Microsoft

Windows Defender Advanced Threat Protection

攻撃シミュレーション

シナリオ 1: ファイル ベースの バックドア型マルウェア

Copyright

Windows Defender ATP

Microsoft

マイクロソフトの攻撃検出の指針

シンプルです。

高度で持続的な攻撃 (APT) の兆候や攻撃手法がテレメトリによって可視化されます。このため、迅速に攻撃の予兆を検知し関連するアラートを発行することができます。

アラートはほぼリアルタイムで発行されます。そのとき、攻撃者の属性、被害に関する情報、地理的な親和性、主な攻撃手法を含むコンテキストも提供します。このようなコンテキスト情報を提供できるのは、以前に実際のマシンで見つかった脅威コンポーネント、感染したサイトや悪意のあるサイトの IP、URL、そこで見つかったスクリプトまたは Web ページの一部、攻撃者のドメインなど、既知の攻撃のサインを集めたリッチでダイナミックなライブラリがあるからです。マイクロソフトでは、このライブラリを新しい脅威インテリジェンスで常に更新しています。脅威インテリジェンスは、独自の APT ハンティング & リサーチ チームが作成しているものですが、パートナーの協力や共有フィードを通じて内容が強化されています。

常に新しい脅威が生み出され、既存の脅威にも変更が加えられています。マイクロソフトでは、新しい未知の攻撃者の活動を特定するため、膨大な量の疑わしい動作や通常と異なる動作を監視しています。そして、疑わしい動作や通常と異なる動作が見つかると、アラートを発行し、セキュリティ オペレーション センター (SOC) のアナリストに問題の検証と対応を依頼します。SOC のアナリストは、同じマシンやその他の関連マするシンで発生している類似したイベントの情報に基づいて、実際のデータ侵害アクティビティの検証、リスクの判断、データ侵害範囲の特定、攻撃を封じ込めるアクティビティの定義を行います。その後、実際に攻撃を封じ込め、脅威を軽減することで、攻撃に対応します。

Windows Defender ATP

Microsoft

はじめに: ファイル ベースのバックドア型マルウェアのシナリオ

ソーシャル エンジニアリング攻撃として、メールを活用したファイル ベースのマルウェアを投下する攻撃は非常によく発生します。受信者が騙されてこのバックドア型マルウェアの実行をしてしまうと、攻撃者は被害に遭ったマシン上のすべてをコントロールできるようになります。

このシナリオでは、選択したテスト マシンにファイル ベースのバックドア型マルウェアが仕掛けられた場合のシミュレーションを行います。Windows Defender ATP が攻撃を検出し、直ちに調査と対処を行う方法を詳しく見ていきましょう。

攻撃者は、ソーシャル エンジニアリング攻撃として実装したドキュメントをスピアフィッシング メールに仕込むことによって攻撃を開始します。このドキュメントは、受信者が疑いを持たず、うっかり開いてしまうようなドキュメントを装っています。

しかし、実際には、このドキュメントには、マシン上に実行可能ファイルをひそかにドロップしてロードするマクロ コードが含まれています。このシミュレーションでは、無害な実行可能ファイルをドロップするドキュメントを使用しますが、実際に攻撃された場合、この実行可能ファイルはあたかも持続的なバックドア型マルウェアのようにふるまい、レジストリの Run キーに書き込みを行ったり、タスクスケジューラを活用したマルウェアの実行スケジュールを作成したりします。これらはいずれも自動開始拡張ポイント (ASEP) として知られています。

ASEP が作成された時点でシミュレーションは終了となります。ただし、実際の攻撃では、攻撃者は設置したバックドアを利用して、被害を受けたネットワーク内でさまざまなアクションを実行します。たとえば、他のマシンに横移動したり、特権を得た上で資格情報を収集したり、企業データをひそかに盗み出したりします。

このシミュレーションで使用するマシンの条件は、次のとおりです。

- Windows Defender ATP のオンボーディングが完了している
- Windows 10 Anniversary Update (バージョン 1607) 以降を実行している
- PowerShell が有効になっている
- Windows Defender ウイルス対策が有効になっている
- Microsoft Word がインストールされている

