proofpoint

Proofpoint Threat Report

December 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)

Cybercrime-as-a-Service という新しい犯罪モデル

ユーロポール (欧州刑事警察機構) 内の欧州サイバー犯罪センター (European Cybercrime Centre: EC3) は先頃、サイバー犯罪は益々商業化しており、それは正規のサービスを隠れ蓑にする犯罪者の仕業であると指摘しました。

EC3 が発表した 2014 Internet Organised Crime Threat Assessment (iOCTA) レポート (https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta) によると、仮想的な地下組織で活動するサービスベースの犯罪産業が成長しており、他の犯罪者の利用に供するための製品やサービスを開発中であるとのことです。

EC3 の捜査官達はレポートの中で、「Crime-as-a-Service」のビジネスモデルがサイバーワールドに出現したために、技術的スキルを持たない犯罪者がサイバー犯罪に参入する障壁が低くなっていると指摘しています。

要旨の中で、「マフィアスタイル」の犯罪者集団が、これらのスキルやツールを入手するために、いかにしてこのマーケットに参入しようとするかが強調されています。

EC3 レポートはまた、サイバー犯罪者は匿名化や暗号化、あるいは仮想通貨などの正規のサービスやツールを悪用して、違法な活動を行っているとも指摘しています。

ただでさえ複雑な状況に加え、2014 iOCTA が指摘しているのは、これらの犯罪者は主に EU の司法権が及ぶ範囲外で活動しており、法的手段の陳腐化や対応能力の欠如から、これらの犯罪者を裁判にかけることができないという問題が露呈されているということです。

法執行におけるこのような複雑な問題は、警察が適切な人員や手段を入手することの難しさによって、さらに困難になっています。現在のサイバー犯罪、特に組織的な犯罪は国境を越えて行われるため、最終的に法執行を成功させるためには、国際的な協力が必要ということです。

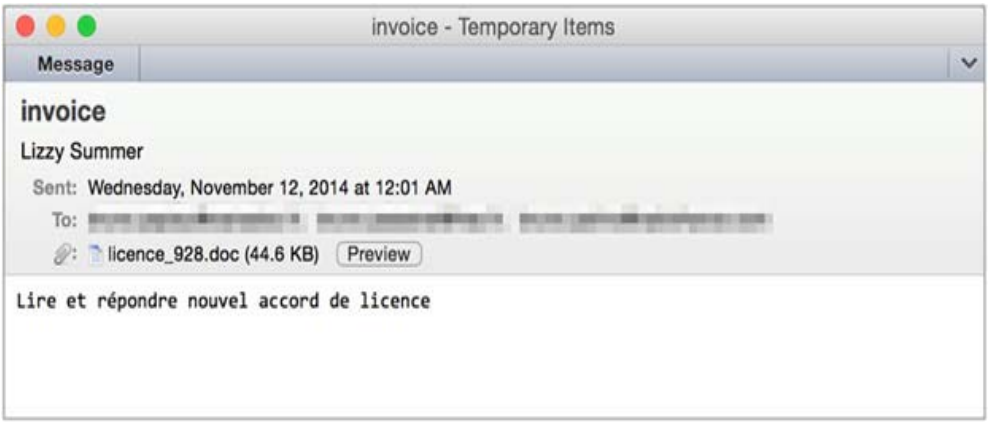
増え続けるこの種の犯罪に対しては、国際的な見地からの対応が必要です。

フィッシングは国際標準語

Proofpoint の研究者は、フランスとドイツの組織を狙ったボリュームが少ない標的型フィッシング攻撃を検知しました。この攻撃から、フィッシング攻撃が複数の言語・国を狙っていることが見えてきました。攻撃者が防御をかいくぐるために、言語自体を変数として扱ったことがわかったのです。

