2017 年 6 月 20 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、全世界 2 億 5,000 万台以上のコンピュータでデジタル広告詐欺を働く中国発の大規模マルウェア攻撃「Fireball」を確認、yahoo.com や Google.com で検索するブラウザのゾンビ化、史上最大規模の感染被害を警告

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、チェック・ポイントの脅威情報およびリサーチ・チームが全世界 2 億 5,000 万台以上のコンピュータが感染した中国発の大規模なマルウェア攻撃「Fireball」（ファイアボール）を確認したと発表しました。デジタルエージェンシーRafotech が提供する Fireball は、ブラウザ・ハイジャッカーとして標的のブラウザを乗っ取り、コンピュータを指示通り動く「ゾンビ」に変えます。

Fireball には、①被害者のコンピュータ上で任意のコードを実行する（ファイルやマルウェアのダウンロードなど）、②感染したコンピュータの Web トラフィックを乗っ取り遠隔操作して広告収入を増やす、という 2 つの主な機能があります。現在、Fireball はプラグインと追加設定を導入して広告の表示機会を増やしているだけですが、高度なマルウェア配布ツールにも容易に変貌します。

Fireball 攻撃は北京を拠点にデジタル・マーケティングを展開する大手広告代理店 Rafotech によるものです。Rafotech は Fireball を使って被害者のブラウザを操作し、デフォルトの検索エンジンとホームページを偽の検索エンジンに変更します。これにより、yahoo.com または Google.com の検索が Trotux.com などの偽の検索エンジンにリダイレクトされます。偽の検索エンジンは、ユーザの個人情報を収集するトラッキング・ピクセルを備えているため、Fireball による被害者の行動追跡、マルウェアの効率的な埋め込み、感染したコンピュータ上の不正なコード実行を可能にします。感染したコンピュータやネットワークはセキュリティ上の重大な欠陥にさらされます。

主な調査結果

- チェック・ポイントが発見した中国発の大規模なマルウェア攻撃 Fireball は、全世界で 2 億 5,000 万台以上のコンピュータと 20%の企業ネットワークへの感染が広がっています。今回の調査報告は、Rafotech のブラウザ・ハイジャッカーの拡散を「おそらく史上最大規模の感染被害」と定義しています。

- Fireball はブラウザ・ハイジャッカーとして機能するほか、フル機能のマルウェア・ダウンローダーにも変貌します。被害者のコンピュータ上で任意のコードを実行できるため、認証情報の窃盗、新たなマルウェアの埋め込みなど、さまざまな被害に発展する可能性があります。

- Fireball はソフトウェア・バンドリング（ユーザが目的のプログラムをインストールする際に、同時にインストールされる仕組み）という不正な方法によって主に拡散します。同意確認が行われることはまれです。
- Fireball 攻撃はデジタル・マーケティングを専門とする中国の広告代理店 Rafotech によるものです。インターネット・サービス会社 ELEX Technology など、他のブラウザ・ハイジャッカーも確認されています。
- 感染の件数が多かった上位 2 か国は、インド（全体の 10.1%）とブラジル（9.6%）です。日本も感染範囲になっています。

Fireball 感染の流れ、感染状況、確認方法と対策についてはチェック・ポイントブログ(http://www.checkpoint.co.jp/threat-cloud/2017/06/fireball-chinese-malware-250-million-infection.html)を参照ください。

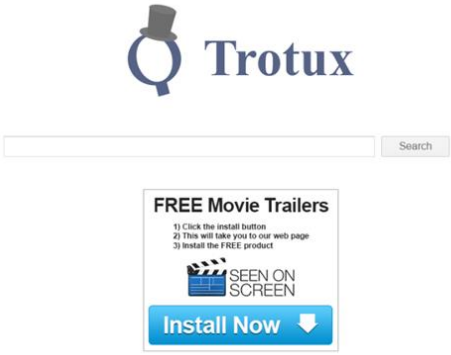

図: Trotux.com（Rafotech が運営する偽の検索エンジン）

■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

