レポート

proofpoint

四半期脅威レポート

2017年第4四半期

proofpoint.com/jp

*Proofpointの四半期脅威レポート*では、当社の大規模な顧客ベースとより広範な脅威環境で確認された攻撃の動向について取り上げ、そこから読み取ることのできる重要ポイントを示しています。

当社は、高度な脅威から世界中の組織を保護するために、日々、10億件を超える電子メールメッセージ、数億件ものソーシャルメディアへの投稿、1億5,000万以上のマルウェアサンプルを分析しています。また、3つの主な感染経路である電子メール、ソーシャルメディア、およびクラウドアプリにわたり、巧妙化する脅威を継続的に監視しています。現代のサイバー攻撃の戦術、ツール、および標的の解明と分析は、こうした取り組みから得られる独自の視点の上に成り立っています。

このレポートは、現代の攻撃への対処、新たな脅威の予測、およびセキュリティ体制の管理をより効果的に実施するために直接活かすことのできる情報をお届けすることを目的としています。レポートでは、当社の調査結果とともに、ユーザー、データ、およびブランドの保護に役立つステップを推奨しています。

目次

重要ポイント：前線にはコインマイナー、主流はランサムウェア

2017年第4四半期の重要ポイントは次のとおりです。

電子メール

悪意のある文書が添付されたメッセージ量が3倍に急増
このトラフィックのほとんどは、Microsoft社のDYNAMIC DATA EXCHANGEプロトコルを悪用し、ソーシャルエンジニアリングを利用した大規模な攻撃活動によるものでした。

ランサムウェアが引き続き、悪意のあるメッセージによって拡散される最大のペイロードに
このタイプの攻撃は、悪意のあるメッセージ量全体の57%を占めました。

仮想通貨の大幅な価格変動を受け、ビットコイン額で指定されたランサムウェアの身代金要求件数が73%低下
身代金の金額を米ドル額または現地通貨の金額で設定する攻撃者は増加傾向にあります（ただし、支払い自体は仮想通貨で行われるのが一般的）。

バンキング型トロイの木馬でTHE TRICKの使用が最多に
The Trickは、バンキング型トロイの木馬を含む悪意のあるスパム全体の84%を占めました。

一見して見分けのつかないドメインやタイポスクワッティングドメインを幅広い攻撃で使用
有名なブランドまたは組織と錯覚する可能性のあるドメインを作成するための手法として、文字の交換（文字の打ち間違い）が最も使用されました。

エクスプロイトキットおよびWEBベース攻撃

Webベース攻撃活動が注目されるなかブラウザエクスプロイトは鳴りを潜め、ソーシャルエンジニアリング手法が増加
エクスプロイトキット（EK）のトラフィックは、前の四半期から31%減少しました。最も使用されたEKはRIG EKでした。

ソーシャルメディア

ソーシャルメディア上の不正な顧客サポートアカウントの数が30%増加
それと並行して、ソーシャルメディアのフィッシングリンクは前の四半期から70%増加しました。

DYNAMIC DATA EXCHANGE
Dynamic Data Exchange（DDE）は、Microsoft Windowsで20年前から使用されている通信プロトコルで、文書が他の文書から情報を引き出せるようにするものです。この技術はほぼ新しいプロトコルに置き換わっていますが、Windowsでのサポートは現在も継続されています。

ランサムウェア
被害者のデータを暗号化してロックし、復号鍵でロックを解除するための「身代金」を支払うよう要求するマルウェア。

仮想通貨
電子マネーの一種。セキュリティと匿名性を確保するように設計されており、支払い経路をたどって攻撃者を突き止めることができないため、ランサムウェアの支払いに適しています。

THE TRICK
TrickBotとも呼ばれる、Dyreと密接な関連性のあるバンキング型トロイの木馬。Dyreの犯行グループは2015年にロシア当局に逮捕されましたが、Dyreは2017年に復活が確認されています。

タイポスクワッティング
詐欺師は、URLを間違って入力したユーザーやメールヘッダーに注意を払わないユーザーをだますため、正規ドメインをスペルミスしたドメインまたは正規ドメインの文字を入れ替えたドメインを登録します。

エクスプロイトキット
エクスプロイトキット（EK）はWeb上で実行され、感染したサイト、悪意のある広告、攻撃者が操るランディングページに接続したコンピュータの脆弱性を検出して悪用します。多くの場合、EKは攻撃者にサービスとして販売され、「ドライブバイ」マルウェアのダウンロードでPCに容易に感染します。積極的なエクスプロイトに頼らないソーシャルエンジニアリング攻撃での使用が増えています。

