Phishing Eager Travelers

By Anna Chung, Swetha Balla

Published: 2021-09-15 · Archived: 2026-04-05 13:15:59 UTC

Executive Summary

Threat actors have always been adept at keeping abreast of worldwide trends – ranging from geopolitical to technical – and rapidly exploiting these trends for their benefit. The current pandemic is no exception. Unit 42 has previously reported on how cybercriminals have preyed on consumers during COVID-19 and on the use of COVID-19 themed phishing attacks impersonating brands like Pfizer and BioNTech. This article provides early warnings for the travel industry and global travelers by sharing information about various attack attempts targeting the travel industry.

At the beginning of the pandemic, when people all over the world scrambled to get protective supplies – personal protective equipment, sanitizer and toilet paper – threat actors tried to take advantage of supply issues by selling fake products. They also tried to trick people by purporting to be credible health organizations (such as the WHO) or pharmaceutical companies, all while the actual organizations and companies were trying to make sense of the virus and come up with metrics, protective measures and vaccines.

Although the pandemic is not over, as the world opens up borders and the vaccines slow down the spread of the virus, people who have been cooped up at home are eager to travel. Threat actors are taking advantage of this trend by using travel as a theme for phishing people and stealing data – account credentials, financial information and so on – subsequently selling this data in underground markets.

Here, we first show that there has been a substantial increase in the registration of travel-related phishing URLs in 2021. Second, we provide two real-life examples demonstrating attackers abusing the travel theme, including the Dridex malware distribution and the abuse of Firebase in phishing campaigns. Third, we talk about how threat actors use various data that they steal. Finally, we conclude with a discussion of best practices for both individuals and organizations.

Please note that Palo Alto Networks Next-Generation Firewall customers are protected from phishing attacks with various security services, including Advanced URL Filtering and WildFire.

Increase in Travel-themed Phishing

To conduct social engineering, threat actors have always leveraged malicious domains and URLs impersonating known brands and websites familiar to end users. The content served on these malicious domains or URLs is crafted to mislead end users, since they look and feel very similar to brands that users know.

Alternatively, threat actors also send phishing emails to end users to trick them into either downloading malicious attachments or clicking on links that lead to malicious content – website pages or attachments. Threat actors use

themes that invoke a sense of urgency (such as outstanding invoices) or appeal to the end user emotionally (such as travel-themed emails sent as the world opens up).

Increase in the Number of Travel-themed Phishing URLs

Unit 42 analyzed travel-themed phishing URLs created between October 2019 and August 2021. As seen in Figure 1 below, there is a gradual upward trend in the registration of phishing URLs starting early 2021, with a significant increase in June 2021. Though the new phishing URLs did not continue to be registered at quite the frenzied rate we saw in June, throughout the summer, threat actors created new travel-themed phishing URLs at a much higher level than at any time in 2020.

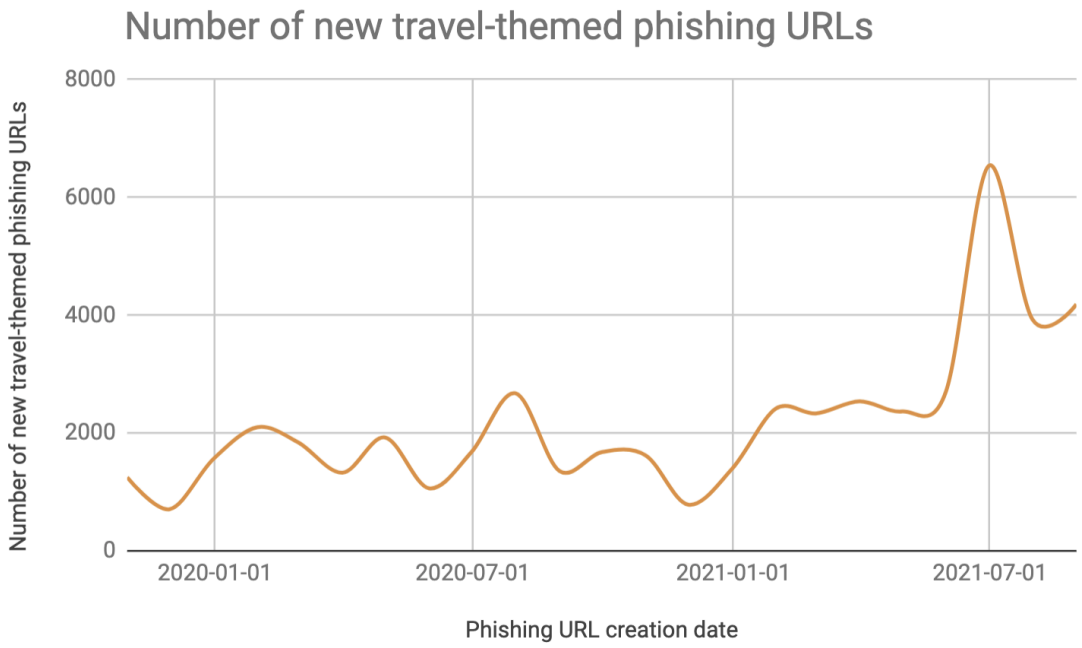

Figure 1. Number of new travel-themed phishing URLs registered between October 2019 and August 2021.

Based on the new phishing URLs that Unit 42 observed, in addition to the use of bespoke/new domains for serving the phishing URLs, threat actors also leveraged URL shorteners such as bit.ly and bit.do, and services such as Firebase that are hosted on Google Cloud Storage. Firebase is backed by Google and supports developers of mobile or web applications. Firebase includes cloud storage that enables developers to store and serve user-generated content. As Firebase leverages Google Cloud Storage, it is possible for phishing URLs to take advantage of it to bypass email protections based on Google's reputation.

Unit 42 observed that not all the phishing URLs that threat actors leveraged were used for directed attacks or campaigns; some of the URLs were used in malspam campaigns to host malicious content, such as Dridex.

Use of Travel-themed Phishing URLs by Dridex

Dridex is mass-distribution malware that is typically sent through malspam. Dridex has been known as an information-stealing malware or banking trojan that targets Windows platforms and is distributed via malicious

spam attachments impersonating legitimate companies.

The threat actor behind Dridex generally uses billing- or invoice-themed emails, a tactic used by most mass-distribution malware. The compromised or malicious URLs host the initial installer for Dridex to establish backdoor access. The backdoor access established by Dridex is later used to distribute followup malware, including ransomware, if the initial infection is not discovered.

The domains associated with the compromised URLs leveraged by Dridex are usually legitimate but compromised websites. For most Dridex campaigns, these URLs are used for a single day before the campaign moves on to a different URL.

Unit 42 researchers have observed two types of malspam pushing Dridex in the past few months: (1) a phishing email with an Excel spreadsheet attachment, and (2) a phishing email with a link to a message to download an Excel spreadsheet.

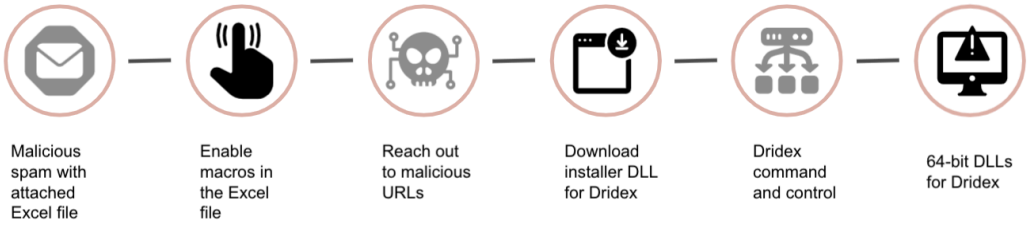

Figure 2. Infection chain for phishing emails with an Excel spreadsheet attachment.

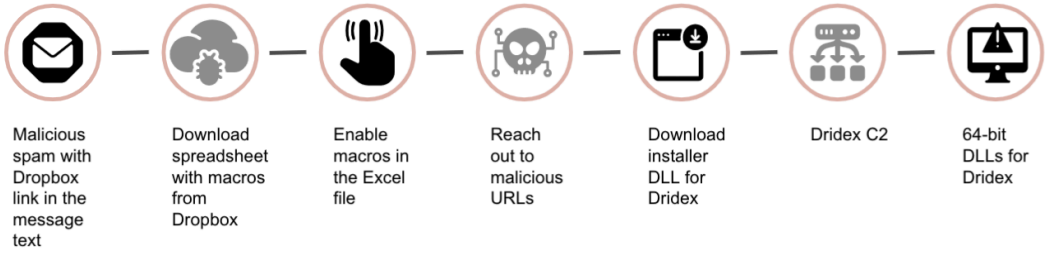

Figure 3. Infection chain for phishing emails linked to a message to download an Excel spreadsheet.

