proofpoint

Proofpoint Threat Report

November 2014

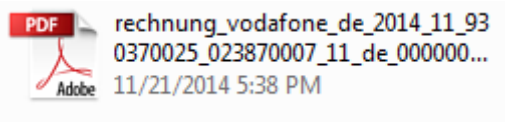
本レポートは、Proofpoint が注目し、お客様および一般企業に対して注意を喚起したいと考えている様々な脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat Models (手法)

ドイツのはえ縄型攻撃が「Emotet」マルウェアをインストール

ここ数週間、Proofpoint の研究者は大規模なメール攻撃を観測しています。ドイツのユーザーを狙ったフィッシング攻撃で、「Emotet」バンキングマルウェアに誘導します。この攻撃は、レピュテーションフィルタを出し抜くために、一日に数十もの侵害された Web サイトを使い捨てることができます。ZIP ファイルとそれにリダイレクトさせるための URL には「rechnung_vodafone_de.zip」のように、餌となるメールに関連する名前が付けられており、実行ファイルを含んでいます。その実行ファイルにも、「rechnung_vodafone_de_2014_11_930370025_023870007_11_de_0000003837_888830.exe」のように、メールの内容に関連する名前が付けられています。さらに、ユーザーに安全なファイルだと思い込ませるために、PDF の(あるいはそれに似た) アイコンが使われています。

ファイル名を長くすることによって拡張子を目立たなくさせ、さらに正規のアイコンと組み合わせることによって攻撃成功の確率を高めています:



ほとんどのアンチウイルスソフトはこのマルウェアを検知することができず、最初の攻撃を検知できたエンジンは 4%以下でした。

最新の攻撃で観測されたメールテンプレートのサンプルは以下の通りです:

Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 (Nr. 4774055700252885)

245444-00104@t-mobile.de
November 21, 2014 at 12:29 AM
To: [redacted]
Ihre Telekom Mobilfunk RechnungOnline Monat November 2014 (Nr. 4774055700252885)

T

ERLEBEN, WAS VERBINDET.

Ihre Rechnung, November 2014

Guten Tag,

mit diesem Schreiben erhalten Sie eine Benachrichtigung über Ihre aktuelle Rechnung. Die zur Zahlung fällige Summe für November 2014 beläuft sich auf: **245,86 Euro**.

Im Anhang finden Sie die gewünschten Dokumente zu Ihrer Mobilfunk RechnungOnline für November 2014. Rechnung_2014_11_46289058_A_1229474_R_91_7237.pdf

Das ist eine automatische generierte Nachricht. Bitte antworten Sie nicht auf diese E-Mail.

Mit freundlichen Grüßen

Ralf Hoßbach
Leiter Kundenservice

24,95
€

ネット投票をハックして PDF 投票用紙を通信途中に改ざん

インターネットを使った投票の試みは、セキュリティ上の懸念からアメリカでは広くは行われていません。

先頃行われた中間選挙の直後、オレゴン州ポートランドのコンピュータサイエンス研究開発企業である Galois は、有権者と選挙機関に対してリマインダーを送り、状況が思わしくないことを知らせました。

Modifying an Off-the-Shelf Wireless Router for PDF Ballot Tampering (http://galois.com/wp-content/uploads/2014/11/technical-hack-a-pdf.pdf) をご覧ください。Daniel M. Zimmerman と Joseph R. Kiniry によって作成されたこの論文は、家庭用の一般的なルーターが攻撃され、PDF 投票用紙が送信される際にハッカーによって改ざんされる恐れがあることを指摘しています。

PDF 投票用紙はアラスカのインターネット投票の試みで使用されており、ハリケーンサンディで住宅を失った有権者のための代替投票手段としてニュージャージーでも使われています。投票用紙をダウンロードし、記入してメールに添付して送信します。このメールは投票所で投票用紙を投票箱に入れるのと同じ行為と見なされます。選挙機関はこれを印刷して手作業で集計するか、OCR で読み込んで集計します。

