

Proofpoint Threat Report

June 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)

脅威インテリジェンスとビジネスインテリジェンス

先頃 Proofpoint が発表した *The Human Factor 2015* (<https://www.proofpoint.com/us/threat-insight/post/The-Human-Factor-2015>) にも触れられているように、サイバー犯罪者による技術の革新と攻撃への適用は果てしなく続いており、検知を逃れ、システムへの侵入を成功させるための新しい手法が次々に見つかっています。犯罪者達は常にビジネス構造を見直して、その手法が有効かどうかを追跡しています。成長と収益性をどう最適化するかが重要なのです。

Proofpoint の研究者は、悪意のあるマクロ制作者の一部で使われている追跡手法に注目しました。この手法は極めてシンプルです。ユーザーがマクロ (VBScript のバッチファイル) の「コンテンツを有効化」を行うと、さらにいくつかのファイルが生成されます。(生成される数は Windows のバージョンによって変わります) これらのファイルは順番に実行され、マルウェアのペイロードをダウンロードし、さらにイメージホスティングサービスからイメージファイルをダウンロードします。このダウンロード数を数えれば、マルウェアの感染数を知ることができるわけです。この「統計機能付きマクロ」は 2015 年の 2 月頃に発見されたもので、以下に詳細があります。

<https://www.proofpoint.com/us/threat-insight/post/When-Threat-Intelligence-Meets-Business-Intelligence>.

この手法を見ると、犯罪者達が技術的な戦略を選択する際にビジネス上の指標を重視していることがわかります。

さらに最近では、この統計機能に進化が見られました。マクロが2つのイメージをダウンロードするようになったのです。一つは、ペイロードがダウンロードされた時点で、そしてさらにマルウェアの感染を確認した後に別のイメージがダウンロードされます。実際の例とその解析についても、上記リンクでご確認いただけます。

イメージ追跡による統計の活用は、攻撃者が「標準的な」メールセキュリティシステムをすり抜ける効率を劇的に向上させたことを物語っています。さらに、マルウェアペイロードをインストールして標的のシステムに侵入する成功率は70%以上と見られています。これはセキュリティ担当者にとって重要な脅威インテリジェンスであり、同時に自らの攻撃を評価しなければならない攻撃者にとっては重要なビジネスインテリジェンスなのです。

Ramnit Botnet 解体から学ぶべき教訓

この有名なボットネットの解体は、ビッグデータの活用によるものでした。今年2月、ユーロポールはMicrosoft、Symantec、AnubisNetworksと協力してRamnitボットネットの解体作業を主導しました。

「侵害されるかもしれないではなく、何時侵害されるかという問題だった」ということが、セキュリティコミュニティ共通の認識になっていました。侵害を防ぐだけでは不十分だったのです。インシデントが起きてから、それを検知して復旧するための戦略は、全体のプロセスの一部であるべきだということです。

ほとんどのケースで、組織は何が起こっているのかを把握しておらず、データが流出していることや自分たちがハッカーに狙われていることをわかっていないという厳しい現実があります。企業イメージの失墜や売上の喪失は計画性 – 基本的な脅威インテリジェンス – の無さから生まれる副産物なのです。

詳しくはこちらでご確認下さい:

<http://www.darkreading.com/endpoint/lessons-learned-from-the-ramnit-botnet-takedown/a/d-id/1320861>.

Threat News (ニュース)

日本年金機構の攻撃には旧来の手法が使われた

日本の年金システムがハックされ、外部からのメールウイルスによって不正アクセスを受けた職員のコンピュータから 100 万件以上の個人情報 (基礎年金番号と氏名、生年月日、住所) が流出しました。

ハッカーは昔ながらの「標的型メール攻撃」を使ったと考えられています。

日本年金機構は攻撃を 5 月 19 日に警視庁に届け出ました。攻撃元はまだ明らかになっていませんが、一部のマスメディアによると、Backdoor.Emdivi というトロイの木馬が使われたということです。興味深いことに、このトロイの木馬は 2014 年末に見つかった重要インフラのセキュリティ侵害にも関わっていたということです。このマルウェアは非常に洗練度されており、これまでも度々注意を喚起されています。

警察の捜査は今も続いています。

データ流出は、職員がメールに添付されたファイルを開いた時に起こりました。添付ファイルは厚生労働省の書類を装っていました。以下は本事件の概要です。

- 年金情報の流出は約 101 万人分
- 4 情報 (基礎年金番号と氏名、生年月日、住所) の流出は約 1 万 5000 人分
- 約 101 万人のうち受給者は約 53 万人分、被保険者は約 49 万人分