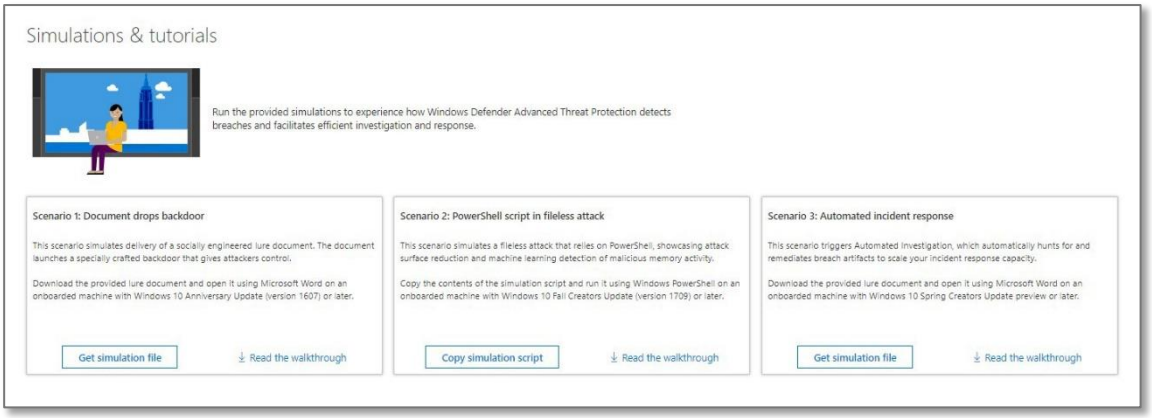
攻撃シミュレーション シナリオ 1: ファイル ベースのバックドア型マルウェア

オンボーディングの方法については、製品ガイドをお読みください。テスト マシンのオンボーディングを行うには、ローカルのオンボーディング スクリプトを実行することをお勧めします。

シミュレーションの実行

攻撃シミュレーションを実行する手順は、次のとおりです。

1. Windows Defender ATP ポータルにログインし、**[Help (?)] > [Simulations & tutorials]** を選択します。



2. **[Scenario 1: Document drops backdoor]** の下の **[Get simulation file]** をクリックして、ルアー ドキュメント **WinATP-Intro-Invoice.docm** をダウンロードします。

3. ルアー ドキュメントをテスト マシンにコピーします。

4. ユーザーの一般的な反応をシミュレーションするため、テスト マシン上にコピーされたルアー ドキュメントをダブルクリックします。Microsoft Word が起動し、パスワードの入力を求めるプロンプトが表示されます。パスワード **WDATP!diy#** を入力して、パスワードで保護されたドキュメントを開きます。

5. ドキュメントが保護ビューで開いた場合は、**[Enable Editing]** をクリックします。マクロが無効になっているというセキュリティ警告が表示された場合は、**[Enable Content]** をクリックします。適切なルアー コンテンツを使うと、多くのユーザーがこうしたセキュリティ セーフガードを回避して、うっかり悪意のある Office ドキュメントを開いてしまいます。

   🖌**注**: 組織全体で、インターネット経由で入手したドキュメントのマクロをブロックする設定になっている場合、**[Enable Content]** オプションを有効化するには、このドキュメントのブロックを解除する必要があります。ドキュメントのブロック

を解除するには、エクスプローラーでファイルの場所へ移動します。エクスプローラーでドキュメントを右クリックし、**[Properties]** を選択します。**[General]** タブで、**[Security]** の下の **[Unblock]** オプションをオンにします。

✎**注**: サード パーティのセキュリティ製品を利用している場合、シナリオをスムーズに実行できないことがあります。テストには、Windows Defender AV を有効にした Windows 10 の既定の設定のマシンを使用することをお勧めします。

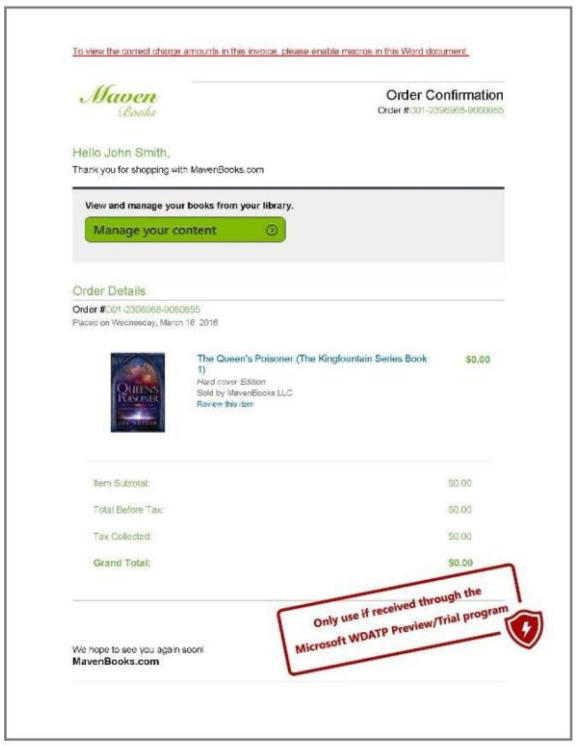
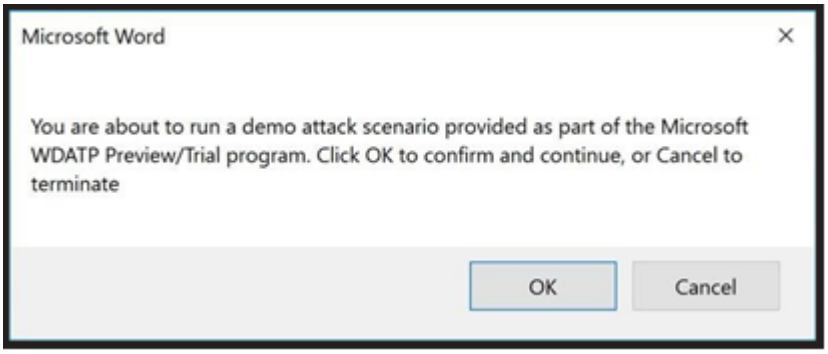


