

Booking.com Phishing Campaign Targeting Hotels and Customers


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

Jeremy Scion, Quentin Bourgue and Sekoia TDR

November 6, 2025



[Jeremy Scion, Quentin Bourgue and Sekoia TDR](#) November 6 2025

 23 minutes reading

This article was originally distributed as a private report to our customers.

Table of contents

-
-
-

Introduction

A Sekoia partner recently reported a **phishing campaign targeting hospitality industry customers** worldwide. The campaign was observed to involve either emails sent from a hotel's compromised Booking.com account or messages distributed via WhatsApp. This activity proved particularly effective because the threat actor possessed customer data, including personal identifiers and reservation details, which further increased the credibility of the phishing attempts.

Sekoia.io analysts assess that the campaign stemmed from a **broader operation** that began earlier with the deployment of **infostealing malware**. The malware likely infected machines across multiple **hotel establishments**, enabling the theft of professional **credentials granting access to booking platforms** (e.g. Booking.com, Expedia). Threat actors then either sold the harvested credentials on cybercrime forums or leveraged them directly to send fraudulent emails to hotel customers, often as part of banking fraud schemes.

TDR uncovered a specific campaign that stood out for its sophisticated tactics and persistence. The intrusion began with a malicious email sent from a compromised address to a hotel reservation or administration email. The subject line referred to a customer request, while the email body reproduced the Booking.com brand identity to convince the recipient of its authenticity. The email included a URL that ultimately led to the **compromise of the victim machine** through the **ClickFix** social engineering tactic.

Once compromised, Booking professional accounts are typically sold and then exploited by other actors to deliver **targeted banking phishing emails to hotel guests**.

Sekoia.io analysts named the report "*I Paid Twice*" after the subject line of an email from a defrauded client. We assess with high confidence that the client who fell victim to this fraudulent scheme paid twice for his reservation: one at the hotel and once to the cybercriminal.

This report provides a detailed overview of the ClickFix campaign leveraged by threat actors to compromise hotel establishments and subsequently target their customers. Furthermore, it examines activities within the related cybercrime ecosystem.

From Hotels to Guests: the First Breach

The analysed campaign has been active since at least April 2025 and remained in operation as of early October 2025. This campaign is one of several that were observed targeting booking platform accounts. In March 2025, [Microsoft documented](#) a comparable operation that pursued

similar objectives but distinct TTPs.

Malicious emails

In the campaign analysed by TDR, the attacker's modus operandi involved using a compromised email account to send malicious messages to multiple hotel establishments. After reviewing messages linked to this campaign since early September, we are highly confident that the sender's address was compromised, since most of the emails originated from legitimate corporate accounts. In some instances, the **"From" header** was altered to impersonate Booking.com. Below is a list of observed subject lines from Sekoia SOC platform telemetry:

- *New last-minute booking ({REF} + DATE)*
- *New guest message in reference to your unit – Tracking code:{ID}*
- *New guest message linked to your listing – Ref:{ID}*
- *New guest message about the guest record Log:{ID}*
- *New guest message about reservation – Tracking code:{ID}*
- *New guest message related to your listing Ref:{ID}*

The same compromised email address was used to target several hotels across multiple countries. This suggests the attacker used a compromised account with no actual reservation to contact the hotels.

In October 2023, the cybersecurity researcher *g0njxa* published a [Medium article](#) describing how threat actors create fraudulent Booking.com accounts to make cancellable reservations solely to contact hotels. While this technique differs from the current campaign, it nonetheless underscores the continuing criminal interest in professional credentials that provide access to booking platforms.

ClickFix infection chain

Step 1: redirection steps

The malicious email sent by the attacker contained a URL that pointed to a redirection infrastructure. Each URLs followed the pattern: `hxxps://{randomname}[,].com/[a-z0-9]{4}`.

Upon visiting, the URL redirects users to a web page hosting a JavaScript with an asynchronous function that, after a brief delay, checks whether the page was displayed inside an iframe.

- If so, the function reportedly forces navigation of the top frame in order to remove the user from the iframe context and thereby redirect the entire browser.
- Else, it redirects the current window.

