Microsoft

Microsoft Defender Advanced Threat Protection

Attack simulation

Scenario 2: PowerShell script in fileless attack

May 2020

Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Please refer to Microsoft Trademarks for a list of trademarked products.

All other trademarks are property of their respective owners.

Our detection philosophy

It's simple.

We make sure that known advanced persistent threat (APT) indicators or techniques are visible in our telemetry, that we recognize them, and that we are able to raise the relevant alerts.

When we raise an alert near real-time, we provide the relevant context, including actor attribution, their victimology, geo-affinity, and main tactics. This is realized through a rich, dynamic library of known attack indicators, including known threat components previously observed on real machines, script and web page snippets from compromised or malicious websites, as well as IPs, URLs, and domains representing the attacker's infrastructure. We constantly update this library with new threat intelligence generated mainly by Microsoft's own APT hunting and research teams, but enriched by collaboration with partners and shared feeds.

Because threats are constantly being crafted and modified, we monitor a large set of anomalous and suspicious behaviors to find new and unknown actor activity. These anomalous and suspicious activities raise alerts for the Security Operations Center (SOC) analyst to validate and address. With the help of information about proximate events on the same machine and other relevant machines, SOC analysts can validate actual breach activity, determine risk, establish the scope of the breach, define containment activities, and then contain, mitigate and fully respond to the attack.

Introduction: PowerShell script in fileless attack

In this scenario, we move up a notch to more sophisticated attack that leverage advanced techniques to stay under the detection radar. This category of attacks usually doesn't include files dropped on the victim's machine—they occur solely in memory. They "live off the land" by using only existing system and administrative tools and injecting their code into system processes to hide their execution and persist on the box.

In this simulation, our example scenario starts with a PowerShell script. A user may be tricked into executing such a script, or the script may be executed remotely from another machine in the organization that was previously infected, with the attacker attempting to move laterally in the network. Detection of such scripts is difficult because administrators also often run scripts remotely to carry out various administrative activities.

During the simulation, the attacker goes on to inject some shellcode into a seemingly innocent process, in this case *notepad.exe*. We chose this process for the simulation, but attackers will more likely target a long-running system process like *svchost.exe*. The shellcode then goes on to contact the attacker's command-and-control (C&C) server to receive instructions on how to proceed.

The test machine require for this simulation should:

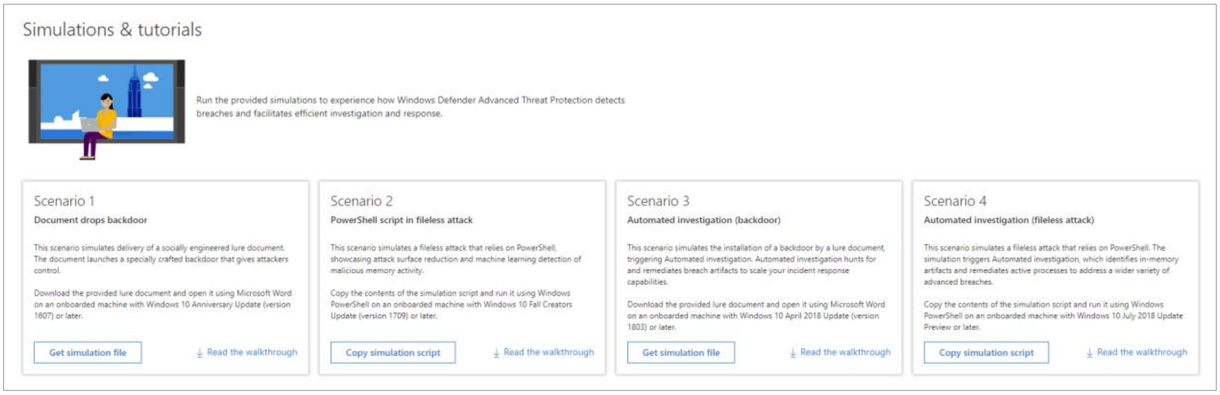
- Be onboarded to Microsoft Defender ATP
- Run Windows 10 Fall Creators Update (version 1709)
- Have PowerShell turned on
- Have Windows Defender Antivirus turned on

For onboarding instructions, read to the product guide. We recommend running the local onboarding script to onboard the test machine.

Run the simulation

To run this attack scenario, follow these steps:

1. On the designated test machine, log in to the Microsoft Defender ATP portal and go to **Help (?) > Simulations & tutorials**.



Simulations & tutorials

Run the provided simulations to experience how Windows Defender Advanced Threat Protection detects breaches and facilitates efficient investigation and response.

Scenario 1

Document drops backdoor

This scenario simulates delivery of a socially engineered lure document. The document launches a specially crafted backdoor that gives attackers control.

Download the provided lure document and open it using Microsoft Word on an onboarded machine with Windows 10 Anniversary Update (version 1607) or later.

Get simulation file ↓ Read the walkthrough

Scenario 2

PowerShell script in fileless attack

This scenario simulates a fileless attack that relies on PowerShell, showcasing attack surface reduction and machine learning detection of malicious memory activity.

Copy the contents of the simulation script and run it using Windows PowerShell on an onboarded machine with Windows 10 Fall Creators Update (version 1709) or later.

Copy simulation script ↓ Read the walkthrough

Scenario 3

Automated investigation (backdoor)

This scenario simulates the installation of a backdoor by a lure document, triggering Automated investigation. Automated investigation hunts for and remediates breach artifacts to scale your incident response capabilities.

Download the provided lure document and open it using Microsoft Word on an onboarded machine with Windows 10 April 2018 Update (version 1803) or later.

Get simulation file ↓ Read the walkthrough

Scenario 4

Automated investigation (fileless attack)

This scenario simulates a fileless attack that relies on PowerShell. The simulation triggers Automated investigation, which identifies in-memory artifacts and remediates active processes to address a wider variety of advanced breaches.

