proofpoint

レポート

四半期脅威レポート

2017年
第3四半期

www.proofpoint.co.jp

Proofpointの四半期脅威レポートは、当社の幅広い顧客ベースやより広範な脅威状況で確認されている脅威、傾向、および重要項目を示すものです。

当社は、毎日、10億通を超える電子メールメッセージや、数億件ものソーシャルメディア投稿、1億5000以上のマルウェアサンプルを分析し、高度な脅威から世界中の組織を保護しています。電子メール、ソーシャルメディア、およびモバイルの3つの主要な侵入経路で、高度な脅威を常に監視しています。これにより、今日のサイバー攻撃の戦術、ツール、および標的を把握して分析できる有利な位置に立つことができています。

本レポートは、今日の攻撃に適切に対処し、新たな攻撃を予測し、セキュリティ体制を管理するための、すぐに行動に移せる情報を提供することを目的としています。本レポートでは、当社の調査結果とともに、ユーザー、データ、およびブランドを保護するためのステップを推奨しています。

目次

重要事項：今後の予測

ここ数年間、第3四半期は脅威研究者にとって一触即発の状況となっています。この時期に、メッセージ量が最大レベルに達し、攻撃者が今後数か月間に渡って使用するツールや手法が出現し始めます。今年も、第3四半期は同様のパターンをたどっています。

悪意のあるURLを使用したメール攻撃の量が急増し、添付ファイルを使用した攻撃に比べ、メール攻撃に占める割合が2年以上に渡って最も高くなっています。ランサムウェアとバンキング型トロイの木馬が引き続き、よく使用されるペイロードとなっています。

その一方で、ソーシャルメディアにおけるメール詐欺と攻撃では、ソーシャルエンジニアリングと標的型手法がさらに進化しています。

また、さまざまな攻撃や詐欺に使用されている、よく似たドメインに関する当社最初の公開レポートで、攻撃者がいち早くドメインを登録していることが示されています。事前予防的に対処している組織は「防御的」な登録を行っていますが、当社はこのような登録に対しても、第三者によって登録された20件の疑わしくよく似たドメインを検出しました。

2017年第3四半期の重要項目はこちらです。

メール

悪意のあるURL攻撃が急増したため、悪意のあるメールの量が前四半期より85%増加。
ホストされたマルウェアにリンクしている、悪意のあるURLが含まれたメールの量が前四半期より約600%急増しており、前年の同四半期より2,200%以上増加しています。この急増では、2017年第1四半期に見られた傾向がさらに強くなっており、2014年以降、その量は、添付ファイルベースのメールに比べ、URLメールの割合が最も高くなっています。悪意のある添付ファイルを使用した大規模なキャンペーンも、この急増を牽引する要因となっています。この場合、圧縮ファイルアーカイブの添付ファイルにマルウェアが潜んでいます。

ランサムウェアが引き続き、マルウェアカテゴリのトップに。
当社のグローバルな顧客ベース全体で、ランサムウェアがメールマルウェア攻撃全体の約64%を占めています。新しい型のランサムウェアが日々出現していますが、Lockyが引き続きペイロードのトップとなっています。Lockyは全メッセージ量の約55%を占めており、全ランサムウェア量の86%以上を占めています。それと同時に、PhiladelphiaおよびGlobeImposterという型が地域を標的とした小規模な型から世界的な脅威へと成長しました。これは、1人の攻撃者が大規模なキャンペーンを何度か行ったためです。

バンキング型トロイの木馬
このタイプのマルウェアは、通常、被害者のブラウザを偽バージョンのバンキングWebサイトにリダイレクトするか、偽のログインフォームを実際のサイトに注入して、被害者のバンキングログイン認証情報を盗みます。

ETERNALBLUE
EternalBlueは、Windowsファイル共有コンポーネントの弱点を悪用する強力なハッキングツールです。2017年初めに米国国家安全保障局から盗まれて一般に流出しました。

