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。

●マルウェア「Emotet」活動再開か…米国機関等が注意喚起-

https://news.mynavi.jp/article/20191029-915623/
https://internet.watch.impress.co.jp/docs/news/1213360.html
https://www.daj.jp/security_reports/191017_1/

このニュースをザックリ言うと･･･

- 10月25日(現地時間)、米セキュリティ機関のUS-CERTおよびCISAより、マルウェア「Emotet」の活動が活発化しているとして注意喚起が出されています。

- Emotetは元々はインターネットバンキングを狙うトロイ型マルウェアですが、近年は感染したPCに別のマルウェアをダウンロードする行動もとっているとのことです。

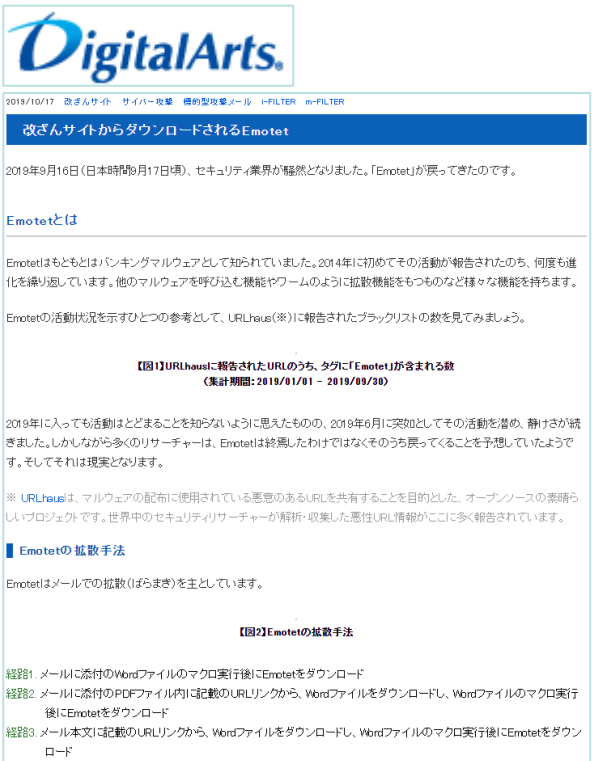
- 同17日には国内セキュリティベンダーのデジタルアーツ社からもEmotetに関するレポートが発表されており、6~8月は活動が落ち着いていたものの、9月から再び活発化したとのことです。

AUS便りからの所感等

- デジタルアーツ社のレポートによれば、主にメールに添付されたWordファイルの不正なマクロ実行後にEmotetがダウンロードされるケースが多く、またダウンロード先として、改ざんされた国内のWebサイトが指定されていることも多いとされています。

- どういった種類のマルウェアが流行するかは日々変動し、一旦沈静化した種類のものでもいつまた再び活動しだすか予測することは簡単ではないため、普段から、アンチウイルスやUTMによる防御が十分に行われているかを確認しつつ、様々な種類のマルウェアがどういった経路で感染するか、どうやって感染する可能性を抑えるかについても随時情報収集していくことが肝要です。

- またWebサイトを運営する側においても、くれぐれも閲覧者をマルウェアに感染させる一端を担うことのないよう、サーバー上にインストールするソフトウェアや外部サービス等、様々な改ざん検知ソリューションを検討すべきでしょう。


DigitalArts.

2019/10/17　改ざんサイト　サイバー攻撃　標的型攻撃メール　i-FILTER　m-FILTER

改ざんサイトからダウンロードされるEmotet

2019年9月16日（日本時間9月17日頃）、セキュリティ業界が騒然となりました。「Emotet」が戻ってきたのです。

Emotetとは

Emotetはもともとはバンキングマルウェアとして知られていました。2014年に初めてその活動が報告されたのち、何度も進化を繰り返しています。他のマルウェアを呼び込む機能やワームのように拡散機能をもつものなど様々な機能を持ちます。

Emotetの活動状況を示すひとつの参考として、URLhaus(※)に報告されたブラックリストの数を見てみましょう。

【図1】URLhausに報告されたURLのうち、タグに「Emotet」が含まれる数
（集計期間：2019/01/01 - 2019/09/30）

2019年に入っても活動はとどまることを知らないように思えたものの、2019年6月に突如としてその活動を潜め、静けさが続きました。しかしながら多くのリサーチャーは、Emotetは終焉したわけではなくそのうち戻ってくることを予想していたようです。そしてそれは現実となります。

※ URLhausは、マルウェアの配布に使用されている悪意のあるURLを共有することを目的とした、オープンソースの素晴らしいプロジェクトです。世界中のセキュリティリサーチャーが解析・収集した悪性URL情報がここに多く報告されています。

