【プレスリリース】

マカフィー株式会社
2019 年 1 月 16 日

※当資料は、2018 年 12 月 18 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、2018 年第 3 四半期の脅威レポートを発表

仮想通貨マイニングは IoT デバイスを悪用、金融機関ではデータ漏えいが 20%増加

ニュース ハイライト

- サイバー犯罪の地下市場および闇フォーラムを分析し、犯罪者の戦術やターゲットを解明
- IoT デバイスを狙った新しいマルウェアは第 3 四半期だけで 73%増加、通年では 203%増加
- 仮想通貨マイニングマルウェアは 71%増加、セキュリティが手薄な大量の IoT デバイスを悪用
- モバイルマルウェアは 24%減少、偽ゲーム、偽出会い系アプリを悪用したサイバー犯罪が増加
- 金融機関でのデータ漏洩が 20%増加、「トロイの木馬」が銀行を意外なアプローチで攻撃
- スパムボットネットが生み出す性的な Web 閲覧履歴を暴露すると脅迫する「セクストーション（性的脅迫）」詐欺が横行
- ランサムウェアは 10%増加したが、新たなランサムウェア ファミリーは引き続き減少

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 2018 年第 3 四半期の脅威レポート「McAfee Labs 脅威レポート：2018 年 12 月」を発表しました。

最新のレポートでは、サイバー犯罪者の地下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 1 分あたり平均 480 件の新たな脅威を検出しており、IoT デバイスをターゲットとするマルウェアの急増を確認しました。2017 年の Hansa と AlphaBay のダークウェブ市場摘発の波紋が続く一方で、サイバー犯罪者は取締り当局の目をかいくぐる新たな手法を使っています。

マカフィーAdvanced Research Team(ATR)の上席セキュリティリサーチャー兼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。「サイバー犯罪者は新旧いずれの脆弱性も攻撃しようとしており、地下市場で多くのサービスとしての攻撃手法が利用可能なため効果は劇的に高くなっています。身代金が支払われ、フィッシング詐欺など比較的容易にできる攻撃が成功し続ける限り、これらの技術が攻撃に使われ続けるでしょう。地下市場、闇フォーラムにおける最新の傾向を追い続けることで、サイバーセキュリティコミュニティは最新の攻撃を防御し、攻撃に対して先手を打てることができるようになるのです」

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の評価を行っています。

サイバー犯罪者の闇チャットフォーラムでトレンドを読む

2018 年の第 3 四半期では、Dream、Wall Street、Olympus といった地下市場がシェアを競い合いましたが、Olympus は忽然と消えてしまいました。サイバー犯罪者の中には、取り締まりを回避し、顧客と直に信頼関係を構築するため、大規模な市場で商品を販売することを止め、独自のショップを開設するようになっています。この転換により、闇ビジネスのオーナーを目指す犯罪者向けの闇店舗を構築するという新種のビジネスチャンスがウェブサイトデザイナーの間で浮上しています。

マカフィーのサイバー犯罪調査部門責任者のジョン・フォッカー（John Fokker）は次のように述べています。「サイバー犯罪者は機会を巧みにとらえ、攻撃を仕掛けてきます。今日私たちが直面しているサイバー脅威は、闇フォーラムでの会話から始まり、地下市場で利用可能な製品やサービスに成長しました。さらに、強力なブランドを持つ犯罪組織は、サイバー犯罪者 にとって、より高い感染率と、運用面および財政面の両面での確実性においてより重要性を増しています。」

ハッカーフォーラムは、サイバー犯罪者同志がサイバー犯罪関連の話題を話し合うための人目を避けた空間になっています。マカフィーは、第 3 四半期において次のトピックに関する会話がなされたことを確認しています。

- **データ漏洩事件の模倣攻撃が増加**
    - **ユーザー認証：**最近数多くの大規模データ漏洩があったことで、ユーザー認証は引き続き関心の高いトピックとなっています。ハッキングされた電子メールアカウントは、他のオンラインサービスのログイン認証の復元に利用されるため、サイバー犯罪者にとってとても重宝されています。
    - **電子商取引サイトを狙うマルウェア：**サイバー犯罪者の関心は POS システムから大規模な電子商取引サイトに設置された決済プラットフォームに移っています。Magecart のようなサイバー犯罪グループは、被害サイトから何千ものクレジットカード情報をスキミングすることに成功し、クレジットカード情報とそれらを盗むために使われる悪意あるツールの両方に対するニーズに拍車がかかりました。さらに、企業がセキュリティ対策を強化するにつれて、サイバー犯罪者もそれに応じて対抗しています。たとえば、オンライン購入の際の IP ロケーション（位置情報）チェックが追加されると、盗まれたクレジットカード情報と同じ郵便番号の感染したコンピューターへの需要が高まります。

- **既知の侵入及び攻撃方法が依然として一般的**
    - **共通脆弱性識別子（CVE）：**ブラウザーのエクスプロイトキット RIG、Grandsoft、Fallout や、GandCrab ランサムウェアに関する議論の中で、CVE への言及が数多くみられました。これらのトピックへの高い関心は、脆弱性管理の重要性を世界中の組織に示しています。
    - **リモート デスクトップ プロトコル （RDP）**：一般ユーザーの自宅から医療機器や政府システムに至るまで、世界中のコンピューターシステムへのログインを提供するショップは、第 3 四半期を通じて人気を集めました。これらのショップは、詐欺を犯そうとしているサイバー犯罪者に、RDP アクセスや社会保障番号、銀行口座取引情報からオンラインアカウントへのアクセス情報までを売るワンストップサービスを提供しています。
    - **サービスとしてのランサムウェア（Ransomware-as-a-Service）：**ランサムウェアによる攻撃は引き続き頻繁に行われ、前年同期以来 45%増となっています。闇フォー