Copy the contents of the simulation script and run it using Windows PowerShell on an onboarded machine with Windows 10 July 2018 Update Preview or later.

Copy simulation script ↓ Read the walkthrough

Figure 1. Simulation scenarios in the portal

2. Click the **Copy simulation script** button under **Scenario 2: PowerShell script in fileless attack** to copy the PowerShell script.

3. Open a Windows PowerShell window with administrative privileges on the test machine.

4. At the prompt, paste and run the provided script.

   A few seconds later, *notepad.exe* is started and the simulated attack code is injected into it. The simulated attack code attempts communication to an external IP address simulating the C&C server.

Congrats – you're done running the attack!

The attack simulation ends here. A real attacker, if successful, would likely continue to scan for information, send collected reconnaissance information to a command-and-control (C&C) server, and use this information to move laterally and pursue other attractive targets.

Next, let's review and investigate the Microsoft Defender ATP alerts that surfaced the simulated attack.

✎ **Note**: Alerts should start to appear 15-30 minutes after the simulated backdoor is launched.

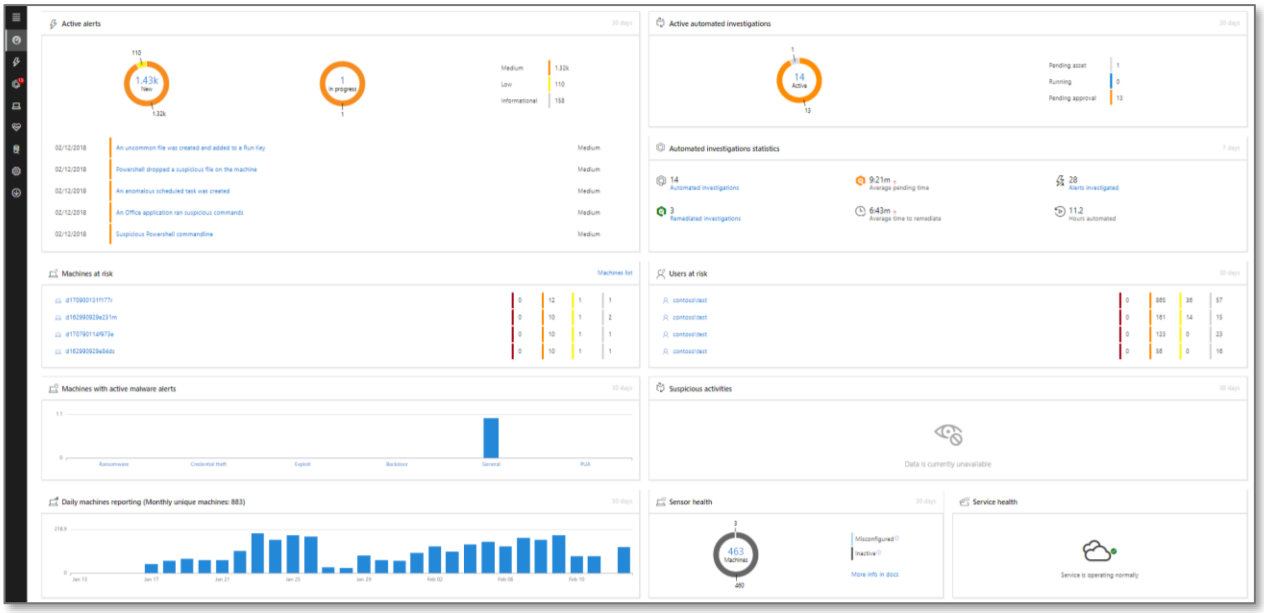
Investigate the attack in the portal

Let’s switch into our defender role and explore the attack from the SOC point of view in the Microsoft Defender ATP portal.

1. Open the Microsoft Defender ATP portal from any machine.

2. Log in with your Microsoft Defender ATP credentials. Default global administrator credentials are provided with your signup email.

3. After 15-30 minutes of the simulated attack, you should find several new alerts on the dashboard.



Active alerts

02/12/2018	An uncommon file was created and added to a Run Key	Medium
02/12/2018	Powershell dropped a suspicious file on the machine	Medium
02/12/2018	An anomalous scheduled task was created	Medium
02/12/2018	An Office application ran suspicious commands	Medium
02/12/2018	Suspicious Powershell commandline	Medium

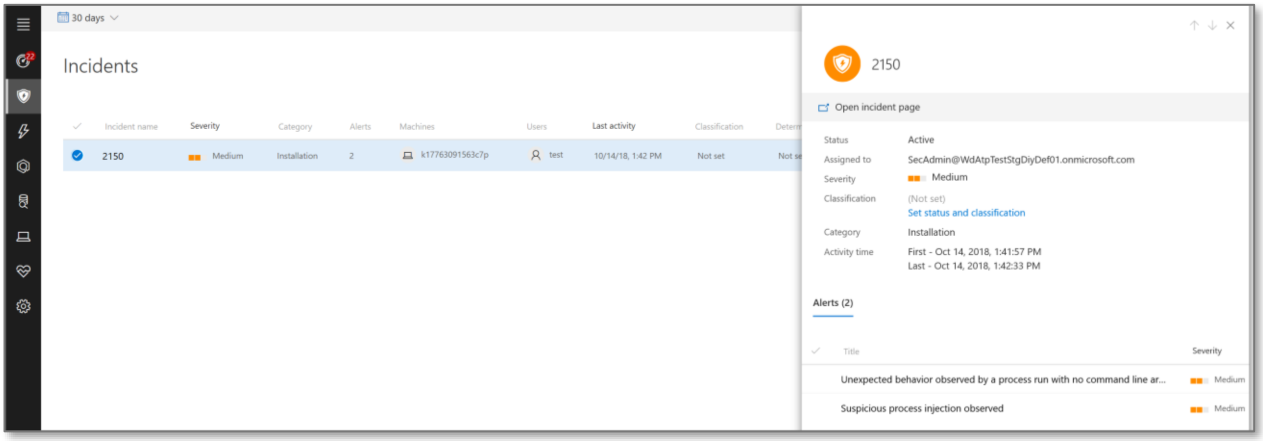
Figure 2. Dashboard view showing the alerts

Investigate the attack as a single incident

Microsoft Defender ATP applies correlation analytics and aggregates all related alerts and investigations into one “incident” entity. By doing so, Microsoft Defender ATP narrates a broader attack story, allowing the SOC analyst to understand and deal with complex threats across the org with the right visuals—through the enhanced incident graph—and data representations.

