Advanced Technology, Secu・Japan

サイバー安全予防対策

サイバー攻撃タイプ

＋ インターネットにより他のコンピュータに不正アクセスし，

相手国や企業に打撃を与える行為

攻撃の主なタイプ

フィッシング攻撃	パーミング攻撃	悪性コード攻撃 ランサムウェア	スカムウェア
			

BEC

BEC(Business e-mail Compromise)

メール詐欺の一形態で、一般的に会社財務へのアクセス権限のある職員を対象にハッカーの銀行口座にお金を振り込ませる方法を使います。

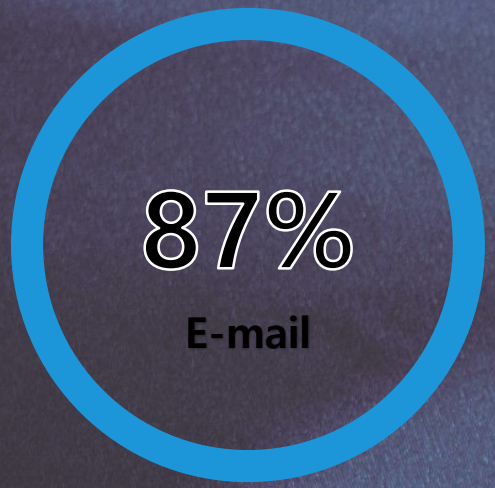
CEOまたは信頼できる人だと勘違いさせるメールを作って詐欺を働き

ランサムウェアなどウイルスを添付ファイルで配布し、さらなる被害を与える。

メール統計

被害取引先

Evolution of Social Engineering e-mail Attack

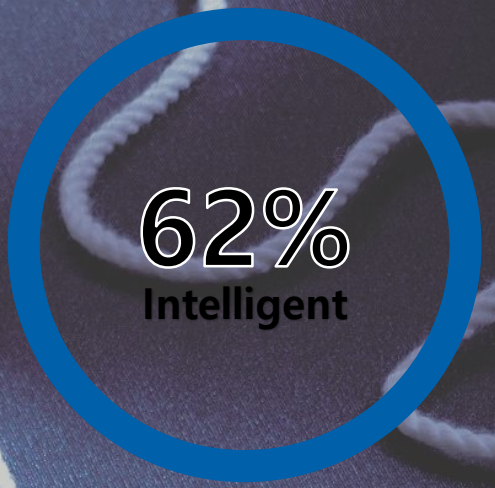


ハッキング流入経路

出典: Palo Alto Networks

BEC被害額

出典: Trend micro paradigm



攻撃タイプ

出典: Valimail

サイバー攻撃タイプ

フィッシング攻撃

フィッシング(Phishing)は、知人または有名企業を詐称したメッセージをメール、メッセンジャー、文字など多様なサービスを通じて攻撃対象者に送信する詐欺手法である。

メッセージを受けたユーザーが、知人または信頼度の高い企業からのメッセージと誤認し、偽サイトにアクセスすると、金融機関でセキュリティ認証手続きを行うように勧める。

このように利用者が自分の金融情報(口座番号、暗証番号、セキュリティカード、IDなど)を直接入力するように誘導する。

自分の金融情報を入力してしまうと、金銭的被害へとつながりかねない。

また、添付ファイルを確認すると、悪性コードにも感染することがある。

パーミング攻撃

フィッシング(Phishing)に続き登場した新しいインターネット詐欺手法である。

広い意味ではフィッシングの一つであり、フィッシングより一段階進化した形といえる。パーミングは、サイトが公式に運営しているドメイン自体を途中で奪い取る手法だ。

フィッシング(Phishing)の場合は、ユーザが注意深く見ていれば気づくだろうが、パーミングの場合には、ユーザーがどんなにドメインアドレスやURLアドレスを注意深く調べていても、容易に騙されてしまう。

フィッシング方式より被害に遭う恐れが大きい。

サイバー攻撃タイプ

スカムウェア

企業のメール情報をハッキングして、フリーウェアなどに同梱されるソフトウェアを使って、貿易取引代金を横取りする犯罪手法のことをいう。

1980年代から現れ、当時はツールとして書面が使われた。

主に被害対象企業に悪性コードを感染させた後、会社が支払決済方式を変えるよう誘導し、メールをハッキングして取引会社の間でやり取りする内容を見守り続ける。送金と関連した内容がある時に割り込んで、主要取引先がメールを送信したかのように、偽の口座情報を送り、取引代金を奪取する方式だ。

悪性コード攻撃(ランサムウェア)

