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。

●MUFGカードかたるフィッシングメール出回る…フィッシング対策協議会が注意喚起

http://www.itmedia.co.jp/news/articles/1706/13/news084.html
https://www.antiphishing.jp/news/alert/mufgcard_20170613.html

このニュースをザックリ言うと･･･

- 6月13日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、クレジットカード「MUFGカード」をかたるフィッシングメールが出回っているとして警告が出されています。

- このフィッシングメールは、件名が「Webサービス利用者」、本文が「親愛なるアカウント保有者 引き続きWebサービスを利用するには、このアカウントで登録カードを確認する必要があります」で始まり、「http://●●●●.com/4000.html」等のURLからなるフィッシングサイトへ誘導するものとなっています。

- 同協議会では、こういったサイトでアカウント情報を絶対に入力しないよう、また同様のサイトやメールを見かけた場合は協議会へ連絡するよう呼び掛けています。

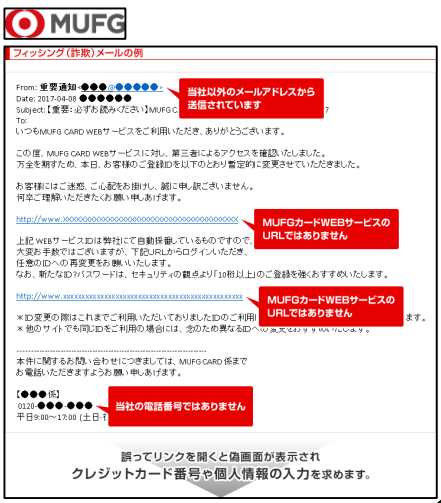
- また、MUFGカードを取り扱う三菱UFJニコス社からも、同社から届くメールのドメインは「mufgcard.com」「cr.mufg.jp」の２種類のみであるとしています（http://www.cr.mufg.jp/member/notice/fishing/index.html）。

AUS便りからの所感等

- 今回確認されたフィッシングサイトはいずれもHTTPSを使っておらず、かつ本物のMUFGカードのサイトではログインページ等においてEV-SSL証明書を使っており、これを踏まえている限りは、フィッシングサイトか否かの確認は十分可能とみられます。

- Webブラウザやアンチウイルスソフト、UTMが提供するフィッシングサイトへのアクセスを警告あるいは遮断する機能は可能な限り有効にすること、他にも通常使用するサービスのログインページはブックマークに登録してそこからアクセスするよう心がけることにより、フィッシングにだまされる可能性を低減できるでしょう。

- ただし、PCにマルウェアが感染している場合、本物のログインページの表示時に偽のログインフォームを表示され、そこからアカウント情報・カード情報を詐取される恐れもあり、この観点からも注意は欠かせません。



●マイクロソフト6月度の月例セキュリティパッチリリース、5月に続きXP向け等も

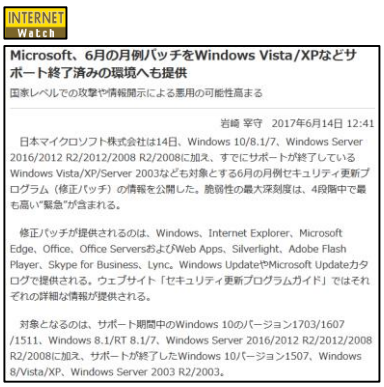
http://internet.watch.impress.co.jp/docs/news/1065158.html

このニュースをザックリ言うと・・・

- 6月14日（日本時間）、マイクロソフトより、Windows・IE・Edge・Office等に対する6月度の月例セキュリティパッチがリリースされました。

- 今回「国家レベルでの攻撃および情報開示による悪用の危険性が高まっている」としており、既にサポートが終了したWindows XP・Server 2003・Vista・8等に対してもパッチをリリースしています。

- 同社では5月にも、ランサムウェア「WannaCry/WannaCrypt」が猛威をふるったことを受けて、脆弱性「MS17-010」のパッチをXP等に対して追加リリースしており（「AUS便り 2017/5/22号」参照）、2ヶ月続けて例外的なリリースが行われる事態となっています。


INTERNET Watch

Microsoft、6月の月例パッチをWindows Vista/XPなどサポート終了済みの環境へも提供

国家レベルでの攻撃や情報開示による悪用の可能性高まる

岩崎 翠守　2017年6月14日 12:41

日本マイクロソフト株式会社は14日、Windows 10/8.1/7、Windows Server 2016/2012 R2/2012/2008 R2/2008に加え、すでにサポートが終了しているWindows Vista/XP/Server 2003なども対象とする6月の月例セキュリティ更新プログラム（修正パッチ）の情報を公開した。脆弱性の最大深刻度は、4段階中で最も高い"緊急"が含まれる。

