【プレスリリース】

マカフィー株式会社
2020 年 8 月 12 日

※当資料は、米国時間 2020 年 7 月 21 日に米国で発表されたプレスリリースの抄訳です。

マカフィー、COVID-19 脅威レポートを発表
パンデミック下の攻撃者の進化が明らかに

ニュースハイライト

- サイバー犯罪者はパンデミックを利用して世界中のシステムに侵入
- サイバー犯罪者は暗号化前のデータを盗むようになり、ランサムウェア攻撃の対象がデータ侵害にまで拡大
- 新たな PowerShell マルウェアは 689%増加し、総数は過去 1 年間で 1,902%増に
- インシデント（公開済）を業種別にみると、公共が 73%増、個人が 59%増、教育が 33%増
- セキュリティインシデント（公開済）の約 47%が米国で発生
- クラウドサービスを標的とする脅威が 630%増加し、多くが Microsoft 365 などのコラボレーションサービスに集中

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ある米国マカフィー（McAfee LLC、本社：米国カリフォルニア州）は、*「McAfee COVID-19 脅威レポート：2020 年 7 月」（英語）*を発表しました。最新のレポートでは、2020 年第 1 四半期における新型コロナウイルス感染症（COVID-19）に関連したサイバー犯罪とサイバー脅威の進化について分析しています。McAfee Labs は、1 分あたり平均 375 件の新たな脅威を検出しており、サイバー犯罪者がパンデミック（感染症の世界的大流行）を悪用して COVID-19 を騙る悪意あるアプリ、フィッシング攻撃、マルウェアなどの事例が急増していることを確認しました。新たな PowerShell マルウェアは第 1 四半期中に 688%増加し、総数は過去 1 年間で 1,902%増加しました。公共、個人、教育、製造を標的としたインシデントが増加し、セキュリティインシデント（公開済）の約 47%が米国で発生しています。

マカフィーのフェロー兼チーフサイエンティストのラージ・サマニ（Raj Samani）は、次のように述べています。「これまでのところ、2020 年の脅威動向の主なテーマは、パンデミックを好機とみたサイバー犯罪者の迅速な適応と、サイバー攻撃がもたらす甚大な影響です。最初はわずかなフィッシング攻撃と散発的な悪意あるアプリを確認する程度でしたが、突然、悪意ある URL が大量にあふれ出し、高度なスキルを持つ攻撃者たちが出現しました。世界中が COVID-19 に関する情報を得ようと躍起になる中、これをシステムへの侵入メカニズムとして利用し始めたのです。」

マカフィーは、徹底した研究、調査分析、および、McAfee® Global Threat Intelligence クラウドが世界中の 10 億超のセンサーを通じて、多様な攻撃経路から収集した脅威データに基づき、サイバー脅威の動向を四半期ごとに検証しています。

高度なスキルを持つ攻撃者がパンデミックを悪用

マカフィーの研究者は、COVID-19 を利用した攻撃の典型的な例として、検査、診療、治療、リモートワークといったトピックを含むパンデミック関連のテーマを誘い水にして、悪意あるリンクをクリックさせたり、ファイルをダウンロードさせたり、PDF ファイルを閲覧させたりしていることを確認しました。これらの攻撃を追跡するために、McAfee Advanced Programs Group（APG）は

COVID-19 Threat Dashboard を公開しました。これには、パンデミックを利用した脅威度の高い攻撃、最も標的となった業種や国、最も使用された脅威の種類と規模が表示されています。ダッシュボードは毎日午後 4 時（米国東部時間）に更新されます。詳細については、McAfee APG COVID-19 Threat Dashboard をご覧ください。

McAfee APG の責任者であるパトリック・フリン（Patrick Flynn）は、次のように述べています。「サイバーセキュリティは定型のアプローチでは解決できません。組織はそれぞれ固有であり、特定のインテリジェンス要件と目的を持っています。マカフィーの COVID-19 Threat Dashboard は、データを利用して有益な分析インテリジェンスを作成します。これにより、ユーザーは脅威を理解し、潜在的な脅威が武器化する前に把握することができます。」

データ侵害：新しいランサムウェア攻撃

McAfee Advanced Threat Research（ATR）は、2020 年第 1 四半期中に悪意ある攻撃者が、製造、法曹、建設といった可用性と完全性が重要な業界に照準を合わせていることを確認しました。

マカフィーの上席プリンシパルエンジニア兼リードサイエンティストのクリスチャン・ビーク（Christiaan Beek）は、次のように述べています。「これらの攻撃を単にランサムウェア攻撃と呼ぶことはできなくなりました。攻撃者はネットワークにアクセスし、暗号化前のデータを盗み、カネを払わなければ情報を漏洩すると脅してきます。これはデータ侵害です。保護が脆弱なリモートデスクトッププロトコルや、闇市場で入手したアカウントの盗難認証情報を使用して、攻撃者が瞬く間に被害者のネットワークを認識し、効率的にデータを盗み、暗号化していることが判明しました。」

第 1 四半期中に新たなランサムウェアは 12%減少しましたが、過去 1 年間でランサムウェアの総数は 32%増加しました。

2020 年第 1 四半期の脅威動向

マルウェア全般　新たなマルウェアのサンプルは 35%減少しました。一方、過去 1 年間でマルウェア総数は 27%増加しました。Mac OS の新たなマルウェアサンプルは 51%増加しました。

モバイルマルウェア　新たなモバイルマルウェアは 71%増加し、過去 1 年間のモバイルマルウェアの総数は約 12%増加しました。

地域別動向　南北アメリカで起きたインシデント（公開済）は 60%増加し、アジア太平洋では 27%増加する一方、欧州では 7%減少しました。

セキュリティインシデント　McAfee Labs の調べでは、セキュリティインシデント（公表済）は 458 件あり、第 4 四半期から 41%増加しました。公開されたすべてのセキュリティインシデントのうち、50%は北米、続いて欧州では 9%となりました。国別では、米国が 47%近くを占めています。

産業別動向　インシデント（公表済）を業界別にみると、公共は 73%、個人は 59%、教育は 33%、製造は 44%とそれぞれ増加しました。

攻撃経路　全体として、マルウェアはまず公開された攻撃経路から侵入し、アカウントのハイジャックや標的型攻撃を実行していました。

仮想通貨マイニング　新たな仮想通貨マイニングマルウェアは 26%増加しました。仮想通貨マイニングマルウェアのサンプル総数は、過去 1 年間で約 97%増加しました。

ファイルレスマルウェア　新たな JavaScript マルウェアは約 38%減少し、過去 1 年間ではマルウェア総数は約 24%増加しています。新たな PowerShell マルウェアは前四半期比で 689%増加し、過去 1 年間でマルウェア総数は 1,902%増となりました。

IoT　新たなマルウェアサンプルは約 58%増加しました。過去 1 年間の IoT マルウェア総数は 82%増加しました。

参考情報:

- McAfee COVID-19 Report: July 2020（英語）
- McAfee COVID-19 Threat Dashboard
- McAfee Advanced Threat Research
- McAfee Advanced Programs Group（英語）

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/ja-jp/ をご覧ください。

McAfee テクノロジーの機能と特徴はシステム構成に依存し、有効なハードウェア、ソフトウェア、またはサービスのアクティベーションが必要になる場合があります。

＜本情報のお問い合わせ＞

マカフィー株式会社（ https://www.mcafee.com/ja-jp/ ）
広報担当 戸田
東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20 階
Tel: 070-2680-0731 Fax: 03-5428-1480
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：住川／中根
mcafee-pr@witan.co.jp