The objective is to redirect the user to the same URL but over HTTP. That resulting page contains only meta tags including the refresh tag `http-equiv='refresh' content='0'`, which instantly forwarded the victim to the ClickFix URL.

As of October 2025, all identified redirection domains resolved to a single IP address. A passive DNS lookup revealed nearly a hundred domain names associated with that IP. Further investigations of those domains reveal redirections to pornographic sites or sites impersonating legitimate software. This redirection infrastructure appears to be a service allegedly used by the attacker to conceal their ClickFix infrastructure and protect it from takedown, possibly a commercialised Traffic Distribution System (TDS).

Step 2: ClickFix tactic

We uncovered that the page hosting the JavaScript used Booking's branding and that the URL contained patterns such as admin and extranet, suggesting access to the hotel booking extranet and thereby lending legitimacy to the page for the victim, who was then prompted to copy a command using the ClickFix reCAPTCHA tactic. The copied and subsequently executed command included PowerShell instructions to compromise the machine with malware.

Pivoting on the IP address associated with the ClickFix URL unveiled numerous other malicious domains. Several of those domains include the admin and extranet patterns, and some even used booking.admin-extranet. Investigations of these domains uncovered URLs with a consistent /bomla path that delivered the same malicious PowerShell script.

Notably, even with an iOS user agent, the server still returned a PowerShell command. This suggests the attacker does not possess a payload compatible with the macOS ecosystem.

Step 3: malware delivery

The infection initiates when the victim executes the PowerShell command copied from the ClickFix page. That command downloads and executes further PowerShell instructions from the attacker's staging URL ending in /bomla. Those instructions perform the following actions:

- **Gathers system information**, including machine name, current user, Windows version, and installed antivirus product.
- **Downloads a ZIP archive** and extracts it into the current user's AppData\Local directory. The archive contains one .exe and three .dll files.
- **Creates a Run registry key** under \CurrentVersion\Run associated with a PowerShell command to run the .exe binary extracted from the ZIP archive.
- **Creates a shortcut file** (.lnk) in AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup, which intends to execute the .exe binary extracted from the ZIP archive. Execution of the binary led to the **infection of the machine via PureRAT**.
- **Reports status updates** to its Command and Control (C2) at each step (download, extraction, persistence, execution) to indicate the successful progression of the action. Collected system information and a GUID associated with the infection are also sent to the server.

The .exe binary triggers **DLL side-loading**, loading one of the malicious DLLs from the ZIP archive. This DLL acts as a **loader** and performs several tasks:

- **Establishing persistence** via a Run registry key. The associated command sets the AppData directory containing the binary and DLLs as the execution directory and runs the binary in order to sideload the DLL.
- **Loading the PureRAT** malware into memory by reflective loading, using AddInProcess32.exe to load an assembly into memory. The malware therefore never exists on disk (fileless).

At the time of writing, we continue analysing this loader, which does not match any known malware family in our databases. It appears to operate like QuirkyLoader, a .NET loader compiled Ahead-of-Time (AOT).

The PowerShell C2 domain resolves to the same IP address as the ClickFix domains. However, the ZIP archive was hosted on a legitimate website, which was very likely compromised.

An analysis of past campaigns revealed that, in addition to the /bomla pattern used in the ClickFix command, the ZIP archives were consistently named updserc.zip. These patterns were described as reliable indicators of potential compromise.

PureRAT Malware

PureRAT, also known as PureHVNC and ResolverRAT, is a Remote Access Trojan (RAT) sold as a Malware-as-a-Service (MaaS) by its alleged developer PureCoder. According to details on PureCoder's former website, distribution of its products began in March 2021. As documented by [AnyRun](#), PureCoder's malware are also sold via a Telegram bot, automatising and anonymising the purchase of malicious software. In addition to PureRAT, PureCoder offers other malware, notably the stealer PureLogs (aka zgRAT) and the crypter PureCrypter, both [documented](#) during a campaign targeting MSSQL honeypots.

