Microsoft

Microsoft Defender Advanced Threat Protection

Attack simulation

Scenario 1: Document drops backdoor

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.

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: Document drops backdoor scenario

Attacks that introduce file-based malware using socially engineered email are quite common. Recipients are tricked into launching a backdoor that gives attackers control over what is now a compromised machine.

This scenario simulates such an attack on your selected test machine. You can then explore and understand how Microsoft Defender ATP detects the attack and enables prompt investigation and response.

This scenario simulates attacks that are launched using a socially engineered lure document in a spear-phishing email. The lure is designed to ensure that the receiver doesn’t suspect a thing and unwittingly opens the document.

The document, however, is weaponized with crafted macro code that silently drops and loads an executable file onto the machine. Although this simulation uses a document that drops a benign executable, the executable behaves as if it is a backdoor attempting to gain persistence—it writes to a registry Run key and creates a scheduled task, both commonly known auto-start extensibility points (ASEPs).

The attack simulation ends when the ASEPs are created. In the real world, however, the attacker is expected to use the implanted backdoor to perform other actions within the compromised network, such as moving laterally to other machines, gathering credentials to gain privileges, and exfiltrating stolen data.

The test machine required for this simulation should:

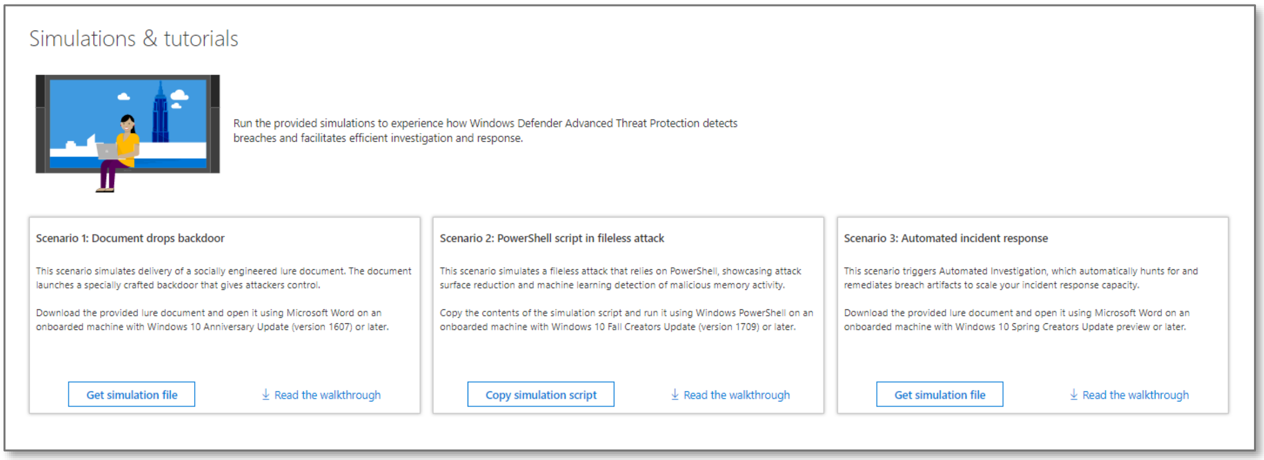
- Be onboarded to Microsoft Defender ATP
- Run Windows 10 Anniversary Update (version 1607) or later
- Have PowerShell turned on
- Have Windows Defender Antivirus turned on
- Have Microsoft Word installed

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 the attack simulation:

1. 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.

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.

Scenario 3: Automated incident response

This scenario triggers Automated Investigation, which automatically hunts for and remediates breach artifacts to scale your incident response capacity.

Download the provided lure document and open it using Microsoft Word on an onboarded machine with Windows 10 Spring Creators Update preview or later.

Simulation scenarios in the portal

2. Click **Get simulation file** under **Scenario 1: Document drops backdoor** to download the lure document **WinATP-Intro-Invoice.docm**.

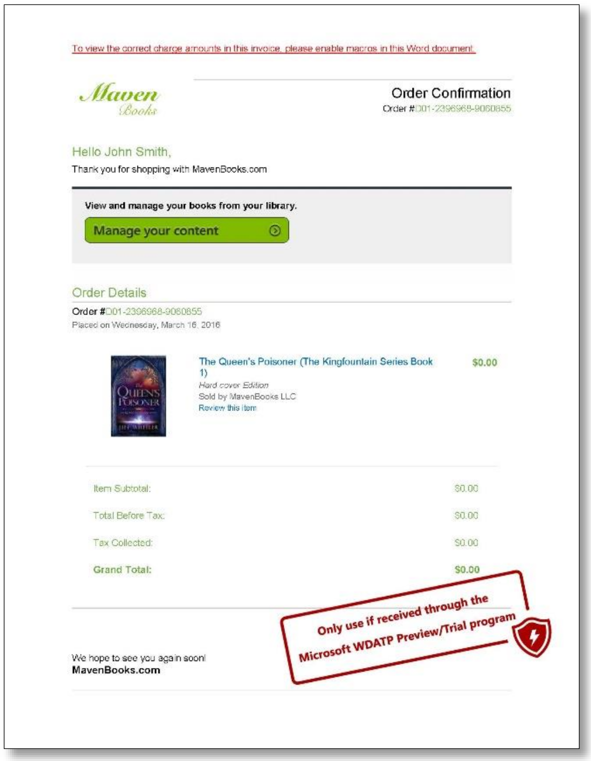
3. Copy the lure document to the test machine.

4. To simulate typical user interaction with the lure document, double-click the copy of the document on the test machine. Microsoft Word will prompt for a password to open the document. To open the password-protected document, use the password **WDATP!diy#**.

5. Click **Enable Editing** if the document opens in Protected View. If you see a subsequent security warning about macros being disabled, click **Enable Content**. With the right lure content, many users are actually enticed to bypass these security safeguards when opening malicious Office documents.

   ✎ **Note**: If your organization blocks macros in documents from the internet, you might need to unblock this specific document for the **Enable Content** option to work. To unblock the document, navigate to its location in File Explorer. In File Explorer, right-click the document, select **Properties**. In the **General** tab, mark the **Unblock** option under **Security**.

   ✎ **Note**: You might encounter difficulties running the scenario if you have third party security products. We recommend using an onboarded test machine with the default out-of-box Windows 10 configuration and Windows Defender AV turned on.



To view the correct charge amounts in this invoice, please enable macros in this Word document.

Maven Books

Order Confirmation
Order #D01-2396968-9060855

Hello John Smith,

Thank you for shopping with MavenBooks.com

View and manage your books from your library.

Order Details

Order #D01-2396968-9060855
Placed on Wednesday, March 16, 2016

The Queen's Poisoner (The Kingfountain Series Book 1) $0.00
Hard cover Edition
Sold by MavenBooks LLC
Review this item

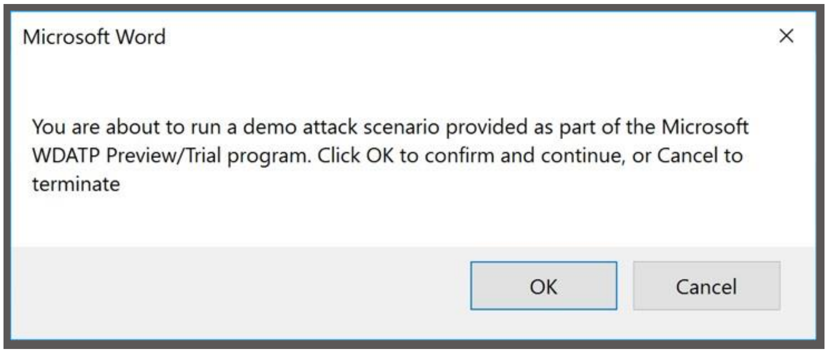
Item Subtotal:	$0.00
Total Before Tax:	$0.00
Tax Collected:	$0.00
Grand Total:	**$0.00**

We hope to see you again soon!
MavenBooks.com

Only use if received through the Microsoft WDATP Preview/Trial program

The lure document

6. Click OK on the message box to confirm that you wish to run the attack simulation.



Microsoft Word

You are about to run a demo attack scenario provided as part of the Microsoft WDATP Preview/Trial program. Click OK to confirm and continue, or Cancel to terminate

7. A few seconds later, a new file **WinATP-Intro-Backdoor.exe**, which represents the backdoor, is dropped onto the Desktop folder by a PowerShell script launched from the document's malicious macro.