バンキング型トロイの木馬が悪意のあるメール量全体の24%を占め、The Trickという型がその70%を占めた。
1人の攻撃者が行った大規模なキャンペーンにより、The TrickがDridexに代わってバンキング型トロイの木馬のトップになりました（Dridexは、第1四半期はほとんど休止していましたが、第2四半期の大規模なキャンペーンに再度出現しました）。Dridexは、Ursnif、Bancos、Zloaderとともに、引き続き地域標的型のキャンペーンに出現しました。また、出現したのは、新しいバージョンのRetefeでした。Retefeでは、内部ネットワークに拡散させるために米国国家安全保障局から流出したETERNALBLUEと呼ばれるエクスプロイトが使用されました。

前四半期と比べ、メール詐欺が29%増加。
攻撃の頻度も増加しており、標的となった組織あたりのメール詐欺攻撃が前四半期より12%増加し、前年の同四半期より32%増加しました。メール詐欺は規模で区別しておらず、より複雑なサプライチェーンを擁している組織ほど標的となる頻度が高くなっています。

エクスプロイトキット（EK）
エクスプロイトキット（EK）はWeb上で実行され、接続しているコンピュータの脆弱性を検出して悪用します。EKは、サービスとして攻撃者に販売されることが多く、「自動的な」マルウェアダウンロードでPCを簡単に感染させます。

エクスプロイトキットとWEBベースの攻撃

エクスプロイトキット（EK）のトラフィックは横ばいの状態。ただし、2016年のピーク時のわずか10%のレベルに。
RIG EKが、EKアクティビティ全体の76%を占めていました。攻撃者はEKキャンペーンにソーシャルエンジニアリングスキームを組み込んでいます。傾向から、検出と入手をさらに難しくするために、攻撃者がエクスプロイト単独を超えたものを検討していることがうかがえます。

防御的な登録
攻撃者が買う前に、自社のインターネットドメインと誤解される可能性があるドメインを買い占めるという推奨される方法。よく似たドメインを、自社のもののように見える偽のWebサイトや不正メールと組み合わせて、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、攻撃者がソーシャルメディアで偽のカスタマサポートアカウントを作成し、支援を必要としているユーザーをだましてフィッシングサイトにアクセスさせたり、認証情報を提供させたりします。

TA505
金銭的利益を動機とするこの脅威攻撃者は、拡散された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、記録上最大規模のメール攻撃キャンペーンの一部を開始しました。

LOCKY
Lockyは、悪意のあるメールに使用される一般的なランサムウェアの型で、被害者のデータを暗号化し、復号化するために被害者が身代金を支払うまで、このデータを「人質」にします。2016年の大半と2017年の数か月間、Lockyは悪意のあるメールトラフィックの大部分を占めていました。

ドメイン

疑わしいドメイン登録が防御的な登録の20倍に。
タイポスクワッティングやドメインなりすましに対処するために、ドメインを積極的に登録している組織もありますが、多くの組織はそうではありません。ブランド所有のドメインの防御的な登録は、前年の同四半期より20%減少しました。疑わしいドメイン登録は20%増加しました。

ソーシャルメディア

ANGLERフィッシングに使用される不正なサポートアカウントが前年の同四半期の2倍に増加。
偽のカスタマサポートアカウントの数が前四半期より5%増加し、ブランドのソーシャルチャネルに対するフィッシングリンクの量も10%増加しました。

メールベースの脅威の傾向

基本統計：URLベースのマルウェアキャンペーンが前四半期より約600%増加し、前年の同四半期より2,200%以上増加。

悪意のあるURLによってマルウェアを拡散させる詐欺メールの量が大幅に増加しました。最大の要因の1つがTA505です。TA505は、非常に多くの型を作成している攻撃者で、拡散手段を添付ファイルからURLに切り替えた大規模なLockyキャンペーンで最もよく知られています。また、TA505は、ランサムウェアPhiladelphiaとGlobeImposterや、バンキング型トロイの木馬のThe Trickを、影響を与えるのに十分な量で送信しました。

