APR-JUN 2016

proofpoint™

QUARTERLY THREAT SUMMARY

Proofpoint Quarterly Threat Summaryは、プルーフポイントのお客様ベース及び一般のセキュリティマーケットから得られる情報を元に、プルーフポイントがその時々で注目する脅威及びトレンド、環境変化などについてまとめたレポートで、四半期毎に作成されます。プルーフポイントは毎日、10億通以上の電子メールメッセージ、数億件のソーシャルメディアへの書き込み、1億5千万個以上のマルウェアサンプルを解析しており、先進的脅威からユーザー、データそしてブランドを守っています。

これらの脅威が四半期毎にどのように変化しているかを知ることで、読者の皆様は、より大きなトレンドを見極め、行動のためのインテリジェンスを蓄え、セキュリティ環境を管理するための知見を得ることができます。私達は、メール、ソーシャルメディア、モバイルという3つの侵入経路に注目しながら、先進的脅威を監視しております。

www.proofpoint.co.jp

オーバービュー

大規模化、多様性、そして静寂

2016年の最初の5ヶ月間は、これまで見たことも無いほど大規模なマリシャス(悪意のある)メール攻撃に見舞われました。ランサムウェアの新たな亜種が急速に広まり、一方でDridexの攻撃者達はLockyランサムウェアの配信を開始しました。攻撃者達はセキュリティシステムによる検知を逃れるために、新たなローダーや添付ファイル形式、難読化技術などを使って、高い頻度で手法を変えています。

5月の終わりに、世界最大のボットネットのひとつが突然沈黙しました。これにより、DridexとLockyの配信はほとんど休止状態になり、同時にそれまで広く使われていたAnglerエクスプロイトキット(EK)の活動も確認できなくなりました。Angler EKはWebベースのサイバー攻撃を自動化するオールインワンのツールキットです。これらが重なり、6月は不気味なほどの静寂が訪れました。

偽のカスタマーサービスアカウントのようなソーシャルメディアの脅威は、引き続き大幅に増加しています。

モバイル分野の脅威は、複数の脆弱性を狙っています。これらの脅威は、被害者のデバイスを制御下に置くこととマリシャスなアドウェアの配信に注力しており、特に古いバージョンのAndroidを狙っています。

以下に2016年第2四半期(Q2)の主な傾向をまとめます。

EMAILとエクスプロイトキット

- **JavaScript添付ファイルが、マリシャスメッセージの爆発的増加を引き起こし、前四半期比で230%増加。**Locky及びDridexの攻撃者の多くが、ペイロードのインストールのためにJavaScriptファイルを使うようになりました。これらの攻撃は、私達がこれまで見たこともないほどの規模で、メッセージ数は1日あたり最大で数億通に達しています。
- **ランサムウェア: CryptXXXがEKトラフィックのほとんどを占め、同様にLockyがメールのほとんどを占拠。**マリシャスな添付ファイルを使うメール攻撃の中で、Lockeyランサムウェアを扱っているものが、Q2は全体の69%を占めました。Q1は24%でした。この急増によって、LockyはDridexを抜いてメールベースのマルウェアのトップに躍り出ました。CryptXXXはQ2になって突然現れ、EK分野でトップに立ちました。ランサムウェアの新たな亜種はほとんどがEKによって配布されますが、2015年Q4に比べて全体として5倍から6倍に増えました。
- **高度にパーソナライズされた攻撃が急増。**攻撃者は、高度にパーソナライズされた攻撃を数万から数十万通の規模で仕掛けてきます。これは、過去に見られたパーソナライズされ標的化された小規模な攻撃からの大きな変化です。
- **ビジネスメール詐欺 (BEC: Business Email Compromise) が驚異的な勢いで増加。**先月1ヶ月間だけでも、サンプルとして抽出したProofpointのお客様の80%が、最低1回のBECフィッシング攻撃を受けています。攻撃者はまた攻撃に使う餌を、所得税申告などの個人的なイベントから様々な他のアプローチに切り替えており、攻撃の効果を上げ規模を拡大しようとしています。
- **平穏な6月?** Proofpointの観測によると、4月から6月中旬にかけて、エクスプロイトキットのトラフィックが96%も減少しました。Necursボットネットが6月にオフラインになり、2016年の前半を主導してきたLockyとDridexが鳴りを潜めました。Angler EKのトラフィックは6月初めには消滅し、それからほどなくNuclear EKも活動を停止しました。6月末には、残されたNeutrinoがEKのトップの座につきました。
- **Lockyランサムウェアの復活。**6月末までに、Lockyメール攻撃の最初の波が押し寄せ、Necursボットネット復活の兆候が現れました。次の四半期に同様なエクスプロイトキットの復活があるのかどうか、引き続き注視していきます。

