サイバーセキュリティ通信 vol.4

平成29年６月
【長崎県サイバーセキュリティに関する相互協力協定機関】

パソコンやスマートフォンを狙った不正プログラムにご注意を！

○　アンドロイド標的のランサムウェアが急増

新聞報道によると、５月３１日、大手セキュリティベンダーから、「 アンドロイドを搭載したスマートフォンやタブレット端末を狙うランサムウェアが急増し、１～３月に前年同期の５．６倍に当たる約１２万３１００種類が世界中で新たに確認された」との調査結果が発表されました。

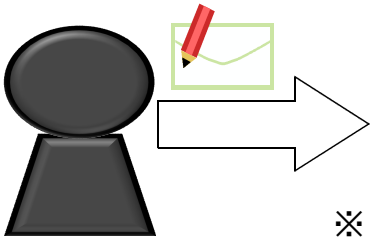
ランサムウェアは、現在、パソコン上で猛威を振るっていますが、ゲームやアダルト動画再生等のアプリを装ってダウンロードさせ、ＦＢＩ等の捜査機関を騙り「法律に違反している」といった警告文が出るものや、日本語で脅迫する種類もあるということで、上記大手セキュリティベンダーが、「 対象がスマートフォンにも広がっている」と警鐘を鳴らしています。

○　「あなたの名前で不審なメールが届いたので確認を」と不安あおるウイルスメール

新聞報道によると、５月２９日、ウイルスが仕込まれたメールを特定の組織や人に送りつける「標的型」サイバー攻撃の手口が巧妙になっているとのことです。

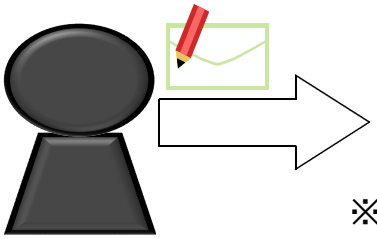
ネットセキュリティ会社によると、平成２８年後半から、「 あなたの名前で不審なメールが届いたので、確認をお願いします」と求めて、メールを開封させる手口が登場しており、専門家は「確実な感染を狙っている」と警戒を呼びかけています。

【 攻撃者側が標的にした人物に送ったメールの例】



「なりすましの偽メールの可能性もあるかと思い、確認させてください。本当に送っていたらすみません」

※　偽メールかどうかの確認と称して、「自分や自分の組織がなりすまされたかも」、「中身を見てあげないと相手が困る」等と被害者側の不安を煽って添付ファイルを開かせます。開封すると、ウイルスに感染してしまいます。



「こんにちは、先生。前回の学会でお目にかかった〇〇と申します」

※　送り主は、別の大学の人物を名乗り、自分の研究分野についての意見を求め、「詳細な質問を添付いたします」とファイルを添付しており、このファイルには遠隔操作ウイルスが仕込まれていました。

かつてのウイルスメールの文面は、不自然な日本語が使われるケースもありましたが、最近は状況設定に現実味が増し、言葉遣いが自然になっているといいます。大手セキュリティ会社は、

○　怪しいと思うきっかけを持つことが重要。
○　ファイルを受け取らないようにパソコンを設定するだけでも被害は大きく減る。

と助言しています。

○　「駐禁報告書」を称するスパムメールが拡散

大手セキュリティ会社は、５月１９日、主に「駐禁報告書」の件名で拡散されているスパムメールについて、銀行やクレジットカードの情報を狙うマルウェアスパムとして注意喚起していると発表しました。同社は、５月１４日から１８日までの約５日間で、４３万３千件のスパムを確認したとのことです。旅行会社を騙るものや郵便局の配達状況を称するものなど、様々なバリエーションがありますが、いずれも同じ不正なＵＲＬへ誘導するもので、スパムメールの件名は、「駐禁報告書 」が全体の約５０％と最多。早朝５～６時の拡散量が多く、ネット利用者の出勤前をねらうところに何らかの意図があるとみられています。

スパムメールに仕込まれているのは、「ＵＲＳＮＩＦ 」という不正プログラムで、従来はインターネットバンキングのアカウント情報をねらうツールでしたが、現在はクレジットカード利用者向けオンラインサービスのアカウント情報を盗みとる機能が追加されているとのことです。また、一部のメールソフトでは、スパムメールのフィルターをかいくぐって受信トレイに届いており、むやみに開かないようにする等の注意が必要です。

○　１１歳の少年がテディベアでサイバー攻撃

５月１８日、海外の新聞が、１１歳の少年がネット接続できるテディベアのおもちゃを操作するためにブルートゥース機器へのハッキングを実演して、セキュリティ専門家らを驚かせ、相互接続されたスマート玩具を「武器化できる」ことを示したと報じました。

この少年は、アメリカテキサス州の小学６年生で、５月１６日、オランダ・ハーグで開催されたサイバーセキュリティの世界フォーラムで実演し、数百人の聴衆を驚嘆させ、「 飛行機から自動車、スマートフォンからスマートホームまで、どんなものでも、あるいはどんな玩具でも、『モノのインターネット（ＩｏＴ）』の一部となる」と壇上から語り、「 ターミネーターからテディベアまで、どんなものでも、どんなおもちゃも武器化されるおそれがある」ことを付け加えました。

今回の実演のために用意されたテディベアは、Ｗｉｆｉとブルートゥースを通してクラウドサービス「ｉＣｌｏｕｄ」に接続し、メッセージを送受信することができるものでした。少年は、実演で利用するブルートゥース機器を探すために、クレジットカード大の小型コンピューター「 ラズベリー・パイ（ＲａｓｐｂｅｒｒｙＰｉ）」を使い会場内をスキャンすると彼自身も含めて誰もが驚いたことに、一部高官のものを含む数十の番号がすぐに見つかりました。

次に、Ｐｙｔｈｏｎ（パイソン）と呼ばれるプログラミング言語を使い、見つかった番号の一つを経由して壇上のテディベアを操作し、ぬいぐるみに付いているライトを点灯させたり、聴衆からのメッセージを録音したりしてみせました。少年は、その後に行われた取材に「インターネットに接続されるものの大半には、ブルートゥース機能が備わっている。今回の実演では、音声を録音したりライトをつけたりすることによって、どのようにしてブルートゥース機器に接続し、それにコマンドを送信できるかを示した」と語り、「 ＩｏＴ家電など日常生活で使用できるもの、自家用車、照明、冷蔵庫など接続機能を持つこの種のあらゆるものは、人々に対してスパイをしたり害を及ぼしたりするために悪用され、武器化される可能性がある」と注意を促しています。

本情報は、長崎県サイバーセキュリティに関する相互協力協定に基づき提供しています。
提供できる情報があれば、警察本部サイバーセキュリティ戦略室までご連絡ください。

長崎県警察本部　☎　０９５－８２０－０１１０（２６６１・２６６２・２６６３）
ﾒｰﾙｱﾄﾞﾚｽ　１０３１０７@police.pref.nagasaki.jp