修正再送

※2 月 27 日付け同名リリース 1 頁にランサムウェア攻撃の割合の誤植がありました。お詫び再送いたします。

2017 年 2 月 28 日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイントの調査によりランサムウェアは 2016 年下半期に倍増と判明

日本においても、ネットワークやモバイル経由のマルウェアとランサムウェアが急増

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社（本社：東京都、代表取締役社長：ピーター・ハレット、以下チェック・ポイント）は、『H2 2016 Global Threat Intelligence Trends（2016 年下半期 脅威情報トレンド・グローバル版）』レポートを発表し、ランサムウェア攻撃が同期間中に倍増した実態を明らかにしました。

同レポートは、チェック・ポイントが運営する ThreatCloud World Cyber Threat Map に蓄積された、2016 年 7～12 月の脅威情報データに基づいて作成されており、企業各社に対するサイバー攻撃で使用されている主な手口と、主要マルウェア・カテゴリ（ランサムウェア、バンキング・マルウェア、モバイル・マルウェア）における脅威動向について解説しています。

Threat Map のデータによると、日本では、2016 年通年でモバイル機器が最大の攻撃対象となりました。Android 端末を狙うモバイル・マルウェア HummingBad が国内マルウェア関連インシデント全体の 16%を占め、最大の脅威の 1 つとなりました。2017 年 1 月には HummingBad の派生種である HummingWhale が出現しているため、引き続きモバイル・セキュリティ対策が必要です。

世界各国で確認されたマルウェア関連インシデント全体に占める、ランサムウェア攻撃の割合は、2016 年 7～12 月にかけて、5.5%から 10.5%へと 90%増加しました。日本におけるランサムウェア攻撃の割合は同期間（2016 年 7～12 月）で 5.6%から 25.2%に 348%増加しました。2016 年通年では CryptoWall が国内マルウェア関連インシデントの 9%、Locky が同 3%を占める 2 大ランサムウェアとなりました。

主な傾向

2016 年下半期に確認された主な傾向は次のとおりです。

- **ランサムウェア市場の寡占化** - 2016 年全体で見ると、ランサムウェアは亜種を含め数千種類の新種が確認されています。しかし、同年後半に限ると、ランサムウェアの集約化が進み、ごく少数のファミリーが大小さまざまな規模の組織を標的とするようになっています。
- **IoT デバイス経由の DDoS 攻撃** - 2016 年 8 月、史上初の IoT（Internet of Things： モノのインターネット）ボットネット、Mirai が発見され、大きな話題となりました。Mirai は、デジタル・ビデオ・レコーダ

ー（DVR）や監視カメラ（CCTV）などの脆弱なインターネット接続デバイスに感染し、そのデバイスをボット化して、大規模な分散サービス妨害（DDoS）攻撃を実施します。Mirai の登場により、ほとんどすべての一般家庭に脆弱な IoT デバイスが存在する現状が明らかとなりました。IoT デバイスを利用した大規模 DDoS 攻撃は、今後も継続的に発生すると予想されます。

- **新しいファイル形式を利用したスパム・キャンペーン** - 2016 年下半期のスパム・キャンペーンで最も多く使用された感染経路は、Windows スクリプト・エンジン（WScript）を利用したダウンローダです。スパム・キャンペーンで使用されるダウンローダのほとんどは、JavaScript（JS）や VBScript（VBS）で記述されていますが、少数ながら、同様の機能を持つ JSE、WSF、VBE などの形式で記述されたダウンローダの存在も確認されています。

2016 年下半期のマルウェア総合ランキング：

1. **Conficker（14.5%）** – 遠隔操作やマルウェアのダウンロードを可能にするワームです。感染したマシンはボットネットの一部として制御され、指令（C&C）サーバと通信して命令を受け取ります。

2. **Sality（6.1%）** – マルウェア管理者による感染システムの遠隔操作やマルウェアの追加ダウンロードを可能にするウイルスです。主な目的として、感染マシンに常駐し、攻撃者による遠隔操作と別のマルウェアのインストールを可能にします。

3. **Cutwail（4.6%）** – スパム・メールの送信を中心に、一部の DDoS 攻撃でも使用されるボットネットです。インストールされたボットは、C&C サーバと直接通信し、送信すべき電子メールに関する命令を受け取ります。目的を達成した後は、自身の活動に関する正確な情報をスパム業者に送り返します。

4. **JBossjmx（4.5%）** – 脆弱なバージョンの JBoss Application Server がインストールされているシステムに感染するワームです。任意のコマンドを実行する不正な JSP ページを脆弱なシステム上に作成します。また、リモートの IRC サーバから指令を受け取るバックドアも作成します。

5. **Locky（4.3%）** - 2016 年 2 月から拡散し始めたランサムウェアです。主な感染経路は、ダウンローダを含む Word ファイルや Zip ファイルが添付されたスパム・メールです。Locky は、このダウンローダによってダウンロードおよびインストールされた後、ユーザ・ファイルを暗号化します。

2016 年下半期のランサムウェア・ランキング：

世界各国で確認されたサイバー攻撃全体に占めるランサムウェア攻撃の割合は、2016 年下半期に 5.5%から 10.5%へとほぼ倍増しています。特に多く確認されたランサムウェアは次のとおりです。

