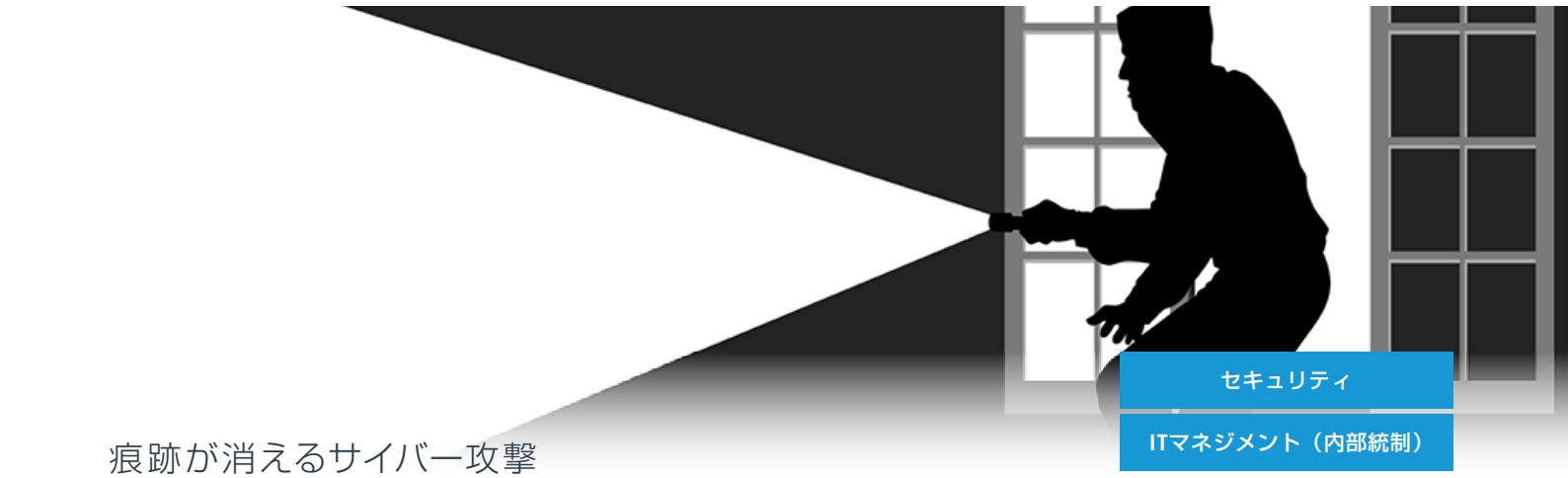

セキュリティ

ITマネジメント（内部統制）

痕跡が消えるサイバー攻撃

Windows標準機能を悪用する「ファイルレスマルウェア」

企業へのサイバー攻撃の約9割が、「メール」を経由したものといわれています。それだけにメールを巡るサイバー攻撃とセキュリティ対策の攻防は激しく、サイバー攻撃者は次から次へと新たな手法を生み出してきました。2017年の夏ごろから確認され始めた「ファイルレスマルウェア」もその1つで、マルウェアをディスク上に作成せず、Windowsに標準で搭載された機能を悪用して感染させるものです。今回は、このファイルレスマルウェアのしくみと対策についてご紹介します。

「ファイルレスマルウェア」に感染する流れ

2017年に、「.rtf」や「.lnk」といった見慣れない形式のファイルが添付されたスパムメールが急増。多くの人がこれらのファイルを開いてしまい、マルウェアに感染する被害が相次ぎました。「.rtf」とはリッチテキストファイル、「.lnk」はショートカットファイルで、いずれもマイクロソフトの「Office」が使用するファイルです。

この攻撃は、セキュリティ対策ソフトなどによる検知を避けるため、複数の手法が組み合わされたものでした。感染の流れは、まずメールの受信者が添付ファイルを開くと、ファイルに書き込まれていたスクリプト（命令文）が実行され、PowerShellを呼び出します。PowerShellとは、Windows 7以降に標準で搭載されている機能で、プロセスの一種です。