MOBILE

- **エクスプロイトキットが1000万台ものAndroidデバイスを侵害。**EKは複数の脆弱性を狙い、デバイスの制御を奪おうとしています。ほとんどのケースで、この制御はアドウェアをダウンロードするために使われ、攻撃者はそれによって収益を得るのです。
- **モバイルマルウェアの98%がAndroid関連。**この比率は前四半期から変わっていません。

SOCIAL MEDIA

- **ソーシャルメディアを使ったフィッシングが150%増加。**組織は引き続き、スパム、アダルトコンテンツ、その他の手作業での修復が必要な問題に対応しなければなりません。

最新の脅威とトレンド - 2016年4月-6月

2016年のQ2は、Q1に私達が指摘したトレンドを概ね踏襲しており、中でもLockyとDridexの配信に関わる主要なメール攻撃の規模は引き続き拡大しています。また同時に、Q1に観測されたランサムウェアの増加も、さらに加速しています。マリシャスな添付ファイルがメールベースの脅威の大半を占めており、メール中のURLから侵害されたサイトに誘導してマルウェアをダウンロードさせる手法とエクスプロイトキットの組み合わせも、引き続き観測されています。

今年前半は、日々の大規模な攻撃と高職位者を狙ったランサムウェアがニュースの見出しを独占しました。しかし、持続的標的型攻撃(APT)と標的型攻撃の入口が電子メールであることは変わりません。マルウェアをメールと共に配信することで、高い収益とさらなる攻撃の機会をもたらすのです。

BECフィッシングが引き続き好調

主な統計値: サンプルとして抽出したProofpointのお客様の80%が、過去30日間のうちに最低1回のBECフィッシング攻撃を受けています。

BEC攻撃が引き続き増加しており、攻撃者達は新しい技術と攻撃のアプローチの実験を続けています。BEC攻撃は広い範囲を狙い始めており、これは標的の中のより大きなグループへ向けてメールを配信するものです。攻撃者はまた、BEC攻撃の効果を高めるために、正規のメールと組み合わせを以前よりも高い頻度で行うようになっています。

BEC攻撃の件名で最も多いのは「Request」で、Q2に私達の顧客ベースが受けたBEC攻撃の11%がこの件名を使っていました。それに続くのが「URGENT」「w2」「Follow up」などの件名です。(W-2はアメリカの源泉徴収票)

図1は、5月中に観測されたBECフィッシングで使われた主要な件名の割合です。

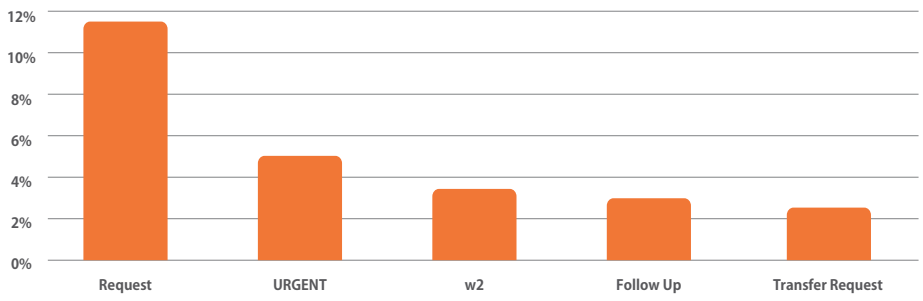

図 1: 2016年5月のBECフィッシングで使われた主な件名

これが意味するもの: メールファイアウォールの拡張などの技術的な防御とユーザートレーニングの組み合わせにより、これらの脅威によるリスクを大幅に低くすることができます。しかし同時に、人々が新しい脅威に対抗する方法を学ぶよりも速く、攻撃者は攻撃手法を変えてきます。

