Microsoft

Microsoft Defender Advanced Threat Protection

Attack simulation

Scenario 1: Document drops backdoor

July 2019

Copyright

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:

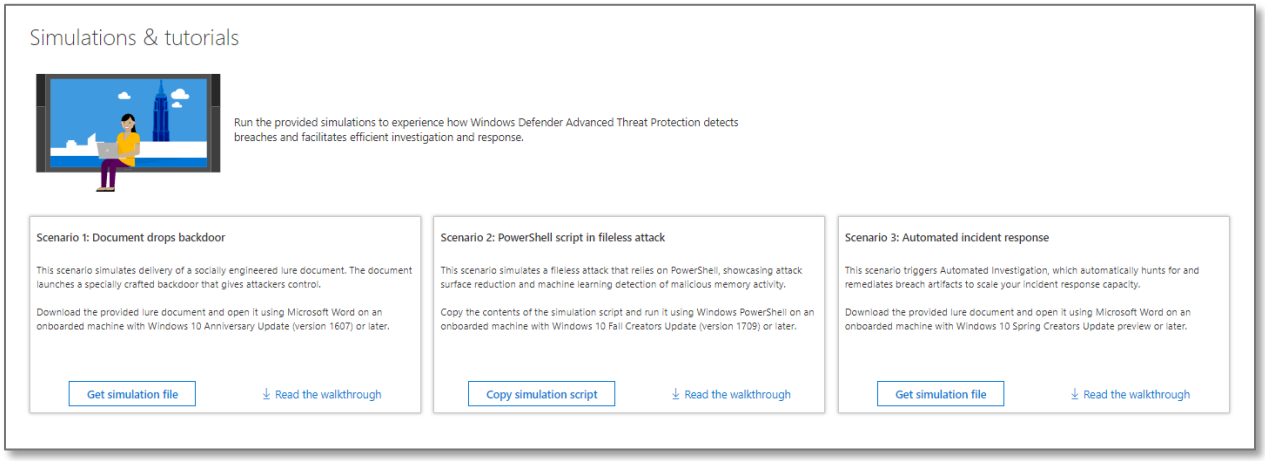
- Be onboarded to Microsoft Defender ATP
- Run Windows 10 Anniversary Update (version 1607) or later
- Have PowerShell turned on
- Have Windows Defender Antivirus turned on
- Have Microsoft Word installed

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**.



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**.

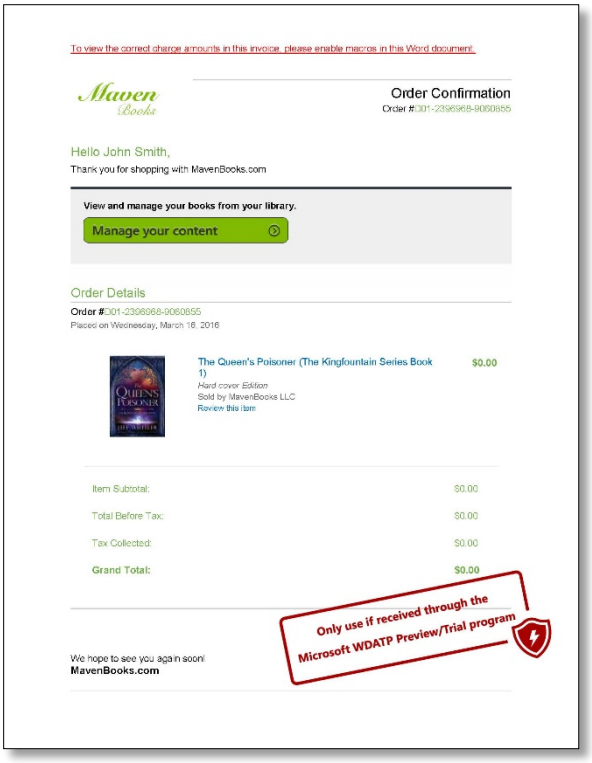
3. Copy the lure document to the test machine.

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 #:001-2396968-9060855

Hello John Smith,

Thank you for shopping with MavenBooks.com

View and manage your books from your library.

Manage your content

Order Details

Order #:001-2396968-9060855

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

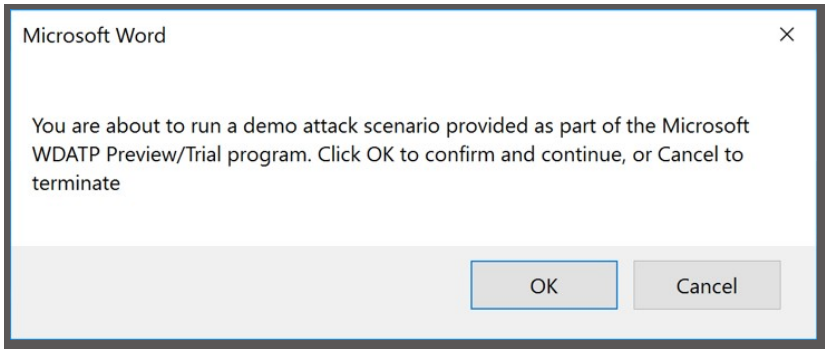
Item Subtotal:	$0.00
Total Before Tax:	$0.00
Tax Collected:	$0.00
Grand Total:	**$0.00**

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

We hope to see you again soon!
MavenBooks.com

The lure document

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



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.

