

HiveForce Labs

THREAT ADVISORY

 **ATTACK REPORT**

I Paid Twice: Inside the Booking.com Phishing Fraud

Date of Publication

November 11, 2025

Admiralty Code

A1

TA Number

TA2025341

Summary

Attack Discovered: April 2025

Targeted Countries: Worldwide

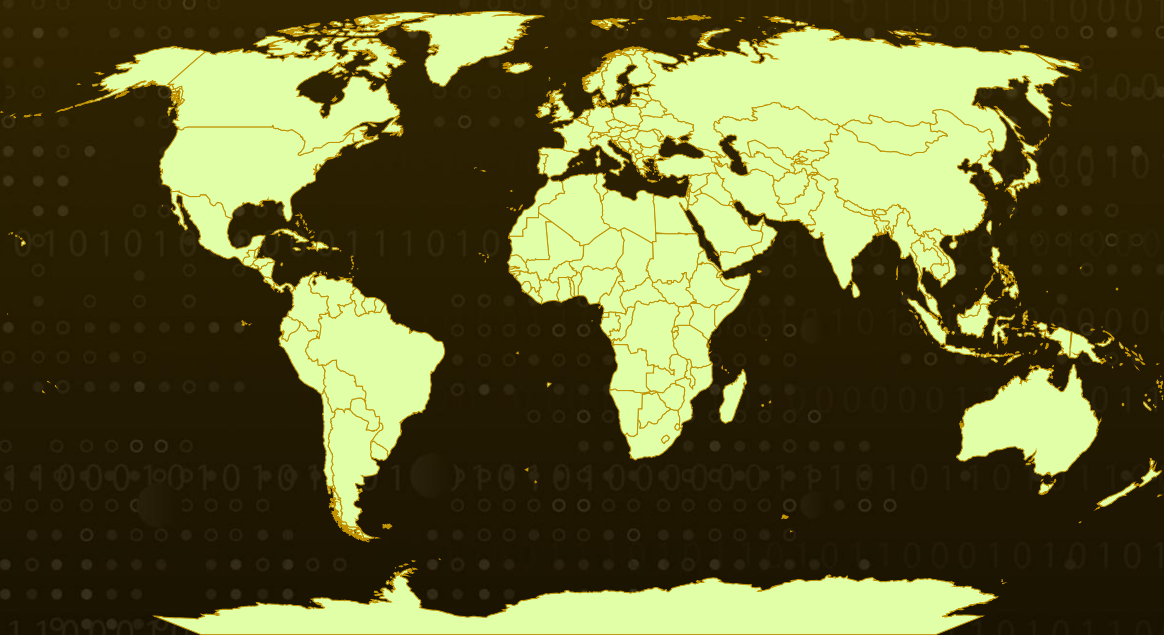
Malware: PureRAT

Targeted Industry: Hospitality

Attack: A sophisticated phishing campaign has been targeting the hospitality industry by hijacking Booking.com and WhatsApp communications to trick hotel guests and staff into revealing financial details. Armed with stolen credentials and real reservation data, attackers made their messages look legitimate, luring victims to malicious links powered by the ClickFix redirection system. This led to the silent installation of PureRAT malware, giving cybercriminals remote access to hotel systems and customer data. The operation has evolved into a professionalized ecosystem where stolen Booking.com accounts are traded and used for large-scale fraud, leaving both hotels and guests vulnerable to financial loss and data theft.



Attack Regions



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

Attack Details

#1

A recent large-scale phishing campaign targeting the hospitality industry has been uncovered, with attackers exploiting compromised Booking.com accounts and WhatsApp messages to deceive hotel guests and staff. These phishing messages appeared highly convincing because they contained real customer data, such as personal identifiers and reservation details, giving them an air of authenticity. The campaign originated from earlier credential theft operations involving information-stealing malware that infiltrated hotel systems, allowing threat actors to harvest login data for booking platforms like Booking.com and Expedia. These stolen credentials were later sold on cybercrime forums or directly used to send fraudulent emails as part of larger financial scams.

#2

One particularly notable case began with a malicious email sent to a hotel's administrative or reservation desk, crafted to appear as a legitimate inquiry from Booking.com. The email contained a malicious link that triggered a redirection mechanism dubbed ClickFix, which compromised the recipient's machine through social engineering. Once infected, the attackers gained control of the hotel's Booking.com account, which they later sold or used to send realistic banking phishing messages to unsuspecting guests. Victims were often deceived into thinking there was a billing issue, leading them to pay twice for the same reservation, hence the report's fitting title, "I Paid Twice."

#3

The ClickFix attack chain relied on cleverly constructed URLs that followed a predictable pattern. These links redirected users through a series of web pages using JavaScript and HTML meta tags that forced full-page redirects outside of iframes. Ultimately, the redirection led to a malicious site impersonating Booking.com, which prompted users to execute a PowerShell command disguised behind a fake reCAPTCHA verification. Many of these redirecting domains shared a single IP address hosting numerous domains, some of which served pornographic or fake websites. This suggests the attackers used a Traffic Distribution System (TDS) to manage redirections and obscure the infrastructure behind their operations.