この攻撃では、12 種類の Microsoft Word の添付ドキュメントが確認されています。これらはレピュテーションベースの防御を逃れるために、複数の送信者により交互に送られ、見出しも変えて古典的な「はえ縄型攻撃」を形成しています。添付ファイルを自動解析したところ、Andromeda あるいは Gamarue マルウェアをダウンロードしてインストールする悪意のあるマクロが含まれていました。マクロと Andromeda ペイロードは難読化されており、攻撃がアンチウイルスエンジンを逃れる確率を上げています。Proofpoint がこれを解析した時には、添付ファイルを検知できたアンチウイルスエンジンは 10%未満で、Andromeda ペイロードの検知率は 5%でした。

また、この攻撃にはフランス語とドイツ語のメールテンプレートが含まれており、様々な餌、件名、メール本文が用意されています。例えば、以下のフランス語のメールは受信者に対して最新のライセンス契約書を読んで回答するよう求めており、ドイツ語のサンプルには請求書が含まれ、1 月 1 日までに支払うよう求めています。



これらのサンプルは単一の攻撃で使われたものであり、添付ファイル名、餌、件名、送信者アドレスに様々なバリエーションがあることがわかります。このため、こういった近代型のはえ縄型攻撃は、レピュテーションやシグネチャベースの防御システムに対して有効なのです。

教訓は以下の通りです: 企業や組織は既存のアンチスパムゲートウェイを補完する為の先進的な検知機能を持つべきです。例え既存の防御システムが最高のものであったとしても、それが従来型である限り、十分ではありません。

Threat News (ニュース)

データ流出の損害賠償を巡る争いが過熱

誰がデータ流出の責任をとるべきなのでしょうか? 新年を迎え、小売業者と銀行の間でどちらが高額の賠償を支払うかについて、見解の相違が表面化してきました。

現在、小売業におけるデータ流出を取り扱う法的なフレームワークはほとんど存在せず、そのために小売業者と銀行は、攻撃を受けたのが誰の責任なのかを言い争って、2014 年の大半を使ってしまいました。

これらの法的責任に関する問題の多くは、データ流出法制によって解決できることに注意が必要です。連邦議会は 2014 年を通じて、最低限のデータセキュリティ標準を制定しようとして複数回のヒアリングを行いましたが、未だに具体的な提案は出てきていません。

小売店と銀行の言い分、そしてその他の興味深い事実についてはこちらをご覧ください。

http://thehill.com/policy/cybersecurity/228161-the-fight-over-paying-for-data-breaches-heats-up

2015 年はスピアフィッシングがより大きな問題に (これまで以上に銀行員が狙われる理由とは)

2014 年には、スピアフィッシングは銀行幹部などを狙うサイバー攻撃の多くで効果を上げたため、ハッカーは今年も銀行の利用者では無く、銀行の職員を狙うフィッシング攻撃にエネルギーを注いでいます。これは、本質的には銀行そのものを狙っていると言えます。

ハッカーは信憑性の高いメール攻撃で銀行の職員を狙います。職員を騙して悪意のあるリンクをクリックさせたり、アカウント保有者とそのアカウントに関する詳細な情報をさせたりし、いったんクリックするとログイン情報やその他の機密情報が侵害され、そして詐欺が始まります。

職員が何故それほど狙いやすいのか、その他の興味深い情報もこちらから。

http://www.bankinfosecurity.com/spear-phishing-bigger-concern-in-2015-a-7742

2014 年のサイバー法制の世界的なトレンド

世界的なサイバー犯罪の観点から見ると、サイバー犯罪とハッキングの問題は巨大で困難なものです。2014 年はサイバー犯罪が数でも深刻さでも脅威を増した年と言うことができます。

それが発しているメッセージは明確です。洗練された防御無しには、どのようなコンピュータシステムもネットワークもサイバー犯罪に対して対抗しえないのです。

インシデントの生々しい現状、恐るべき統計データ、サイバー法制の現状などについて、こちらをご覧ください。http://www.business-standard.com/article/technology/emerging-global-cyberlaw-trends-in-2014-115010500301_1.html