8. The script goes on to create a scheduled task to launch the backdoor at a predefined time. This mechanism of indirect process launch is sometimes used for stealth, as it is harder to trace back to the document.

9. When the backdoor is launched, it creates an auto-start entry under the registry Run key, allowing it to stay persistent by starting automatically with Windows. A Command Prompt window opens, indicating that the simulated backdoor is running.

10. Close the Command Prompt window to end the **WinATP-Intro-Backdoor.exe** process.

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.

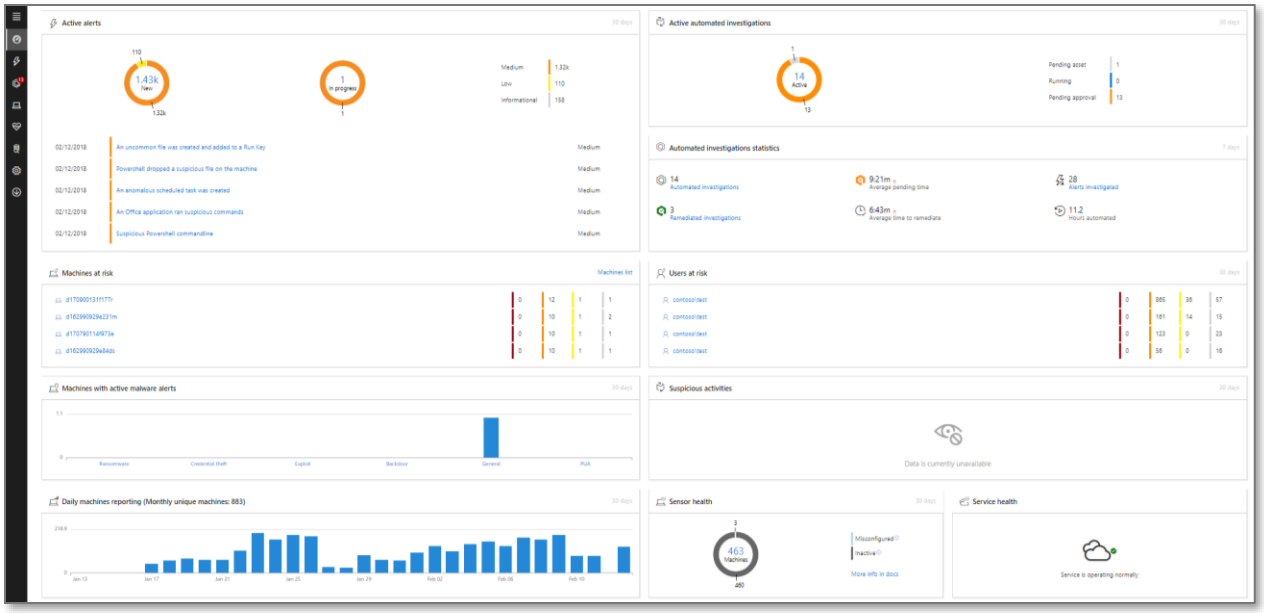
Next, let's review and investigate the Microsoft Defender ATP alerts that surface the simulated attack.

✎ **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.



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

d170900131f177r	0	12	1	1
d162990929e231m	0	10	1	2
d170790114f973e	0	10	1	1
d162990929e84ds	0	10	1	1

contoso\test	0	865	36	57
contoso\test	0	161	14	15
contoso\test	0	123	0	23
contoso\test	0	56	0	16

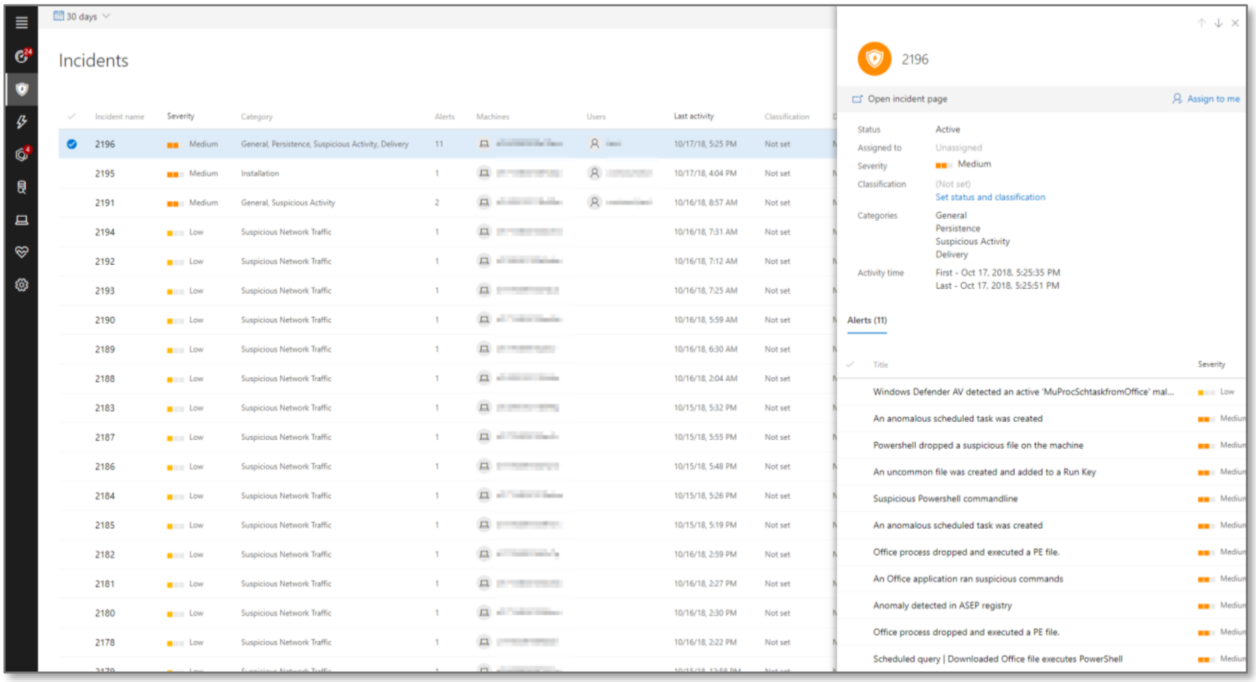
Dashboard view showing the alerts

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
✓	2196	Medium	General, Persistence, Suspicious Activity, Delivery	11	[redacted]	[redacted]	10/17/18, 5:25 PM	Not set
	2195	Medium	Installation	1	[redacted]	[redacted]	10/17/18, 4:04 PM	Not set
	2191	Medium	General, Suspicious Activity	2	[redacted]	[redacted]	10/16/18, 8:57 AM	Not set
	2194	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:31 AM	Not set
	2192	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:12 AM	Not set
	2193	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:25 AM	Not set
	2190	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 5:59 AM	Not set
	2189	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 6:30 AM	Not set
	2188	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:04 AM	Not set
	2183	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:32 PM	Not set
	2187	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:55 PM	Not set
	2186	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:48 PM	Not set
	2184	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:26 PM	Not set
	2185	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:19 PM	Not set
	2182	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:59 PM	Not set
	2181	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:27 PM	Not set
	2180	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:30 PM	Not set
	2178	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:22 PM	Not set
	2179	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 12:58 PM	Not set

2196

Status	Active
Assigned to	Unassigned
Severity	Medium
Classification	(Not set) Set status and classification
Categories	General Persistence Suspicious Activity Delivery
Activity time	First - Oct 17, 2018, 5:25:35 PM Last - Oct 17, 2018, 5:25:51 PM