図 1: ルアー ドキュメント

6. メッセージ ボックスが表示されたら、[OK] をクリックして、攻撃シミュレーションを実行します。



7. 数秒後、ドキュメントの悪意のあるマクロによって PowerShell スクリプトが実行され、[Desktop] フォルダーに **WinATP-Intro-Backdoor.exe** という新しいファイルがドロップされます。これがバックドアになります。

8. 同じスクリプトにより、事前にスケジュールされた時刻にバックドアを実行する予定されたタスクが作成されます。この間接的なプロセス実行のメカニズムは、ドキュメントをトレース バックすることが難しいため、しばしばステルス攻撃に使用されます。

9. バックドアが実行されると、レジストリの Run キーの下に自動起動エントリが作成されます。バックドアは Windows と同時に自動的に起動するため、持続的な脅威となります。[コマンド プロンプト] ウィンドウが開きます。これはシミュレーションのバックドアが実行中であることを示します。

10. [コマンド プロンプト] ウィンドウを閉じて、**WinATP-Intro-Backdoor.exe** プロセスを終了します。

お疲れ様です。攻撃が完了しました。

これで攻撃シミュレーションは終わりです。実際の攻撃者は、多くの場合、情報のスキャンを続け、収集した偵察情報をコマンド アンド コントロール (C&C) サーバーに送信し、この情報を利用して他の魅力的なターゲットに横移動します。

次に、シミュレーションの攻撃を知らせる Windows Defender ATP アラートについて見ていきましょう。

🖉**注**: アラートは、バックドア型マルウェアのシミュレーションの実行後 15 ～ 30 分で Windows Defender ATP ポータルに表示されます。

ポータル内の攻撃の調査

ここからは、防御者の役割に切り替えて、Windows Defender ATP ポータルから SOC の視点で攻撃を分析していきましょう。

1. 任意のマシンから https://securitycenter.windows.com にアクセスし、Windows Defender ATP ポータルを開きます。

