

IoT デバイスへの攻撃が急増、 エフセキュアが 2019 年上半期の攻撃トラフィックレポートを発表

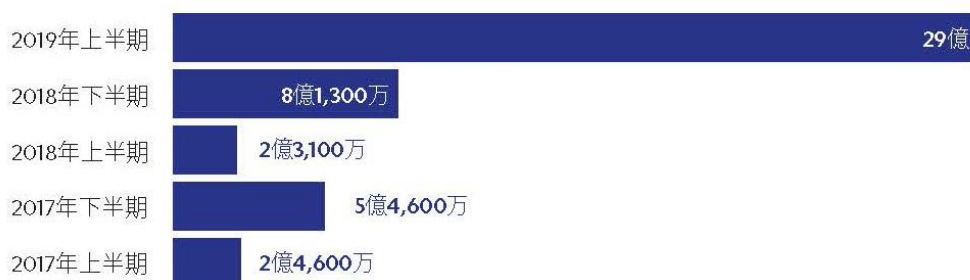
ハニーポットへの攻撃件数は 2018 年上半期の 12 倍に

2019 年 9 月 18 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、最新の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。同調査では、2019 年上半期 (1 月～6 月) には IoT および Windows Server Message Block (SMB) 関連の攻撃の強度が高まったことがわかりました。同レポートは、IoT デバイスがオンラインで適切に保護されていない場合に直面する脅威、そして依然衰えぬ Eternal Blue や発生から 2 年が経過した WannaCry に関連するエクスプロイトの継続的な活動が目立っていると説明しています。

F-Secure 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) への攻撃は期間中 29 億回にのぼり、昨年同時期 (2 億 3,100 万回) と比較して 12 倍に達しています。この結果は、IoT デバイスで使用される Telnet および UPnP プロトコルを標的とするトラフィックと、ランサムウェアおよびバンキング型のトロイの木馬を拡散させるために Eternal のエクスプロイトファミリーで使用される SMB プロトコルにおける増加に起因しています。

調査期間中のハニーポットへの攻撃件数



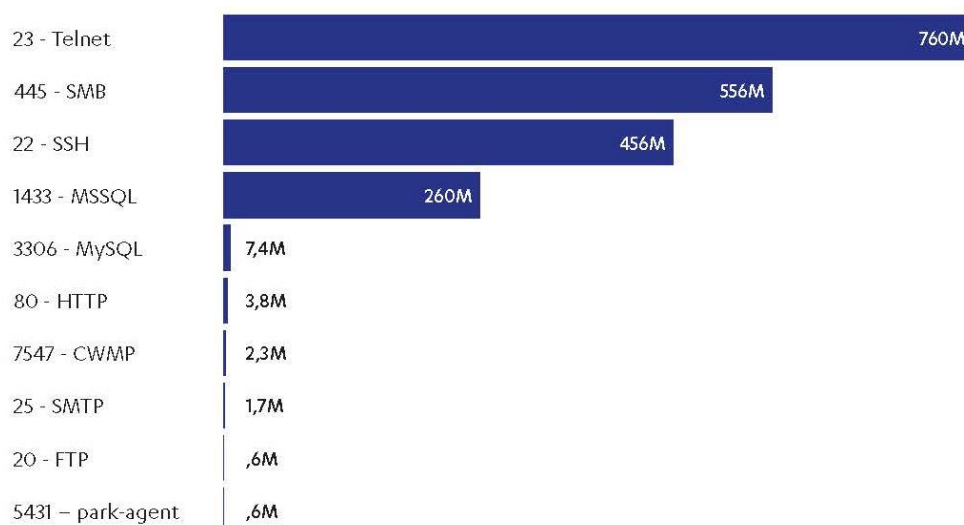
ポートとプロトコル

調査期間中、Telnet トラフィックが全トラフィック中 26% と最大のシェアを占め、ログに記録された攻撃イベントは 7 億 6,000 万にのぼりました。次点は UPnP で、6 億 1,100 万件 (21%) の攻撃が発生していました。IoT デバイスを標的にするためにも使用される SSH は、4 億 6500 万件 (16%) の攻撃を受けましたが、これは Mirai などのマルウェアに感染した IoT デバイスがソースとして考えられます。Mirai は、ルータ、監視カメラ、および工場出荷時のデフォルト認証情報を使用する IoT デバイスなどに感染します。

SMB ポート 445 への攻撃トラフィックは 5 億 5,600 万件となっています。これは、2017 年に壊滅的被害をもたらした WannaCry の発生で最初に使用された Eternal のエクスプロイトファミリーがまだ健在であり、未だにパッチが適用されていない数百万台のマシンを破壊しようとしていることを示しています。エフセキュアのプリンシパル・リサーチャーである Jarno Niemela (ヤルノ・ニエメラ) はこれについて以下のように語っています。

「Mirai の登場から 3 年、WannaCry から 2 年が経過していますが、これらのアウトブレイクで引き起こされた問題がまだ解決されていないことが当社の調査でわかりました。IoT の不安定さがますます深刻になりつつある一方、次々に登場する多くのデバイスがボットネットによる攻撃を受けています。また、SMB に対する攻撃は、未だに多くのマシンにパッチが適用されていないことを示しています」

標的となった上位TCPポート



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中国、米国、ロシア、ドイツの順に多かった。
- 標的となった国は米国、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、リモートデスクトッププロトコル (RDP) 経由で、31%だった。
- Telnet トラフィック発信源のシェアは米国、ドイツ、英国、オランダの順に大きかった。
- SMB トラフィックの最大の発信源は中国だった。

今回の調査レポートは以下の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-h1-2019-iot-smb-traffic-abound/>

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人工知能、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