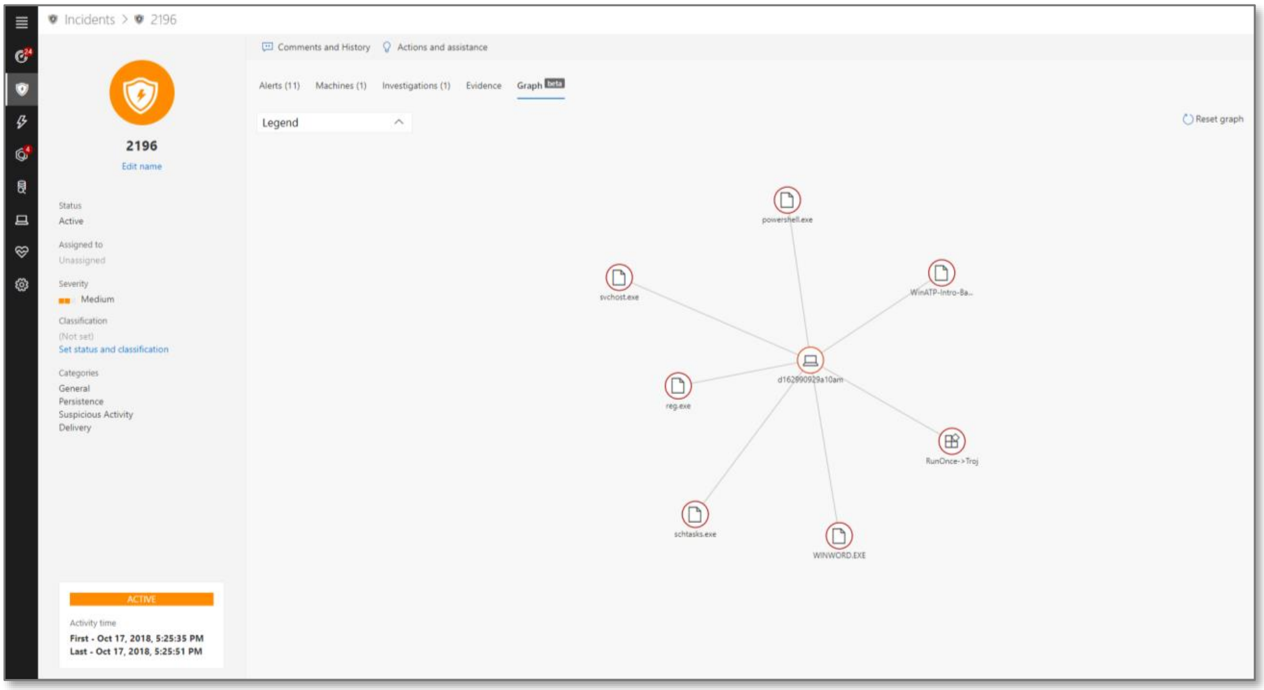
Alerts (11)

✓	Title	Severity
	Windows Defender AV detected an active 'MuProcSchtaskfromOffice' mal...	Low
	An anomalous scheduled task was created	Medium
	Powershell dropped a suspicious file on the machine	Medium
	An uncommon file was created and added to a Run Key	Medium
	Suspicious Powershell commandline	Medium
	An anomalous scheduled task was created	Medium
	Office process dropped and executed a PE file.	Medium
	An Office application ran suspicious commands	Medium
	Anomaly detected in ASEP registry	Medium
	Office process dropped and executed a PE file.	Medium
	Scheduled query | Downloaded Office file executes PowerShell	Medium

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**.



Incidents > 2196

Comments and History | Actions and assistance

Alerts (11) | Machines (1) | Investigations (1) | Evidence | **Graph** beta

2196
Edit name

Status
Active

Assigned to
Unassigned

Severity
Medium

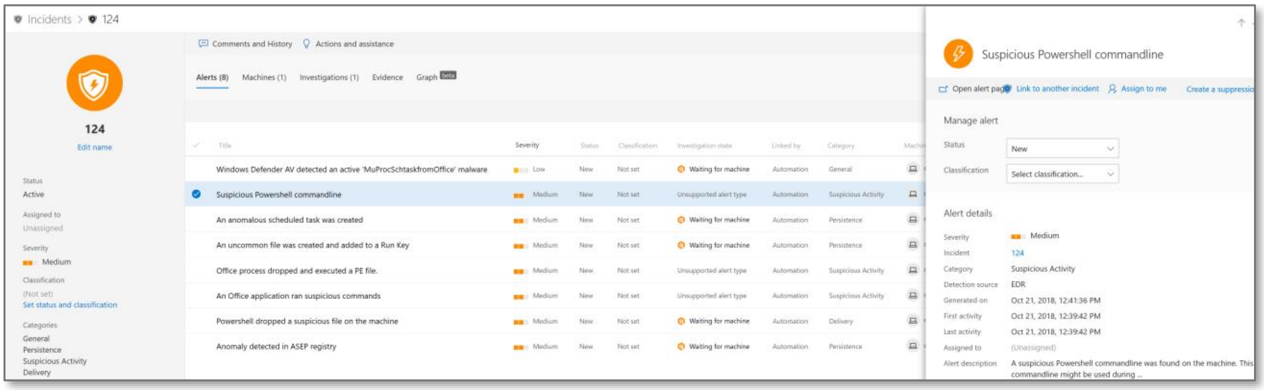
Classification
(Not set)
Set status and classification

Categories
General
Persistence
Suspicious Activity
Delivery

ACTIVE
Activity time
First - Oct 17, 2018, 5:25:35 PM
Last - Oct 17, 2018, 5:25:51 PM

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



Incidents > 124

Comments and History | Actions and assistance

Alerts (8) | Machines (1) | Investigations (1) | Evidence | Graph beta

124
Edit name

Status
Active

Assigned to
Unassigned

Severity
Medium

Classification
(Not set)
Set status and classification

Categories
General
Persistence
Suspicious Activity
Delivery

Title	Severity	Status	Classification	Investigation state	Linked by	Category
Windows Defender AV detected an active 'MuProcSchtaskfromOffice' malware	Low	New	Not set	Waiting for machine	Automation	General
Suspicious Powershell commandline	Medium	New	Not set	Unsupported alert type	Automation	Suspicious Activity
An anomalous scheduled task was created	Medium	New	Not set	Waiting for machine	Automation	Persistence
An uncommon file was created and added to a Run Key	Medium	New	Not set	Waiting for machine	Automation	Persistence
Office process dropped and executed a PE file.	Medium	New	Not set	Unsupported alert type	Automation	Suspicious Activity
An Office application ran suspicious commands	Medium	New	Not set	Unsupported alert type	Automation	Suspicious Activity
Powershell dropped a suspicious file on the machine	Medium	New	Not set	Waiting for machine	Automation	Delivery
Anomaly detected in ASEP registry	Medium	New	Not set	Waiting for machine	Automation	Persistence

Suspicious Powershell commandline

Open alert page | Link to another incident | Assign to me | Create a suppressio

Manage alert

Status: New
Classification: Select classification...

Alert details

Severity	Medium
Incident	124
Category	Suspicious Activity
Detection source	EDR
Generated on	Oct 21, 2018, 12:41:36 PM
First activity	Oct 21, 2018, 12:39:42 PM
Last activity	Oct 21, 2018, 12:39:42 PM
Assigned to	(Unassigned)
Alert description	A suspicious Powershell commandline was found on the machine. This commandline might be used during ...

Actions and assistance options for managing the incident

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.