悪意のある添付ファイルが含まれたメールは74%減少したにもかかわらず、この急増により、悪意のあるメールの量全体が前四半期より85%増加しました。

悪意のある添付ファイルは引き続き、全体の大きな部分を占めています。攻撃者は、少数の添付ファイルキャンペーンを開始し、それと同時に、圧縮ファイルのアーカイブに悪意のあるコードを隠した非常に大規模なキャンペーンをいくつか開始しました。キャンペーンにはRARおよび7-Zipアーカイブファイル形式が使用され、大抵の場合は悪意のあるJavaScriptまたはVBScriptが含まれていました。ファイルを実行すると、スクリプトによってランサムウェアLOCKYがダウンロードされてインストールされました。

図1および図2に示すように、グローバルなメッセージ量全体で、悪意のあるURLメッセージの割合は64%に達しました。これは、2014年以降は見られなかった割合であり、昨年は、攻撃キャンペーンのメッセージのほとんどが悪意のあるURLメールでした。結局のところ、両方のアプローチの目的は同様です。URLで拡散するのか添付ファイルで拡散するのかに関係なく、Lockyはこれらの大規模なキャンペーンの大部分にペイロードとして使用されました。

疑わしい登録と防御的ブランド登録の比較、2017年現在まで

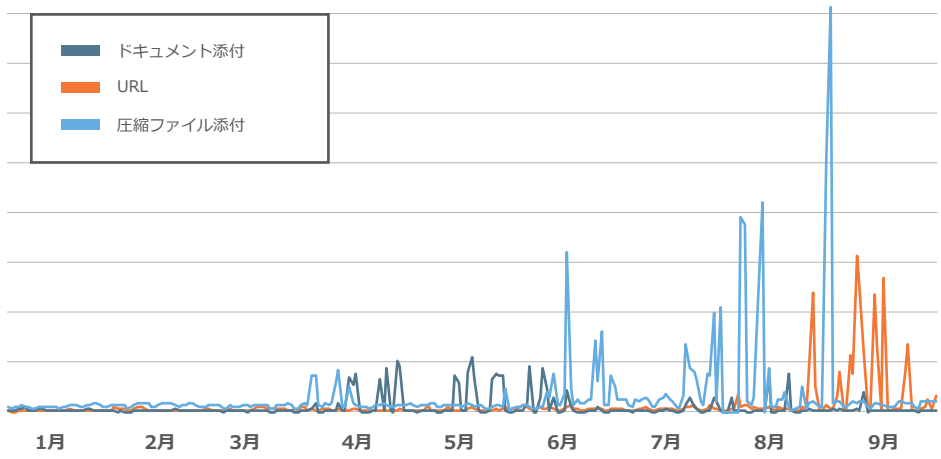

図1：インデックス付き、攻撃タイプの傾向、2017年1月から9月まで（273日間）

インデックス付き、攻撃タイプ別、悪意のあるメッセージの一日あたりの量の比較、2017年第3四半期

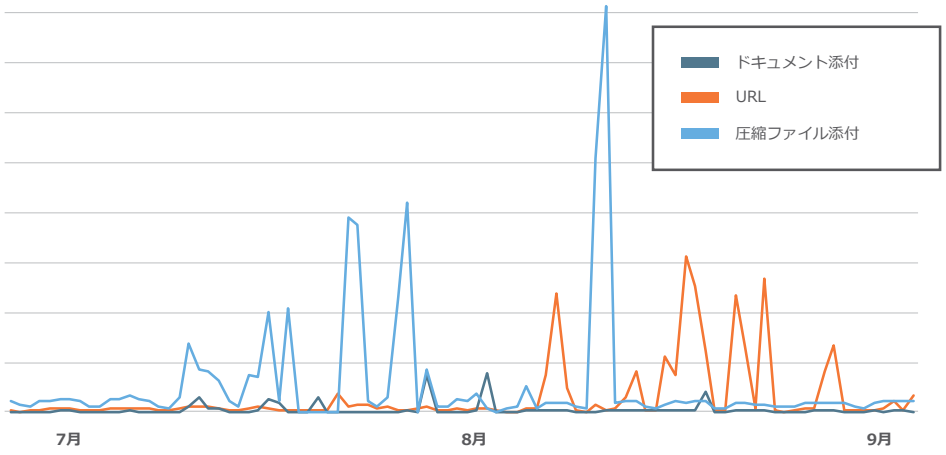

図2：インデックス付き、攻撃タイプの傾向、2017年7月から9月まで（92日間）

図3は、ランサムウェア（特にLocky）が現在主流であることを示しています。バンキング型トロイの木馬の**THE TRICK**を拡散させる大規模なキャンペーンが数回行われたため、この四半期の後半に何度か急増しました。

