2022/04/15

セキュリティトピックス03

重要なインフラが常に運用できるように🥺 (2022/04/14)

ZDNet Japanの「狙われる重要インフラ、欧州などで活発な10の脅威グループ」という記事を読みました。ありがとうございます。😊この記事では、サイバーセキュリティ企業であるDragosが発表したレポートをもとに、電力、石油、ガスなどの生活に欠かせない重要なインフラが、サイバー攻撃のリスクに晒されていることの説明、また10のサイバー攻撃グループの紹介をしております。以下はこの記事の引用です:

> このリストには、**ロシア軍との関連が指摘されている Electrum（別名Sandworm）**や、北朝鮮のLazarus GroupとつながりがあるとみられるCovellite、中国政府の指示を受けているAPT41と連携している可能性のあるVanadiniteなどの、国家の指示を受けているハッキンググループもいくつか含まれている。

> 重要インフラがインターネットに接続されていたり、スタッフがリモートデスクトッププロトコルやVPNを介してアクセス可能であったりするケースが増えていることから、国家の指示を受けたグループや、将来攻撃を行うための下準備としてOTネットワークへの侵入と調査を行っているサイバー犯罪グループの標的となることが増えている。

記事にある用語:
運用技術（OT）

> **産業用ネットワークに侵入したハッカーが、ただちに運用プロセスを制御しているシステムに手を出す可能性は低い。これは、攻撃者がすべてを理解するためには何年もかかる場合があり、将来のために足場を固めることを優先するためだ。**

> Dragosが追跡しているサイバー攻撃グループの目的は、グループによってさまざまだ。情報を盗むことを目的としているグループもあれば、ランサムウェア攻撃を仕掛けようとするサイバー犯罪グループなどの、混乱を引き起こすことを目的としたグループもある。**産業用ネットワークには、運用技術の性質上、そして古いソフトウェアやプロトコルに大きく依存している関係上、セキュリティ侵害の兆候が見逃され、ハッカーに内部で動き回り、ネットワークを理解してコントロールを獲得するまでの十分な時間を与えてしまう可能性がある。**

> 研究者らは、この問題は産業用ネットワークが抱えている「サイバーセキュリティ上の最大の弱点」だと述べている。これは、**全体像を把握してサイバー攻撃から何を守るべきかを理解しない限り、ネットワークを完全に守ることは不可能だからだ。**

> また同レポートでは、ロシアのウクライナ侵攻以降に産業インフラを標的としたサイバー攻撃に関する活動が観測されており、西側のサイバーセキュリティ関連機関がネットワークを攻撃から保護する必要があると警告を発していると注意喚起している。

> ネットワーク上に何があるかを十分に把握することは当然として、OTネットワークの安全性を確保するためにも有効

> な一般的なサイバーセキュリティ対策は多い。これには例えば、**セキュリティアップデートを適用してソフトウェアの既知の脆弱性を修正することや、可能な限り多要素認証を使用することなどが含まれる。**

私たちは使用している重要なインフラについて考えていかなくてはならないと思いました。🥺重要なインフラが常に運用できるように、もちろん企業にセキュリティを強化してもらうだけでなく、それが、使えなくなった時のことも考える必要があると思います。最終的には私たちが困ることになります。🥺

Electrum（別名Sandworm）についての情報を追加していこうと思います。😃以下はこの記事の引用です：

> Electrum：このグループは、OTの運用手続きを変更してコントロールすることができるマルウェアの開発能力を持っている。Dragosの研究者らによれば、Electrumは2016年12月にウクライナの電力網に対する攻撃に使用された「CrashOverride」（別名「**Industroyer**」）と呼ばれるマルウェア攻撃に関与したという。Electrumには、ロシア軍の諜報機関であるロシア軍参謀本部情報総局（GRU）に所属する攻撃的なハッキンググループである、Sandwormとの結びつきがあると考えられている。

Catalin Cimpanuのリツイートのおかげで、ウクライナ特別通信情報保護国家サービス（SSSCIP Ukraine）のツイートについて知ることができました。ありがとうございます。😊最近、ウクライナの変電所に対して**Industroyer2**マルウェアが使われたという情報が書かれております。インターネットセキュリティ企業のESETの調査でIndustroyer2マ

ルウェアは上の記事で説明がありましたIndustroyerマルウェアの新たなバージョンだとしています。以下はこのツイートの引用です：

> #Industroyer2と#CaddyWiperマルウェアを訴えるウクライナのエネルギーインフラに対する#Sandworm(UAC-0082)#cyberattackを@_CERT_UAの下で@Dsszziが報告した。

> 攻撃者は、ターゲットのいくつかのインフラストラクチャコンポーネント、つまり次のものを取り壊そうとしました: (1/5)

> **変電所 - #Industroyer2マルウェアを使用。**すべての実行可能ファイルには、ターゲット変電所の1つに対して静的に設定された一意のパラメータセットが含まれていました。
> (2/5)

> Windowsが運営するコンピューティングシステム(ユーザーコンピュータ、サーバー、APCSワークステーション) - #CaddyWiper破壊データワイパーを使用。
> Linuxが運営するサーバー機器 - 悪意のあるデストラクタスクリプトを使用。
> アクティブネットワーク機器 (3/5)

