Attention!

This document is part of a benign demo attack scenario for the Windows Defender Advanced Threat Protection service. It should only be used if received through the Microsoft WDATP Preview/Trial program!

Some information relates to pre-released product, which may be substantially modified before it’s commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

In this part of our introduction to Windows Defender ATP, we’ll take you step-by-step through a typical attack sequence that you will run yourself (don’t worry, it’s not really dangerous!). We’ll simulate an attack using some common techniques, then put on the Security Operation Center (aka SOC) analyst hat and take a tour through the Windows Defender ATP portal to review and investigate alerts and take some responsive actions to thwart the attack.

To run the scenario, you’ll need a machine with the Windows 10 Anniversary Update (version 1607), Creators Update (version 1703) or Fall Creators Update Insider Preview (build 16241 or higher), with Microsoft Office Word installed, and onboarded to your Windows Defender ATP trial/preview tenant.
Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site 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. This document is confidential and proprietary to Microsoft. It is disclosed and can be used only pursuant to a non-disclosure agreement. CONFIDENTIAL. Distribution Only to Partners Under Nondisclosure. Microsoft makes no warranties, express or implied.
1 Detect

Our detection philosophy

It’s simple:

We make sure that if we identify any advanced persistent threat (APT) indicator anywhere in our telemetry, we’ll recognize it when we see it again.

When we alert a security analyst about it near real-time, we provide the relevant context including actor attribution, their victimology, geo-affinity and main tactics. This is realized by maintaining a rich dynamic library of known attack indicators, including known threat components previously observed on user’s machines, script and web page snippets of compromised or malicious websites, IPs, URLs, or domains representing the attacker’s infrastructure, and so forth. This library is constantly updated by new threat intelligence generated from collaboration with partners, shared feeds, and mainly from Microsoft’s own APT hunting and research teams.

New and modified threats are constantly being crafted. We monitor a large set of abnormalities and generic suspicious behaviors on any Windows 10 endpoint in the organization, which might indicate potential unknown actor activity. These monitors raise alerts for the Security Operation Center (aka SOC) analyst to verify, including context of other events occurring around the same time on the relevant machine(s), enabling the SOC analyst to determine risk, establish the scope of breach, determine containment, and finally, respond to, mitigate, and contain the attack.
If you’ve set up your Windows 10 Anniversary Update (version 1607), Creators Update (version 1703) or Fall Creators Update Insider Preview (build 16241 or higher) machine and installed Microsoft Office Word on it, you’re ready to begin!

Quick instructions for onboarding are in the email you received. More detailed ones in case you need them are available here.

Our sample scenario starts with a Word document. Typically, this document (or a link to it) would be sent via email to someone in your organization. Careful social engineering would have been used to ensure the receiver doesn’t suspect a thing and unwittingly opens the document. The document, however, is weaponized with crafted macro code which silently drops a malicious executable file onto the machine (Note: We use a benign executable file in our simulation.) The executable is a backdoor file that attains persistence on the machine and will go on to open a remote shell communication to the attacker, and enabling them to run commands on the victim’s machine. On the Creators Update, the backdoor proceeds to gain control of one of the system processes and inject their malicious code into it, so they can stay in memory and remain undetected in preparation to collect and exfiltrate data to their command and control server. On the Fall Creators Update Preview, configuring key system processes to be protected by the new Exploit Guard feature stops the attacker from manipulating these processes and thus thwarts the attack early on.

Here’s an overview of the activities performed in this guide:

1. Running the attack scenario
2. Attack scenario with Exploit Guard configured (Fall Creators Update Preview)
3. Exploring the portal while investigating resulting alerts
4. Performing deep analysis of suspect files
5. Responding to the attack

Let’s go!
Let’s run an attack demo

To run the attack scenario, follow these steps:

21. Open the **WinATP-Intro-Invoice.docm** Word document from [this location](#) on the machine you have set up to be monitored by Windows Defender ATP (we are skipping the email part for simplicity).

