proofpoint

Proofpoint Threat Report

May 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)

インシデントレスポンスの自動化に関するベストプラクティス

2015 年初め、Proofpoint の研究者はインシデントレスポンスのプロセスにおける主要なフェーズについて検討しました。デジタルフォレンジック及びインシデントレスポンス (DFIR) をひとつのまとまりとしてとらえ、現在の検知・予防ツールにおける重要性に注目したのです。その結果は「インシデントレスポンスの自動化は、セキュリティの自動化の流れの中で自然な進化である」ということです。これは効果的な DFIR のための鍵のひとつです。

自動化とは、情報収集のための API 呼び出しから自動的なネットワークの切り離し、アカウントの無効化までのあらゆるプロセスを含みます。

インシデントレスポンスのプロセスに自動化を適用するために、以下のユースケースやベストプラクティスを参考にして下さい。当然のことながら、目指す方向性は高い効果と効率性です。

■明らかに必要な自動化

自動化のためには、まず最初に、インシデント担当者がどのようにして彼らのミッションを遂行するのかを理解する必要があります。攻撃者と攻撃対象に注目することで、プロセスはシンプルになります。その攻撃は:

- 財務部門のような主要な部門を狙っているのか?
- ソースコードのサーバーを狙っているのか?
- CFO や上級管理職が被害に遭っているか?
- 狙われたシステムは感染しているか?
- 普段ビジネス上の付き合いの無い国からの攻撃か?
- 攻撃は既知の CCS (command and control server) から行われているのか?
- 攻撃は情報リストにある IP から行われているか?
- マルウェアを使った攻撃について、少数のアンチウイルスツールでのみ検知できるのか、ほとんどのツールで検知できるのか?

セキュリティ警告を手作業で収集し、統合してデータセットを構成するのは時間がかかる退屈な作業です。また、よく知られているように人間はミスを犯します。つまり、このプロセスは大変な上にミスの可能性をはらんでいます。

インシデントレスポンスの初期段階に自動化を組込んでおくことは、効果的で効率的なレスポンスのために非常に重要です。

■既存、あるいは生成されたデータの処理を自動化

インシデント担当者は解析の後、予防のための対策を立てなければなりません。しかしその前に、集めたデータセットを徹底的に解析し、処理する必要があります。詳しくは以下をご覧ください。

https://www.proofpoint.com/us/threat-insight/post/Best-Practices-in-Incident-Response-Automation

理想は、インシデントに関する詳細なデータを含んだドキュメントがひとつのファイルに統合されることです。この情報により正確な状況認識が可能になり、その結果、効率的な優先度付けが可能になります。

このフェーズにおける主要なベストプラクティスについて、以下で解説しています:

https://www.proofpoint.com/us/threat-insight/post/Best-Practices-in-Incident-Response-Automation

その他のプロアクティブなアクションやアドバイスについては以下をご覧ください:

https://www.proofpoint.com/us/threat-insight/post/Best-Practices-in-Incident-Response-Automation

GPU マルウェアは WindowsPC や Mac にも影響

ある開発者グループが、グラフィックスカード上で動作する Linux 向けのルートキットを開発しました。彼らはその後、Windows で動作するマルウェアのサンプルも開発し、Mac OS X 版についても開発中とのことです。

この開発者グループの狙いは、マルウェアが GPU (graphics processor unit) 上でも動作することを広く告知することです。

開発者によると、既存のセキュリティツールには GPU 上のメモリ (RAM) をスキャンしないという問題があります。

Windows 用のサンプルマルウェア (デモ用) は「WIN_JELLY」と呼ばれており、Remote Access Tool (RAT) あるいはトロイの木馬として動作します。

RAT は侵害したコンピュータを越えて遠隔操作を行う事ができ、近年の標的型攻撃でも多く使われています。

詳しくは、以下でご確認下さい。

http://www.itworld.com/article/2921095/gpu-malware-can-also-affect-windows-pcs-possibly-macs.html

Threat News (ニュース)

欧州最大の航空会社が 500 万ドルのサイバー犯罪の犠牲に

Ryanair が 500 万ドルの国際銀行間取引攻撃の標的になりました。

このアイルランドの航空会社は最近、中国の銀行経由の詐欺的な電子送金について捜査を受けました。関係者と銀行との共同調査の結果、資金は凍結されていることがわかり、それは近日中に返金される模様です。実際に盗難に遭った金額は少額でしたが、この事件は銀行及び金融システムを狙ったサイバー犯罪の脅威を浮き彫りにしました。

Scotiabank の Guy Haselmann 氏はこの攻撃について「新たな冷戦」と呼んでいます。彼の著作である「*The Invisible Army*」には、オバマ大統領が一般教書演説の中で海外からのサイバー脅威を「国家的危機」と宣言したことが触れられています。Haselmann 氏の明快な論拠と表現は、新たな冷戦がサイバー戦争の一部であることを示しています。

