— AUS（アルテミス・ユーザ・サポート）便り 2017/05/22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。

●【再編集】Windowsの脆弱性を突くランサムウェア「WannaCrypt」が世界中で猛威…XP等にも特例でパッチリリース

http://www3.nhk.or.jp/news/html/20170513/k10010980311000.html
http://pc.watch.impress.co.jp/docs/news/1059552.html
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html
https://www.jpcert.or.jp/at/2017/at170020.html
https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/
http://blog.trendmicro.co.jp/archives/14884
https://www.symantec.com/connect/ja/blogs/wannacry-1

このニュースをザックリ言うと・・・

- 5月12日（米国時間）以降、ランサムウェア「ワナクリプト/ワナクライ(WannaCrypt, WannaCry, Wcry)」への感染被害が日本を含む全世界で報告されており、セキュリティベンダーやIPA・JPCERT/CCといった専門機関等から警告が相次いでいます。

- WannaCryptは3月15日にパッチがリリースされたWindowsの古いファイル共有機能(SMBv1)の脆弱性「MS17-010」を突いて感染し、PC上のファイルの暗号化と身代金の要求を行い、また「DoublePulsar」と呼ばれるバックドアを設置します。MS17-010の発表時点でサポートが終了していたWindows XP・Windows 8・Windows Server 2003を使用しているPCにおいて主に被害が出ているとされており、MicrosoftではWannaCryptによる顧客への影響の大きさを鑑み、XPや8等に対しても、特例としてセキュリティパッチを公開しています。

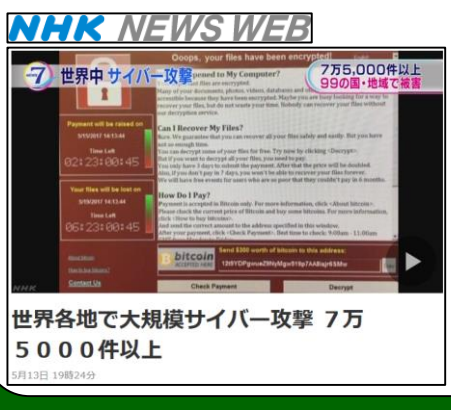
AUS便りからの所感等

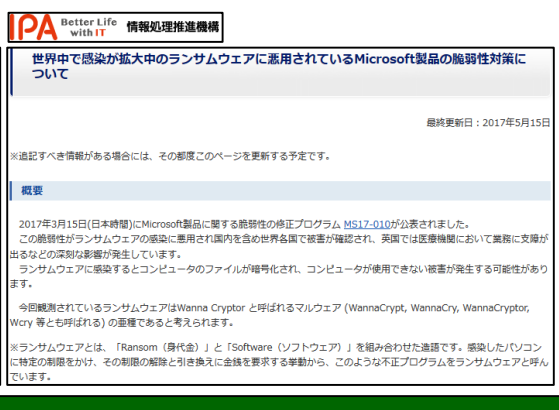
- NSAから流出したハッキングツール（AUS便り 2017/4/24号 参照）にMS17-010の脆弱性を悪用する攻撃コードが含まれており、WannaCryptはその攻撃コードを流用したものとみられています。

- 感染経路の大多数は「あるPCに感染し、そこから社内LAN上で他のPCに拡散する」ケースと考えられます。一方で、メールの添付ファイル等からの感染の可能性も少なからずあり、またランサムウェアへの警告文をかたり添付ファイルからマルウェアに感染させようとする動きも確認されています。

- 現在サポートが続いているWindows 10, 8.1, 7およびサポート終了までにパッチが公開されていたVistaについては、Windows Updateによる更新を確実に実施しているか、必ず確認を行ってください（当然ながら、アンチウイルスのパターンファイルが最新のバージョンかの確認も欠かせません）。一方、XPや8等に対して特例で公開されたパッチは、各OSに対応する実行ファイルを「Microsoft Update Catalog」からダウンロードし、手動で適用する必要があることに注意してください。

- UTMを用い、適宜LANの分割を行う等により、感染の拡大を食い止められるネットワーク構成とすることが重要です。特に、XP等サポートが終了したOSを使用し続けているPCについては、他のPCから隔離を行い、一刻も早いアップグレードの実施を検討すべきです。





