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。

●Webベースの攻撃を阻止…Microsoft、法人向けセキュリティ機能をChrome・Firefoxにも提供する拡張機能をリリース

https://www.itmedia.co.jp/news/articles/1903/19/news077.html
https://forest.watch.impress.co.jp/docs/news/1175151.html

このニュースをザックリ言うと･･･

- 3月15日（現地時間）、Microsoftより、Windows 10のEdgeブラウザ向けに提供されている法人向けセキュリティ機能「Windows Defender Application Guard（WDAG）」をChromeやFirefoxにも提供すると発表されました。

- WDAGはWindows10 Enterprise（バージョン1709以降）およびPro（バージョン1803以降）によって提供されており、管理者が信頼できるWebサイトとして指定した以外のサイトへのアクセスをOS上の別環境に隔離して実行する機能です。

- 今回、ChromeやFirefoxからの信頼できないサイトへのアクセスを、隔離環境上のEdgeで実行するための拡張機能が各ブラウザの公式ストアでリリースされています。

AUS便りからの所感等

- WDAGは、前述のとおりWindows 10の法人向けセキュリティ機能に関するもので、無印の10では使用できず、またハードウェア面でも使用するための条件がありますので、導入の検討にあたってはMicrosoftの情報（※）を十分確認する必要があります。
（※）https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview

- Windows 7や8.1については新たな機能を追加するフェーズが終了しており、Windows 10において次々と追加されている新たなセキュリティ機能が今後8.1以前に追加される可能性は低いため、そういった機能が使えるかどうか等、なるべく早く10への移行を前提とした各種検証を急ぐべきでしょう。


ITmedia NEWS

Webベースの攻撃を阻止　Microsoft、ChromeとFirefox向けの拡張機能を提供

2019年03月19日 11時53分 公開　[鈴木聖子，ITmedia]

印刷　25　29　B!　18

米Microsoftは3月15日、Webブラウザベースの攻撃阻止を目的とした拡張機能「Windows Defender Application Guard」を、Googleの「Chrome」と、Mozillaの「Firefox」向けに提供すると発表した。

MARCH 15, 2019 2:02 PM
Announcing Windows 10 Insider Preview Build 18358
By Dona Sarkar and Brandon LeBlanc

同拡張機能では、ユーザーがChromeやFirefoxで閲覧するWebサイトのURLを、企業の管理者が指定した信頼できるWebサイトのリストと照合。信頼できないWebサイトと判断した場合は、自動的にMicrosoftのWebブラウザ「Edge」のセッションへとリダイレクトして隔離する。

ユーザーは、隔離されたMicrosoft Edgeのセッション内で、他のシステムを危険にさらすことなく、そうしたサイトを自由に閲覧できるという。

セッションは動的な切り替えができ、Microsoft Edgeの隔離されたセッション内にいたユーザーが、信頼できるサイトに戻ろうとすると、デフォルトのブラウザに切り替わる。

ChromeとFirefox向けのWindows Defender Application Guardは、3月15日にリリースされたWindows 10 Insider Preview版に搭載され、間もなく公開される「Windows 10 Pro」と「Windows 10 Enterprise」の更新版で正式提供開始を予定している。


窓の杜 WINDOWS FOREST

“Windows Defender Application Guard”がGoogle Chrome/Firefoxでも利用可能に

信頼できないサイトへのアクセスをサンドボックスへ隔離する法人向けセキュリティ機能

樽井 秀人　2019年3月18日 12:00

米Microsoftは3月15日（現地時間）、“Windows Defender Application Guard”を「Google Chrome」や「Firefox」で利用するためのWebブラウザー拡張機能をリリースした。各ブラウザーのストアから無償でダウンロードできる。

“Windows Defender Application Guard（WDAG）”は、最近のWindows 10に搭載されているエンタープライズ（法人）向けのセキュリティ機能。あらかじめ信頼できるWebサイトを定義しておき、それに含まれていないWebサイトへのアクセスをハードウェアから隔離された“Hyper-V”サンドボックスに閉じ込めることで、悪意あるサイトから機密情報を守ることが可能。インターネットを介してローカルネットワークやデバイスへ侵入しようとする高度な攻撃に対して有効であるという。

“Windows Defender Application Guard（WDAG）”の仕組み

●人気スマホゲームかたるフィッシング報告相次ぐ、運営も警告

https://www.itmedia.co.jp/news/articles/1903/14/news127.html

このニュースをザックリ言うと･･･

- 3月8日（日本時間）頃より、人気スマートフォンゲーム「Fate/Grand Order」（以下FGO）をかたるフィッシングメールが確認されたとの報告がTwitter上等で相次ぎ、同13日にはFGO運営チームより注意喚起が出されています。