Ryanair はこの種の送金が 2 度と起こらないよう、対策を行うと言うことです。詳しくは以下をご覧ください。

http://www.zerohedge.com/news/2015-04-29/europe%E2%80%99s-largest-airline-falls-prey-5-million-cyber-theft

アノニマスが数千台のホームルーターを使ったボットネットを運用したとして告発される

貧弱なセキュリティは、アノニマスに代表される様々なハッカーグループの活動を許してしまいます。サイバーセキュリティ企業の Incapsula によると、数十万台のホーム及びオフィス向けインターネットルーターが乗っ取られたと言うことです。

ハッカーがルーターを狙う手口は、工場出荷時のユーザー名とパスワードを使う方法です。Incapsula は、これは ISP とユーザーによる「不可解な怠慢」によるミスと言っています。

乗っ取られたルーターはほとんどがアメリカ、タイ、ブラジルのもので、異なる種類のマルウェアに感染していました。これらのルーターは、2014 年 12 月末から始まった無数の標的に対する攻撃に使われたボットネットを構成しています。(ボットネットはマルウェアに感染したコンピュータのネットワークであり、犯罪者の指示によりスパムメールを配信したり、Web サイトを攻撃したりします)

この静かな攻撃と、恐るべき怠慢によるセキュリティの欠如についての詳細は、以下をご覧ください:

http://www.dailydot.com/politics/botnet-incapsula-research-report-default/

これに関連して、Proofpoint では数ヶ月前に少数の組織を狙った 4 週間にわたるスパム攻撃を観測していました。この攻撃は最初、ブラジルのインターネットユーザーを狙っていました。ブラジル最大の ISP からのメールを装っており、未払いの料金についての警告についてのものです。特筆すべきは、このメールのリンクをクリックすると、その ISP から提供されたルーターをハックする仕掛けが施されていたことです。

これは最終的にはオンラインバンキングのアカウント情報やその他の重要情報を取得することを目的としています。

レポートと Proofpoint の Kevin Epstein のコメントをご覧ください。

http://krebsonsecurity.com/2015/02/spam-uses-default-passwords-to-hack-routers/

https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm

データ流出の平均コストが 380 万ドルに

組織に被害を及ぼすサイバー攻撃がより頻繁に、より広範囲で起こっています。Ponemon Institute の調査によると、攻撃の結果組織が負担するコストは増加しています。データ流出によるコストの世界的な平均は 380 万ドルに上り、昨年の 350 万ドルから増加しました。また、悪意のある、あるいは犯罪的なサイバー攻撃の頻度が増えていることも明らかになりました。

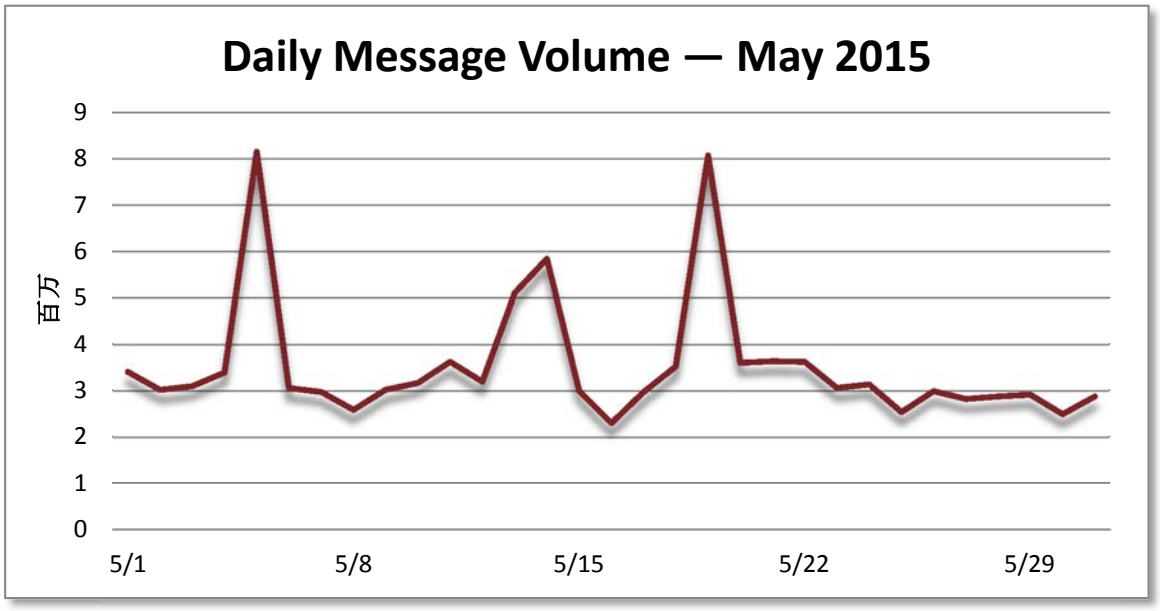
Ponemon が毎年行っている「*Cost of a Data Breach*」調査では、上級管理職を狙った強力な攻撃についてまとめています。いくつかの企業名を挙げると、JPMorgan Chase、Sony、Target などです。レポートでは、悪意のある、あるいは犯罪的な流出は増えており、よりコストもかかるようになっていると結論づけており、その他にも気になるニュースがあります。詳しくは以下でご確認下さい。