Galois による指摘は、おそらくネット投票に関連する脅威のひとつに過ぎないでしょう。この他にも、有権者のコンピュータに感染したマルウェアがトラフィックをリダイレクトしたり、選挙機関に対する DoS 攻撃を行ったりする攻撃があるかもしれません。しかし、この論文で解説されている攻撃手法は、より見つけにくく、十分に目的を果たします。研究者は、フォレンジック解析によっても見つけることは困難だろうと言っています。

「私たちは、(PDF 投票券が) 有権者のコンピュータと選挙機関の間の電子メールシステムを通過する際に、トランスポートレベルで生データを変更する巧妙な攻撃について解説しています。」と、Zimmerman と Kiniry は書いています。

ハッカーがトラフィックストリームの中に入り込むことができれば、投票用紙を傍受し、PDF 内のデータを改ざんして投票結果に影響を与えることができるのです。

Threat News (ニュース)

サイバークライムの犯罪者達はホテルの WiFi を使ってどのようにして出張中の企業幹部を狙うのか

「Darkhotel」として知られる洗練されたマルウェア攻撃は、有名企業の幹部を狙うためにアジアやその他の世界中の高級ホテルの WiFi を利用します。

Kaspersky Lab の「Darkhotel espionage campaign」(Darkhotel のスパイ攻撃) によると、この攻撃は過去 4 年間にわたって行われており、今日もホテルやビジネスセンターの WiFi を使って高い情報価値を持つ世界中のターゲットを狙っています。

Kaspersky Lab の Costin Raiu (Director of Global Research and Analysis) によると、ハッカー達は組織的に運用されており、同じ標的を 2 度は狙わないと言うことです。

Kaspersky Lab は、顧客の感染数が増加していることを自社のセキュリティネットワークを介して観測し、この攻撃に気づきました。

Darkhotel の攻撃は続いています。全体の感染数は数千に上っており、今後も増え続けるとみられています。

全体のプロセスの詳細な説明および運用上の回避策については以下をご覧ください:

http://abcnews.go.com/Technology/cyber-crime-gang-targets-travelling-executives-hotel-wi/story?id=26806725.

ID 詐欺が増加: 情報流出の 61%が盗まれたログイン情報によるもの

Javelin Strategy & Research が発表した「*2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends*」によると、2013 年には 1,310 万人のコンシューマが ID 詐欺によって持続的な被害を被っているということです。これは過去 2 番目に高い数値です。

トレンドの一つは、既存のカードアカウントに関する詐欺と損失が増えていることです。既存のカードアカウントとは、アカウント番号と実際のカード、およびそのカードに紐付けられているデビットカードを含みます。既存アカウントの詐欺による被害は 45%増えて 1,600 億ドルに達し、アメリカ全体の詐欺被害の 88%を占めています。

詳しい情報はこちらでご確認下さい: http://www.duosecurity.com/blog/identity-fraud-rises-61-percent-of-breaches-caused-by-stolen-credentials.

「悪意のあるフィッシング攻撃は、企業が考えているよりも遙かに効果をあげている」と専門家が指摘

ハッカーによる執拗な攻撃が続いているにも関わらず、多くの組織では未だにセキュリティ対策に十分な優先度が当てられていません。そのため、サイバー犯罪者による進化し続ける攻撃に対して脆弱なままです。

セキュリティ専門家の Neira Jones によると、組織はサイバー犯罪者からデータを守らなければならない事態に追い込まれても、「必要最小限の対策もできていない」ということです。最大の理由は「サイバーセキュリティへの認識の欠如」です。

Jones の分析はこちらでご覧いただけます:
http://www.computing.co.uk/ctg/news/2382628/malicious-phishing-attacks-are-far-more-effective-than-most-businesses-realise-claims-expert.