The alerts generated during this simulation are associated with the same threat, and as a result are automatically aggregated as a single incident.

To view the incident, go to the **Incidents** queue and select the relevant item as shown below. A side panel displays additional information about the incident, including all the related alerts.



Incidents

✓	Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification	Determ
✓	2150	Medium	Installation	2	k17763091563c7p	test	10/14/18, 1:42 PM	Not set	Not se

2150

Status: Active
Assigned to: SecAdmin@WdAtpTestStgDiyDef01.onmicrosoft.com
Severity: Medium
Classification: (Not set)
Set status and classification
Category: Installation
Activity time: First - Oct 14, 2018, 1:41:57 PM
Last - Oct 14, 2018, 1:42:33 PM

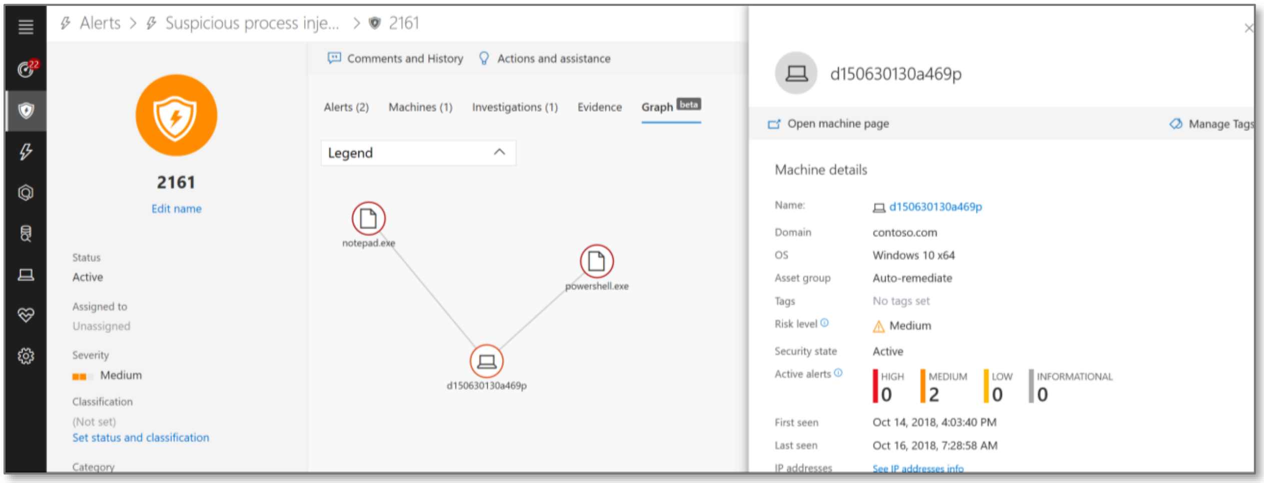
Alerts (2)

✓	Title	Severity
	Unexpected behavior observed by a process run with no command line ar...	Medium
	Suspicious process injection observed	Medium

Figure 3. Incident aggregating alerts generated during the simulation

Select **Open incident page** to get more information about the incident.

In the incident page, you can check all the affected machines and the related alerts. For a broader view of the entities involved in the incident, select **Graph**.



2161

Edit name

Status: Active

Assigned to: Unassigned

Severity: Medium

Classification: (Not set)

Set status and classification

Category

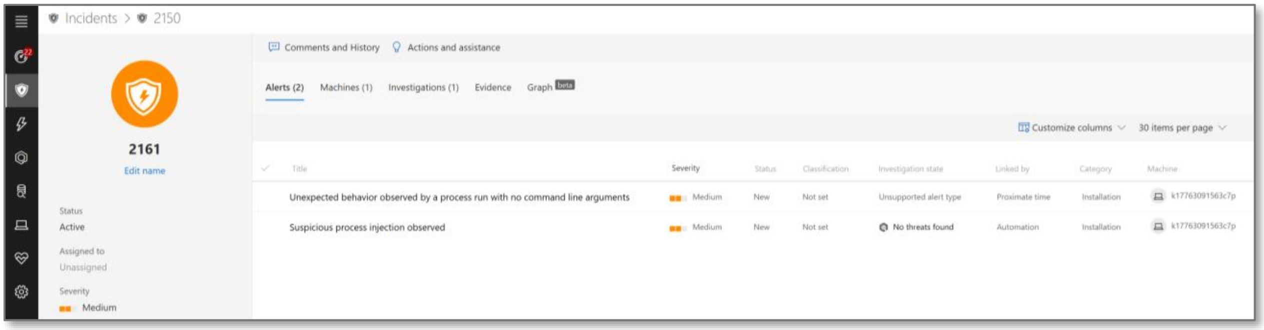
d150630130a469p

Machine details

Name:	d150630130a469p
Domain	contoso.com
OS	Windows 10 x64
Asset group	Auto-remediate
Tags	No tags set
Risk level	Medium
Security state	Active
Active alerts	HIGH 0 MEDIUM 2 LOW 0 INFORMATIONAL 0
First seen	Oct 14, 2018, 4:03:40 PM
Last seen	Oct 16, 2018, 7:28:58 AM
IP addresses	See IP addresses info

Figure 4. Graph of the incident

Reviewing the incident alert list unfolds the progression of the attack. From this view you can dive into the individual alerts



