毎秒 13 回の攻撃、重要インフラが標的に

Forescout は 2023 年のグローバル脅威レポート「2023 Global Security Roundup」にて、重要インフラのためのより強力なサイバーセキュリティ対策を提言

2024 年 3 月 12 日（2024 年 1 月 24 日サンノゼ，カリフォルニア発プレスリリース抄訳） – **昨年、**世界の重要インフラ - 医療、電力、通信、廃棄物、製造、および人々と機械をつなぐ交通機器 - はほぼ絶え間ない攻撃を受けてきました。Forescout Research - Vedere Labs は、2023 年 1 月から 12 月までに 4 億 2000 万回以上の攻撃を記録しました。これは 1 秒あたり 13 回の攻撃であり、2022 年から 30%の増加です。

グローバルなサイバーセキュリティリーダーである Forescout は、新しいレポート「2023 Global Threat Roundup」で、Adversary Engagement Environment (AEE) で記録された攻撃のグローバルな調査結果を公開しました。AEE は、重要インフラの脆弱性と脅威を分析する世界有数のチーム、Vedere Labs によって運営されています。

サイバー攻撃の継続的な急増によって生じる厳しい現実にもかかわらず、前向きな道があります。Forescout Research - Vedere Labs の研究副社長である Elisa Costante は、ポジティブな変化を強調し、「現在の取り組みが重要な資産を強化し、リスクを評価するための重要な技術を十分に活用することには至っていないのは事実ですが、改善の機会があります」と述べています。

2023 年グローバル脅威レポート「2023 Global Threat Roundup」: サイバー攻撃、エクスプロイト、マルウェアのトレンド（英語）を読む

https://www.forescout.com/resources/research-report_2023-threat-roundup

ブログ（日本語）を読む

https://forescout.jp/2023-global-threat-roundup-trends-in-cyberattacks-exploits-and-malware/

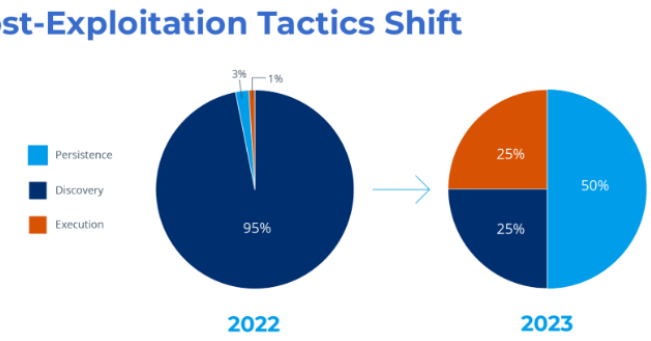
Forescout Research によるトップ 5 の考察は次の通りです：

1. **いまだ沈静化せず：Log4j がソフトウェアライブラリのエクスプロイトを抑制**
   Log4j のエクスプロイトの件数が減少したことにより、ソフトウェアライブラリに対するエクスプロイトが減少しています。この静けさが、ネットワークインフラストラクチャとモノのインターネット（IoT）デバイスを対象としたエクスプロイトの急増につながっています。IoT の市場では、IP カメラ、ビルディングオートメーションシステム、ネットワーク接続ストレージが、悪意のあるアクターにとって最も人気のあるターゲットとして浮上しています。悪用された脆弱性のうち、35%のみがサイバーセキュリティおよびインフラストラクチャセキュリティ局（CISA）の既知の悪用脆弱性（KEV）リス

