【プレスリリース】

マカフィー株式会社
2019 年 3 月 5 日

※当資料は、2019 年 3 月 3 日に米国で発表されたプレスリリースの抄訳です。

マカフィーによる調査で国家レベルでの サイバースパイ活動の内部指揮系統が明らかに

ニュースハイライト

- マカフィーがコマンド&コントロールサーバーのデータとコードを分析し、グローバルなサイバースパイ活動の内部構造が判明
- サーバーのデータとコードから、2018 年以前にも活動があったことが明らかに
- 主に世界的な金融機関、政府機関、重要インフラを標的にした活動が継続中

米国マカフィー（McAfee LLC、本社：米国カリフォルニア州）は本日、2018 年に確認された Operation Sharpshooter が、実はより複雑で、広範囲、長期間にわたっている証拠を明らかにしました。マカフィー Advanced Threat Research(ATR)は、このグローバルなサイバースパイ活動の背後で作戦、ツール、およびスパイ技術を管理するコマンド&コントロールサーバーのコードとデータについて詳細に分析しました。このコンテンツは、マルウェア攻撃に関するマカフィーがこれまで公表した調査をよく知る政府機関から、マカフィーに分析のため提供されたものです。分析の結果、以前には知られていなかった複数のコマンド&コントロールセンターが確認され、Sharpshooter の攻撃が 2017 年 9 月に開始され、多くの業界や国の広範な組織を対象に、いまも活動が継続中であることがわかりました。

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。「マカフィーATR によるコマンド&コントロールサーバーのコードとデータの分析によって、Sharpshooter の背後にいる攻撃者がどのように統制のためのインフラを開発し、構成したかについてより詳細に知ることができます。マルウェアをどのように配布し、実行に先だってどのように秘密裡にテストしたかについての詳細です。この知見は、攻撃者に対する理解を深めるために非常に有益であり、最終的にはより堅牢な防御につながります」

2018 年 12 月、マカフィー ATR は Sharpshooter が通信、エネルギー、政府、防衛分野などを含む基幹産業全体で世界 80 以上の機関を標的とするグローバルなサイバースパイ活動であることを初めて確認しました。新たな証拠の分析によって、2018 年の活動における技術指標、技法および手順と、サイバー犯罪組織「Lazarus」 グループによるものとみなした他の複数の攻撃特徴が、非常に似ていることがわかりました。例えば、Lazarus グループが 2017 年に Rising Sun インプラントの類似バージョンを使用したことや、Lazarus グループの悪名高い 2016 年のバックドア「Trojan Duuzer」のソースコードなどです。

マカフィーの上席プリンシパルエンジニア兼リードサイエンティストであるクリスチャン・ビーク（Christiaan Beek）は、次のように述べています。「サイバー攻撃を完全に理解するには、技術的な証拠だけでは十分ではなく、それで謎の全貌が判明するわけではないのです。敵のコマンド&コントロールサーバーのコードにアクセスできる機会など滅多にありません。これらのシステムを探る

ことで、サイバー攻撃のインフラの内部構造について深く知ることができます。これらは通常、法執行機関に差し押さえられることはあっても、民間の研究者が参照できる機会は滅多にありません。このコードにアクセスすることで得られた知見は、今日の最も顕著で巧妙なサイバー攻撃を理解し、戦うために不可欠です」

以前確認された時期よりも約 1 年早く開始されていたことがわかり、そして今も続くこれらの活動は、現在、主に金融サービス、政府機関および重要インフラに集中しているようです。また最近は、ドイツ、トルコ、英国、米国を中心に多く発生しています。以前は米国、スイス、イスラエルなどの通信業界、政府機関、および金融業界に集中していました。

その他分析結果

- **ハンティングとスピア型攻撃** ：Sharpshooter はいくつかの活動と設計や戦術が重複しています。例えば、Lazarus グループによるものとされている 2017 年の偽の求人募集を悪用した活動に非常に類似しています。

- **アフリカ・コネクション：**コマンド&コントロールサーバーのコードとファイルログを分析したところ、アフリカのナミビアにあるビントフック市から発信された IP アドレスのネットワークブロックが発見されました。マカフィーATR のアナリストは、Sharpshooter の背後にいる攻撃者が、広範な攻撃を展開するのに先立ち、この地域でインプラントやその他技法をテストした可能性があるのではないかと見ています。

- **アセットへのアクセスを維持：**攻撃者は、Hypertext Preprocessor (PHP)および Active Server Pages（ASP）で書かれたコアバックエンドを有するコマンド&コントロールインフラを使用しています。このコードはカスタマイズされており、グループに固有のもののようです。マカフィーの分析によると、2017 年からの攻撃に利用されていたことが判明しました。

- **進化する Rising Sun**：Sharpshooter の攻撃者は、コアのインプラント機能とは独立して開発されてきた Rising Sun を構成するさまざまな悪意あるコンポーネントで構成される工場のようなプロセスを使用しています。2016 年からのさまざまなインプラントでこれらのコンポーネントが確認されています。これは、攻撃者が先進の機能に意のままにアクセスできることを示すものの一つです。

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 http://www.mcafee.com/jp/ をご覧ください。

McAfee Labs および ATR(Advanced Threat Research)について

McAfee Labs と McAfee ATR は、脅威調査、脅威に関する知見、サイバーセキュリティにおける主要機関です。McAfee Labs 及び、McAfee ATR は、ファイル、Web、メールやネットワークなどの主な脅威対象項目にわたる 10 億以上のセンサーからのデータを元に、リアルタイムで脅威情報、分析、防御力の向上及びリスクの軽減を目指しています。

＜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
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：住川／中根
Tel: 03-4570-3169
mcafee-pr@witan.co.jp