THE TRICK

The TrickはTrickbotとも呼ばれ、Dyreと密接に関係のあるバンキング型トロイの木馬です。Dyreのオペレータは2015年にロシア当局に逮捕されましたが、このマルウェアは2017年に再開されました。

ランサムウェア、バンキング型トロイの木馬、その他のマルウェアの比較

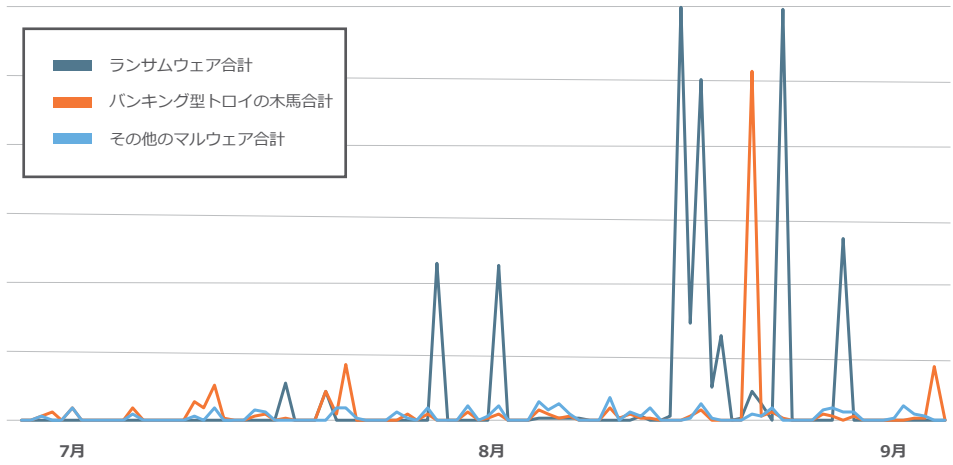

図3：2017年7月から9月まで（92日間）

バンキング型トロイの木馬：従来の攻撃者の新しい傾向

基本統計：バンキング型トロイの木馬を送信する全メールの70%をThe Trickが占めた。
このマルウェアの大部分は、ランサムウェアLockyとバンキング型トロイの木馬のDridexを使用して大規模なメールキャンペーンを行った、脅威攻撃者TA505によるものです。

TA505がThe Trickに切り替えたため、**DRIDEX**トラフィックは大幅に減少しました。同時に、**ZLOADER**アクティビティは、この四半期のほとんどの期間は横ばいの状態でしたが、第2四半期よりも低いレベルになりました。一方、Zeus Panda、Emotet、およびURLZoneが地域を標的とした大規模なキャンペーンに使用されました。

より大規模な開発では、**RETEFE**やThe Trickなどのバンキング型トロイの木馬がエクスプロイトEternalBlueと併用されました。この併用により、最初のメール感染の後で、トロイの木馬が単独で内部ネットワークに拡散できるようになっています。ドイツ語により主にスイスの銀行を標的とするRetefeは、DridexやZeusの量や範囲には到達していません。ただし、初夏に発生した**WANNACRY**の大流行の余波（EternalBlueも使用）が、2018年の傾向を示唆しています。さらに多くの攻撃者が、WannaCryやNotPetyaで明らかになったセキュリティ脆弱性を利用する可能性があります。

図4は、バンキング型トロイの木馬の1日あたりの発生数を示しています。The Trickのトラフィック急増がこの四半期に何度か発生しており、主にZloaderとPanda Bankerによるトラフィック増加を小さく見せています。

上位のバンキング型トロイの木馬の一日あたりのメッセージ量の傾向、インデックス付き、2017年第3四半期

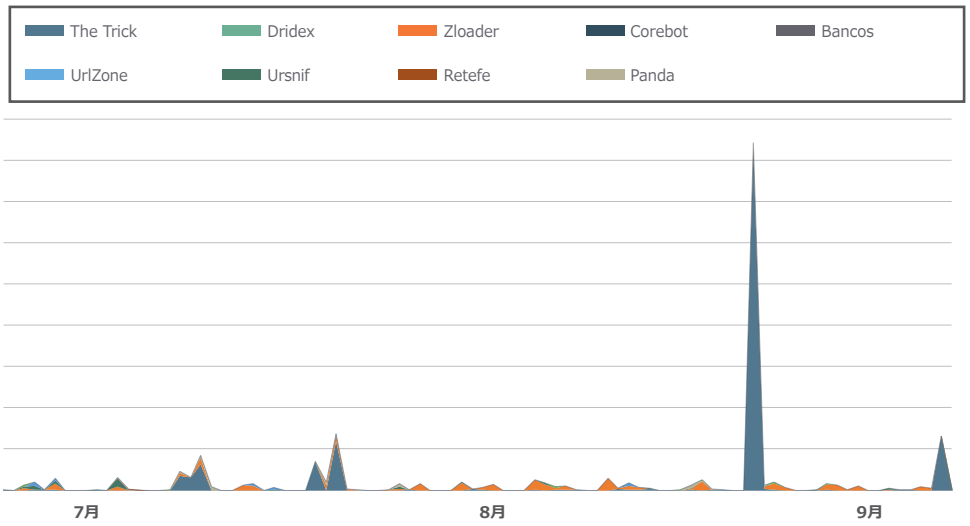

図4：上位のバンキング型トロイの木馬の型の一日あたりのメッセージ量、インデックス付き、2017年7月～9月

DRIDEX
Dridexは広く使用されているバンキング型トロイの木馬で、さまざまな侵入経路（主にメール）を介して拡散され、被害者に感染し、バンキングに関する認証情報を盗みます。

ZLOADER
ZloaderはTerdotとも呼ばれるダウンローダで、バンキング型トロイの木馬のZbotやほかのマルウェアの型とともに使用されることが多くなっています。

RETEFE
このバンキング型トロイの木馬は、主にヨーロッパを標的にしています。Retefeは、多くのバンキング型トロイの木馬とは異なり、認証情報を盗むために正規のバンキングWebサイトに偽のログインフォームを注入するのではなく、一連のプロキシサーバーを介して偽バージョンのバンキングWebサイトにユーザーをリダイレクトします。

WANNACRY
5月に150か国以上で数万のシステムを感染させたランサムウェアで、この感染は記録上最大のサイバー攻撃の一つとなりました。Microsoft Windowsのファイル共有コンポーネントの弱点を介して拡散します。