2161

Edit name

Status: Active

Assigned to: Unassigned

Severity: Medium

Title	Severity	Status	Classification	Investigation state	Linked by	Category	Machine
Unexpected behavior observed by a process run with no command line arguments	Medium	New	Not set	Unsupported alert type	Proximate time	Installation	k17763091563c7p
Suspicious process injection observed	Medium	New	Not set	No threats found	Automation	Installation	k17763091563c7p

Figure 5. Incident related alerts

Review generated alerts

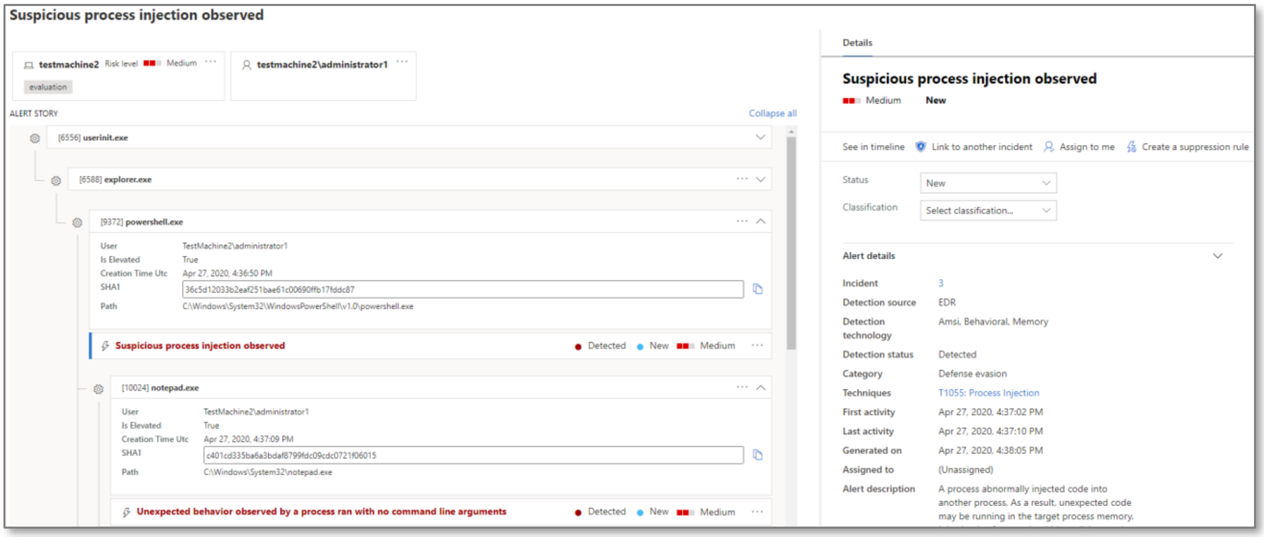
Let’s look at some of the alerts generated during the simulated attack.

Note: We will walk through only a few of the alerts generated during the simulated attack. Depending on the version of Windows and the Windows Defender Antivirus protection updates running on your test machine, you might see more alerts and they might appear in a slightly different order.

Alert: Suspicious process injection observed

Advanced attackers will use more sophisticated and stealthy methods to persist in memory and hide from detection tools. One common technique is to operate from within a trusted system process rather than a malicious executable, making it hard for detection tools and security operations to spot the malicious code.

To allows SOC personnel to catch such advanced attacks, deep memory sensors in Microsoft Defender ATP provide our cloud service with unprecedented visibility into a variety of cross-process code injection techniques. As show below, Microsoft Defender ATP detected and alerted on the attempt to inject code to notepad.exe.


Suspicious process injection observed
testmachine2 Risk level Medium
evaluation
testmachine2\administrator1
ALERT STORY
Collapse all
Details
See in timeline
Link to another incident
Assign to me
Create a suppression rule

[6556] userinit.exe

[6588] explorer.exe

[9372] powershell.exe

User	TestMachine2\administrator1
Is Elevated	True
Creation Time Utc	Apr 27, 2020, 4:36:50 PM
SHA1	36c5d12033b2eaf251bae61c00690ffb17fddc87
Path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Suspicious process injection observed ● Detected ● New Medium

[10024] notepad.exe

User	TestMachine2\administrator1
Is Elevated	True
Creation Time Utc	Apr 27, 2020, 4:37:09 PM
SHA1	c401cd335ba6a3bdaf8799fdc09cdc0721f06015
Path	C:\Windows\System32\notepad.exe

Unexpected behavior observed by a process ran with no command line arguments ● Detected ● New Medium

Suspicious process injection observed

Medium New

Status	New
Classification	Select classification...

Alert details

Incident	3
Detection source	EDR
Detection technology	Amsi, Behavioral, Memory
Detection status	Detected
Category	Defense evasion
Techniques	T1055: Process Injection
First activity	Apr 27, 2020, 4:37:02 PM
Last activity	Apr 27, 2020, 4:37:10 PM
Generated on	Apr 27, 2020, 4:38:05 PM
Assigned to	(Unassigned)
Alert description	A process abnormally injected code into another process. As a result, unexpected code may be running in the target process memory.