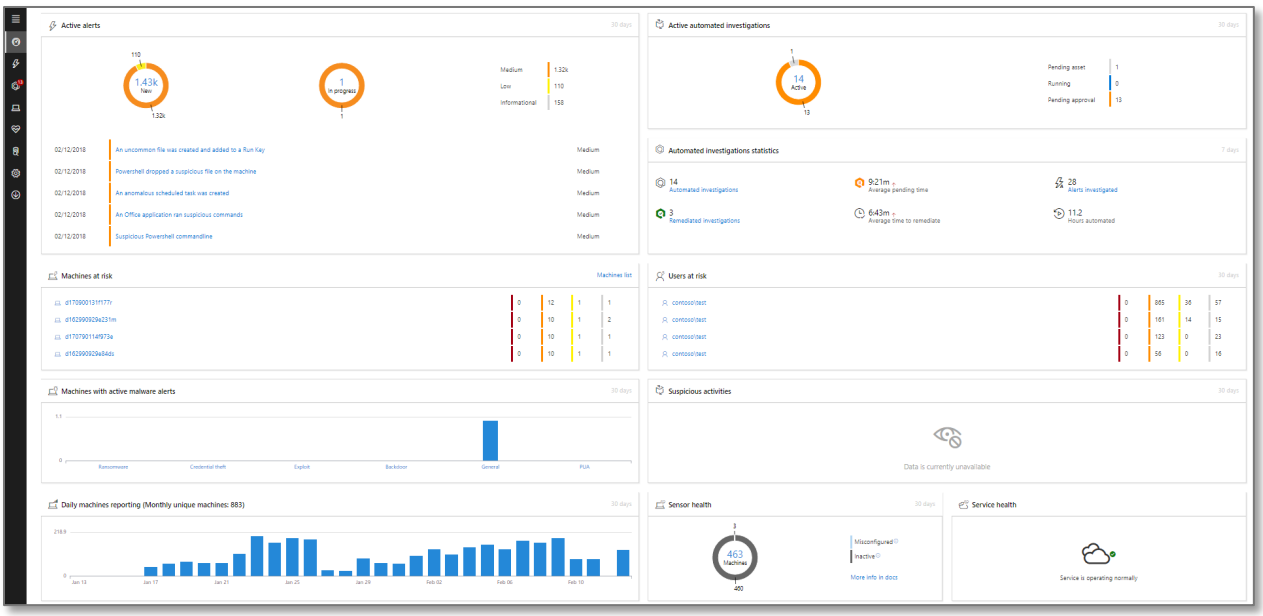
Next, let's review and investigate the Microsoft Defender ATP alerts that surface the simulated attack.

✎ **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.



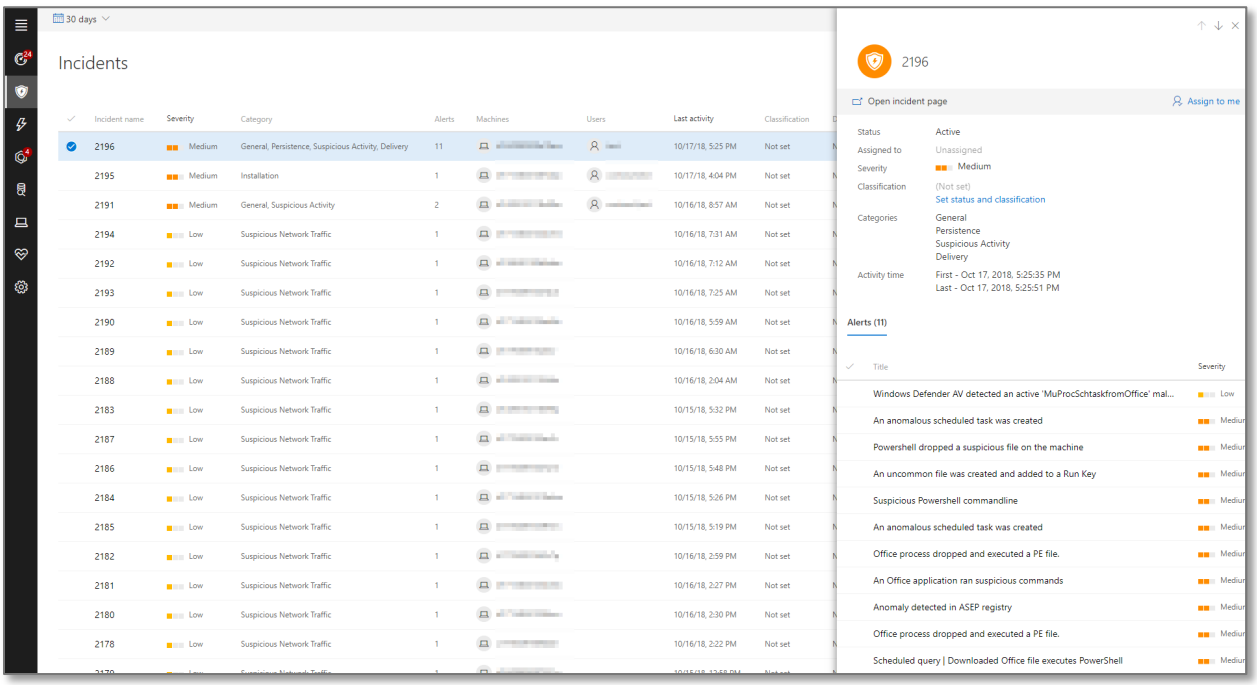
Dashboard view showing the alerts

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.

