



報道発表資料

2011年5月11日

フォーティネットジャパン株式会社

米国時間 2011年5月5日に発表されたプレスリリースの抄訳です。

フォーティネット、脅威動向調査を公表 – Facebook ユーザを ターゲットとした2つの新しいマルウェア亜種を報告

FBI による米国での最大のボットネットのおとり捜査の結果、230万台のマシンを感染させた *Coreflood* ボットネットを閉鎖。スパムレベルは *Rustock* ボットネットが最近閉鎖されて以降で前月比15%減を維持。

Unified Threat Management/統合脅威管理 (以下、UTM) 市場のリーディングベンダー、Fortinet®(本社：米国カリフォルニア州サニーベール、日本法人：フォーティネットジャパン株式会社、東京都港区、以下、フォーティネット)は本日、脅威動向に関する最新レポートをリリースしました。本調査レポートでは、Facebook ユーザをターゲットとした2つの新しいマルウェア亜種について詳しく述べています。そのマルウェアには Facebook から送信されているように見せる仕掛けがあり、ユーザの Facebook パスワードをリセットして不正な添付ファイルに新しいパスワードをつけるように要求します。その添付ファイルをクリックするとすぐに感染する恐れがあります。

フォーティネットのシニア セキュリティ ストラテジストである Derek Manky は次のように述べています。「弊社が調査した Facebook のマルウェア亜種はボットネット ローダーです。実行にあたり、C&C (Command and Control ; コマンド・アンド・コントロール) サーバに接続してダウンロードし、正規版に見せかけるために偽造のパスワードを見せるドキュメントを表示します。その後、そのボットネットはバックグラウンドで動作し続け、1つずつ、ファイルに対してダウンロードおよび実行を要求します。常に添付ファイルに注意して、未承諾のリクエストによる情報は絶対に開かないこと。さらに、送信元の身元を確認することも絶対にしないでください。」

スパム アクティビティが減少状態を維持

4月16日、大規模な Coreflood ボットネット（2002年頃発生）が米国史上最大の FBI 捜査活動によって閉鎖されました。サイバー犯罪者の国際組織が支配していたサーバとドメインが差し押さえられました。この特定のボットネットは230万台のマシンを感染させ、何百万ドルものお金が疑いをもたないコンピュータ ユーザから盗まれました。

Derek Mankyは続けて次のように述べています。「CorefloodボットネットはRustockボットネットの足跡をたどっていったことにより明らかになりました。Rustockボットネットは、Microsoft社や数多くの連邦政府関係機関の助けにより3月中旬に閉鎖されていました。結果として、2つの主要なボットネットが減少しており、世界中のスパム レートがRustockボットネットの閉鎖前と比べて約15%減を維持しています。」

最新の脅威動向に関するレポート (英文)は次の URL よりご覧いただけます。

http://www.fortiguard.com/report/roundup_04_21_2011.html

FortiGuard Labsについて (www.fortiguard.com)

FortiGuard Labs は、世界中で稼働している FortiGate ネットワーク セキュリティ アプライアンスおよび FortiGuard Labs の監視システムから収集したデータに基づいて、過去4週間の脅威に関する統計およびトレンドを収集・集計しています。

FortiGuard サービスは、アンチウイルス、不正侵入防止、Web コンテンツ フィルタリング、アンチスパム機能などを含めた包括的なセキュリティ ソリューションを提供します。このサービスによって、アプリケーション層とネットワーク層の両方における脅威から保護することができます。FortiGuard サービスは FortiGuard Labs によってアップデートされており、これを通じてフォーティネットは、マルチレイヤ セキュリティ インテリジェンスと新たに台頭する脅威に対するゼロデイ保護を提供することが可能となっています。FortiGuard のサブスクリプション サービスを契約しているお客様には、すべての FortiGate、FortiMail および FortiClient 製品に対して上記のアップデートが適用されます。

「[最新の脅威動向に関するレポート](#)」 は現在ご覧いただけます。いくつかのカテゴリおよび特定の部門での脅威の上位ランキングも掲載されています。現在進行中の調査結果は、[FortiGuardセンター](#)または[FortiGuard Lab](#)の[RSSフィード](#)を通してご覧いただけます。セキュリティ テクノロジーおよび脅威分析に関するさらなる見解は、Fortinetの[セキュリティに関するブログ](#)およびフォーティネットの月間[Security Minute](#)ビデオキャストでご覧いただけます。

フォーティネットについて (www.fortinet.com)

フォーティネットは (NASDAQ: FTNT) ネットワーク セキュリティ アプライアンスのワ

ワールドワイド プロバイダであり、統合脅威管理 (UTM) のマーケット リーダーでもありません。フォーティネットの製品とサブスクリプション サービスは、ダイナミックなセキュリティ脅威に対抗する広範で高性能な統合プロテクション機能を提供しつつ、IT セキュリティ インフラの簡易化も実現します。フォーティネットの顧客には、米フォーチュン誌が選出する 2009 Fortune Global 100 の大部分を含む世界中の大規模企業、サービスプロバイダ、行政機関が名を連ねています。フォーティネットのフラグシップである FortiGate 製品は ASIC による高速なパフォーマンスを誇り、アプリケーションやネットワークの脅威から保護する多層セキュリティ機能が統合されています。フォーティネットの幅広い製品ラインは UTM にとどまらず、エンドポイントからデータベースやアプリケーションなどの境界やコアに至る大規模エンタープライズのセキュリティを保護します。フォーティネットは本社をカリフォルニア州サニーベールに構え、世界中にオフィスを展開しています。

Copyright© 2011 Fortinet, Inc. All rights reserved. ® と ™ のマークはいずれも、Fortinet, Inc.、その子会社および関連団体の米国における登録商標および未登録の商標であることを示します。フォーティネットの商標には、Fortinet、FortiGate、FortiGuard、FortiManager、FortiMail、FortiClient、FortiCare、FortiAnalyzer、FortiReporter、FortiOS、FortiASIC、FortiWiFi、FortiSwitch、FortiVoIP、FortiBIOS、FortiLog、FortiResponse、FortiCarrier、FortiScan、FortiAP、FortiDB、FortiWeb がありますが、これだけにとどまりません。その他の商標は、各所有者に帰属します。フォーティネットは、サードパーティに帰する本書での声明や認可について中立的な立場で実証してはならず、またフォーティネットはそのような声明を保証することはありません。本ニュースリリースには、不確実性や仮説を伴う前向きな内容が含まれている場合があります。不確実性が現実になったり、あるいは仮定が正しくないことが判明したりした場合、そうした前向きな声明や仮説で表明または暗示された内容とは実質的に結果が異なる場合があります。史実に関する声明を除くすべての声明は、前向きな声明であると判断されるべきものです。フォーティネットは、どの前向きな声明についても改正する義務を負わず、またこれらの前向きな声明を改正する方針もありません。