詳しくはこちらでご確認下さい:

<http://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/#.VXhyWkZSUXh>

<http://www.nenkin.go.jp/n/data/service/0000028648uArRENS1eQ.pdf>

レントゲン機器も危険?: 病院ネットワークへのマルウェア感染に医療機器が関与

セキュリティ企業の TrapX は、放射線治療機器を含む医療関連のデバイスが攻撃者に利用されていると警告しています。

TrapX のレポートによると、病院ネットワークの「重大な」侵害は明らかに増えており、「侵害された医療機器がマルウェアの感染とデータ流出の痕跡を隠してしまう」ということです。

TrapX のレポートによると、攻撃者は放射線治療機器を含むセキュリティ保護されていない医療機器を使い、ヘルスケアネットワーク上に居場所を見つけ、セキュリティソフトウェアや IT スタッフからの検知を免れていました。

このレポートには、TrapX が顧客であるヘルスケア企業や医療機器アナリストなどから得た詳細な情報も含まれています。

TrapX は、医療機器の中でも特に PACS (picture archiving and communication: 放射線画像処理技術) システムはセキュリティシステムからチェックすることが難しく、病院ネットワークに感染するマルウェアの足がかりとなり、IT 資産を狙う攻撃の温床となることを明らかにしています。

詳しくはこちらをご覧ください:

https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf.

このレポートは「医療機器は、標準的な情報機器よりも無防備で、ヘルスケア機関をリスクに晒している」と結論づけています。

レポートの締めくくりは衝撃的です。TrapX の科学者達は「多くの病院は現在マルウェアに感染しており、それが何ヶ月もの間、あるいは何年もの間、放置されているのです。」

この示唆に富むレポートはこちらからご覧ください:

<https://securityledger.com/2015/06/x-rays-behaving-badly-devices-give-malware-foothold-on-hospital-networks/>

ホワイトハウスが 2016 年末までに連邦政府の Web サイトを標準で暗号化するよう要求

米国政府は、来年末までに一般からアクセスされる Web サイトおよび Web サービスの全てで HTTPS (HyperText Transport Protocol Secure) の利用を義務づけます。HTTPS に限定された指針が示されたのは初めてのことです。

簡単に言えば、HTTPS の採用は政府の Web サイトでのユーザー認証セッションを暗号化するということです。このプロトコルは現在利用できるインターネット技術のなかでも、Web 接続において最も効果的にプライバシーを守ることができるものとされています。

連邦政府の説明をご覧ください: <https://https.cio.gov/>.

現時点では、連邦政府の機関のうち 28%しか暗号化を行っていません。今 HTTPS を使っている Web サイトは whitehouse.gov, cia.gov, nsa.gov,

and omb.gov などです。驚いたことに dhs.gov (米国土安全保障省) もまだ HTTPS を使っていません。こちらをご覧ください

<https://pulse.cio.gov/https/domains/>

さらに言えば、HTTPS は 2 つのシステムの間接続しか保護しません。システム自身の真正性については保証できません。HTTPS は Web サーバーがハックされたり侵害されたりすることを防ぐことはできません。また、Web サービスが通常の運用時にユーザー情報を流出させないよう、保護するようにも作られていません。

詳しくはこちらからどうぞ:

<http://www.darkreading.com/application-security/white-house-calls-for-encryption-by-default-on-federal-websites-by-late-2016/d/d-id/1320789?>

世界の大規模データ流出

世界のデータ流出事件をまとめたサイトです:

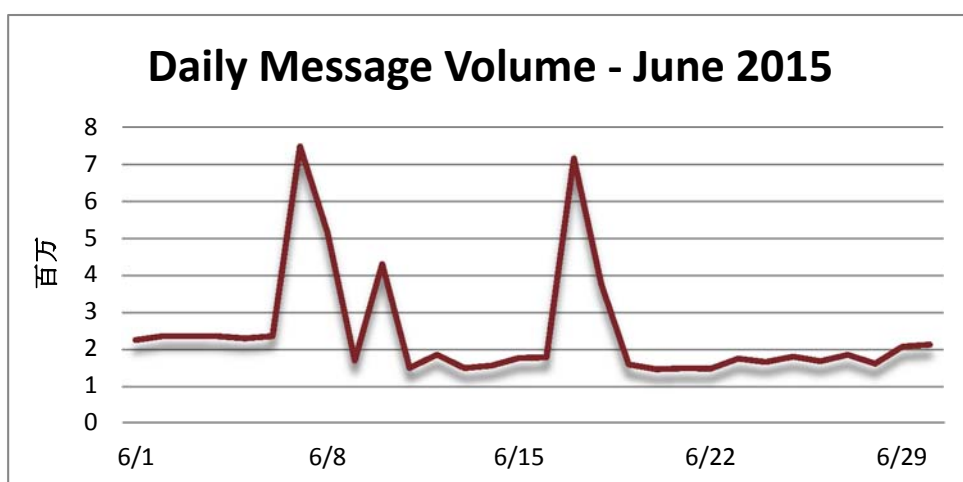
<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

このインフォグラフィックスは、3 万件以上のデータ流出事件の一部を表示しています。

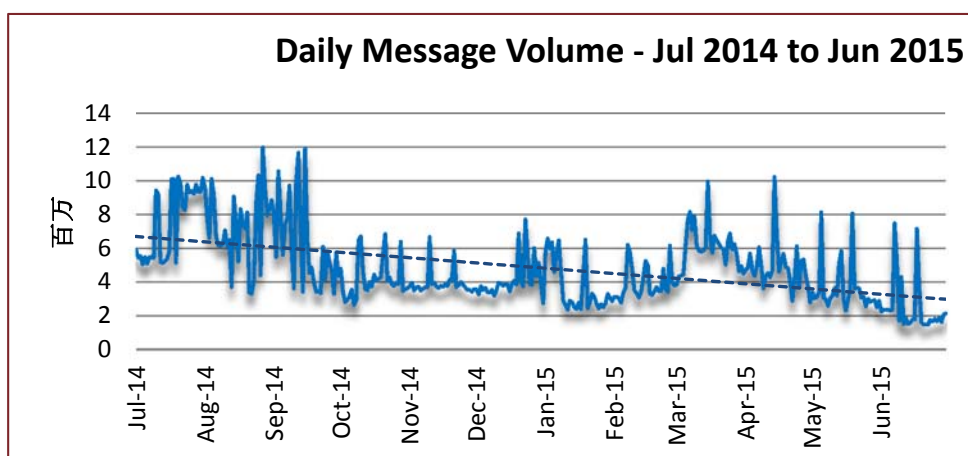
Threat Trends (トレンド)

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。6 月のスパム量は大荒れでした。月初めに 200 万通/日で始まったスパム量はいきなり 700 万通/日に跳ね上がりました。すぐに 200 万通まで急降下し、その後 400 万通まで上がったと思うと、また 200 万通まで減少しました。数日間そのままのレベルをキープした後、第 3 週にはまた 700 万通のピークを記録しました。このピークもすぐにおさまり、6 月の残りは 200 万通で推移し、そのまま月末を迎えました。



5 月と 6 月を比べると、スパム量は 30.33%減少しました。前年同月と比べると、64.33%の減少です。



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

国別のスパムの発信量では、EU が相変わらずトップで US が 2 番です。この順位は 6 ヶ月間変わっていません。その後中国、ロシアが続き、5 位にアルゼンチンが入りました。

以下の表は、過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

	Jan '15	Feb '15	Mar '15	Apr '15	May '15	Jun '15
Rank	1 st	EU	EU	EU	EU	EU
	2 nd	US	US	US	US	US
	3 rd	Vietnam	Vietnam	Russia	China	China
	4 th	Argentina	Argentina	India	India	Russia
	5 th	China	Russia	China	-	Indonesia

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 は全体の 29.15% を配信しており、残りの 4 カ国を合わせても 21.83% で、EU に遠く及びません。

May 2015			June 2015		
1	EU	23.59%	1	EU	29.15%
2	US	11.98%	2	US	12.11%
3	China	9.11%	3	China	4.80%
4	Russia	4.27%	4	Russia	2.52%
5	Indonesia	2.09%	5	Argentina	2.40%

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。

May 2015			June 2015		
1	Germany	2.27%	1	Germany	4.71%
2	Spain	2.04%	2	Spain	3.48%
3	Italy	1.92%	3	Romania	3.10%
4	Netherlands	1.87%	4	Italy	2.67%
5	France	1.42%	5	Bulgaria	1.65%



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