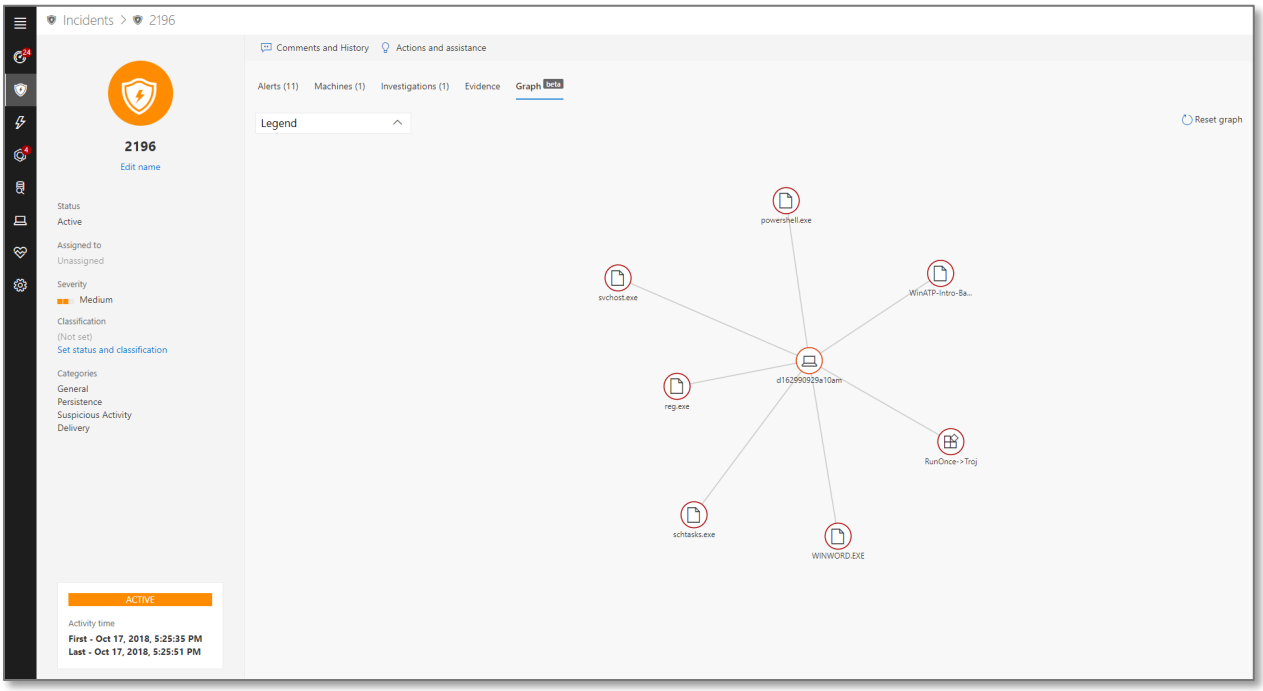
To view the incident, go to the **Incidents** queue and select the relevant item as shown below. A side panel displays additional information about the incident, including all the related alerts.



Incident aggregating alerts generated during the simulation

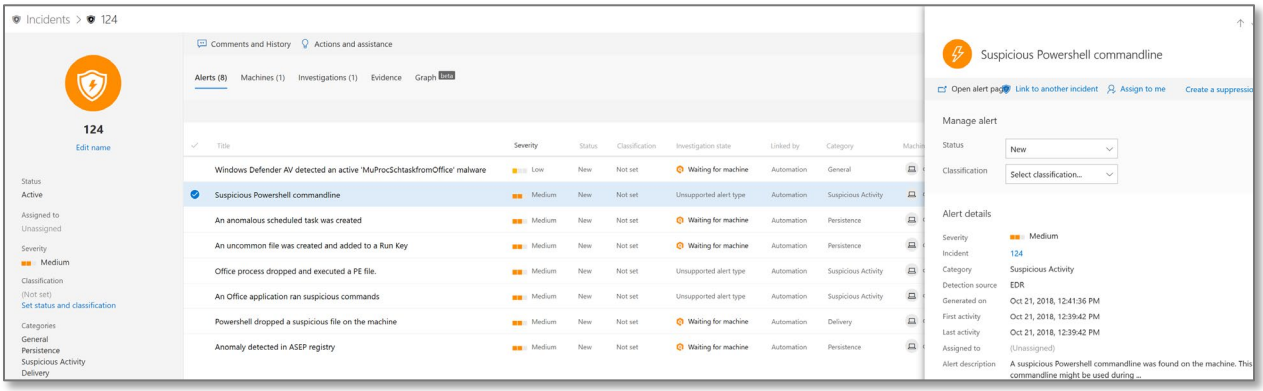
Select **Open incident page** to get more information about the incident.

