Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

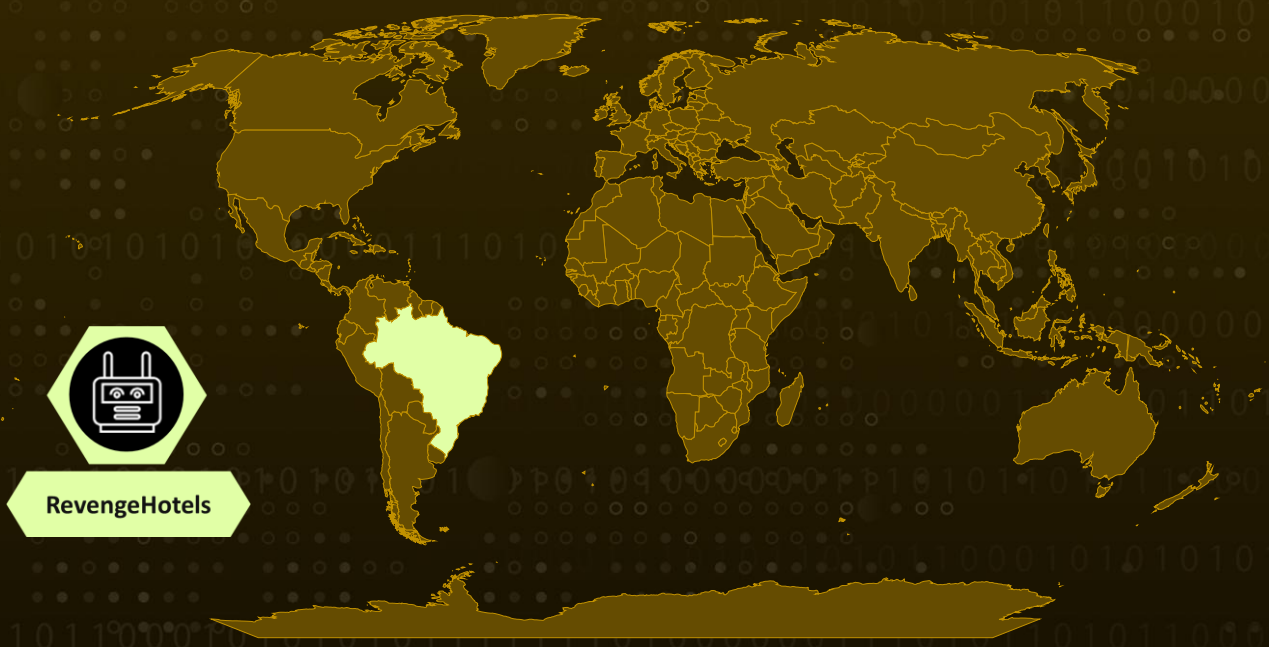
# From Bookings to Breaches: RevengeHotels Latest Attacks on Hospitality

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| September 18, 2025 | A1 | TA2025287 |

# Summary

**Attack Discovered:** 2025
**Targeted Countries:** Brazil
**Targeted Industry:** Hotels
**Affected Platforms:** Windows
**Malware:** VenomRAT
**Actor:** RevengeHotels (aka TA558)
**Attack:** RevengeHotels (TA558) has quietly turned hotel front desks into gateways for cybercrime, luring staff with fake invoices and job applications that mask hidden malware. Once inside, the attackers deploy VenomRAT, a powerful tool that lets them spy on systems, steal payment data, and even disable security tools to stay undetected. In their latest campaigns, the group has started using AI-generated code, which makes their attacks more polished, quicker to execute, and tougher to detect. With Brazil at the epicenter and Spanish-speaking hotels increasingly in its sights, RevengeHotels is evolving into a serious threat to the global hospitality industry.

## Attack Regions



# Attack Details

**#1** RevengeHotels (aka TA558) is a threat actor that has been stealing credit card data from hotel guests and travelers since 2015. Over the years, the group has refined its methods, relying heavily on phishing emails that lure victims to websites imitating document storage services, while also exploiting vulnerabilities. From there, script-based loaders infect targeted machines and eventually deliver remote access Trojans (RATs). In mid-2025, a new activity was observed by the actor, marked by more advanced tools and implants, with Brazil remaining the primary focus while Spanish-speaking markets also came under fire.