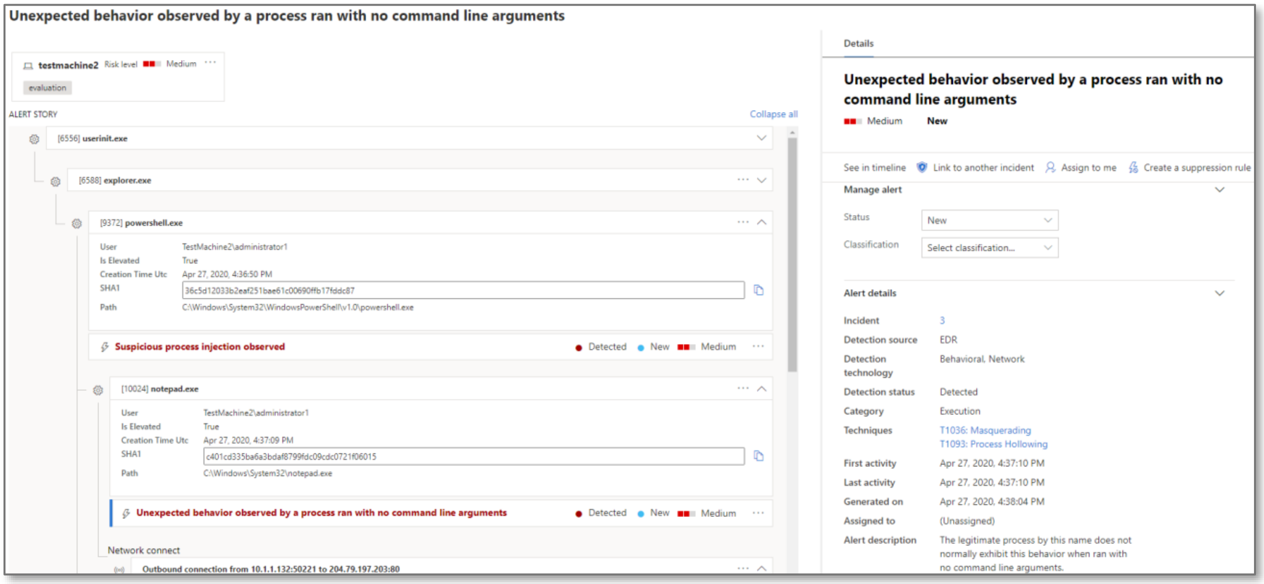
Figure 6. Alert for injection of potentially malicious code

Alert: Unexpected behavior observed by a process run with no command line arguments

Microsoft Defender ATP detections are often targeting the most invariant aspect of an attack technique. This ensures durability and raises the bar for attacker's to switch to newer tactics.

We employ large-scale learning algorithms to establish normal behavior of common processes within an organization and worldwide, and watch for when these processes exhibit anomalous behaviors. These anomalous behaviors often indicate that extraneous code was introduced and running in the otherwise trusted process.

In our case, the well-known process *notepad.exe* is exhibiting abnormal behavior, involving communication with an external location. Note that this outcome is independent of the specific method used to introduce and execute the malicious code.



Unexpected behavior observed by a process ran with no command line arguments

testmachine2 Risk level 🟥🟥 Medium ···
evaluation

ALERT STORY

Collapse all

[6556] **userinit.exe**

[6588] **explorer.exe**

[9372] **powershell.exe**

User TestMachine2\administrator1
Is Elevated True
Creation Time Utc Apr 27, 2020, 4:36:50 PM
SHA1 36c5d12033b2eaf251bae61c00690ffb17fddc87
Path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Suspicious process injection observed ● Detected ● New 🟥🟥 Medium

[10024] **notepad.exe**

User TestMachine2\administrator1
Is Elevated True
Creation Time Utc Apr 27, 2020, 4:37:09 PM
SHA1 c401cd335ba6a3bdaf8799fdc09cdc0721f06015
Path C:\Windows\System32\notepad.exe

Unexpected behavior observed by a process ran with no command line arguments ● Detected ● New 🟥🟥 Medium

Network connect

Outbound connection from 10.1.1.132:50221 to 204.79.197.203:80

Details

Unexpected behavior observed by a process ran with no command line arguments

🟥🟥 Medium **New**

Manage alert

Status New
Classification Select classification...

