2021 年度版　基本的なマルウェア紹介

目次

はじめに

この冊子「基本的なマルウェア紹介」を作るきっかけとなったのは、１年前初学時に、自分がマルウェアについて学習する際に、もっと分かりやすい軽めの資料は無いのかと思ったからです。
初学時(特にセキュリティーを勉強し始め)に、セキュリティーベンダー会社の公式サイトを見て、理解するのは大変です。

こちらの冊子では、全てのマルウェアについて説明すると膨大なページ数になってしまう為、代表的なマルウェアについて１０個紹介します。

新型コロナウイルスのため、図書館等で文献の収集ができないため、主に手元の本、セキュリティーベンターの公式 web サイトから情報をまとめています。

各ページに記載している対策につきましては、完全にマルウェアの感染を止めることが出来るわけではありません、安全性を高め、マルウェアの感染の抑制にはつながります。

また、2021 年度での代表的なマルウェア、特徴、感染方法、行うこと、対策を記載しております。

2021 年度以降、これらが更新される可能性があるからです。

また、提出期限が急遽変更になったことにより、掲載するマルウェアの数を半数にしました。

ご了承くださいませ。

No.1 「ワーム」

特徴:

2つの強力な特徴により強い拡散性を持つマルウェア

・自己増殖性
感染したコンピューター上で、自分の分身を作成できる
・単独性
何か(ソフトウェア、ファイル等)に寄生せずに、独立して行動できる

感染方法:

・ネットワーク
コンピューターがワームに感染すると、ランダムに IP アドレスを作り、その IP アドレスと合致するコンピュータにワームを送り込む

・メール
受信したメールにワームが添付され、それを開くことで感染し、さらに感染先のコンピュータ内のアドレス帳を探して、見つかったメールアドレスにワームを添付して大量にメール送信する

・共有フォルダ
感染したコンピューターがネットワークに接続されている共有フォルダにワームのコピーを置いて、同じネットワーク上の他のコンピューターに感染させる手口

・USB メモリ等の外部ドライブ(HDD 等)
ワームが侵入した USB メモリーをコンピューターに差し込むことで感染する

行うこと:

・コンピュータを止める

・情報を盗む
→金銭になる情報を盗むワームもいる

・別のマルウェアをダウンロードする

・メールの送信とメッセージの投稿
→中には SNS への投稿もある

対策:

・OS と使用するソフトウェアの更新を自動化し、常に最新バージョンにする

・不審なメールの添付ファイルを開かない

・ファイヤウォールを設置する
→ワームはネットワークを介し感染する

No.2 「ウイルス」

特徴:

以下の 3 つの特徴を1つ以上有する悪意のあるプログラム

・自己伝染機能
ネットワークやメディア(情報を記録する媒体を指す 例:CD など)を介して、
他のプログラムに自身(悪意のあるプログラム)をコピーし、それを利用してシステムを伝染する

・潜伏機能
ある程度時間が経ってから、感染を開始する

・発病機能
不正な処理を実行し、システムデータ破壊やシステム設計者の意図しない動作をする

感染方法:

・添付ファイル
電子メールなどの画像、オーディオ/ビデオファイルといった形式の添付ファイルを開くと、感染する

・インターネット
インターネットからソフトウェアなどをダウンロードし、そのまま確認せずに開くと、感染する

行うこと

・ウイルスが作動して負荷がかかり、勝手に PC の電源が落ちたり再起動してしまう

・セキュリティソフトが停止する

・重要なファイルを無意味な画像ファイルに変換する

対策:

・OS と使用するソフトウェアの更新を自動化する

・ウイルス対策ソフトを常に最新バージョンにする

・不審なメール・添付ファイルは開かない

・不審な USB メモリーなどを使用しない

・不審なソフトウェアをダウンロードしない

No.3 「トロイの木馬」

特徴:

悪意のないプログラムに見せかけるマルウェア

・偽装
ターゲットにとって悪意のないプログラムだと見せかける

・単独性
ソフトウェア、ファイル等に寄生せずに、独立して行動できる

感染方法:

・メールの添付ファイルや URL
添付ファイルを開くと感染したり、URL をクリックすると悪意のある Web サイトに誘導される

・Web サイト、SNS からのダウンロード
ウェブサイトの検索結果や SNS 上で拡散された URL をクリックし、ファイルをダウンロード・実行することで感染する

・ソフトウェアやアプリのダウンロード
有益なソフトウェアやアプリに偽装した、実行プログラムをインストールすることで感染する

行うこと:

トロイの木馬は様々なタイプがあり、ここでは分かりやすく代表的な4つのタイプを紹介する

1.バックドア型
ターゲットに気が付かれないようにポートを開き(ポートを開けておく→攻撃者の通信のドアを開けておく)、遠隔操作を実行。情報漏洩や、犯罪行為の実行役にされてしまう

2.ダウンローダ型
勝手に他のマルウェアをターゲットの PC にダウンロードさせる

3. クリッカー型
Web ブラウザの設定を勝手に変更したり、特定の場所を強制的にクリックさせ、悪意のある Web サイトに誘導し、マルウェアをダウンロードさせる

4. キーロガー型
ターゲットがよく使用する ID やパスワードのキーボード操作を記憶して、そのログを攻撃者に送信する

対策:

・OS と使用するソフトウェアの更新を自動化し、常に最新バージョンにする

・添付ファイルや URL は不用意に開かない

・ファイアウォールや IPS 等の入口対策
→トロイの木馬の感染の入り口の守りを堅める

・NGFW(次世代型ファイヤーウォール)で出口対策
→アプリケーションの挙動を監視する

No.4 「ランサムウェア」

特徴:

身代金を要求する不正プログラム

・身代金要求
コンピューターの制限を解く代わりに、金銭を要求する

・制限
感染したコンピューターに対して制限をかける

感染方法:

・メールの添付ファイルや URL
添付ファイルを開く、又は URL をクリックすると悪意のある Web サイトにを閲覧し、感染する

・Web サイト
攻撃者が改ざんした正規の Web サイトや不正広告から C&C サーバー(攻撃用サーバー)へ誘導させ、感染する

行うこと:

・データの暗号化
コンピューター内のデータを勝手に暗号化され、使用出来なくなる

・金銭要求
被害者がマルウェアの作者に身代金を支払うよう要求する

タイプによって分かれていて、特徴が異なる

ここでは代表的な2つのタイプを紹介する

・暗号化型
ファイルを開けないように暗号化する

・ロックスクリーン型
パソコンやスマホのスクリーン一面に Web サイトや画像を表示し、ロックする

対策:

・OS と使用するソフトウェアの更新を自動化する

・既存の脆弱性を認識する
→既存の脆弱性を再認識し、該当箇所にセキュリティパッチを適用する

・ファイアウォールや IPS 等の入口対策
→不正な通信をシャットダウンする

・バックアップを取る
→重要なデータが暗号化された時、復元できるようにする為

No.5 「ルートキット」

特徴:

システムに侵入した後に不正操作をする為のツールを統合したソフトウェア

・バックドア
ほかのマルウェアを侵入されるための通信の入り口を作る

・継続性
継続的にターゲットのシステムに侵入し、不正操作を試みる

感染方法:

・OS やアプリケーションの脆弱性
OS やアプリケーションの既知または未知の脆弱性を標的にし、エクスプロイトコード（悪意を持ったプログラム）を使ってシステムやデバイスの権限を取得し、感染する

・USB メモリー、CD-ROM などの物理メディア
物理メディアの内部にエクスプロイトコードが入っており、感染する

・メールの添付ファイル
ファイルの内部にエクスプロイトコードが入っており、感染する

行うこと:

ルートキットには不正操作を行うための多くのツールが含まれている。
その中でも代表的なツール 4 つを紹介する

・ログ改ざんツール
マルウェアの侵入を隠蔽し、マルウェアやルートキット自体の検知・駆除を遅らせる

・バックドア生成ツール
ターゲットを不安にさせるポップアップを表示し、金銭やクレジットカードの情報を要求する

・トラフィック監視ツール
ネットワークを介してやり取りされるデータを盗聴する

・キーロガーツール
キーボード入力を盗み見てログを記録し、キーボード入力から個人情報や機密情報を抽出し、他のコンピューターへ送信する

対策:

・OS と使用するソフトウェアの更新を自動化する

・添付ファイルや URL は不用意に開かない

・USB メモリなどの使用を制限する

・ルートキットスキャンの導入（ルートキットの検出に特化したツールを指す）

No.6 「ボットウイルス」

特徴:

コンピューターを乗っ取り、攻撃者に利用される

・乗っ取り
ボットウイルスに感染したコンピューターは攻撃者によって乗っ取られる

・直接的被害無し
コンピューターに直接的な被害を与えない
→ターゲットに気づかれにくい

感染方法:

・Web サイトにアクセス、ファイルをダウンロードする
ダウンロードしたファイルにより、感染する

・メール、SMS
受信したメール、SMS の不正なリンクを開き、リンク先の Web サイトで感染する

・非公式アプリマーケットからのアプリのダウンロード
非公式のアプリマーケットで公開されているアプリをダウンロードして感染する

行うこと:

・DDoS 攻撃に加担させられる
DDos 攻撃とは、ターゲットのサーバーに対して、多数のコンピューターから一斉にアクセスして、サーバーのサービスを停止させる攻撃

・仮想通貨の採掘に利用される
攻撃者はボットネット(ボットウイルスに感染したコンピューターをゾンビと呼び、そのゾンビがたくさん集まったネットワークをボットネットと呼ぶ)の強力なパワーを利用してビットコインなどの仮想通貨の採掘をする

・迷惑メールの送信元にされる
C&C サーバーからの指令により迷惑メールの送信元にされる

対策:

・OS と使用するソフトウェアの更新を自動化する

・セキュリティソフトを常に最新バージョンにする

・添付ファイルや URL は不用意に開かない

・ファイヤウォール導入

No.7 「スパイウェア」

特徴:

個人情報、機密情報を盗む

・情報収集
ユーザーに告知せずに個人情報を収集する

感染方法:

・フリーソフトウェアのダウンロード
フリーソフトウェアに付属し、インストール時に感染する

・ActiveX
ActiveX から感染する
→インタネット エクスプローラーの機能拡張を ActiveX と呼ぶ

行うこと:

・フリーソフト
フリーソフトの中にスパイウェアが仕込まれており、インストールすることで感染する

・偽の広告やポップアップ
ターゲットの不安を煽るような偽のメッセージが表示され、クリックしてしまうと感染する

・Web サイト
不審な Web サイトを閲覧することで、自動的に感染する

・メール
不審なメールの添付ファイルを開くことで感染する

・直接仕込まれる
攻撃者によって、コンピューターやスマホを直接操作され、感染する

対策:

・OS と使用するソフトウェアの更新を自動化する

・不審なソフトはインストールしない

・怪しいポップアップなどはクリックしない

・不審な Web サイトには接続しない

・不審なメールは開かない

・離席時の画面ロックを徹底する

No.8 「アドウェア」

特徴:

広告収入を目的としたスパイウェアの１種

・目的
広告の表示で、収入を得ることが目的であることが多い

・情報収集
ユーザーに告知せずに個人情報を収集する

感染方法:

・フリーソフトウェアのダウンロード
フリーソフトウェアに付属し、インストール時に感染する

・Web サイト
不審な Web サイトを閲覧しただけで感染する

行うこと:

・広告表示
不適切な内容の広告を表示する

・金銭要求
ターゲットを不安にさせるポップアップを表示し、金銭やクレジットカードの情報を要求する

・ホームページ(本来の意味の方)変更
ホームページを勝手に変える(この機能に特化したマルウェアを「ブラウザハイジャッカー」と呼ばれる)

・ブラウザーにツールバーを表示する
ツールバーで画面が見えにくく、閲覧時の視認性が悪化する
→ツールーバーを削除すると駆除できる

対策:

・OS と使用するソフトウェアの更新を自動化する

・セキュリティソフトを常に最新バージョンにする

・フリーソフトウェアのダウンロードを出来るだけしない
→挙動がおかしいソフトウェアをダウンロードした場合は速やかにアンインストールする

・アンチウイルスソフト
→アドウェア自体を駆除する

No.9 「ファイルレスマルウェア」

特徴:

メモリ内で悪質なコードを実行するマルウェア

・実行ファイル無し
従来のマルウェアは、メールの添付ファイル、Web サイト経由でダウンロードされ侵入する際に、実行ファイルとして PC のディスク上に保存されたが、ファイルレスマルウェアはメモリ上に保存される

・シグネチャパターンには引っかからない
マルウェア対策ソフトウェアが備えているシグネチャ（攻撃パターンを記録したファイル）との照合による防御が効かない。

・Windows の標準搭載のツール使用
PowerShell や Windows Management Instrumentation（WMI）が攻撃に使用されるケースが多い
→PowerShell とは、マイクロソフトが開発した拡張可能なコマンドラインインターフェイス シェルおよびスクリプト言語
Windows Management Instrumentation とは、システムの構成要素について情報収集と通知を行うオペレーティングシステム のインタフェースである

感染方法:

迷惑メール
メールに添付されたファイルをクリックすると、PowerShell などのコードが実行され、ターゲットコンピューターのディスク内にファイルを残さず PC 内のメモリに書き込むコードがダウンロードされる。

行うこと:

・情報を取得する

・情報改竄

・情報抜き取り

対策:

・EDR の導入

・不正なメールは開かない

No.10 「バンキングマルウェア」

特徴:

インターネットバンキングのユーザーを狙うマルウェア

・ユーザーID／パスワードの窃取
ターゲットの インターネットバンキングのユーザーID／パスワードを盗む

・不正送金
ターゲットのインターネットバンキングの口座から攻撃者の口座へ

感染方法:

・メール
ターゲットによって魅了的な内容のメールを送り、添付されているリンク、ファイルを開く感染する

・Web サイト
金融機関のページを不正に改ざんして、ターゲットを誘導し、感染する

行うこと:

・遠隔操作
攻撃者サーバーによって遠隔操作される

・不正送金
ターゲットが知らない間に ID／パスワードの窃取し、インターネットバンキングの口座から多額の預金が不正送金させる

対策:

・OS と使用するソフトウェアの更新を自動化し、常に最新バージョンにする

・不正な引き出しがないか、インターネットバンキングの口座を小まめに確認する

・既存の脆弱性を認識する
→既存の脆弱性を再認識し、該当箇所にセキュリティパッチを適用する

・ファイヤウォール導入
→怪しい通信をシャットダウンする

まとめ

実際に調査してみると、今までマルウェアだと思っていたものが厳密には攻撃の一種でした。

また、この冊子を作成する前までの私はマルウェアの機能しか理解しておらず、具体的な対策を理解しておりませんでした。

この冊子で紹介したマルウェアはあくまでも原素的なマルウェアであり、世の中にはより細分化されたマルウェアが多く存在します。

今回は、10種類しか掲載することができませんでしたが、自らより多くのマルウェアについて深く知りたいと思いました。

引用・参考サイト

マカフィー株式会社 ”McAfee Blog” https://blogs.mcafee.jp/(参照:2021/02/02)

カスペルスキー株式会社 ”脅威に関する最新情報” https://www.kaspersky.co.jp/resource-center/threats(参照:2021/02/02)

ノートン株式会社 ”ウイルスについて” https://japan.norton.com/category/antivirus(参照:2021/02/02)

神奈川県警察 ”コンピュータウイルス対策について” https://www.police.pref.kanagawa.jp/mes/mesd7013.html(参照:2021/02/02)

日本ネットワークセキュリティ協会 ”マルウェア とは” https://www.jnsa.org/ikusei/03/08-01.html(参照:2021/02/02)