修正パッチが提供されるのは、Windows、Internet Explorer、Microsoft Edge、Office、Office ServersおよびWeb Apps、Silverlight、Adobe Flash Player、Skype for Business、Lync。Windows UpdateやMicrosoft Updateカタログで提供される。ウェブサイト「セキュリティ更新プログラムガイド」ではそれぞれの詳細な情報が提供される。

対象となるのは、サポート期間中のWindows 10のバージョン1703/1607/1511、Windows 8.1/RT 8.1/7、Windows Server 2016/2012 R2/2012/2008 R2/2008に加え、サポートが終了したWindows 10バージョン1507、Windows 8/Vista/XP、Windows Server 2003 R2/2003。

AUS便りからの所感等

- 今回修正された脆弱性は、上記のMS17-010と同様、NSAから流出した攻撃ツール（「AUS便り 2017/4/24号」参照）にて悪用される恐れがあったとみられます。

- 例えば、Windows Server 2003（およびXP）に含まれるWebサーバソフト「IIS 6」には、3月にサーバを乗っ取ることが可能な脆弱性（CVE-2017-7269）が確認されていましたが、当初は修正の見込みはないとされていたものの、これも今回修正の対象となっています。

- サポートが終了したOSは、現在サポート中の新しいOSと比べてマルウェアに感染するリスクが高いと言え、度々繰り返していることですが、リリースされているパッチを全て適用した上で、他のPC等が存在するLANからUTM等によって隔離することが肝要です。

●ウクライナで大規模停電発生…マルウェアが侵入

http://www.itmedia.co.jp/enterprise/articles/1706/13/news052.html

このニュースをザックリ言うと・・・

- 6月12日（現地時間）、スロバキアのアンチウイルスベンダーESET社より、2016年12月にウクライナで発生した「マルウェアが原因とされる大規模停電」の事例が同社ブログで紹介されています。

- 記事によれば、「Industroyer」と名付けられたマルウェアは、電力供給等の世界中の公共インフラで使われている産業通信プロトコルによる通信機能を備えており、これにより変電所のスイッチやブレーカーを直接制御していたとされています。

- 他にも暗号化通信により外部からの指令を受ける機能や、攻撃終了後に自分の痕跡を完全に消す機能を備えていたとのことです。

- ウクライナではこの1年前の2015年12月にも別のマルウェアによる停電事故が発生しており、同社では今回の事例を、イランの原子力関連施設を攻撃した「Stuxnet」以来最大の産業制御システムに対する脅威と位置付けています。


ITmedia エンタープライズ

停電の原因は産業制御システム狙うマルウェアか
「Stuxnet以来、最大の脅威」

ウクライナで停電を発生させた原因とみられるマルウェア「Industroyer」は、世界中の公共インフラで幅広く使われている産業通信プロトコルを利用していた。

[鈴木聖子、ITmedia]

セキュリティ企業のESETは6月12日、ウクライナの首都キエフで2016年12月に発生した停電について、産業制御システムを狙うマルウェアを使ったサイバー攻撃だった公算が大きいと発表した。「Stuxnet以来最大の産業制御システムに対する脅威」と位置付けている。

• 関連記事→ウクライナでサイバー攻撃による停電、発端はマルウェア

この事件では、ウクライナの送電網がサイバー攻撃を受けて首都キエフの一部が1時間にわたって停電した。ESETが分析したマルウェアは、送電網に重大な障害を発生させることができるほか、手を加えれば他の重要インフラを標的にできる可能性もあることが判明。同社はこのマルウェアを「Win32/Industroyer」と命名した。

AUS便りからの所感等

- 2015年12月の停電の際、ウクライナ政府は対立関係にあるロシアのハッカーグループによる攻撃と批判しており、今回も同様にロシアが背後にいる可能性が指摘されています。

- いわゆるIoT（モノのインターネット）の流れの一つとして「スマートグリッド」と呼ばれる新たな電力網が日本を含め世界中で進んでいますが、今回挙げられたようなサイバー攻撃の影響を受けやすくなることにも当然注意が必要であり、制御網にマルウェアが侵入するのみならず、そこから指令ホストとの通信、さらにはそこを踏み台にした攻撃等が行われるというシナリオも想定したネットワーク構成が重要となってくるでしょう。