**#2** They target hotel reservation and front-desk addresses, often using invoice-themed lures or fake job applications that play on the daily realities of hospitality staff. These messages are localized in Portuguese and Spanish, and each malicious email points to attacker-controlled websites designed to change frequently, complicating detection efforts. Once visited, these sites drop WScript JS loaders that begin the infection chain.

**#3** The loaders, commonly named in the format Fat{NUMBER}.js, decode an obfuscated payload buffer and write it to a PowerShell script named with a timestamp to avoid reuse across infections. This PowerShell then retrieves further Base64-encoded files from the attacker's server, which acts as the entry point for VenomRAT, and assists with in-memory execution. Many of these initial-stage scripts bear the hallmarks of large language model (LLM) generation, cleaner structure, readable variable names, detailed comments, and minimal obfuscation, suggesting that AI assistance is now part of the actor's toolkit.

**#4** At the heart of the intrusion chain is VenomRAT, an evolution of QuasarRAT first observed in 2020. VenomRAT provides operators with a wide feature set: hidden VNC sessions, file-stealing modules, reverse-proxy capabilities, UAC bypass exploits, and strong AES-based encryption for configuration data. It also offers anti-kill protections that harden the malware's process against termination and continuously monitor running processes to eliminate security tools. Persistence is achieved through registry keys, VBS scripts, and process monitoring, ensuring the RAT stays resident even after reboots.

**#5** RevengeHotels further demonstrates sophistication by deploying tunneling tools such as ngrok to expose remote access services, while also disabling Windows Defender and modifying scheduled tasks to reduce detection. The recent activity has concentrated on Latin America, particularly Brazil. This shift underscores the actor's growing ambition and adaptability as it continues to refine its operations against the global hospitality sector.

# Recommendations

- **Be cautious with emails:** Train hotel and front-desk staff to spot phishing attempts, especially those that look like invoices, job applications, or booking requests. Encourage them to double-check suspicious attachments or links before opening.
- **Use strong email filtering:** Deploy advanced spam filters and threat detection tools that can block malicious attachments and links. This adds an extra layer of defense before phishing emails reach staff inboxes.
- **Restrict scripting and macros:** Limit or disable the use of Windows scripting (like WScript, PowerShell, or VBS) on staff computers unless absolutely necessary. These tools are often abused by attackers to load malware.
- **Back up critical data:** Maintain secure, offline backups of important files such as reservation databases and payment records. This ensures business continuity even if systems are compromised.
- **Monitor unusual activity:** Watch for signs like unfamiliar processes running, unexpected PowerShell scripts, or the presence of tunneling tools such as ngrok. Early detection can stop attackers before they dig deeper.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0007<br>Discovery | TA0008<br>Lateral Movement | TA0010<br>Exfiltration |
| TA0011<br>Command and Control | T1566<br>Phishing | T1059<br>Command and Scripting Interpreter | T1059.007<br>JavaScript |