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**.



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



Actions and assistance options for managing the incident

Review generated alerts

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

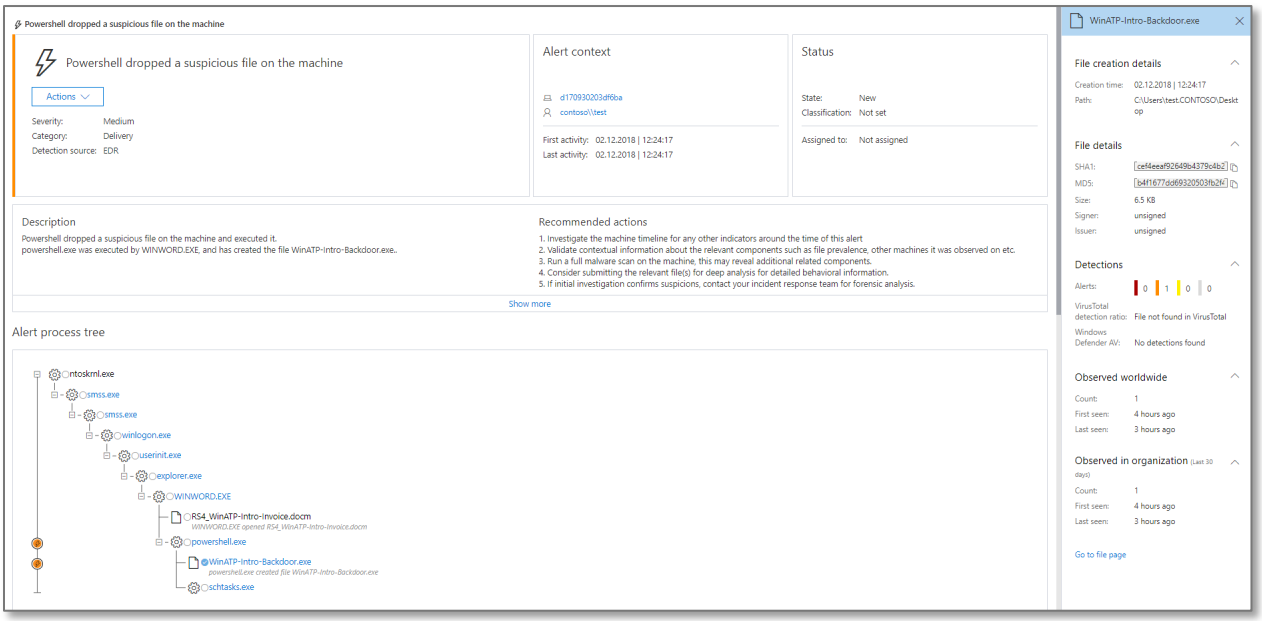
Note: We will walk through only a few of the alerts generated during the simulated attack. Depending on the version of Windows and the Windows Defender Antivirus protection updates running on your test machine, you might see more alerts and they might appear in a slightly different order.

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 machine details page or any of the alert queues, click the name of this alert to see details such as:

- Detailed description and recommended actions
- The process tree related to the files and processes in the alert, including command lines, times of execution, and other details shown in the side pane for selected processes
- The incident graph, including other machines in the organization this file was observed on
- The artifact timeline, providing details of the event(s) that triggered the alert on this machine, including time observed, as well as the name, path and SHA1 hash of the dropped file.



Alert details page

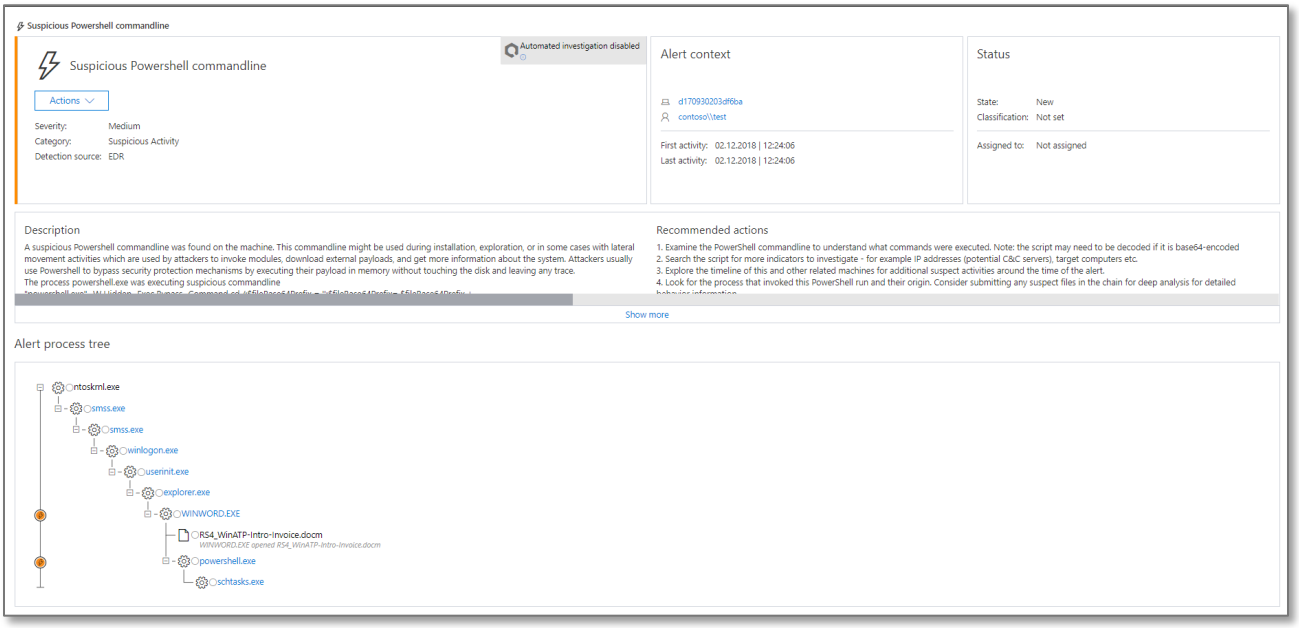
Select the file in the alert process tree (checking the circle next to it) to display the File Details pane at right. Here you can see details about the file, including hashes, size, Virus Total summary, and more.