TA505
この脅威集団は金銭的利益を目的に、バンキング型トロイの木馬のDridex、ランサムウェアLocky、ランサムウェアJaff、バンキング型トロイの木馬のThe Trickなどを拡散した史上最大規模のいくつかの電子メール攻撃活動を仕掛けました。

LOCKY
悪意のある電子メールで使用されている一般的なランサムウェアの亜種。被害者のデータを暗号化し、被害者が復号化のための身代金を支払うまでデータを「人質」にします。2016年のほぼ全般および2017年の数か月間にわたり、Lockyは悪意のある電子メールトラフィックの大部分を占めていました。

GLOBEIMPOSTER
このランサムウェア亜種はFake Globeとも呼ばれ、先行のランサムウェア亜種Globeを模倣し、このランサムウェアにちなんだ名前が付けられています。当初は限定的な地域活動で使用されましたが、多くのマルウェアを生んだ脅威集団TA505が後に大規模活動で使い始めると、世界的な脅威へと発展しました。

電子メール：悪意のある文書がURLを追い抜く

基本統計：悪意のある文書が添付されたメッセージ量が第3四半期の3倍に急増

悪意のあるファイルが添付されたメッセージの全体量は勢いを取り戻し、前の四半期の3倍以上に急増しました。脅威集団**TA505**が仕掛けた大規模活動を筆頭に、このタイプの多くのメッセージにより、バンキング型トロイの木馬であるThe Trick、または**LOCKY**や**GLOBEIMPOSTER**などのランサムウェアの各種亜種が拡散されました。

Microsoft社のDynamic Data Exchange（DDE）を悪用するための手法の公開に乗じて、大規模および小規模活動でマルウェアを配布した攻撃者もいました。

10月末までに、ほとんどの攻撃者はこの手法の使用をやめ、悪意のあるマクロやその他の形式の埋め込みコードを悪用する通常の手口に戻りました。ただし、DDE手法を利用した活動は、脅威集団の手持ちのツールキットの1つとして定着したことから、11月および12月にも散発的に続きました。

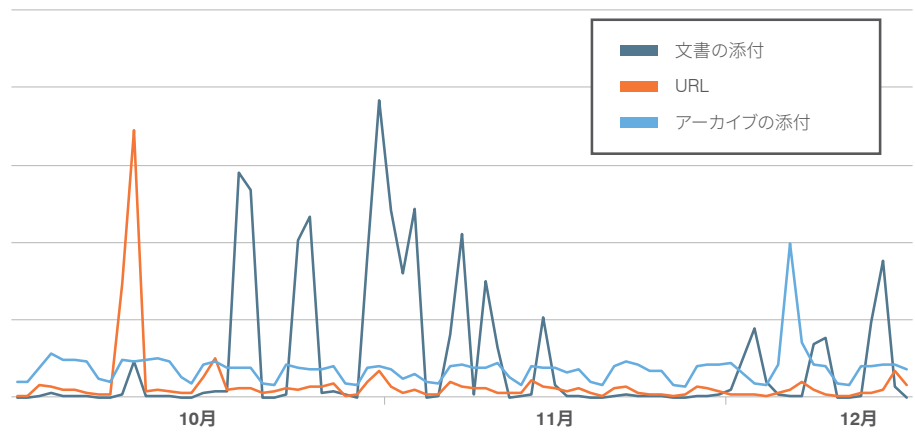


図1：攻撃タイプ別の動向指数、2017年10月～11月（77日間）

対照的に、悪意のあるURLの使用は激減し、大規模な大量発生を記録した第3四半期が例外的な状況だったことが判明しました。とは言え、どの攻撃タイプも脅威集団の幅広い支持を保ち続けています。

図1は、悪意のあるURL、文書の添付、およびアーカイブファイル（ZIPや7-Zipなど）の添付を使った悪意のあるメッセージ量の劇的な変動を示しています。各攻撃タイプの絶え間ない変化は、攻撃者の柔軟性を示しています。攻撃の効果を高め、最大限の利益を得るために、攻撃者が攻撃タイプ、ペイロード、および感染手法を次々に切り替えていることが分かります。

バンキング型トロイの木馬
通常は被害者のブラウザを銀行の偽Webサイトにリダイレクトするか、正規のサイトに偽のログインフォームを差し込むことにより、被害者から銀行のログイン資格情報を盗み取るマルウェア。

ZEUS PANDA
このバンキング型トロイの木馬はPanda Bankerとも呼ばれ、初期のバンキング型トロイの木馬の1つであるZeusと関連性があります。

コインマイナー
仮想通貨は、コンピュータの計算能力を使用して複雑な数学的問題を解く「マイニング」プロセスによって作成されます。コインマイナーは、これを目的に、感染したシステムを乗っ取るマルウェア亜種で、このマルウェアの配布元の脅威集団のために仮想通貨を生成します。