Unit 42 has published multiple articles over the past few years using the tag "Dridex."

From the newly registered phishing URLs, Unit 42 observed that a couple of phishing URLs with travel-related keywords – "airlines" and "vacation" – were used by Dridex in 2021. These URLs are:

- animalairlines[.]org/wp-content/plugins/wordpress-seo/inc/options/tk2xzwhphujenf.php
- soleravacation[.]net/wp-content/plugins/mojo-marketplace-wp-plugin-is-broke/inc/cli/mxq6awnfhnmadd2.php

Technical Details About

animalairlines[.]org/wp-content/plugins/wordpress-seo/inc/options/tk2xzwhphujenf.php

In January 2021, there was a malspam campaign that comprised emails that used Dropbox links to call animalairlines[.]org/wp-content/plugins/wordpress-seo/inc/options/tk2xzwhphujenf.php and download the malware DLL to install Dridex.

```
Received: from mail.emag.ro (91.206.36.5) by [information removed];
Wed, 13 Jan 2021 16:33:22 +0000
Date: Wed, 13 Jan 2021 16:14:59 +0000
Subject: Notification 42017.xls
From: [name removed] <[email address removed]>
To: "[name removed]" <[email address removed]>
Message-Id: <[information removed]>
Content-Language: en-US
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: multipart/alternative;
boundary="16105897430.113CCD.12443"

--16105897430.113CCD.12443
Content-Type: text/plain; charset="UTF8"
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

hi i have attached please see attached hxxps://www.dropbox[.]com/s/
2ecvxn2608g28as/Confidential%20961121.xls?dl=1

--16105897430.113CCD.12443--
```

Figure 4. Example email associated with the campaign.

The SHA256 values associated with some of the samples identified by Unit42 researchers are:

Hash	**Filename**
2741a353c6d7bc69bf43aef709ead2d6f452e895561943b01ad5359561506092	Rep_598531.xls
5134f99242ea705442aaf857d43c4e689cd117a64fe103353be7f8ec5fd165f4	Name unknown
6846ae3db07fdc05aa310d157f9300bd7d26c33e5e81594dc89b70b47c73ee43	Name unknown
80d50ab8fe6f880270a2d8c3646a2272efed3f7a68140afacb72317a2e0c42c7	Note_7706.xls
b25edec6855cd5c3b74fa1a897d33978a227ccd039ac175c71521ec3655ebe10	Information_24837.xls
f3c837323c135a7d7ed9d03f856c81463abb80174211117f4bda193a55f1b78e	Notification_30123.xls

A list of Dropbox URLs associated with this wave of malspam are:

- hxxps://www.dropbox[.]com/s/qmi112rc4ns75eb/Confidential_123.xls?dl=1
- hxxps://www.dropbox[.]com/s/pfs4wf7a8mzxxkf/Notification%20%23591501.xls?dl=1
- hxxps://www.dropbox[.]com/s/dz2b5ypqvoy7tpa/Reports%2078497.xls?dl=1
- hxxps://www.dropbox[.]com/s/azswbhh7gmxouk2/Rep%20%231018.xls?dl=1
- hxxps://www.dropbox[.]com/s/myz2ytmvd08vfl4/Invoice%20%2392899.xls?dl=1
- hxxps://www.dropbox[.]com/s/66j21yxz64fwfg2/Documentation%20644.xls?dl=1
- hxxps://www.dropbox[.]com/s/81pphar6s4e93vz/Detailed%20079.xls?dl=1
- hxxps://www.dropbox[.]com/s/yryqu9i368uib62/Report_%23_301.xls?dl=1
- hxxps://www.dropbox[.]com/s/1ds4kb2limantm5/Notification_836524.xls?dl=1
- hxxps://www.dropbox[.]com/s/yo9cy2y1su23ga1/Rep%20%23621.xls?dl=1
- hxxps://www.dropbox[.]com/s/zakw3n6nvxqoyav/Subconract%20415.xls?dl=1
- hxxps://www.dropbox[.]com/s/7vgj2bvv3vnd8dj/Note%20%2383008.xls?dl=1
- hxxps://www.dropbox[.]com/s/l1bl35aybsvu8wl/Notification_71823.xls?dl=1
- hxxps://www.dropbox[.]com/s/myoyguvb1qhrwsk/Reports_6633.xls?dl=1
- hxxps://www.dropbox[.]com/s/4xecieojug0y28l/Information%20714353.xls?dl=1
- hxxps://www.dropbox[.]com/s/glyefet40tkve8u/Contract%2030964.xls?dl=1
- hxxps://www.dropbox[.]com/s/6f1amba84r7sf4a/Inv%204529.xls?dl=1
- hxxps://www.dropbox[.]com/s/8y95urd2as2eeu8/Inv%20%23147.xls?dl=1
- hxxps://www.dropbox[.]com/s/9wj6fcxxw29sfcp/Contract_724269.xls?dl=1
- hxxps://www.dropbox[.]com/s/qu6npuiok79zpeo/Inv_225.xls?dl=1
- hxxps://www.dropbox[.]com/s/ckihhm4uaxfi5hs/Report_18392.xls?dl=1
- hxxps://www.dropbox[.]com/s/ryyogkwdvwof8rs/Scan%20108.xls?dl=1
- hxxps://www.dropbox[.]com/s/5jgm0ktunwiby10/Subconract_848.xls?dl=1
- hxxps://www.dropbox[.]com/s/luee4b7upuo2kak/Rep%20%23226186.xls?dl=1
- hxxps://www.dropbox[.]com/s/c6rqxbq9ydl2sd1/Reports%20%2348406.xls?dl=1
- hxxps://www.dropbox[.]com/s/4jczljfya09ye2o/Notification_30123.xls?dl=1
- hxxps://www.dropbox[.]com/s/f62i6djdmb4qm6b/Subconract_1541.xls?dl=1
- hxxps://www.dropbox[.]com/s/cvrhnc9h6e9ny1y/Contract_%23_599848.xls?dl=1
- hxxps://www.dropbox[.]com/s/5nz7l5ftiu48irm/Fax%20740.xls?dl=1
- hxxps://www.dropbox[.]com/s/atagwpkwhmpmvi4/Detailed_%23_670.xls?dl=1
- hxxps://www.dropbox[.]com/s/v0hmuvpunssgon3/Note%202365.xls?dl=1
- hxxps://www.dropbox[.]com/s/9779leob93657a9/Invoice_%23_76493.xls?dl=1
- hxxps://www.dropbox[.]com/s/agx2xx6bbpetdh7/Copy_%23_824.xls?dl=1
- hxxps://www.dropbox[.]com/s/l3d6i2x6f2ui9pk/Notice%200118.xls?dl=1

Once Dropbox was provided Palo Alto Networks threat intelligence, it immediately disabled sharing of those links and disabled the associated account to prevent further threat actor activity.

The URL hxxp://go7wallet[.]com/app/plugins/cordova-plugin-statusbar/src/browser/HLn3obcR1vMJZNt.php was also contacted as part of the campaign.

Technical Details About

soleravacation[.]net/wp-content/plugins/mojo-marketplace-wp-plugin-is-broke/inc/cli/mxq6awnfhnmadd2.php

In February and March 2021, there was a malspam campaign that comprised emails with Excel attachments to call soleravacation[.]net/wp-content/plugins/mojo-marketplace-wp-plugin-is-broke/inc/cli/mxq6awnfhnmadd2.php and subsequently download the malware DLL to install Dridex.

The SHA256 values associated with some of the samples identified by Unit 42 researchers are:

Hash	Filename
0edda7d9dfd825e5e69c1ae55e26adf6e7ade746492f48bff0c0cbcf4c924b84	Attach 05680.xlsm
4dc9b2f11546e5bf8fb9901809a0707ff1e23acdc52742b991ddff18ce03733c	Name unknown
bc30505fbd196a16346fc37c84ff8db3491fadc7c1b25e35b92954d570699eac	Name unknown
bcaac658e2d7b0a51112b76f75ff678082300a12225ae9226274dbddd94a270c	Invoice 689160.xlsm
c5c34cf419acecfbdb8c63fd603f11cbcf6ef84453bfe27a975f2295acb68be2	Attach 689160.xlsm
e7cef58dba5c455b29b55d4d670449a69708ef17ed2866732177ea3e9fdbb69b	Name unknown
ff5b57033bb5373fdebfe5efc84adcdd0bdddad382fa753b9c08483742401407	Name unknown

Of note for this particular campaign, the malicious spreadsheets try to connect to five or more URLs to retrieve Dridex, in addition to soleravacation[.]net/wp-content/plugins/mojo-marketplace-wp-plugin-is-broke/inc/cli/mxq6awnfhnmadd2.php.

