



平成30年11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。)

○ 正規ソフトを利用したサイバー攻撃

新聞報道によると、11月9日、米セキュリティ企業が、PCの動画再生ソフトの更新やインストールをもちかけて、利用者が応じると正規ソフトの更新等を実際に行いながら、別の不正なソフトを入り込ませる新手のサイバー攻撃を発見したと報じた。不正の隠れみものとして、正規ソフトのインストールを行う手口が確認されたのは初めてだという。



新たに発見された手口は、攻撃相手のPCに、仮想通貨のマイニングを実行するソフトを入り込ませ、PCの所有者が知らない間にその計算処理能力を使わせることを目的としているという。こうした攻撃は今年3月ころから米国や台湾など海外で約1,000件確認されているといい、日本に来るのも時間の問題だという。

ただ、マイニングのためのソフトの代わりに、より悪質なコンピュータウイルスを忍び込ませることも技術的に難しくない。サイバーセキュリティに詳しい国立大学の教授は、「現在は『マイニングは稼げる』というブームになっている。稼げるなら続けるだろう。そうでないとなれば、今度は別のウイルスを侵入させてくる可能性がある」と注意を促しているという。

なお、代表的な仮想通貨であるビットコインの価格について、新聞報道等によると、11月29日、昨年12月のピーク時の5分の1以下まで急落したと報じた。ビットコインから派生したビットコインキャッシュが分裂したことを主因に、規制強化への懸念なども下落を後押ししたという。

今年11月の1ビットコイン4,000ドルを割った水準では、増大するマイニングにかかるコストを賄えず、マイニングを続けるほど赤字が膨らむ構図に陥っているという。

○ 「アダルトサイトを閲覧している姿を録画」詐欺被害拡大

新聞報道によると、11月26日、10月中に国内で「アダルトサイトを閲覧している姿を録画した」などとメールを送りつけて仮想通貨をだまし取る詐欺で、約1,000万円相当の被害が発生したと報じた。利用者が過去に使っていたパスワードをメールの件名にするなどして動揺させる手口が被害拡大につながっていると見られるという。



メールは、「パソコンに内蔵されたカメラでアダルトサイトを閲覧している姿を撮影した。家族や同僚らにばらまく」などと脅す内容で、今年9月19日に国内で初めて確認され、同月末までに、少なくとも250万円相当が攻撃者の仮想通貨口座に払い込まれたとみられる。

調査を行っているセキュリティ企業によると、10月に入っても同様のメールが12回にわたって約5万2,000通送信されたといい、9月末までの被害分を含めて、10月末までに少なくとも約1,240万円相当の仮想通貨が指定の口座に払い込まれたのが確認されたという。

○ 経産省が中小企業のサイバー攻撃対策を強化する方針

新聞報道によると、11月5日、経済産業省が、2019年度からIT企業等と協力し、中小企業がサイバー攻撃を受けた際の相談窓口の設置や外部の専門家チームがすぐに対応できる体制を整備し、中小企業のサイバー攻撃対策を強化する方針を固めたと報じた。



相談窓口は、IT企業やサイバー保険を販売する損害保険会社に設け、サイバー攻撃を受けたと疑われる中小企業からの連絡や相談を受け付ける。

専門家による調査や復旧が必要と判断すれば、新たに設置される「サイバーセキュリティお助け隊」の派遣を要請する。お助け隊には、普段は他の仕事に従事するシステムエンジニア等を非常勤として登録するという。

経産省は、2019年度から2年間、相談窓口の運営費やお助け隊の報酬等を補助するという。中小企業が集中しており、サイバー攻撃を受けると部品供給に大きな影響が出やすい国内5か所程度で行う方針だといい、大阪府や愛知県の一部地域などが対象となる見込み。

○ サイバー防衛で日本とASEANが情報共有

新聞報道によると、11月11日、日本と東南アジア諸国連合(ASEAN) 10か国が、サイバー攻撃に関する情報を共有する連絡体制を立ち上げたと報じた。専用サイトを使って巧妙化する攻撃の手口や有効な対処法を11か国が速やかに共有できるようにするといい、日本が外国のサイバー防衛当局と専用サイトで情報共有する枠組みをつくったのは初めてだという。



ASEAN域内国には、セキュリティ対策が不十分なサーバが多く、悪用されるリスクが高い。2017年に猛威をふるった「ワナクライ」等の強力なウイルスを使った攻撃を受ければ、域内で被害が一気に広がるおそれもある。また、域内の外交交渉の記録や軍事的な動きが漏えいする可能性もある。

専用サイトは、各国のサイバー防衛当局の担当者が利用でき、外部から接続できないよう厳重管理されるという。例えば、ASEAN加盟国の1つが他国のサイバー部隊から攻撃を受けて情報漏えい等がおきた場合、その手口や被害の状況をサイトを通じて日本や他の加盟国に周知し、情報を得た国は類似する被害があれば報告したり、攻撃の特徴を踏まえた有効な対処策があれば加盟国に助言したりするという。

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)

メールアドレス e103107@police.pref.nagasaki.jp



サイバアちゃん