2c42c414d08f2392e1e511137f0 |
| b18b61306aba922e4f746ea3d032a8d0a29ecd67 |
| e676ebf47af3cc412bb92585bb8a7e8475cb6afb |

**Follow us on:**
**kpmg.com/in/socialmedia**

KPMG

# KPMG Cyber Threat Intelligence Platform

## Janela RAT – Advanced Multi-Stage Attack on LATAM FinTech

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
|---|
| 142a574251873d9be9432efdd5de2ebb763fe571 |
| a05df139e676da07fe0b17adb4e3780b56862327 |
| 83ae5dc85f772c87863d78d97b15178563e35c0f |
| 053142b705964971847348a67e14fc697fedd401 |
| 4e6ded77b20b7fac76a98c1849507b4f8db5079b |
| 539fec46b4e148cd40ac547c6088a2bbc4b9bfea |
| b9976daf3b503fe540af652ed3cf3f2421a4b9a6 |
| ae27b9b0c9dfd41a9eb99c0d05e3ba0d28ff8b09 |
| 9ddc99425f8f9da3491e04c673164f6311f0fb78 |
| c05783e2837615cc751d7003c0729f83b6891c81 |
| 9416c6f4dc80684b4222a3fe3dcf932d6443ac52 |
| f062ea7ef775321a6e3c5abcf726ace13aba889a |
| 2eb075fd728097e0963a38c88d38e108a93e1086 |
| 37577413d134a87b0e9605b38a3e688b862a8daa |
| 676c3a0d27693ad4d0449d5ad6696326842449fa |
| a9d2d2709cc8dab2e893de6322ed0093af5bdd95 |
| 2e91f2e51e46ee2557230bdb2fb3da8c7b1a58b7 |
| 8537133c2e445183dd61f6bfd25c01090bbc7cf3 |
| 325423f6ae40237953e4a9499a9a844c8a2c6d2e |
| 67bba07e645e0d9551cb6b8d4198bcd23a16910e |
| 766e0129e7c4b2a6daeee2befe5b87853ba7edac |
| 10bb373322796ccb467103bd2f4c7c46dad8b8f8 |
| ac6de6bc3ffa762f6b511f1e04b22a5c498ec7fd |
| cc7f458199e293a27090da8559c20cb291689bab |
| ee9a1e0831534178bd4ed44b6aa58c7e503c9954 |
| 31e778378306b9ce2c1cf2ddcecbfc7d42021763 |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Janela RAT – Advanced Multi-Stage Attack on LATAM FinTech

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
|---|
| 006fab2aad27c01f702d60b0210a3dde420fe6e5 |
| dcdde5f2219bfe5b8b2c57549ebbef8e166086ec |
| 45aa646b6a3e825bcb29a665f69d48c30424fa30 |
| 2563f9bcf8a42f0cb31a5b59bd825272dfb13c5f |
| 6e7ea7d2412183fa7dceeebdd5dfe8049baee38a |
| a22f7c9f292853cafe9a79498873733f0ddf6fdd |
| 1501bca70dd9ce99d0762a0151424ec767eb55be |
| da6b97b245c65193eb231de0314508759a69db35a8f76afc66b4757702a231d0 |
| 248ee6233a85daaa3ddc2d9aaf6f24a26969a1f46981aa2a13af0c661fe006d8 |
| 666ba2708be3fc6a208d1e961af343a8105959fa87bfd3322a36d6c4e57d1122 |
| 6ed7ec9d0c366310d647f44830a6b9bc353a0d8b9e3345253c770bb23a90bdd3 |
| 97364179ab942af483b973653b89c0dfb8ed5c7d56ed62dbbf7a62933c473fa6 |
| e2a86247b7089a5ffb4d0a3c421cedc044c744d37852ebac17291855c54713cf |
| e200158dcca9b28c65d297cc2ff44a2183d8228568c2ebf98ac888d494e18649 |
| f6edcd66b7c14920bc0f820eaf537bf5ee101c91b618ea3fbbb1b8978a40a775 |
| cef2b3501cd53bf6eebd1f80ec0d2abcd7b8488943f51b5feac1e2d223b78c95 |
| e9e864184fd63731a28272c1e5d27154c74e5764bbf017b375afcc64398accc7 |
| ae466c8aef4fcce140a34ede8e1b7a0f2efe4daac528c3c093e2c44d08d288ef |
| a670835f7c69ade92bd64535ce19e388ad906c774ac07f52b7a08b068de5b1bd |
| e310b8142f342cd614065283f3219895d8c1e1b9d4ddf566c75f489fa83be05a |
| 569ad9fd3a3f7797b1d5bf295bd722404c414b1a351796683b3c71fa83019995 |
| f1e948cf6b89ae0a0361d8494fac220f62d1481dd15315fe4aa4ee66b01f5573 |
| 000356ff8bab0222fad9572b640997eed54390280fee8605d5ee3aec4cb01413 |
| cd4f8137e7732238303257a714252e76b6c1c61d3ba27f5ffc6a82fae5b0497b |
| fca602926f8334c86d9329964089f241f0ab454336ab64bcf4e28adc11e092ea |
| 5767b8991728ba9de1f7c020b23624b5009b93c1a8457f060f9d6067839f3dda |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Janela RAT – Advanced Multi-Stage Attack on LATAM FinTech