#4

Upon execution, the PowerShell command downloaded additional scripts that collected system data and fetched a ZIP archive from a compromised legitimate website. The archive contained binaries that exploited DLL side-loading to stealthily deploy PureRAT directly into memory. Once active, PureRAT established persistence via Windows registry keys and communicated securely with its Command-and-Control (C2) servers. Its modular design allowed it to execute commands, exfiltrate sensitive data, control user interfaces remotely, and even capture webcam or microphone feeds, all without leaving obvious traces on disk.

#5

This campaign sheds light on a growing cybercrime ecosystem targeting the hospitality sector. Compromised Booking.com extranet credentials are now a lucrative commodity, sold through Russian-speaking forums and Telegram bots. Organized groups, known as "traffers," distribute malware at scale in exchange for profit shares, while specialized "log checkers" verify the authenticity of stolen credentials. Together, these actors form a professionalized underground market that enables large-scale fraud against hotels and guests.

Recommendations



Verify Before You Click: Always double-check the sender’s email address and the content before opening attachments or clicking on links, even if the message looks like it’s from Booking.com or another trusted brand. If anything feels off, such as unusual urgency, payment requests, or unfamiliar links, contact the company directly through their official website or app.



Secure Your Booking and Hotel Accounts: Hotel administrators should use strong, unique passwords and enable multi-factor authentication (MFA) on all booking platform accounts. Regularly review login activity and immediately revoke access if suspicious logins appear.



Train Staff on Phishing Awareness: Employees who handle reservations or payments are often the first targets. Conduct regular awareness sessions showing how phishing emails look, what red flags to spot, and how to safely report suspicious messages.



Monitor Network and PowerShell Activity: Keep an eye on unusual PowerShell executions, registry modifications, or processes making network connections. These are common signs of PureRAT or similar malware.



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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link
T1586 Compromise Accounts	T1586.002 Email Accounts	T1204 User Execution	T1204.001 Malicious Link

<u>T1656</u> Impersonation	<u>T1204.004</u> Malicious Copy and Paste	<u>T1059.001</u> PowerShell	<u>T1082</u> System Information Discovery
<u>T1547</u> Boot or Logon Autostart Execution	<u>T1547.001</u> Registry Run Keys / Startup Folder	<u>T1574</u> Hijack Execution Flow	<u>T1574.001</u> DLL
<u>T1056</u> Input Capture	<u>T1056.001</u> Keylogging	<u>T1027</u> Obfuscated Files or Information	<u>T1071</u> Application Layer Protocol
<u>T1071.001</u> Web Protocols	<u>T1518</u> Software Discovery	<u>T1518.001</u> Security Software Discovery	<u>T1113</u> Screen Capture
<u>T1055</u> Process Injection	<u>T1055.012</u> Process Hollowing	<u>T1555</u> Credentials from Password Stores	<u>T1555.005</u> Password Managers
<u>T1041</u> Exfiltration Over C2 Channel	<u>T1005</u> Data from Local System	<u>T1036</u> Masquerading	<u>T1090</u> Proxy
<u>T1057</u> Process Discovery	<u>T1573</u> Encrypted Channel	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.007</u> JavaScript

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[://]headkickscountry[.]com/lz1y, hxxps[://]activatecapagm[.]com/j8r3, hxxps[://]homelycareinc[.]com/po7r, hxxps[://]byliljedahl[.]com/8anf, hxxps[://]byliljedahl[.]com/8anf, hxxps[://]jamerimprovementsllc[.]com/ao9o, hxxps[://]seedsuccesspath[.]com/6m8a, hxxps[://]zenavuurwerkofficial[.]com/62is, hxxps[://]brownsugarcheesecakebar[.]com/ajm4, hxxps[://]hareandhosta[.]com/95xh, hxxps[://]zenavuurwerkofficial[.]com/62is, hxxps[://]customvanityco[.]com/izsb, hxxps[://]byliljedahl[.]com/lv6q,

TYPE	VALUE
URLs	hxxps[:]//]ctrlcapaserc[.]com/bomla, hxxps[:]//]bknqsercise[.]com/bomla, hxxps[:]//]bkngssercise[.]com/bomla, hxxps[:]//]bkngpropadm[.]com/bomla, hxxps[:]//]cquopymaiqna[.]com/bomla, hxxps[:]//]emprotel[.]net[.]bo/updserc[.]zip, hxxps[:]//]cabinetifc[.]com/upseisser[.]zip, hxxps[:]//]ctrlcapaserc[.]com/loggqibkng, hxxps[:]//]bqknsieasrs[.]com/loggqibkng, hxxps[:]//]confirmation887-booking[.]com/17149438, hxxps[:]//]verifyguest02667-booking[.]com/17149438, hxxps[:]//]guest03442-booking[.]com/17149438, hxxps[:]//]confirmation8324-booking[.]com/17149438, hxxps[:]//]cardverify0006-booking[.]com/37858999, hxxps[:]//]verifycard45625-expedia[.]com/67764524
Domains	whooramisercisea[.]com, whooramisercise[.]com, aidaqosmaioa[.]com, bqknsieasrs[.]com, update-infos616[.]com, mccplogma[.]com, mccp-logistics[.]com, cquopymaiqna[.]com, contmasqueis[.]com, update-info1676[.]com, admin-extranet-reservationsinfos[.]com, eiscoaqscom[.]com, comsquery[.]com, caspqisoals[.]com, ctrlcapaserc[.]com, admin-extranet-reservationsexp[.]com, admin-extranetmngrxz-captcha[.]com, admin-extranetrservq-cstmrq[.]com, admin-extranetadmns-captcha[.]com, extranet-admin-reservationssept[.]com, bkngssercise[.]com, admin-extranetmnxz-captcha[.]com, bknqsercise[.]com, admin-extranetadm-captcha[.]com, bookreservfadrwer-customer[.]com, bookingadmin-updateofmay2705[.]com, breserve-custommessagehelp[.]com, confvisitor-doc[.]com, confirminfo-hotel20may05[.]com, guestinfo-aboutstay1205[.]com, confsvitor-missing-items[.]com,

