攻撃の「高速道路」

悪性 DNS トラフィックの詳細な分析

エンタープライズを狙う脅威

10%-16%

どの四半期においても、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の割合

36%

脅威につながるトラフィックが見られた、影響を受けたデバイスの割合。この脅威は、ネットワークに接続されたストレージデバイスに保存された、バックアップや内部データを狙う

26%

イニシャル・アクセス・ブローカーに関連したトラフィックが見られた、影響を受けたデバイスの割合。これはランサムウェア攻撃を促進する役割を果たすことが多い

組織で見られる攻撃手法の種類

組織のネットワークに対する脅威の種類は多く存在しますが、そのすべてが同じように作成されているわけではありません。当社は、攻撃者のグループに関連する脅威の痕跡情報を通して、さまざまな攻撃者グループを特定することができました。これにより、悪性トラフィックに関連する攻撃手法とその目標を理解することができます。

イニシャル・アクセス・ブローカー
イニシャル・アクセス・ブローカー（IAB）は主に、ランサムウェアグループをはじめ他のサイバー犯罪者が組織ネットワークへの足がかりとなる最初の侵入ポイントを提供することを目的としています。

ボットネット
攻撃者がボットネットを利用する目的は、クリプトマイニングや DDoS 攻撃によるデータ漏えい、マルウェアの展開やラテラルムーブメントなどさまざまです。

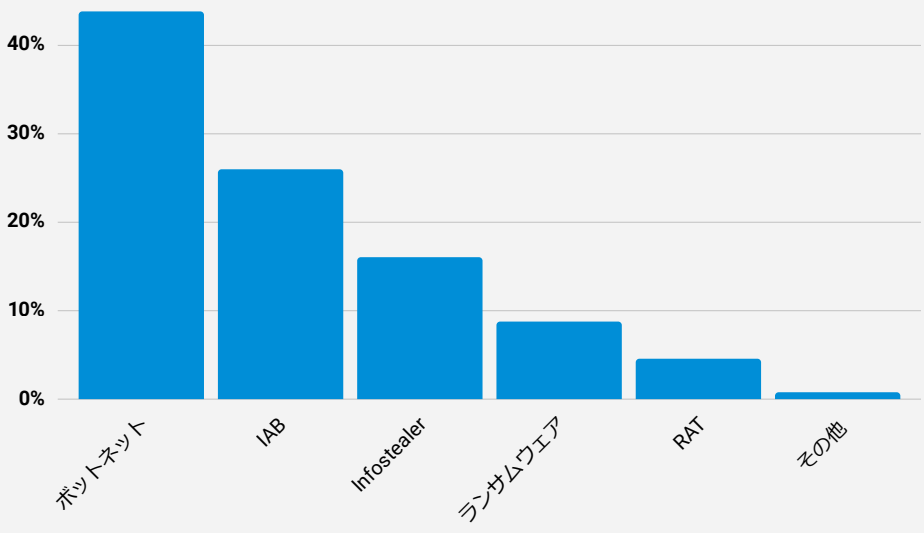
RaaS（Ransomware as a Service）グループ
（技術知識のない者も含めた）他の攻撃者を仲間とし、ランサムウェアソフトウェアを有償で利用するグループです。

情報窃取（infostealer）
infostealer はユーザー名、パスワード、システム情報、銀行の認証情報、cookie などの各種データを収集します。

リモート・アクセス・ツール
リモート・アクセス・ツール (RAT) は、偵察、特権の昇格、ネットワークを介したラテラルムーブメント（横方向の移動）、永続化の確立、侵入後のリモートペイロード実行、データ流出など、サイバー犯罪者に多くのユースケースを提供します。

脅威カテゴリごとのデバイスの割合

2022 年 1 月 1 日～2022 年 12 月 31 日



エンタープライズ組織を主に標的とするのは、ボットネット、IAB、infostealer。
それぞれの脅威は、組織のセキュリティと機密データに対するリスクを表します。

マルチステージ攻撃における DNS の役割

マルチステージ攻撃では、攻撃者は正規と悪性、両方のツールを組み合わせて使用して、攻撃を進める必要があります。C2 ドメインはコマンドの送信、ペイロードのダウンロード、攻撃対象となるネットワークへの攻撃の誘導など、攻撃のさまざまな段階で重要な役割を果たします。

攻撃者のドメインから第二段階のペイロードをダウンロード

初期アクセス
武器と化したドキュメントや悪意のあるペイロードが次の段階のマルウェアをダウンロードします

C2 ドメインにコールバックして新しいコマンドを確認

潜伏
マルウェアは標的となったマシン上で休止状態になり、攻撃者のアクティベーションを待ちます

攻撃者が制御するドメインによる C2 通信

C2
侵入に成功した後、攻撃者は直接的な手法で、C2 ドメインからマルウェアにコマンドをプロアクティブに送信します

ペイロードを別のマシンにダウンロード

ラテラルムーブメント
攻撃者が一度ネットワーク内の他のマシンへの上位のアクセス権限を得ると、ドメインを使用してネットワーク内の他のマシンにマルウェアをダウンロードする可能性があります

ホームユーザーを狙う攻撃

2 億 1600 万
Android マルウェアである FluBot に関連する悪性クエリーの数。SMS を介して拡散され、ユーザーを悪性のリンクをクリックするように誘導。この脅威は銀行の認証情報を盗むことが可能。

1 億 5600 万
IoT ボットネットである Mirai に関連する悪性クエリーの数。感染したユーザーデバイスを使用して、注目度の高いターゲットに対する大規模な妨害攻撃を開始。

3 億 6700 万
Skype のメッセージ機能を介して拡散するマルウェアである Pykspa に関連する悪性クエリーの数

8000 万
ランサムウェアなどの他のマルウェアを展開するボットネットである Necurs に関連する悪性クエリーの数

エンタープライズとホームユーザーの両方で見られる悪性 DNS トラフィックの詳細については、レポートをダウンロードしてご確認ください

レポートの全文をダウンロード

 | サポート | 公開日：2023 年 3 月