Abuse of Firebase by Threat Actors

Threat actors have targeted multiple organizations within the travel industry and have used Firebase to host phishing pages to either target employees working in the travel industry or customers. Some of the organizations that have been targeted by Firebase-hosted web applications include an online marketplace for vacation rentals, upscale hotel chains, resort management companies and airline companies such as Tui.

As mentioned above, Firebase is backed by Google and supports developers of mobile or web applications, allowing them to store content in Google Cloud Storage. Unit 42 observed attackers taking advantage of the inherent legitimacy of the Google Firebase domain to deceive targets and to bypass security filters that block domains and files that are known to be malicious. Once Unit 42 notified Google, it immediately removed and blocked these phishing URLs to prevent further threat actor activity.

A sample of phishing URLs hosted on Firebase include:

URL	Purpose
firebasestorage[.]googleapis[.]com/v0/b/owambe-4ce77.appspot.com/o/arsenaldozens/index%20copy%202.html?	Targeting employees

alt=media%26token=bbb56e5d-96d2-4da7-a82f-e0bfed8d24c3%26email=creader@palaceresorts.com	working in the travel industry.
ehdewbml[.]firebaseapp[.]com/01iofurjdor.html#iuser=corp@tui.ru	Targeting employees working in the travel industry.

How Attackers Use the Data Gathered Through Phishing

Cybercriminals often want to monetize any "data" that they acquire through attacks, and data gathered about travelers or organizations operating in the travel sector is no different. We have observed that threat actors monetize data by selling stolen account credentials, stolen customer data or stolen payment information.

During the pandemic, Unit 42 researchers noticed the supply for travel-themed services and products in underground markets drastically decreased (see Figure 5), possibly due to the global travel restrictions. However, we expect that both supply and demand will increase as the world reopens for travel.

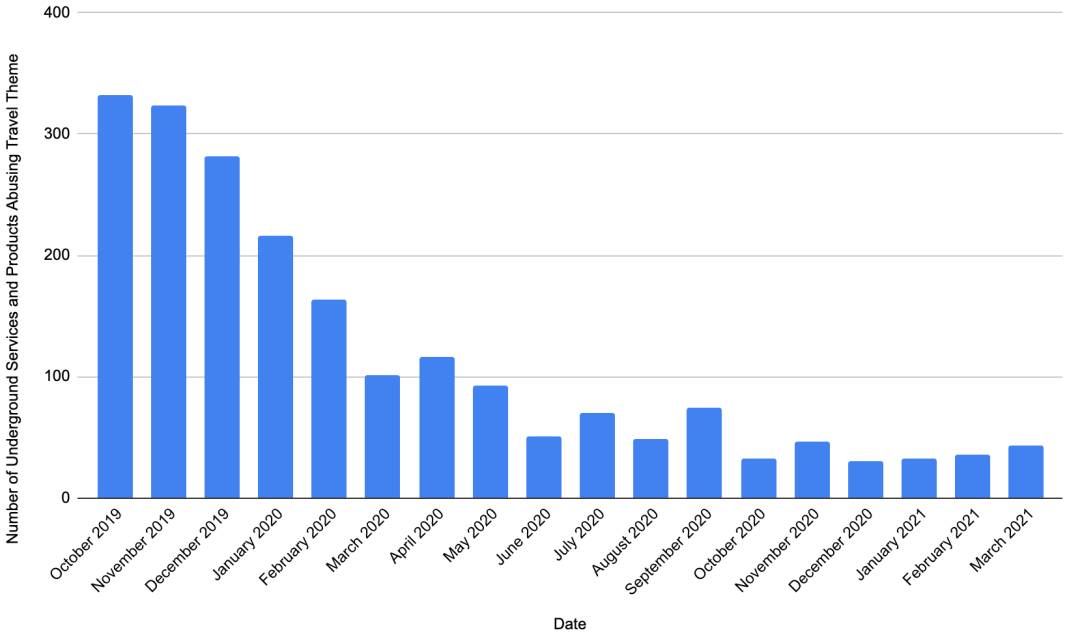

Figure 5. Travel-themed products and services listed in underground marketplaces, October 2019-March 2021. (Data for later months not available.)

Stolen Account Credentials

There are two main reasons criminals are attracted by data sets containing stolen usernames, emails and passwords. First, they give criminals access to victims' mileage or hotel points, which can easily be resold for profit. Second, the credentials can easily be used for compromising and taking over victims' accounts on other platforms, if the same credentials were used. With all the potential financial gains from stolen login credentials,

the strong demand in underground marketplaces encourages threat actors to actively acquire this data through social engineering, brute-forcing or exploiting vulnerable systems.

Stolen Customer Data

Organizations in the travel industry have access to a wealth of data, including personally identifiable information (PII), payment information and the contact information of customers. In the recent SITA passenger service system attack, 4.5 million global data subjects were compromised. While researchers attributed the attack to APT41, it was observed that financially motivated criminals also showed interest in this data.

There are three possible ways cybercriminals can abuse this type of data.

1. **Identity theft**: Using stolen individual information collected from website A to create new accounts on website B. Because victims are not aware of these accounts on website B, they are less likely to be notified until later.
2. **Reconnaissance**: Using the information for reconnaissance and setting the stage for spear phishing attacks.
3. **Resale of data**: Data can easily be resold to other criminals, fraudsters or illicit marketing service providers for further abuse.

Stolen Payment Information

Cybercriminals have been offering a “shadow travel agency” service for years. They reach out to individual travelers through various social media or instant messaging platforms such as Telegram, providing flight bookings, hotel reservations, car rentals, car rides and sightseeing tours with heavily discounted prices. While travelers transfer clean money to the “shadow travel agency,” the “shadow travel agency” pays the actual service providers such as hotels or airlines with stolen payment information. Due to the time gap in payment processing, service providers only realize they have been defrauded when they see the disputed card transactions or chargebacks weeks or months later.

There are three groups of victims in this scenario. The first victim group is the payment information owners and stolen credit card holders. The second victim group is the travelers who were unknowingly a part of the money laundering process, giving cybercriminals opportunities to cash out the stolen payment information they previously collected. Travel industry organizations are considered the third victim group; they are the most impacted in this scheme. Not only did they fail to profit from the products and services they provided, but they also had to cover the costs and chargeback penalties, as well as addressing the reputational impacts of the crime.

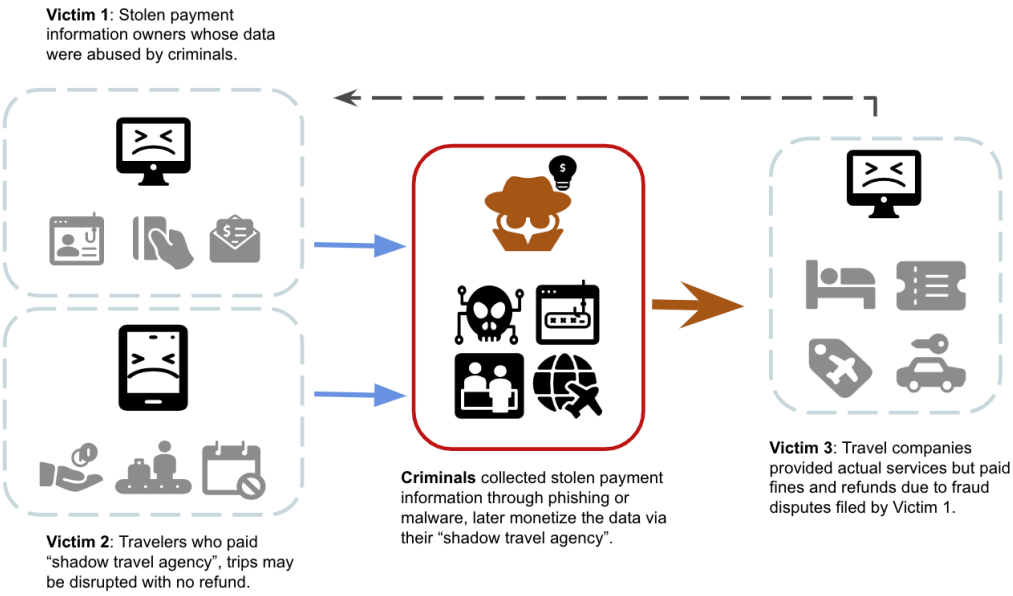

Figure 6. Abuse of stolen payment information by threat actors.

