2023 年 5 月 16 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：APAC における最大の悪性 DNS トラフィックが QSnatch 感染であることを観測

Emotet と Qsnatch の世界的な拡散を追跡

- **現在、QSnatch 感染はエンタープライズ環境において最大のコマンド&コントロール（C2）通信発生元となっている**
- **攻撃により、サーバーのダウン、データの窃盗、サービスの中断が発生する懸念がある**
- **過去 1 年間に全世界で侵害の兆候を示した組織の割合は約 12% に及ぶ**

オンラインの力となり、守るクラウドカンパニーの Akamai Technologies, Inc.（NASDAQ：AKAM）は、最新の脅威レポート「SOTI インターネットの現状 | 攻撃の『高速道路』悪性 DNS トラフィックの詳細な分析」を発表しました。このレポートでは、悪性のドメイン・ネーム・システム（DNS）トラフィックがアジア太平洋地域の事業者と消費者にもたらしている脅威を取り上げています。

アジア太平洋地域（APAC）に関する主な調査結果は以下のとおりです。

- **APAC では QSnatch が最大の脅威になっている**：QSnatch は、企業でバックアップやファイル保存に使用されるネットワーク接続ストレージ（NAS）デバイスの一種である QNAP のみを標的とするマルウェアです。2022 年には APAC のエンタープライズ環境における最大の C2 通信数を確認しました。APAC では C2 ドメインへのアクセスの約 60% が QSnatch に関連しており、その量は北米に次いで世界第 2 位となっています。
- **エンタープライズに対する C2 トラフィックが増加している：**世界の組織のうち、四半期ごとにネットワーク内で C2 トラフィックが発生している組織は 10～16% に達しており、攻撃や侵害が進行している可能性を示唆しています。Akamai の観測によると、APAC では影響を受けたデバイスの約 15% がイニシャル・アクセス・ブローカー（IAB）のドメインに接続しています。こうしたブローカーはサイバー犯罪集団であり、侵入したネットワークへの不正アクセス情報をランサムウェア集団など他のサイバー犯罪者に売っています。
- **世界的に見ても APAC のホームネットワークは最も大きな脅威に晒されている：**APAC では家庭向けホームネットワークの脅威が、他のどの地域よりもはるかに高い数値を示しています。同地域は世界第 2 位の北米地域に比べ、2022 年後半に発生した悪性のクエリー数が 2 倍となっています。APAC では 3 億 5,000 万以上のクエリーが Pykspa に関連していることが判明しています。なお、Pykspa

とは影響を受けたユーザーの連絡先に Skype を通じて悪性のリンクを送信して拡散する情報窃取ワームです。

企業における DNS 攻撃の脅威は増大している

インターネット利用は DNS を介して行われることが大半なので、DNS はその普遍性から攻撃インフラとして重要な役割を負わされるようになりました。Akamai では 1 日あたり約 7 兆件におよぶ DNS リクエストを観測しており、悪性の DNS トランザクションをマルウェア、フィッシング、コマンド＆コントロールという 3 つの大きなグループに分類しています。

Akamai のデータによると、世界の組織のうち、四半期ごとにネットワーク内でコマンド＆コントロール（C2）トラフィックが発生している組織は 10～16% に達しています。C2 トラフィックが存在しているということは、攻撃や侵害が現在進行形で発生している可能性があります。脅威としては、ボットネットが情報を窃取する、IAB が侵害したネットワークへの不正アクセス情報を他のサイバー犯罪者に売りつけるなど、さまざまなことが考えられます。

APAC では、影響を受けたデバイスの 15% が、Emotet をはじめとする既知の IAB C2 ドメインに接続しています。IAB C2 ドメインはまず侵害し、その後に Lockbit などのランサムウェアグループや他のサイバー犯罪者グループにそのアクセス情報を売りつけます。同地域では、Revil や Lockbit のようなランサムウェアの亜種も、あらゆる組織のデバイスに影響を与える C2 脅威の上位 5 種にランクインしています。

ネットワークに接続されたストレージデバイスは、パッチを適用されることが少なく、貴重なデータが保存されているため、悪用の格好の的になっています。Akamai のデータによると、APAC では 2022 年に感染したデバイスの 60% 近くが NAS デバイスを標的として情報を盗み出すマルウェア「QSnatch」によるものであり、感染デバイス数は北米に次いで世界第 2 位となっています。全体的な感染台数が増加した大きな要因として、APAC にはデータセンターが密集しており、中小企業向けの NAS が普及していることが考えられます。

Akamai の APJ 担当 Director of Security Technology and Strategy の Reuben Koh は次のように説明しています。「アジア太平洋地域が経済とデジタルトランスフォーメーションのグローバルハブとして進化し続ける中、攻撃者があらゆる手を尽くしてエンタープライズを攻撃し、金銭的利益を得ようと画策を続けているのは意外なことではありません。Akamai による最新の調査結果によって、各地域で最もよく見られる攻撃だけでなく、アジア太平洋地域における最近のサイバー環境でマルチステージ攻撃が定番となっている現状も明らかになりました。攻撃者は互いに協力したり、1 回の攻撃に多様なツールを組み合わせたりすることで、成功率　を増しています。C2 インフラは通信目的だけでなく、ペイロードや次の段階のマルウェアをダウンロードしやすくして攻撃を前進させることができるため、攻撃の成功に極めて大きな役割を果たしています」