Its capabilities include remote user interface access (VNC-like), mouse and keyboard control, webcam and microphone capture, keylogging, file upload/download, traffic proxying, data exfiltration, and remote execution of commands or binaries. These features are implemented

modularly: the core binary can fetch and load plugins to extend its capabilities based on the operator's objectives.

Furthermore, PureRAT is **protected by .NET Reactor**, a software-protection and licensing system that obfuscates the code and prevents reverse engineering. This adds a layer of complexity for analysts attempting to examine the malware, as it protects assemblies from static analysis and hampers code inspection.

Persistence: In the observed case, PureRAT establishes persistence by creating a Run registry key. On Sekoia Defend, this behavior is caught by the *Malware Persistence Registry Key* detection rule.

C2 communications : It communicates over TCP/TLS, primarily using ports 56001, 56002 and 56003. The transport layer is encrypted (TLS), and internal configurations/packages are often compressed (gzip) and serialised. Once the TLS connection to the C2 server is established, it sends system information such as the hostname, operating system, installed antivirus software, and a screenshot, to the C2 server at the start of the communication.

Plugin extensions : PureRAT implements a plugin model: following initialisation and the sending of system fingerprints (VictimID, AV information, paths of targeted applications), the C2 server can deliver plugins, which are stored and dynamically loaded into memory. Observed plugins include:

- **PluginRemoteDesktop:** Remote control of the interface (mouse/keyboard control, screenshot capture).
- **PluginExecuting:** Downloading and executing files, updating, uninstalling, in-memory execution (process hollowing/injection). This plugin provides several commands, including *DownloadAndExecuteDisk*, *DownloadAndExecuteMemory*, *UninstallConnection*, and *RestartConnection*.
- **Targeted theft modules:** Collection of extensions, wallets, password managers, and 2FA authenticators (scanning known paths/applications).
- **Exfiltration mechanisms:** Compression and sending of data via the encrypted C2 channel. The logic for storing/loading plugins (writing to HKCU\Software\{VictimID}, extraction and in-memory loading) has been documented in multiple analyses.

Booking Partners' Data and Customer Funds at Risk

The fraud scheme targeting hotel customers

In the case reported by our partner, the hotel's customers were contacted via WhatsApp or email. In both cases, the messages contain legitimate reservation details of the target. The message claimed an alleged security issue had occurred during the verification of the customer's banking details and urged them to confirm their information. To strengthen the credibility of the message,

the attacker explained that this was a procedure implemented by Booking to protect against cancellations. To validate its banking details, the victim was invited to visit a URL, which led to the phishing page.

The phishing page mimics Booking.com's typography and layout, and was designed to harvest victim's banking information. It is protected by Cloudflare and its antibot mechanism Cloudflare Turnstile. Infrastructure analysis revealed the page's IP address behind Cloudflare, which is located in Russia and belongs to the autonomous system AS216341 (OPTIMA LLC). The commercial site for this ASN appears to be an empty shell, pointing to another Russian hosting provider reg[.]ru. Abuse reports sent to the listed contact went unanswered, suggesting that this ASN operates as a BulletProof Host (BPH).

Analysis of the page enabled us to develop a tracking heuristic for this phishing cluster. By tracking associated phishing pages, we found that in addition to Booking.com, the Expedia brand was also impersonated. This confirms that the attacker targeted customers of various booking platforms.

The cybercrime ecosystem targeting Booking.com

Alongside the phishing campaigns detected in the Sekoia SOC platform telemetry, we have uncovered various underground activities concerning Booking.com data on Russian-speaking cybercrime forums. Since 2022, the cybercrime ecosystem has massively begun discussing campaigns involving phishing, data harvesting, and fraud targeting Booking.com's partners and customers. Since then, we have identified multiple publications offering malicious services, facilitating the buying and selling of data, including harvested information related to Booking.com accounts.

The following sub-sections provide an overview of the main discussions on cybercrime forums that involve Booking.com data and are closely associated with the phishing campaigns analysed in this report.