Emotetの拡散手法

Emotetはメールでの拡散（ばらまき）を主としています。

【図2】Emotetの拡散手法

経路1. メールに添付のWordファイルのマクロ実行後にEmotetをダウンロード
経路2. メールに添付のPDFファイル内に記載のURLリンクから、Wordファイルをダウンロードし、Wordファイルのマクロ実行後にEmotetをダウンロード
経路3. メール本文に記載のURLリンクから、Wordファイルをダウンロードし、Wordファイルのマクロ実行後にEmotetをダウンロード


INTERNET Watch

ニュース

「Emotet」に感染させるばらまき型メールに注意、9月から拡散活動が再び活発化

磯谷 智仁　2019年10月17日 19:17

ツイート　リスト　いいね！42　シェア　B! 3　Pocket　9

モジュール型のマルウェア「Emotet」の感染を狙ったばらまき型メールが再び拡散されているとして、デジタルアーツ株式会社がセキュリティレポートを公開した。

Emotetは、元々はバンキングマルウェアとして利用されていたが、現在では主に他のマルウェアに感染させるローダーとして利用されている。2019年6月から8月にかけて拡散活動が一時的に落ち着いていたが、9月ごろから再び活発化している。

URLhaus-tags: emotet

マルウェアの配布に使用されているURLを共有するプロジェクト「URLhaus」に報告されたもののうち、タグに「Emotet」が含まれる数（集計期間：2019年1月1日～9月30日）

●niconicoで「リスト型攻撃」による不正ログイン発生、パスワードの見直しを

https://internet.watch.impress.co.jp/docs/news/1215658.html
https://blog.nicovideo.jp/niconews/121368.html

このニュースをザックリ言うと・・・

- 10月27日(日本時間)、ドワンゴ社より、同社が運営する「niconico(ニコニコ動画)」において本人によるものではないと思われるアカウントへのログインを複数検出しているとして注意喚起が出されています。

- 外部のサービスで不正に入手したアカウント情報(メールアドレス・パスワード)でログイン試行を行う、いわゆる「リスト型アカウントハッキング(リスト型攻撃)」の可能性があるとしています。

- 同社では、niconicoで被害がなくとも、同じメールアドレス・パスワードを用いている他サービスにおいて被害が発生する場合があるとし、niconico上で「身に覚えのないログイン履歴があった」「従来のパスワードではログインできないようになっていた」場合には、他サービスでも見直しを行うよう推奨しています。

AUS便りからの所感

- niconicoでは2018年5月や7月、あるいはそれ以前にも度々リスト型攻撃による不正ログインが発生しています。

- このような大手Webサービスに契約している場合はどこでも攻撃を受けると考えて良く、パスワードを他のサービスと同じものにしないことはもちろん、2段階認証が利用可能(niconicoでも提供されています)であれば是非とも有効にし、アカウントの保護を行うことを推奨致します。

- 不特定多数にサービスを提供していないとしても、自社サーバーが被害を受けないということは決してなく、組織で使用しているオンプレミスあるいはクラウド上のWeb・メールサーバーに対し不正ログインの試行が行われる可能性もありますので、不正ログイン試行の兆候を検知し遮断できるよう、サーバーの設定やUTM等によるIDS・IPS機能の有効化も検討に値するでしょう。

●件名「LINE緊急問題」、LINE騙るフィッシングに注意喚起

https://internet.watch.impress.co.jp/docs/news/1215229.html
https://www.antiphishing.jp/news/alert/line_20191028.html

このニュースをザックリ言うと・・・

- 10月28日(日本時間)、フィッシング対策協議会より、LINEを騙るフィッシングメールが確認されたとして注意喚起が出されています。

- 例に挙げられているメールは、件名が「LINE緊急問題」や「LINEにご登録のアカウント（名前、パスワード、その他個人情報）の確認」で、LINEアカウントに不正ログインが確認されたと偽り、メールアドレス・パスワード・電話番号を詐取しようとする偽サイトへ誘導するものとなっています。

- 同協議会では、少なくとも発表の時点でフィッシングサイトは稼働中、また今後もURLを変える可能性があるとし、このようなフィッシングサイトにて、アカウント情報や電話番号等を絶対に入力しないよう警告しています。

AUS便りからの所感等

- LINEを騙るフィッシングは、最近では9月10にも同協議会から警告が出されています
(https://www.antiphishing.jp/news/alert/line_20190910.html)が、「お客様のLINEアカウントに異常ログインされたことがありました。お客様のアカウントの安全のために、ウェブページで検証してお願いします」という少々不自然な文言が共通しています。

- LINE公式サイトにおいても以前から同様のフィッシングがあることから注意喚起を出しています
(https://help.line.me/line/?contentId=20000293)ので、利用者は必ず目を通し、慎重に行動するようにしてください。

- もちろん、何の防御もなしに「慎重に行動する」だけではなく、Webブラウザー・アンチウイルスあるいはUTMのアンチフィッシング等のセキュリティ機能を有効にし、不審なサイトへのアクセスを水際で遮断できるような体制を整えておくことが重要です。