Threat Actors Prey on Eager Travelers

fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers

June 2, 2022

Sitting on a sunny beach full of sparkling sand. Exploring the jungle looking for exotic animals and plants. Diving into a deep blue sea where sunlight has a difficult time reaching. Partying all night at clubs in a city you have never been to. Holding hands with friends around a campfire singing Kumbaya. Eating warm food and drinking coffee in a cave in a snowy mountain.

Those are some of what recently seemed to be unattainable travel fantasies that many people around the globe have been dreaming of since Covid-19 started to rapidly spread in early 2020. We've come a long way since then. Today, vaccinations and quarantining have led some governments to soften some of the regulations that have restricted how we live our everyday lives. Such eased regulations include eliminating travel restrictions so tourists can fill those delayed dreams.

However, it's essential for eager travelers to understand that malicious actors are just as eager to leverage that feeling of liberty to deliver malware. This blog will provide a few examples of such attacks that FortiGuard Labs recently discovered.

Affected Platforms: Windows
Impacted Parties: Windows users
Impact: Controls victim's device and collects sensitive information
Severity Level: Medium

Adversaries Pushing Unsanitary Itineraries

Itineraries are one of the must-haves for most travelers. Without one, they won't know when, how, and where to go, where to stay, and when and how to come home. An itinerary can also provide details on how much time travelers have at the destination so they can plan activities.

AsyncRAT

FortiGuard Labs recently discovered a malicious file called "itinerary.zip" that was hosted on dc5b-163-123-142-137[.]ngrok[.]io.

Inside the archive file is a file entitled, "Itinerary.pdf_____.exe", which is really an .exe file disguised as a PDF. Hiding an .exe extension behind a long series of underscores is a classic trick that threat actors have used for decades. The fact it is still being used today indicates that the trick still has some success. While we do not know how victims were directed to the file, it's an easy guess that a travel-related email or website was used to lure the victims to the file's location.

Running the .exe file installs AsyncRAT on the victim's machine. AsyncRAT is an open-source Remote Access Trojan (RAT) written in .NET that has been used in a number of attacks. FortiGuard Labs has previously posted a blog on a spearphishing campaign that delivered AsyncRAT:

Spear Phishing Campaign with New Techniques Aimed at Aviation Companies

AsyncRAT provides remote access to attackers and allows them to remotely monitor and control a compromised machine through a secure encrypted connection. The RAT's features include keylogging, taking screenshots, and uploading and downloading files. This installed version of AsyncRAT connects to its C2 servers located at "znets[.]ddns[.]net" and "dnets[.]ddns[.]net". In an attempt to further hinder analysis, this AsyncRAT variant uses multiple .NET obfuscators such as Xenocode, Babel, Yano, DotNetPatcher, CryptoObfuscator, Dotfuscator, SmartAssembly, Goliath, NineRays, and 198 Protector V2.

Further investigation revealed that itinerary.zip was not the only file hosted on dc5b-163-123-142-137[.]ngrok[.]io. The files travel_details.iso, activities_and_dates.iso, and Itinerary.exe were also on the same domain and they also install AsyncRAT variants that connect to the same C2 servers.

An ISO file (often called an ISO image) is an archive file that contains the identical content (i.e. the folder and file hierarchy) of a physical disc such as a CD, DVD, or Blu-ray. ISO files used to require third-party software to open. However, the file type is now supported natively in Windows, starting in Windows 8. Unfortunately, this provides another infection method to the attackers. Furthermore, the .iso file format avoids being tagged with the Mark-of-the-Web (MOTW). MOTW forces saved webpages to run in the security zone of the location the page was saved from as a security measure. Files that are tagged with MOTW also usually go through additional safety checks, such as Microsoft Defender's SmartScreen and various AV scanning engines. This variant of AsyncRAT hides itself inside the .iso file format to dodge extra scanning and is a known technique.

Once the ISO image is mounted (typically done by simply double-clicking it), the victim needs to manually run the exe file in the mounted ISO to get infected with AsyncRAT.

Another AsyncRAT sample, "Booking details.exe", was observed in early February 2022. All of these samples have travel-themed filenames, which is a clear indication that the attacker specifically targeted travelers.

Figure 1. Files inside the mounted ISO images

Netwire RAT

Netwire RAT is another malware being delivered via a travel-themed infection vector. Flight_Travel_Intinery_Details.js is a malicious file FortiGuard Labs recently came across. Given the file was hosted on an oft-abused Discord CDN, combined with the filename, leads us to surmise that the malicious javascript was likely distributed through a link in an email or an attached document file associated with travel.

The javascript (.js) file eventually drops Update.exe, which is a variant of Netwire RAT that connects to its C2 server at kingshakes1[.]linkpc[.]net. This C2 server appears to have been used by Netwire RAT since May 2021 at the latest. Netwire RAT is a commodity Remote Access Trojan designed to work on Windows, OSX, and Linux. Just like AsyncRAT, Netwire RAT takes control of the compromised machine and performs malicious activities such as data exfiltration and reconnaissance.

Colombian Military Under Attack

Quasar RAT

Another example of a travel-themed cyberattack arrived in what appears to be a spearphishing attack against a military organization in Colombia.

The email has “Solicitud de Reserva para Mayo 2022” (English translation: “Reservation Request for May 2022”) as the email subject, with “RESERVA.ISO” as an attachment.

Figure 2. Screenshot of the email with a malicious ISO file sent to a military organization in Colombia

The message reads in English:

Good afternoon,

I hope you are well.

I am [removed] from the Product Dept. of AMV Travel.

I would like to request a reservation for 5 rooms in which we will be staying for a week. Please find attached the details of the reservation.