WEBインジェクション
ユーザーに表示されるWebページを改ざんする手法。攻撃者は、安全に見えるWebサイトに安全でないフォームを付加するためにWebインジェクションを使用します。ユーザーがフォームを完成させると(銀行取引のための資格情報などを入力)、その情報は銀行ではなく攻撃者に送信されます。

バンキング型トロイの木馬:標的は銀行取引だけじゃない

基本統計:The Trickを拡散するメッセージが**バンキング型トロイの木馬**のメッセージ量の84%を占有

The Trickは、メッセージの全体量において、引き続きバンキング型トロイの木馬のトップとなりました。このマルウェアの出現件数は、観察された他のバンキング型トロイの木馬のメッセージ総数の6倍にのぼりました。この状況は、DridexおよびVawtrakが上位バンカーで、The Trickがごく少数の特定地域を標的とした活動に限定されていた2016年とは大きく異なっています。

第4四半期の活動では、The Trickとともに**ZEUS PANDA**(別名Panda Banker)およびEmotetも頻出しました。また、一部の攻撃常習者は、IcedIDと呼ばれる新たなトロイの木馬を直ちに採用しました。

一際目を引くThe Trickをはじめとする一部のバンキング型トロイの木馬では、仮想通貨マイニングモジュールまたはボットが追加されました。また、その他のバンカー活動では、後の段階でペイロードとなる**コインマイナー**が追加され、第3四半期に報告した傾向が拡大しつつあることを示しています。

ここ数年、バンキング型トロイの木馬では、秋期に標的が多様化することが確認されています。2017年の第4四半期も同じでした。Zeus Panda活動では、従来型のオンラインバンキング**WEBインジェクション**が補強、拡張され、人気のあるさまざまな実店舗のオンラインショッピングサイトが標的となりました。

これらの変化は、金融サービス機関の顧客ばかりがバンキング型トロイの木馬の標的ではないことをはっきりと示唆しています。すなわち、あらゆるビジネスまたはサービスのオンライン顧客が標的候補なのです。

ランサムウェア:ビットコインの価格変動がビジネスを震撼

基本統計:ビットコイン額でのランサムウェアの身代金要求が73%減少

単一の攻撃者がThe Trickを使って仕掛けた大規模活動を中心に、バンキング型トロイの木馬のメッセージ量は急増しましたが、電子メール活動で悪意のあるペイロードの主流となったのは、相変わらずランサムウェアでした。図2に示すように、ランサムウェアは悪意のあるメッセージ全体の57%以上を占めました。

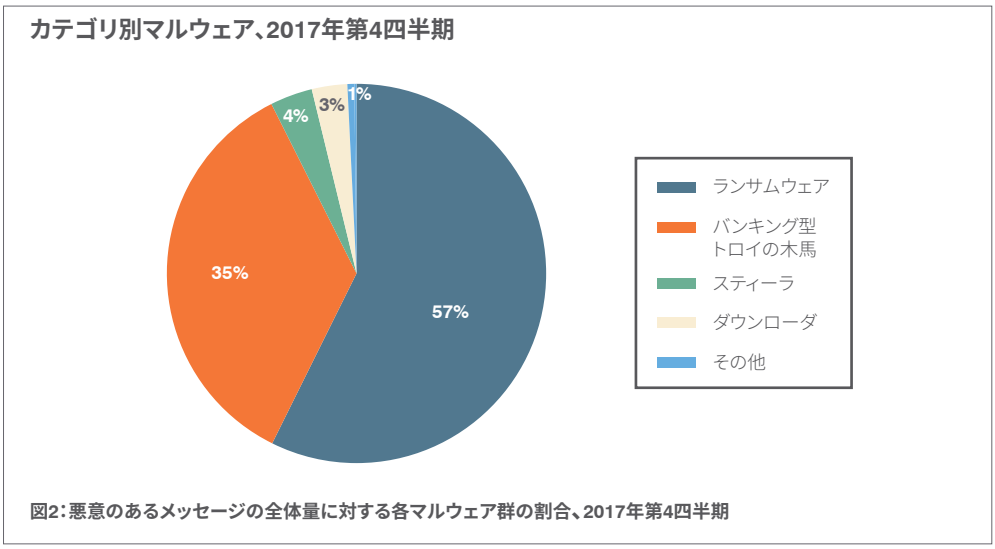


図2:悪意のあるメッセージの全体量に対する各マルウェア群の割合、2017年第4四半期

過去2年間のほとんどで、攻撃者は身代金をビットコイン額で指定していました。要求額は、整数または「0.5」や「0.15」などの小数で指定したビットコイン数で表されます。

