報道関係者各位

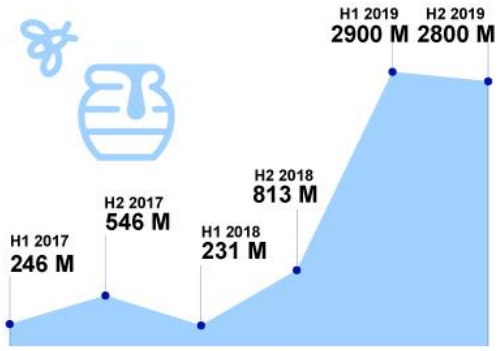
ランサムウェアの悪質化が顕著に、エフセキュアが 2019 年下半期の攻撃トラフィックレポートを発表

～ 増加する IoT デバイスに対する攻撃は継続傾向に ～

2020 年 3 月 11 日
エフセキュア株式会社

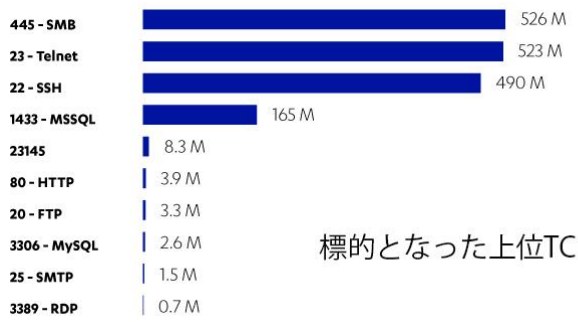
先進的サイバー・セキュリティ・テクノロジーのプロバイダである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Samu Konttinen、日本法人: 東京都港区、以下、エフセキュア) は、2019 年下半期 (7 月～12 月) における攻撃トラフィックに関する調査レポートを発表しました。同期間においては、ランサムウェアの悪質化、感染した IoT デバイスのボットネット、『エターナルブルー (EternalBlue)』エクスプロイトによるサイバー攻撃が依然として多数観測されています。また、過去数年で比類のない攻撃トラフィックの急激な増加が見受けられました。

調査期間中、エフセキュアが情報収集のために設置したグローバルハニーポット (攻撃者を誘惑するためのおとりサーバ) に対して、28 億件の攻撃イベントが発生しました。同年上半期の 29 億件との合計では、通年で 57 億件となります。また、2018 年には通年で 10 億件、2017 年には約 8 億件の攻撃がありました。



調査期間ごとのハニーポットへの攻撃総数

トラフィックの中では SMB プロトコルへの攻撃が多数を占めていました。これは、攻撃者のエターナルブルーに関連するワームとエクスプロイトの使用に関する関心が引き続き非常に高いことを示しています。また、Telnet トラフィックや SSH への攻撃も多く、本年上半期に見られた、IoT デバイスに対する攻撃の増加傾向が継続していることを示しています。ハニーポットで見つかったマルウェアには、Mirai のさまざまなバージョンを含んでいます。



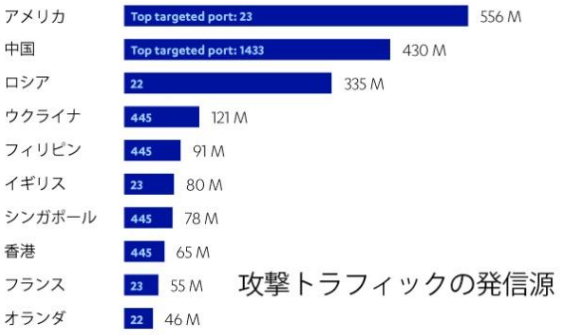
標的となった上位TCPポート

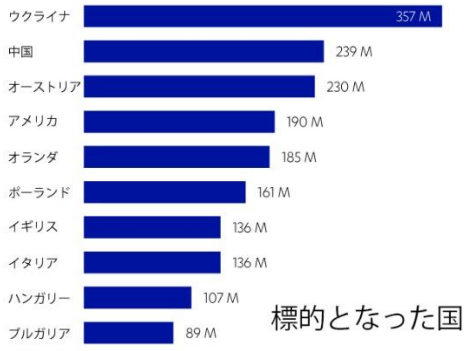
ランサムウェアスパムの総数は減少が確認されましたが、ランサムウェア自体はよりターゲットを絞り込んだものとなり、1 件あたりの被害はより大きくなっています。モジュール型マルウェアはさまざまなトリックを使用しましたが、その 1 つはランサムウェアを第 2 ステージのペイロードとしてドロップすることでした。

本レポートではまた、多くのデータ侵害、国家ハッカーによるマルウェアの出現、壊滅的被害をもたらしたサプライチェーン攻撃など、過去 10 年間の情報セキュリティにおける様々な出来事を取り上げています。エフセキュアのチーフ・リサーチ・オフィサー (CRO) である Mikko Hypponen (ミッコ・ヒッポネン) はこうした傾向について、次のように述べています。
「過去 10 年間は情報セキュリティにとって悪い状況が続いていましたが、今後の 10 年間はそうした状況が多少は改善されるものと考えています。私たちの社会は常に重大な侵害とデータ漏洩に取り囲まれているように見えるかもしれませんが、そこまで悲観的な状況ではありません。10 年前と現在では、サイバー攻撃対策に使用されるセキュリティツールのレベルが飛躍的に向上しています。セキュリティ対策において、私たちは正しい方向に進んでいるのです。」

今回の調査からのその他ファクト

- 攻撃トラフィックの発信源は、米国、中国、ロシア、ウクライナの順に多かった。
  (2019 年上半期: 中国、米国、ロシア、ドイツの順)
- 標的となった国は、ウクライナ、中国、オーストリア、米国の順。
  (2019 年上半期: 米国、オーストリア、ウクライナ、英国、オランダ、イタリアの順)
- 調査期間中のランサムウェア配信方法で最大のシェアを占めたのは、手動インストール／第 2 ステージペイロード経由の 28%。次点が電子メール／スパム。
  (2019 年上半期: リモートデスクトッププロトコル (RDP) 経由の 31%が最大)
- Telnet トラフィック発信源のシェアは米国、アルメニア、英国、ブルガリア、フランスの順に大きかった。
  (2019 年上半期: 米国、ドイツ、英国、オランダの順)
- SMB トラフィックの最大の発信源はフィリピンと中国だった。
  (2019 年上半期: 中国が最大)





F-Secure の戦術防衛ユニット (Tactical Defense Unit) のマネージャーである Calvin Gan (カルビン・ガン) は、今回の調査について以下のように語っています。
「スパムは、2019 年も引き続き攻撃者の間で多く用いられる攻撃手法でした。受信したメールに疑いを持たない個人ユーザやサイバー攻撃に対する認識の低い企業は、マルウェア作成者にとって格好の標的となっているのです。また、データ侵害につながるランサムウェアへの感染など、攻撃の更なる高度化が見受けられます。こうしたサイバー攻撃に対して、より強固な対策を施すことが、企業や団体にとってこれまで以上に重要になっています。」

今回の調査に基づくレポートは、F-Secure ブログでもご覧いただけます。
https://blog.f-secure.com/ja/attack-landscape-h2-2019-an-unprecedented-year-cyber-attacks/

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
PR マネージャ:　秦　和哉
TEL：03-4578-7745 (直通)　　japan-pr@f-secure.com