悪性コードはマルウェア、悪性プログラムとも呼ばれます。

製作者が、故意にユーザーに被害を与えるために作った悪意的な目的のプログラムをいいます。 最近の悪性コードは、自ら伝播されるという特徴があります。

特に、トロイの木馬は攻撃者がコンピュータに侵入して使用者のコンピューターを操縦できるプログラムを言います。

不正なコードはインターネット検索、シェアウェアや不正コピープログラムの使用時などに、メールの添付ファイルやメッセンジャーを通じて送信されたファイルを開く際に侵入します。

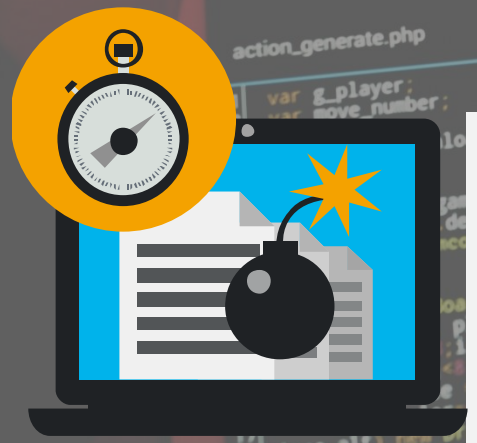
不正コードがインストールされると、コンピュータのシステム性能低下、個人情報漏洩、ファイルの削除、攻撃者のコンピュータ遠隔制御といった症状が現れます。

攻撃経路

スパムメール及びフィッシングメール

- ✓ 出典不明のメール受信時、添付ファイルまたはメールにURLリンクを通じて悪性コードを流布する事例があるので、添付ファイルの実行またはURLリンクのクリックには注意が必要です。
- ✓ 最近、ユーザーからのメール確認を誘導するため、“年末調整案内”、“忘年会案内”、“領収書添付”などのように日常生活と密接な内容を偽装しており、出典の明確な添付ファイルはすぐに実行せず、パソコンに保存してワクチンで検査してから開けることをお勧めます。

信頼できないサイト



- ✓ 信頼できないサイトの場合、単なるホームページ訪問だけでも感染する可能性があり、ドライブバイダウンロード(Drive-by-Download)技法で流布されます。
- ✓ これを防止するためには、使用するPCの運営体制および各種SWのセキュリティパッチを常に最新にアップデートすることが重要です。
  また、わいせつ物、無料ゲームサイトなどはセキュリティ管理が行き届いていないサイトとして、利用自制を勧告します。

攻撃経路

ファイル共有サイト

✓トレント、ウェブハードなどP2Pサイトを通じて動画などのファイルをダウンロードし、これを実行した場合、悪性コードに感染する事例があり、注意が必要です。

社会ネットワークサービス(SNS)

✓最近フェイスブック、リンクドメインなどの社会ネットワークサービス(SNS)に掲載されている短縮URLや写真を利用してランサムウェアを流布する事例があります。特に、SNSアカウントハッキングを通じて信頼できるユーザーになりすまし、悪性コードを流布できるため、注意が必要です。

被害事例

2018.03.27

履歴書ファイルに偽装した“シグマ”ランサムウェアが全世界で流布

セキュリティ会社ハウリによると、最近世界中を対象に"シグマ(Sigma)"ランサムウェアが広範囲に流布されているという。このランサムウェアはメールを通じて送信され、メールには悪性コードが含まれた履歴書ワード文書ファイルが添付されている。

例えば、メールのタイトルで“入社志願”という言葉と“志願者の名前”はそれぞれ違う類型に制作される。

履歴書ワード文書にはパスワードを設定し、メール本文にある暗号を入力したユーザーのみ、文書を閲覧できるようにする。これによって受信者の信頼を得て、暗号のない文書を事前に閲覧して悪性コードを探知する自動分析システムをかいくぐるわけである。

受信者が履歴書文書を開く時には、特定のサーバからランサムウェアをダウンロードして実行する。

攻撃者は、パソコン内の主要ファイルを暗号化したあと、ランサムノート(メッセージ)を通じて復旧費用として4000ドル(約50万円)相当を要求した。

セキュリティ会社ハウリは、「履歴書を装ったランサムウェアおよび知能型持続脅威(APT)攻撃が発見されている企業の人事担当者たちは、履歴書閲覧時に別途に隔離された空間である仮想環境などで閲覧する必要がある」としている。

