報道関係者各位

データ窃盗と脅迫の組み合わせによる『ランサムウェア 2.0』の被害が急増

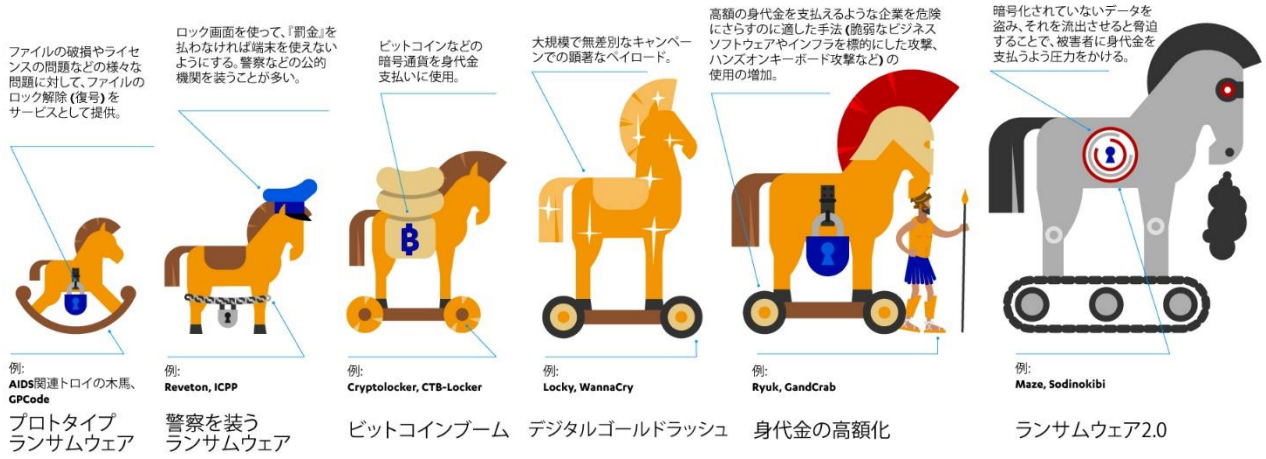
エフセキュア、2020 年下半期分のセキュリティ脅威レポートを発表

～ ランサムウェア 2.0、マルウェア、サプライチェーン攻撃が企業にとって大きな脅威に ～

2021 年 4 月 9 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) は本日、2020 年下半期 (7 月～12 月) における攻撃トラフィックに関する調査レポートを発表しました。同期間において観測された攻撃の特徴としては、データを盗み出し暗号化するだけでなく、身代金の支払いが拒否されると情報を公開すると恐喝する『ランサムウェア 2.0』の急増、情報を搾取するマルウェア、そしてサプライチェーン攻撃などが企業にとって重要な脅威となっています。

最も注目すべき傾向は、ランサムウェアの進化です。ランサムウェアとは、企業ネットワークに侵入しデータを盗み出して暗号化し、復号キーのための身代金を要求する手法です。2020 年にはこのタイプの攻撃が爆発的に増加しただけでなく、企業が身代金の支払いを拒否すると、攻撃者は盗んだ情報をリークすると脅すようになりました。エフセキュアが『ランサムウェア 2.0』と呼ぶこの攻撃の増加により、攻撃者は被害者に対してより大きな支払い圧力を持つようになりました。



ランサムウェアの進化

2019 年にはこの手法を使用しているサイバー犯罪集団は『Maze』と呼ばれるグループだけでしたが、2020 年末には、15 ものランサムウェアファミリーが同様の手法を採用していました。さらに、2020 年に発見された様々なランサムウェアの 40%近くが、複数のこれまでのファミリーと同様に、標的からデータを盗むことも判明しました。

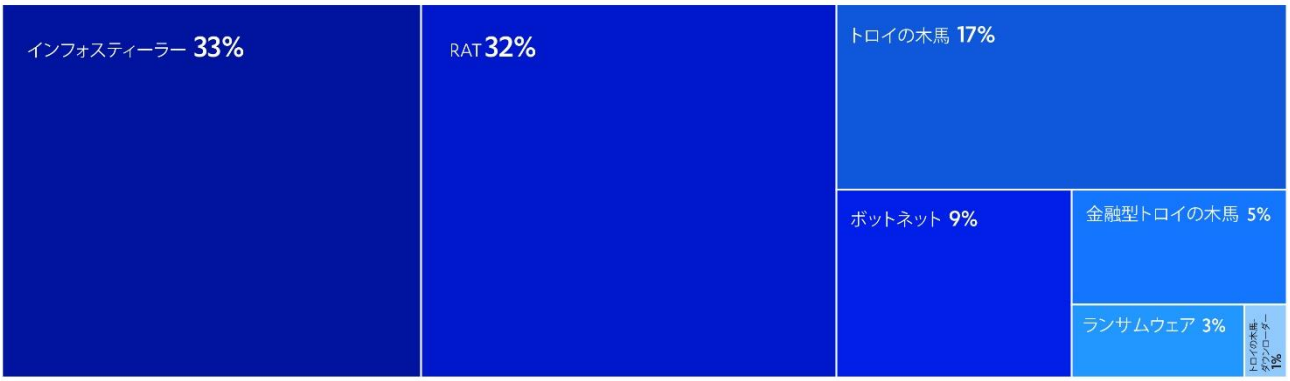
Ako	Darkside	**JungleSec**	**Nemty**	**SNAKE**
Avaddon	**DroppelPaymer**	Lock2Bits/LuckyDay	Pay2Key/Cobalt	**Snatch**
BitPyLock	Egregor	**LockBit**	ProLock	**Sodinokibi/Sodin/REvil**
ChaCha / Maze	EvilQuest/ThiefQuest	Mailto/NetWalker	PwndLocker	SunCrypt
Clop	FTCode	Mespinoza/Pysa	**Ragnar Locker**	Zeppelin
Conti	Hades	Mount Locker	Ranzy Locker	
CryLock / Cryakl 1.9	Hakbit/Quimera/Thanos	Nefilim/Nephilim	**Sekhmet**	