2. Windows Defender ATP の資格情報を使ってログインします。サインアップ時のメールでは、既定のグローバル管理者の資格情報が提供されます。

3. シミュレーションの攻撃から 15 ～ 30 分経つと、ダッシュボードに複数の新しいアラートが表示されます。

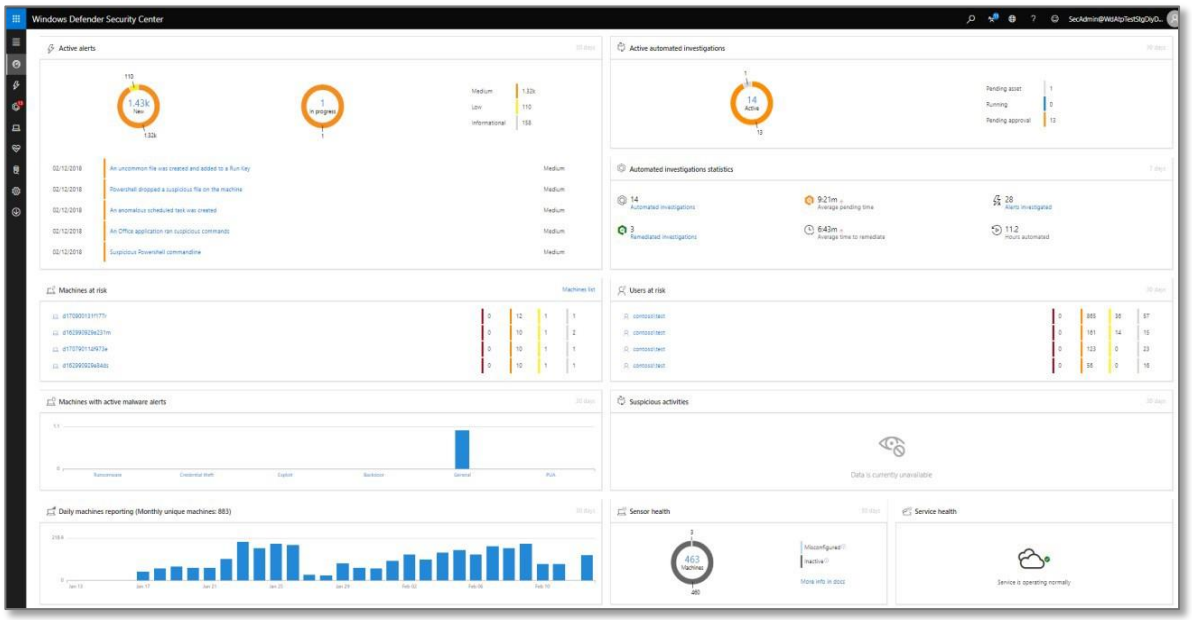


図 2: ダッシュボードに表示されるアラート

4. **[Machines at risk]** ウィジェットで、テスト マシンをクリックしてマシンとすべての関連アラートの詳細を表示します。

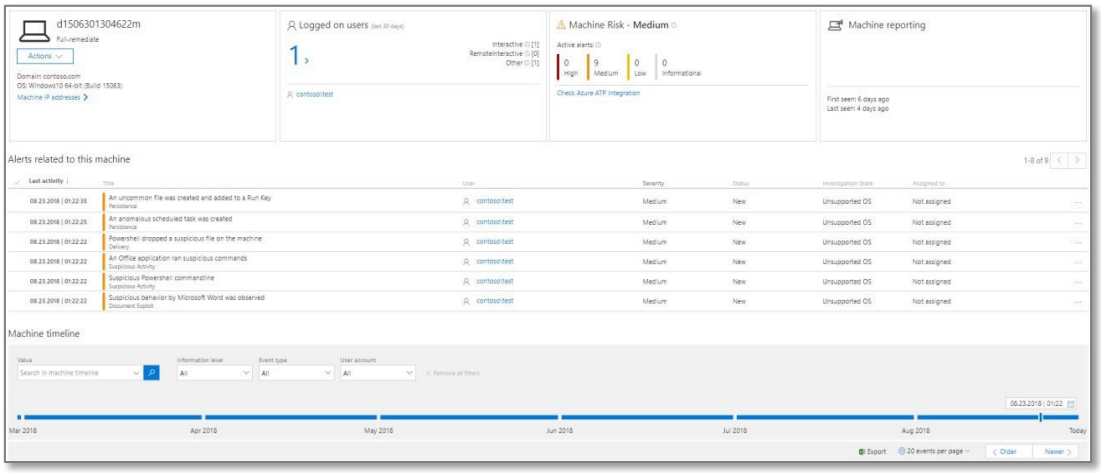


図 3: 被害を受けたマシンとアラート

5. アラートの調査中、アラートのステータスを **[New]** から **[In progress]** (処理中) に変更して、Security Operations Center ワークフローをサポートできます。このためには、アラートの左の円をクリックします。サイド パネルでアラートのステータスを設定し、オプションとしてコメントを入力します。

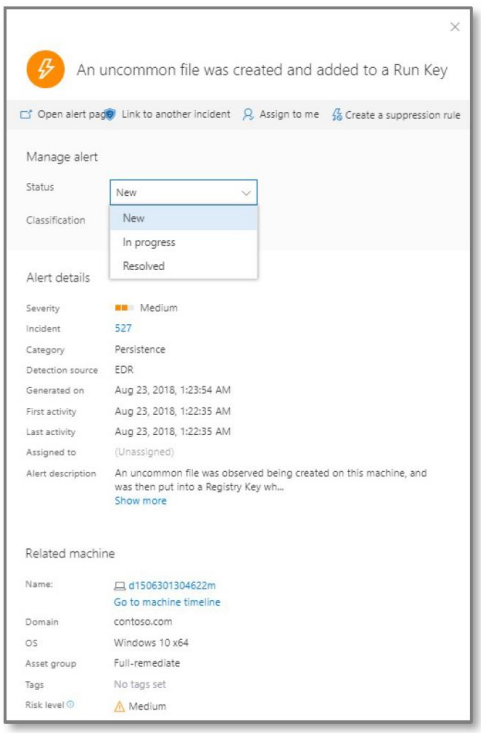


図 4: アラートのサイド パネル

攻撃シミュレーション シナリオ 1: ファイル ベースのバックドア型マルウェア

生成されたアラートの確認

シミュレーションの攻撃で生成されたいくつかのアラートを見ていきましょう。

📝 **注**: シミュレーションの攻撃で生成されたアラートのうち、いくつかについて検証します。テスト マシンで実行中の Windows と Windows Defender ウイルス対策の製品更新プログラムのバージョンによって、表示されるアラートの数や順序が変わる可能性があります。