そのため、自動化された先進的なメール防御の導入を考える必要があります。

2015年12月からのランサムウェアの亜種の増加

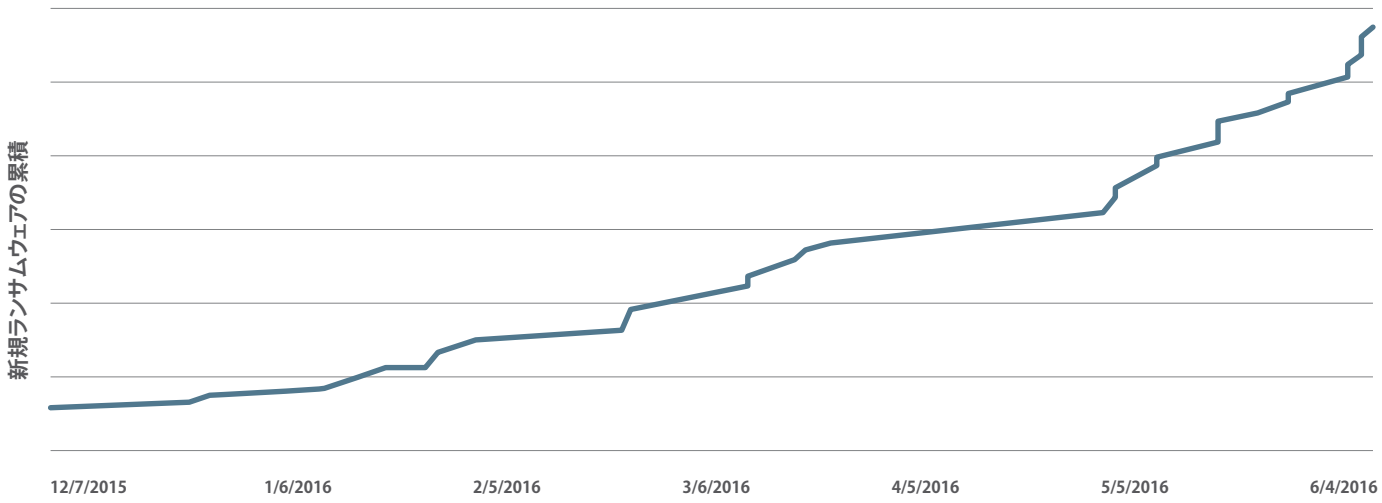

図 2: 2015年12月以降のランサムウェアファミリーの増加

ランサムウェアがどこにでも

主な統計値: 私達がQ2に観測したマリシャスな添付ファイルを持つメール攻撃の69%が、Lockyランサムウェアを扱っていました。これはLockyに限ればQ1から45%の増加です。その一方で、ランサムウェアのファミリー数は昨年12月から600%増加しました。

メッセージ数の単純な比較で、Q2はLockyランサムウェアがDridexバンキングトロージャンを抜きました。6月中活動を休止していたNecursボットネットが復活した際の最初のペイロードがLockyでした。6月の休止期間中、CerberがLockyの代わりに増加していましたが、それでも、Cerberも他の亜種も、期間中のペイロードトップ10には入りませんでした。

エクスプロイトキットもまた、ランサムウェアの活用に積極的です。CryptXXXは最初Angler EK経由で、四半期の後半にはNeutrino経由で広まり、ランサムウェアの中で最も大きな勢力となっています。CryptXXXはますます混み合う沼の中の、ますます巨大な魚となっているのです。

図2は、ランサムウェアの新しいファミリーが増加する様子を昨年12月からグラフにしたものです。それほど急激に伸びているわけではありませんが、メールやエクスプロイトキット、その他どのような経路で配布されるかに関わらず、ランサムウェアの多様化が進んでいることを示しています。6月末、それまでDridexとLockyを配布していた攻撃者が「Bart」という新しいランサムウェアファミリーの大規模なテストを開始したことがわかりました。他の亜種とは異なり、Bartはファイルの暗号化にあたってC&Cインフラとの接続を必要としません。

これが意味するもの: 新たな亜種と継続的な技術革新により、ランサムウェアは本流に戻ってきました。組織はこれらの破壊的攻撃がデータを暗号化し、重要なシステムをダウンさせる前に止めることができる防御技術を必要としています。

JavaScript添付ファイルを使ったマリシャスなメッセージが爆発的に増加

主な統計値: JavaScriptの添付ファイルを使ったマリシャスなメールメッセージが、Q1に比べて230%増加しました。複数の攻撃による数億通のメッセージが、私達のお客様を狙って送信されています。