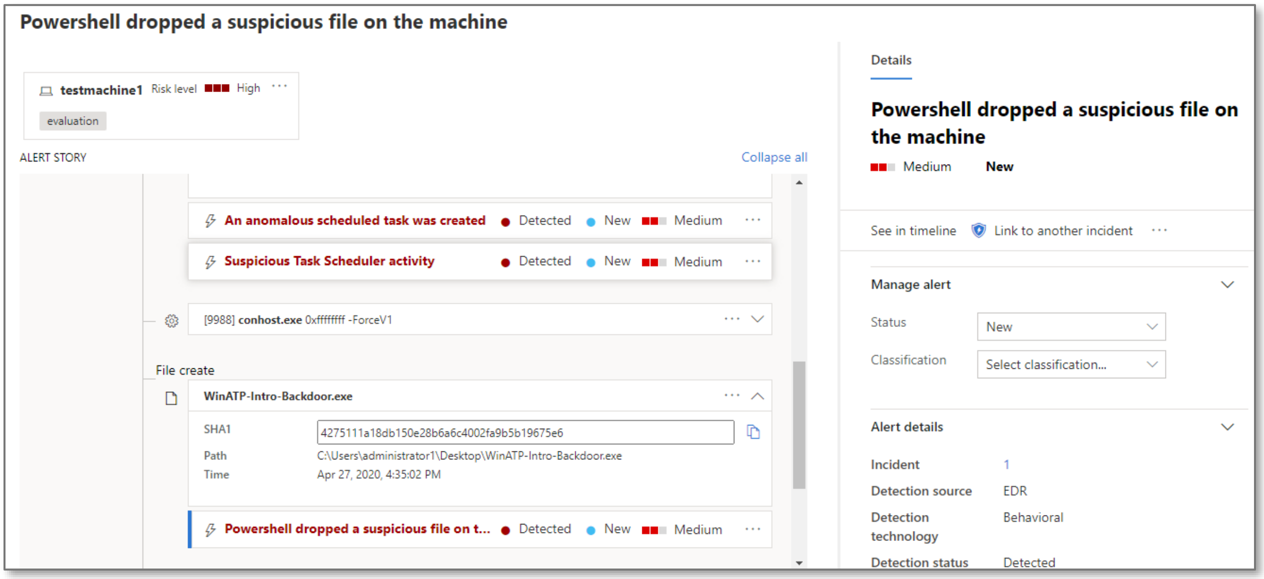
Alert: PowerShell dropped a suspicious file on the machine

A macro in the Word document we opened used PowerShell to write an executable to disk. Microsoft Defender ATP monitors executables created by Office applications, including executables dropped using PowerShell, and looks for files that are rare relative to your organization or to everyone else.

On the alerts tab within the incident, select the "Powershell dropped a suspicious file on the machine" alert. This will open the alert page.

With the selected alert in focus by default, you will see information like:

- This alert's story, containing entities related to the alert – these can include files, processes command lines, events, related alerts, as well as other details and actions available through expanding or clicking on these entities
- Affected entities, which shows devices or users affected by this alert – these are clickable and provide additional details and action on the user\device, such as identifying information, health state, other related alerts, and the ability to restrict or isolate the entity
- The details pane will display in-context information and actions based on the type of the selected entity



Powershell dropped a suspicious file on the machine

testmachine1 Risk level High ···

evaluation

ALERT STORY

Collapse all

An anomalous scheduled task was created ● Detected ● New Medium ···

Suspicious Task Scheduler activity ● Detected ● New Medium ···

[9988] **conhost.exe** 0xffffffff -ForceV1

File create

WinATP-Intro-Backdoor.exe

SHA1 4275111a18db150e28b6a6c4002fa9b5b19675e6

Path C:\Users\administrator1\Desktop\WinATP-Intro-Backdoor.exe

Time Apr 27, 2020, 4:35:02 PM

Powershell dropped a suspicious file on t... ● Detected ● New Medium ···

Details

Powershell dropped a suspicious file on the machine

Medium **New**

See in timeline · Link to another incident ···

Manage alert

Status: New

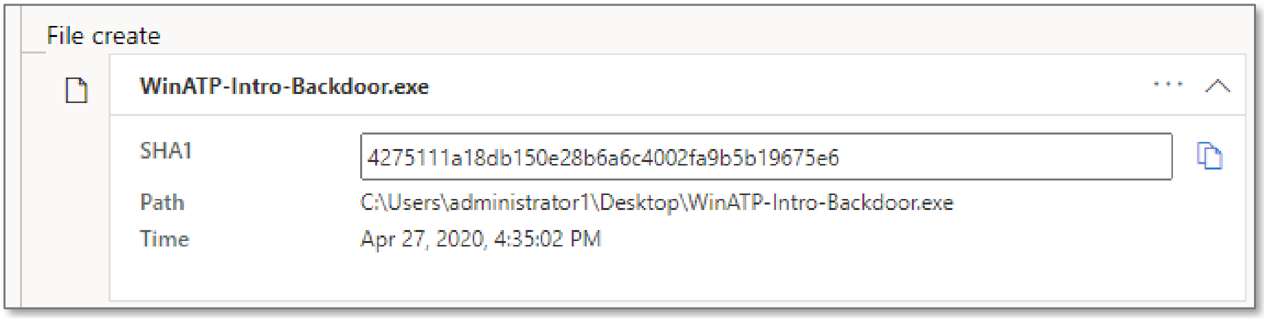
Classification: Select classification...

Alert details

Incident	1
Detection source	EDR
Detection technology	Behavioral
Detection status	Detected

Alert details page

Select the file, under *File create*, in the alert story, to switch to its context in the details pane on the right. Here you can see details about the file, including hashes, size, Virus Total summary, and more. You can also add an indicator or download it directly from the details pane.



File create

WinATP-Intro-Backdoor.exe

SHA1 4275111a18db150e28b6a6c4002fa9b5b19675e6

Path C:\Users\administrator1\Desktop\WinATP-Intro-Backdoor.exe

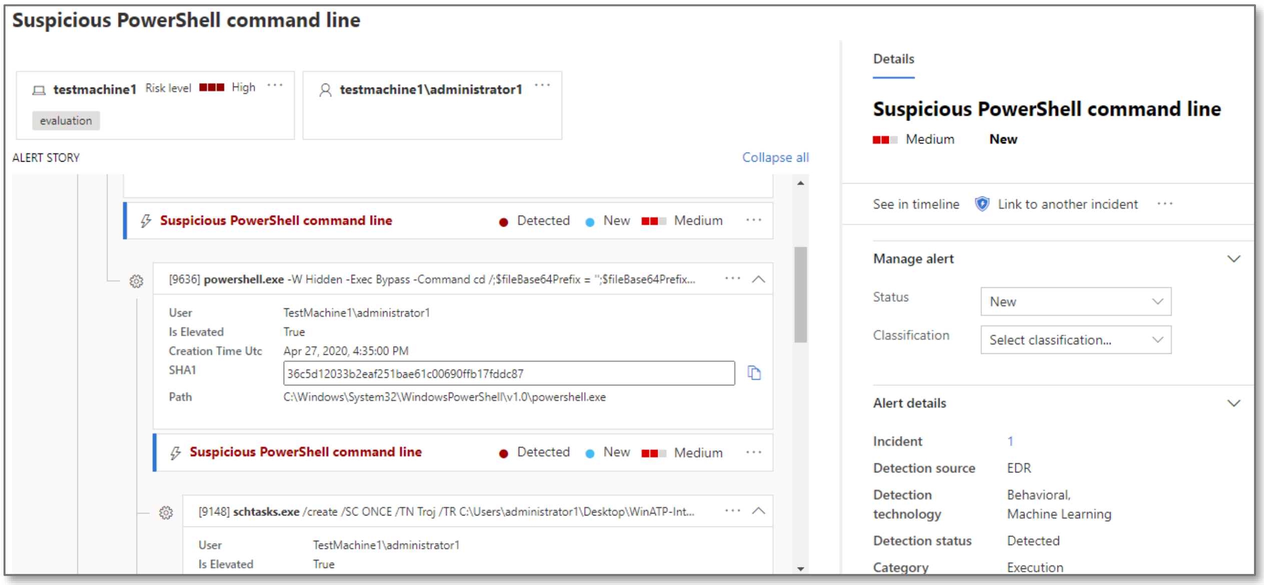
Time Apr 27, 2020, 4:35:02 PM

To inspect the file further, click **Open file page**. For more information about the file page, read Inspect and download the backdoor file.

Alert: Suspicious PowerShell command line

The PowerShell invocation pattern used in the macro exhibited traits indicating stealth and intent to evade detection. This attempt to remain stealthy triggered this alert.

When viewed, the alert page shows more information about the suspicious PowerShell execution, including the full command-line arguments and the base64-encoded script that was executed.



Suspicious PowerShell command line

testmachine1 Risk level ■■■ High ···
evaluation

testmachine1\administrator1 ···

ALERT STORY

Suspicious PowerShell command line ● Detected ● New ■■□ Medium ···

[9636] **powershell.exe** -W Hidden -Exec Bypass -Command cd /;$fileBase64Prefix = '';$fileBase64Prefix...