Booking-management accounts

Conducting successful phishing campaigns targeting administrators of Booking.com establishments requires early gathering of their contact information, which is not necessarily publicly released. This notably allows attackers to identify a list of vetted contacts and to send them emails or messages via messaging platforms, such as WhatsApp, Facebook, and others.

To this end, certain threat actors have specialised in collecting email addresses from high-value hotel establishments. Their primary methods involve parsing hospitality-industry websites, and extracting data from existing databases.

On cybercrime forums such as LolzTeam, which presents itself as a social engineering community, cybercriminals offer services for harvesting Booking.com partner emails or selling databases of hotel administrators' contacts. Database prices vary considerably depending on data quality, freshness, and exclusivity, but also on the degree to which data is processed. For example, bulk database sales start at tens of dollars, while those tailored by country or hotel category are charged per email at higher rates (with fees typically negotiated privately), or sometimes calculated as a percentage of the funds extracted from a compromised Booking.com account.

In some cases, these malware delivery campaigns also leverage drive-by downloads via malvertising, SEO poisoning, or social networks. Therefore, this approach does not require obtaining a list of email addresses, but rather relying on generating targeted traffic from hotel administrators to malicious web content.

Distributing Booking.com phishing

Once attackers have compiled a list of email addresses of interest, they conduct targeted phishing campaigns aimed at compromising hotel administrator's systems with malware, typically an infostealer or a remote access trojan (RAT).

According to publications observed on cybercrime forums, this attack phase is sometimes outsourced to specialists in distributing malware, also known as "traffers". The figure below illustrates a threat actor recruiting a traffer to spread its Booking.com phishing, preferably sourcing traffic from Twitter, Facebook and Google. The cybercriminal offers to the collaborator a share of the illicit financial gain.

Such groups of attackers organising themselves to distribute malware through specific delivery methods and share profit are very common in the Russian-speaking cybercrime ecosystem, often referred to as “[traffers teams](#)”. Most of them spread malicious content at scale using drive-by download attacks or target specific communities (web3, cryptocurrency, NFTs) with tailored fraudulent schemes. The actors conducting hospitality-industry phishing are even more specialised, and we assess with high confidence that they are fewer in number and likely organised into closed communities. Traffers specialised in generating traffic from the hospitality-industry are less common on open cybercrime forums.

Business of logs

Booking.com extranet accounts play a crucial role in fraudulent schemes targeting the hospitality industry. Consequently, data harvested from these accounts has become a lucrative commodity, regularly offered for sale in illicit marketplaces.

Attackers trade these accounts as authentication cookies or login/password pairs extracted from infostealer logs, given that this harvested data typically originates from malware compromise on hotel administrators’ systems. An infostealer log refers to the collection of stolen credentials and files from an infected system.

On cybercrime forums and marketplaces, these Booking.com logs are sold either individually or in bulk. As with most commercialised infostealer logs, high-quality entries are sold at unit prices, ranging from \$5 to \$5000, whereas poor quality logs are sold in bulk from \$0.20 to \$2, or even cheaper. For infostealer logs, the quality depends on factors such as exclusivity, freshness, geolocation, and the number of authentication data associated with the log.

The value of a Booking.com log also varies based on the number of establishments administered by the account, the volume of reservations, and the Genius partner tier. All these factors influence cybercriminals' potential profits from compromised accounts. Consequently, access to extranet accounts managing multiple hotels in a developed country with numerous active reservations can be put for sale for several thousand dollars.

In 2025, the threat actor operating under the moniker `moderator_booking` actively promoted a Booking log purchasing service on **cybercrime forums, including Exploit.in, LolzTeam, and WWHClub**. The attacker claims to collaborate “with a team of like-minded people who have earned over \$20M in this field”. According to its advertisements, `moderator_booking` purchases Booking logs that include affiliate program access and active reservations at prices from \$30 to \$5000 for high-value entries. The threat actor also offers remuneration based on a percentage of the profit.

Of note, in 2025, moderator_booking expanded its service to include Expedia, Airbnb and Agoda logs. TDR analysts assess with high confidence that the same *modus operandi* used against Booking.com partners extends to other accommodation booking platforms. Cybercriminals likely broadened their targeting to maximise profits.