仮想通貨の価格急騰は、ビットコイン保有者には朗報ですが、製品やサービスをビットコインで値付けしようとする者にとっては悩みの種です。脅威集団も例外ではありません。

第4四半期には、これを考慮した新たなランサムウェア亜種が現れました。11月中旬に初めて出現したランサムウェアSigmaは、身代金を米ドル額で指定して要求するものでした。

政府発行の通貨での身代金の指定には、実際の支払いがビットコインで行われる場合でも、攻撃者に2つの大きなメリットがあります。それは、脅威集団が長期的に安定した価格を設定でき、しかも当面はそのままの価値の通貨で支払いを匿名で受け取ることができることです。

12月中旬までの90日間にわたってランサムウェアの身代金要求を分析したところ、通貨の切り替えが、各種攻撃に共通する大きな流れの1つであることが容易に判明しました(図3)。

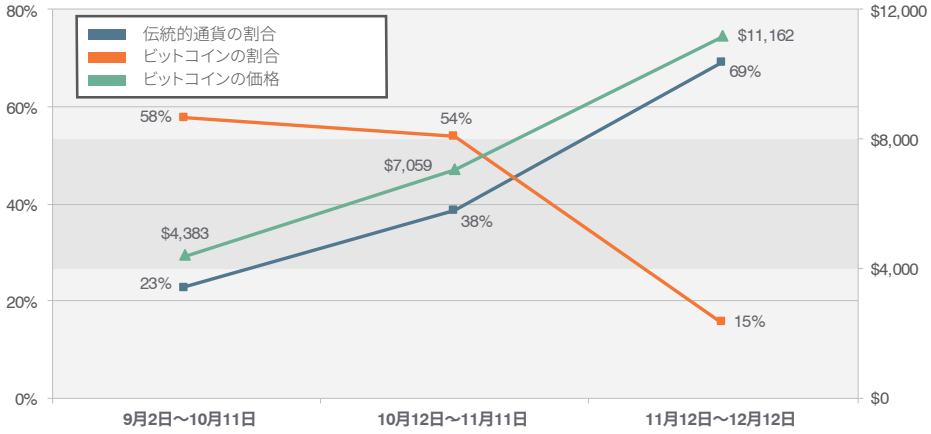


図3:身代金をビットコインで指定したランサムウェアと伝統的通貨で指定したランサムウェアの比較、90日間の動向

ビットコインに代わって、またはビットコインに加えて伝統的通貨で指定されたランサムウェアの身代金要求が、ビットコインの価格急騰と関連していることは明らかです。経済的観点から、ビットコインの急騰が伝統的通貨での指定に至ったと言えます。

この傾向は、ビットコインの価格が元に戻れば逆行する可能性があります。今後どのような状況になるにせよ、この関連性は、現代のサイバー犯罪者の利潤動機をさらに裏付けるものです。すなわち、最も効率よく「金を追う」ことのできるツールと手法を選んでいるわけです。

標的型攻撃の脅威集団が浮上

当社の研究者が第4四半期に追跡した活動の多くは、広範囲に拡散した、コモディティ化されたマルウェアのペイロードでした。この他にも、Lazarusグループ、APT28、当社がLeviathanと名付けた新たな脅威集団など、高度な標的型攻撃の脅威集団の活動もいくつか分析し、報告しています。

これらの攻撃で使用された電子メールおよび文書は通常、標的となる受信者の関心やビジネスに合わせてパーソナライズされ、調整されていました。攻撃者が使用したのは、盗み取られたブランド文書や公開文書です。また、受信者をだましてリンクをクリックさせたりファイルをダウンロードさせるために、タイポスクワッティングドメインや一見して見分けのつかないドメインも利用されました。

電子メール詐欺の脅威：不正なドメイン名の手口を理解する

防御を目的としたドメイン登録
正規ブランドのドメインと誤解される可能性のあるインターネットドメインを攻撃者に先んじて購入する、推奨される防御方法。一見して見分けのつかないドメインは、正規の組織のもののように見える偽のWebサイトや不正な電子メールで顧客やパートナーをだますために使用される可能性があります。

ANGLERフィッシング
Anglerフィッシングでは、攻撃者はソーシャルメディア上に偽の顧客サポートアカウントを作成し、サポートを求めているユーザーをだましてフィッシングサイトに誘導したりアカウントの資格情報を提供させたりします。