Threat Insight Blog (ブログ)

Proofpoint のセキュリティブログである Threat Insight から、興味深い記事をピックアップしました。皆様も Threat Insight のディスカッションに是非ご参加ください。
http://www.proofpoint.com/threatinsight.

感謝祭後はフィッシングの季節

アメリカでは感謝祭後のブラックフライデー、サイバーマンデー以降、年末セールが始まります。サイバー攻撃が急増する季節でもあります。

フィッシングやスパムは今やよく知られる攻撃手法となっていますが、最近ではソーシャルメディアが新しい攻撃ツールを提供しています。多くの企業では未承認メールに対する対策がとられていますが、ソーシャルメディアを使ったスパムやフィッシング攻撃には未だ対応しきれていません。これらの攻撃には、電子メールを止めても効果が無いのです。

典型的な攻撃手法について、こちらで開設しています:
http://www.proofpoint.com/threatinsight/posts/tis-the-season-to-be-phishy.php.

マルバタイジングに狙われたストリーミングメディアサイト

Proofpoint の研究者によると、有名なライブビデオ配信プラットフォームがマルバタイジング攻撃の被害を受けました。このサイトが利用しているオープンソースの広告サーバーである OpenX への大規模なインジェクション攻撃 (今でも続いています) の影響で、このサイトは訪問者に対してマルウェアをばらまいてしまったのです。このケースは、インジェクションされた JavaScript の運用についての良い教材となります。

感染したサイトから配信されたエクスプロイトにより、Web サイトを訪れただけで (クリックなどをしなくとも) マルウェアに感染します。

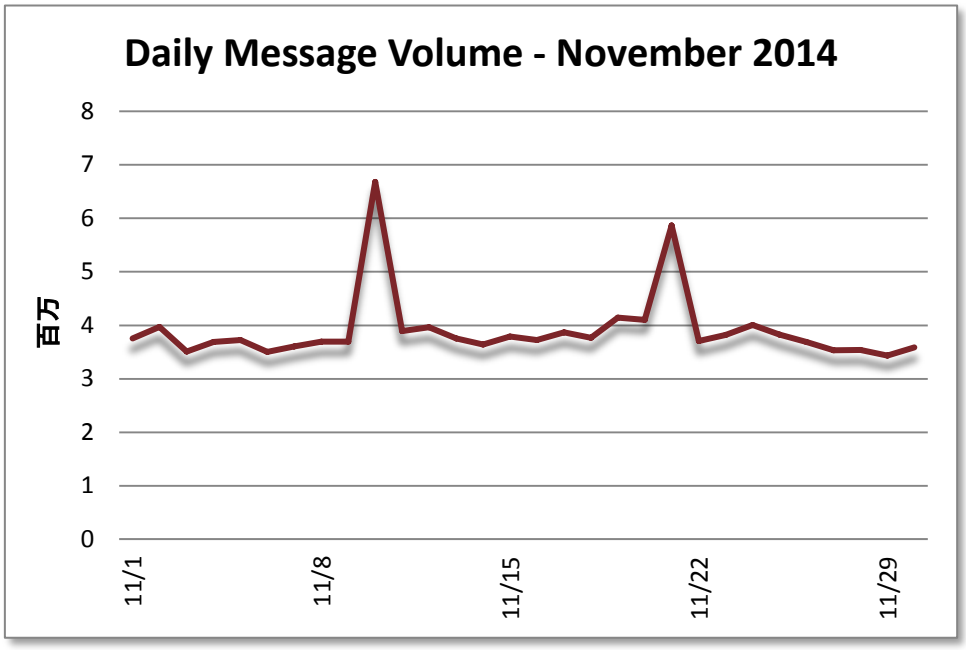
Proofpoint は感染したサイトのオーナーに連絡を取り、協力して問題の解決にあたっています。

このサイトから配信されたマルウェアと、その他の興味深い事実についてはこちら:
http://www.proofpoint.com/threatinsight/posts/streaming-media-site-hit-by-malvertising.php.