Additionally, we have identified a threat actor who deployed a Telegram bot to purchase Booking.com logs, highlighting the professionalisation of the market for Booking extranet accounts. The threat actor seeks regular sellers and long-term partnerships, likely to purchase a high volume of extranet accounts. We assess with medium confidence that this threat actor could be embedded in a team conducting Booking.com fraud and requires a continuous influx of logs to support multiple collaborators.

Checking harvested Booking accounts

To verify a log validity, *i.e.* to confirm that harvested credentials still grant access to the associated Booking.com account, cybercriminals use dedicated software to automatically parse and test the authentication details. These tools, known as “log checkers”, generally authenticate compromised accounts via proxies and emulate HTTP headers that mimic legitimate traffic. Testing is designed to avoid detection by intrusion detection systems at the authentication services.

On cybercrime forums, attackers frequently express interest in purchasing log checkers for Booking.com accounts. In addition to validating credentials, some of them seek account metadata, such as region, number of establishments, and the number of active reservations. Prices for log checkers tailored to Booking.com accounts generally start at \$40.

All the services mentioned above highlight the **prevalence of this *modus operandi* targeting Booking.com partners and customers for fraud**. Monitoring threat actors’ activities shows that these phishing campaigns, which result in the theft of customer funds, are **highly profitable** and widely adopted.

The proliferation of cybercrime services supporting each step of the Booking.com attack chain reflects a **professionalisation of this fraud model**. By adopting the “as-a-service” model, cybercriminals lower entry barriers and maximise profits.

Detection Opportunities

ClickFix infection via PowerShell

The execution of this infection chain within a sandbox monitored by Sekoia Defend was detected by several detection rules, notably those relating to the misuse of PowerShell, including:

- **PowerShell Download From URL** — detection of the initial ClickFix command.
- **Correlation Suspicious PowerShell Drop and Exec** — expected to detect the first phase of the infection.
- **Suspicious PowerShell Invocations** — detection based on the use of certain cmdlets, notably the creation of the Run registry key.
- **PowerShell Invoke Expression With Registry** — detects keywords from well-known PowerShell techniques to get registry key values.

Creating .lnk files in the Startup directory is commonly used by system administrators to configure enterprise workstation environments. However, depending on the context, a detection rule for this TTP may generate a large number of irrelevant alerts and would therefore require fine-tuning. Hunting queries often are a better approach for this technique.

The Sekoia Operating Language (SOL) query below allows to:

- Search for .lnk files added to the Startup directory via PowerShell.
- Count the number of unique hosts per file name and retain only low-prevalence files (seen on few machines), thereby excluding shortcuts added by system administrators, for whole computers.

```
events
| where timestamp >= ago(24h)
| where process.name == "powershell.exe"
| where file.path contains~ "startup" and file.path endswith ".lnk"
| aggregate dc_shortcut_by_host = count_distinct(host.name) by file.name
| where dc_shortcut_by_host < 5
```

Loader

As previously documented, persistence on the system is achieved by creating a **Run** registry key. This behaviour is detected by the **Malware Persistence Registry Key** rule. In addition, the loader's execution via DLL side-loading can also be detected, but this requires a specific configuration to capture *ImageLoad* events (Sysmon Event ID 7). To enable this, the following section was added to the Sysmon configuration.

```
<ImageLoad >
  <ImageLoaded condition="contains">AppData</ImageLoaded>
  <ImageLoaded condition="contains">Temp</ImageLoaded>
</ImageLoad>
```

After executing the infection chain in a sandbox monitored by Sekoia Defend, the SOL query below made it possible to trace the DLL side-loading.

```

events
| where timestamp >= ago(24h)
| where event.code == 7
| where process.executable contains~ "temp" or process.executable contains~ "appdata"
| where dll.path contains~ "temp" or dll.path contains~ "appdata"
| where action.properties.SignatureStatus != "Valid"
| select timestamp, host.name, user.name, process.pid, process.executable, dll.path,
dll.hash.sha256, action.properties.SignatureStatus, action.properties.Company,
action.properties.Description