ラムでは Gandcrab など主要な RaaS ファミリーへの関心が根強くあります。GandCrab ランサムウェアとファイル暗号化サービス NTCrypt の間の連携が第 3 四半期に見られるなど、重要なサービス間の連携が増加した一方で、新規のランサムウェアファミリー数は、2017 年第 4 四半期以降減少しました。連携やアフィリエイト構造によって、サイバー犯罪者に提供するサービスのレベルが上がり感染率を高めました。

2018 年第 3 四半期の脅威動向

- **仮想通貨マイニングと IoT ：**カメラやビデオレコーダのような IoT デバイスは、デスクトップやラップトップコンピューターなどと比べ CPU パワーが不足しているため、これまで仮想通貨マイニングに悪用されることはほとんどありませんでした。ところが、サイバー犯罪者は IoT デバイスが普及し、またセキュリティ対策が甘いことに気づき、数千のデバイスを利用してマイニングできるスーパーコンピューターをつくり出すことに取り組み始めました。IoT デバイスをターゲットとする新たなマルウェアは 72%増加し、合計サンプル数は過去 1 年間で 203%増となりました。新たな仮想通貨マイニングマルウェアは約 55%増加し、合計サンプル数は過去 1 年間で 4,467%の伸びとなりました。

- **ファイルレス マルウェア**：新たな JavaScript マルウェアは 45%増加し、新たな PowerShell は 24%の増加となりました。

- **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は公開ベースで 215 件となり、第 2 四半期から 12%の減少となりました。発生場所は、南北アメリカが 44%、続いて欧州が 17%、アジア太平洋が 13%でした。

- **特定の産業が攻撃対象に：**金融機関をターゲットとするインシデントは公表ベースで 20%増加しました。 電子メールの基本的なセキュリティ機能をかいくぐろうと珍しいファイルタイプを悪用したスパム攻撃の増加が確認されました。また、金融機関をターゲットとしたマルウェアで、2 要素認証を回避するために Web インジェクションにおいて 2 要素運用が行なわれていることも確認されています。近年の金融機関側のセキュリティ強化に向けた幅広い取り組みを受けて、これらの手法が使われるようになっています。
医療機関をターゲットとしたインシデントは低迷し、公的機関は 2%減少し、教育機関は 14%減少となりました。

- **地域別動向：**マカフィーのリサーチャーは、第 3 四半期に ブラジルをターゲットとした新たなマルウェアファミリーCamuBot を発見しました。CamuBot はターゲットとする金融機関が要求するセキュリティモジュールであるかのように偽装しています。ブラジルでのサイバー犯罪グループは自国民をターゲットとする活動が活発ですが、過去の攻撃手法は単純でした。CamuBot は、ブラジルのサイバー犯罪者たちが他の犯罪者から学んだようで、マルウェアはより洗練され、他の大陸で見られるマルウェアに匹敵するようになっています。

南北アメリカをターゲットとしたインシデントは 18%減少し、アジア太平洋も 22%減少、欧州は 38%の増加となりました。

- **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、漏洩、不正アクセス、および脆弱性が続いています。

- **ランサムウェア**：第 3 四半期に最も活動的だったファミリーの 1 つは GandCrab で、身代金の支払い要求額は 1000 米ドルから 2400 米ドルに吊り上がりました。多くのサイバー攻撃の配信手段であるエクスプロイトキットは脆弱性やランサムウェアをサポートするようになりました。過去 1 年間で、新たなランサムウェアサンプル数は 10%、合計サンプル数は 45%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 24%減少しました。下降傾向にあるにもかかわらず、いくつかの特殊なモバイル脅威が確認されており、その中には Fortnite の“チート”アプリや偽出会い系アプリがありました。イスラエルの国防軍の職員らをターゲットとした攻撃では、出会い系アプリを通じてデバイスの位置情報、連絡先、カメラにアクセスし、電話の通話を傍受する機能もありました。

- **マルウェア**：新たなマルウェアサンプル数は 53%増、合計サンプル数は過去 1 年間で 34%の増加となりました。

- **Mac マルウェア：**新たな MaC OS マルウェアは 9%増で、合計サンプル数は過去 1 年間で 51%の増加となりました。

- **マクロ マルウェア：**新たなマクロマルウェアは 32%増で、合計サンプル数は過去 1 年間で 24%の増加となりました。

- **スパム攻撃：** スパムボットネットによるトラフィックの 53%は、「セクストーション（性的脅迫）」スパムを生み出す最大のスパム製造ボットネット Gamut によるもので、被害者のサイト閲覧履歴をばらすと脅迫して金銭を要求する手口です。

『McAfee Labs Threats Report: December 2018（McAfee Labs 脅威レポート：2018 年 12 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-dec-2018.pdf

McAfee Labs 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 Advanced Threat Research（ATR）チームは、ファイル、Web、ネットワークなど、主要な脅威ポイントに配置された数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。さらに、McAfee Labs は、核となる脅威検出テクノロジーを開発し、それらを業界で最も包括的な自社のセキュリティ製品群に統合しています。

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超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 http://www.mcafee.com/jp/ 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　（http://www.mcafee.com/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

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
Tel: 03-4570-3169
Fax: 03-4580-9131
mailto:mcafee-pr@witan.co.jp