基本統計：**防御を目的としたドメイン登録**数は平均300ドメイン。大企業の場合、疑わしい登録済みのドメイン数は、正規ブランドの登録済みドメイン数の20倍にのぼる可能性がある。

当社の調査では、正規ブランドによる防御を目的とした登録を大幅に凌ぐハイペースで、脅威集団が疑わしいドメインを登録していることが示唆されています。この差が大きいため、正規ブランドは詐欺、フィッシング、なりすましなどに対して脆弱なままになっています。

組織は、自社を守るために、自社ドメインの考え得る文字の並べ換えをすべて登録する必要はありません。最も一般的な変更や置換を分析すれば、防御を目的とした登録に優先順位を付け、可能性のあるタイポスクワッティングドメインの合理的なサブセットを管理することができます。

一見して見分けのつかないドメインは、電子メール詐欺攻撃全体の3%をわずかに上回る程度です。ただし、この数字からかけ離れた数のドメインが考え出され、電子メール詐欺、フィッシング、**ANGLERフィッシング**などの攻撃で使用されているのも事実です。

新規または見慣れないトップレベルドメイン（TLD）での不正な登録に神経質になっている観察者もいますが、疑わしい登録の圧倒的多数は依然として標準的な「.com」です。

疑わしい登録のうち約82%が「.com」を使用しています。また、疑わしい登録の約90%が、なりすまそうとしているブランドと同じTLDを使用していました。多くの電子メール詐欺師は、なりすまそうとするブランドのTLD内の正規ドメイン名を単純に変更したものを使用しています。

図4は、疑わしいドメイン登録で一般的なスペルパターンを示しています。

類似ドメインのタイプ	異なるTLD	同じTLD	総計
個々の文字の交換	3.49%	37.60%	41.09%
追加文字の挿入	0.97%	31.15%	32.12%
先頭/末尾文字の追加または削除	0.73%	12.51%	13.25%
文字の削除	0.41%	5.10%	5.51%
まったく同じ文字列にハイフンを追加	1.23%	3.40%	4.63%
まったく同じ文字列	3.40%	0.00%	3.40%
総計	10.23%	89.77%	100.00%

図4：タイポスクワッティング手法

同じTLD内でブランド名の個々の文字を交換する手口は、最も一般的なタイポスクワッティング手法です。図5は、交換された具体的な文字の内訳です。

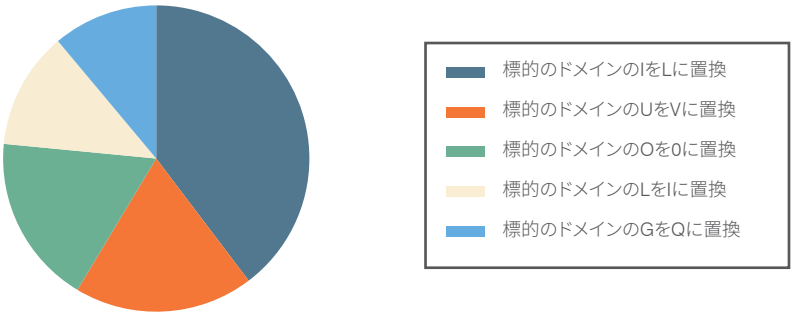


図5：疑わしいドメインのタイポスクワッティングで使用された文字置換パターン

Webベースの脅威：統合とソーシャルエンジニアリング

基本統計：観察されたエクスプロイトキットのトラフィックが第3四半期から31%減少

RIG EK
2016年6月にAnglerの犯行グループが逮捕され、Anglerが姿を消してから間もなく最も広範囲に拡散したエクスプロイトキット。

すでに制圧されたエクスプロイトキットのトラフィックは、数四半期にわたって2016年のピーク時の10%前後で低迷していましたが、第4四半期にはさらに減少しました。2017年第4四半期に観察されたエクスプロイトキットのトラフィックは、ほぼ98%をRIG EKが占めました。ただし、年末のMagnitude EKの急増を受けて、四半期末には、トラフィック全体に対するRIG EKの割合は減少しました（図6）。