アラート: PowerShell dropped a suspicious file on the machine

ユーザーが開いた Word ドキュメント内のマクロが PowerShell を使ってディスクに実行可能ファイルを書き込みました。Windows Defender ATP は、Office アプリケーションによって作成された実行可能ファイルを監視し (PowerShell を使ってドロップされた実行可能ファイルも対象)、組織やユーザーとの関連性が希薄なファイルを探します。

マシンの詳細ページまたは任意のアラート キューで、アラート名をクリックして詳細を表示します。

- 詳しい説明と推奨アクション
- アラートに含まれるファイルとプロセスに関連するプロセス ツリー (コマンド ライン、実行時刻のほか、選択したプロセスの作業ウィンドウに表示されるその他の詳細を含む)
- インシデント グラフ (このファイルが見つかった組織内の他のマシンを含む)
- このマシン上でアラートをトリガーしたイベントの詳細を提供するアーティファクト タイムライン (ドロップされたファイルの検出時刻、ファイル名、パス、SHA1 ハッシュを含む)

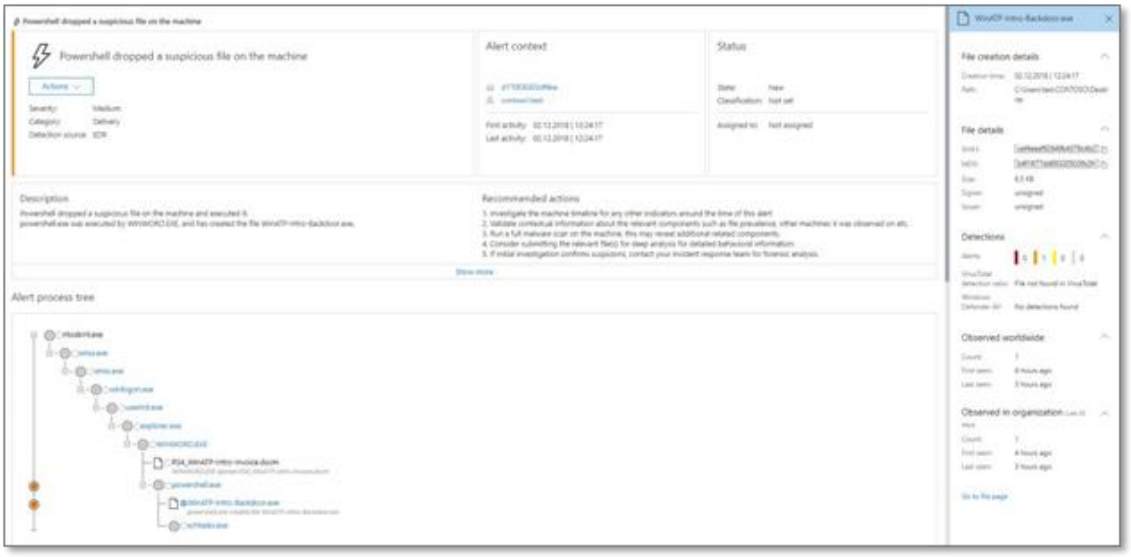


図 5: アラートの詳細ページ

アラート プロセス ツリー内でファイルを選択 (ファイル名の横の円を選択) して、右側に [File Details] パネルを表示します。このパネルでは、ファイルのハッシュ、サイズ、ウイルスの総数といった詳細情報を確認できます。

ファイルの詳細情報の確認

[File Details] ウィンドウの **[Go to file page]** リンクをクリックして、**[File View]** を開きます。ここには、次のようなファイルの追加情報が表示されます。

- ファイル ハッシュ
- 署名者名 (有効な署名がある場合)
- 詳細分析用にファイルを提出するオプション (制御された環境内でファイルを実行し、その性質を調査)
- このファイルで発行されたアラート
- このファイルが見つかった組織内、または世界各国のマシンの数
- 組織内の同じファイルで使用されている名前
- このファイルが見つかった組織内のマシン (ファイルの発生元と組織内のフットプリントがわかる)