User	TestMachine1\administrator1
Is Elevated	True
Creation Time Utc	Apr 27, 2020, 4:35:00 PM
SHA1	36c5d12033b2eaf251bae61c00690ffb17fddc87
Path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Suspicious PowerShell command line ● Detected ● New ■■□ Medium ···

[9148] **schtasks.exe** /create /SC ONCE /TN Troj /TR C:\Users\administrator1\Desktop\WinATP-Int...

User	TestMachine1\administrator1
Is Elevated	True

Details

Suspicious PowerShell command line

■■□ Medium **New**

Manage alert

Status	New
Classification	Select classification...

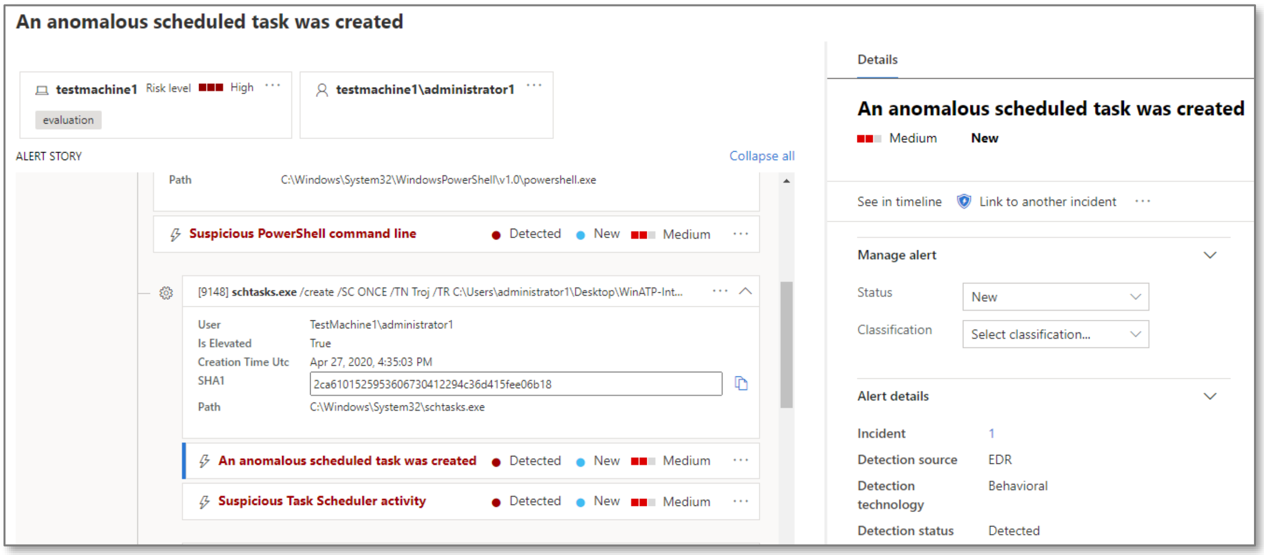
Alert details

Incident	1
Detection source	EDR
Detection technology	Behavioral, Machine Learning
Detection status	Detected
Category	Execution

Suspicious PowerShell command line

Alert: An anomalous scheduled task was created

Attackers also commonly use scheduled tasks as a persistence technique. However, these can also be used for other purposes, such as to delay the next phases of an attack, remaining quiet and stealthy in the process. Regardless of its usage, Microsoft Defender ATP detects anomalous scheduled tasks—including ones that are rare and not seen elsewhere in the organization—and alerts about it.



An anomalous scheduled task was created

testmachine1 Risk level 🟥🟥🟥 High ···

evaluation

testmachine1\administrator1 ···

ALERT STORY

Collapse all

Path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Suspicious PowerShell command line ● Detected ● New 🟥🟥 Medium ···

[9148] **schtasks.exe** /create /SC ONCE /TN Troj /TR C:\Users\administrator1\Desktop\WinATP-Int... ···

User	TestMachine1\administrator1
Is Elevated	True
Creation Time Utc	Apr 27, 2020, 4:35:03 PM
SHA1	2ca6101525953606730412294c36d415fee06b18
Path	C:\Windows\System32\schtasks.exe

An anomalous scheduled task was created ● Detected ● New 🟥🟥 Medium ···

Suspicious Task Scheduler activity ● Detected ● New 🟥🟥 Medium ···

Details

An anomalous scheduled task was created

🟥🟥 Medium **New**

See in timeline · Link to another incident ···

Manage alert

Status	New
Classification	Select classification...

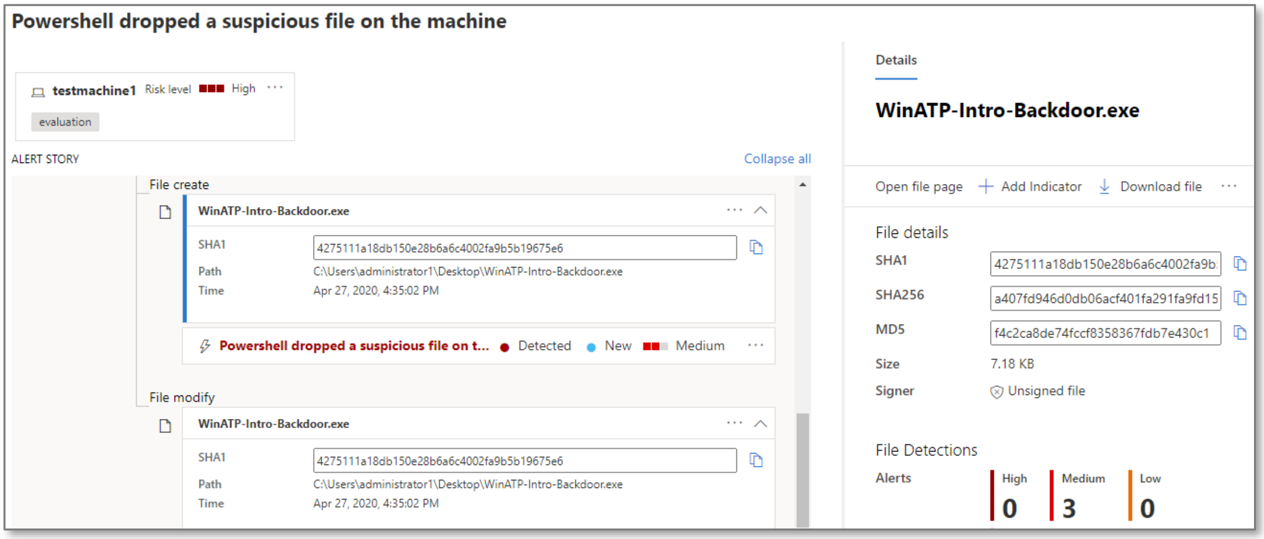
Alert details

Incident	1
Detection source	EDR
Detection technology	Behavioral
Detection status	Detected

Alert for anomalous creation of a scheduled task

Inspect and download the backdoor file

In this simulation, you can inspect the simulated backdoor by selecting its file name, **WinATP-Intro-Backdoor.exe**, on the alert **PowerShell dropped a suspicious file on the machine** and looking at the details pane.