To inspect the file further, select **Go to file page**. For more information about the file page, read Inspect and download the backdoor file.

Alert: Suspicious PowerShell commandline

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.

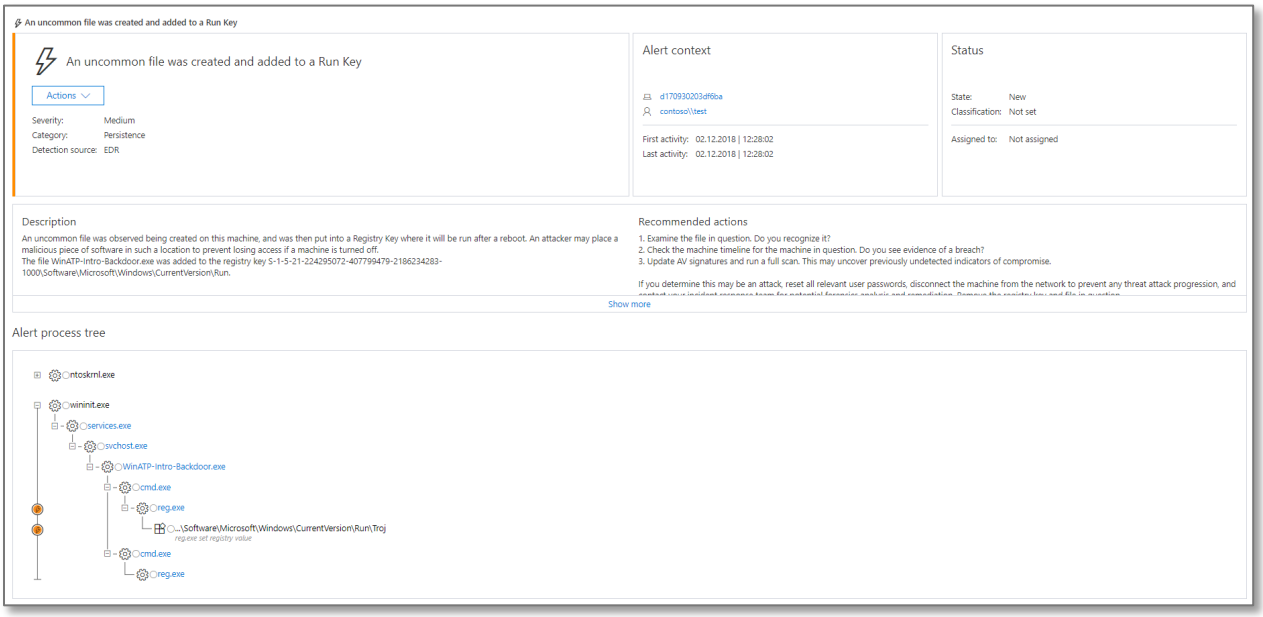
When viewed, the alert details show more information about the suspicious PowerShell execution, including the full command-line arguments and the base64-encoded script that was executed.