```

The event contains the path of the loaded DLL and the binary that loaded it, along with hashes and signature information.

```

"Hashes":
"MD5=D4845669F7F56C6C4EB82147A1F82615, SHA256=9BAB404584F6A0D9D82112D6E017CFA37D0094D97E510
101D6A0132FD145DD32, IMPHASH=799E73863806DF2964D80D12CE4E61EA",
"SignatureStatus": "Unavailable",
"Signature": "-",
"User": "desktop-REDACTED\REDACTED",
"Image": "C:\Users\REDACTED\AppData\Local\Temp\randomname\microserciasmb32rv1.exe",
"ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}",
"SourceName": "Microsoft-Windows-Sysmon",
"Severity": "INFO",
"UtcTime": "2025-09-30 07:39:36.036",
"OriginalFileName": "StapedialMummeries.exe",
"ImageLoaded": "C:\Users\REDACTED\AppData\Local\Temp\randomname\jli.dll",
"Product": "Pits Abeigh",
"Keywords": "0x8000000000000000",
"RuleName": "-",
"Company": "Truculentness Ltd.",
"ProcessGuid": "{ad823bbf-8938-68db-0203-000000001e00}",
"Description": "Psycter hermaphrodites archphylarch hexasyllable eucalypteol.",
"Signed": "false"

```

In this case, the DLL was unsigned and its Description and Company Name fields contained random strings, which together constitute a strong set of indicators pointing to the DLL's malicious nature.

PureRAT

AddInProcess32.exe is a legitimate Windows component used primarily to host and execute COM add-ins, particularly in Microsoft Office applications. It loads .NET assemblies into isolated processes, providing modular functionality while maintaining application stability. However, threat actors can abuse this capability: by loading arbitrary assemblies, it can be leveraged as a loader for malicious code, allowing malware to execute entirely in memory. This reflective loading of assemblies is inherently difficult to monitor with tools like Sysmon, as no suspicious DLL file is written to disk. Nevertheless, anomalous behaviour of the AddInProcess32 process — such as unexpected network connections, unusual thread activity, or the loading of obfuscated assemblies — can be detected and constitutes strong indicators of compromise.

In this case, several indicators point to malicious behaviour:

- **Process tree:** As previously described, **AddInProcess32.exe** is invoked by the loader whose execution path is located in the AppData directory. This is not a normal parent process for AddInProcess32, which is usually launched by legitimate applications such as Microsoft Office. This unusual process relationship is a strong anomaly.
- **Network connections:** Once AddInProcess32 loads the PureRAT assembly, it initiates network connections to the C2 server. Under normal circumstances, AddInProcess32 does not perform network communication.
- **Certificate access:** In this instance, AddInProcess32 also accesses the machine certificate store, specifically
\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\EnterpriseCertificates\\Root\\Certificates, according to Windows Security Event Log ID 4656. This event shows a successful audit where AddInProcess32.exe requests access to certificate keys with AccessMask=0x3001F. Such access to the machine certificate store is not standard behaviour for this process.

These behavioural markers can be used to build a Sigma correlation rule to detect this malicious activity.

```

name: addinprocess
detection:
  selection:
    process.parent.executable|contains:
      - "appdata"
      - "temp"
    process.name: "AddInProcess32.exe"
    process.pid: "*"
  condition: selection
---
name: network
detection:
  selection:
    process.name: "AddInProcess32.exe"
    process.pid: "*"
    destination.ip: "*"
    destination.geo.country_iso_code: "*"
  condition: selection
---
name: cert
detection:
  selection:
    process.name: "AddInProcess32.exe"
    process.pid: "*"
    action.properties.ObjectName:
      "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\SystemCertificates\\ROOT\\Certificates"
  condition: selection
---
action: correlation
type: temporal
rule:
  - addinprocess
  - network
  - cert
group-by:
  - process.pid
  - host.name
timespan: 5m
ordered: false

```

Conclusion

Over the past few years, a **prevalent modus operandi** has emerged, actively **targeting hospitality professionals and their customers**. In these campaigns, attackers deploy malware against hotel administrators, **compromising their booking-management accounts**, including Booking.com, Expedia, and Airbnb. Once in control of these hacked accounts, cybercriminals **bill customers a second time for their already existing reservations**, extorting large amounts of money at scale.