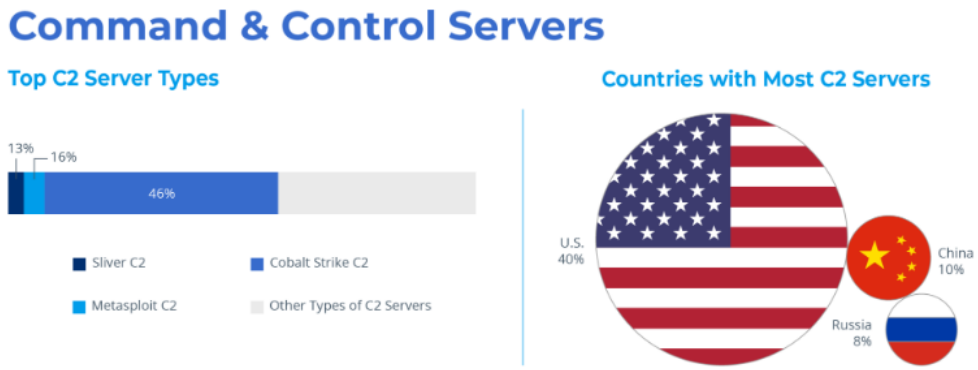
トに登場しました。この乖離は、既知の脆弱性データベースへの依存を超えた、積極的かつ包括的なサイバーセキュリティアプローチの必要性を強調しています。

2. **運用技術（OT）プロトコルに大打撃**
   運用技術（OT）は絶え間ない攻撃にさらされており、5 つの主要なプロトコルが執拗な攻撃の矢面に立っています。主なターゲットには、Modbus のような産業オートメーションおよび電力セクターで使用されるプロトコルが含まれ、全攻撃の 3 分の 1 を占めています。これに続くのは Ethernet/IP、Step7、DNP3 で、それぞれが攻撃の約 18%を占めています。IEC10X がこのリストを 10%の攻撃で締めくくり、残りの 2%はさまざまなプロトコルに分散しており、その中で BACnet が大半を占めています。BACnet のようなビルディングオートメーションプロトコルは、スキャンの頻度が少ないです。しかし、スキャンの相対的な希少性は、ビルディングオートメーションデバイスの脆弱性に対するターゲット攻撃がより一般的であるという警鐘を鳴らしています。

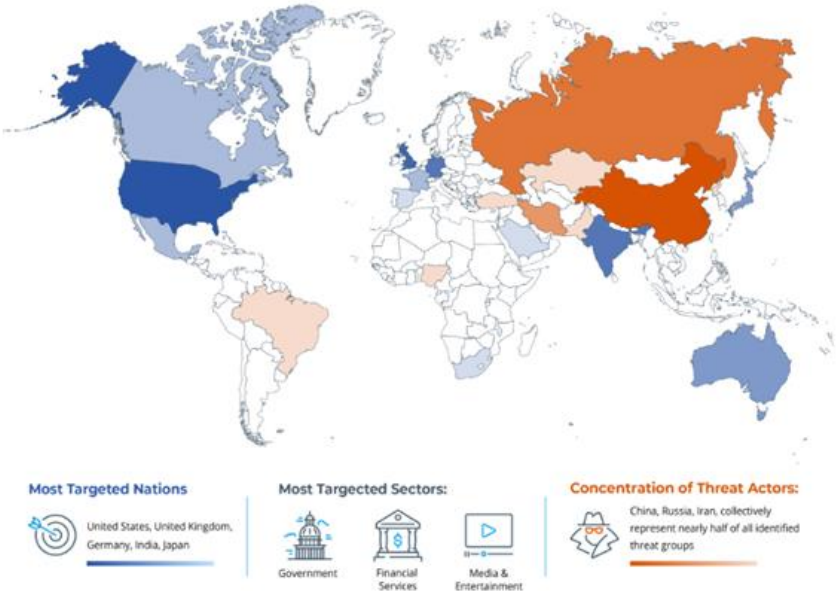
3. **悪用後の戦術の変化**
   持続性戦術は 2022 年の 3%から 50%の急増を示し、それに発見（約 25%）と実行（残りの約 25%）が続きます。脅威アクターによって使用される観察されたコマンドのほとんどは一般的な Linux システムを対象としていますが、広く使用されているルーターに搭載されたネットワークオペレーティングシステム用に実行される特定のコマンドに関する顕著な傾向があります。