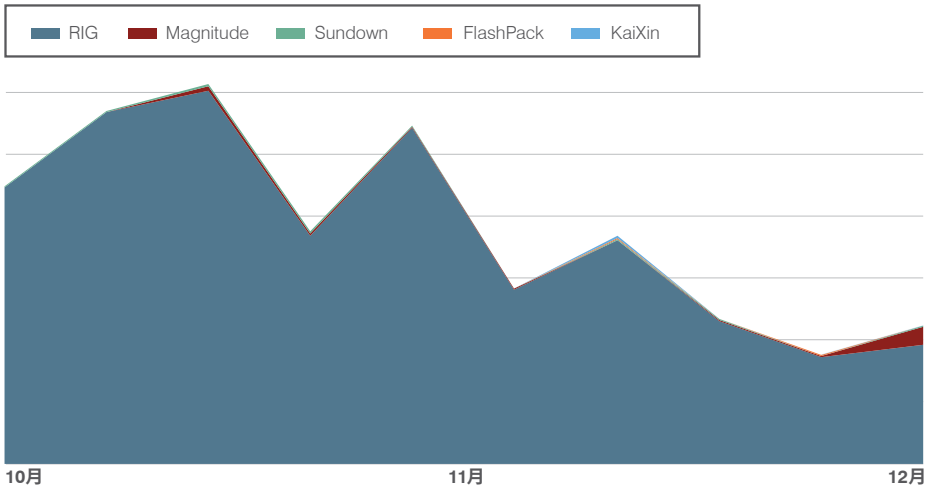


図6：全体に対する上位エクスプロイトキットのトラフィックの割合、2017年10月～11月

BAD RABBIT
ロシアおよびウクライナのユーザーを標的に10月に初めて出現したランサムウェア亜種。ランサムウェア亜種のNotPetyaに類似し、Adobe Flashのアップデートを偽装して「ドライブバイ」ダウンロードによってシステムに感染し、さらにこの偽のアップデートを起動するように犠牲者に要求します。

人気の高いアダルト動画サイトのユーザーを標的とした大規模で巧妙なマルバタイジング活動が発見されたことは、一大ニュースとなりました。このタイプの攻撃は、Webブラウザの技術的な欠陥を悪用する代わりに、ユーザーをだましてマルウェアをインストールさせるものでした。攻撃者は、高度なフィルタリングを使用して場所やインターネットプロバイダで標的を定め、標的になったユーザーに、ブラウザまたはAdobe Flashのアップデートをダウンロードするように指示するWebページを表示しました。ところが、ユーザーが実際に入手したのは、10月のBAD RABBITランサムウェアの大流行で確認された広告詐欺マルウェアKovterでした。

攻撃者は、感染手法として今後利用できるWebブラウザエクスプロイトの不足やエクスプロイト全体の限界に直面しています。そこで、大きな効果が期待できる、電子メール攻撃と同様のソーシャルエンジニアリングベースの手口に目を向けるようになりました。その前兆は、2016年後半に見られる初期の例に現れています。

浮き沈みを繰返すPOSマルウェア

2016年のブラックフライデーの週末には、特定の販売時点情報管理(POS)マルウェア亜種が4倍に増加し、それに伴うトラフィックが確認されました。2017年の急増は控え目でした。上位を占めるPOSマルウェア亜種は、ブラックフライデー前後だけでなく、1年を通してさまざまなタイミングで活発化しました(図7を参照)。

例えば、FindPOSは3月に活発になり、夏にかけて沈静化した後、10月末に活動を再開しました。それとほぼ並行してMagikPOSが減速していることから、単一の集団がツールを切り替えたものと推測されます。一方、NewPosThingsのトラフィックは、6月の急増を別として、1年を通してほぼ低いレベルを保ちました。

このことからチップアンドピン構想の普及がPOSマルウェアへの対策として功を奏し、トラフィックの急増につながる季節的な活動の成功に水を差しているものと推測できます。今後、脅威環境が既存の亜種および新たな亜種にどのように融合するのか、または融合するのかしないのかを見極めるには、POSマルウェアの循環的動向をさらに詳しく調査する必要があります。