マリシャスなURLを伴うメッセージのボリュームは、Q1と比べてあまり変化はありません。マリシャスな添付ファイルを伴うメッセージはむしろ減少しており、これは主に6月のNecursの休止によるものです。しかし、Necursの休止にもかかわらず、マリシャスなJavaScriptファイルが添付されたメッセージは、Q1に比べて230%も増加したのです。これらのメッセージは2015年にはほとんど見られませんでした。

これが意味するもの: 組織を狙うマリシャスなメッセージは既に大量に存在しますが、世界最大のボットネットのひとつが1ヶ月近く休止したにもかかわらず、今でも増え続けています。特にマリシャスなJavaScriptファイルを添付したメッセージは、かつて見たことが無いほどの規模に達しており、企業のセキュリティチームが手作業で対抗できる量を遙かに超えています。組織はメールベースの先進的脅威に対抗するために、早急にスケーラブルで自動化された防御技術を導入し、新しい技術とアプローチを採用する必要があります。

攻撃タイプ別のマリシャスメッセージ (週次)

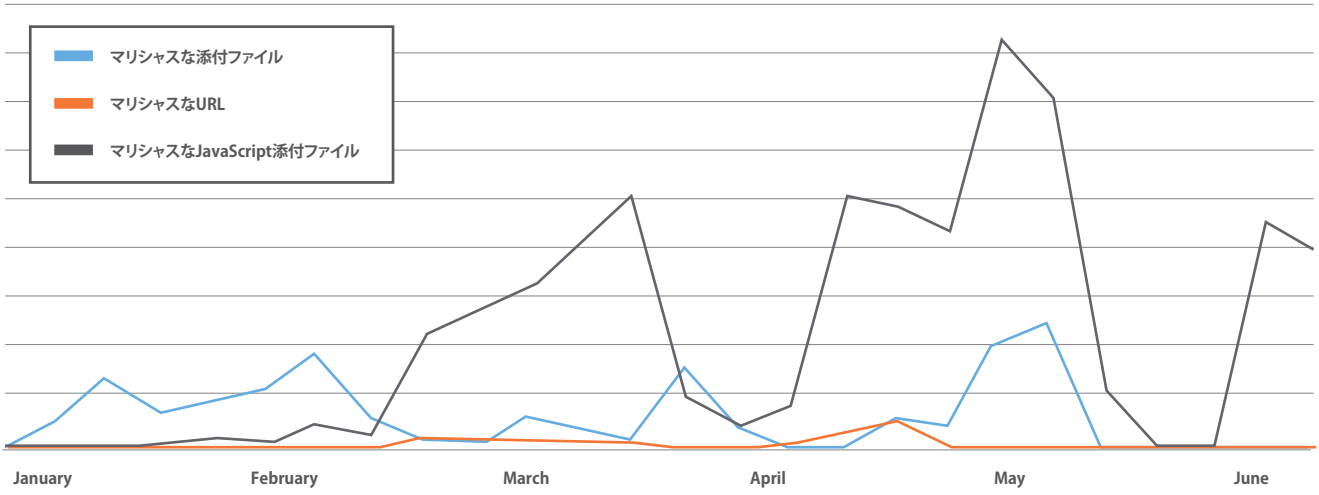

図 3: 攻撃タイプ別のマリシャスメッセージのインデックスチャート (週次) 2016年1月-6月

配信方法・感染プロセス・ペイロードの多様化

主な統計値: LockyがDridexを抜いて、マルウェアペイロードのトップに。Q2に観測したマリシャスメールのトップ10の中で、ランサムウェアは全てのペイロード中41%を占めています。

Lockyがメールベースの脅威トップ10の中でのシェアを2倍近くに伸ばし、Dridexを抜いてマルウェアペイロードのトップに立ちました。しかし、今後の大きなトレンドとしては、以前のように単一のタイプのマルウェアだけが伸びていくことは無いでしょう。2つのマルウェアローダー (RockLoader と Pony)、そして情報窃盗 (Kegotip) がトップ5に名を連ねています。RockLoaderは多くの場合LockyとDridexを配布しているため、Necursボットネットが休止したことにより、LockyとDridexのシェアが大幅に上がりました。