Conclusion

The travel industry and international travelers have been long-term targets for cybercriminals, suffering financial and reputational damage. Threat actors not only sell fabricated information but also stolen information that they gather through phishing attacks. During the pandemic, we noticed that travel-themed products and services offered by cybercriminals in underground marketplaces decreased significantly, possibly due to low demand. However, as travel resumes, we expect travelers and the travel industry to be targeted again due to the high profitability associated with this data. Therefore, it is important to be aware of phishing campaigns.

Best practices to protect yourself and your organization from phishing attacks include:

For individuals:

- Exercise caution when clicking on any links or attachments contained in suspicious emails, especially those relating to one's account settings or personal information, or otherwise trying to convey a sense of urgency.
- Verify the sender's address for any suspicious emails in your inbox.
- Double-check the URL and security certificate of each website before inputting your login credentials.
- Report suspected phishing attempts.

For organizations:

- Implement security awareness training to improve employees' ability to identify fraudulent emails.
- Regularly back up your organization's data as a defense against ransomware attacks initiated via phishing emails.
- Enforce multi-factor authentication on all business-related logins as an added layer of security.

Palo Alto Networks customers are protected by:

- Advanced URL Filtering: Detects unknown, newly malicious URLs in milliseconds instead of minutes, preventing successful attacks.
- WildFire: All known samples are identified as malware.
- AutoFocus: Tracking related activity using the Dridex tag.

Additional Resources

- Worldwide Phishing Attacks Ramped Up at the Peak of Working From Home
- Fake Websites Used in COVID-19 Themed Phishing Attacks, Impersonating Brands Like Pfizer and BioNTech
- COVID-19: The Cybercrime Gold Rush of 2020
- Studying How Cybercriminals Prey on the COVID-19 Pandemic

Acknowledgements

Special thanks to Bradley Duncan, Lucas Hu, Zhanhao Chen and Bennett Woo for all the insightful data and experience sharing.

Indicators of Compromise

URLs

- soleravacation[.]net/wp-content/plugins/mojo-marketplace-wp-plugin-is-broke/inc/cli/mxq6awnfhnmadd2.php
- animalairlines[.]org/wp-content/plugins/wordpress-seo/inc/options/tk2xzwhphujenf.php
- hxxp://go7wallet.com/app/plugins/cordova-plugin-statusbar/src/browser/HLn3obcR1vMJZNt.php
- hxxps://www.dropbox[.]com/s/qmi112rc4ns75eb/Confidential_123.xls?dl=1
- hxxps://www.dropbox[.]com/s/pfs4wf7a8mzxxkf/Notification%20%23591501.xls?dl=1
- hxxps://www.dropbox[.]com/s/dz2b5ypqvoy7tpa/Reports%2078497.xls?dl=1
- hxxps://www.dropbox[.]com/s/azswbhh7gmxouk2/Rep%20%231018.xls?dl=1
- hxxps://www.dropbox[.]com/s/myz2ytmvd08vfl4/Invoice%20%2392899.xls?dl=1
- hxxps://www.dropbox[.]com/s/66j21yxz64fwfg2/Documentation%20644.xls?dl=1
- hxxps://www.dropbox[.]com/s/81pphar6s4e93vz/Detailed%20079.xls?dl=1
- hxxps://www.dropbox[.]com/s/yryqu9i368uib62/Report_%23_301.xls?dl=1
- hxxps://www.dropbox[.]com/s/1ds4kb2limantm5/Notification_836524.xls?dl=1
- hxxps://www.dropbox[.]com/s/yo9cy2y1su23ga1/Rep%20%23621.xls?dl=1
- hxxps://www.dropbox[.]com/s/zakw3n6nvxqoyav/Subconract%20415.xls?dl=1
- hxxps://www.dropbox[.]com/s/7vgj2bvv3vnd8dj/Note%20%2383008.xls?dl=1
- hxxps://www.dropbox[.]com/s/l1bl35aybsvu8wl/Notification_71823.xls?dl=1
- hxxps://www.dropbox[.]com/s/myoyguvb1qhrwsk/Reports_6633.xls?dl=1
- hxxps://www.dropbox[.]com/s/4xecieojug0y28l/Information%20714353.xls?dl=1
- hxxps://www.dropbox[.]com/s/glyefet40tkve8u/Contract%2030964.xls?dl=1
- hxxps://www.dropbox[.]com/s/6f1amba84r7sf4a/Inv%204529.xls?dl=1
- hxxps://www.dropbox[.]com/s/8y95urd2as2eeu8/Inv%20%23147.xls?dl=1