4. **マルウェアファミリーは依然として強力な脅威**
   Agent Tesla リモートアクセストロイの木馬（RAT）は、観測された悪意ある活動の大きな 16%のシェアを占めています。これに続くのは、Mirai ボットネットのバリアントで 15%を占め、Redline 情報窃取ツールが 10%でその地位を保っています。コマンドアンドコントロールサーバーの中では、Cobalt Strike が圧倒的なリーダーとして浮上し、全体の 46%のシェアを占めています。これには Metasploit が 16%、新興の Sliver C2 が 13%で続きます。これらのサーバーのほとんどはアメリカ合衆国にあり、世界の風景の 40%を構成しており、中国とロシアがそれぞれ 10%と 8%で続いています。



5. **163 ヶ国で脅威が蔓延**
   脅威アクターはデジタルの網を広く深く展開し、163 ヶ国に影響を与えています。アメリカ合衆国が主なターゲットとなり、168 の悪意あるアクターがこの国を狙っています。他の国々には、イギリス（88）、ドイツ（77）、インド（72）、そして日本（66）が含まれます。攻撃者は特定の地域に集中しています。中国（155）、ロシア（88）、そしてイラン（45）で、これらはすべての特定された脅威グループのほぼ半分を代表しています。これらの悪意ある実体の照準は主に 3 つの重要なセクターに固定されています：政府、金融サービス、そしてメディアとエンターテイメント。これらの産業は社会インフラの主要な柱として、サイバー戦争の最前線にあり、強化されたセキュリティ対策と協力的な努力の必要性を強調しています。



Costante は次のように続けます、「重要なのは、管理されているかどうかにかかわらず、すべてのデバイスに対して包括的な可視性を実現し、リアルタイムの状況認識を確保することです。

これを行うことで、大企業は受動的な防御姿勢からより積極的なアプローチに移行し、無意味なセキュリティのモグラたたきゲームを避けることができます。この強化された可視性と積極的な防御戦略へのシフトは、重要インフラのためのより明るい展望を示しています。

Forescout Research の仕組み

Forescout Research は、実際の接続デバイスとシミュレートされた接続デバイスの組み合わせを活用して分析を行うために、Adversary Engagement Environment (AEE) を使用しています。このダイナミックな環境は、事件の特定と複雑な脅威アクターのパターンの識別を詳細なレベルで可能にする強力なツールとして機能します。包括的な目的は、この特殊な仮想環境から得られる詳細な洞察と理解を活用して、複雑な重要インフラ攻撃への対応を向上させることです。AEE は、重要インフラの脆弱性と脅威を明らかにすることに専念する世界有数のチームである Vedere Labs によって運営されています。Forescout の製品はこの研究を直接活用しており、この研究はベンダー、代理店、および他の研究者とも公開して共有されています。

Forescout について

Forescout Technologies, Inc.は、グローバルなサイバーセキュリティリーダーとして、IT、IoT、IoMT、OT を含む、管理対象および非管理対象のすべての接続されたサイバー資産を継続的に識別、保護し、コンプライアンスを支援します。20 年以上にわたり、Fortune 100 企業や政府機関は、Forescout がベンダーに依存しない自動化されたサイバーセキュリティを大規模に提供することを信頼してきました。Forescout® プラットフォームは、ネットワークセキュリティ、リスクおよびエクスポージャー管理、拡張検出および対応のための包括的な機能を提供します。エコシステムパートナーを介したシームレスなコンテキスト共有とワークフローのオーケストレーションにより、顧客はサイバーリスクをより効果的に管理し、脅威を軽減することができます。

当プレスリリースに関するお問い合わせ先

英語： Carmen Harris, Corporate Communications
carmen.harris@forescout.com
日本語： フォアスカウト・テクノロジーズ株式会社
japan@forescount.com