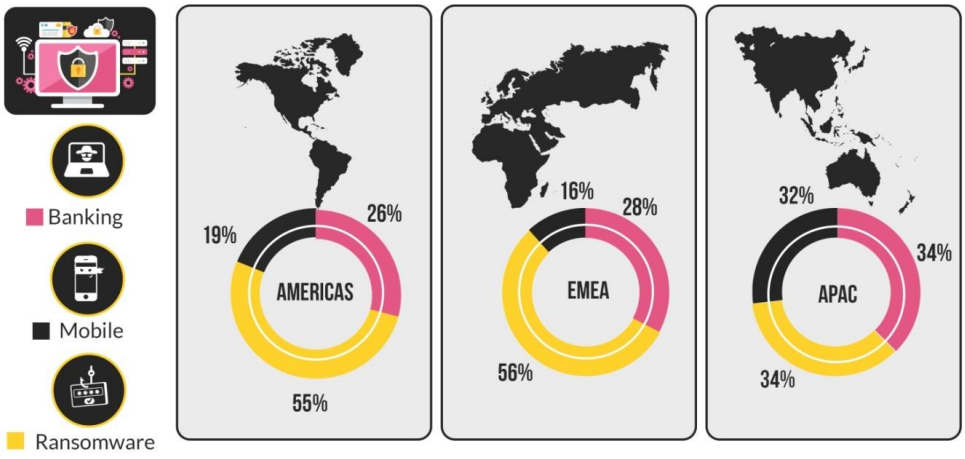
2017 年 8 月 29 日
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイント、オンライン調査プラットフォーム「Check Point Research」を発表、
『サイバー攻撃トレンド 2017 年上半期レポート』を公開
世界約 25%の組織が、不正なインターネット広告キャンペーン RoughTed の被害に

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、セキュリティ脅威情報の知見をコミュニティに提供する新たなオンライン・プラットフォーム「Check Point Research」を通じた情報提供の開始を発表しました。Check Point Research は、脅威情報コミュニティを対象に、チェック・ポイント独自の調査結果、サイバー・セキュリティ分野のトレンド情報、脅威動向の詳細情報を提供する調査プラットフォームです。

チェック・ポイントは同時に、『チェック・ポイント サイバー攻撃トレンド 2017 年上半期レポート』を発表しました。本編は、マルウェアの中でも特に多く検出されているランサムウェア、バンキング・マルウェア、モバイル・マルウェアに関するトレンドを包括的に解説しています。チェック・ポイントの ThreatCloud World Cyber Threat Map で 2017 年 1 月～6 月に収集した脅威情報データに基づいています。



マルウェア・カテゴリ別の感染状況（地域別）

2017 年上半期、不正なインターネット広告キャンペーンの RoughTed による影響を受けた組織は 23.5%、Fireball マルウェアの影響を受けた組織は 19.7%に上りました。また、北中南米地域とヨーロッパ、中東、アフリカ地域（EMEA）では、ランサムウェア攻撃の検出数が前年同時期に比べて 2 倍近くに増加しました。

2017 年上半期のレポートで確認された主な傾向は次のとおりです。

● **アドウェアの突然変異：** Fireball マルウェアの登場により、正当な大企業が提供するよう見せかけたアドウェアに対するアプローチの転換、阻止が不可避となっています。並行して、モバイル・デバイスを標的とするアドウェア・ボットネットが勢力を拡大し、モバイル・マルウェア分野で圧倒的なシェアを占めるようになっています。

● **国家レベルのハッキング・ツール：** 国家レベルのハッキング・ツールやゼロデイ脆弱性情報、エクスプロイト、攻撃手法がリークされ、容易に入手可能となったことで、技術力の低いハッカーでも高度な攻撃を実行できるようになっています。

● **マクロ・ベースのダウンローダの進化：** 2017 年上半期には、マクロを有効にさせる必要のない、Microsoft Office ファイルの新しい攻撃手法が複数確認されています。

● **台頭する新たなモバイル・バンキング・マルウェア：** 攻撃者は、オープンソースとして公開されているバンキング・マルウェアのコードと、複雑な難読化手法を組み合わせることで、検出を困難にし、アプリ・ストアの審査を何度もすり抜けることに成功しています。

● **ランサムウェア攻撃の急増：** 2017 年の上半期、北中南米地域、EMEA、アジア太平洋地域（APAC）のすべてで、攻撃カテゴリに占めるランサムウェア攻撃の割合が前年同期比でほぼ倍増し、世界平均で 26%から 48%に増加しています。

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、「多くの組織は、増加するセキュリティ脅威の対処に苦労しています。マルウェアは高度化し、技術力のないハッカーでも簡単に大きな被害を引き起こせるようになっています。しかし、セキュリティ脅威が蔓延する中でも、多くの組織は依然として、適切なセキュリティ対策を導入できていません。検出アプローチに依存し、被害の発生を未然に防ぐプロアクティブな防御ソリューションを導入していません」と述べています。

チェック・ポイントのリサーチ・チームは、ハッカーによる攻撃を未然に防ぐため、Check Point Threat Cloud で世界のサイバー攻撃データを収集、分析しています。サイバー攻撃トレンドレポートをはじめとする Check Point Research の資料により、新たなセキュリティ脅威やトレンド、セキュリティの知見に関する議論を促進します。Check Point Research は、脅威動向の正確な把握と、適切なセキュリティ対策の実施に貢献することを目的としています。

「チェック・ポイント サイバー攻撃トレンド 2017 年上半期レポート」については、以下をご覧ください。
http://www.checkpoint.co.jp/report/cyber_attack_trend_2017h1.pdf

「Check Point Research」については、以下をご覧ください。
https://research.checkpoint.com/

■チェック･ポイントについて　　WELCOME TO THE FUTURE OF CYBER SECURITY

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　宮
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　花岡・上瀧
Tel: 03- 3571－5238 / Fax: 03- 3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

