【プレスリリース】

マカフィー株式会社
2019 年 8 月 29 日

※当資料は、米国時間 2019 年 8 月 28 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、2019 年第 1 四半期の脅威レポートを発表

McAfee Labs は 2019 年第 1 四半期において毎分 504 件の新たな脅威を検出、データ漏えいは大規模企業への攻撃が増加、ランサムウェアが再流行

ニュースハイライト

- 新たなランサムウェアが 118%増、サイバー犯罪者は新たな戦略と革新コードを利用
- 20 億以上の盗難アカウント情報がサイバー犯罪者の闇市場で入手可能
- 標的型攻撃は初期段階でスピアーフィッシング、攻撃実行段階でユーザーに依存
- 新たな仮想通貨マイニングマルウェアは 29%増、CookieMiner マルウェアは Apple ユーザーを標的に
- 新たな PowerShell マルウェアは 460%増、開発者は新しい技術を試行
- アジア太平洋地域を標的とするインシデント（公開済）が 126%増

米国マカフィー（McAfee LLC、本社：米国カリフォルニア州）は、最新の 2019 年第 1 四半期の脅威レポート「McAfee Labs 脅威レポート：2019 年 8 月」を発表しました。

最新のレポートでは、サイバー犯罪活動とサイバー脅威の進化について分析しています。McAfee Labs は第 1 四半期に 1 分あたり平均 504 件の新たな脅威を検出しており、ランサムウェアの再流行とサイバー攻撃の実行とコードの変化を確認しました。22 億以上の盗難アカウント情報が、サイバー犯罪者の闇市場で入手可能でした。標的型攻撃の 68%は初期段階にスピアーフィッシングを利用し、77%はユーザー側の行動に依存したサイバー攻撃でした。

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。「これらの脅威の影響は無視できるものではありません。特定の種類の攻撃が増加または減少したという数値だけでは、この事象のほんの一部しかわからないことを認識すべきです。どんな『感染』でも、機能停止や大規模な詐欺に対処する必要が生じます。どんなサイバー攻撃であっても人的負荷が生じることを忘れてはいけません。」

マカフィーは徹底的な調査と分析、世界中の複数の脅威の経路にある 10 億を超えるセンサーから McAfee® Global Threat Intelligence（McAfee GTI）Cloud が集めた脅威データを基に、四半期ごとにサイバー脅威情勢を分析しています。

ランサムウェアの再流行が特徴付けるコード革新とサイバー攻撃の新しい戦略

McAfee Advanced Threat Research（ATR）は、初期のアクセス経路やサイバー攻撃管理における変化、コードの技術革新によって、ランサムウェアによるサイバー攻撃において大きな変化を確認しました。

スピアーフィッシングは依然として多く利用されている一方、ランサムウェア攻撃は、リモートデスクトッププロトコル（RDP）などの公開されたリモートアクセスポイントを標的とする傾向が高まりました。これらの認証は、ブルートフォース攻撃によって解読されるか、サイバー犯罪者の闇

市場で入手できます。RDP 認証は、企業ネットワーク上でマルウェアを配布および実行するための完全な権限を与える管理者権限の取得に使用されます。

マカフィーの研究者は、コマンド・アンド・コントロール（C2）サーバーをセットアップする従来のアプローチとは異なり、サイバー攻撃を管理するために匿名の電子メールサービスを使用するランサムウェア攻撃の背後にいる攻撃者も観察しています。関係機関と民間パートナーは通常 C2 サーバーを探し復号化キーを取得し、回避ツールを作成します。したがって攻撃者は、電子メールサービスの使用が犯罪ビジネスを行うための匿名性をより高める方法だと認識しています。

この四半期で最も活発なランサムウェアファミリーは、Dharma（Crysis としても知られる）、GandCrab、および Ryuk とみられます。この四半期で注目すべき他のランサムウェアファミリーには、広範囲に拡散させる以前に McAfee ATR が明らかにした Anatova や、定期的に新しい亜種が発見されているランサムウェアファミリーである Scarab があります。全体として、新しいランサムウェアのサンプル数は 118%増加しました。