2014 年のボットネット: ZeuS の急伸、厳格で無いポリシーが Web ユーザーを危機に

2015 年は、ボットネットの進化や新手のセキュリティ侵害の登場が容易に予想できることから、セキュリティの展望も変わってくるでしょう。

ボットネットはますます一般的なツールとなっており、Spamhaus プロジェクトの *Botnet Summary for 2014* で指摘されているように、活動は活発化しています。

ボットネットを運用している犯罪者達は、機密の金融や銀行情報、個人情報などを集めることができ、それらは闇市場で取引されます。

これらの金融・個人情報の価値が高くなれば、ボットネットの利用も増えるわけです。企業はこの流れを止めるために何をしているでしょうか? 事実と統計を読み、いくつかの助言に耳を傾けて下さい。

http://www.zdnet.com/article/botnets-in-review-2014-zeus-surge-lax-policies-place-web-users-at-risk/

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.

Dyreza as a Service

10 月号の本レポートで“Dyreza”または“Dyre”と呼ばれるバンキングマルウェアをご紹介しました。今回の記事は、より複雑な *Dyreza as a Service* についてです。

Dyre は、侵入したコンピュータ上にできるだけ長く留まるために、自らを *Google Update Service (googleupdate)* というサービスとしてインストールします。このサービスは、他のあらゆるサービスが立ち上がるときにロードされ開始されます。本体の実行ファイルは Windows フォルダから実行され、拡張子.exe を持つ様々な名前のファイルを使います。

この製品は、そのプロセスの複雑性と困難さによって証明されているように、常に革新を続けています

続きはこちらから: http://www.proofpoint.com/threatinsight/posts/dyreza-as-a-service.php.

2015 年のサイバー犯罪予測

2014 年は、10 億人規模のユーザー情報漏洩、重要なインフラの侵害、ビジネスの中断による深刻な損失などのデータ流出事故が相次ぎ、洗練された情報セキュリティの必要性がクローズアップされた年でした。

サイバー犯罪者は常に改善を続けています。彼らの戦略と技術力は継続して進化しています。

2015 年は、より精密な調査が不可欠になるでしょう。深刻な影響を及ぼす新規の先進的な脅威を作り出そうとするサイバー犯罪者に対抗するためです。

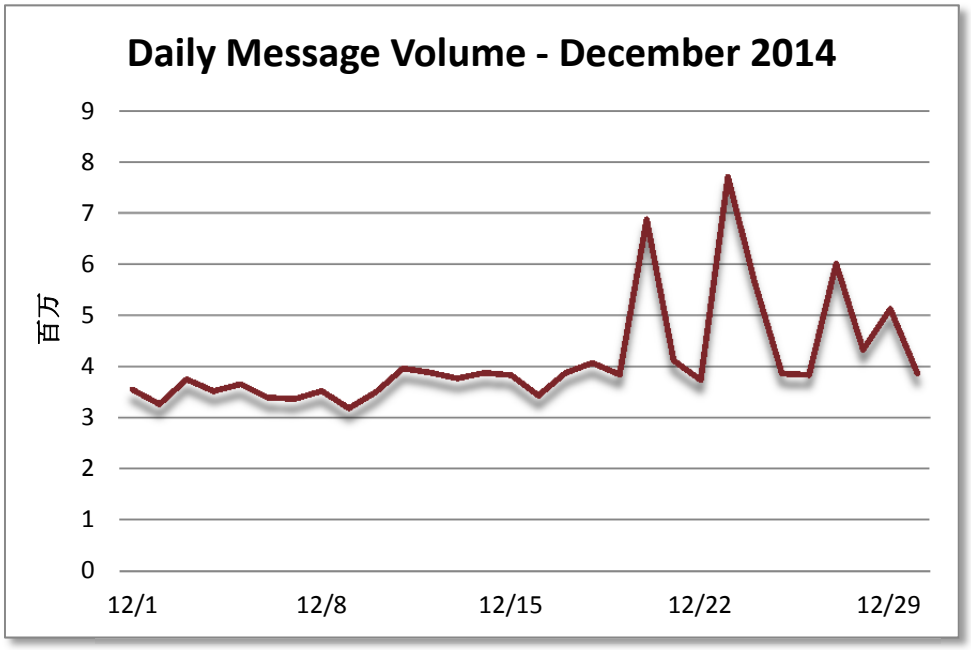
2015 年の最初に、どの脅威が攻撃してくるのか、Proofpoint の専門研究者や科学者達からのアドバイスをお聞き下さい。

http://www.proofpoint.com/threatinsight/posts/cybersecurity-predictions-for-2015.php.