TYPE	VALUE
Domains	guesting-servicesid91202[.]com, booking-agreementstatementapril0429[.]com, booking-agreementaprilreviews042025[.]com, booking-viewdocdetails-0975031[.]com, booking-agreementstatementapril0225[.]com, api-notification-centeriones[.]com, booking-visitorviewdetails-64464043[.]com, booking-reservationsdetail-id0025911[.]com, booking-refguestitem-09064111[.]com, reserv-captchaapril04152025[.]com, booking-reviewsguestpriv-10101960546[.]com, booking-aprilreviewstir-9650233[.]com, booking-confviewdocum-0079495902[.]com, booking-confview-doc-00097503843[.]com, booking-reservationinfosid0251358[.]com, sqwqwasresbkng[.]com
SHA256	703355e8e93f30df19f7f7b8800bd623f1aee1f020c43a4a1e11e121c53b 5dd1, 5301f5a3fb8649edb0a5768661d197f872d40cfe7b8252d482827ea2707 7c1ec, 64838e0a3e2711b62c4f0d2db5a26396ac7964e31500dbb8e8b1049495 b5d1f3
IPv4:Port	85[.]208[.]84[.]94[:]56001, 77[.]83[.]207[.]106[:]56001

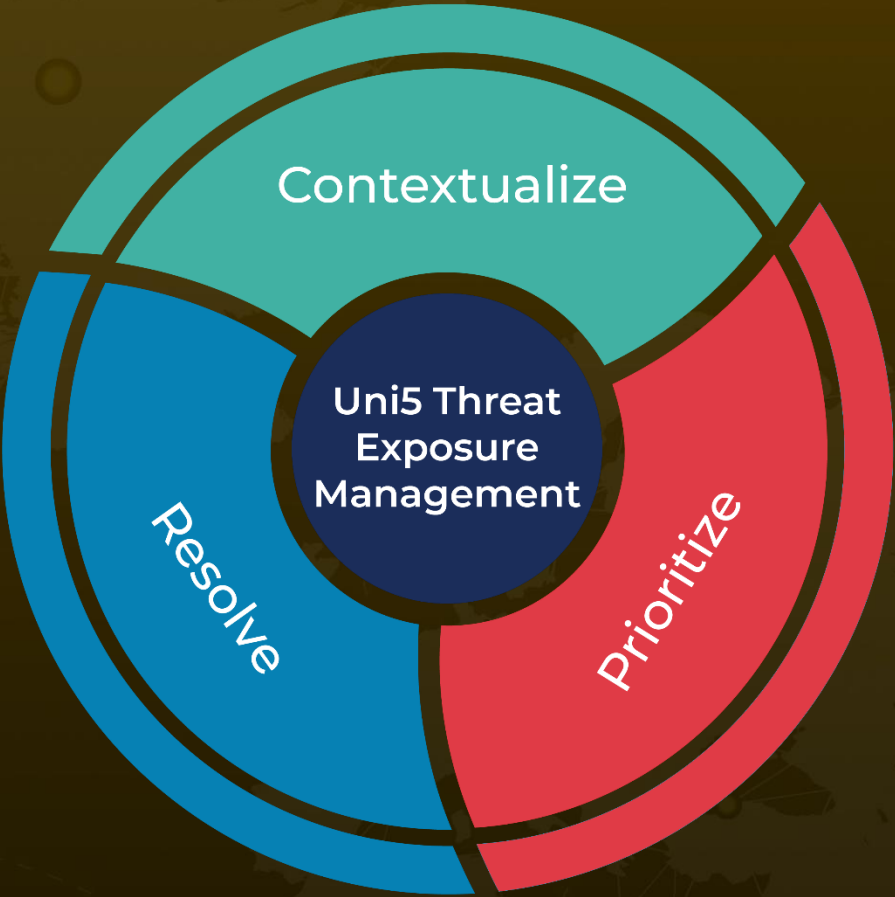
References

<https://blog.sekoia.io/phishing-campaigns-i-paid-twice-targeting-booking-com-hotels-and-customers/>

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
November 11, 2025 • 6:00 AM