Thank you very much.

I am waiting for your reply to continue.

While an ISO file was also used in this attack, the payload is a different Remote Access Trojan, “Quasar RAT”. The use of Quasar RAT is not surprising because this RAT has a history of being used for cyberespionage in number of targeted attacks reported in blogs from various security vendors. One such example is in a blog, “Uncovering New Activity By APT10”, published by FortiGuard Labs in October 2019, where the APT10 threat actor group targeted government and private organizations with Quasar RAT. Because the malware is an open-source RAT and has been observed to have been widely used, CISA released “Analysis Report (AR18-352A)” on Quasar RAT in February 2019.

Quasar RAT is an open-source commodity RAT. As such, it’s not a unique tool for threat actors to have in their arsenal. The RAT is advertised to run on various versions of Windows OS (Windows 10, Windows 8/8.1, Windows 7, Windows Vista, Windows Server 2019, Windows Server 2016, Windows Server 2012 and Windows Server 2008). Older versions of Quasar RAT also work on older Windows OS versions. It supports features typical of Remote Access Trojans. These include:

- Keylogging
- Password recovery/stealing from common Web browsers and FTP Clients
- Upload/download & execute files
- Collect system information
- Remote desktop
- Registry editor

Like the AsynRAT attack, the Quasar RAT ISO file gets mounted when the ISO file is double-clicked. The victim must then manually run the malicious executable file “RESERVA.exe” to start the infection process.

Figure 3. Malicious RESERVA.exe in the mounted ISO file

The installed Quasar RAT connects to the C2 server at opensea-user-reward[.]serveusers[.]com (DDNS). Fortinet’s telemetry, as well as OSINT, did not observe any connections to the DDNS over the past three months. This could indicate that the attack was unsuccessful.

Interestingly, FortiGuard Labs also discovered another Quasar RAT sample that shares the same resource section and the same C2 address. This sample was submitted from Hong Kong the day after the malware that was sent to a Colombian military service became public. While no evidence could be gathered to connect the samples to a single threat actor, given the similarities in the samples, it is possible that the same attacker targeted an organization in Hong Kong.

Conclusion

The attacks described in this blog are not complicated. All that is needed is for the victim to manually run a plain executable file manually to get infected. What is unique is that for the past two years, most opportunities for travel and vacation were taken away due to COVID. And now that the liberty to travel is back, threat actors are exploiting the enthusiasm people have to get out and explore again.

Always practice cyber security hygiene, and bon voyage!

Fortinet Protections

FortiGuard Labs has AV coverage in place for the malicious file samples in this report as:

- MSIL/VRN.WN!tr
- MSIL/Injector.VRI!tr
- MSIL/Kryptik.YVP!tr
- MSIL/Agent.CJR!tr
- JS/Agent.OOU!tr
- W32/VBKrypt.C!tr

Fortinet customers are also protected from this malware through FortiGuard’s Web Filtering, FortiMail, FortiClient, FortiEDR, and CDR (content disarm and reconstruction) services.

In addition to these protections, Fortinet has multiple solutions designed to help train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

We also suggest that organizations have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats that is designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

IOCs

File IOCs

AsyncRAT

- 7e40ffe649eebe5a8f156f2051d670ccb1c2580b387190b60a928149c0db071e (travel_details.iso)
- a1a82789bcd4b8f4400e2d3dcd723722c4528cb3a188ffb54d7e684fdb808792 (Travel_details.exe)
- 981139ca1539c9db49c7e2cd2cfde1a463feec421a3f73d0cca9f880fbdb1919 (Itinerary.iso)
- aada737aa6be290e37a9da366a195b83a7597fbce1ef427b829049df7684cdf1 (ITINERARY.PDF.EXE)
- 98a8e1b3ff49c4b979127e2c02a04b41971fdb3d612c0d66e2e8a95f4f08a5e3 (activities_and_dates.iso)
- 906ca464f50e99eb1478d81dffa3c64abfc6819ec93b991cf890d52f5cfb1143 (Activities_and_dates.exe)
- f49c2c23d606fd7779d900604d9b45b7329c4f6ee5fbafdf77fbdd2c2ab26445 (itinerary.zip)
- aada737aa6be290e37a9da366a195b83a7597fbce1ef427b829049df7684cdf1 (Itinerary.pdf_____.exe)
- ffd561a46ec49ff9c232005dc95ea1e3315e02e497e55adbfcc9f31ac668353a (Booking details.exe)
- b899fc7141b866552940b6ee0f8ab0d214a05c8338906fd85fae67c507d652bb (Itinerary.exe)

Netwire RAT

5f4bbe855651ea0417c10f470c010eb86a8eae4ac3b1569bcfaaac4eab648c9f (Flight_Travel_Intinery_Details.js)

Quasar RAT

- 5f336cc401742fab95092241ba8a6ab721390a52646b105b721376169152f982

- af5b5409b49d74f90ce2ccd62d03b890c3dc2b22a44b6a5f35dfa18a40a198da
- c928d42edbb368f61da40e6f78e7bd223736ecc0ac988359af51d7b6b4299f03

Network IOCs

AsyncRAT

- dc5b-163-123-142-137[.]ngrok[.]io/itinerary.zip
- dc5b-163-123-142-137[.]ngrok[.]io/travel_details.iso
- dc5b-163-123-142-137[.]ngrok[.]io/Itinerary.exe
- 33b4-163-123-142-137[.]ngrok[.]io/activities_and_dates.iso
- znets[.]ddns[.]net
- dnets[.]ddns[.]net

Netwire RAT

kingshakes1[.]linkpc[.]net

Quasar RAT:

opensea-user-reward[.]serveusers[.]com

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.