http://ww2.cfo.com/data-security/2015/06/data-breach-costs-climb-average-3-8m/

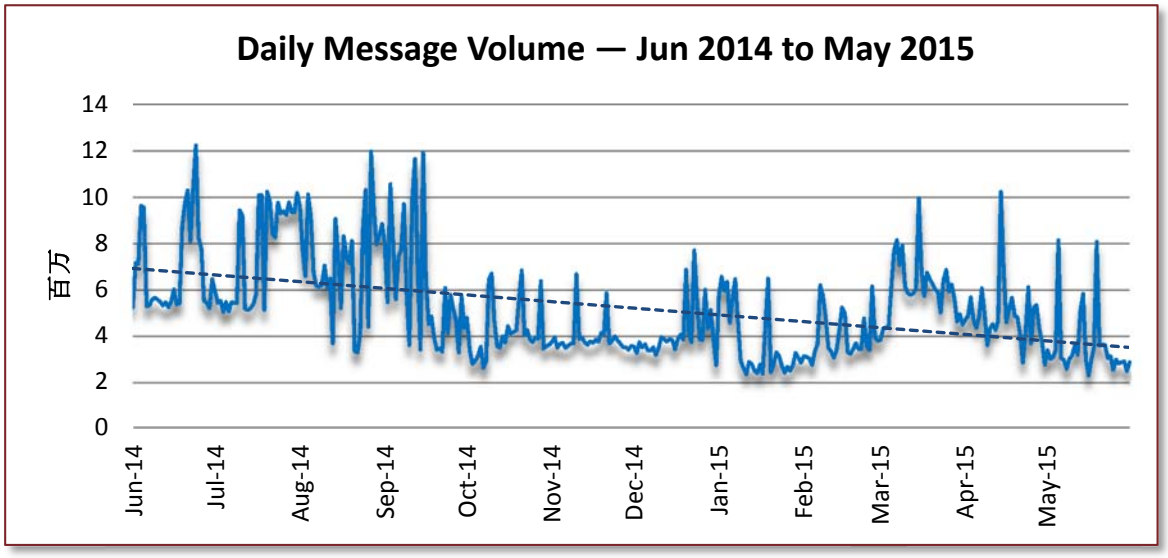
Threat Trends (トレンド)

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。5 月のスパム量は振り子のように上下しました。300 万通/日で始まり、その週の中頃にはいきなり 800 万通に達し、その後また 300 万通に戻りました。第 2 週も第 1 週と似ており、250 万通から 600 万通の間でした。第 3 週はまた最高で 800 万通まで急伸し、その後 300 万通で月を終えました。



4 月と比較したスパム量は 27.16%減少し、対前年比では 52.66%の減少となりました。



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

EU が 6 ヶ月連続で第 1 位に輝き、アメリカは 2 位をキープしました。中国が引き続き 3 位、ロシアが 4 位に浮上しています。インドネシアが初めて 5 位に入りました。

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。

		Dec '14	Jan '14	Feb '15	Mar '15	Apr '15	May '15
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	China	US	US	US	US	US
	3rd	US	Vietnam	Vietnam	Russia	China	China
	4th	Russia	Argentina	Argentina	India	India	Russia
	5th	Vietnam	China	Russia	China	TBD	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 は全スパム量の 23.59%を配信しており、最大の配信国となっています。残りの 4 ヵ国を合わせると 27.45%となり、EU を上回っています。

April 2015			May 2015		
1	EU	14.45%	**1**	EU	23.59%
2	US	10.45%	**2**	US	11.98%
3	China	6.73%	**3**	China	9.11%
4	India	1.16%	**4**	Russia	4.27%
5	TBD	TBD	**5**	Indonesia	2.09%

The

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。

April 2015			May 2015		
1	Italy	1.09%	**1**	Germany	2.27%
2	Netherlands	0.84%	**2**	Spain	2.04%
3	UK	0.49%	**3**	Italy	1.92%
4	Germany	0.44%	**4**	Netherlands	1.87%
5	Czechoslovakia	0.43%	**5**	France	1.42%

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

