



報道発表資料

2011年11月8日

フォーティネットジャパン株式会社

米国時間 2011 年 11 月 1 日に発表されたプレスリリースの抄訳です。

フォーティネットが脅威動向調査で、高度に進化した Android マルウェアの攻撃が活発化していることを警告

DroidKungFu が、巧妙なボットネットとして活動開始。追加のマルウェアをダウンロード、アプリケーションやブラウザの開始、ファイルの削除などを実行。

ネットワークセキュリティのリーディングプロバイダーであり、UTM (Unified Threat Management : 統合脅威管理) ソリューションの世界的リーダーである、フォーティネット (Fortinet, Inc. 本社 : 米国カリフォルニア州サニーベール NASDAQ : FTNT)は本日、10月の脅威動向に関するレポートをリリースしました。今月、FortiGuard Labs は新しい DroidKungFu マルウェアが攻撃を活発化していることを検知しました。そのマルウェアは、複数の亜種を持っていることが発見され、PC 上で発見されたマルウェアに極めて類似した攻撃行動をとります。

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。「DroidKungFu はモバイル マルウェアが更なる進化を遂げていることを明らかに表しています。Zeus のモバイル版 (Zitmo) などの Android マルウェアによる初期の攻撃は、たとえば、口座所有者がログインの際に銀行が使用する本人確認の方法である二要素認証の入力を途中で盗み取ることが可能ですが、DroidKungFu はそれ以上の攻撃行動を実行します。正規の VPN クライアント アプリケーションに偽装することで、DroidKungFu はソーシャルエンジニアリングによりデバイスのルートアクセスを素早く盗み取ります。一旦それが実行されたら、DroidKungFu はマルウェアのダウンロード、ブラウザでの URL へのアクセス、プログラムの開始、システム上のファイル削除を行うことができるようになります。」

URL 短縮サービスの脅威

TinyURL などの URL 短縮サービスは、特定の受信者に対して長くて扱いにくい Web サイトのアドレスを短縮して、送信する便利な機能を提供します。ユーザが短縮されたリンクをクリックすると、Web サイトのオリジナルのアドレスに即座にリダイレクトされます。URL 短縮サービスは通常の Web アドレスで文字数を削減することができるので、Twitter ユーザ間で人気があります。これは E メール送受信にも頻繁に使用されています。なぜなら、Eメールのアプリケーションの中には送受信中に長いリンクは改行するものがあるからです。しかし、URL 短縮サービスは、ユーザのシステムにマルウェアを感染させるために準備された悪意のある Web サイトへのリンクを犯罪者が難読化させることができるので、このサービスのメリットは最大の弱点にもなり得ます。ユーザが疑わしい URL に遭遇したら、そのリンクが実際疑わしいページにリダイレクトされるのかを確かめるために、クリックする前にその URL にカーソルを置いてみることをフォーティネットは以前からずっと推奨してきました。この安全対策は短縮された URL には適用することができません。悪意のあるサイトにリダイレクトされそうになった場合にユーザが短縮された URL をクリックしないように、前もって知らせる確かな方法がありません。

Manky は続けて次のように述べています。「アンチスパムの技術が発達したことによって今日の短縮されたリンクのマルウェアの大半を検知できるようになりました。しかし、悪意のあるソフトウェアの作成者が最新のスパム検知技術を回避するために自身の URL 短縮サービスを作るようになってきました。これはサイバー犯罪者が提供する“サービスとしての犯罪 (CaaS : crime as a service)” のもう一つの例です。

短縮された URL が悪意のあるサイトを指しているかどうかを判断する一つの方法は、リンクの最後にあるドメインをチェックすることです。確認された悪意のある URL 短縮サービスのほとんどは最近、.info ドメインを使用しています。短縮された URL が悪意のあるサイトにリダイレクトしているかどうかを判断する別の方法として、フォーティネットの URL Lookup などの URL フィルタリング ツールに疑わしいリンクを貼り付けることができます。最後に、適切な Web フィルタリング ソリューションは、ドメイン名を判定し、確認するため、悪意ある URL 短縮サービスに対抗するのに役立ちます。

FortiGuard Labs について (www.fortiguards.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。

最新のウイルス対処状況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 Labs 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す。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 2010 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 などがありますが、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

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。