— AUS（アルテミス・ユーザ・サポート）便り 2016/03/28号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●件名「Document 2」、差出人は自分自身、本文なしのランサムウェア添付メールが拡散

http://www3.nhk.or.jp/news/html/20160324/k10010454921000.html
http://canon-its.jp/eset/malware_info/news/160323/

このニュースをザックリ言うと・・・

- 3月17日（日本時間）以降、ランサムウェア「Locky」が添付されたとみられるメールが国内で大量に確認されており、24日にはNHKニュースでも報じられています。

- メールの特徴として、①差出人が宛先と同じアドレスに偽装されており、②「Document 2」といった件名で、③本文はなく、④ファイル「Document2.zip」が添付されている、ということが挙げられます。

- 各種情報によれば、添付されたzipファイルにはjavascriptファイルが入っており、誤ってクリックするとLockyがダウンロードされ、感染する可能性がある模様です。

AUS便りからの所感等

- Lockyは2月頃から拡散が見られており、昨年末に確認された「vvvウイルス」こと「TeslaCrypt」と同様、暗号化したファイルを「.locky」という拡張子がついたファイル名にリネームする特徴があります。

- 差出人が自分自身になっていることから、相手の興味を引いてランサムウェアに感染させようとする工夫がなされているようですが、くれぐれもこういった拡散者の意図にはまることなく、アンチウイルス・UTMを導入しつつ、メールを慎重に扱うことを心がけてください。

こちらの動画は要チェック!!

NHK NEWS WEB

身代金要求型ウイルス急増 今月国内で20万件以上に

3月24日 17時47分

電子メールに添付されたファイルを開くとパソコンに保存されている画像などすべてのデータが使えなくなり、元に戻す見返りとして金銭を要求する「身代金要求型」のコンピューターウイルスが、今月、国内だけで20万件以上確認され、専門家は悪質なサイバー犯罪として注意を呼びかけています。

このコンピューターウイルスは、「Document2」などというタイトルの電子メールに添付されたファイルを開くと感染し、画像や文書などパソコン内のすべてのデータが利用できなくなります。さらに、画面には、元に戻す見返りとして金銭を求めるメッセージが表示されることから、悪質なサイバー犯罪に使われる身代金要求型のウイルス、いわゆる「ランサムウエア」の一種とみられています。

情報セキュリティーサービスを提供しているキヤノンITソリューションズによりますと、このウイルスが仕組まれた電子メールは、今月、国内だけで20万件以上確認されたということです。

また、独立行政法人の情報処理推進機構には、このウイルスによる被害も今月50件以上報告されていて、中には「クラウド」と呼ばれるサービスでネット上に保管されているデータも利用できなくなった例もあるということです。

キヤノンITソリューションズによりますと、「身代金要求型」のウイルスは3年ほど前から世界中で大きな被害が出ていますが、国内でこれほど大量に送りつけられているのは初めてだということで、ウイルスの分析を担当している長谷川智久さんは「身代金要求型のウイルスは今後も国内で広がっていくとみられるので、不審な添付ファイルは決して開かないよう十分に注意してほしい」と話しています。

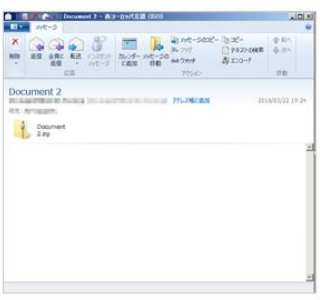
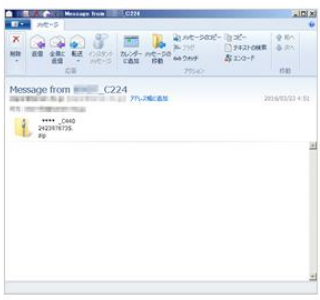
Canon キヤノンITソリューションズ株式会社

2016/03/23

不正送金マルウェアとランサムウェア感染を狙ったメール攻撃が集中して発生

2016年3月22日から3月23日にかけて、メールを利用した「ばらまき型」攻撃による広範囲でのキャンペーンと見られる兆候がいくつか確認されました。今回のキャンペーンでは、主に「Locky」ランサムウェア感染を狙ったものと、不正送金マルウェア「Rovnix」感染を狙ったものが確認されています。