**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
|---|
| 4fcf6d8e463adc77621dcc2ae0c1dbb8b653737e3f12a2b48f7a17ef116ff5fe |
| e3d96eff89cbcfe1d45a72cf657158dee2ab1db835a7814c506a76de1bc68dca |
| 000356ff8bab0222fad9572b640997eed54390280fee8605d5ee3aec4cb01413 |
| adf1786364d43f70e70be770728b0e89b6a0ea164cd8f088dee87d32342edf97 |
| 569ad9fd3a3f7797b1d5bf295bd722404c414b1a351796683b3c71fa83019995 |
| cef2b3501cd53bf6eebd1f80ec0d2abcd7b8488943f51b5feac1e2d223b78c95 |
| c6ef29299570852806fadedb6a677de1690e3aacf222dd685b01be26cd0670cb |
| e9e864184fd63731a28272c1e5d27154c74e5764bbf017b375afcc64398accc7 |
| 16748fc7cc71ff6568a09d5ea4d4ac2fa23667b9aa9dd0766e425bb18f842aa8 |
| f6edcd66b7c14920bc0f820eaf537bf5ee101c91b618ea3fbbb1b8978a40a775 |
| c206df6a4e25c65d77a65358093d81d07072169598abb48e14e0749b12f096a6 |
| a98370fb8325d0ba5ab2b2133e743eadfcfe530cc973295ca48dae2f485df742 |
| 000356ff8bab0222fad9572b640997eed54390280fee8605d5ee3aec4cb01413 |
| f1e948cf6b89ae0a0361d8494fac220f62d1481dd15315fe4aa4ee66b01f5573 |
| 569ad9fd3a3f7797b1d5bf295bd722404c414b1a351796683b3c71fa83019995 |
| e310b8142f342cd614065283f3219895d8c1e1b9d4ddf566c75f489fa83be05a |
| a670835f7c69ade92bd64535ce19e388ad906c774ac07f52b7a08b068de5b1bd |
| ae466c8aef4fcce140a34ede8e1b7a0f2efe4daac528c3c093e2c44d08d288ef |
| e9e864184fd63731a28272c1e5d27154c74e5764bbf017b375afcc64398accc7 |
| cef2b3501cd53bf6eebd1f80ec0d2abcd7b8488943f51b5feac1e2d223b78c95 |
| f6edcd66b7c14920bc0f820eaf537bf5ee101c91b618ea3fbbb1b8978a40a775 |
| ae466c8aef4fcce140a34ede8e1b7a0f2efe4daac528c3c093e2c44d08d288ef |
| f1e948cf6b89ae0a0361d8494fac220f62d1481dd15315fe4aa4ee66b01f5573 |
| 08f09a220fb0fdc02fa3981358957df48ffc955978382cd6c1870c429d78a165 |
| 0c6e12d23d94eddb3bdf15a2108401bcf47a5bc3796a4e5e5fa985eaacbae454 |
| e310b8142f342cd614065283f3219895d8c1e1b9d4ddf566c75f489fa83be05a |