マカフィーのリードサイエンティスト兼上席プリンシパルエンジニアのクリスチャン・ビーク（Christiaan Beek）は、次のように述べています。「2018 年末、新しいファミリーと開発の周期的減少の後、2019 年第 1 四半期は、コードの革新とより標的を絞った新たなアプローチのランサムウェアが再び活性化しました。身代金の支払いは、サイバー犯罪ビジネスを支援し、攻撃を持続させます。ランサムウェアの被害者は別のオプションも選択できます。暗号化解読ツールとサイバー攻撃情報は、『No More Ransom プロジェクト』（https://www.nomoreransom.org/ja/index.html）などのツールの活用をお勧めします。」

2019 年第 1 四半期の脅威動向

- **攻撃経路：**攻撃経路はマルウェアが最も多く、続いてアカウントの乗っ取り、標的型攻撃が続いています。

- **仮想通貨マイニング：**新しい仮想通貨マイニングマルウェアは 29%増加しました。McAfee ATR は CookieMiner マルウェアが Apple ユーザーを標的にし、ビットコインウォレットの認証を入手しようと試みていたことを確認しました。また、マルウェアはパスワードとブラウジングデータにもアクセスしていました。仮想通貨マイニングマルウェアの合計サンプル数は過去 1 年間で 414%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 13%減少する一方、過去 1 年間のマルウェアの合計サンプル数は 62%増加しました。新たな PowerShell マルウェアは、ダウンローダースクリプトの使用により 460%の増加となりました。マルウェアの合計サンプル数は過去 1 年間で 76%増加しました。

- **IoT：**サイバー犯罪者は引き続き、IoT デバイスの不十分なセキュリティ対策を悪用していました。新たなマルウェアサンプルは 10%増加し、IoT マルウェアの合計サンプル数は過去 1 年間で 154%増加しました。

- **マルウェア全体：**新たなマルウェアサンプルは 35%の増加でした。一方、新たな Mac OS マルウェアサンプルは 33%減少しました。

- **モバイルマルウェア：**新たなモバイルマルウェアのサンプルは 15%の減少となり、マルウェアの合計サンプル数は過去 1 年間で 29%増でした。

- **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 412 件あり、第 4 四半期から 20%増加しました。公開されているすべてのセキュリティインシデントのうち、32%が南北アメリカで、続いて欧州とアジア太平洋がそれぞれで 13%となりました。

- **地域別動向：**インシデント（公開済）でアジア太平洋地域を標的にしたものは 126%増加し、南北アメリカを標的にしたものは約 3%減少、欧州を標的にしたものは約 2%減少しました。

- **産業別動向：**インシデント（公開済）で個人に影響を与えるものは 78%と急増したほか、教育機関が 50%増、医療機関が 18%増、公共機関は 10%減、そして金融機関が 89%増でした。

- **標的型攻撃：**マカフィーは、攻撃を成功させるために必要なデータ偵察を最小化した多数のサイバー攻撃を特定しました。攻撃者は主に政府や行政機関の大規模組織に焦点を当て、金融、化学、防衛、教育の各機関がそれに続きました。
スピアーフィッシングにより初期アクセスが成功したのは攻撃全体の 68%で、攻撃実行においてユーザーの特定のアクションに依拠したものは 77%ありました。

- **闇市場：**この四半期中に、サイバー犯罪者の闇市場では、22 億以上の盗難アカウント情報が、入手可能でした。最大の闇市場である「Dream Market」は、多数の分散型サービス拒否（DDoS）攻撃のため、閉鎖する計画を発表しました。法執行機関は、約 7 万台のハッキングされたマシンへのアクセスを販売したとして、最大の RDP ショップの 1 つである xDedic を検挙し、事業を閉鎖させました。

『McAfee Labs Threats Report: August 2019（McAfee Labs 脅威レポート：2019 年 8 月）』のレポート全文（英語）は以下からダウンロードが可能です。
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

参考情報：
- McAfee Advanced Threat Research

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 Labs および Advanced Threat Research
McAfee Labs および McAfee Advanced Threat Research は、主な攻撃経路上（ファイル、Web、メッセージ、ネットワーク）に配置されている 10 億を超えるセンサーからのデータに基づく、脅威に関するリサーチ、知見やサイバーセキュリティの有識者として、業界をリードしています。

＜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: 03-5428-1226 Fax: 03-5428-1480
hiromi_toda@mcafee.com