【プレスリリース】

マカフィー株式会社
2021 年 1 月 26 日

※当資料は、米国時間 2021 年 1 月 13 日に米国で発表された参考資料の抄訳を基に編集しています。

マカフィー、2021 年の脅威動向予測を発表

主な予測：
- 増殖するサプライチェーンバックドア技術
- 家をハッキングしてオフィスをハッキング
- クラウドプラットフォームへの攻撃が高度に進化
- 新たなモバイル決済詐欺
- Qshing：ウィズコロナ時代の QR コードの乱用
- 攻撃経路として悪用されるソーシャルネットワーク

マカフィー株式会社は、2021 年に注意すべき重要なセキュリティ動向を解説する「2021 年 脅威予測レポート」を発表しました。昨年末、サプライチェーンが新たに注目すべき攻撃経路であることが明らかになりました。世界で外出自粛を余儀なくされる状況下において、家でのデジタルの利用が増加し、攻撃の標的とされる機会が増加しました。それにより、感染したデバイスやアプリを経由して、企業までもがリスクにさらされる可能性も出てきました。また、モバイル決済サービスを介した攻撃や、QR コードを悪用した攻撃にも注意する必要があると予測しています。

米国マカフィーのチーフサイエンティストであるラージ・サマニ（Raj Samani）は、次のように述べています。「2020 年は歴史的なパンデミックの中、私たちは前例のない規模でリモートワークへと移行することになり、COVID-19 に便乗した脅威を活発化させる攻撃者が目立った年となりました。我々、マカフィーは今後数か月だけでなく、数年後に直面するであろうサイバー脅威にも目を向け、日々、脅威対策の研究、開発に注力しています」。

増殖するサプライチェーンバックドア技術

2020 年 12 月 13 日、国家の関与が想定される攻撃者が SolarWinds の Orion IT 監視・管理ソフトウェアを侵害し、SUNBURST と呼ばれる悪意あるソフトウェアバックドアを米国政府機関などに配信していたことが明らかになりました。これにより、攻撃者は政府間通信から国家機密に至るまで、あらゆる種類の情報を盗み、悪用することが可能になりました。本キャンペーンは「警鐘を鳴らすべき攻撃」とされ、初の大規模サプライチェーン攻撃となりました。このようなサプライチェーンのサイバー攻撃への活用は、攻撃に対する防御を検討する方法を変化させました。

この種の攻撃は、家電会社を侵害することで、高度に相互接続された現代の家庭に存在するテレビ、仮想アシスタント、スマートフォンなどのスマートアプライアンスへのアクセスを悪用して情報を搾取することを可能にします。ユーザーが自宅からリモートで作業している際に情報を盗まれたり、企業を攻撃するためのゲートウェイとして悪用することが可能になり、個人やその家族にも脅威をもたらします。マカフィーは SUNBURST キャンペーンの発見により、世界中の他の攻撃者が今後、同様の攻撃手法を用いたセキュリティ事案が明らかになると予測しています。

家をハッキングしてオフィスをハッキング

COVID-19 の世界的大流行により在宅勤務が常態化し、“家”が職場へと変化しました。McAfee Secure Home Platform デバイスの監視によると、世界中で接続されているホームデバイスの数が 22%増加し、米国では 60%増加しました。デバイスからのトラフィックの 70%以上は、スマートフォン、ラップトップ、その他 PC および TV から発信され、29%以上は、ストリーミングデバイス、ゲーム機、ウェアラブル端末、スマートライトなどの IoT デバイスから発信されていました。攻撃者は通信チャネル全体にさまざまなフィッシングメッセージ施策を急増させ、マカフィーがブロックしたフィッシングのリンク数は、昨年 3 月から 11 月にかけて 21%を超え、1 世帯あたり平均 400 超となりました。

エンタープライズレベルでのセキュリティ対策が施され、「強化」されたデバイスで満たされたオフィス環境とは対照的に、ホームデバイスの多くは、製造元が新しい脅威や脆弱性に対処するセキュリティアップデートで適切にサポートできていないという点において、「孤立」しているのが実状です。このため、攻撃者は家を家族だけでなく企業を標的とした攻撃対象領域と考え始めました。攻撃者は、定期的なファームウェアアップデートの欠如、攻撃対応機能の欠如、脆弱なプライバシーポリシー、脆弱性などを悪用します。このような状況下、2021 年、攻撃者は企業および個人向けデバイスに対してさまざまな攻撃を仕掛けることが予測されます。

クラウドプラットフォームへの攻撃が高度に進化

COVID-19 の世界的大流行に伴い、企業のクラウド移行が加速しました。世界中の 3,000 万人を超える McAfee MVISION Cloud ユーザーからの集積データの分析結果から、2020 年の最初の 4 カ月間において、エンタープライズクラウド使用量が全体で 50%増加したことが明らかになりました。すべてのクラウドカテゴリで増加が見られ、 Microsoft O365 が 123%増加し、Salesforce などのビジネスサービスの使用が 61%増加、Cisco Webex（600%増）、Zoom（350%増）、Microsoft Teams（300%増）、Slack（200%増）などのコラボレーションサービスが大きく成長を遂げました。またエンタープライズクラウドにアクセスする管理されていないデバイスが 100%増加するなど、ホームネットワークが企業ネットワークの範疇に組みこまれつつあることが読み取れます。これにより、何千もの異種ホームネットワークに対する攻撃の効果を高めるために、高度に機械化された広範囲に渡る新たな攻撃が開発されることが予測されます。