被害事例

2017.11.23

ポータルサイト、DHLのアカウント情報を狙った メールフィッシングが蔓延

最近は、HTM、HTML添付ファイルによりIDとパスワードを奪取する攻撃が増加している。
アカウント奪取は、追加被害の可能性が高い添付ファイルを利用して、アドレスをフィッシングすることであり、この手法が幅を利かせている。特に、国内代表ポータルである国際輸送サービスDHL社のアカウントを狙ったことが確認され、ユーザの注意が求められている。
脅威情報対応専門サービスを提供するZeroCert社は、「添付ファイルを利用したアカウント奪取フィッシングがDHL社で確認された」と発表した。これまで〝△Sample.html、△BL No EE76429352TW.htm〟など2つの添付ファイルが確認され、アカウントを奪取するサーバーは米国とオーストリアに分かれている。
添付ファイルをクリックすると、DHL社を偽装した偽のホームページに移動し、ID(ID)とパスワード(PW)を入力するように誘導する。アカウントを奪取するのが目的だ。（中略）
一方、アカウント奪取は、単にIDとパスワードだけが奪取されることで終わらない。大半の人々が、一つのIDとパスワードを同様に使用するため、初回の攻撃で奪取した情報をもとに、さらに危険な攻撃といえる他のウェブサイトの攻撃が可能になる。
一度アカウント情報を奪取された時には、同じIDを使うすべてのウェブサイトのパスワードを変えなければならない。

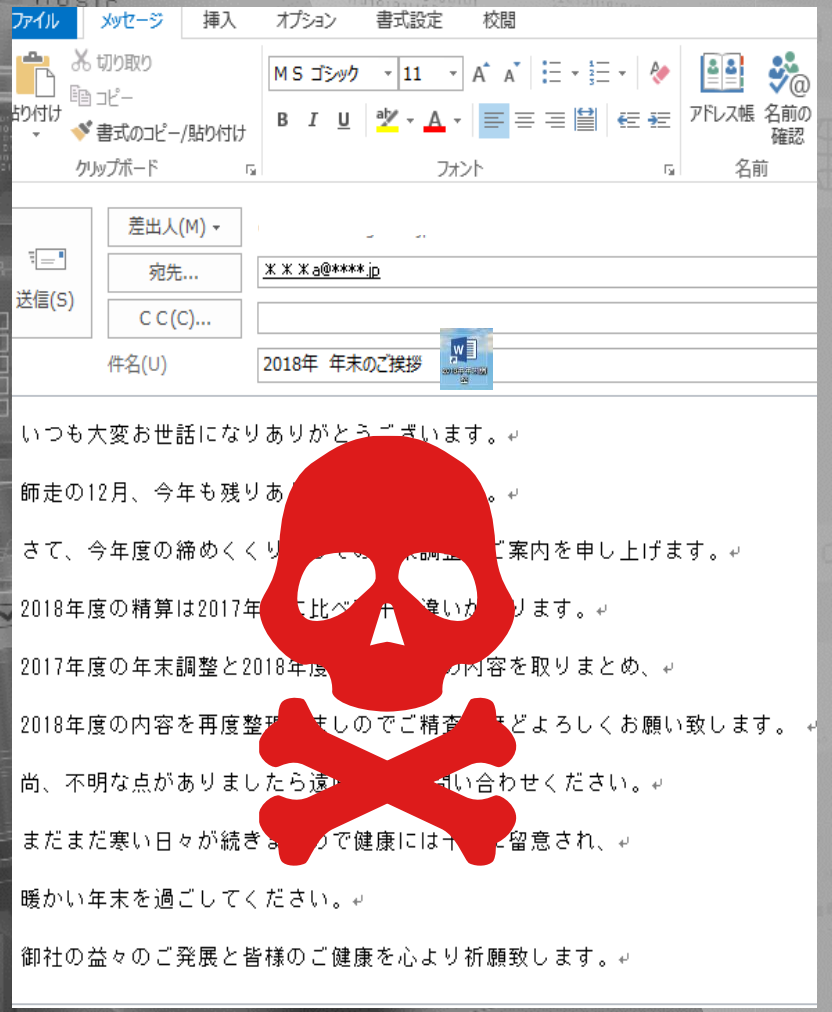
被害事例

2018.12.13

“年末調整案内"で悪質なメール拡散

2018年、公共機関と民間企業に“なりすましメール”をばら撒いた攻撃組織が再び活発に活動

年末調整の時期には、年末調整と関連した内容を偽装した悪性メールが流されるため、特に注意が求められる。イーストセキュリティ社は、「昨年と今年の年末調整の内容の違いを案内する」という内容のメールと共に添付された“2018年度年末調整”というdoc.文書の添付ファイルを開くよう誘導していると明らかにした。メール受信者がその内容を確認する為に、添付された文書ファイルを開いてコンテンツ使用ボタンを押すと、直ちにMSワードのマクロ機能が活性化し、特定のC&C(命令制御)サーバーを通じて悪性コードがダウンロードされる。 MSワードで提供するマクロ機能とは、文書作成中に反復的な動作が必要な場合、事前に記録された命令を自動で実行し、文書編集の効率性を高める機能である。



