

プレスリリース

ブラチスラバ、2011年2月16日

Facebook を狙う最新マルウェアへの注意喚起

ブラチスラバ - Facebook ユーザーはここ最近、Win32/Yimfoca.AA や Win32/Fbphotofake をはじめとする、大量のワームの標的にされています。Win32/Yimfoca.AA にいたっては最近数週間、オーストリア、イタリア、チェコ、スロバキアなど多くのヨーロッパ諸国で、ThreatSense.Net によるマルウェアランキングのトップテンにランクインしています。

ESET のマルウェア研究者である Marek Polesensky によると、Yimfoca ワームは Facebook チャットを利用して攻撃し、ソーシャルエンジニアリングを利用するワームである Fbphotofake は Facebook からの通知を装ったスパムを通じて自身や別のマルウェアを広めます。Polesensky は、「Yimfoca はリモートからコントロール可能なワームで、感染の拡散には Skype や MSN Messenger、Yahoo Messenger などのインスタントメッセージャーも利用される」と述べています。さらに、Yimfoca は偽のアンチウイルスソフトウェアなど、インターネット上の別の悪意のあるソフトウェアをダウンロードして実行することもできます。実行されると、セキュリティ設定の意図せぬ変更や Windows ファイアウォールの無効化に至ります。Fbphotofake ワームは、主に Facebook スパムを介して感染を広めます。ユーザーは、不審な添付ファイルや未知の添付ファイルを開いたり、疑わしいリンクをクリックしたりしないよう十分に注意してください。

インスタントメッセージャーワームの Win32/Yimfoca.AA



Facebook ワームの Win32/Fbphotofake



ESET のシニアリサーチフェローである David Harley は最近のマルウェア攻撃に関して、Facebook がますます「ナイジェリアの手紙」詐欺に悪用されていると指摘しています。「人々の慈悲の気持ちに付けこみ、それほど労せずして金銭を搾取る一般的な詐欺行為の類だ」と Harley は述べ、ユーザーに対し、「差出人の身元、およびインスタントメッセージャーや Facebook のメッセージ内容について怪しい点がないか常に注意する必要があります」と忠告しています。ESET 北米のテクニカルエデュケーション担当ディレクターである Randy Abrams は、「Facebook が狙われる要因の 1 つはセキュリティの認識が全社的に低い点で、セキュリティ専門家にとっては非常に厄介な障害だ」と指摘しています。

Facebookを狙う最新脅威の注目点は次のとおりです。

- Win32/Yimfoca.AA ワームは最近数か月にわたり感染を拡大しており、多くのヨーロッパ諸国で ThreatSense.Net によるマルウェアランキングのトップテンにランクイン。
- Fbphotofake は、Facebook スпамを介して感染を広める。いずれのワームには十分に注意を払う必要があり、不審な添付ファイルや未知の添付ファイルを開いたり、疑わしいリンクをクリックしたりしないようにする。
- 「ナイジェリアの手紙」詐欺も同様に、Facebook を介して広がっている。
- Facebook のセキュリティアップデートなどの情報については、<http://www.facebook.com/security> を参照。

ThreatSense.Net®について

ThreatSense.Net®は、世界中の ESET ソリューションのユーザーからのデータを活用した、「In-the-Cloud(インターネット上)」のマルウェアの情報収集システムです。継続的な情報収集が可能のため、ESET のウイルスラボの専門家は世界中のマルウェア攻撃の性質と範囲をリアルタイムかつ正確に把握できます。ESET は、脅威とその攻撃手段、パターンについて慎重な分析を重ね、ユーザーを今後の脅威から保護するためにあらゆるヒューリスティックとシグネチャの更新を細かくチューニングしています。

ESET 社について

1992 年に設立された ESET は、コンシューマおよび法人向けのセキュリティソリューションを提供しているグローバルプロバイダです。ESET のプロアクティブなマルウェア検出技術は業界随一の性能と実績を誇り、ESET NOD32 Antivirus は Virus Bulletin 誌が主催する「VB100 Award」の最多受賞回数を記録しているほか、1998 年の同アワード開始以来、「In-the-Wild(実際に感染報告がある)」のワームおよびウイルスについて一度も検出漏れがないという記録を保持しています。

ESET はスロバキアのブラティスラバに本社を、米国カリフォルニア州サンディエゴ、アルゼンチンのブエノスアイレス、チェコのプラハ、シンガポールに事業所を構えるほか、ブラティスラバ、サンディエゴ、プラハ、ポーランドのクラクフ、カナダのモントリオール、ロシアのモスクワにマルウェアのリサーチセンターを開設しています。また、180 か国に広範なパートナーネットワークを築いています。ESET は、ヨーロッパ、中東、およびアフリカ地域において最も急成長を遂げている企業の 1 つとして、Deloitte の Technology Fast 500 に継続して選出されています。