22. Like your typical user, double-click **WinATP-Intro-Invoice.docm** to open the Microsoft Office Word document.

23. The document is password protected. Type **WDATP!diy#** to open it.

24. Click **Enable Content** if the document opens in Protected mode. Click **Enable Macros** in the yellow notification at the top of the opened document (most users will do this with the right lure in the document).

If your organization’s policy blocks macros in Internet-originating documents, you must first unblock this document for **Enable Content** to work. You can do this by selecting the document in the File Explorer, then right-click, select Properties and check the Unblock checkbox.

You may encounter difficulties running the scenario with some 3rd party security products installed on the machine. We recommend using the default out-of-box Windows 10 configuration with Windows Defender AV and Windows Defender ATP enabled.

25. Click **OK** on the message box to confirm running the attack simulation.
26. A few seconds later, two new files are dropped on the machine’s desktop (or Desktop folder): diy_rs3_jscript_executes_ps.js and WinATP-Intro-Backdoorexe.jpg. The former, a file containing JavaScript, is part of the attacker’s delivery mechanism, while the latter, an executable posing as a .jpg picture using the right-to-left-override technique, is the attacker’s backdoor to the compromised machine.

27. The backdoor runs and registers itself for auto-start by writing to the registry ASEP (Auto Start Extensibility Point) ‘run’ key. This results in the backdoor being run automatically after a machine reboot, ensuring the attacker is able to retain control of the machine for the long run.

28. Finally, if you are running on a Creators Update or Fall Creators Update Preview build, the backdoor will proceed to start a trusted system process, in this case RuntimeBroker.exe, and inject malicious shellcode into it so it can continue to operate in this process’s memory while remaining hidden. (Note: if running the Anniversary Update, the scenario ends at the previous step).

29. End the WinATP-Intro-Backdoorexe.jpg process by closing the cmd window.

Fall Creators Update with ExploitGuard

2.10. The Fall Creators Update Preview contains a powerful new feature called Exploit Guard. Exploit Guard provides controls restricting how code runs on machines, and tools to mitigate exploits at runtime. You can read more about Exploit Guard’s capabilities [here](#). Exploit Guard is also fully integrated into Windows Defender ATP for SOC visibility into its encounters. If you are running this build, let’s use it in our attack scenario to demonstrate its capabilities. Specifically, we will configure it to disallow dynamic code execution in our system process of interest, RuntimeBroker.exe. To do that, open PowerShell with administrative privileges and run the following commands:

```powershell
$path = "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\runtimebroker.exe"
$value = ([byte][])0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x11,0x11,0x01,0x01,0x00,0x00,0x0x00,0x01,0x01,0x00,0x00,0x00)
New-Item -Path $path -Force
New-ItemProperty -Path $path -Name "MitigationOptions" -Value $value -PropertyType Binary -Force
```

Exploit Guard configuration on a system process is provided here solely for the purpose of illustrating this functionality and should not be used in production without proper analysis of potential impact to the system.
2 Detect
Let’s run an attack demo

2.11. To watch what happens to the protected RuntimeBroker.exe now, open Task Manager on the
desktop before continuing.

2.12. Now, run the backdoor WinATP-Intro-Backdoorexe.jpg a second time by double-clicking it on the
desktop (do not close the window so we can see it terminated during response actions below). The
backdoor starts the system process RuntimeBroker.exe again, injects its malicious shellcode into it and
attempts to execute it as before - however, this time it is stopped by Exploit Guard, which results in
RuntimeBroker.exe being terminated.

2.13. (Optional) To return the machine’s Exploit Guard configuration to its previous state, run the
following command in the PowerShell window:

```
Remove-ItemProperty -Path $path -Name "MitigationOptions" -Force
```

Congrats – you’re done running the attack!

Our attack simulation stops here. The real attacker, when successful, would likely continue from here to
explore and scan for information, send this collected reconnaissance information to their C&C server,
and use it to follow up with attempts to lateral move within the organization to attractive targets.

Next, we’ll move to explore the reflection of this attack in the Windows Defender ATP portal,
review alerts raised, investigate, and perform the appropriate response actions.