それでも、RockLoaderは最近の新規の配信方法の急増の一例に過ぎません。これらの新しい方法には、侵害されたコンテンツ管理システム上のエクスプロイトキットにリンクする手法や、マリシャスなドキュメントとJavaScriptを組み合わせて複数の連続した感染を引き起こす手法も含まれています。

私達の研究者は以下の事象も観測しました:

- 単一の攻撃の中で複数のペイロードを配布
- 高度にパーソナライズされた大規模な攻撃
- 変化を繰り返す、地域を限定した餌ドキュメント
- クレデンシャルフィッシングにマルウェアを添付する「クロスオーバー」攻撃

攻撃者の狙いは攻撃対象を広げ、ソーシャルエンジニアリングを使った攻撃をクリックさせて収益を稼ぐことで、そのために様々な技術を駆使しているということです。

主要マルウェアペイロード (2016年4月-6月)

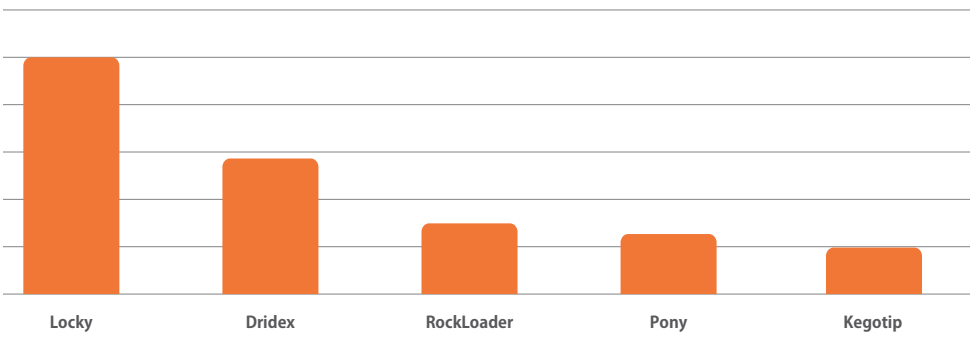

図 4: メールベースのマルウェア脅威トップ5の相対比較

これが意味するもの: これまでは、大量のメッセージにいかに取り組むかが組織の課題でしたが、今ではユーザーにマルウェアを送り込むための革新的技術と常に変化する脅威の複合への対応に変わっています。

手作業による処理と定期的なアップデートだけでは、動的で多様な脅威に適切に対抗することはできません。組織はメールベースの先進的脅威に対抗するために、スケーラブルで自動化された防御システムを備える必要があります。