1. **Locky（41%）** - 2016 年上半期のランサムウェア・ランキングで第 3 位だった Locky は、下半期に入って検出数が急増しています。

2. **Cryptowall（27%）** - Cryptolocker の模倣版として登場した Cryptowall ですが、最終的に本家を上回るランサムウェアへと成長を遂げました。Cryptolocker の背後組織が摘発を受けた後、Cryptowall は、史上最も有名なランサムウェアの 1 つとなっています。このランサムウェアの特徴は、AES 暗号化アルゴリズムを使用し、匿名ネットワークの Tor 経由で C&C 通信を行う点です。エクスプロイト・キットや不正なインターネット広告、フィッシング・キャンペーン経由で広範囲に拡散しています。

3. **Cerber（23%）** - 世界最大規模の「Ransomware-as-a-Service」モデルの下で利用されているランサムウェアです。Cerber の開発者は、フランチャイズ型のビジネス・モデルを採用しており、Cerber の感染を広げる協力者を募って、身代金による利益を分配しています。

2016 年下半期のモバイル・マルウェア・ランキング：

1. **HummingBad（60%）** – モバイル・デバイスに永続的な rootkit を組み込み、詐欺的なアプリをインストールする Android マルウェアです。HummingBad は、チェック・ポイントのリサーチ・チームの手によって発見されました。キーロガーのインストールや認証情報の窃取、ユーザが導入した電子メール暗号化機能の回避といった追加機能を備える亜種も存在します。

2. **Triada（9%）** - Android デバイスに感染するモジュール型のバックドアです。ダウンロードしたマルウェアにスーパーユーザの権限を付与することで、そのマルウェアのシステム・プロセスへの組み込みを可能にします。ブラウザに読み込まれる URL を偽装するタイプも確認されています。

3. **Ztorg（7%）** – root 権限を使って活動するトロイの木馬です。感染先のモバイル・デバイスに密かにアプリケーションをダウンロードし、インストールします。

2016 年下半期のバンキング・マルウェア・ランキング：

1. **Zeus（33%）** – Windows プラットフォームに感染するトロイの木馬です。多くの場合「Man-in-the-Browser」攻撃やキー入力内容の記録、フォーム入力内容の取得により、金融機関情報を盗み出す目的で使用されます。

2. **Tinba（21%）** – バンキング型トロイの木馬です。ユーザが銀行の Web サイトにログインしようとしたタイミングで活動を開始し、Web インジェクションによりユーザの認証情報を窃取します。

3. **Ramnit（16%）** – バンキング型トロイの木馬です。銀行の認証情報や FTP のパスワード、セッション cookie、個人情報を窃取します。

同レポートの統計情報データを提供するチェック・ポイントの ThreatCloud は、サイバー犯罪阻止を目的とした業界最大規模の協調型ネットワークです。グローバルな脅威センサー・ネットワークで収集された、セキュリティ脅威に関する最新のデータやサイバー攻撃のトレンド情報を配信します。ThreatCloud のデータベースには、1 日あたり数百万件のマルウェア情報が追加されるほか、ボット発見を目的として分析された 2 億 5,000 万件以上のアドレスや 1,100 万件以上のマルウェア・シグネチャ、550 万件以上の不正 Web サイトの情報が登録されています。

チェック・ポイントの脅威情報グループ・マネージャを務めるマヤ・ホロウィッツ（Maya Horowitz）は、「サイバー空間の現状を示したこのレポートによって、ランサムウェア攻撃が急激に増加している事実が明らかとなりました。ランサムウェア攻撃が急増している理由は、ひとえに、その手口が効果的であり、攻撃者に多額の金銭的利益をもたらすからです。多くの組織は、ランサムウェア攻撃への対処に苦慮しています。しかしその一方、適切な防御策を導入しておらず、電子メール経由のランサムウェア感染を防ぐために注意すべきポイントについてユーザ教育を実施していないケースが多いのも実情です」さらに、「同レポートでは、少数のマルウェア・ファミリーが大半の攻撃に関わっており、他の多くのマルウェア・ファミリーはごくわずかしか検出されていないという傾向も判明しています。また、ほとんどの脅威は、地域の枠を超えてグローバルに活動していますが、アジア太平洋地域に関しては、マルウェア・ファミリー・ランキングの上位に、他の地域のランキングには登場しないファミリーが 5 種類もランクインしているという特徴があります」と述べています。
レポートの全文は、こちら(英語)をご覧ください。

■チェック･ポイントについて　ONE STEP AHEAD

チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、あらゆる規模の組織に対応する世界トップクラスのセキュリティ・リーディング・カンパニーです。業界随一の検出率を誇る先進のセキュリティ対策により、お客様のネットワークをマルウェアなどの多岐にわたるサイバー攻撃から保護します。大規模ネットワークからモバイル・デバイスまでを保護する包括的なセキュリティ・アーキテクチャに加え、直感的で使いやすい総合的なセキュリティ管理ソリューションを提供しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社（ http://www.checkpoint.co.jp/ ）は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

####

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

担当　マーケティング　石黒・溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行　共同ピーアール株式会社

担当　中村・小林・上瀧

Tel: 03- 3571－5238 / Fax: 03- 3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp