— AUS（アルテミス・ユーザ・サポート）便り 2017/04/10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。

●IPA、PCサポート詐欺に注意喚起…マウス動作など手口が巧妙化

https://japan.zdnet.com/article/35098949/
https://www.ipa.go.jp/security/anshin/mgdayori20170329.html

このニュースをザックリ言うと・・・

- 3月29日（日本時間）、情報処理推進機構（IPA）の「安心相談窓口だより」において、マルウェアに感染したと見せかけるような偽の警告画面を表示する詐欺行為の手口が1月に確認されたとして、注意が呼び掛けられています。

- 主な手口としては、①偽のマウスカーソルが勝手に動いているように見せかけるアニメーションを表示（本物のマウスカーソルは非表示にされる）、②偽のWindows Defenderの警告画面を表示、③ブラウザを全画面表示にしてマイクロソフトのURLにアクセスしているような偽のアドレスバーの画像等を表示、等により「5分以内に」といった時間制限を設けて偽のサポート窓口へ電話をかけるよう誘導するものが挙げられています。

- IPAでは、インターネット利用中に「ウイルスに感染」「個人情報の流出」等の警告メッセージと共に電話番号が表示された際には、その電話番号に電話せずIPA等の公的機関の相談窓口へ相談するよう呼び掛けています。

AUS便りからの所感等

- IPAに寄せられた偽の警告に関する相談件数は2016年に入ってから徐々に増加、同8月以降は月200～300件近くに上っており、これを受けて同6月および今年1月にもそれぞれ注意喚起を行っています。

- アンチウイルスやUTM等のセキュリティ製品によってはこういった詐欺行為を行うスクリプトの実行を遮断してくれるものもあるため、可能な限り有効にすること、そして手口に関する情報を普段から収集・共有し、いざ遭遇した場合に慎重に行動できる体制を整えておくことが重要です。

ZDNet Japan

PCサポート詐欺に警戒を--マウス動作など手口が巧妙化

ZDNet Japan Staff 2017年03月29日 18時40分

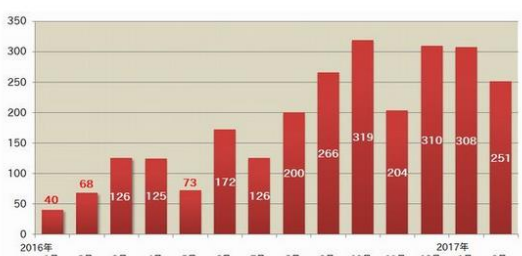
いいね！ 62　G+1 0　B! 0　Pocket 18

印刷　メール▼　ダウンロード▼　クリップ

情報処理推進機構（IPA）は3月29日、偽のPCサポートを持ち掛ける手口への注意を呼び掛けた。2016年秋から被害相談が多数寄せられる状況にあり、最近ではユーザーをだます手口が巧妙化している。

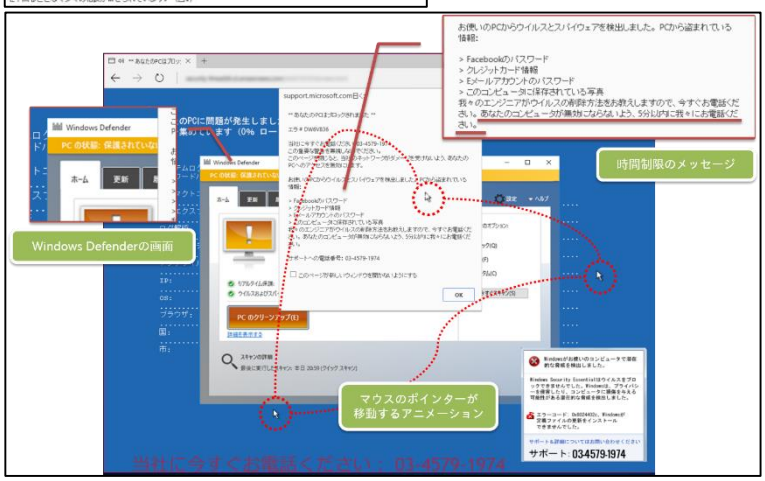
この手口では、ユーザーがPCなどを操作している最中に、いきなり「ウイルスに感染している」などと警告画面が表示され、「サポート窓口」と称する電話番号などへの連絡を要求する。ユーザーが連絡すると、相手から詳細不明のソフトをインストールさせられるなどの被害が確認されている。

IPAへの相談件数は2016年に入って増え始め、同年8月以降は毎月200件以上の相談が寄せられている状況にある。



IPAへの相談件数の推移（出典：IPA）

IPA Better Life with IT 情報処理推進機構



●マルウェアに感染したIoT機器からのアクセスが増加…警察庁が注意喚起

http://www.npa.go.jp/cyberpolice/important/2017/201703221.html

このニュースをザックリ言うと・・・

- 3月22日（日本時間）、警察庁より、マルウェアに感染したIoT機器が発信元とみられる特定ポートへのアクセスが1月下旬以降増加しているとして、注意が呼びかけられています。

- 特に急増しているのが「TCPポート5358番」で2月のアクセス数はIPアドレス毎に200件/日に上っていて、これらの約半数は「TCPポート23番(telnet)」にもアクセスしており、これらのアクセス元のIPアドレスにWebアクセスしたところ、ネットワークカメラ・ルータ等のログイン画面が表示されたことから、これらが踏み台にされた可能性があるとしています。

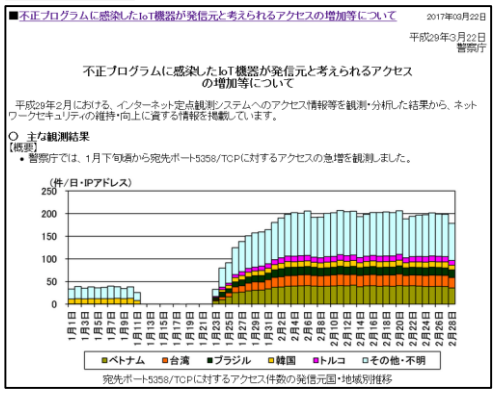
- この他、TCPポート32番・3232番および19058番へのアクセスも2月上旬に急増しており、警察庁では、IoT機器のデフォルトのID・パスワードの変更、ファイアウォールによる不必要な外部アクセスの遮断および製品の脆弱性情報の確認とファームウェアのアップデートを呼び掛けています。

AUS便りからの所感等

- 今回特にアクセスが急増したとされるTCPポート5358番については、アクセスの特徴が以前流行した「Mirai」と異なることから、それとは異なるマルウェアによるもの、またその他のポートについては、Miraiの亜種によるものとそれぞれ推測されています。

- いわゆるIoT機器やネットワーク機器の管理画面に意図せず外部の不特定多数がアクセス可能になっていないか、ネットワーク診断サービス等で確認の上、UTM等によって管理画面のポートへのアクセスを遮断することが重要です。

@police



●FTPサーバの匿名アクセスでヘルスケアデータ流出…FBIが警告

http://news.mynavi.jp/news/2017/03/31/117/

このニュースをザックリ言うと・・・

- 3月22日（現地時間）、米FBIより、FTPサーバへのサイバー攻撃によるヘルスケアデータの流出事件が確認されているとして、注意が呼びかけられており、また同29日にはセキュリティ情報ブログ「Threatpost」において警告が取り上げられています。

- FBIが警告している手口は、ID・パスワードが不要な匿名FTP（anonymous FTP）アカウントが設定されているFTPサーバへアクセスし、内部のデータをコピー、さらにそのデータをサーバ上から削除し、サーバやデータの持ち主にデータ復旧の為の身代金を要求するというものです。

- 匿名FTPアカウントが設定されたFTPサーバ情報の機密情報を狙う攻撃は、国内でも以前から度々警告が出されています（AUS便り 2016/05/23号参照）。

AUS便りからの所感等

- FTPサーバの設定次第では、今回のようにデータを削除されるケースの他にも、マルウェア等を不正にアップロードされる恐れもあるとされ、注意が必要です。

- 今日、ファイルサーバやNAS等では、FTPではなく、共有フォルダ機能によるファイルのやり取りが用いられる傾向が強い一方、特にNASにおいては、こちらもログインなしで任意のユーザがデータの読み書き可能な設定にしているケースが多々あるとみられます。

- FTPであれ共有フォルダであれ、利便性のために不特定多数が読み書き可能な設定とするのは極めて危険であり、必ずアクセスするユーザ毎にアカウントを作成し、ログインしたユーザのみが利用可能な設定であること、また外部からアクセスされないようにサーバ自体の設定やUTMの設置によるアクセス制限も行うようにすること、などが肝要です。

マイナビニュース

FTPサーバのAnonymousアカウントでヘルスケアデータ流出　- FBIが警告

後藤大地
[2017/03/31]

3月29日(米国時間)、Threatpostに掲載された記事「'Anonymous' FTP Servers Leaving Healthcare Data Exposed | Threatpost | The first stop for security news」が、匿名アカウントが有効になったFTPサーバなどがサイバー攻撃の対象となっており、データ漏洩や身代金要求に利用されていると伝えた。米連邦捜査局(FBI; Federal Bureau of Investigation)はこうした事態を受けて警告を発表している。