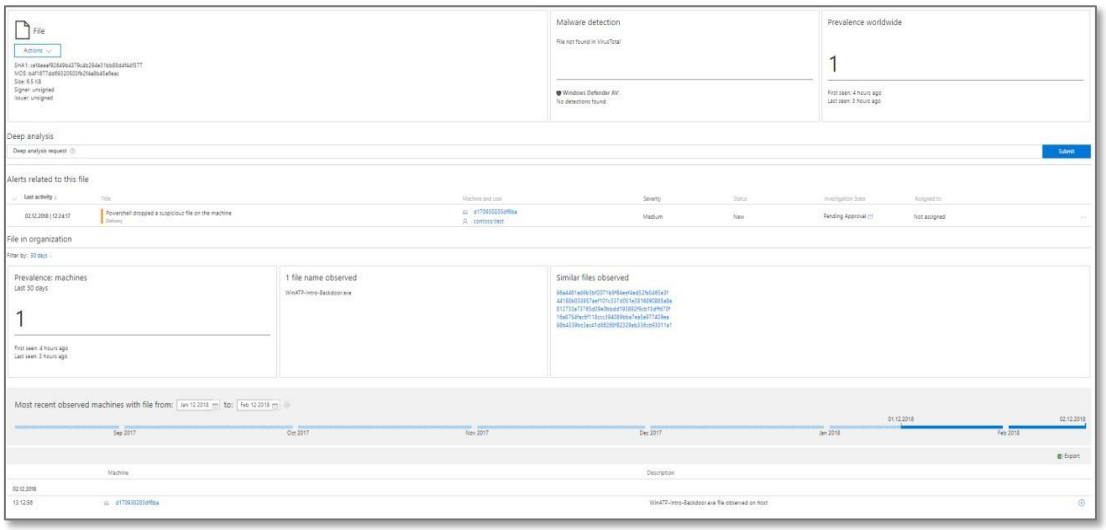


図 6: ファイルの詳細ページ

アラート: Suspicious PowerShell commandline

マクロで使用されている PowerShell 呼び出しパターンがステルス攻撃と検出回避の意図を示しています。ステルス状態を維持しようとする試みによって、アラートがトリガーされました。

アラートの詳細ページに、実行されたフル コマンドライン引数や base64 でエンコーディングされたスクリプトを含む、疑わしい PowerShell 実行の詳細情報が表示されます。

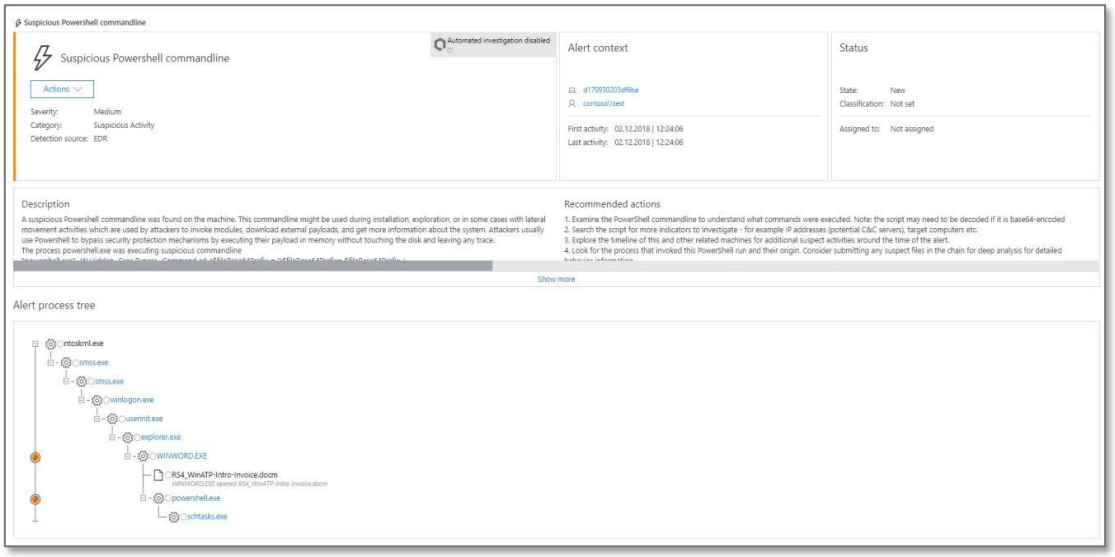


図 7: 疑わしい PowerShell コマンドライン

アラート: An uncommon file was created and added to a Run Key

攻撃者が攻撃したマシンに長期間にわたって留まるためによく使用するテクニックとして、レジストリを操作して、リブート後の自動起動を設定する方法があります。これには、ASEP (自動開始拡張ポイント) レジストリ キーが使用されます。Windows Defender ATP は、通常と異なる自動起動レジストリを監視します。たとえば、ここでは、マシン上にシミュレーションのバックドアがインストールされています。