> 報告されたように、ターゲット組織は2つの攻撃波に苦しんだ。最初の攻撃は遅くとも2022年2月までに起こった。そして4月8日金曜日の夜、攻撃者は変電所を閉鎖し、企業のインフラを破壊することを計画した(4/5)

> しかし、この悪意の目的は防げています。

> 他のウクライナの組織に同様の脅威があるかどうかを判断

> するために、悪意のあるソフトウェアサンプルを含む情報は、国際的なパートナーや#ウクライナのエネルギーセクター企業と共有されています(5/5)

ウクライナ政府のコンピュータ緊急対応チーム(CERT-UA)とESETがうまく対応できたのがすごいです。👏日本の変電所も大丈夫でしょうか? 🥺

また、Catalin CimpanuのリツイートとDr. Dan Lomasのツイートのおかげで、ロシアのサイバーオペレーションと諜報機関に関するの英国政府の調査分析を知ることができました。ありがとうございます。😊以下はこの調査分析の引用です:

> **世界的に重要な国家インフラに対するサイバー作戦**
> FSBセンター16番は、国が機能し、日常生活が依存する世界中の国々で不正アクセスシステムを獲得しています。センター16番は、重要な国家インフラとして知られるエネルギー、医療、金融、教育、地方自治体/国家政府に不可欠なシステムをターゲットにしてきました。これは長年にわたり、ヨーロッパ、南北アメリカ、アジアの幅広い国で協調的なキャンペーンです。

> NCSCとサイバーセキュリティ企業は、この活動パターンによってもたらされるリスクについて、ネットワークディフェンダーに何度も警告してきました。FSBの関与の憶測がありましたが、英国政府は、この活動がFSBセンター16番によって行われたことを確認し、脅威に関する意識と透明性を高めるために、この活動の具体的な例の詳細を提供しています。

この調査分析には、その後、ロシアのサイバーオペレー

ションの事例が紹介されています。😀

また、Wired UKのポッドキャストの最新エピソードに、ウクライナの地下鉄の駅が爆弾シェルターとして機能していることも知ることができました。ありがとうございます。😊それに関する動画が「Ukraine Civilians Use Subway Station As Bomb Shelter Amid Russian Invasion」でありました。ありがとうございます。😊

このエピソードでも紹介されていましたが、Arsenalnaという駅が世界一深い地下鉄駅というのは初めて知りました。😳😳

また「The Deepest Metro Stations in The World」という記事も読んでいました。ありがとうございます。😊以下はこの記事の引用です：

> アルセナルナ駅は地表から下105.5メートルに位置し、世界で最も深い地下鉄駅です。地球上で垂直シャフトを深く作った場合、自由の女神像全体をその中に落とし、他のものを落とすための12メートル以上の空間が残っている可能性があります。この駅で地下鉄に乗るには、通勤者は終わりのない2つのエスカレーターを一番下まで連れて行かなければならない。旅には最大5分かかります。

画像：アルセナルナ駅のエスカレーター　ウクライナのwikiページから

Keywords: 重要インフラ, Dragos, Electrum, Industroyer, Industroyer2, ウクライナ政府のコンピュータ緊急対応チーム, ESET, FSBセンター16番, 爆弾シェルター, アルセナルナ駅

管理者権限はある意味怖い🥺(2022/03/28)

ポッドキャストWired UKの最新エピソードを聴いていました。一つの話として、米国の通信会社Viasatがロシアのウクライナへの侵略が始まった時に衛星インターネット接続障害を起こしたという話がありました。ありがとうございます。😊また、以前にMatthew GreenのリツイートでRuna Sandvikのツイートからもその話は知ることができました。ありがとうございます。😊そのツイートにロイター記事の紹介がありました。以下はこの記事の引用です：

> 影響を受けるネットワークを所有する米国の通信会社Viasatの関係者によると、結果はまだ調査中ですが、ヨーロッパの数万人の顧客に属する衛星モデムがオフラインにされました。

> ハッカーは、ウクライナを含むヨーロッパの一部の顧客にインターネットアクセスを提供するViasat IncのKA-SAT衛星と通信するモデムを無効にしました。2週間以上経っても、一部はオフラインのままである、と再販業者はロイターに語った。

> ロイターがレビューした政府契約は、KA-SATがウクライナの軍事および警察部隊にインターネット接続を提供していることを示しています。

> 米国特殊作戦司令部(SOCOM)の元技術者であるパブロ・ブロイヤーは、衛星インターネット接続をノックアウトすると、ウクライナのロシア軍と戦う能力がハンディキャップされる可能性があると述べた。

> Viasat当局者は、衛星ネットワークの「管理セクション」の設定ミスにより、ハッカーがモデムにリモートアクセスできるようにし、オフラインにしたと述べた。彼は、影響を受けるデバイスのほとんどは、現場の技術者または修理デポで再プログラムする必要があり、一部を交換する必要があると述べた。

Wired UKの話によると、この影響はウクライナ国内ではなく１ヶ月たった今でも、フランス、ドイツ、イギリス、ポーランド、モロッコでもモデム障害が起きている模様です。ネットワークを管理する「管理セクション」の設定ミスを防がないと、場合によっては甚大な被害が起こるということがわかりました。🧐

Keywords: 衛星インターネット接続, モデム, KA-SAT, 衛星, ハッカー, ロシア, ウクライナ