2016年3月28日

ご担当者各位

株式会社コムイン

【注意喚起】メール添付ファイルからのウイルスの感染が拡大しています。

●ウイルスの感染を狙ったメールが多発しています

ここ最近、メールを利用したばらまき型攻撃と見られる兆候がいくつか確認されており感染被害が拡大しています。この中では主に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感染を狙ったものが確認されています。

●ランサムウェアとは？

ランサムウェアはパソコン内に侵入してファイルやシステムの一部もしくはすべてを使用不能にし、その復旧と引き換えに金銭を要求する不正プログラムのことです。常に新種・亜種が存在しており、企業でも感染報告が増加しています。

●不正送金マルウェアとは？

日本のオンラインバンキングなどをターゲットにしたもので、感染したまま攻撃対象の銀行にアクセスすると、ブラウザー上に改ざんした銀行のウェブサイトを表示。アカウント情報を入力してしまうと不正送金が行われます。

●今回確認されているメールの一例

件名	本文	添付ファイル名	特徴
Document 2	なし	Document 2.zip	差出人を偽装し自社のアドレスから送られてきたかのように見せる
Voicemail from (10桁の数字)	ボイスメール情報を装った内容	msg_(36桁のハイフン含む英数字)	
文字化けによりコード表記	「いつもお世話になります。」「宜しくお願い致します。」	○○○-DOC.zip → 展開すると「レポート 03.2016.DOC.exe」のマルウェア本体が含まれる	添付ファイルをワード文書に偽装している。
なし	注文完了のメッセージを装った内容	(6桁の数字).zip	

●感染しないための対策

1.差出人のはっきりしないメールに添付されたzipファイルやexeファイルはけして開かないようにし、速やかに削除してください。
2.ウイルス対策ソフトのウイルス定義データベースが最新のものかどうか確認し、定期的にスキャンを行ってください。
3.Windows Updateを行う。(※こちらは現在Windows10への自動アップグレードを防ぐため弊社からは無効に設定するようお願いしております。行うことを希望される場合は別途配布いたします手順書をご参考の上作業を行っていただくこととなります。)

●もしも感染してしまった場合

1.速やかにLANケーブルを抜いて社内の他のPCに感染が広がらないよう隔離してください。
2.ウイルス対策ソフトでチェックを行ってください。(対策ソフトでウイルスを駆除しきれない時、システムの復元のためOSの再インストールが必要になる場合があります)
3. すでに暗号化されてしまったファイルを元に戻すには攻撃者が持つ秘密鍵が必要なため、一度暗号化されてしまうと元に戻すことができません。この場合バックアップファイルが存在すればそこから復元することが可能です。

今後も亜種によるメール攻撃が継続されると思われますので、メールの取り扱いにご注意ください。また、万が一ランサムウェアの感染に備え、重要なデータは定期的にバックアップを取るなどの対策を講じてください。

●参考URL

【ESETセキュリティニュース】http://canon-its.jp/eset/malware_info/news/160323/
【トレンドマイクロQ&A】http://esupport.trendmicro.com/solution/ja-JP/1113758.aspx
【シマンテック/感染後の対処法】https://www.symantec.com/ja/jp/security_response/infected_systems.jsp

なにかございましたら弊社担当者までご連絡ください。
株式会社コムイン Email : system-b@com-in.jp TEL :06-6354-2135 FAX:06-6242-2135