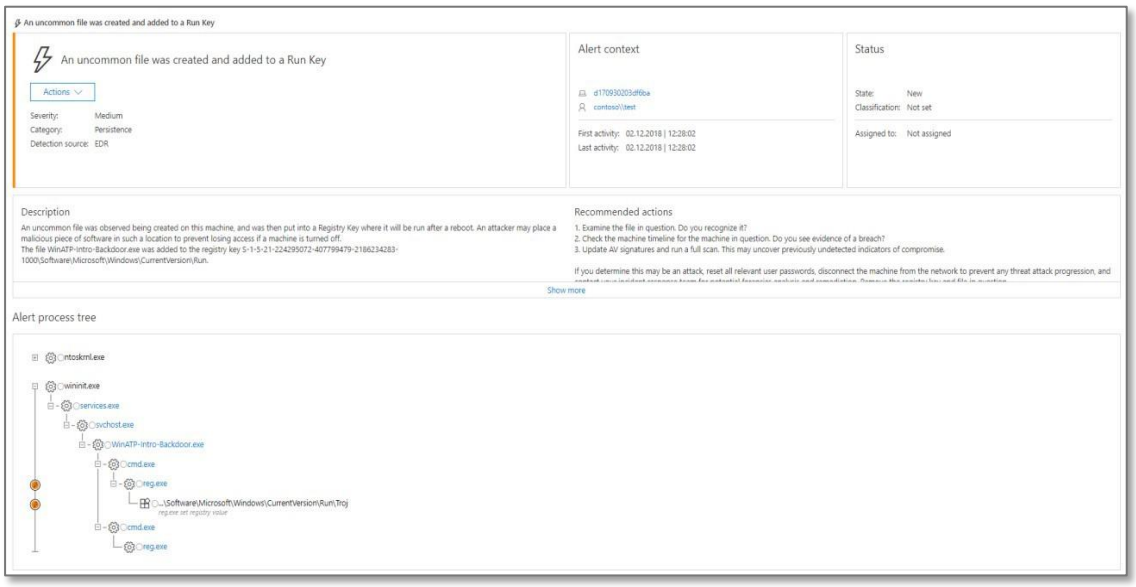


図 8: アラートの詳細ページ - ファイル、レジストリ Run キー

アラート: An anomalous scheduled task was created

予定されたタスクは、攻撃者が攻撃したマシンに長期間留まるテクニックとしてよく使用します。しかし、他の目的、たとえばそのプロセスに潜んで、攻撃の次のフェーズを遅らせる目的で使用される場合もあります。目的にかかわらず、Windows Defender ATP は通常と異なる予定されたタスク (組織内の他の場所で見かけない特殊なものを含む) を検出し、アラートを発行します。