ランサムウェア感染を狙ったメール文の例

件名が「Document 2」 本文はなし 添付ファイルは、「Document 2.zip」	件名が「Message from ****_OOOO」 本文はなし 添付ファイルは、「****_OOOO_(10桁数字).zip」
	

●「404 Not Found」エラーメッセージにマルウェアへの命令を隠す攻撃手法を確認

http://www.itmedia.co.jp/enterprise/articles/1603/18/news083.html

このニュースをザックリ言うと・・・

- 3月17日（日本時間）、警察庁より、指定したURLにファイルが存在しないことを示す「404 Not Found」エラーメッセージに偽装し、マルウェアへ指令を送る手口を確認したとして、特徴・対策情報が発表され、注意が呼びかけられています。

- 一例として、「HTTP/1.1 404 Not Found」を含むヘッダの後に、エラーメッセージとしてURLが示されており、これがマルウェアに対し次の接続先を示しているというものが挙げられています。

- 警察庁では、ファイアウォールやプロキシサーバで取得している外部への通信ログを検証する際、HTTPステータスコードが404などあっても接続の失敗と決め付けず、慎重に調べる必要があるとしており、また対策として、このようなエラーメッセージをプロキシ独自のメッセージに差し替えることにより、サーバからの指令を遮断することを挙げています。

AUS便りからの所感等

- 今後、リダイレクト（301・302）やサーバエラー（50x）等に偽装して指令を送信するケースも現れることは当然予想されるでしょう。

- 念の為、利用しているアンチウイルス・UTMにおいて、万が一このようなエラーメッセージについてチェックを行わずスルーするような仕様でないか、ベンダーに問合せることも検討事項となるでしょう。

ITmedia エンタープライズ

2016年03月18日 11時16分 更新

404応答にマルウェアへの命令を隠す攻撃手法を確認、ネットワーク監視で注意を

サイバー攻撃の新たな手口が確認され、警察庁が対策などをアドバイスしている。

[ITmedia]

警察庁は3月17日、サイバー攻撃者がHTTPステータスコードを偽装してマルウェアに指令する手口を確認したとして、特徴や対策情報を公開した。ネットワーク監視などの際に注意するよう呼び掛けている。

それによると、見つかった手口ではマルウェアが感染先の端末から攻撃者のC2（コマンド＆コントロール）サーバへ接続した際に、サーバがHTTPステータスコード「404」を返す中に、別のC2サーバへ接続する命令を埋め込む。「404」は端末がリクエストしたファイルなどが接続先サーバに見つからない場合にサーバが返すコードであるため、ネットワーク監視時に接続が失敗したと誤認して、攻撃者の命令を見逃してしまう可能性がある。

●マイナンバー紛失相次ぐ・・・横浜市・鹿児島県など

http://www.asahi.com/articles/ASJ3962G4J39UTIL02Z.html

このニュースをザックリ言うと・・・

- 本年1月より運用開始されたマイナンバーについて、企業等で収集した通知カードやマイナンバーを記載した書類の紛失が相次いでいるとのことです。

- 1月27日（日本時間）、横浜市教育委員会は、市立小学校の職員が教職員38人とその家族16人、計54人分のマイナンバーが書かれた書類を26日に紛失し、神奈川県警などに遺失物の届け出をしたことを発表しました。

- また、鹿児島県では、2月19日までの時点でマイナンバーカードの紛失届が418件あったとされています。

- この他、年末調整のために通知カードのコピーではなく原本を要請されて書留で送付した上に、届いた先の会社で紛失されたといったケースも挙げられています。

AUS便りからの所感等

- マイナンバーについては、電子的な管理はもちろん、前述したような物理的管理についても、万が一にも紛失しないような管理体制が必要となります。

- 当社マイナンバー制度対策特設サイトが「電子的」「物理的」のいずれについても厳重かつ確実な管理を行うための環境構築の一助となれば幸いです。
（https://www.artemis-jp.com/mynumber/index.html）

朝日新聞 DIGITAL