主要エクスプロイトキットの活動 2016年4月-6月

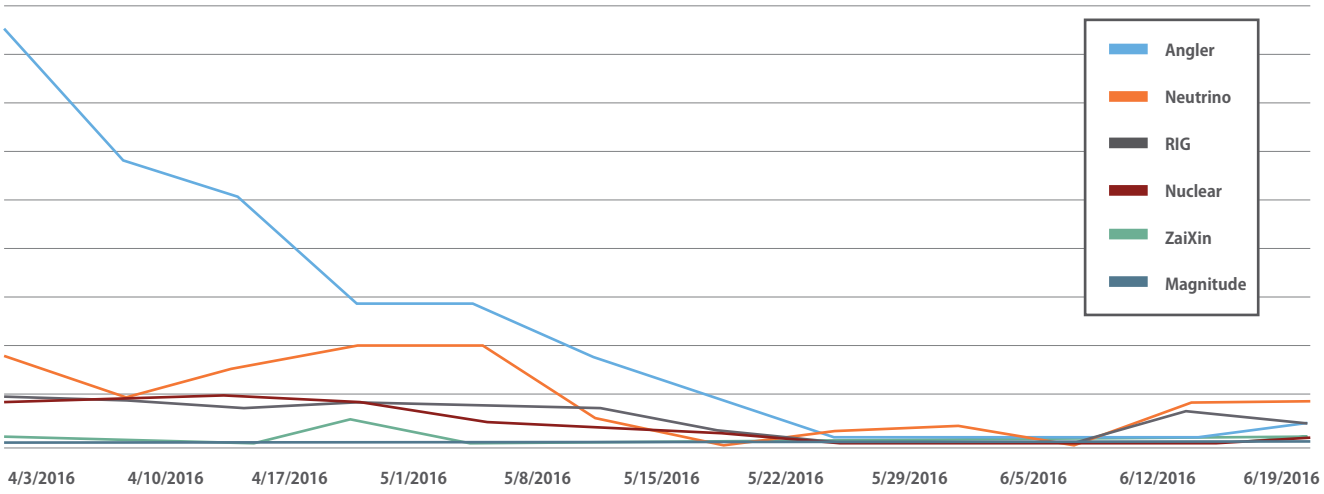

図 5: エクスプロイトキットの活動がQ2に急減

Anglerが一服し、エクスプロイトキットのボリュームが急落

主な統計値: Proofpointは、4月から6月中旬にかけてエクスプロイトキットのトラフィックが96%も減少したことを観測しました。

2015年から2016年のQ1にかけて、攻撃者はAngler EKに群がり、それが全EKトラフィックの60%を占めていました。しかし、6月半ばにかけてEK全体の活動が96%も減少すると、Anglerの活動も急激に減少しました。

Anglerの急落により、多くの攻撃者(CryptXXXランサムウェアを配信している攻撃者など)がマルウェアの配信をNeutrinoに切り替え、このEKがQ1にシェアを伸ばし、他の攻撃者はエクスプロイトキットを使う攻撃を休止しました。Q2が終る頃、EK全体の活動がゆっくりと再開しましたが、Q1のレベルにはまだ戻っていません。

これが意味するもの: 一時的な休止は珍しいことではありません。今回の休止は過去1年間で3回目の(そして最大の)休止でした。これらの休止は、当局が行う法的措置の影響や季節的要因、その他犯罪組織のインフラに起こった何らかの不具合などによって起こります。いずれのケースでも、活動再開後は休止以前のレベルを超える活動が観測されるのが一般的です。私達はEKのエリアで起こった今回の変化がこのまま続くとは考えていませんが、他のEKがAnglerと同じレベルで支配的になり活動的になるかどうか、注視していきます。

Anglerの活動が抑えられているため、相対的にNeutrinoやRIGのような他のEKの活動が活発化しており、恐らくはそれらへの開発投資も行われているでしょう。標的を狙う上でEKは依然として重要な感染経路で、時にメールベースのURLを使った脅威と組み合わせたり、持続的標的型攻撃(ATP)や、流行のマルバタイジングのプロセス中で重要な役割を担ったりします。組織は通常のパッチ当て作業に加え、脅威インテリジェンス情報を継続的に監視し、EKによって狙われる脆弱性を追跡して対策を行う必要があります。

モバイル向けのマリシャスなアプリはデバイスの乗っ取りとマリシャス広告に注力

主な統計値: 1000万台ものAndroidデバイスが、複数の脆弱性を狙うモバイルエクスプロイトキットに感染しています。

Q2は、既知のルート化脆弱性を使ってデバイスを侵害したり、偽のアプリをインストールしたり、ユーザーの同意無しに広告を送り込んだりするアプリの増加が見られました。

「カクテル」アプローチを使ったアプリは、デバイスを乗っ取ることができる複数の脆弱性を混ぜ合わせ、できるだけ多くのバージョンのデバイスを侵害できるようになっています。このタイプの活動は主にAndroidを狙っており、EKを使ったアプリは1000万台ものデバイスに感染しています。これらの多くはAndroid 5.1及びそれ以前のバージョンを狙っています。デバイスがいったん侵害されると、ユーザーの同意無しに他のアプリをダウンロードします。これらのアプリはマリシャスな広告を表示して攻撃者に収益をもたらします。

マリシャスなアプリは様々なアプリストアにアップされています。しかし私達は、世界中のユーザーへ向けて配信されるスパムメールやSMSメッセージに含まれるリンクからも、これらをダウンロードできることを確認しています。例えば、複数のアプリストアで手に入る「Swiping Whale」というアプリは、HummingBadに感染していますが、同時にこれはスパムメッセージに含まれるリンクを辿って様々なWebサイトからダウンロードされることもあります。この構造は、多くのWindowsマルウェアの配信方法と同じです。

これが意味するもの: モバイルマルウェアが活動の場を広げるにつれ、脅威をとりまく環境は、デスクトップのそれとどんどん似てきています。エクスプロイトキット、マリシャスダウンロード、アドウェアなどがモバイルでも見られるようになっており、その傾向は、特にAndroidプラットフォームで顕著です。多くの企業では、モバイルデバイスがデスクトップPCを置き換えたり、同等に扱われるようになってきており、モバイルアプリの持つリスクを動的に解析し、MDMソリューションと統合できる防御システムの導入を急ぐ必要があります。同時に、これらのモバイル防御システムは、全体の企業システムに適用されるのと同じ脅威インテリジェンスによってサポートされる必要があります。