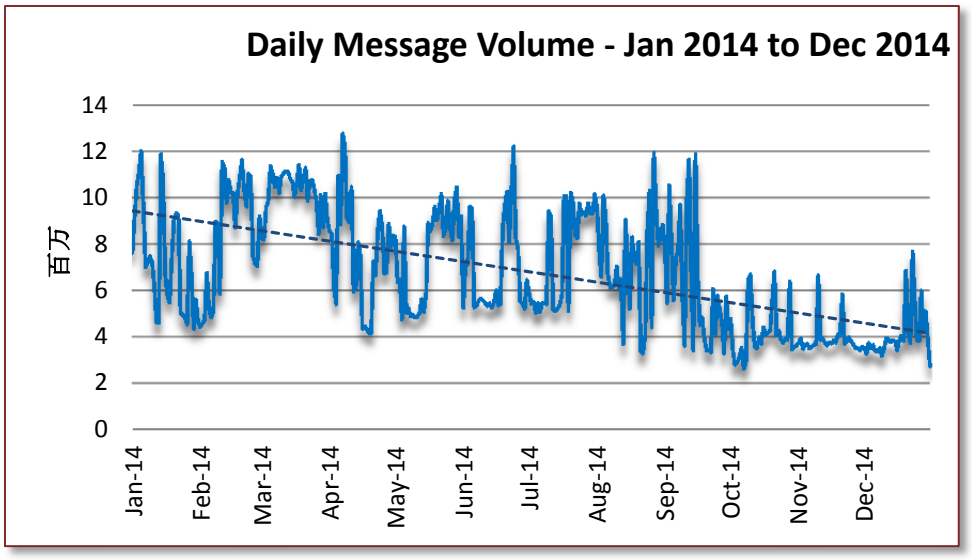
Threat Trends (トレンド)

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。12 月のスパム量は第 3 週の中頃まで 300 万～400 万通/日の間を変動し、第 3 週の中頃には 400 万通に達しました。その後、4 回の様々な値 (700, 750, 600, 500 万通) のピークがあり、最初の 2 回の急増の後は 400 万通まで落ち込み、3 回目の急増では 425 万通、最後の急増で 400 万通に落ち込んで 12 月を劇的に終りました。



11 月と 12 月を比較するとスパム量は若干 (4.98%) 増加していますが、前年同月比では 40.88%の大きな落ち込みとなっています。



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

EU が長年の強さを見せつけて 1 位に返り咲き、中国は 14%もの大差を付けられて 2 位に落ちました。USA が 3 位でロシアが 4 位です。ベトナムが 5 位に入り、トップ 5 に戻ってきました。

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。

		Jul '14	Aug '14	Sep '14	Oct '14	Nov '14	Dec '14
Rank	1st	EU	EU	EU	China	China	EU
	2nd	USA	USA	Vietnam	EU	EU	China
	3rd	China	Argentina	China	Russia	USA	USA
	4th	Argentina	Russia	Argentina	Vietnam	Russia	Russia
	5th	Russia	China	Korea	USA	Argentina	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。EU は全体の 24.49%のスパムを生み出しており、第 1 位です。残りの 4 カ国を足しても 25.36%にしかならず、EU を少し上回る程度です。

November 2014			December 2014		
1	China	20.60%	**1**	EU	24.49%
2	EU	20.06%	**2**	China	10.34%
3	USA	7.81%	**3**	USA	6.71%
4	Russia	4.66%	**4**	Russia	4.36%
5	Argentina	1.77%	**5**	Vietnam	3.95%

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