サイバーセキュリティ通信 Vol.3

平成30年９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】

平成30年８月中のサイバー空間における脅威ニュース

（ニュースの内容は、各種報道、インターネット等で公表されている情報に基づくものです。）

○　日本人を狙う不正な仮想通貨マイニングが１か月で最大310万件超

報道によると、日本人を標的とした仮想通貨マイニングマルウェアを用いた攻撃の数が仮想通貨の価格と連動して推移する傾向にあることが分かりました。仮想通貨の価格が高い時は、サイバー犯罪者も仮想通貨マイニングを積極的に行い、価格が低いときはそのような攻撃も少なくなっているそうです。

2017年12月に、仮想通貨の価格が史上最高値を記録したと同時に、日本人ユーザを標的とした仮想通貨マイニングマルウェアを用いた攻撃の数も急上昇し、攻撃数は310万件を上回りました。しかし、2018年に仮想通貨の価格が下落した際には、攻撃数も同様に下落し、６月には50万件強まで落ち込みました。

ブラウザベースのマイニングマルウェアは、マイニング・スクリプトを通じてWebサイトのコード内に実装されます。Webサイトを訪問すると、スクリプトは訪問者の演算能力を悪用する形で仮想通貨マイニングを開始し、その結果、被害者の電気代の高騰やデバイスのパフォーマンス低下、生産性の損失が発生するほか、PCやスマートフォン等の製品寿命に悪影響がもたらされます。この攻撃は、ブラウザベースで実行されるため、ブラウザを実行できるデバイスであれば、感染の可能性があります。

○　拡張子“.ipy”の添付ファイルを日本語マルウェアスパムで初確認

セキュリティ企業のブログによると、日本語のスパムメールで拡張子“.ipy”のファイルの添付を初めて確認したとして、その実例を紹介し注意喚起しました。この拡張子の添付ファイルによる攻撃は、海外では本年５月下旬以降に見られていましたが、日本語マルウェアスパムとしては、初確認だそうです。

「お世話になります」や「ご確認ください」等の件名が確認されており、確認すべき書類の送付を偽装して、受信者にファイルを開かせようとする内容の本文は、マルウェア拡散を目的とする常套手段となっています。添付ファイルとしては、例えば、「８月・428680.ipy」など、「○月」プラス「数字列」に加え、「受信者名」プラス「数字列」という例が確認されており、いずれのファイル名であっても内容は同じものです。

同社の統計では、日本国内での同一ファイルを添付したメールを、８月６日の１日のみで29万件以上確認しているそうです。この様なメールは、数時間のうちに大量送信された後に止むことが多く、今回確認したメールの送信も８月６日の夜には終了しましたが、数日間のインターバルを挟んで繰り返す場合もあるようです。

そもそも、この“.ipy”という拡張子のファイルは、WindowsではWebサイトからデータを取り込むためのファイルとしてMicrosoft Excelに関連づけられており、ファイルを開くとExcelが起動して処理が行われます。攻撃者は、この仕組みを利用し、不正スクリプトファイルをダウンロードさせて、最終的にオンライン銀行詐欺ツールである「URSNIF（アースニフ）」を感染させます。

同社の解析によると、不正な“.ipy”ファイルを開いた場合、Excelのセキュリティ機

能により、実行を確認するメッセージが２回にわたって表示されるといい、確認メッセージで「無効にする」又は「いいえ」を選択することにより、最終的なマルウェアの侵入を防ぐことができるそうです。

Excelの「セキュリティセンター」から「ファイル制限機能の設定」で、意図しない“.ipy”ファイルの機能実行を防止することもできますし、法人組織では、“.ipy”のファイルのメール受信を制限する対策も有効です。

○　Wi-Fiパスワードを破る新たな攻撃手法

報道によると８月９日、セキュリティプロトコルの「WPA」及び「WPA2」を無効にする新たな攻撃手法が、新しい「WPA3」規格を調査中の研究者によって偶然発見されたと報じれらました。この攻撃手法を利用すれば、WPA/WPA2で守られたルータに侵入し、Wi-Fiパスワードを破ることができるそうです。

WPA3は、最新バージョンのWi-Fi規格で、公共スペースや飲食店等によくあるオープンWi-Fiネットワークやアクセスポイントを中心に、ユーザ保護の強化を目指すもので、ネットワーク上の各機器とルータ間の接続を個別に暗号化するデータ暗号化手法を採用するほか、パスワードを破ろうとする総当たり攻撃に対する新たな防護機能も備えていますが、古いWPA2規格には、こうした防護機能がありません。

これまで最も多く利用されていた攻撃手法は、ユーザがWi-Fiに接続して４ウェイハンドシェイクの認証プロセスが実行されるのを待ち、使用されているパスワードに総当たり攻撃するためにその情報を盗み取るというものでしたが、新たな攻撃手法は、単一のEAPOLフレームを使用するRobust Security Network Info-rmation Element (RSN IE)上で、一般ユーザの介在なしで実行されるそうです。

攻撃に成功すると、攻撃者は、ログインパスワードの取得、通信の傍受、中間者攻撃が可能となります。なお、この攻撃手法は、WPA3に対しては機能しません。

総務省は、調査結果を受けて、今夏をめどに安全対策の手引きを改定し、利用者や施設が実施すべき対策を明確にするほか、安全なWi-Fiをスマホで選べるアプリの開発も後押しするそうです。

○　企業の４割が詐欺メールの受信を経験

セキュリティ企業の調査によると、８月15日、ビジネスメール詐欺について、企業のIT部門や経理部門の責任者の39％が、この種のメールを受信した経験があることが分かりました。

調査は、今年６月、計1,030人を対象に行い、39％に当たる406人が詐欺メールの受信経験があると答えました。内容は、「振込先の口座が変わった」「至急対応案件」などで、このうち５％に当たる22人が、実際に送金の手続をしたといい、金融機関が送金を止めるなどして被害を防いだものもありますが、５億円以上を送金したケースもあったそうです。

従業員規模別では、詐欺メールの受信経験があるうち、5,000人以上の企業の比率が48％と高かった一方で、49人以下の企業も28％あり、調査したセキュリティ企業は、「中小企業も標的になっている」としています。金銭だけでなく、勤務先の幹部の個人情報や非公開の決算、新製品等に関する情報の送付を求めるメールについても、209人が受信したと答えました。

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情報提供しています。
提供すべき情報があれば、警察本部サイバーセキュリティ戦略室まで御連絡ください。
長崎県警察本部　☎　095-820-0110（2661・2662・2663）
ﾒｰﾙｱﾄﾞﾚｽ e103107@police.pref.nagasaki.jp

サイバァちゃん