Powershell dropped a suspicious file on the machine

testmachine1 Risk level ■■■ High ···
evaluation

ALERT STORY

Collapse all

File create

WinATP-Intro-Backdoor.exe

SHA1	4275111a18db150e28b6a6c4002fa9b5b19675e6
Path	C:\Users\administrator1\Desktop\WinATP-Intro-Backdoor.exe
Time	Apr 27, 2020, 4:35:02 PM

Powershell dropped a suspicious file on t... ● Detected ● New ■■ Medium ···

File modify

WinATP-Intro-Backdoor.exe

SHA1	4275111a18db150e28b6a6c4002fa9b5b19675e6
Path	C:\Users\administrator1\Desktop\WinATP-Intro-Backdoor.exe
Time	Apr 27, 2020, 4:35:02 PM

Details

WinATP-Intro-Backdoor.exe

Open file page + Add Indicator ↓ Download file ···

File details

SHA1	4275111a18db150e28b6a6c4002fa9b
SHA256	a407fd946d0db06acf401fa291fa9fd15
MD5	f4c2ca8de74fccf8358367fdb7e430c1
Size	7.18 KB
Signer	Unsigned file

File Detections

	High	Medium	Low
Alerts	0	3	0

File details on the alert page

Get detailed information about the file

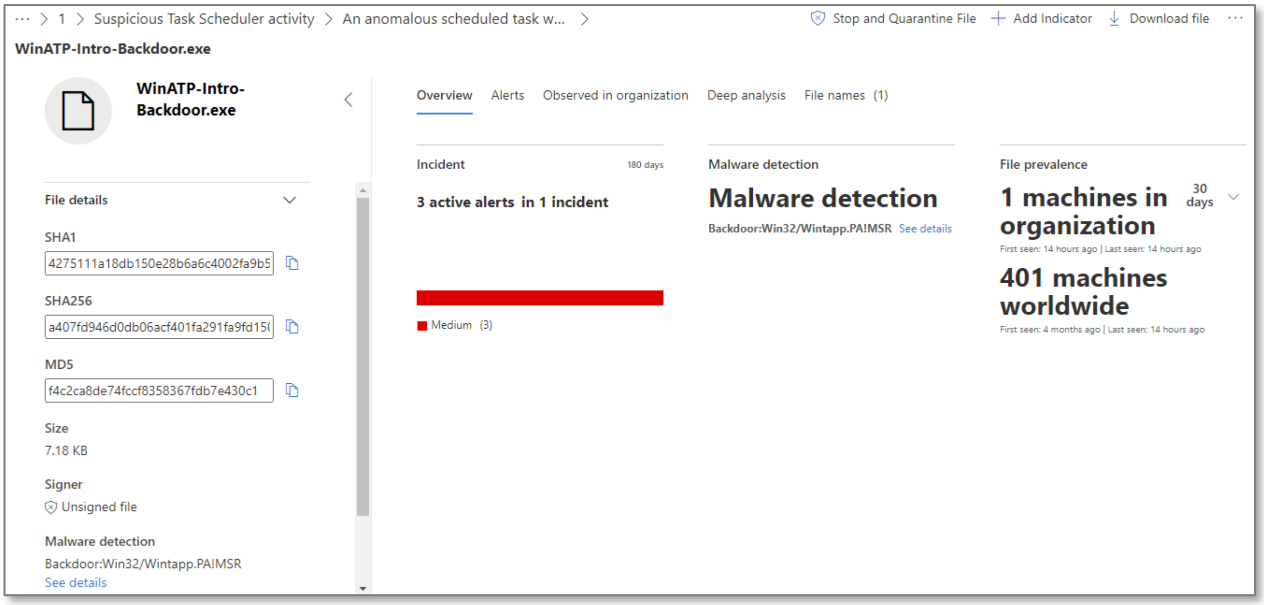
With the file in focus on the details pane, you get comprehensive information about the simulated backdoor, including:

- File hashes
- Signer name if it is validly signed
- Alerts raised on this file
- The number of machines it was observed on, in the organization and worldwide

Here you can download the file or add an indicator for it. To view additional details, click on **Open file page**, where you can view all the above details, as well as:

- Names used by the same file in the organization
- Machines in the organization it was observed on, indicating its origins and the footprint in the organization

To perform further forensics on the file itself, submit the file for deep analysis, which provides automated analysis in a controlled environment, or you can download the file.



··· > 1 > Suspicious Task Scheduler activity > An anomalous scheduled task w... >

Stop and Quarantine File | Add Indicator | Download file ···

WinATP-Intro-Backdoor.exe

WinATP-Intro-Backdoor.exe

File details

SHA1: 4275111a18db150e28b6a6c4002fa9b5

SHA256: a407fd946d0db06acf401fa291fa9fd15(

MD5: f4c2ca8de74fccf8358367fdb7e430c1

Size: 7.18 KB

Signer: Unsigned file

Malware detection: Backdoor:Win32/Wintapp.PA!MSR See details

Overview | Alerts | Observed in organization | Deep analysis | File names (1)

Incident — 180 days

3 active alerts in 1 incident

🟥 Medium (3)

Malware detection

Malware detection

Backdoor:Win32/Wintapp.PA!MSR See details

File prevalence — 30 days

1 machines in organization

First seen: 14 hours ago | Last seen: 14 hours ago

401 machines worldwide

First seen: 4 months ago | Last seen: 14 hours ago

File page for the simulated backdoor

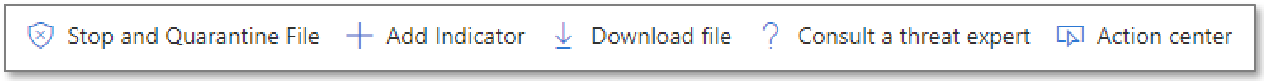
Download the file

To download a file, it must already be in Microsoft Defender ATP sample storage. If the file is not in storage, the action bar shows a **Collect file** option.

Select **Collect file** to gather the file from one of your machines.

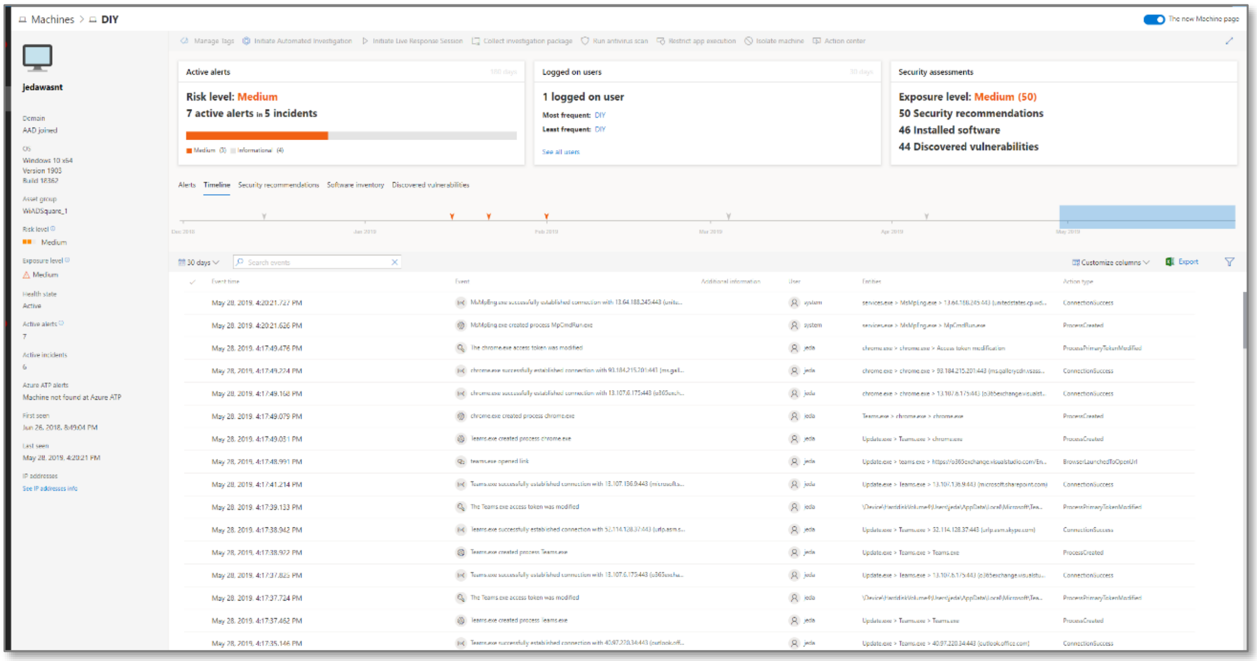
Note: File collection might take several hours depending on the availability of machines.

As soon as the file has been collected, select **Download file** to obtain a copy of the file.