また、企業のクラウド利用が成熟し、クラウド間を移動する機密データの量が増加する一方で、攻撃者は特定の企業、ユーザー、およびアプリケーション向けに高度にターゲットを絞ったエクスプロイトの作成を余儀なくされると予測しています。CapitalOne のデータ侵害のケースでは、攻撃は完全にクラウドネイティブで、クラウドアプリケーション（およびインフラストラクチャ）全体の多くの脆弱性と設定ミスが悪用されて連鎖しているという点で高度且つ複雑でした。

今後数カ月から数年のうちに、攻撃者がレバレッジを効かせることで、これらの方法を基にデバイス、ネットワーク、クラウド全体にさらなる脅威が現れると予測しています。

新たなモバイル決済詐欺

モバイル決済の浸透が進む中、2020 年の Worldpay Global Payments Report（英語）は支払いの 41%がモバイルデバイスで行われていると推定し、2023 年までの予測ではクレジットカードやデビットカードに代わり増加すると予想されています。Allied Market Research による 2020 年 10 月の調査では、世界のモバイル決済市場の規模は 2019 年に 1.48 兆ドルと評価され、2027 年までに 12.06 兆ドルに達すると予測されており、2020 年から 2027 年までの複合年間成長率は 30.1%です。攻撃者たちも、金銭を搾取する対象を PC ブラウザやクレジットカードからモバイル決済へと移行を進め、RSA の詐欺およびリスクインテリジェンスチームの調査（英語）によると、2019 年の第 4 四半期にサイバー詐欺活動の 72%がモバイルチャネルに関係していることが判明しました。研究者たちは、

ほぼ 2 年間でモバイルアプリに関連する詐欺の割合が最も高くなり、PC 上の Web ブラウザに関連する詐欺からのシフトを確認しています。

マカフィーは、フィッシングメッセージやスミッシングメッセージを決済用 URL と組み合わせる「受信」ベースのモバイル決済の脅威が増加すると予測しています。攻撃者が製品の返品とサービス詐欺を行うための偽のコールセンターを設置し、電子メールまたは SMS でリンクを送信し、モバイル決済アプリを介して偽の払い戻しを提供するスキームです。ユーザーは実際には払い戻しを受けるのではなく、支払いに同意することになり、そのことに気づかず結果的にだまされてしまいます。マカフィーは、攻撃者にとって技術の向上が詐欺行為での利便性も向上させると予測しています。

Qshing：ウィズコロナ時代の QR コードの乱用

パンデミックの時代において、特に QR コードはレストランからパーソナルケアサロン、フィットネススタジオに至るまで、あらゆる環境で企業と消費者の直接的な接触を避ける際に活用されています。MobileIron による 2020 年 9 月の調査（英語）では、69%が悪意ある URL を識別できると回答しているのに対し、悪意ある QR コードを識別できると回答した回答者は 37%に留まっています。また、QR コードが支払いを行ったり、ユーザーにソーシャルメディアで誰かをフォローさせたり（22%）、電話をかけたり（21%）できることを認識しているのは 3 分の 1 未満（31%）です。QR コードがどのように機能するかについてのユーザーの知識が不足しているため、QR コードは攻撃者にとって有用なツールになっています。QR コードは過去にフィッシングで使用され、フィッシング対策ソリューションが電子メール内の悪意ある URL を識別しようとする試みの回避に悪用されました。

マカフィーは、攻撃者が QR コードを活用し、ソーシャルエンジニアリングの手法と組み合わせ、攻撃を拡大すると予測しています。

攻撃経路として悪用されるソーシャルネットワーク

マカフィーでは、LinkedIn、What's App、Facebook、Twitter といったソーシャルネットワークを使用して、従業員と関係を築いた上で侵害する、より高度な攻撃者に注目しています。攻撃者は標的を通して、彼らの勤務先である企業や組織を危険にさらします。マカフィーは、2021 年以降、この攻撃経路の使用が拡大すると予測しています。APT34、Charming Kitten、Threat Group-2889（その他）などの著名な攻撃者は、特定の被害者タイプに向けてカスタマイズしたコンテンツを有効にするメディアの効力を活かして、ターゲットを絞った攻撃を行うことが確認されています。オペレーション ノーススターは、この種の最先端の攻撃です。 2020 年 8 月にマカフィーによって発見されたこの攻撃キャンペーンは、ソーシャルメディアの緩いプライバシー管理、偽の LinkedIn ユーザーアカウントの作成と使用の容易さ、および職務記述書を使用し防衛関連企業の従業員をだまし攻撃する手法を明らかにしました。

企業は、自社で調達して提供したデバイスに対するセキュリティを制御し、従業員のデバイスが企業の IT 資産にアクセスする方法に制限を課していますがソーシャルネットワーク プラットフォームでのユーザーアクティビティは、現在、同じ方法で監視または制御は行われていません。マカフィーは、ソーシャルネットワーク プラットフォームの悪用が、特に最先端の攻撃者の間でより一般的になると予測しています。

マカフィーについて
マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。
詳細は https://www.mcafee.com/enterprise/ja-jp/home.html をご覧ください。

＜本情報のお問い合わせ＞
マカフィー株式会社（ https://www.mcafee.com/enterprise/ja-jp/home.html ）
広報担当 戸田
Tel: 070-2680-0731
hiromi_toda@mcafee.com

マカフィー広報担当
ウィタンアソシエイツ 担当：中根／桑村
mcafee-pr@witan.co.jp