Suspicious PowerShell commandline

Alert: An uncommon file was created and added to a Run Key

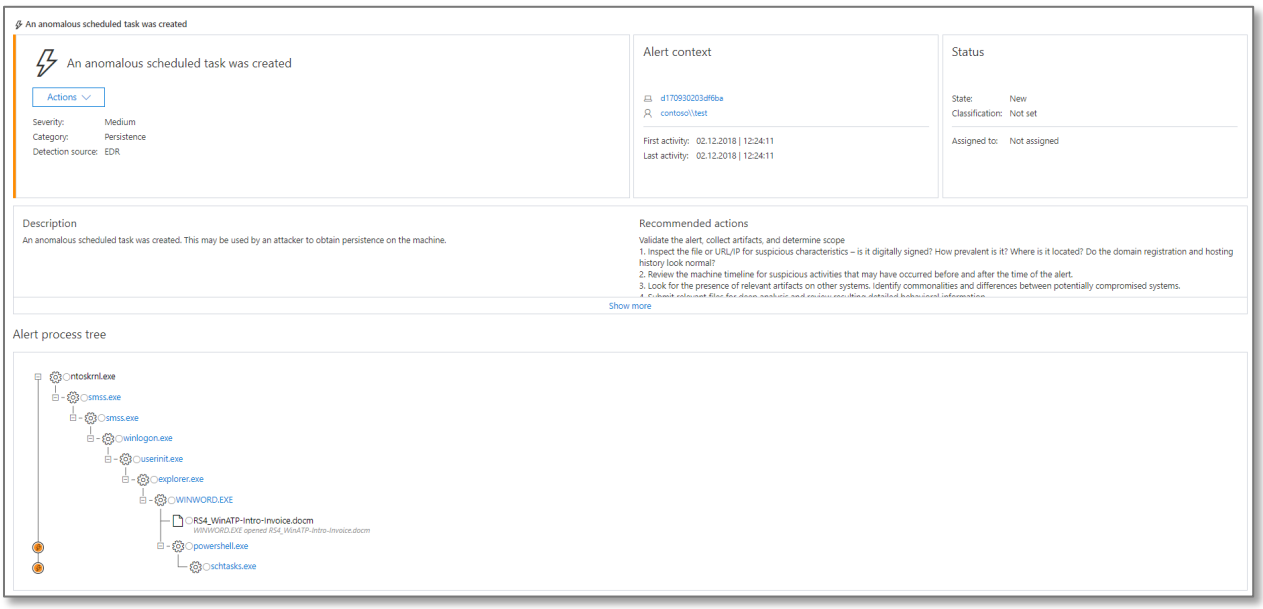
A common technique used by attackers to obtain long-term persistence on victim machines is to register for automatic start after reboot using one of several ASEP (Automatic Start Extensibility Point) registry keys. Microsoft Defender ATP monitors for such anomalous auto-start registrations, as we see performed on this machine to install our simulated backdoor.



Alert details showing the file and the registry Run key

Alert: An anomalous scheduled task was created

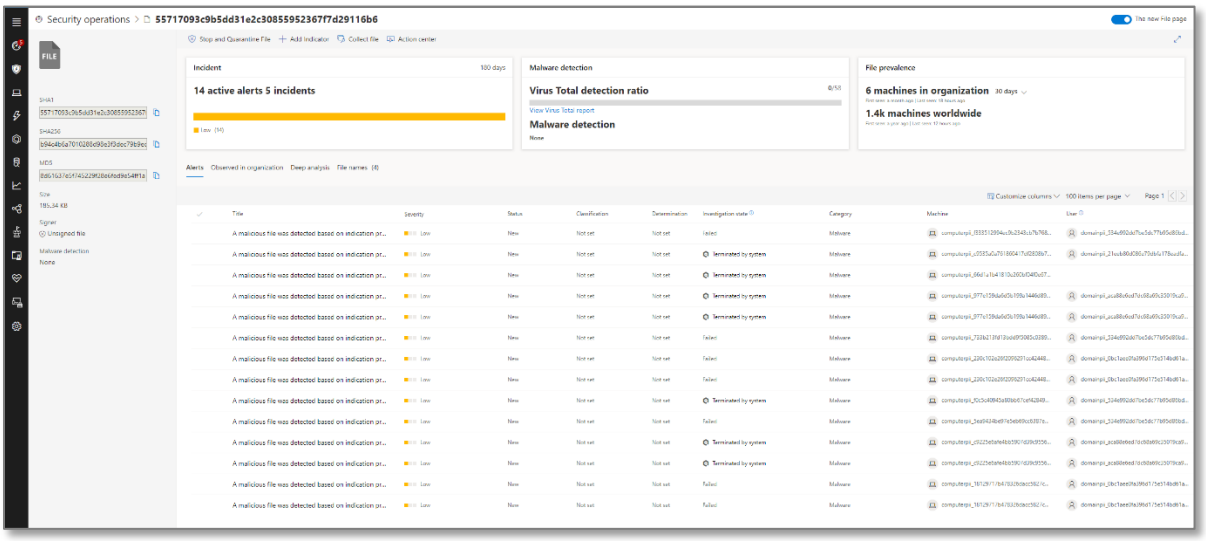
Attackers also commonly use scheduled tasks as a persistence technique. However, these can also be used for other purposes, such as to delay the next phases of an attack, remaining quiet and stealthy in the process. Regardless of its usage, Microsoft Defender ATP detects anomalous scheduled tasks—including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



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**. Selecting **Go to file page** takes you to a full page about the file.



File page for the simulated backdoor

Get detailed information about the file

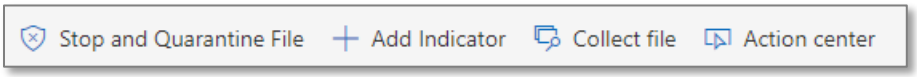
In the file page, you get comprehensive information about the simulated backdoor, including:

- 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
- 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.

Download the file

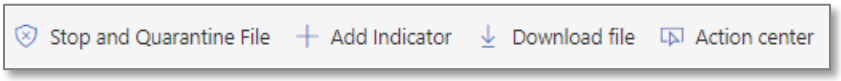
To download a file, it must already be in Microsoft Defender ATP sample storage. If the file is not in storage, the action bar shows a **Collect file** option.