●「WannaCrypt」の裏で43万件以上のスパムメール拡散

http://internet.watch.impress.co.jp/docs/news/1060577.html

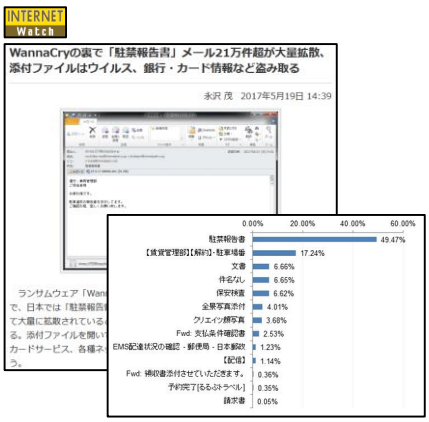
このニュースをザックリ言うと・・・

- 5月19日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、国内のオンラインバンキングやクレジットカード利用者を狙うマルウェア「URSNIF(gozi)」が添付されたスパムメールの大量拡散が確認されたとして警告が出されています。

- 同社によれば、5月14日から18日15時までの間に確認されたマルウェアスパムは43万件以上で、「駐禁報告書」という件名のものが約半数を占めており、他にも「【賃貸管理部】【解約】・駐車場番」「文書」「保安調査」「全景写真添付」「クリエイツ顔写真」「Fwd: 支払条件確認書」「EMS配達状況の確認・郵便局・日本郵政」等が確認されています。

- 特に多くの拡散が確認されたのは16日と17日で、1時間毎でみると午前5時から6時が最も多かったとされています。

AUS便りからの所感等



- 拡散が最も活発だった16日・17日は火曜・水曜にあたり、週明けにWannaCryptが大きく騒ぎとなった状況を狙ったのかはわかりません。

- URSNIFは、特に2016年から頻繁に確認されるようになったマルウェアであり、メールの件名だけでなく、アンチウイルスのチェックを回避しようとする亜種も日々新しいものが作られているとみられます。

- 日本サイバー犯罪対策センター（JC3）のWebサイト（https://www.jc3.or.jp/topics/virusmail.html）では確認されたスパムメールの件名が随時更新されており、こういった情報や、TwitterといったSNSでの言及等、ウイルスメールの拡散情報を常に意識しておくこと、そしてもちろんアンチウイルスのパターンファイルを最新に保つこと、UTMを設置すること等、マルウェアへ感染しないようにする様々な方策をとっていくことが重要です。

●Gmailアカウントに対する巧妙なフィッシング攻撃、Google Docsに偽装したリンクに誘導

http://blog.trendmicro.co.jp/archives/14824

このニュースをザックリ言うと・・・

- 5月3日（米国時間）、Gmailのアカウントを狙うフィッシングが確認されたとして、Googleより警告が出されており、また、5月9日にはトレンドマイクロ社により、フィッシングの詳細が解説されています。

- フィッシングの内容は、Google Docs（Gmailアカウントで利用できるGoogleの文書作成・管理サービス）の正規のアプリをかたって文書を共有する旨のメールを送ってくるもので、メールに記載されたURLをクリックすると本物のGoogleの認証ページを経由して、Gmail上のメールと連絡先リストへのアクセス権限を要求してきて、これを承認してしまうと、ユーザを送信元として、連絡先リストに掲載されたユーザへさらにフィッシングメールが拡散される恐れがあるとされています。

- Googleは既に不正なアプリを削除しており、全てのユーザに「アカウントに接続されているアプリ」のページ（https://myaccount.google.com/permissions）で不正な連携を行っていないか確認するよう呼び掛けています。

AUS便りからの所感等


TREND MICRO トレンドマイクロ セキュリティブログ
Gmailアカウントに対する巧妙なフィッシング攻撃、Google Docsに偽装したリンクに誘導
投稿日: 2017年5月9日
脅威カテゴリ: メール、フィッシング、攻撃手法
執筆: Trend Micro
2017年5月3日（米国時間）、報道によると、Gmail のアカウントを狙って、正規のアプリケーションに偽装した「Google Docs」へのリンクに誘導する巧妙なフィッシング攻撃が確認されました。この攻撃は、Google Docs の正規のアプリに巧みに偽装したサードパーティのアプリケーションを利用した非常に効果的なもので、典型的なフィッシング攻撃に比べて気付くのが困難です。

- Googleでは「oAuth」という技術を使って、アプリやWebサービスとGoogleのアカウントとを連携する機能を提供していますが、Twitter等も同様にoAuthを利用しており、これにより、外部のアプリやWebサービスが連携先のアカウントの権限として利用可能になります。

- 悪意のあるアプリと連携した場合、今回のフィッシングのように、アカウント内のプライベートな情報を読み取られたり、不正な投稿を行われたりする可能性があり、アプリによるこういった挙動は必ずしもユーザ自身のPCやスマホ等から発生するものとは限らないため、UTM等での通信の遮断による防御も困難です。

- GoogleでもTwitterでも、アプリとの連携の際には、必ずアプリが要求する権限とともに承認を求めてきますので、信用できるアプリかどうか、外部の情報を確認する等した上で連携の判断を行うことが肝要です。