サイバーセキュリティ通信 Vol.4

平成30年11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】


サイバァちゃん

平成30年10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。）

○　日本気象協会を装った迷惑メールが拡散中、ウイルスに感染するおそれ

日本気象協会は、10月５日、同協会や同協会の天気予報専門メディア「tenki.jp」を装った迷惑メールが確認されたとして、注意喚起した。

同協会は、tenki.jp等のサービスを利用する個人の電子メールアドレスを保有しておらず、同協会から特定・不特定の個人に対するメールによる案内を行っていない。

迷惑メールは、同協会やtenki.jpから発信されているように装って、「台風は最悪のコースへ。今後の動向にご注意ください。」や、「この先24時間でお住まいの地域が冠水する危険性があります。ご注意ください。」といった説明とともに、詳細情報を装ったURLが貼られていたり、添付ファイルがついていたりするという。

同協会は、緊急の気象変化に関するメールや心当たりのないアドレス、見知らぬアカウントで投稿された災害通知を装ったSNSの投稿等について、記載されたリンク先アドレスを絶対にクリックしないことやメールを削除することなどを呼びかけている。

○　５か国のセキュリティ機関がサイバー犯罪に利用される公開ツールに関して注意喚起

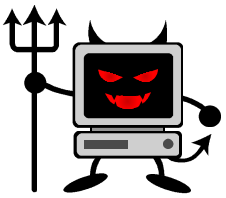
ネットニュースによると、10月12日、米国のセキュリティ機関が、オーストラリアやカナダ等４か国と合同で、世界のサイバー攻撃に利用されることの多いツールについて解説した報告書を発表し、広く流通している５種類のツールにスポットを当てて、それぞれの機能や対策等を紹介して警戒を促したと報じた。

報告書で取り上げられたのは、リモートアクセス型トロイの木馬（RAT）の「JBiFrost」、WebShellの「China Chopper」、ログイン情報を盗み出すツール「Mimikatz」、階層移動フレームワーク「PowerShell Empire」、C2難読化ツール「HUC Packet Transmitter」の５種類。

それぞれのツールについて、機能や手口、過去の攻撃に使われた実例等を紹介し、検出や防御の手掛かりとなる情報を共有している。

こうしたツールは、医療や金融、政府機関等を含む幅広い業界から情報を盗み出す目的で使われているといい、国家や犯罪集団のほか、侵入テスターやサイバー犯罪者等、誰もが自由に利用できる状態にあると解説している。ただし、報告書では、取り上げられたツールが、攻撃者が利用するツールの一部に過ぎず、ネットワークの防御を計画するに当たり、これが全てだと思ってはいけないとも指摘している。

○　カード利用者を狙うウイルス「パンダバンカー」



新聞報道によると、10月14日、国内のクレジットカード会社の利用者のPCに、今年７～８月「パンダバンカー」と呼ばれる情報窃取型のウイルスを感染させることを狙ったメールがばらまかれたとみられると報じた。報道時点では被害は確認されていないという。

東京の情報セキュリティ会社によると、パンダバンカーは、２年前に登場し、欧米を中心にオンラインバンキング攻撃等に使われてきたが、同社の調査で、今夏、日本の11のクレジットカード会社も標的になったことが判明したという。

このウイルスは、請求書等の送付を装ったメール経由でパソコンに送り込まれた別のウイルスが、外部のサーバと通信することで感染する。インターネットの閲覧サイトが細工され、標的企業のサイトへの接続を検知すると、正規サイト上に、カード情報の再登録等を求める偽画面が表示され、入力した内容が盗まれてしまうという。

東京の情報セキュリティ会社は、「ブラウザが細工されるため、サイト側で対策が取れず、ユーザも気付きにくい。被害を防ぐには、メールの添付ファイルを安易に開かず、カード番号等の再入力を求められたら、別の端末で接続してみるなど慎重な対応が必要」と話しているという。

○　世界の銀行を狙う北朝鮮のハッキング集団「APT38」

ネットニュースによると、10月４日、米国のセキュリティ企業が、北朝鮮政府が関与する集団が世界中の銀行から多額の現金を盗み出している手口等を解説した調査報告書を公表したことを報じた。

北朝鮮政府を後ろ盾とするハッキング集団としては、これまで「Lazarus」等の集団について調査が進められているが、米国のセキュリティ企業は今回の集団は動機や手口等が明らかに他の集団と異なるとし、この集団を「APT38」と名付けたという。ただし、攻撃に使用するマルウェアには重複する部分や共通する部分があることから、同じ開発者の関与等をうかがわせるとしている。

米国のセキュリティ企業によると、APT38は、標的とする組織について詳しく調べ上げた上で、ApacheStruts2の古いバージョンのぜい弱性をつくなどの手口で、システム上でコードを実行し、国際銀行間金融通信協会の取引に使われるサーバにマルウェアを仕込んで、他行の口座に現金を不正送金していたという。

APT38は、2014年以降、少なくとも11か国で16以上の組織を標的とし、巧妙な手口を使って被害者のネットワークに侵入して、平均で155日間潜伏したという。判明している事件だけでも、11億ドルを金融機関から盗もうとしたことが分かっているという。

米国のセキュリティ企業は、「APT38は今も活動を続け、世界の金融機関にとって危険な存在であり続けている」と指摘し、被害額は少なくとも１億ドルに上ると推定しているという。

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