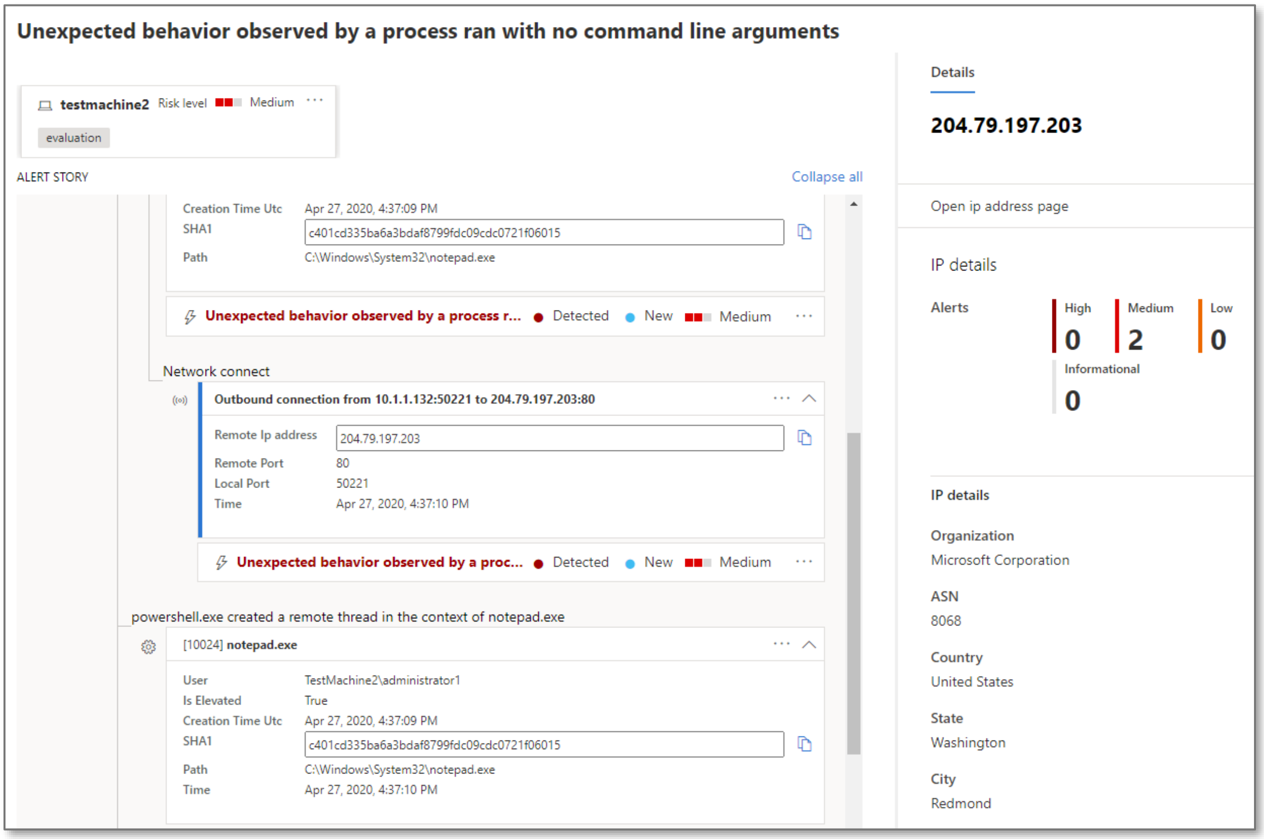
Alert details

Incident 3
Detection source EDR
Detection technology Behavioral, Network
Detection status Detected
Category Execution
Techniques T1036: Masquerading
T1093: Process Hollowing
First activity Apr 27, 2020, 4:37:10 PM
Last activity Apr 27, 2020, 4:37:10 PM
Generated on Apr 27, 2020, 4:38:04 PM
Assigned to (Unassigned)
Alert description The legitimate process by this name does not normally exhibit this behavior when ran with no command line arguments.

Figure 7. Alert for unexpected behavior by a process run with no command line arguments

Note: Because this alert is based on machine-learning models that require some backend processing, it might take some time before it is actually generated on the portal.

Notice that the alert story includes a network connect—an indicator you can use as a pivot to expand investigation. Click the outbound connection in the **Alert story** to view additional information in the details pane.



Unexpected behavior observed by a process ran with no command line arguments

testmachine2 Risk level Medium
evaluation

ALERT STORY — Collapse all

Creation Time Utc	Apr 27, 2020, 4:37:09 PM
SHA1	c401cd335ba6a3bdaf8799fdc09cdc0721f06015
Path	C:\Windows\System32\notepad.exe

Unexpected behavior observed by a process r... ● Detected ● New Medium

Network connect

Outbound connection from 10.1.1.132:50221 to 204.79.197.203:80

Remote Ip address	204.79.197.203
Remote Port	80
Local Port	50221
Time	Apr 27, 2020, 4:37:10 PM

Unexpected behavior observed by a proc... ● Detected ● New Medium

powershell.exe created a remote thread in the context of notepad.exe

[10024] notepad.exe

User	TestMachine2\administrator1
Is Elevated	True
Creation Time Utc	Apr 27, 2020, 4:37:09 PM
SHA1	c401cd335ba6a3bdaf8799fdc09cdc0721f06015
Path	C:\Windows\System32\notepad.exe
Time	Apr 27, 2020, 4:37:10 PM

Details

204.79.197.203

Open ip address page

IP details

Alerts: High 0, Medium 2, Low 0, Informational 0

IP details

Organization
Microsoft Corporation

ASN
8068

Country
United States

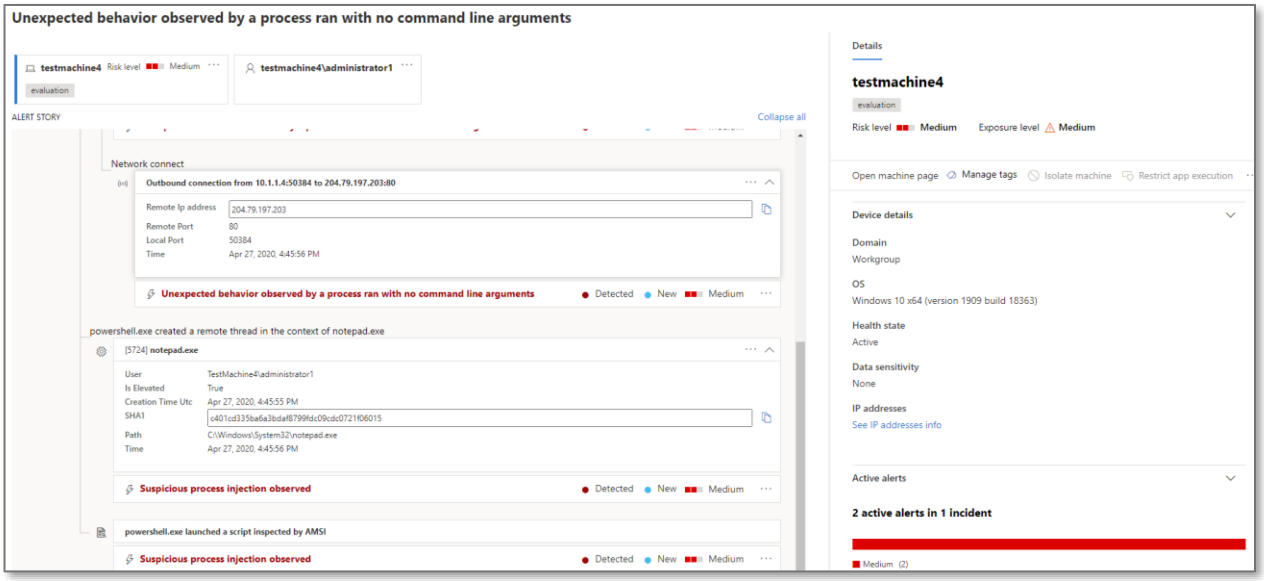
State
Washington

City
Redmond

Figure 8. Outbound connection details

Review other entities in the alert page

Clicking on the machine name in the affected assets part of the alert pages opens changes the details pane to the context of that machine. The details pane provides relevant information and actions to ease the investigation. You can directly isolate the machine while you're investigating or click on **Open machine page** for an in-depth view into that machine.