- hxxps://www.dropbox[.]com/s/9wj6fcxxw29sfcp/Contract_724269.xls?dl=1
- hxxps://www.dropbox[.]com/s/qu6npuiok79zpeo/Inv_225.xls?dl=1
- hxxps://www.dropbox[.]com/s/ckihhm4uaxfi5hs/Report_18392.xls?dl=1
- hxxps://www.dropbox[.]com/s/ryyogkwdvwof8rs/Scan%20108.xls?dl=1
- hxxps://www.dropbox[.]com/s/5jgm0ktunwiby10/Subconract_848.xls?dl=1
- hxxps://www.dropbox[.]com/s/luee4b7upuo2kak/Rep%20%23226186.xls?dl=1
- hxxps://www.dropbox[.]com/s/c6rqxbq9ydl2sd1/Reports%20%2348406.xls?dl=1
- hxxps://www.dropbox[.]com/s/4jczljfya09ye2o/Notification_30123.xls?dl=1
- hxxps://www.dropbox[.]com/s/f62i6djdmb4qm6b/Subconract_1541.xls?dl=1
- hxxps://www.dropbox[.]com/s/cvrhnc9h6e9ny1y/Contract_%23_599848.xls?dl=1
- hxxps://www.dropbox[.]com/s/5nz7l5ftiu48irm/Fax%20740.xls?dl=1
- hxxps://www.dropbox[.]com/s/atagwpkwhmpmvi4/Detailed_%23_670.xls?dl=1
- hxxps://www.dropbox[.]com/s/v0hmuvpunssgon3/Note%202365.xls?dl=1
- hxxps://www.dropbox[.]com/s/9779leob93657a9/Invoice_%23_76493.xls?dl=1
- hxxps://www.dropbox[.]com/s/agx2xx6bbpetdh7/Copy_%23_824.xls?dl=1
- hxxps://www.dropbox[.]com/s/l3d6i2x6f2ui9pk/Notice%200118.xls?dl=1

SHA256 and Filenames

Hash	Filename
2741a353c6d7bc69bf43aef709ead2d6f452e895561943b01ad5359561506092	Rep_598531.xls
5134f99242ea705442aaf857d43c4e689cd117a64fe103353be7f8ec5fd165f4	Name unknown
6846ae3db07fdc05aa310d157f9300bd7d26c33e5e81594dc89b70b47c73ee43	Name unknown
80d50ab8fe6f880270a2d8c3646a2272efed3f7a68140afacb72317a2e0c42c7	Note_7706.xls
b25edec6855cd5c3b74fa1a897d33978a227ccd039ac175c71521ec3655ebe10	Information_24837.xls
f3c837323c135a7d7ed9d03f856c81463abb80174211117f4bda193a55f1b78e	Notification_30123.xls
0edda7d9dfd825e5e69c1ae55e26adf6e7ade746492f48bff0c0cbcf4c924b84	Attach 05680.xlsm
4dc9b2f11546e5bf8fb9901809a0707ff1e23acdc52742b991ddff18ce03733c	Name unknown
bc30505fbd196a16346fc37c84ff8db3491fadc7c1b25e35b92954d570699eac	Name unknown
bcaac658e2d7b0a51112b76f75ff678082300a12225ae9226274dbddd94a270c	Invoice 689160.xlsm
c5c34cf419acecfbdb8c63fd603f11cbcf6ef84453bfe27a975f2295acb68be2	Attach 689160.xlsm

---

Source: https://unit42.paloaltonetworks.com/travel-themed-phishing/