【プレスリリース】

マカフィー株式会社
2021 年 7 月 6 日

※当資料は、米国時間 2021 年 6 月 24 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、2021 年 第 1 四半期 脅威レポートを発表

RaaS、暗号通貨、IoT への脅威の急増を確認

ニュースハイライト：

- 収益性の低い標的を狙った拡散型攻撃から、より収益性の高い標的に絞った攻撃へとシフト
- 64-bit のコインマイナーアプリケーションの増加により、暗号通貨のコインマイナーマルウェアが 117%増加
- IoT デバイスを狙うマルウェア「Mirai」の新種により、IoT と Linux への脅威が増加
- 新たに検出されたマルウェアの脅威は全体で平均毎分 688 件

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 Corp、本社：米国カリフォルニア州、Nasdaq：MCFE）は、「McAfee 脅威レポート：2021 年 6 月」を発表しました。最新のレポートでは、2021 年第 1 四半期におけるマルウェア関連のサイバー犯罪活動とサイバー脅威の進化を分析しています。同四半期にサイバー犯罪者は、収益性の低い標的を狙った広範囲なランサムウェア攻撃キャンペーンから、収益性の高い大規模組織を狙った、少数のカスタマイズされた RaaS（Ransomware as a Service）を利用した攻撃手法にシフトしました。暗号通貨を生成するコインマイナーマルウェアは、64-bit のコインマイナーアプリケーションの普及により 117%増加しました。さらに、Mirai マルウェアの新種の急増により、IoT（55%）と Linux（38%）システムを標的としたマルウェアが増加しました。

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。「サイバー犯罪者は、複雑さやリスクを最小限に抑えて金銭的な利益を最大化するために、あらゆるツールを組み合わせ、手口を常に進化させています。当初は、ランサムウェアを使って何百万人もの個人から少額の身代金を引き出す手口が確認されていましたが、現在では、組織を人質に取り、多額の身代金をだまし取る策略をサポートする RaaS が多く存在しています。」

マカフィーは、徹底した研究、調査分析、世界中の様々な脅威経路における 10 億超のセンサーを通じて McAfee Global Threat Intelligence クラウドに収集された脅威データに基づき、サイバー脅威の状況を四半期ごとに評価しています。

ランサムウェア

第 1 四半期にランサムウェアが半減したのは、攻撃者が同じサンプルで多くのターゲットを攻撃する広範囲な攻撃キャンペーンから、少数の大規模な組織を狙い、独自のサンプルを使う攻撃手法に移行したことが一因です。1 種類のランサムウェアで多くの被害者を感染させ、支払いを要求する攻撃キャンペーンは、やがて数多くのシステムが悪名高い「ノイズ」として認識して防御するようになります。RaaS のアフィリエイトネットワークは、攻撃者が独自の攻撃を仕掛けられるようにすることで、大企業のサイバー防衛システムに検知されるリスクを最小限に抑え、被害者を無力にし

て多額の身代金を要求できるようにしました。この変化は、2021 年 1 月には 19 種類あった有名なランサムウェアファミリーが 2021 年 3 月には 9 種類に減少していることにも表れています。

DarkSide と呼ばれる RaaS グループの攻撃が 2021 年第 2 四半期に発覚し、注目を集めましたが、第 1 四半期に最も検出されたのは REvil であり、RansomeXX、Ryuk、NetWalker、Thanos、MountLocker、WastedLocker、Conti、Maze、Babuk の亜種が続きました。

コインマイナーマルウェア

人目を引いたランサムウェア攻撃の一方で、犯罪者がランサムウェアを用いて暗号通貨での支払いにより収益化する方法に注目が集まっています。第 1 四半期に暗号通貨を生成するコインマイナーマルウェアが 117%に急増したのは、64-bit のコインマイナーアプリケーションの急増が要因と考えられます。

コインマイナーマルウェアは被害者のシステムをロックし、暗号通貨による身代金の支払いが完了するまで人質にするのではなく、侵害したシステムに感染し、そのシステムの処理能力を利用して暗号通貨を密かに生成し、この攻撃キャンペーンを企てて実行したサイバー犯罪者に渡します。サイバー犯罪者にとっての利点は、加害者と被害者間のやり取りの必要性が全くない点です。また、被害者のコンピュータがコインマイニングの作業負荷によって通常よりも動作が遅くなる可能性がありますが、被害者は自分のシステムが犯罪者のために金銭的な価値を生み出していることに気づくことはありません。

サマニは次のように続けます。「ランサムウェアとコインマイナーの動向から得られる教訓は、暗号通貨の使用制限や違法にする必要があるということではありません。サイバー犯罪の歴史から何かを学んだとすれば、犯罪者は、自分のツールや技術を改善し、政府の規制を回避し、常に防衛者の一歩先を行くことで、防衛者の努力に対抗するということです。もし、暗号通貨を制限しようとする動きがあれば、犯罪者は犯罪を収益化するために新たな手法を開発するでしょうし、彼らが利益を得続けるためには、政府の 2、3 歩先を行くだけで良いのです。」

脅威と被害者

- **マルウェア：**2021年第1四半期に1分あたり平均688件の新しい脅威を確認しました。これは、2020年第4四半期に比べ、1分あたり40件の増加となります。

- **IoTとLinuxデバイス：**第1四半期は、Miraiマルウェアのさまざまな新種が、IoTとLinuxのマルウェアカテゴリで増加しました。Moobotファミリー（Miraiの亜種）はMiraiの複数の亜種で構成されており、大量に拡散していることが確認されています。これらの亜種は、DVR、ウェブカメラ、インターネットルーターなどのIoT機器の脆弱性を狙っています。感染すると、マルウェアはシステム内に隠れ、攻撃の次の段階のマルウェアをダウンロードし、コマンド&コントロール・サーバー（C2）に接続します。感染したIoTデバイスがボットネットに接続されると、DDoS攻撃に協力させるために乗っ取られることがあります。

- **産業別動向：**マカフィーの調査によると、2021 年第 1 四半期にテクノロジー業界を標的としたインシデント（公開済）が 54%増となったことが確認されました。続いて教育が 46%、金融・保険が 41%増加しました。一方、卸売・小売が 76%、公共部門が 39%減少しました。

- **地域別動向：**セキュリティインシデントは、アジアでは 54%、ヨーロッパでは 43%急増し、北米では 13%減少しました。米国ではインシデント（公開済）が 14%減少しましたが、一方、フランスでは 84%、英国では 19%増加しました。

参考情報：

- **McAfee Labs Threats Report : June 2021**（英語）
- **MVISION Insights Public View**（英語）
- **McAfee Threat Center**

McAfee Labs と Advanced Threat Research について

McAfee Labs と マカフィーの Advanced Threat Research（ATR）チームは、脅威調査、脅威インテリジェンス、サイバー セキュリティに関する世界有数の情報ソースです。McAfee Labs と McAfee Advanced Threat Research（ATR）チームは、ファイル、Web、メッセージ、ネットワークなど、主要な脅威ポイントに配置された数十億のセンサーから脅威データを収集しています。そして、それら脅威ポイントから収集された脅威インテリジェンス、重要な分析結果、専門家としての見解をリアルタイムで配信し、より優れた保護とリスクの軽減に取り組んでいます。

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。

*McAfee、マカフィー、McAfee のロゴは、米国およびその他の国における米国法人 McAfee, LLC またはその関連会社の商標又は登録商標です。
*その他の会社名、製品名やブランドは、該当各社の商標又は登録商標です。

＜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