2018 年以降にデータの流出を実行したランサムウェアファミリー／ユニークバリアントの一覧。

(太字は、情報を公開すると脅して企業に身代金の支払いを要求するランサムウェア)

エフセキュアの戦術防衛ユニット (Tactical Defense Unit) のシニアマネージャーである Calvin Gan (カルビン・ガン) は、こうしたランサムウェアのトレンドについて、次のように語っています。
「信頼性の高いバックアップと効果的な復号手段を備えている企業は、ランサムウェアによる攻撃を受けても、身代金の支払いをせずにデータの回復することができます。しかし、ランサムウェア 2.0 による潜在的なデータ漏えいの管理は、特に機密情報を有する企業にとっては、全く異なる課題なのです。現在、そして将来的にも、ランサムウェアを使用するサイバー攻撃者たちは新しい手法を導入し続けており、新たな脆弱性の発見に注力しています。」

Gan はまた、過去 10 年間の注目すべきサプライチェーン攻撃を振り返り、その半数以上がユーティリティーソフトウェアまたはアプリケーションソフトウェアを標的としていることを強調し、昨年の SolarWinds 社のハッキング事件をきっかけに、これらの攻撃がもたらす影響に注目が集まるであろうと推測しています。
「セキュリティ分野では、企業が自らを守るために、強固なセキュリティ境界線、侵害を迅速に発見するための検知メカニズム、侵入を阻止するための対応計画と能力を持つことが重要視されています。しかし、企業が業界や国境を越えて協力し、サプライチェーンにおけるセキュリティの課題に取り組むことも必要なのです。高度なサイバー攻撃を仕掛ける APT (Advanced Presistent Threat = 持続的標的型攻撃) グループたちは様々な方法で多くの企業を危険にさらす準備と意思があることは明らかであり、我々は協力して対抗しなければならないのです。」

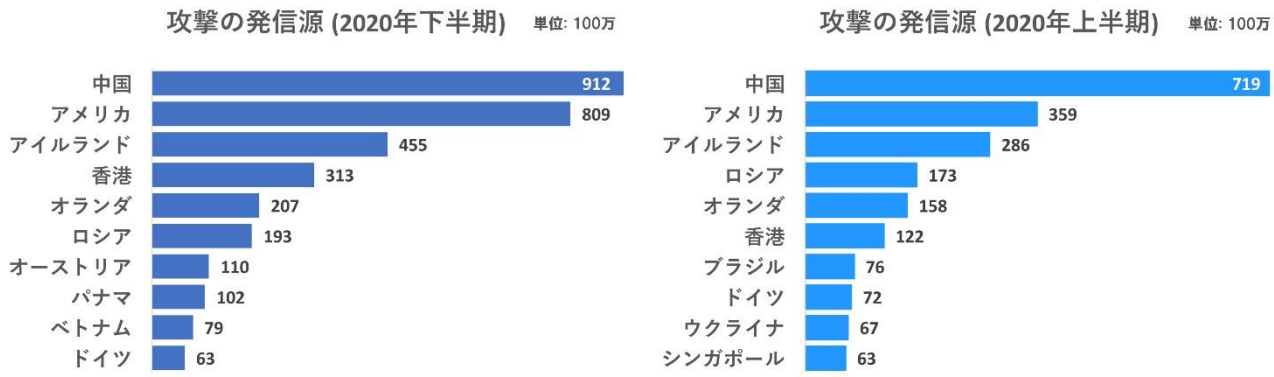


2020 年下半期に観測されたマルウェアのタイプ

今回の調査からのその他ファクト

- 攻撃者が悪意のあるコードを難読化するために、ブロックできないデフォルトの機能である Excel の数式を使用するケースが、前回調査時から 3 倍に増加した。
- フィッシング詐欺で使用されたブランド名では Outlook が最も多く、次いで Facebook、Office365 が上位に。
- フィッシングページのホストに使われたドメインの約 4 分の 3 は、Web ホスティングサービスだった。
- マルウェアの感染試行回数の半分以上を電子メールが占めており、サイバー攻撃においてマルウェアを拡散する際の最も広く使用される経路となっている。

- 2020 年下半期に最も流行した 2 つのマルウェアはインフォスティーラー（情報搾取型マルウェア）は Lokibot と Formbook であり、被害者からデータや情報を自動的に収集するマルウェアは前回の調査時に続き、大きな脅威となっている。
- 企業ネットワークで発見された脆弱性の 61%は 2016 年以前に既知となっていたものであり、少なくとも 5 年以上前から存在する脆弱性である。
- 攻撃の発信源として観測された上位 3 ヶ国は前回調査時と変わらず中国、アメリカ、アイルランドの順。それに続くのが香港、オランダ、ロシアとなっている。



2020 年における攻撃の発信源

本レポートの全文（日本語版）は、以下ブログページよりダウンロードいただけます。
https://blog.f-secure.com/ja/attack-landscape-update-h1-2021/
エフセキュア　プレスリリースページ:
https://www.f-secure.com/jp-ja/press

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