How long before alerts show up?

Our generic behavior monitoring, geared to detect anomalies, requires large-scale processing in the
Windows Defender ATP backend. As a result, some alerts may take longer than others to appear,
depending on complexity. Please allow a few hours (up to 4) for the last of the alerts to be raised before
moving to view the results of the simulation in the Windows Defender ATP portal.

When can I try response features?

If you wish to experiment with response actions before alerts are generated, log on to the portal (see
4.1 & 4.2) and go to ‘Response’ in section 4 below.
Explore
How the attack looks like in the portal

Here, we’ll switch into our defender role and explore the attack from the SOC point of view in the Windows Defender ATP portal:

3.1. Open the Windows Defender ATP portal by navigating to https://securitycenter.windows.com from any machine’s browser

3.2. Log in with your Windows Defender ATP credentials (provided in the email you received)

3.3. The dashboard should display several new alerts for the victim machine resulting from the attack we simulated:

![Image 2: Dashboard view showing the alerts](image-url)
3.4 To view the alerts, navigate to the victim machine in the Machines View:

![Alerts related to this machine](image)

**Image 3: Victim machine with alerts**

While investigating an alert, you can change the status of the alert from New to In Progress to indicate it is being handled and to support your Security Operations Center workflow processes. To do this, click on the circle to the left of the alert timestamp to display the alert side pane, then select In Progress in the alert side pane and provide an optional comment.

Let’s look at some of the alerts raised on behaviors identified by Windows Defender ATP.

You may see more alerts for this machine than the ones described below – we will only describe a subset of them here – and they may appear in slightly different order.

Also, alerts may span over more than one page – use the < and > arrows at the top of the alert list to scroll through the list.
Explore
PowerShell dropped a suspicious file to the machine

3.5. “PowerShell dropped a suspicious file to the machine”

The macro in the Word document we opened used PowerShell to write its executable to disk. Windows Defender ATP monitors executables created from Office applications - including via PowerShell, and looks for files that are not common in the organization or in the world.

Click the alert link to see details about the alert, for example:

- 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.

![Image 4: Alert details page](image)

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.
Clicking on the Go to file page link in the File Details pane (either filename or SHA1) displays the **File View** with additional information about the file, including:

- File hashes
- Signer name, if it is validly signed
- An option to submit the file to Deep Analysis – enabling investigation of the nature of the file (details further below)
- Alerts raised on this file
- The number of machines it was observed on - in the organization and world-wide
- File names observed in the organization
- Machines in the organization it was observed on, to investigate its origins and footprint in the organization.

**Image 5: File View**
3.6. “Suspicious PowerShell commandline”

The PowerShell invocation pattern used in the macro exhibited traits indicating stealth and trying to avoid detection – suspicious behavior triggering this alert. The alert details show more information about the suspicious PowerShell execution including the full command-line arguments – showing the base64-encoded script that was executed.

![Suspicious PowerShell commandline](image6.png)
3.7. “Right-to-Left-Override (RLO) technique observed”

Another indication picked up by Windows Defender ATP regards the file name of the dropped executable – specifically the use of the RLO support, a capability for correctly displaying left- to-right and right-to-left language text together, used here to make the file name appear like it has a “.jpg” extension instead of its true extension of “.exe”. This is typically used to hide the fact that the dropped file is an executable, raising further suspicion that results in an additional alert.

![Image 7: RLO technique observed]
3.7 “An uncommon file was created and added to a Run Key”

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

Image 8: An uncommon file was created and added to a Run Key

If your machine is running the Windows 10 Anniversary Update, the alerts raised because of this attack end here. Please continue to item 3.10 below.