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

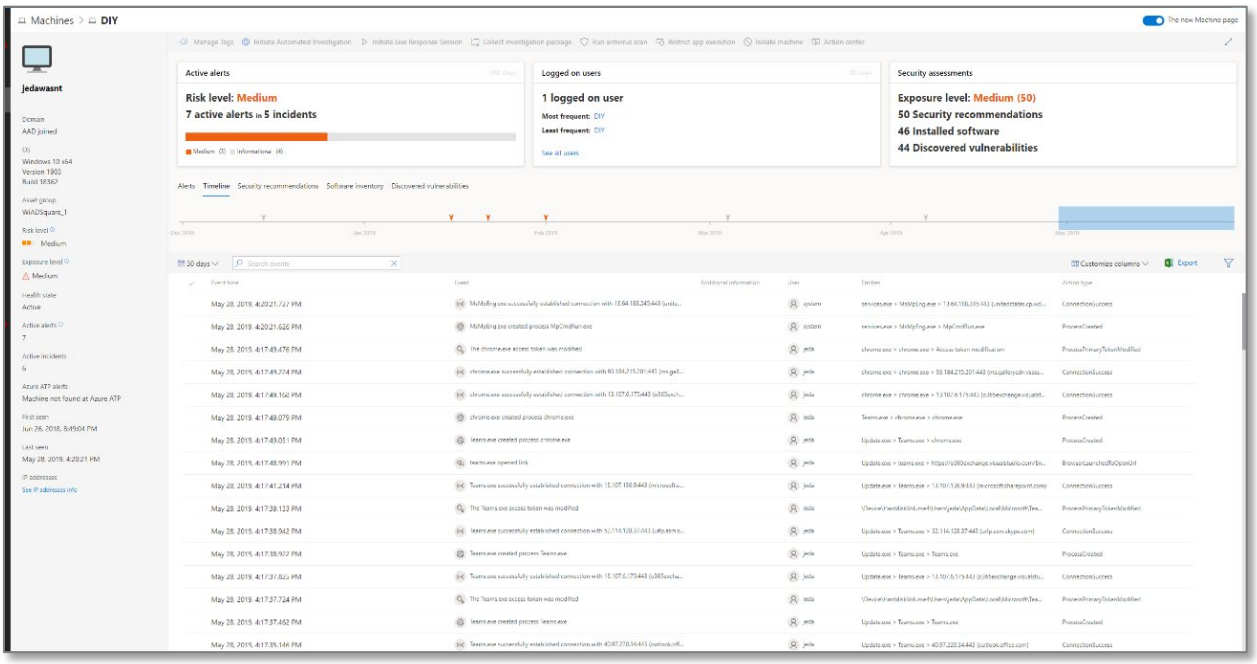
Note: File collection might take several hours depending on the availability of machines.

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



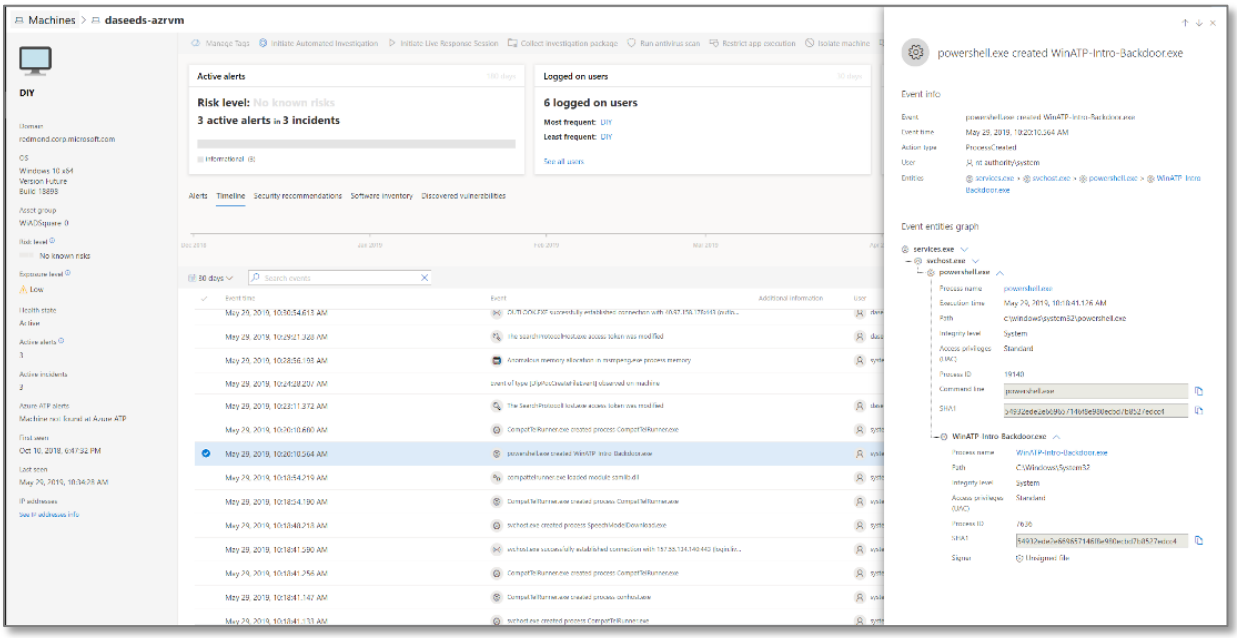
Review the machine timeline

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.



