【プレスリリース】

マカフィー株式会社
2020 年 11 月 17 日

※当資料は、米国時間 2020 年 11 月 5 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、新型コロナウイルス関連の脅威と PowerShell マルウェアの急増を確認
2020 年第 2 四半期 脅威レポートを発表

ニュースハイライト

- 2020 年第 2 四半期、新型コロナウイルス関連のサイバー攻撃の検出が前四半期比 605%に
- 悪意ある Donoff ドキュメントの急増で、PowerShell マルウェアが 117%増
- クラウドサービス利用者への攻撃を約 750 万件確認
- 新しいマルウェアサンプルは 11.5%増、平均で毎分 419 件の脅威が出現
- 新しいコインマイニング アプリケーションの出現により、コインマイニング マルウェアが 25%増
- IoT ボットネットである Gafgyt と Mirai の再活性化により、新たな Linux マルウェアが 22%増
- Android Mobby Adware の急増により、モバイルマルウェアが 15%増
- セキュリティインシデント（公開済）は 22%増。中でも、テクノロジー（科学技術）業界を標的とするインシデントが 91%増

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：2020 年 11 月」を発表しました。最新のレポートでは、2020 年第 2 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。調査では、1 分あたり平均 419 件の新たな脅威を検出し、新たなマルウェアのサンプル数は全体で 11.5%増加しました。悪意ある Donoff Microsoft Office ドキュメント攻撃の激増により、新たな PowerShell マルウェアが 117%増加しました。世界的なコロナ禍において、サイバー犯罪者はパンデミック（感染症の世界的大流行）に関連する話題で被害者を罠にかけたり、在宅勤務が常態化する現状を悪用したりするなど、状況に適応したサイバー攻撃を仕掛けています。

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 年の第 2 四半期には、PowerShell マルウェアなどの革新的な脅威カテゴリで継続的な進化を確認しています。また、サイバー犯罪者が状況に順応して、リモート環境で働く従業員を介して組織を標的としていることが確認されています。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、悪意ある大量の URL があふれ出し、クラウド利用者に対する攻撃が始まりました。腕利きの攻撃者たちは、世界中が COVID-19 に関する情報を得ようと躍起になる中、それをシステムへの侵入口として悪用したのです」。

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配置された10億を超えるセンサーを通じて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。

COVID-19 に便乗したサイバー攻撃

世界がパンデミックに陥った第1四半期に続き、第2四半期では、企業は前例のない大規模な在宅勤務を継続し、この新たな常態に適応するサイバーセキュリティ対策に取り組みました。こうした状況に対応するため、マカフィーはMcAfee COVID-19脅威ダッシュボードを新設しました。悪意ある攻撃者が高度な技巧を使って、新型コロナウイルスに伴う制約やリモートデバイ

スと帯域幅のセキュリティにおける潜在的な脆弱性に対処しようとする企業、政府、学校、従業員にどのように攻撃を繰り返しているかを、最高情報セキュリティ責任者（CISO）とセキュリティ担当者が理解できるよう支援するためです。第2四半期を通じて、10億を超えるセンサーで形成されるマカフィーのグローバルネットワークが検出した新型コロナウイルス関連の攻撃は、前四半期比605%となりました。

Donoff と PowerShell マルウェア

Donoff Microsoft Office ドキュメントは TrojanDownloader として機能し、Windows のコマンドシェルを利用して PowerShell を起動し、悪意あるファイルをダウンロードして実行させます。Donoff が機動力となり PowerShell マルウェアは急増し、2020 年第 1 四半期には 689%増を記録しました。第 2 四半期に入って、Donoff 関連のマルウェアの成長速度は鈍化しましたが、それでも堅調に推移し、PowerShell マルウェアは 117%増となり、全体で 103%増となった新しい Microsoft Office マルウェアの伸びを後押ししました。この動向は、PowerShell の脅威が全体的に増加傾向にあるという背景を踏まえてとらえる必要があります。2019 年から 1 年間で、PowerShell マルウェアのサンプル総数は 1,902%増加しています。

クラウド利用者への攻撃

マカフィーは、クラウド利用者のアカウントに対する外部からの攻撃を約750万件確認しました。これは、2020年第2四半期に3,000万人を超える世界中のMcAfee MVISION Cloud利用者からもたらされた匿名化されたクラウド利用状況データの集計に基づいています。このデータセットは、金融サービス、医療、公共機関、教育、小売、テクノロジー（科学技術）、製造、エネルギー、公益事業、法曹、不動産、輸送、ビジネスサービスなど、世界中の主要産業の企業を網羅しています。

2020 年第 2 四半期の脅威動向

- **マルウェア：**McAfee Labsは、2020年第2四半期に1分あたり419件の新しい脅威を確認しました。これは、第1四半期に比べて約12%増です。ランサムウェアは、2020年第1四半期と同程度でした。

- **コインマイニングマルウェア：**第1四半期に26%増加した新たなコインマイニング マルウェアは、新しいコインマイニング アプリケーションの人気に支えられ、第2四半期は25%増となりました。

- **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、第 1 四半期には 71%増加しましたが、第 2 四半期では Android Mobby Adware の急増にもかかわらず、15%増と鈍化しました。

- **IoT（Internet of Things）**：第 2 四半期、新しい IoT マルウェアは 7%の伸びにとどまりました。ただし、Gafgyt と Mirai の脅威による大規模な活動が確認されており、調査期間において双方とも新たな Linux マルウェアを 22%増加させました。

- **地域別動向**　セキュリティインシデント（公開済）は561件あり、第1四半期から22%増加しました。北米でのインシデント（公開済）は、第1四半期から30%減少しました。このうち、米国では47%減少しましたが、カナダでは25%増加しました。また、英国では29%の増加でした。

- **攻撃経路**　全体として、攻撃経路の中でマルウェアは主要な役割を果たしており、公開済のインシデントの35%を占めています。アカウントハイジャックと標的型攻撃は、それぞれ17%と9%でした。

- **産業別動向**　インシデント（公開済）を産業別にみると、テクノロジー（科学技術）が第1四半期から91%増加しました。製造業のインシデントが10%増加する一方、公共部門は14%減少しました。

参考情報:

- McAfee Labs 脅威レポート（英語）※
- McAfee Threat Center（英語）
- McAfee COVID-19 Threats Dashboard（英語）
  ※日本語版も順次公開を予定しています。

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(Nasdaq: MCFE)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