Review the machine timeline

Clicking on the machine name on one of the alert pages opens the machine details page. On this page, the alert itself and related events on the machine are provided to ease investigation. You can scroll through the machine timeline and view all events and behaviors observed on the machine in chronological order.



jedawasnt

Domain
AAD joined

OS
Windows 10 x64
Version 1903
Build 18362

Asset group
WiADSquare_1

Risk level
Medium

Exposure level
Medium

Health state
Active

Active alerts
7

Active incidents
6

Azure ATP alerts
Machine not found at Azure ATP

First seen
Jun 26, 2018, 8:49:04 PM

Last seen
May 28, 2019, 4:20:21 PM

IP addresses
See IP addresses info

Active alerts 180 days
Risk level: Medium
7 active alerts in 5 incidents
Medium (3) Informational (4)

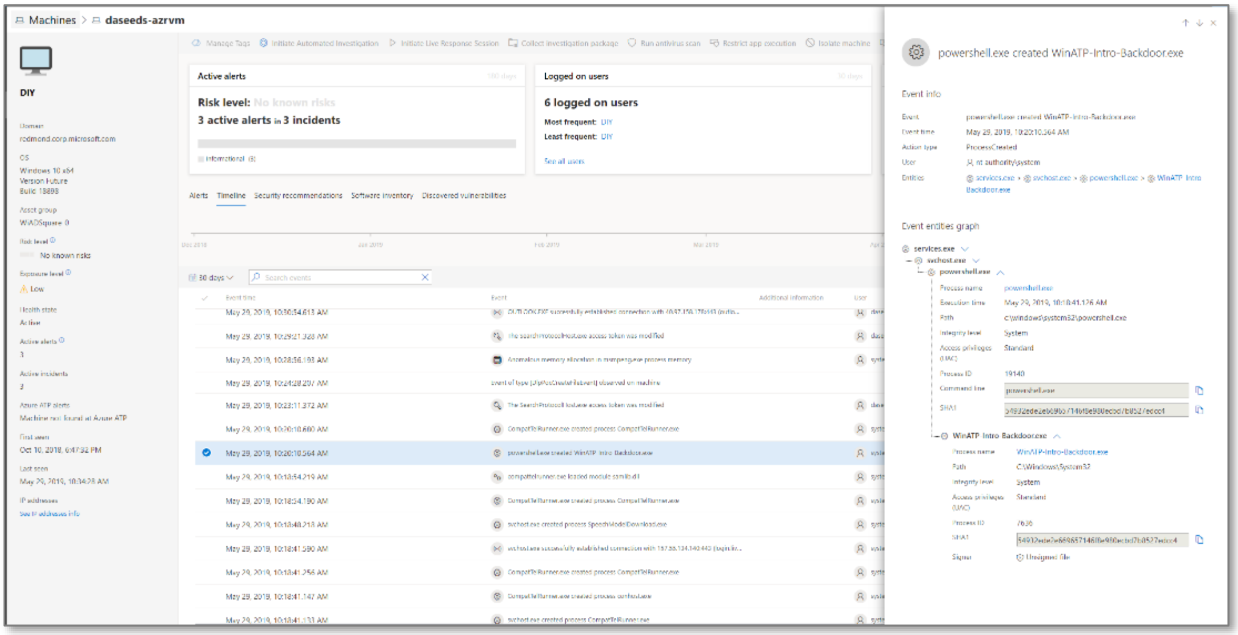
Logged on users 30 days
1 logged on user
Most frequent: DIY
Least frequent: DIY
See all users

Security assessments
Exposure level: Medium (50)
50 Security recommendations
46 Installed software
44 Discovered vulnerabilities

Event time	Event	Additional information	User	Entities	Action type
May 28, 2019, 4:20:21.727 PM	MsMpEng.exe successfully established connection with 13.64.188.245:443 (unite...		system	services.exe > MsMpEng.exe > 13.64.188.245:443 (unitedstates.cp.wd...	ConnectionSuccess
May 28, 2019, 4:20:21.626 PM	MsMpEng.exe created process MpCmdRun.exe		system	services.exe > MsMpEng.exe > MpCmdRun.exe	ProcessCreated
May 28, 2019, 4:17:49.476 PM	The chrome.exe access token was modified		jeda	chrome.exe > chrome.exe > Access token modification	ProcessPrimaryTokenModified
May 28, 2019, 4:17:49.224 PM	chrome.exe successfully established connection with 93.184.215.201:443 (ms.gal...		jeda	chrome.exe > chrome.exe > 93.184.215.201:443 (ms.gallerycdn.vsass...	ConnectionSuccess
May 28, 2019, 4:17:49.168 PM	chrome.exe successfully established connection with 13.107.6.175:443 (o365exch...		jeda	chrome.exe > chrome.exe > 13.107.6.175:443 (o365exchange.visualst...	ConnectionSuccess
May 28, 2019, 4:17:49.079 PM	chrome.exe created process chrome.exe		jeda	Teams.exe > chrome.exe > chrome.exe	ProcessCreated
May 28, 2019, 4:17:49.031 PM	Teams.exe created process chrome.exe		jeda	Update.exe > Teams.exe > chrome.exe	ProcessCreated
May 28, 2019, 4:17:48.991 PM	teams.exe opened link		jeda	Update.exe > teams.exe > https://o365exchange.visualstudio.com/En...	BrowserLaunchedToOpenUrl
May 28, 2019, 4:17:41.214 PM	Teams.exe successfully established connection with 13.107.136.9:443 (microsoft.s...		jeda	Update.exe > Teams.exe > 13.107.136.9:443 (microsoft.sharepoint.com)	ConnectionSuccess
May 28, 2019, 4:17:39.133 PM	The Teams.exe access token was modified		jeda	\Device\HarddiskVolume4\Users\jeda\AppData\Local\Microsoft\Tea...	ProcessPrimaryTokenModified
May 28, 2019, 4:17:38.942 PM	Teams.exe successfully established connection with 52.114.128.37:443 (urlp.asm.s...		jeda	Update.exe > Teams.exe > 52.114.128.37:443 (urlp.asm.skype.com)	ConnectionSuccess
May 28, 2019, 4:17:38.922 PM	Teams.exe created process Teams.exe		jeda	Update.exe > Teams.exe > Teams.exe	ProcessCreated
May 28, 2019, 4:17:37.825 PM	Teams.exe successfully established connection with 13.107.6.175:443 (o365excha...		jeda	Update.exe > Teams.exe > 13.107.6.175:443 (o365exchange.visualstu...	ConnectionSuccess
May 28, 2019, 4:17:37.724 PM	The Teams.exe access token was modified		jeda	\Device\HarddiskVolume4\Users\jeda\AppData\Local\Microsoft\Tea...	ProcessPrimaryTokenModified
May 28, 2019, 4:17:37.462 PM	Teams.exe created process Teams.exe		jeda	Update.exe > Teams.exe > Teams.exe	ProcessCreated
May 28, 2019, 4:17:35.146 PM	Teams.exe successfully established connection with 40.97.220.34:443 (outlook.off...		jeda	Update.exe > Teams.exe > 40.97.220.34:443 (outlook.office.com)	ConnectionSuccess

Machine timeline with behaviors

Expanding some of the more interesting behaviors provides useful details, such as process trees and file creation relationships. For example, clicking on the item **powershell.exe created WinATP-Intro-Backdoor.exe** displays the full process tree for this behavior.



Machines > daseeds-azrvm

Manage Tags
Initiate Automated Investigation
Initiate Live Response Session
Collect investigation package
Run antivirus scan
Restrict app execution
Isolate machine

DIY

Domain
redmond.corp.microsoft.com

OS
Windows 10 x64
Version Future
Build 18898

Asset group
WiADSquare 0

Risk level
No known risks

Exposure level
Low

Health state
Active

Active alerts
3

Active incidents
3

Azure ATP alerts
Machine not found at Azure ATP

First seen
Oct 10, 2018, 6:47:32 PM

Last seen
May 29, 2019, 10:34:28 AM

IP addresses
See IP addresses info

Active alerts — 180 days

Risk level: No known risks
3 active alerts in 3 incidents
Informational (3)

