報道関係者各位

エフセキュア、サイバー脅威を取り巻く環境に関する 2020 年の総括および 2021 年の予測を発表

～ IoT デバイスやリモートワークにおける脆弱性を悪用するサイバー攻撃が増加へ ～

2020 年 12 月 15 日
エフセキュア株式会社

先進的サイバー・セキュリティ・テクノロジーのプロバイダーである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、エフセキュア) は、同社のセキュリティエキスパートによるサイバー脅威を取り巻く環境に関する 2020 年の総括と 2021 年の予測についてのコメントを発表しました。

1. IoT デバイスへの攻撃は更に増加

Tom Van de Wiele (トム・ヴァン・デ・ヴィーレ)
F-Secure Consulting　プリンシパルセキュリティコンサルタント

インターネット接続デバイスのセキュリティとプライバシーに対処する効果的な品質管理対策が浸透するまでは、今後 1～3 年の間に別のワームや Mirai のような攻撃が発生し、定期的に再発すると考えられます。
2021 年に向けて、IoT デバイスの透明性 (通信先や送受信するデータ) に関しては、大きな変化はないでしょう。ユーザーがスマートデバイスを購入する際、攻撃者がデバイスやユーザーのデータ／プライバシーに対してどのようなレバレッジをかけることができるのかを知らないことは大きな懸念ですが、残念ながらこうした状況は今後何年も継続することでしょう。
忘れてはならないのは、IoT は何年にもわたって私たちのプライバシーに大きな影響を与え、データ漏洩による個人情報盗難のリスクを高めるということです。デバイスメーカーはユーザーに関して驚くべき量の情報を入手できる立場にあり、メーカーはこれらの情報をもとに新たな収益源やビジネスを開拓することができるのです。
EU (欧州連合) のような機関は、マイクのデフォルトでのオフ設定など、プライバシーに関する法律を施行しようとしていますが、ソフトウェア開発プロセスの大部分は、どのような技術が使用され、どのように使用され、どのくらいの期間サポートされ、どのような情報が収集されて第三者に送信されるのかについて、何の透明性もないままに行われています。そして、DDoS ボットネット運用者は、脆弱性を抱える特定のブランド／モデルのデバイスの数の多さにつけ込んで大規模なボットネットを構築して、破壊的なオペレーションのために使用するサイバー攻撃者たちに販売していくことになるでしょう。

2. ランサムウェアを使用する新しい攻撃が登場

Maria Patricia Revilla Dacuno (マリア・パトリシア・レヴィラ・ダクノ)
戦術防衛ユニット　リサーチャー

2020 年における大きな出来事の 1 つは、「Buer」と「BazarLoader」という、Ryuk ランサムウェアを展開するための新しいローダーの登場です。Emotet の威力の大きさが実証されたことが、新しい「ローダー・アズ・ア・サービス」につながったと推測されます。Emotet が侵害された Web サイトを使用していたのに対して、新しいローダーはペイロードを配信するために Google Docs などのクラウドストレージを使用しています。2021 年にはランサムウェアを使用するサイバー犯罪者に対して新しいツール／サービスを提供する者が増加することは間違いありません。
また、パスワード保護された悪意のある添付ファイルを利用するキャンペーンが観測されていますが、サイバー攻撃者たちはこの手法を使用して、悪意のある添付ファイルがサンドボックスによる自動分析を受けないようにしたり、セ

キュリティツールによるスキャンを受けないようにしたりしています。この手法は 2020 年の Emotet のキャンペーンにも使用されましたが、2021 年以降は同様の手法を用いた攻撃が増加することが予想されます。

3. リモートワークにおけるシステムの不備／デバイスの脆弱性／対人関係の希薄さを突いた攻撃が増加

Vic Harkness (ヴィク・ハークネス)
F-Secure Consulting　セキュリティコンサルタント

リモートワークが奨励されている中、企業は新しいワークスタイルに対応していくことを余儀なくされていますが、技術的／社会的レベルの両方においてより大きな攻撃可能領域を生み出しており、2020 年はランサムウェア攻撃が増加する結果となりました。
コロナ以前にリモートワークに対応できていなかった企業が付け焼き刃で実施したリモートアクセスは、攻撃者が内部ネットワークに侵入するための演習場と化しています。しかし、企業内の対人関係の希薄さが一因となっている可能性があります。リモートワーク環境においては、自社の技術サポート部門の担当者だと名乗る人物が本物かどうか、判断が難しくなるケースが出てきます。大きな変化が生じるタイミングは、攻撃者にとっては大きなチャンスとなり得るのです。
「オフィスへの出社の際は、このリンクをクリックして個人情報を入力のうえ、出勤日をお知らせください」や「社員のリモートワークの状況を把握するため、このツールをインストールしてください」など、攻撃者たちは様々な罠を仕掛けてくることでしょう。リモートワークがニューノーマルとなるまでは、攻撃者は社員を操り安全でない行動を取らせ、自分たちに有利な状況を作り出していくことが予想されます。

