

# Proofpoint Threat Report

December 2015

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)

### DarkSideLoader – もう、マルウェアを見つけるために iPhone で「脱獄」する必要はありません

その昔、“rogue app store” (闇 app store – Apple を通さずにアプリを配信するサイト) のソフトウェアをインストールしようとする iOS ユーザーは、Apple の制限を解除するために iPhone を「[Jailbreak \(脱獄\)](#)」させる必要がありました。このプロセスによって、様々な無料・海賊版・違法なソフトウェアにアクセスできるようになりますが、もっと重要なことは、アプリベースのマルウェアからのアクセスも可能になることです。

しかしこの 12 月、Proofpoint の研究者は「iPhone や iPad を *Jailbreak* させずに、100 万本のアプリをダウンロードできる闇 app store を発見しました。」こうした闇サイトにアクセスした場合、デバイスに侵入されるリスクは非常に高く、脱獄していないデバイスを介してリモートアクセストロージョンや悪意のあるコンフィグレーションファイルをダウンロードさせられたり、企業や個人の情報を盗み出すための橋頭堡を築かれる可能性もあります。

Proofpoint の研究者はこのタイプの闇 app store を「DarkSideLoader」と名付けました。これまで不可能だったアプリ (良いアプリであれ悪いアプリであれ) の迂回ダウンロードを可能にしたからです。

正規の app store にも危険なアプリはありますが、これらの闇 app store は「riskware」と呼ばれるソフトウェアの主要なソースです。ユーザーが最低限気をつけなければならないのは、どのようなソースからのものであれ、インストールするアプリには気をつけなければならないということです。一見無害に見えるアプリでも、パーミッションを操作したり、悪意のありそうなサーバーや侵害されたサーバーにアクセスしたり、ネットワークデータにアクセスしたりすることは驚くほど多いのです。

DarkSideLoader に関する Proofpoint の専門家の解説と一見無害なアプリが個人や組織に与える脅威については以下をご覧ください:

- <http://proofpoint.com/us/threat-insight/post/DarkSideLoader-Rogue-App-Stores-Targeting-Non-Jailbroken-iOS-Devices>
- <http://www.proofpoint.com/us/threat-insight/post/Risky-Mobile-Apps-Steal-Data>

## Angler エクスプロイトキットを新たな方法で活用するマルバタイジング攻撃

ドメインシャドウイングは通常、盗み出したレジストレーション認証情報を使って、正規のドメインの下に悪意のあるサブドメインを作成します。攻撃者は一見問題無さそうに見えるこれらのサブドメインを使ってレピュテーションベースのフィルターをくぐり抜け、攻撃者の指定するエクスプロイトキットへユーザーを誘導します。

Proofpoint の研究者は、あるマルバタイジング攻撃が、広告ネットワークやある種のセキュリティインフラの何層もの防御階層をバイパスして Angler エクスプロイトキットを配信するためにシャドードメインを使っていることを発見しました。この研究者は「マルバタイジングが変化することにより、今後数ヶ月間はマルウェアの有効な配信方法であり続けるでしょう。」と言っています。

マルバタイジングでのシャドウドメインの活用についての詳細は、こちらをご覧ください: <http://proofpoint.com/us/threat-insight/post/The-Shadow-Knows>

## Gootkit が勢力を拡大

Gootkit は JavaScript ベースのバンキングトロージャンで、元々はフランスの銀行のユーザーを狙っていました。2015 年を通じて勢力を拡大し、Angler エクスプロイトキットを使って直接、あるいは Bedep トロージャンを使って間接的に PC に感染することが知られていましたが、2015 年 3 月にはイタリアの銀行が狙われ始めました。Proofpoint の研究者は 11 月末までに、カナダ及びイギリスでの Gootkit 攻撃を観測しています。

イギリスでは、いくつかの金融機関の顧客を狙って、Anglerを使ったマルバタイジング攻撃の最後に Gootkit が投下されます。この動きは、かつて地域限定だったマルウェアでも、攻撃者が新たな標的を探してその範囲を広げていくことを示しています。

Proofpoint の研究者による Gootkit の最新情報は、こちらからご確認下さい: <http://proofpoint.com/us/gootkit-banking-trojan-jumps-channel>

## Threat News (ニュース)

### Proofpoint の研究者が 2016 年のサイバーセキュリティ予測を発表

Proofpoint の研究者は毎年、過去のデータと現在のトレンドをベースに、その年の最大のサイバーセキュリティの予測を発表しています。2016 年については、相変わらず「人的要因」が最大の問題として残り、攻撃者はエンドユーザーを狙ってソーシャルエンジニアリングによる成功を狙うでしょう。サイバーセキュリティツールは日々進化していますが、エンドユーザーはそうはいかないからです。

Proofpoint の研究者は、エンドユーザーが 2016 年もサイバー犯罪者の主要な標的になることの他に、以下の様なトレンドがあるだろうと予測しています:

