【プレスリリース】

マカフィー株式会社
2018 年 10 月 11 日

※当資料は、2018 年 9 月 25 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 2 四半期の脅威レポートを発表

第 2 四半期も仮想通貨をマイニングするマルウェアが継続的に増加

ニュースハイライト
• 2018 年第 2 四半期に仮想通貨をマイニングするマルウェアが前期比 86%増加
• パッチ適用可能な脆弱性を狙ったマルウェアが前期比 151％増加
• モバイルマルウェアが 2 四半期連続して増加し、前期比で 27％増加
• JavaScript マルウェアが 204％増加した一方、PowerShell を悪用したマルウェアは減速
• Windows コルタナ、Google Play およびブロックチェーンでセキュリティインシデントを特定

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 2 四半期の脅威レポート「McAfee Labs 脅威レポート：2018 年 9 月」を発表しました。

最新のレポートでは、新しい脅威の増加と傾向について説明しています。第 2 四半期では、仮想通貨マイニングマルウェアの増加が引き続き確認されました。仮想通貨マイニングマルウェアは、2017 年第 4 四半期から増え始め、2018 年上期を通して爆発的に増加しました。また、2017 年に世界的規模で発生した WannaCry や NotPetya で悪用された脆弱性を狙うマルウェアが引き続き確認されました。

仮想通貨マイニングマルウェアは、ランサムウェアほど一般的ではありませんが、脅威の一形態としての存在感を高めています。2017 年第 4 四半期に約 40 万件に達したサンプル数はその後、2018 年第 1 四半期には 290 万超と急増し、その増加率は前期比 629%増という、脅威的な数字となりました。この傾向は第 2 四半期も継続し、新たに発見されたサンプル数は 250 万件を超え、累計サンプル数は 86%増を記録しました。MacAfee Labs は、ランサムウェアなどの従来のマルウェアが新たにマイニング機能を搭載し、機能を強化していることを確認しています。

一部のケースでは、仮想通貨マイニングマルウェアは幅広い標的対象ではなく、特定の団体に標的を絞る動きが確認されています。ロシアではゲームコミュニティのユーザーを標的として、人気の高いゲームを強化すると触れ込む「MOD」になりすました仮想通貨マイニングのマルウェア亜種が確認されました。騙されたゲーマー達はこの悪意あるソフトウェアをダウンロードしたため、彼らのコンピューターはマイニング処理のリソースとして悪用されていたことが確認されました。

仮想通貨マイニングマルウェアは主にパソコンを標的としますが、パソコン以外のデバイスにも被害が及んでいます。その一例として、中国と韓国では ADB.Miner マルウェアに感染した Android 携帯端末が、仮想通貨モネロのマイニングに悪用されるケースが確認されています。

マカフィーAdvanced Threat Research (ATR) チーム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ティアーン・ビーク（Christiaan Beek）は、「数年前は、インターネットのルーター、動画レコーダーや他の IoT 機器などは、CPU 速度がマイニング処理には不十分であったことから、仮想通貨マイニングのプラットフォームになり得るとは考えられませんでした。今日では、このようなデバイスがオンライン上に豊富に出回り、またそういった装置はパスワード機能が脆弱な傾向にあることから、攻撃者にとって非常に魅力的なプラットフォームとなっています。仮に感染した IoT 機器が 1 万台規模のボットネットであれば潤沢な仮想通貨の獲得が可能で、サイバー犯罪者にとってはただ同然で新たな収益性のある収入源を得ることができるのです」と述べています。

脆弱性を狙うマルウェア

WannaCry および NotPetya による大規模攻撃から一年、2018 年第 2 四半期には、ソフトウェアの脆弱性を狙うべく作成された新たなマルウェアのサンプルが前期比 151%増加しました。これらの特筆すべき脅威で悪用されたエクスプロイトが新たなマルウェアの亜種に再利用され、これまでと同様に脆弱性のエクスプロイトに適用された結果、以前には存在しなかった全く新しい脅威を生み出していることが新たに確認されました。

さらにビークは、「WannaCry や NotPetya の例はどのようにしてマルウェアが脆弱性を悪用し、システムへの足がかりを得てネットワークに急速に拡散するのかをサイバー犯罪者に示してしまいました。脆弱性を狙う攻撃を回避する適用可能なパッチがすでに何か月、何年と提供されているにも関わらず、2014 年にまで遡るような脆弱性がいまだ膨大に存在し、スピア攻撃が成功していることに驚きを隠せません。ユーザーや組織は修正パッチが公開されたら、脆弱性に対してパッチをできるだけ早期に適用すべきです。ユーザーや組織は修正パッチが公開されたら、脆弱性に対してパッチをできるだけ早期に適用すべきであることを忘れないでください」と述べています。

Windows 10 コルタナの脆弱性

MacAfee Labs と ATR チームは、マイクロソフト Windows 10 に搭載された音声アシスト「コルタナ」の脆弱性を特定しました。マイクロソフトが 6 月にパッチを公開済のこの欠陥を悪用すれば、公開済のパッチ（RS3 と RS4）を適用した Windows 10 のデバイス上のロック画面からでもコードが実行されるという危険性がありました。マカフィーは 3 つの側面から調査を行い、マイクロソフトと共同して CVE-2018-8140 の脆弱性情報を公開しています。マカフィーは、「責任ある開示」方針のもと、マイクロソフトに対して 4 月に本脆弱性を報告していました。（詳細）*1

Google Play 上の不正請求アプリ

マカフィーモバイルリサーチチームは、新たな不正請求詐欺のサイバー攻撃を確認し、Google Play のストア上に少なくとも 15 個の不正請求アプリを発見しました。この新たな攻撃は、サイバー犯罪者が Google Play などの公式サイトを悪用してユーザーから金銭を騙し取る新たな手法を継続的に模索していることを示唆しています。この攻撃の黒幕であるサイバー犯罪集団「AsianHitGroup」は、少なくとも 2016 年後半から積極的に活動しており、人気の高いアプリのコピーをダウンロードする偽インストーラーアプリ Sonvpay.A を配布し、主にタイとマレーシアで少なくとも 2 万人に及ぶユーザーに課金詐欺を働きました。その一年後の 2017 年 11 月には、再び Google Play のストア上で、今度は Sonvpay.B の配布が確認されました。Sonvpay.B は、IP アドレスによる位置情報を利用してユーザーの地域を特定し、この詐欺行為に馴染みの浅いロシアのユーザーをその標的対象に追加しました。（詳細）*2

ブロックチェーンのセキュリティ脅威

マカフィーの ATR チームは、ブロックチェーンのユーザーと運用者に及ぼす重大なセキュリティ脅威を特定しました。リサーチャーの分析によれば、主な攻撃経路はフィッシング、マルウェア、そして脆弱性への攻撃であることが確認されました。（詳細）*3

2018 年第 2 四半期の脅威動向

2018 年第 2 四半期中、McAfee Labs では 1 秒あたり平均 5 個の新しいマルウェアサンプルを検知しました。その中には、標的側の防御の裏をかく最新のテクノロジーや戦術によって改良され、著しい技術的進歩を示した脅威も含まれていました。

- **ランサムウェア：** ランサムウェアの合計サンプル数は増加を続け、過去一年間で 57%増となりました。新たなランサムウェアファミリーの出現は直近の四半期では全体的に減速する一方で、マカフィーは既存のランサムウェアファミリーから作成された新亜種を確認しています。例えば、Scarab ランサムウェアファミリーからは、第 2 四半期だけで 12 の新亜種が確認されました。この数は、2017 年中盤に同ファミリーが出現して以降、Scarab の亜種として特定された合計数の 50%以上を占める驚異的な数字です。

- **モバイルマルウェア：**第 2 四半期で発見された新たなモバイルマルウェアのサンプル数は前期比 27%増で、2 四半期連続での増加となりました。また、感染率が最も高かった地域は南米の 14%でした。発見されたモバイルマルウェアの合計サンプル数は過去 1 年間で 42%の増加となりました。

- **JavaScript マルウェア：**新たに発見されたサンプル数が 204%増という数字からもわかるように、サイバー犯罪者の間で JavaScript マルウェアが新たなフェーズに入ったことを示唆しています。JavaScript マルウェアの当期サンプル数は、過去 3 四半期において著しく減退した後、700 万件以上と史上最高を記録しました。

- **LNK マルウェア**：直近の四半期において、ファイルレスマルウェアの開発者の間では PowerShell の積極的な採用が見られていたものの、新たに発見されたサンプル数は 15%増と減速しました。一方で、LNK ファイルを利用した新たなマルウェアの増加が続き、サイバー犯罪者の間では「.lnk」拡張子のファイルを利用して PowerShell スクリプトやその他のマルウェアを水面下で拡散する手法が増加しています。この分野の合計サンプル数は、過去 1 年間で 489%の増加を見せています。

- **スパムボットネット**：第 2 四半期最大のスパム ボットネットは Gamut でした。これは、特に「カナダ歳入庁」の大量のフィッシングメールを拡散したことで顕在化しました。最近の注目すべき攻撃は偽の求人サイトに関連した動きで、「マネーミュール（不正資金の運び屋）」の募集で一般的に使われる攻撃手法が確認されています。

『McAfee Labs Threats Report: June 2018（McAfee Labs 脅威レポート：2018 年 6 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-jun-2018.pdf

参考：
*1：コルタナに聞けば、ロックされた Windows 10 のデバイスにだって侵入できる
https://blogs.mcafee.jp/want-to-break-into-a-locked-windows10
*2：サイバー犯罪集団 AsiaHitGroup による課金詐欺アプリが Google Play に再登場
https://blogs.mcafee.jp/asiahitgroup-again-google-play
*3：ブロックチェーン脅威レポート
https://www.mcafee.com/enterprise/ja-jp/assets/reports/rp-blockchain-security-risks.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
mcafee-pr@witan.co.jp