プロセスとは、メモリ上で実行されるプログラムのことで、さまざまな動作が可能です。ファイルレスマルウェアでは、呼び出したPowerShellにドロッパーと呼ばれるマルウェアを生成します。ドロッパーはサイバー攻撃者が用意したC&C（コミュニケーション&コントロール）サーバーと通信を行い、新たなマルウェアをダウンロードし、実行します。ドロッパーによりダウンロードされるマルウェアにはさまざまなものがあり、ランサムウェアやバンキングマルウェアなどが確認されています。

なぜ、セキュリティ対策ソフトが検知できないのか？

一連のファイルレスマルウェアによる攻撃を、セキュリティ対策ソフトはなぜ検知できないのでしょうか。まずは感染のきっかけとなるメールです。攻撃に使われるメールは一般的なメールを装っているので、スパムフィルターで検知できる可能性は高くありません。また、添付ファイルに使用された「.rtf」や「.lnk」などのファイルは、当時セキュリティ対策ソフトは検知の対象にしていませんでした。

ファイル形式が検査の対象になっていないので、セキュリティ対策ソフトはファイルの動作を確認しません。結果、ファイルに仕込まれたスクリプトがブロックされないことになります。また、PowerShellもWindows上で動作する正規のサービスと認識されているので、その上で実行されているプログラムもチェックしていません。このようにサイバー攻撃者は、セキュリティ対策ソフトが検査を行う対象を見極めることで、その穴を突くという新たな攻撃手法を編み出したのです。

さらにこの攻撃では、PowerShellとドロッパー、ダウンロードするマルウェアがメモリ上で動作するようにしていました。つまり、従来のマルウェアのようにPCのディスク上にマルウェアが作成されません。これがファイルレスと呼ばれる理由です。マルウェアの痕跡がディスク上に残らず、メモリの内容はPCを再起動すると消えてしまいます。このことが事後の調査（フォレンジック）を困難にしました。

このように、ファイルレスマルウェアはセキュリティ対策の“抜け穴”を狙った攻撃手法です。ファイルレスマルウェアの存在が明らかになったのち、多くのセキュリティベンダーが検査対象のファイル形式を拡大したことで、感染の被害は減少しています。しかし専門家の中には、ファイルレスマルウェアの手法と脆弱性を悪用する手法を組み合わせることで、「完全なファイルレスマルウェア」が実現できると、警鐘を鳴らす人もいます。

効果的なのは、仮想環境やクラウドなどを活用した「多層・多段防御」

ファイルレスマルウェアによって、PowerShellのようなWindows上で動作する正規のサービスも攻撃に使えることが明らかになりました。それゆえ、これまでマルウェア感染に使用されていなかったファイル形式や正規のサービスが今後、悪用される可能性は十分にあります。PCにインストールするセキュリティ対策ソフトは、検査の対象ファイルやサービスを拡大した製品を利用すべきですし、マルウェアを検知するためには、さらなる多段防御、多層防御が必要です。

企業のPCを狙ったマルウェア攻撃はますます巧妙化しています。対策を複数実施することが社内の機密情報を守るためのポイントになっています。

関連サービス

WideAngle マネージドセキュリティサービス	ファイアウォールやIPS/IDS、アンチウイルスなど、ご要望の高いネットワークセキュリティやコンテンツセキュリティを一括してアウトソーシングできるパックメニューです。 セキュリティ運用基盤（SIEM）とリスク分析官による相関分析で、ファイアウォールなど機能単体での運用では気がつかない未知の脅威をあぶりだします。
Menlo Security	インターネット分離・無害化の技術で、従来の検知技術による多層防御では防ぎきれなかった新種のマルウェア攻撃やゼロデイ攻撃も防ぎ、安全で自由なWeb閲覧を実現します。