Logged on users — 30 days

6 logged on users
Most frequent: DIY
Least frequent: DIY
See all users

Event time	Event	Additional information	User
May 29, 2019, 10:30:54.613 AM	OUTLOOK.EXE successfully established connection with 40.97.158.178:443 (outlo...		dave
May 29, 2019, 10:29:21.328 AM	The searchProtocolHost.exe access token was modified		dase
May 29, 2019, 10:28:56.193 AM	Anomalous memory allocation in msmpeng.exe process memory		syste
May 29, 2019, 10:24:28.207 AM	event of type [ZipPostCreateFileEvent] observed on machine		
May 29, 2019, 10:23:11.372 AM	The SearchProtocolHost.exe access token was modified		dase
May 29, 2019, 10:20:10.680 AM	CompatTelRunner.exe created process CompatTelRunner.exe		syste
May 29, 2019, 10:20:10.564 AM	powershell.exe created WinATP-Intro-Backdoor.exe		syste
May 29, 2019, 10:18:54.219 AM	compattelrunner.exe loaded module samlib.dll		syste
May 29, 2019, 10:18:54.190 AM	CompatTelRunner.exe created process CompatTelRunner.exe		syste
May 29, 2019, 10:18:48.213 AM	svchost.exe created process SpeechModelDownload.exe		syste
May 29, 2019, 10:18:41.590 AM	svchost.exe successfully established connection with 157.55.134.140:443 (login.liv...		syste
May 29, 2019, 10:18:41.256 AM	CompatTelRunner.exe created process CompatTelRunner.exe		syste
May 29, 2019, 10:18:41.147 AM	CompatTelRunner.exe created process conhost.exe		syste
May 29, 2019, 10:18:41.131 AM	svchost.exe created process CompatTelRunner.exe		syste

powershell.exe created WinATP-Intro-Backdoor.exe

Event info

Event	powershell.exe created WinATP-Intro-Backdoor.exe
Event time	May 29, 2019, 10:20:10.564 AM
Action type	ProcessCreated
User	nt authority\system
Entities	services.exe > svchost.exe > powershell.exe > WinATP-Intro-Backdoor.exe

Event entities graph

services.exe
— svchost.exe
  └ powershell.exe

Process name	powershell.exe
Execution time	May 29, 2019, 10:18:41.126 AM
Path	c:\windows\system32\powershell.exe
Integrity level	System
Access privileges (UAC)	Standard
Process ID	19140
Command line	powershell.exe
SHA1	54932ede2eb69b57146f8e980ecbd7b8527edcc4

└ WinATP-Intro-Backdoor.exe

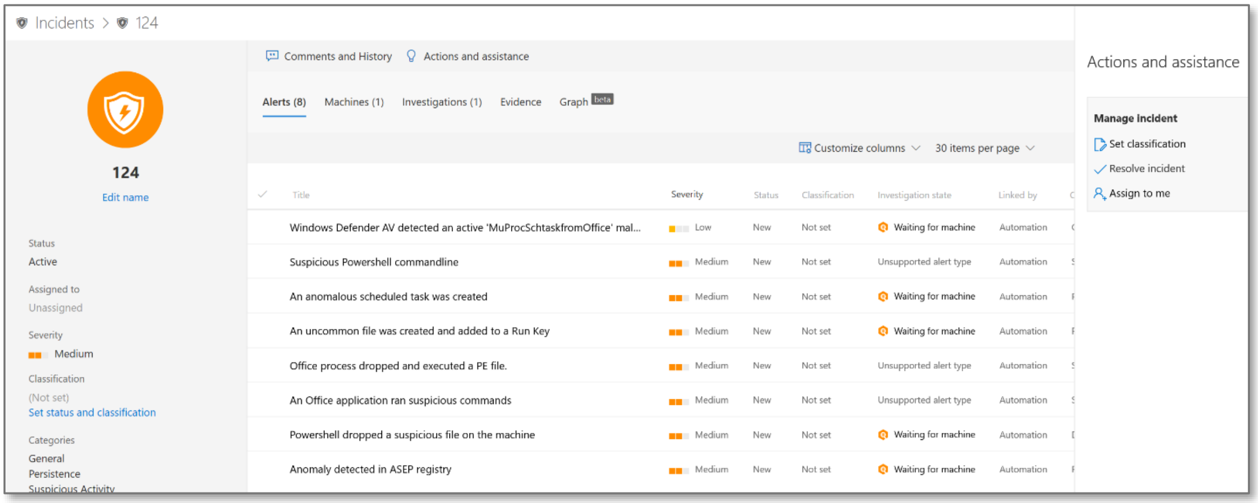
Process name	WinATP-Intro-Backdoor.exe
Path	C:\Windows\System32
Integrity level	System
Access privileges (UAC)	Standard
Process ID	7636
SHA1	54932ede2e6696571468e980ecbd7b8527edcc4
Signer	Unsigned file

Process tree for selected PowerShell file creation behavior

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.



124

Status
Active

Assigned to
Unassigned

Severity
Medium

Classification
(Not set)

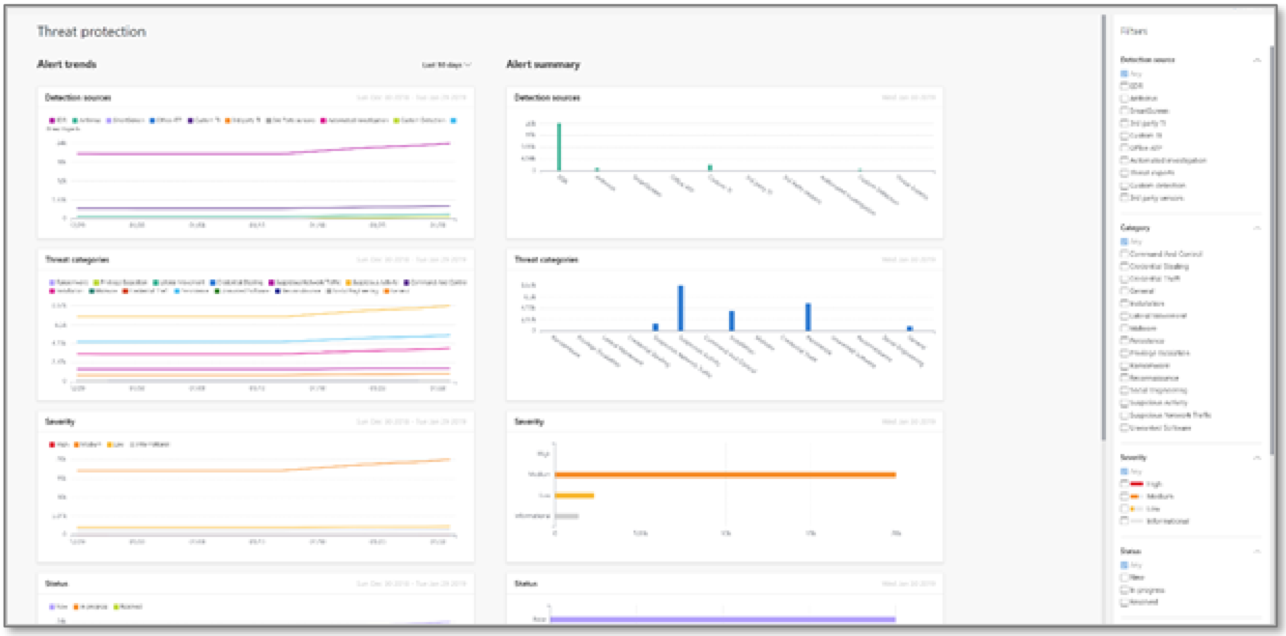
Categories
General
Persistence
Suspicious Activity

Title	Severity	Status	Classification	Investigation state	Linked by
Windows Defender AV detected an active 'MuProcSchtaskfromOffice' mal...	Low	New	Not set	Waiting for machine	Automation
Suspicious Powershell commandline	Medium	New	Not set	Unsupported alert type	Automation
An anomalous scheduled task was created	Medium	New	Not set	Waiting for machine	Automation
An uncommon file was created and added to a Run Key	Medium	New	Not set	Waiting for machine	Automation
Office process dropped and executed a PE file.	Medium	New	Not set	Unsupported alert type	Automation
An Office application ran suspicious commands	Medium	New	Not set	Unsupported alert type	Automation
Powershell dropped a suspicious file on the machine	Medium	New	Not set	Waiting for machine	Automation
Anomaly detected in ASEP registry	Medium	New	Not set	Waiting for machine	Automation

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.



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 a common attack and walked through how Microsoft Defender ATP surfaces that attack. We saw what the alerts look like and the detailed contextual file, machine, and event information provided with each alert.

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!