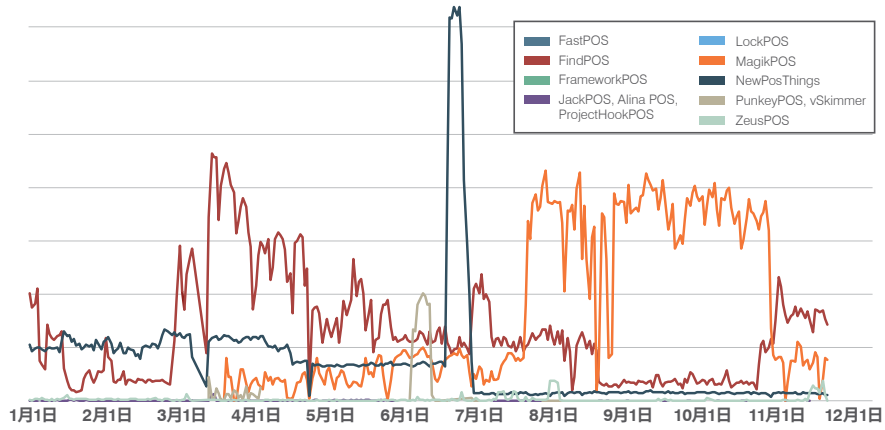


図7:販売時点情報管理(POS)マルウェアのトラフィック、2017年1月～11月

2018年に向けてソーシャルメディアの脅威が急増

基本統計:ソーシャルメディア上の不正な顧客サポートアカウントが前の四半期および前年の合計より30%増加

ソーシャルメディアの脅威は前の四半期に急増しました。偽の顧客サポートアカウント数は、前の四半期および2016年の同期間よりも30%増加しました。

ソーシャルメディアのフィッシングリンクは、2017年を通してほぼ横ばいでしたが、第4四半期に入って着実な伸びを見せ、第3四半期から約70%の急増となりました(図8)。

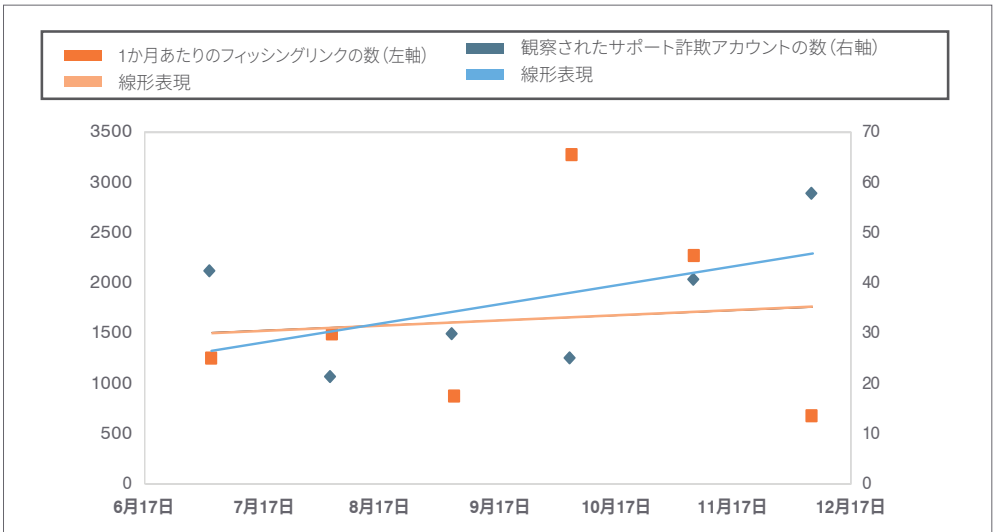


図8:ソーシャルメディア経由でのフィッシングリンクの配布および不正なサポートアカウントの月ごとの相対的活動の比較

推奨事項

このレポートでは、各企業のサイバーセキュリティ戦略に活かせるように、移り変わる脅威環境に対する見解を示しています。今後数か月にわたって企業および自社ブランドを保護するための推奨事項を次に示します。