If your machine is running the Windows 10 Creators Update Preview, the following additional alerts represent new activity detected by new memory-based sensors and detection rules.
3.8. “A process was injected with potentially malicious code”

Advanced attackers will use more sophisticated and stealthy methods to persist in memory and better hide from detection tools. One common technique is to operate from within a trusted system process rather than their own executable, making it hard for detection tools and security operations to spot the malicious code. However, the new memory sensors in the Windows Defender ATP Creators Update client now provide unprecedented visibility into a variety of cross-process code injection techniques, and as a result it detects and alerts on the injection to RuntimeBroker.exe observed here:

![Image 9: A process was injected with potentially malicious code](image-url)
Windows Defender ATP detections are often targeting the most invariant aspect of an attack technique. This ensures durability and raises the bar on the attacker’s effort to change their tactics. We employ large-scale learning algorithms to establish normal behavior of common processes within an organization and world-wide, and watch for behaviors of these processes that are out of the norm – which quite often indicates that extraneous code was introduced and running in this otherwise trusted process. Note that this outcome is independent of the specific method used to introduce and execute the malicious code:

![Image 10: Unexpected behavior observed by a process run with no command line arguments](image)

Note - this alert may appear after a little while longer, as its model is machine-learning based and requires more backend processing.
In this case, the abnormal behavior involves communication with an external location. The alert details include the IP address - another indicator that can serve as a pivot during investigation.

Click on the IP address in the Alert Process Tree to navigate to the IP details page:

![Image 11: IP details page](image-url)
3.10. Machine timeline

Clicking on the machine name navigates to the machine page, where the alert and the related events are highlighted to ease investigation. We can scroll through the machine timeline and view all events and behaviors observed on the machine in chronological order, interleaved with the alerts raised.

![Image 12: Machine timeline with behaviors](image12.png)

Expanding some of the more interesting behaviors provides all relevant details such as process trees, file creation relationships, and so forth. For example, click on the `powershell created WinATP-Intro-Backdoorexe.jpg` behavior to display the full process tree for this behavior:

![Image 13: Process tree in machine timeline](image13.png)
3.11. “Suspicious script execution”

In the Fall Creators Update Preview, we've added deeper and wider support for various script execution engines, including dynamically-generated or downloaded PowerShell, JavaScript or VBScript. When our attacker used JavaScript from the Word document’s macro to initiate the compromise, WDATP was now able to see this suspicious behavior and alert on it:

![Image 14: Suspicious script execution alert](image)
3.12. “Exploit Guard blocked Export Address Table access”

Also in the Fall Creators Update Preview, when we ran our backdoor for the second time, after configuring Exploit Guard to protect the RuntimeBroker.exe process, Exploit Guard detected an attempt to run unexpected code in this process and blocked it from executing, causing the process to terminate and by this actually stopping the attack.

This also results in a “Exploit Guard blocked Export Address Table access” alert in the WDATP portal – even though the attack was stopped, the security team is notified that a possible exploitation attempt was made so they can take precautions and be on the alert for a potentially persistent attacker.

Image 15: Exploit Guard blocked Export Address Table access
3.13. Deep Analysis / Detonating interesting timeline artifacts

To get more details about the potential content and behavior of the dropped executable, the file can be submitted to Deep Analysis. This will collect the file from the machine where it resides (if not already collected) and safely execute it in the Windows Defender ATP cloud sandbox, recording all activities observed during its execution.

Try out Deep Analysis on our suspected backdoor:

- In the machine timeline, search for $WinATP-Intro-Backdoorexe.jpg$ (which is really $WinATP-Intro-Backdoorgpj.exe$) and click on the file name to navigate to the file page

- In our scenario, this file is already available in the sample store, so it does not need to be collected from the machine, and deep analysis results are readily available. These results can be refreshed (optional) by clicking the **Submit (or Resubmit)** button in the Deep analysis request section. Fresh deep analysis results will be available in the portal within a few minutes (around 10) after submission.

- In the Deep Analysis section, expand the **Deep analysis summary** to view a summary of recorded behaviors from the last deep analysis run for this file.