| | | | |
|---|---|---|---|
| **T1059.001** PowerShell | **T1027** Obfuscated Files or Information | **T1059.005** Visual Basic | **T1189** Drive-by Compromise |
| **T1547** Boot or Logon Autostart Execution | **T1547.001** Registry Run Keys / Startup Folder | **T1053** Scheduled Task/Job | **T1548** Abuse Elevation Control Mechanism |
| **T1548.002** Bypass User Account Control | **T1112** Modify Registry | **T1057** Process Discovery | **T1021** Remote Services |
| **T1021.001** Remote Desktop Protocol | **T1071** Application Layer Protocol | **T1041** Exfiltration Over C2 Channel | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | fbadfff7b61d820e3632a2f464079e8c, d5f241dee73cffe51897c15f36b713cc, 1077ea936033ee9e9bf444dafb55867c, b1a5dc66f40a38d807ec8350ae89d1e4, dbf5afa377e3e761622e5f21af1f09e6, 607f64b56bb3b94ee0009471f1fe9a3c, 3ac65326f598ee9930031c17ce158d3d, 91454a68ca3a6ce7cb30c9264a88c0dc |
| SHA256 | 0109B0D2C690FED142DAD85CED4F1E277464ACC49DF4BEF3C5F5ED58F3925AED, F308A8CC0790F07F343D82AE0D9DA95248FB1BA4D4E01F30D0A8A43B9E6D3CA0, 156943B1DF6141AB7C2910B7CD5B8BCB2FFE839AA6C99D663ABF12588F11615B, D6CC784BE51F8B784BD9AFD2485F3766D89CA5AE004AE9F2C4DAE7E958DBE722, F10CC01B4988138A55FA7ED05ECA435DB636D820BD98BE7AC788E2480ED6165A, 89C73024FC9D700209ECADDF3628B59224D27750E188DCE0015313DA77346925, A5D1E69076FD9F52D8A804202A21852FE2B76FB4534F48455DEF652E84CCEAAB, 706AAFE4ED32AA4B13E65629C2496D9B1E2E9D1753AA0F92833586ACD1AA591E |

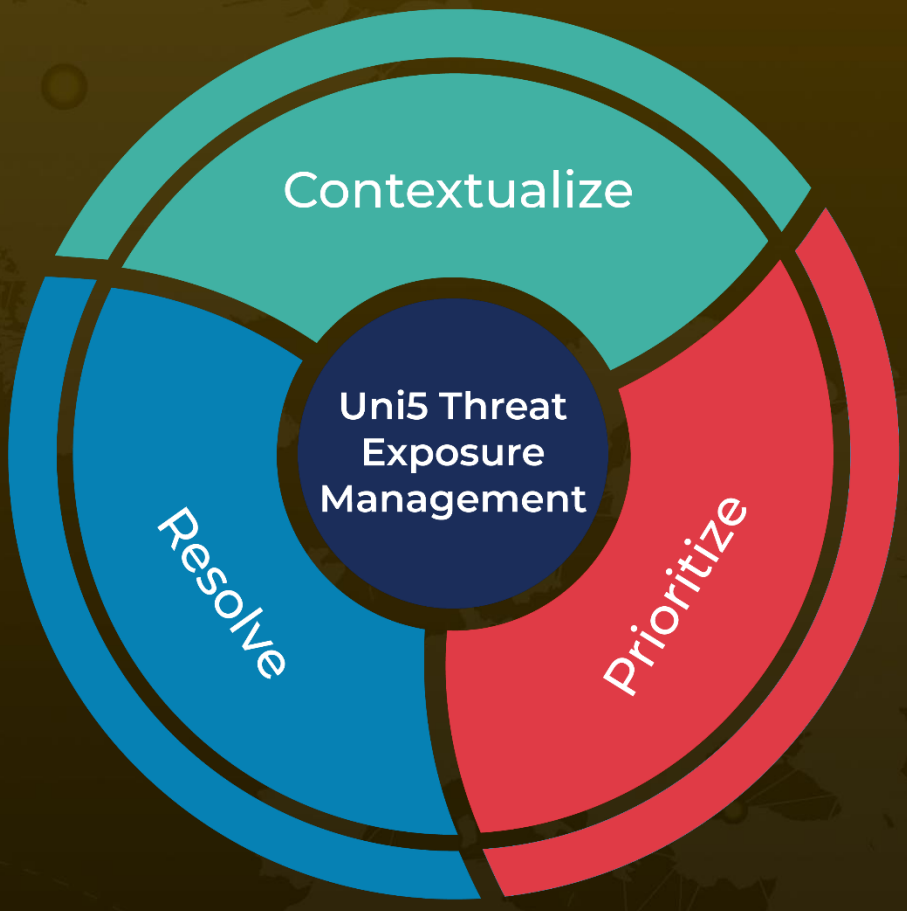
# References

https://securelist.com/revengehotels-attacks-with-ai-and-venomrat-across-latin-america/117493/

# 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 18, 2025 • 6:30 AM**



More at www.hivepro.com