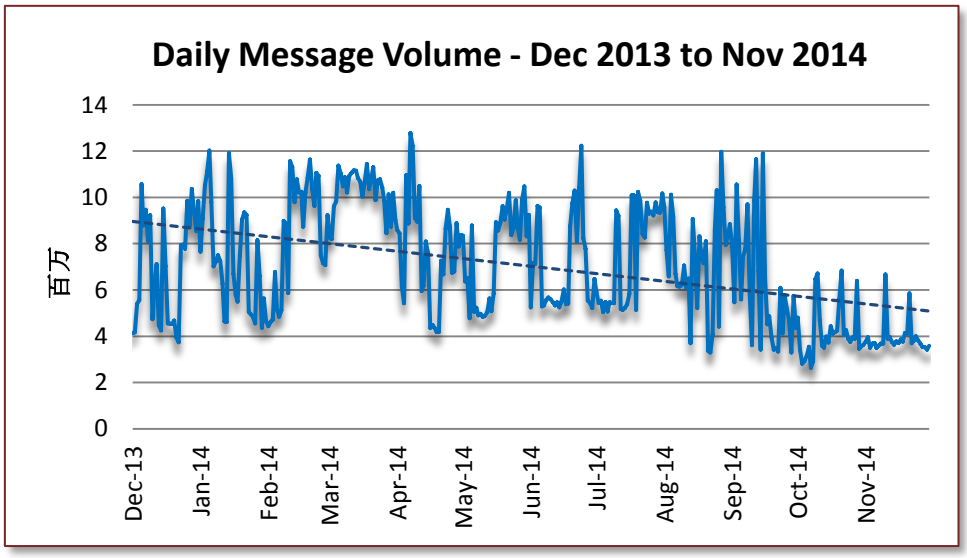
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

Proofpoint では、スパム量についてハニーポットを使って追跡していますが、この値は Proofpoint のお客様からの報告ともほぼ一致します。11 月第 1 週のスパム量は 400 万通以下で推移しましたが、第 2 週初めに 700 万通に急増しました。その直後にまた 400 万通付近で安定し、第 4 週が始まる直前にまた 600 万通に急増しています。そしてまた元のレベルに戻り、月末までこのレベルが続きました。



10 月から 11 月にかけてのスパム量は若干(6.21%)減少し、前年比では 13.7%の減少となっています。



Spam Sources by Country (スパム発信源)

中国が 10 月に引き続き 1 位の座を勝ち取りました。EU は僅差で 2 位です。アメリカがそれに続き、ロシアは 4 位に落ち、アルゼンチンが 5 位となりました。

以下は過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

		Jun '14	Jul '14	Aug '14	Sep '14	Oct '14	Nov '14
Rank	1st	EU	EU	EU	EU	China	China
	2nd	Vietnam	US	US	Vietnam	EU	EU
	3rd	US	China	Argentina	China	Russia	USA
	4th	China	Argentina	Russia	Argentina	Vietnam	Russia
	5th	Russia	Russia	China	Korea	USA	Argentina

以下の表は、各国が総スパム量に占める発信量の割合を示したものです。EU の数値は全加盟国を含んでおり、以前よりも正確に傾向をつかむことができます。中国は全体の 20.60%を配信して 2 ヶ月連続で 1 位となり、残りの 4 カ国を合わせると 34.30%となり、中国を上回ります。

October 2014			November 2014		
1	China	18.82%	**1**	China	20.60%
2	EU	15.61%	**2**	EU	20.06%
3	Russia	9.25%	**3**	USA	7.81%
4	Vietnam	5.10%	**4**	Russia	4.66%
5	USA	3.65%	**5**	Argentina	1.77%

この他の情報については以下をご覧ください
www.proofpoint.com/threatinsight

proofpoint

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com