Using telemetry from the Sekoia SOC platform, we uncovered a **widespread, persistent campaign targeting multiple hospitality establishments**. This campaign leverages spearphishing emails that impersonate Booking.com to redirect victims to malicious websites, employing the **ClickFix social engineering tactic to deploy PureRAT**. PureRAT access then allows attackers to compromise hotels' Booking.com accounts.

TDR analysts also examined fraudulent schemes that employ tailored **phishing pages impersonating Booking.com's billing service** to extort money from establishments' guests. Unveiling the adversary infrastructure revealed hundreds of malicious domains active for several months as of October 2025, demonstrating a resilient and likely profitable campaign.

Services offered on cybercrime forums have substantially **facilitated these campaigns**, targeting Booking.com hotels and customers, notably through the sale of compromised Booking.com extranet accounts.

To protect our customers from malware distribution and phishing campaigns against hotel establishments and their customers, Sekoia.io analysts will continue to proactively monitor this threat, tracking adversaries' infrastructure, analysing campaigns, and enhancing our Sekoia SOC platform's detection capabilities.

Thank you for reading this blog post. Please don't hesitate to provide your feedback on our publications by [clicking here](#). You can also contact us at [tdr\[at\]sekoia.io](mailto:tdr[at]sekoia.io) for further discussions or future IOCs.

IOCs

The indicators listed below are available in CSV format with additional metadata in [the SEKOIA-IO/Community GitHub repository](#).

ClickFix cluster

Initial phishing – Redirect URL

```
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[://]brownsugarcheeseecakebar[.]com/ajm4
hxxps[://]hareandhosta[.]com/95xh
hxxps[://]zenavuurwerkofficial[.]com/62is
hxxps[://]customvanityco[.]com/izsb
hxxps[://]byliljedahl[.]com/lv6q
```

ClickFix – PowerShell URL and payload

```
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
```

Cluster domains

whoaamiscisea[.]com
whoaamiscise[.]com
aiaqosmaioa[.]com
bqknsieasrs[.]com
update-infos616[.]com
mccplogma[.]com
mccp-logistics[.]com
cquopymaiqna[.]comThe indicators listed below are available in CSV format with additional metadata in the SEK0IA-IO/Community GitHub repository.
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
confsvisitor-missing-items[.]com
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

PureRAT – Staging payload and C2

```
hxxps[://]ctrlcapaserc[.]com/loggqibkng  
hxxps[://]bqknsieasrs[.]com/loggqibkng  
703355e8e93f30df19f7f7b8800bd623f1aee1f020c43a4a1e11e121c53b5dd1  
5301f5a3fb8649edb0a5768661d197f872d40cfe7b8252d482827ea27077c1ec  
64838e0a3e2711b62c4f0d2db5a26396ac7964e31500dbb8e8b1049495b5d1f3  
sqwqwasresbkng[.]com  
85.208.84[.]94:56001  
77.83.207[.]106:56001
```

Phishing targeting hotel customers

```
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
```

More IoCs associated with these phishing clusters targeting Booking.com partners and customers are available in Sekoia.io CTI feed.

Feel free to read other Sekoia.io TDR (Threat Detection & Research) analysis here:

- [TransparentTribe targets Indian military organisations with DeskRAT.](#)
- [Silent Smishing : The Hidden Abuse of Cellular Router APIs](#)
- [Global analysis of Adversary-in-the-Middle phishing threats](#)
- [ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery](#)
- [Detecting Multi-Stage Infection Chains Madness](#)
- [Sneaky 2FA: exposing a new AiTM Phishing-as-a-Service](#)

 [CTI](#)  [Cybercrime](#)  [Malware](#)  [phishing](#)