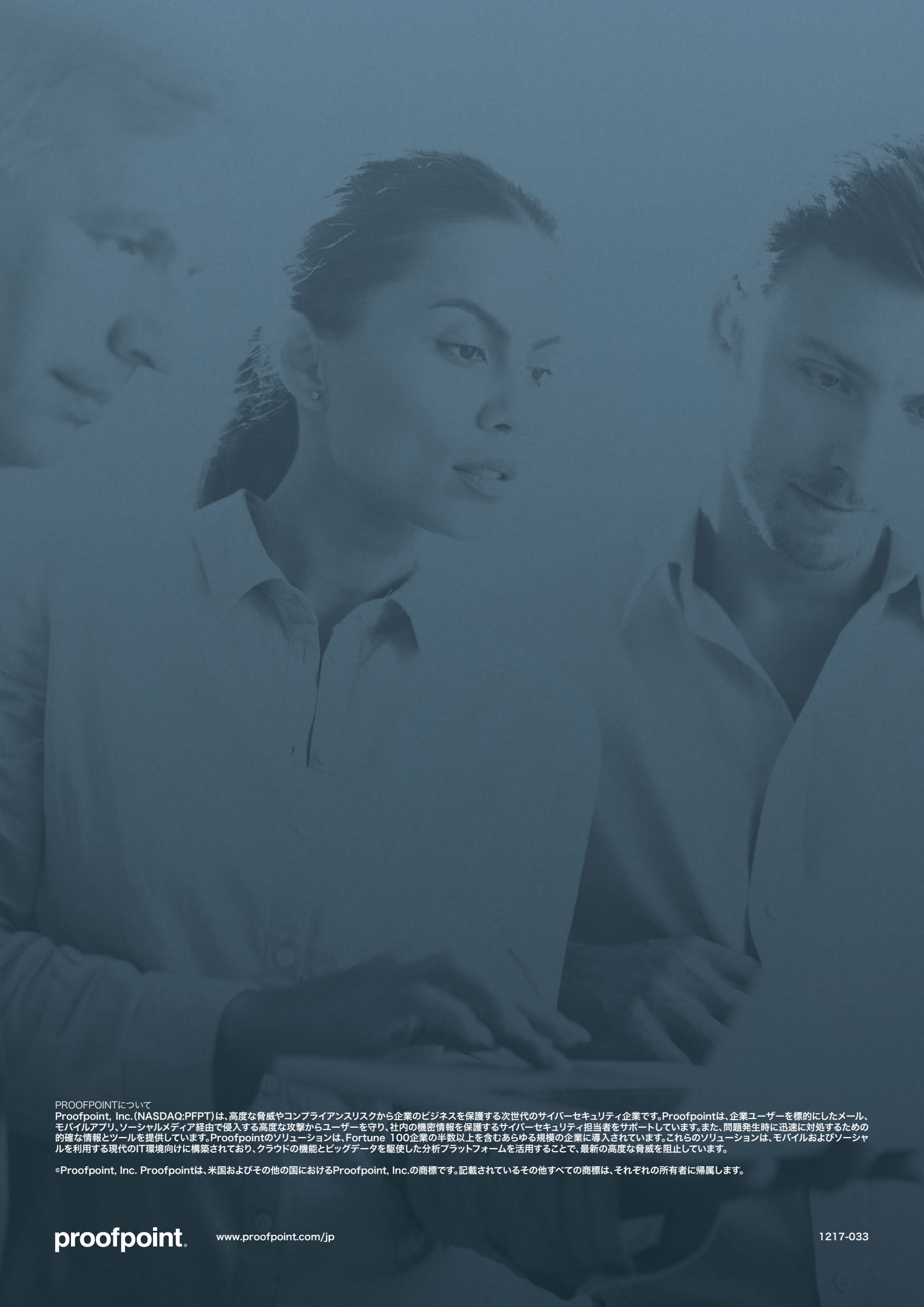
ユーザーはクリックするものと思うべし。ソーシャルエンジニアリングは、電子メール攻撃を仕掛けるための手段として一般化しつつあり、犯罪者は人的要因を悪用する新たな方法を次々に見つけ出します。従業員を標的とした着信メールの脅威および顧客を標的として送信される脅威の両方を受信トレイへの到達前に突き止め、隔離するソリューションを活用してください。

メール詐欺から守る強固な防御を築くべし。標的を絞り込んだ少量のメール詐欺は、ペイロードがまったくないケースがほとんどのため、検出は容易ではありません。隔離およびブロックポリシーの構築に利用できる動的分類機能を備えたソリューションに投資してください。

ブランドの評判と顧客を守るべし。ソーシャルメディア、電子メール、およびモバイルで、顧客を標的とした攻撃、特に自社ブランドに便乗する不正なアカウントへの対策を講じてください。また、ソーシャルネットワークをすべてスキャンし、不正な活動を報告する包括的なソーシャルメディアセキュリティソリューションを導入してください。

脅威インテリジェンスベンダーと提携すべし。比較的小規模な標的型攻撃に対抗するには、高度な脅威インテリジェンスが必要です。静的および動的手法を組み合わせて新たな攻撃ツール、戦術、標的、さらに絶えず移り変わる状況を検出し、そこから学習することのできるソリューションを活用してください。

最新の脅威の調査結果および現代の高度な脅威とデジタルリスクに関するガイダンスについては、proofpoint.com/jp/threat-insightをご覧ください。



PROOFPOINTについて

Proofpoint, Inc.（NASDAQ:PFPT）は、高度な脅威やコンプライアンスリスクから企業のビジネスを保護する次世代のサイバーセキュリティ企業です。Proofpointは、企業ユーザーを標的にしたメール、モバイルアプリ、ソーシャルメディア経由で侵入する高度な攻撃からユーザーを守り、社内の機密情報を保護するサイバーセキュリティ担当者をサポートしています。また、問題発生時に迅速に対処するための的確な情報とツールを提供しています。Proofpointのソリューションは、Fortune 100企業の半数以上を含むあらゆる規模の企業に導入されています。これらのソリューションは、モバイルおよびソーシャルを利用する現代のIT環境向けに構築されており、クラウドの機能とビッグデータを駆使した分析プラットフォームを活用することで、最新の高度な脅威を阻止しています。

proofpoint®

www.proofpoint.com/jp

1217-033