- 入手してそのまま使える便利なマルウェアにより、攻撃がより簡単で低コストになり、練度の低い犯罪者でも成功の確率が高まるでしょう。
- サイバー犯罪者は攻撃の範囲を広げるでしょう。例えばバンキングトロージャンであれば、これまでのようなオンラインバンキングの利用者ではなく他の標的を狙ったり、エンドユーザーの PC ではなく ATM やその他の組込み機器を狙ったりするでしょう。
- 「Next Big Thing」がやってきます。添付ファイルベースの仕組みが限界に達しつつあるという証拠が増加しています。
- ソーシャルとモバイルの脅威が続き、個人にも組織にも大きな危険となります。

詳細とその他の予測についてはこちらをご覧ください:

<https://www.proofpoint.com/us/threat-insight/post/Cybersecurity-Predictions-for-2016>.

## 税の季節 – マルウェアペイロードを配信する IRS メールがやってくる

アメリカではもうすぐ税金の申告シーズンですが、サイバー犯罪者は既に IRS (Internal Revenue Service: 米内国歳入庁) の名前を騙る税関連の攻撃を開始しています。

[SCMagazine](#) などが報じた最新の税関連のフィッシング攻撃は、メールの受信者が IRS からの税還付を受けられると注意喚起するものです。

興味深いことに、このメールには JavaScript を含んだ ZIP ファイルが添付されており、この JavaScript ファイルがペイロードをダウンロードするために Windows PowerShell を起動します。これは ZIP ファイルが開かれた瞬間に行われます。

このペイロードを詳細に解析したところ、Kovter (最初のペイロード) と CoreBoT (2 番目のペイロード) の 2 つのペイロードファミリーが含まれていました。

詳細はこちらをご覧ください: <https://heimdalsecurity.com/blog/security-alert-fileless-kovter-teams-modular-corebot-malware-irs-spam-campaign/>

## BBC の Web サイトが攻撃によりオフラインに

最近、大規模な Web 攻撃が BBC の全ての Web サイトを一時的にアクセス不能に追い込み、DDoS 攻撃の威力を見せつけました。[DDoS 攻撃](#) は、大量のアクセス源から膨大なトラフィックを送り込んでオンラインサービスを麻痺させる攻撃です。

攻撃はグリニッジ標準時 12 月 31 日木曜日の午前 7 時にサイトを襲い、サイト訪問者はエラーメッセージに迎えられました。BBC が復旧を発表するまで、障害は 4 時間に及びました。4 時間とはいえ影響は大きく、インターネット解析企業の comScore によると、イギリスの訪問者数で Google と Facebook に遅れをとったということです。

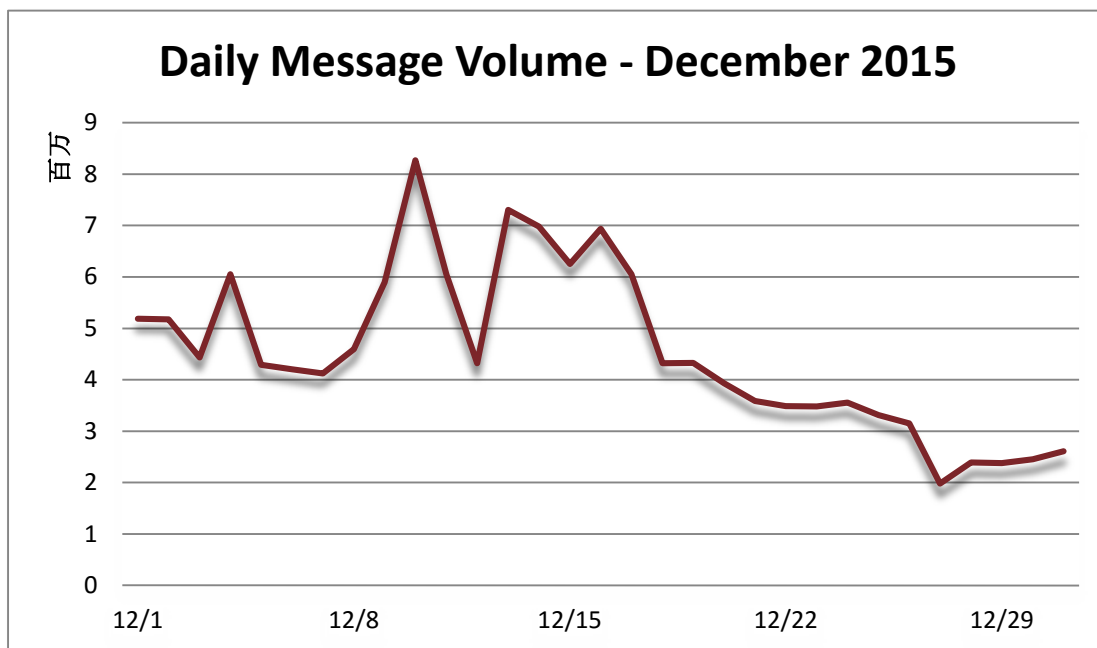
世界的に DDoS 攻撃の規模は拡大しており、「平均的」な攻撃でも、悪意のあるトラフィックは毎秒 1 ギガビットに達します。攻撃から復旧するためのインフラが BBC よりも弱い組織については、サイトダウンのリスクが非常に高いといえるでしょう。

詳しくはこちらをご覧ください: <http://www.bbc.com/news/technology-35204915>.