さらに、こうも語っています。「マルチステージ攻撃はビジネスに悪影響を及ぼしかねないため、組織は攻撃者の一歩先を行くことが非常に重要です。直接的な金銭的損失や顧客の信頼喪失という短期的な影響だけでなく、法的コスト、補償コスト、クリーンアップコストなど、侵害されたインフラを回復するための長期的なコストも発生します」

DNS 攻撃に対して自宅も厳重に警戒すべき

エンタープライズはネットワークの侵害が成功すれば利益が大きいため、攻撃者の標的にされがちです。一方、個人の住宅はネットワークのセキュリティが企業環境ほど厳重ではないため、簡単にすばやく攻撃されます。コンピューターのような従来のデバイスだけでなく、携帯電話や家電のような IoT デバイスも攻撃者による悪用の対象となります。

Akamai のデータによると、2022 年後半にホームネットワークの脅威に関連したクエリーの数は、APAC が世界トップとなっています。そ　の数は、世界第 2 位である北米の 2 倍でした。

APAC では、Pykspa に関連するクエリーが 3 億 5,000 万件以上観測されました。Pykspa とは、影響を受けたユーザーの連絡先に悪性のリンクを送りつけ、Skype を通じて拡散する脅威です。攻撃者は Pykspa のバックドア機能を使用してリモートシステムに接続し、ファイルのダウンロードやプロセスの終了といった任意のコマンドを実行し、ドライブのマッピングやネットワーク共有など、さまざまな手段で広めることができます。

また、APAC では金融ブランドを標的として、フィッシングだとは疑わない消費者を誘い込むフィッシングキャンペーンも活発です。Akamai の調査によると、フィッシングキャンペーン全体の 40% 以上が金融サービスの顧客を狙ったものであり、その結果、金融関連のフィッシング詐欺や攻撃で被害を受けた顧客は全体の 70% 近くに上っています。この数字を見ると、2022 年に行われた金融サービスやその顧客に対する攻撃が非常に効果的だったことが明らかです。

Reuben Koh は「ホームユーザーは自宅のネットワークが侵害されればデータを全て失う可能性があるという個人的な危機に瀕しているだけにとどまりません。知らず知らずのうちに自分のデバイスが攻撃者のサイバー犯罪行為に悪用される踏み台として、スパムや組織への DDoS 攻撃など大規模なボットネットに加担させられていれば、個人的な危機よりもはるかに由々しき事態に直面することになります」と述べています。

さらに「現在 12 億人以上がモバイル・インターネット・サービスにアクセスしており、2026 年には IoT 支出が 4,360 億ドルに達すると予測されているアジア太平洋地域でこのような攻撃が増加しているのは当然です。この地域ではモバイルデバイスとスマートデバイスの利用と普及が継続的に進んでいるため、このような攻撃がおそらく増加すると思われます。ホームユーザーはサイバー攻撃の被害に遭わないよう、厳重に警戒すべきです」と語りました。

ビジネスユーザーとホームユーザーへのアドバイス

Akamai は DNS の状況を分析した結果、ビジネスユーザーとホームユーザーに次のような対策を推奨します：

- **これまでと同様、デジタルアセットとデジタルユーザーに対して事前に最適なサイバー検疫の実践を継続する**：
    - まずは、すべてのソフトウェア資産とハードウェア資産を可視化し、組織のデータジャーニーの各段階における重大な脆弱性と、そのために必要なコントロールをマッピングしましょう。例として、DDoS、マルウェア攻撃、スクラップ、ラテラルムーブメント（攻撃の横展開）、データ窃盗などが挙げられます。

- ベストプラクティスとして、あらゆるシステムとソフトウェアを最新の状態に保つこと、アンチマルウェアと多要素認証を導入すること、ユーザーとデバイスに付与するアクセス権は常に最低限にすることなどを推奨します。組織の規模が大きい場合や要件が複雑な場合は、専門のプロバイダーにサポートを依頼すべきですが、その場合でも積極的にパフォーマンスや異常なイベントを監視してください。

- **自宅で正しいセキュリティ習慣を身に付ける**：
  - 自宅では、ソフトウェアの定期的なアップデートの徹底、アンチ・マルウェア・ソフトウェアのインストール、家庭用 Wi-Fi ネットワークにおける WPA2 AES や WPA3 の暗号化の適用により、事前にすべてのデバイスのセキュリティを確保しましょう。疑わしい Web サイトやダウンロードファイル、メールやテキストメッセージにも厳重な注意が必要です。

Akamai について：

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。広範に分散したエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com/ja および akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。