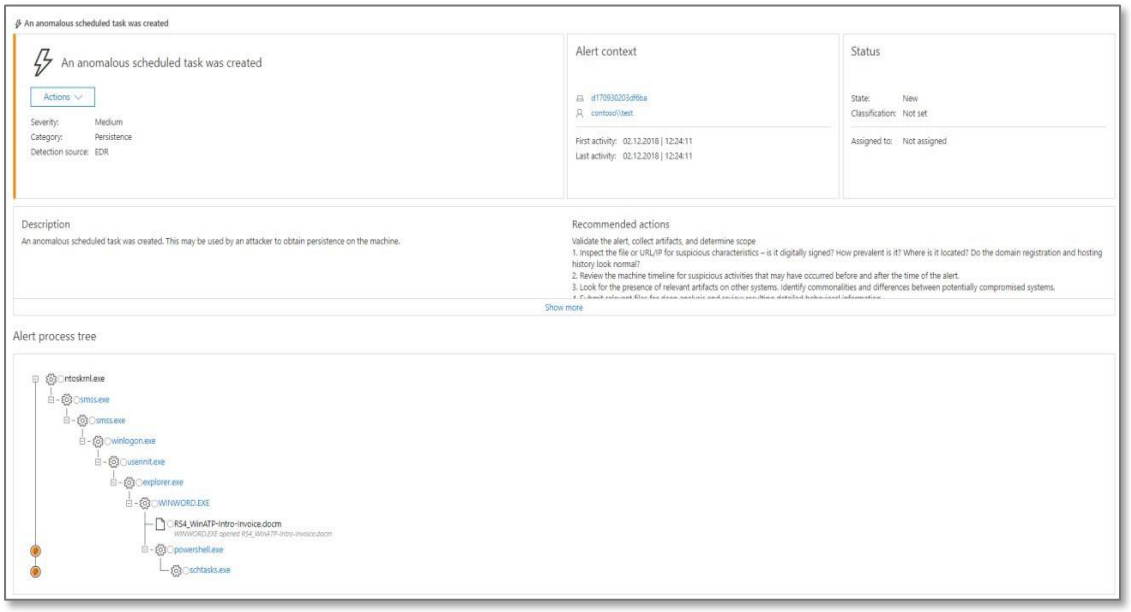


図 9: 通常と異なる予定されたタスクの作成に関するアラート

マシンのタイムラインの確認

アラート ページでマシン名をクリックすると、マシンの詳細ページが開きます。ここでは、アラートそのものとマシン上の関連イベントを簡単に調査できます。マシン タイムラインをスクロールして、このマシンで発生したすべてのイベントと動作を時系列で確認できます。その合間に、複数のアラートも発生しています。情報レベルとして、[Verbose]、[Behaviors]、[Detections] のいずれかを選択できます。

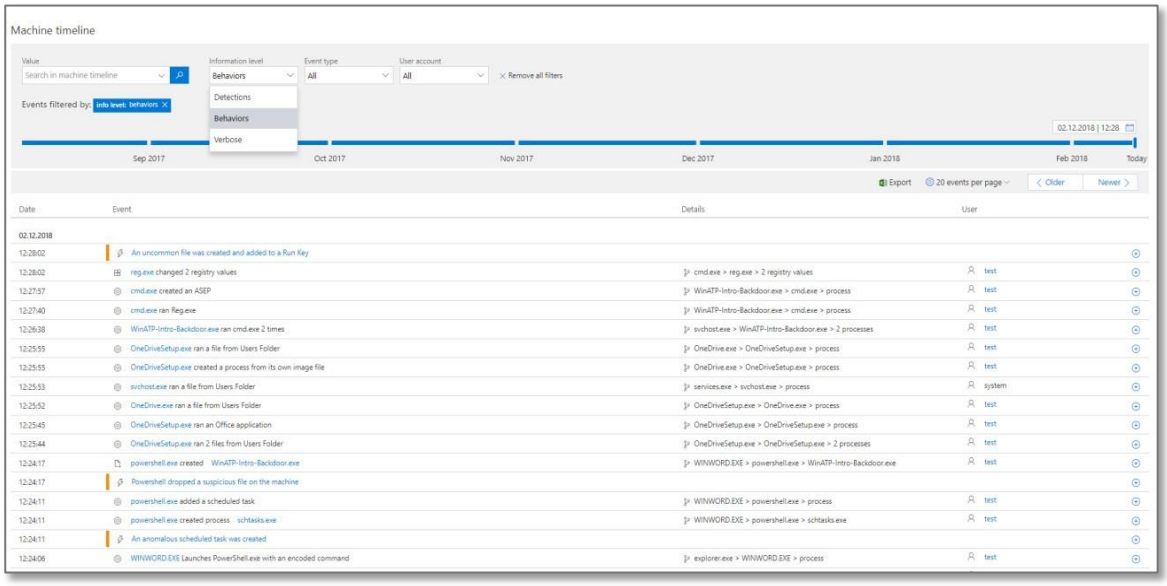


図 10: マシン タイムラインと動作

興味のある動作があったら、展開してみましょう。プロセス ツリー、ファイル作成のリレーションシップなど、有用な詳細情報が表示されます。たとえば、**powershell.exe created WinATP-Intro-Backdoor.exe** をクリックすると、この動作の完全なプロセス ツリーが表示されます。

図 11: 選択した PowerShell ファイル作成の動作のプロセス ツリー

まとめ

ここでは、一般的な攻撃をシミュレーションし、Windows Defender ATP が攻撃を検出するしくみを紹介しました。アラートと、各アラートから確認できるコンテキスト ファイル情報、マシン情報、イベント情報についても確認しました。

シミュレーションを楽しんでいただけましたら幸いです。他の機能もぜひ利用してみてください。詳細については、製品ガイド (docs.microsoft.com) をご覧ください。

また、Windows Defender ATP ポータルのフィードバック アイコンから、このシミュレーションや製品に関するご意見、ご感想をお寄せください。お寄せいただいたご意見やアイデアは、今後のシミュレーションやチュートリアルのために利用させていただきます。ご協力よろしくお願いいたします。