Calvin Gan (カルビン・ガン)
戦術防衛ユニット　シニアマネージャー

新型コロナウイルスの感染拡大／ロックダウン／リモートワークなどの要素により、働き方改革が着々と進んでいる中、E メールは依然としてマルウェアの主要な感染経路となっており、特に個人所有のデバイス (PC、スマートフォン、タブレット) が業務に使用される場合、ソフトウェアの脆弱性が悪用され、更にメール経由での感染が広がる可能性があると言えます。より多くの CVE (共通脆弱性識別子) が発行され、ショッピングアプリや配送追跡アプリなど、多くのコンシューマが使用するソフトウェアの脆弱性が発見されることを期待しているとともに、セキュリティリサーチャーはサイバー犯罪者より先にこうした脆弱性を発見／修正することにより注力していくであろうと考えます。

Teemu Myllykangas (テーム・ミリカンガス)
F-Secure Radar　ソリューションディレクター

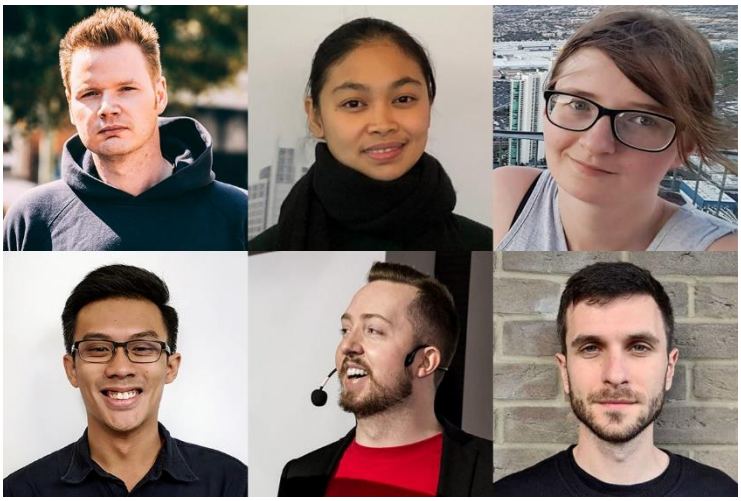
2021 年になっても、多くの企業は、パンデミックの初期に急遽採用したしたリモートワークの制度を、少なくとも部分的には維持しようとしていくものと考えられます。このような状況下で新しい手法や技術を導入しても、セキュリティ上上手くいくことはほとんどありません。2021 年には、攻撃者は企業がまだ対処できていないリモートワークにおけるセキュリティの脆弱性を悪用する方法を模索している可能性が高いでしょう。今後の攻撃に対処するうえで、企業はアプリケーションとデータを保護し続けるために、新しい分散型ネットワークとクラウドの導入を推進し、より適切にセキュリティを担保していく必要があります。

4. 政府／司法機関による、より積極的なランサムウェア対策への関与

Callus Roxan (カルム・ロクサン)
MDR　シニアレスポンス調査官

近年のランサムウェアの進化のほとんどは、技術的な進化ではなく、ランサムウェアとデータの流出を組み合わせて攻撃者が収益源を多様化／最大化するなど、運用面での進化なのです。2021 年には多くの政府／司法機関がこうした動きを追い、法的手段を用いてランサムウェアとの戦いに、より積極的に関与していくことが予想されます。

また、特にいくつかの業種が攻撃者の標的となることが考えられます。例えば、特に機密性の高いデータを扱う企業(法律関係など)や、製造業などランサムウェアの被害を受けやすい業種が想定されます。また、企業のランサムウェア対策費が増加していくため、当局はより高い意欲を持って攻撃に対処しようとするのではないでしょうか。
しかし、サイバー犯罪のエコシステムは分散化され、様々な断片化された性質を持っているため、標的型攻撃に対してはどのような対策を講じても完全に防ぐことは難しいと言えます。例えば、攻撃者への身代金の支払いを制限しようとする取り組みは、響きのいい措置ではありますが、企業が直面するビジネス上の現実と、サードパーティが身代金支払いのエージェントとして介在可能であることから、このような戦略の有効性は疑問視されるものとなります。



上段: 左から Tom Van de Wiele, Maria Patricia Revilla Dacuno, Vic Harkness
下段: 左から Calvin Gan, Teemu Myllykangas, Callum Roxan

エフセキュア　プレスリリースページ:
https://www.f-secure.com/jp-ja/press
本リリースに掲載の各エキスパートからのコメントは抜粋版であり、全文は以下のブログにてご覧いただけます。
https://blog.f-secure.com/ja/

エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関する AI テクノロジー、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200 社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。
エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は https://www.f-secure.com/en/welcome (英語) および https://www.f-secure.com/ja_JP/ (日本語) をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

※以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】

エフセキュア株式会社
広報部　　秦　和哉
TEL：03-4578-7745 (直通)　　japan-pr@f-secure.com