![Deep analysis summary section](Image 16: Deep analysis summary section)
3. Explore
Deep analysis of suspect files

Each section can be expanded to view additional details:

![Deep analysis summary and details]

In this example, we can see behaviors such as:

- The malicious file communicating with an external IP
- Performing some memory injection
- Launching a cmd.exe shell
- Modifying the security zone configuration. Often, deep analysis will reveal rich details about the file’s potential activities which may not have been observed on the machine.
Now that you’ve reviewed and confirmed files and machines involved in the attack, it’s time to **perform some response actions to contain and mitigate the attack.**

*Note: Response actions require Windows 10 Creators Update version 1703 or higher*

In the Windows 10 Creators Update, Windows Defender ATP introduces response capabilities such as isolation of compromised machines from the network, stop and quarantine of attack related files, and prevention of further propagation by blocking the file from subsequent execution. We’ll use these capabilities to contain the attack demonstrated here.

### 4.1. Stop and quarantine the dropped backdoor on the victim machine:
This action will stop the backdoor execution and quarantine the file on the victim machine where it was observed running.

- In the search box at top, select **File** search, then search for *WinATP-Intro-Backdoorexe.jpg*
- On the File page, open the **Actions** menu and select **Stop & Quarantine File**.
4 Respond
Stop and quarantine the file

- Type a comment and select Yes to take action on the file. The comment will be saved in the Action center as context for the action.

- In the Action center, you can view the status of the action and the machines to which this action will be applied to.
4 Respond
Stop and quarantine the file

- Log in to the victim machine
- Note the file on the machine’s desktop
  - Within a few minutes, a notification is shown indicating that the file was removed. Note that the process is terminated (if running) and the file removed from the desktop.

![Enterprise Unwanted Application found
This application was removed because it is blocked by your IT security settings.](image)

- Return to the Windows Defender ATP portal, re-open the Action Center, click the Success column and click the machine name.
  Notice a new event WinATP-Intro-Backdoorexe.jpg quarantined is shown in the machine timeline, and a matching “CustomEnterpriseBlock” alert is raised.
4.2. Prevent subsequent execution of the attack on other machines

To prevent further propagation of the attack in the organization, you can issue a block on a file to prevent future read, write, and execution of the file in the organization.

Note: This feature requires Windows Defender AV with cloud-based protection enabled in your organization. To ensure it is enabled, open Windows Defender Security Center > Virus & threat protection > Virus & threat protection settings on the victim machine and ensure Real-time protection and Cloud-delivered Protection are On.

Return to the Windows Defender ATP portal to enable the Block File feature:

- In the navigation pane, select Preferences setup > Advanced features > Block file.
- Toggle the setting to On
4 Respond
Block the file from running in the organization

- Go to the *WinATP-Intro-Backdoorexe.jpg* file page, open the Actions menu and select **Block File**.

- Type a comment and select **Yes** to act on the file.

- Allow ~10 minutes from the time the block command was invoked for it to take effect across machines.

- Log in to a different onboarded machine (preferred, however, if a second machine is not available you can re-use the victim machine)

- Run the same **attack** (open the doc file and enable the macro as before) on the machine.

- Observe that the WinATP-Intro-Backdoorexe.jpg is not allowed to run anymore.

- A notification that the file was blocked should appear on the machine.

- Notice a new event *WinATP-Intro-Backdoorexe.jpg was blocked by enterprise response policy* is shown in the machine timeline, and a matching “CustomEnterpriseBlock” alert is raised.

**Note:** You can remove the file from the blocked file list by opening the Actions menu and select **Remove file from blocked list**.
4

Respond
Disrupt attacker activity on compromised machines

While we have remediated the file from the compromised machine, depending on the sensitivity of the machine or severity of the attack, you may want to take additional actions and disrupt additional attacker activities on the compromised machine.

4.1. Restrict applications from running

In the Creators Fall update (build 16257 or above) we’ve added the ability to lock down a machine and prevent subsequent attempts of potentially malicious programs from running.

The action to restrict app execution applies a code integrity policy that only allows running of files that are signed by a Microsoft issued certificate. This can help prevent an attacker from performing further malicious activities.

