Excel Web クエリファイル（.iqy ファイル）に注意

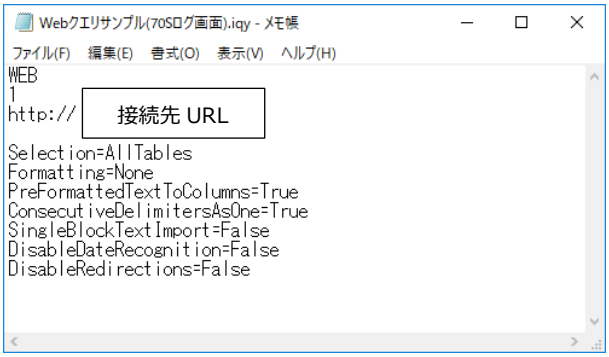
脅威の概要

Excel の Web クエリファイル形式である拡張子 .iqy のファイルがマルウェア感染に悪用されているケースが報告されています。

Excel の Web クエリ機能は本来、Web ページ上の表を Excel 内に取り込む際に利用される機能です。
今回のケースでは、接続先情報等を保存したファイル(.iqy ファイル) に、マルウェアに感染する接続先 URL を記述したものを実行させ、感染させようとするものです。
メールに添付された.iqy ファイルを開くと、マルウェアがダウンロードされ実行される恐れがあります。

.iqy ファイルのアイコン

.iqy ファイルの内容

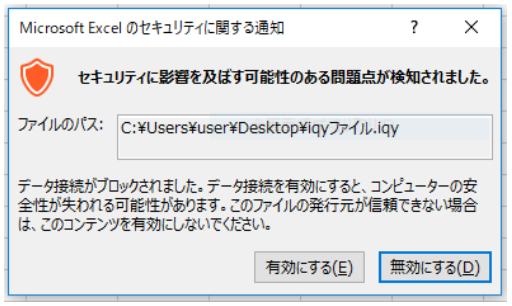


実行した場合の影響

.iqy ファイルを開くと、Excel が実行され、セキュリティ警告が表示されます。

「有効にする」を押すとマルウェアがダウンロードして実行されます。

ファイルを開いた場合の警告画面



この脅威への対策

【NetStable の対応状況】

拡張子が.iqy のファイルが添付されたメールを検知するシグネチャをリリースしております。

- 3000131 Pop3 .iqy
- 3000132 Pop3 .iqy 2

このシグネチャが検知された場合は、受信先 IP アドレスの端末で.iqy ファイルが添付されたメールを受信しておりますので、該当メールは開かず、添付ファイルは絶対に実行しないでください。

また、スパムメール等で大規模に拡散された .iqy ファイルに記載されていた、
不正な接続先を遮断するシグネチャもリリースしております。

- 2001005 Malware iqy file download 1
- 2001006 Malware iqy file download 2

このシグネチャが検知された場合は、不正な.iqy ファイルを実行した恐れがあります。
送信元 IP アドレスの端末のウイルスチェックを行ってください。

【その他の対策・回避策】

今回の.iqy ファイルの場合は、万が一メールの添付ファイルを開いた場合でも、
Excel のセキュリティ機能にて実行前に一旦警告画面が表示されます。
この場合「無効にする」を押せば影響はありません。
また、メールに添付された不審なファイルは開かないよう注意してください。

まとめ

- Excel Web クエリファイル（.iqy ファイル)からの感染事例がある
- 実行した場合も、「有効にする」を押さなければ悪影響はない
- 不審なファイルが添付されたメールは開かない・添付ファイルも開かない