Unexpected behavior observed by a process ran with no command line arguments

testmachine4 Risk level Medium ···
evaluation

testmachine4\administrator1 ···

ALERT STORY

Collapse all

Network connect

Outbound connection from 10.1.1.4:50384 to 204.79.197.203:80

Remote Ip address	204.79.197.203
Remote Port	80
Local Port	50384
Time	Apr 27, 2020, 4:45:56 PM

Unexpected behavior observed by a process ran with no command line arguments ● Detected ● New Medium ···

powershell.exe created a remote thread in the context of notepad.exe

[5724] **notepad.exe**

User	TestMachine4\administrator1
Is Elevated	True
Creation Time Utc	Apr 27, 2020, 4:45:55 PM
SHA1	c401cd335ba6a3bdaf8799fdc09cdc0721f06015
Path	C:\Windows\System32\notepad.exe
Time	Apr 27, 2020, 4:45:56 PM

Suspicious process injection observed ● Detected ● New Medium ···

powershell.exe launched a script inspected by AMSI

Suspicious process injection observed ● Detected ● New Medium ···

Details

testmachine4
evaluation

Risk level **Medium** Exposure level ⚠ **Medium**

Open machine page | Manage tags | Isolate machine | Restrict app execution

Device details

Domain
Workgroup

OS
Windows 10 x64 (version 1909 build 18363)

Health state
Active

Data sensitivity
None

IP addresses
See IP addresses info

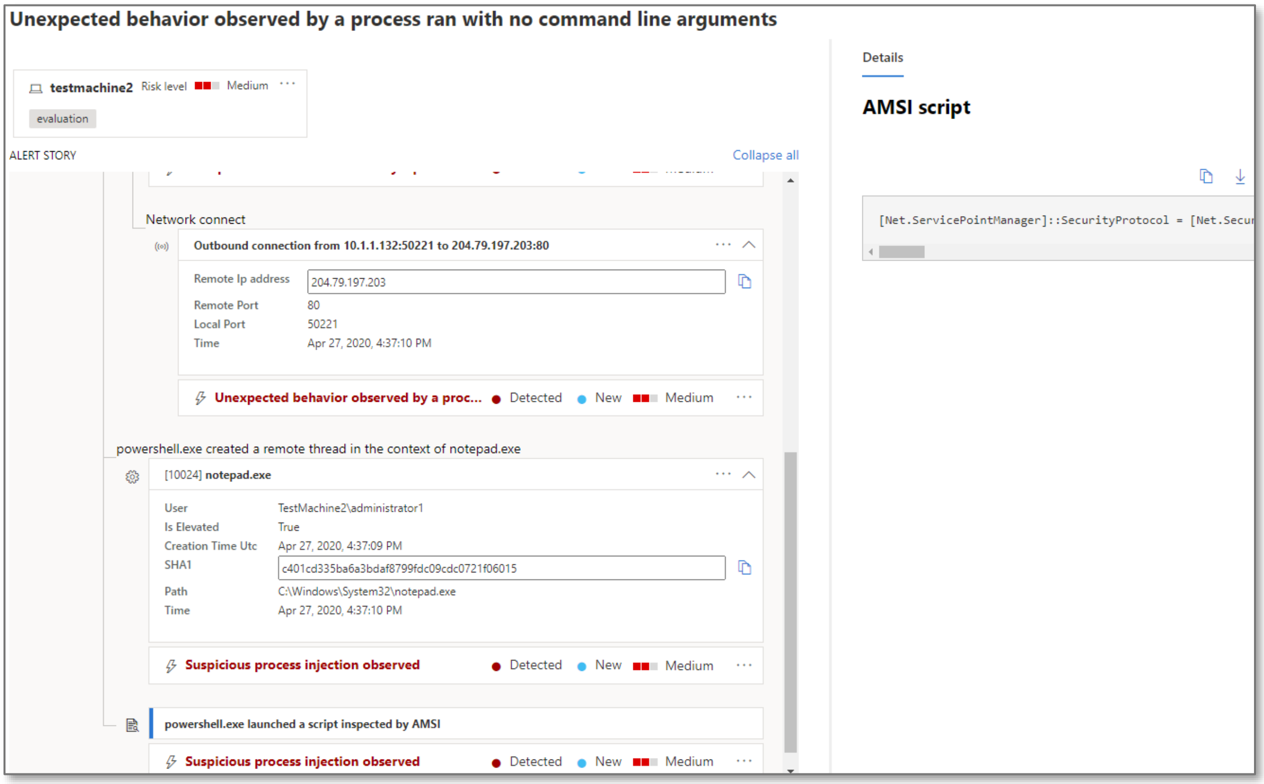
Active alerts

2 active alerts in 1 incident

🟥 Medium (2)

Figure 9. Machine details next to the attack story

Expanding some of the more interesting entities in the attack story provides useful details. For example, clicking on the item **powershell.exe launched a script inspected by AMSI** will show more information on this specific execution.