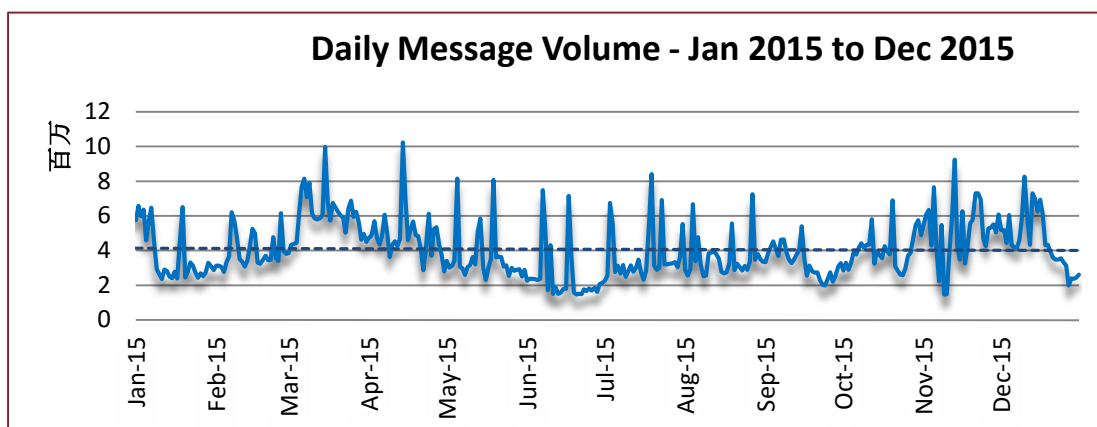
## Threat Trends (トレンド)

### 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。12 月のスパム量はクリスマス休暇が始まるまでは非常に高いレベルでした。12 月第 2 週にはスパム量が 800 万通/日を超えましたが、第 3 週には落ち始め、月の後半は 400 万通を下回り、年末は 200 万通と 300 万通の間で終わりました。



休暇に関連した落ち込みにより、月間スパム数は 11 月に比べて 11.6%減少しました。しかし、前年同月に比べると 10.8%の増加です。



## Spam Sources by Region and Country (スパム発信源)

過去数ヶ月、EUは突出して世界最大のスパム発信源でしたが、12月は中国がアメリカを抜いて2位になり、EUに迫っています。ロシアが4位で、ベトナムが5位に返り咲きました。

以下の表は、過去6ヶ月間のスパム配信量上位5カ国です。

		Jul '15	Aug '15	Sep '15	Oct '15	Nov '15	Dec '15
Rank	1 <sup>st</sup>	EU	EU	U.S.	EU	EU	EU
	2 <sup>nd</sup>	U.S.	U.S.	China	China	U.S.	China
	3 <sup>rd</sup>	China	China	EU	U.S.	China	U.S.
	4 <sup>th</sup>	Russia	Vietnam	Russia	Russia	Russia	Russia
	5 <sup>th</sup>	Vietnam	Russia	Vietnam	Indonesia	Panama	Vietnam

以下の表は、各国が総スパム量に占める発信量の割合を比較したものです。EUの数値はすべての加盟国を含んでおり、より正確な比較ができます。EUは全世界のスパムの18.57%を配信しており、残りの4カ国を合わせると34.7%で11月よりも大幅に増えました。EUは比率を少し落としています。

November 2015			December 2015		
1	EU	19.09%	1	EU	18.57%
2	U.S.	11.22%	2	China	13.99%
3	China	9.72%	3	U.S.	13.21%
4	Russia	5.47%	4	Russia	4.73%
5	Panama	2.25%	5	Vietnam	2.78%

以下は、先月と今月のEU内のスパム配信量上位5カ国の表です。

November 2015			December 2015		
1	Germany	2.35%	1	Germany	4.79%
2	Italy	2.07%	2	UK	1.20%
3	U.K.	1.54%	3	Spain	1.10%
4	Romania	1.11%	4	France	0.93%
5	Spain	1.04%	5	Bulgaria	0.89%



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

**proofpoint™**

Proofpoint, Inc.  
 892 Ross Drive, Sunnyvale, CA 94089  
 Tel: +1 408 517 4710  
[www.proofpoint.com](http://www.proofpoint.com)