*Note: This action is reversible and you’ll be able to undo app execution restriction on the machine.*

- In the portal, navigate to the victim machine page
- Open the actions menu and select **Restrict app execution**
- Type a comment and select **Yes** to confirm

- A few minutes later, log in to the victim machine.
- Try to run non-Microsoft signed 3rd party applications and observe execution blocked. In an attack scenario, this will interfere with the attacker’s ability to deliver & execute malicious files on the victim’s machine.
4.2. Isolate the machine from the network to disrupt and disconnect the attacker.

Depending on the sensitivity of the machine or severity of the attack, you may want to isolate the machine from the network to disrupt the attack and prevent further attacker activities, this operation will disconnect the victim machine from the network while retaining connectivity to Windows Defender ATP service.

*Note: This action is reversible and you’ll be able to reconnect the machine to the network.*

- In the portal, navigate to the victim machine page
- Open the actions menu and select **Isolate machine**
- Type a comment and select **Yes** to confirm isolating the machine

A few minutes later, log in to the victim machine. Note: while the machine is isolated, connection through RDP is not available.

- Try to navigate to an Internet website and observe communication is unsuccessful. In an attack scenario, this will interfere with the attacker’s ability to control the victim machine and their ability to perform further malicious activity.
- If there are other machines on the network, you can attempt connections to them as well and note connection is unsuccessful. This is intended to prevent lateral movement.
- Return to the Windows Defender ATP portal, close and re-open the action center. You’ll notice the isolation configuration was applied and a new event in the machine timeline represents this action.
4.3. Forensic data collection.

After containing the attack, you can collect an investigation package from the machine to help identify the current state of the machine and collect evidence of more tools and techniques used by the attacker. The investigation package contains a rich set of data points such as: running processes, installed programs, network information, persistency, User & Groups, Event logs, Prefetch files and more.

- On the victim machine page, open the Action menu and click **Collect investigation package**
- This operation executes on the victim machine and collects data related to suspicious events. The collection can take up to 15 minutes to complete.
- Allowing time for the operation to complete, close and re-open the Action center. Once completed, you can select **Package available** to download the package.
- Extract the package and view the results.
4 Respond

Undo the execution restriction, network isolation

Now that you have verified the malicious file was removed and confirmed, possibly with the help of the forensics package, that there are no additional remnants of the attack on the machine, you can undo execution restriction and/or reconnect the machine to the network depending on the response actions taken.

4.4. Remove app execution restrictions

- On the machine page, open the Action menu and select **Undo restrict app execution**
- The application execution restriction policy will no longer apply on the machine.

4.5. Reconnect the machine to the network.

- On the machine page, open the Action menu and select **Undo machine isolation**
- The machine will be reconnected to the network.

To summarize, using Windows Defender ATP response capabilities, you we able to:

- Contain the attack by stopping the backdoor communication and quarantining the file
- Block the file across the entire organization, to prevent further propagation
- Disrupt additional attacker activities on the machine by restricting app execution and/or isolating the machine the network
- Collect forensic data to identify status and additional attack remnants

**Note:** If you want to experiment with response capabilities again, you can re-run the attack scenario on a different machine – by running the steps in Section 2 above - then follow directly with Section 4. Before running, verify that you have removed the file from the blocked files list in the file Action menu.
5 Respond

Resolving the alerts

5.1. Resolving alerts

When you’ve completed investigating the alerts, made a determination of their correctness, and taken remediation steps as needed, you will want to resolve the relevant alerts to remove them from the active alerts queue.

To change the alert status, click on the circle next to the alert (in the Alerts queue or machine/file/IP page) or the vertical ellipsis “…” at the top right hand side (in the Alert page) to manage the alert.

When resolving, select the conclusion for the alert:

- True alert – the alert correctly identified malicious activity
- False alert – the alert incorrectly identified benign activity

In either case, provide additional information about the nature of the detection by choosing the most appropriate classification.

This concludes our example attack scenario, its investigation in the Windows Defender ATP portal and the remediation actions taken for it.

We hope you like what you see, and hopefully also have feedback to give us about the product’s look & feel, the attack simulation, generated alerts, file deep analysis, investigation capabilities and experience and finally response actions.
Thank you again
for your time and collaboration!