Unexpected behavior observed by a process ran with no command line arguments

testmachine2 Risk level Medium ···
evaluation

ALERT STORY

Collapse all

Network connect

Outbound connection from 10.1.1.132:50221 to 204.79.197.203:80

Remote Ip address 204.79.197.203
Remote Port 80
Local Port 50221
Time Apr 27, 2020, 4:37:10 PM

Unexpected behavior observed by a proc... ● Detected ● New Medium ···

powershell.exe created a remote thread in the context of notepad.exe

[10024] notepad.exe

User TestMachine2\administrator1
Is Elevated True
Creation Time Utc Apr 27, 2020, 4:37:09 PM
SHA1 c401cd335ba6a3bdaf8799fdc09cdc0721f06015
Path C:\Windows\System32\notepad.exe
Time Apr 27, 2020, 4:37:10 PM

Suspicious process injection observed ● Detected ● New Medium ···

powershell.exe launched a script inspected by AMSI

Suspicious process injection observed ● Detected ● New Medium ···

Details

AMSI script

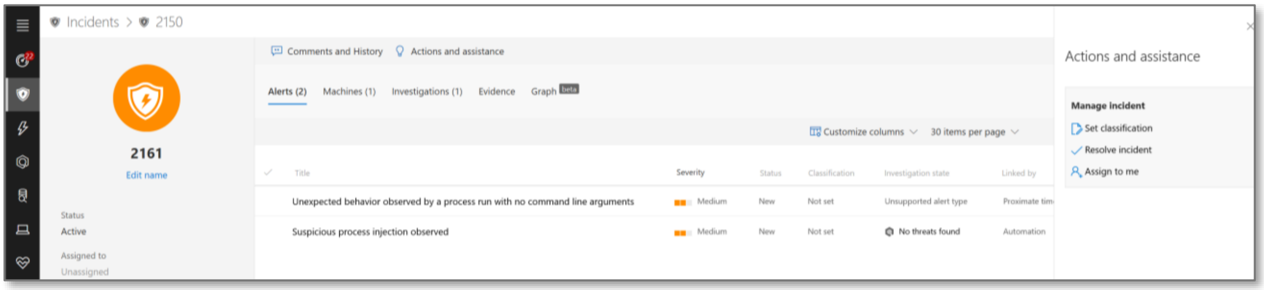
```
[Net.ServicePointManager]::SecurityProtocol = [Net.Secur
```

Figure 10. Attack story with the launched PowerShell script in focus

Resolve the incident

Now that the investigation is completed and, in our case, confirmed to be a benign activity, it is time to close the incident.

On the incident page, select **Actions and assistance** to get management options that apply to the entire incident and all related alerts.



Status
Active

Assigned to
Unassigned

Title	Severity	Status	Classification	Investigation state	Linked by
Unexpected behavior observed by a process run with no command line arguments	Medium	New	Not set	Unsupported alert type	Proximate tim
Suspicious process injection observed	Medium	New	Not set	No threats found	Automation

Figure 11. Resolving the incident and related alerts

Review the reports

Before concluding the investigation, it's a good idea to look at the reports dashboard. It provides high-level information about alerts and machine related information generated in your organization. The report includes trends and summary information on alerts and machines.

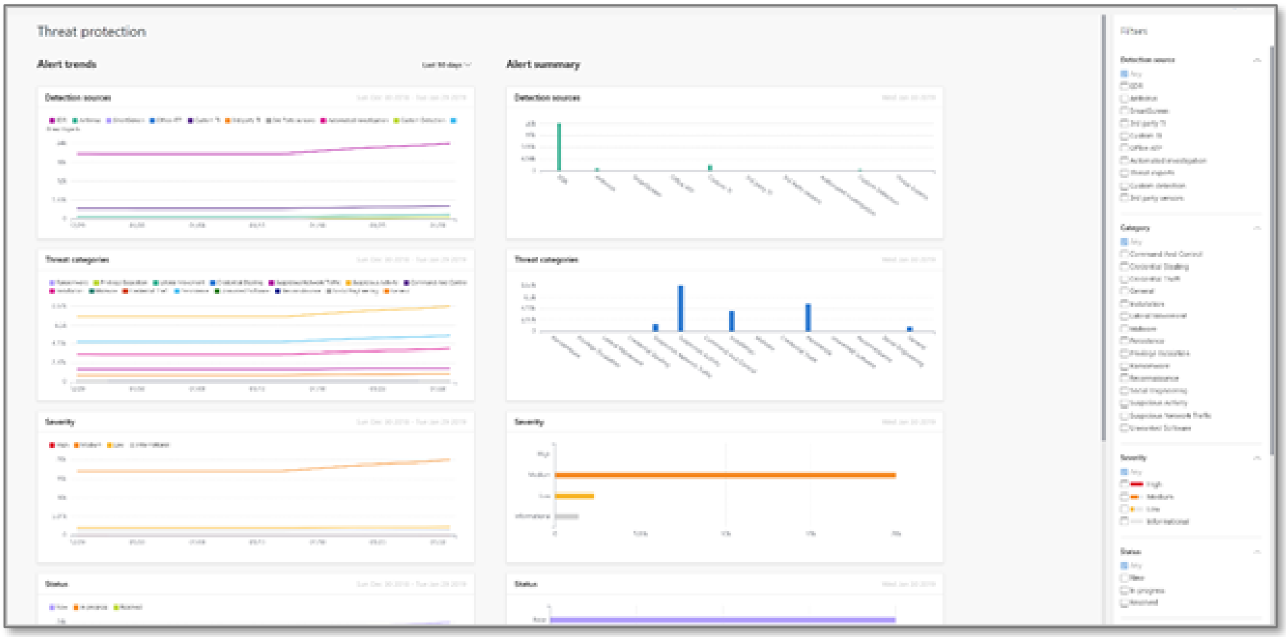


Figure 12. Threat protection report page

Knowing the trends and summaries related to alerts and machines in your organization can help identify where focused improvements can be made. For example, if you see a sudden spike in a specific kind of alert, you can drill down and start investigating directly from the relevant card to pivot into the alert or machine queue with the relevant filters applied and determine what action to take to address an issue.

Conclusion

We've simulated an advanced memory-only attack, and walked through how Microsoft Defender ATP detects and alerts on stealthy malicious activity with the help of deep OS sensors. We've seen how alerts are delivered along with other contextual information, enabling SOC personnel to investigate and take necessary action.

We hope you enjoyed this simulation and are now encouraged to explore other features and capabilities. For more information, read the product guide at docs.microsoft.com.

Click the feedback icon on the Microsoft Defender ATP portal to let us know how you feel about this simulation or any other aspects of the product. We would love to hear your ideas about additional simulations and tutorials. Thank you!