ソーシャルメディアを使ったフィッシングが増加

主な統計値: 2016年の最初の6ヶ月間のソーシャルメディアを使ったフィッシング攻撃は、前年同期に比べ150%増加しました。

ソーシャルメディアは従来型のWebサイトに代わり、多くの企業・ブランドにとって一般への窓口になっています。サイバー犯罪者達が、この状況を利用して顧客を攻撃するために、ソーシャルメディアを利用しようとしていることには疑いの余地はありません。アンコウは生物発光を餌にして小さな魚を捕食しますが、ソーシャルメディアでは最近、偽のカスタマーサポートアカウントを餌に使う手口が急増しています。企業・ブランドの顧客をサポートすると見せかけて、ユーザーの認証情報を盗み取るのです。

同時に、ソーシャルメディアスパム、アダルトコンテンツ、マリシャスリンクなども、ソーシャルメディアにとっては依然として大きな問題です。これらはブランドにとって大きなリスクであり、このチャネルが提供する価値を危険にさらします。

これが意味するもの: ソーシャルメディアは、企業・ブランドが顧客との関係を構築するための素晴らしいチャネルです。しかし、対話がフィッシング攻撃や危険なコンテンツによって脅かされれば、顧客は離反し、チャネルを維持することが難しくなります。フィッシングやスパムなどのリスクを自動的に特定し、影響を緩和するためのソリューションの導入が重要です。それにより、ソーシャルチャネルをクリーンに保ち、有効に活用できるのです。

Proofpoint からのアドバイス

本レポートで詳述した脅威を取り巻く環境において最新の攻撃に対抗するために、私達は以下の対策を推奨します。

- ほとんどの攻撃は電子メール経由で行われます。そのため、先進的攻撃やマルウェアを含まない攻撃でも、検知し予防できる能力を持ったメールゲートウェイソリューションを導入する必要があります。この対策により、ネットワーク内に侵入する脅威の数を最小にすることができます。一度これらの脅威がネットワーク内に侵入してしまうと、マルウェアやマリシャスなトラフィックを検知して正規の通信と区別するのは困難になります。
- 実行形式の添付ファイルを含むメールを配信してはなりません。同様に、従業員がメールを使ってプログラムをやりとりすることを禁止すべきです。これらの見え透いた脅威をネットワーク内に持ち込まないために、.exeや.jsの添付ファイルを禁止する単純なルールを作れば良いのです。
- ソーシャルメディアを使ったフィッシングが増加しているため、ユーザーを狙う外部リスクに気をつけるべきです。特に、詐欺アカウントを使うものは悪質です。ソーシャルメディア上でのリスクを可視化できるセキュリティソリューションを導入すべきです。また、ソーシャルメディアを使ったフィッシングを見分けられるよう、従業員を教育しましょう。
- 組織とその従業員を狙うため、攻撃者達は様々な手法を使います。複数の攻撃経路を横断して行動を監視できるセキュリティソリューションが必要です。これにより、攻撃に関する深い知見を得ることができ、問題の解決、将来の攻撃からの防御、より迅速な検知が可能になります。

PROOFPOINTについて
Proofpoint Inc. (NASDAQ:PFPT) は、クラウドベースの包括的脅威保護、インシデント対応、セキュアなコミュニケーション、ソーシャルメディア及びモバイルセキュリティ、コンプライアンス、アーカイブ/ガバナンスを提供する、次世代の主導的セキュリティ/コンプライアンス企業です。世界中の組織がProofpoint の専門知識、パテント取得済みの技術およびオンデマンドのデリバリーシステムを使ってフィッシング、マルウェアやスパムメールからシステムを守り、暗号化された機密情報や個人情報を守り、重要な情報や電子メールをアーカイブし管理します。

proofpoint www.proofpoint.co.jp

© Proofpoint, Inc. Proofpointは米国及びその他の国々におけるProofpoint, Inc.の商標です。
本ドキュメントに記載されている会社名、製品名、サービス名は、一般に各社の登録商標または商標です。
本ドキュメントの記載内容、製品及びサービスの仕様は予告なく変更されることがあります。