被害事例

LG化学,メールフィッシングで240億ウォンの詐欺被害

2016.04.29

LG化学社が海外取引先を装った国際メール詐欺で、取引代金240億ウォンを騙し取られた。
29日、関連業界によると、LG化学社は、国際メール詐欺に遭い、取り引き代金240億ウォンを騙し取られた事件の調査をソウル中央地検に依頼した。 事件は、国際犯罪を担当する外事部に割り当てられた。
LG化学社は、サウジアラビアのアラムコプロダクトトレーディング社から化学原料であるナフサを輸入している。LG化学は先月、アラムコ社側の名義で取引代金の口座が変更されたというメールを受け取り、これに疑いを抱かず240億ウォンの取引代金を送金した。しかし、メールを送ったのはアラムコ社を装った国際犯罪組織だった。取引代金として送金した約240億ウォンを騙し取られたのだ。LG化学社は、今回の事件はメールハッキングによる貿易代金詐欺だと見ている。ハッカーがLG化学社やアラムコ社側のメールをハッキングした後、精巧に取引請求書を作って詐欺を働いたのだ。

Hot issue

ランサムウェア

ランサムウェアとは“身代金(Ransom)とソフトウェア(Software) ”の合成語である。

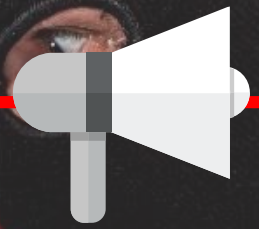
システムをロックしたり、データを暗号化して使用できないようにした後、

これを回復するための金銭を要求する悪性プログラムである。

ランサムウェア類

文書に隠れている
ロッキー(Rocky)

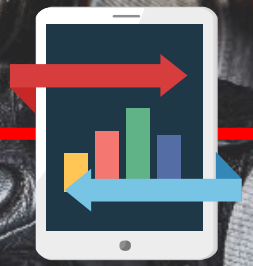
金銭を要求する
ケルベル(Cerber)



ウェブサイト自動実行
エレボス(Erebus)

dll形の
クリプト・XXX(Crypt.xxx)

運営体制感染
ワナークライ(WanaCry)



添付ファイルを流布
テスラクリプト(TeslaCrypt)

ランサムウェア被害

①重要文書暗号化

- 重要文書流出
- 情報流出
- 業務麻痺

②企業ネットワーク障害

- システム稼働不可
- 社内ネットワークPC連結感染
- コンピューターシステム麻痺

③金銭被害

- 業務障害の間、金銭的被害が発生
- 復旧の見返りとして金銭要求

予防規則（１）

①すべてのソフトウェアは最新バージョンにアップデートして使用すること

✓ウィンドウズを最新バージョンにアップデートすると、ロッキー(Rocky)、ランサムウェアなどOS基盤のランサムウェアを防御することができます。

✓Windows 10 OS では、独自のスクリプト攻撃を防御する機能が搭載されており、ヘルメスなどのスクリプトランサムウェアを防御することができます。

②ウィルス対策ソフトウェア(ワクチン）を設置し、最新バージョンにアップデートすること

✓最新のアップデートバージョンは既存のランサムウェアを検出することができます。

✓世界共通のアップデートバージョンで特定国での攻撃に対応できます。

③出所が不明確なメールとＵＲＬリンクは実行しません。

✓相手のメールアドレスを類似に偽造･変造した攻撃に留意しなければなりません。

✓URLは、いつでもファイルを転送してアップロードできるので、もっと留意しなければなりません。

予防規則（２）

④ファイル共有サイトなどでファイルをダウンロードする時には注意する必要があります。

✓出所が不明なファイルには多数の悪性ファイルが存在しますので、必ず認証されたサイトのファイルのみをダウンロードすること。

✓不正ファイルのダウンロードは、社内PC全体に影響を及ぼす危険性があるため、十分に留意する必要があります。

⑤重要資料は定期的にバックアップすること。

✓ランサムウェアの主な行為は文書の暗号化なので、重要な文書は別途バックアップをして保護すること。

✓USBなどの外部機器も感染の道具になることがありますので、バックアップの後、必ず連結を解除して保管しなければなりません。

⑥ウェブサイトに接続する際、安全なサイトなのかもう一度確認しなければなりません。

✓サイトにログインおよび個人情報の入力を強要するようなサイトは十分な注意・確認をすること。

✓メッセンジャーなどで受信したウェブサイトはアクセスを止め、コンピューター関連のお知らせメールは必ず保安チームに報告すること。