McAfee
Together is power.

2019 年の脅威予測

McAfee Labs

サイバー犯罪者の連携

サイバー犯罪者の連携が進み、サービスとしてのマルウェアが増加します。

必要なものがすべて揃うマーケット

アンダーグラウンドの市場でマルウェア、エクスプロイト、ボットネット、サービスが販売されています。経験やスキルに関係なく、攻撃を簡単に開始できます。

ブランドの強化で勢力を拡大

強力なブランドが増加し、より高度な暗号通貨マイニング、モバイル マルウェア、クレジットカードや認証情報の盗難が増加します。

地下組織の統合

サービスとしてのマルウェアの統合が進みます。ランサムウェアを支援するエクスプロイト キット（GandCrab）のように、この連携はアフェリエイト経由で進みます。

より迅速な攻撃

サイバー犯罪者はより迅速に攻撃を仕掛けてきます。脆弱性の検出からマルウェアの作成までの時間を短縮しています。2019 年は新しい脆弱性の悪用が増えるでしょう。

回避技術

攻撃のアウトソーシング化が進み、回避技術で人工知能が活用されます。

回避ツール

これまで、検出回避のためにパッカーやクリプターなどのツールが使用されてきました。サイバー犯罪者は人工知能を利用することで、より迅速で効率的に保護対策を回避するでしょう。

アジャイルな検出回避

タスク マネージャーやスキャンの実行時に停止するコイン マイナー。プロセス インジェクションやメモリー空間の操作でコードを挿入するエクスプロイト キット。難読化コードを追加してリバース エンジニアリングを遅らせるボットネット。盗み出した認証情報を使用する APT。検出回避に様々な技術が利用されています。

人工知能

犯罪者は人工知能を利用して標的の選択を自動化し、感染した環境を事前に確認して検出を回避するでしょう。

攻撃の特定は？

複数の脅威が連携し、効果的な攻撃が実行されます。
攻撃の全体像が見えにくくなり、攻撃手段の特定が難しくなります。

フィッシング詐欺メール → 感染した動画 → 偽のビデオ コーデック → Stegware Polyglot → スケジュール タスク → 感染したパケット → PowerShell スクリプト → インメモリー → ランサムウェア

多面的な攻撃

攻撃者は複数の手段を組み合わせて攻撃を仕掛けてきます。たとえば、ランサムウェアを煙幕として使い、クリプトジャッキング、フィッシング詐欺、ファイルレス、ステガノグラフィーなどを一連の攻撃として実行します。

再利用可能なコンポーネント

攻撃者は、複数の脅威を連携させるため、基盤、キット、再利用可能な脅威コンポーネントを開発しています。

1 つの攻撃を防ぐだけでは不十分

1 つの脅威に対応するだけで攻撃を検出したり、問題を修復することはできません。攻撃を 1 つのカテゴリに分類してしまうと、全体像を見失い、効果的な対策を実施できなくなります。

クラウドを狙うデータ侵害攻撃

より多くのデータが盗まれる

複数のクラウド モデル（SaaS、PaaS、IaaS）を採用する企業が増え、クラウド上に存在するデータも増大しています。攻撃者もこのような動向を見逃しません。クラウド サービスを狙った攻撃が増加するでしょう。

機密情報

『McAfee Cloud Adoption and Risk Report』によると、クラウド上に保管されている**データの 21%** は、知的財産、顧客情報、個人情報などの機密データです。

MITM 攻撃

GhostWriter: **クリプトジャッキングやランサムウェア攻撃を実行するため、**クラウド ネイティブの仲介者攻撃を実行しました。

Office 365 が標的に

KnockKnock: Office 365 を採用する企業の増加に伴い、Office 365、特にメールを狙った攻撃が急増しています。たとえば、**KnockKnock ボットネットは多要素認証を使用していないシステム アカウントを標的にしました**。

音声制御のデジタル アシスタント

家庭への新たな侵入口

家庭内の IoT 機器を管理する音声制御のデジタル アシスタントが増えています。ここがホーム ネットワークへの新たな侵入口として狙われる可能性があります。

スマートフォンで接続

マルウェアの作成者は、パスワード クラッキングや脆弱性の悪用により、スマートフォンやタブレットから IoT 機器を乗っ取ろうとします。

信用済みデバイス

信頼されたデバイスが送信元のため、不審なトラフィックには見えません。攻撃経路の特定はさらに難しくなります。

音声でトリガー

バックドアを開いて指令サーバーに接続するなどの攻撃がユーザーの音声コマンド（「音楽を再生して」、「今日の天気は？」）で開始する可能性があります。

ボットネットの予備軍

感染した IoT 機器がボットネットに組み込まれ、DDoS 攻撃や個人情報の窃盗に利用されます。

ID プラットフォームとエッジ デバイスへの攻撃

大規模な ID プラットフォームでは、IT 環境のユーザー、デバイス、サービスの認証と承認が一元管理されています。このようなプラットフォームを犯罪者は見逃しません。

ソーシャル メディア

プラットフォーム プロバイダーもセキュリティの強化に努めていますが、このデータの宝庫を諦めるサイバー犯罪者はいないようです。この領域の戦いは激しさを増すでしょう。

エッジ デバイス

ネットワーク対応のシステム ハードウェアや IoT 製品に組み込みのプロトコルでは、静的なパスワードが使用され、セキュリティ機能が限定されています。エッジ デバイスに対するリモートからの攻撃は今後も続くでしょう。

信頼モデルの破壊

IoT の信頼モデルは、信頼と境界のセキュリティを前提として脆弱な基盤の上に成り立っています。多くの IoT エッジ デバイスには自己防御機能が搭載されていません。侵入に成功すれば、乗っ取るのは簡単です。

システムの保護

このような激化する環境を保護するには、多要素認証と ID インテリジェンスが不可欠になります。

企業に関する偽情報の増加

ソーシャル メディアを利用して企業にフェイクニュースを配信したり、強請りを行う国家組織や犯罪グループが増えるでしょう。

ミスリードするコンテンツ

ボットネット アカウントは多くのメッセージを散布します。このメッセージが賛否両論の議論を巻き起こすことも少なくありません。ブランドを傷つけるメッセージを散布すると企業を強請る可能性もあります。

急速な拡散

他のボットと同様に、279 のフォロワーを持つ 1 つのボット アカウントが組織への攻撃を開始しました。このボット アカウントは、不正なコンテンツをツイートすることで、フォロワー数をわずか 4 週間で 1,500 以上に増やしました。

詳細については、『McAfee Labs 脅威予測レポート』をご覧ください。レポートの完全版は www.mcafee.com/2019Predictions をご覧ください。

McAfee
Together is power.

2018 年 12 月