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.

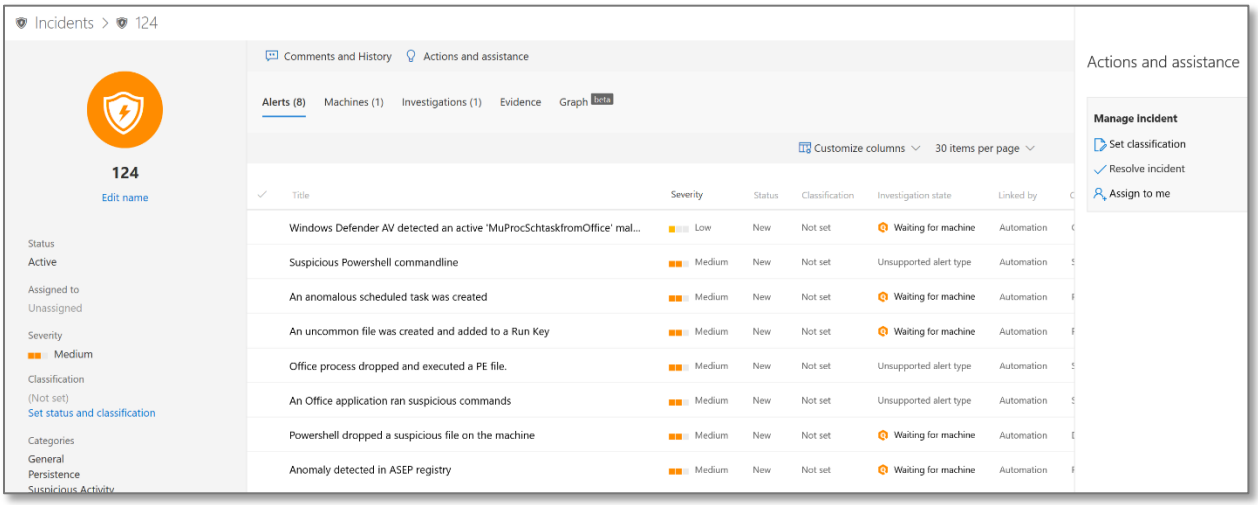


Process tree for selected PowerShell file creation behavior

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.

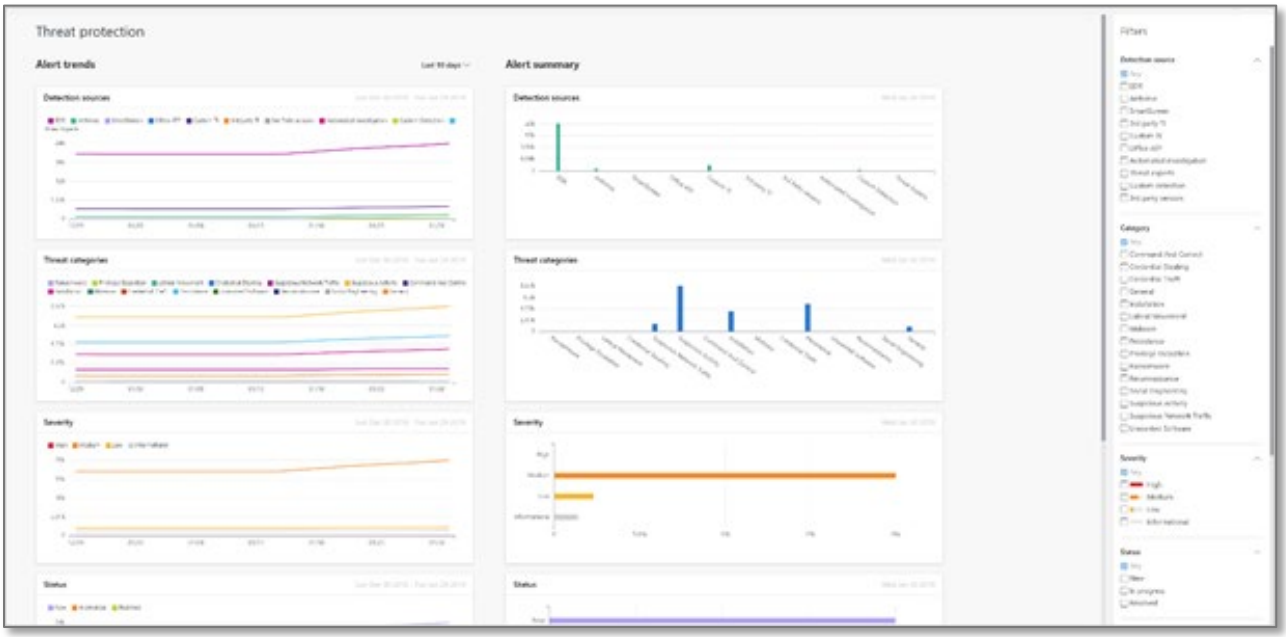
On the incident page, select **Actions and assistance** to get management options that apply to the entire incident and all related alerts.



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!