- フィッシングメールは、件名が「Re:[情報の完全なオーダー]:請求書の領収書xxxx年xx月xx日受領」等で、課金アイテムの購入明細を装ったものとされていますが、本文が「購入日」が「入購日」になっているなど不自然な日本語であり、送信元も運営公式のアドレスではないとされています。

- 運営チームでは、個人情報等およびクレジットカード情報の収集を目的としている可能性が高いとし、心当たりのないメールの開封およびリンクのクリックは控えるよう呼びかけています。

AUS便りからの所感等

- AmazonやiCloud、PayPalといった大手Webサイトをかたったメールによるフィッシングやマルウェアの拡散は既に当たり前となっており、FGOのような人気のあるゲームがなりすましの対象となることも決して驚くべきものではないでしょう。

- メールはこのゲームで一度も遊んだことがない者も含め無差別に送信されており、特にアカウントを登録したまま遊ばなくなり放置している者がフィッシングに騙される恐れがあるとみられます。

- こういった不審なメールへの対策として、他に報告されていないか件名や本文の一部で検索するよう心がけること、またフィッシングやマルウェア感染に対する一般的な対策として、PCにおいてもスマホにおいてもアンチウイルス等セキュリティソフトを導入し、Webブラウザのセキュリティ機能を有効にすることが重要と言えます。


ITmedia NEWS

FGOの明細かたるフィッシングメール出回る　件名に「請求書の領収書」など

2019年03月14日 17時20分 公開　[ITmedia]

スマートフォンゲーム「Fate/Grand Order」（FGO）運営チームは3月13日、FGOの課金アイテム「聖晶石」の購入明細を装ったフィッシングメールが確認されていると注意を呼び掛けた。FGOで遊んだ覚えがない人にも送信されているといい、メールを開封したりURLのクリックしないよう呼び掛けている。

運営の注意喚起より

●IoTマルウェア「Mirai」の標的が企業にシフト、攻撃の威力さらに増大の恐れ

https://www.itmedia.co.jp/news/articles/1903/19/news056.html

このニュースをザックリ言うと･･･

- 3月18日（現地時間）、セキュリティベンダーの米Palo Alto Networks社より、IoTマルウェア「Mirai」の新しい亜種が発見されたとして警告が出されています。

- 警告によれば、亜種には新たに法人向けのワイヤレスプレゼンテーションシステム「WePresent WiPG-1000」と「LG Supersign TV」の脆弱性を突くコードが組み込まれており、またデフォルトの認証情報を使って総当たり方式のブルートフォース攻撃を仕掛ける機能なども強化されていたとしています。

- 同社ではMiraiの標的が企業へとシフトする傾向が一層鮮明になったとして、企業はネットワーク上のIoTデバイスについて、デフォルトのパスワードを変更し常に最新のパッチを適用すること、またパッチが適用できない機器への最終手段として機器をネットワークから取り外すこと、も呼びかけています。

AUS便りからの所感等

- 同社は2018年9月にも、Miraiの亜種にApache StrutsやSonicWallの脆弱性を突くコードが追加されていたことを指摘しており、Miraiが企業をターゲットとする傾向は徐々に強まっているようです。

- とにかく、企業ネットワーク内に設置されているあらゆる機器の存在を把握し、ファームウェアを最新に保つ等確実な管理を行う体制を整え、また万が一マルウェアに感染した機器からの攻撃を最小限に抑えられるよう、UTMを用いたネットワークの適宜分割等の対策をとることを推奨致します。


ITmedia NEWS

IoTマルウェア「Mirai」の標的が企業にシフト、攻撃の威力さらに増大の恐れ

2019年03月19日 07時20分 公開　[鈴木聖子, ITmedia]

セキュリティ企業の米Palo Alto Networksは3月18日、2016年に猛威を振るったIoTマルウェア「Mirai」の新しい亜種が見つかったと伝えた。Miraiの標的が企業へとシフトしつつあり、攻撃の威力が一層増大する恐れもあると警告している。

Miraiは、ルーターや防犯カメラといったIoT機器に感染するマルウェア。2016年に史上最大級の分散型サービス妨害（DDoS）攻撃を引き起こしたことで知られる。

Palo Alto Networksによると、今回見つかったMiraiの亜種には、新たに法人向けのワイヤレスプレゼンテーションシステム「WePresent WiPG-1000」と「LG Supersign TV」の脆弱性を突くコードが組み込まれていた。

同社は2018年9月の時点で、MiraiにApache Strutsの脆弱性を突くコードが追加されたと伝えており、今回の亜種によって、Miraiの標的が企業へとシフトする傾向が一層鮮明になった。

企業を標的とすることで悪用できる帯域幅が増大し、Mirai感染デバイスで構成されるbotネットが仕掛けるDDoS攻撃の威力も高まるとPalo Alto Networksは警告する。