ランサムウェア：Lockyによる高利益の一方で、破壊的なランサムウェアが増加

基本統計：当社のグローバルな顧客ベース全体で、ランサムウェア攻撃が悪意のあるメッセージ量全体の約64%を占めた。

ランサムウェアは引き続き、脅威状況において主流となっていました。新しい型が毎日のように出現し、破壊的なランサムウェアの開発が続き、標的型攻撃が増加しました。

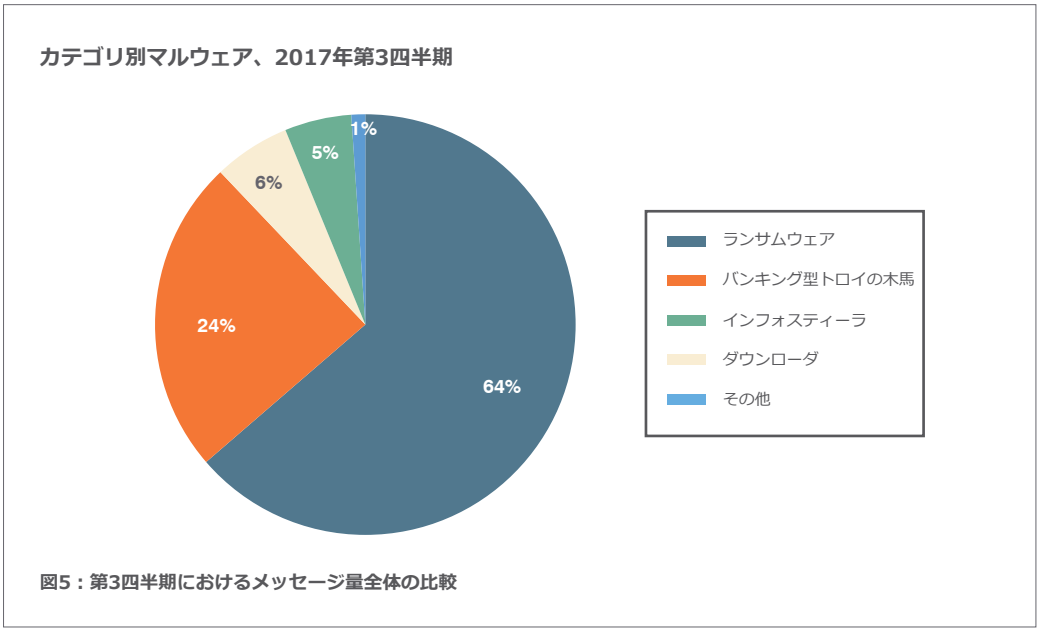

図5：第3四半期におけるメッセージ量全体の比較

ほとんどのランサムウェアは、TA505が行った非常に大規模なLockyキャンペーンで使用されました。ただし、TA505はランサムウェアの型であるGlobeImposterとPhiladelphiaも拡散させました。特に、これらの型の1つにLockyの「オフライン」バージョンが含まれており、被害者のファイルを暗号化するために、中央のコマンドアンドコントロール（C&C）インフラストラクチャは必要ありませんでした。

アフィリエイトID
マルウェア作成者は、多くの場合アフィリエイトに有償でマルウェアを拡散してもらいます。正しい作成者が感染の功績を認められるように、アフィリエイトIDはマルウェアのバージョンにハードコードされます。

ほかの攻撃者は、無差別型の大規模なキャンペーンから、より標的を絞った攻撃に移行しました。ある攻撃者が、8月に医療機関と教育機関を標的とした小規模な攻撃にランサムウェアの型Defrayを取り入れ、ほかの攻撃者もそれにならいました。キャンペーンに使用されたLockyの新しい**アフィリエイトID**のいくつかは、より高レベルの教育機関や医療機関を主に標的としていました。これらの少なくとも1つ（Affid=36）が、オフラインバージョンのLockyを拡散させました。

NOTPETYA
このマルウェアの型はランサムウェアPetyaになりすましましたが、身代金を集めるのではなく混乱を引き起こすための、国家ぐるみのツールと見られています。

第2四半期後半にウクライナで発生したWannaCryおよびPetya-Likeの攻撃に続いて、ほかの型が出現しました。Hell（7月に検出）とIsraByte（8月に検出）は弾みがつかず、注目されませんでした。ただし、**NOTPETYA**やWannaCryと同様に、HellとIsraByteも金銭的利益よりも破壊を目的としているようでした。

図6に示すように、第3四半期に発生した大規模な攻撃では、新しい型とその使用にもかかわらず、攻撃者はより少数のランサムウェアの型を統合していました。TA505が推進したため、Locky、GlobeImposter、およびPhiladelphiaが主流になりましたが、新しいLockyの拡散も総数に追加されています。SAGEやTorrentLockerなどの型は、大幅に減少しました。

上位のランサムウェアの型の一日あたりのメッセージ量の傾向、インデックス付き、2017年第3四半期

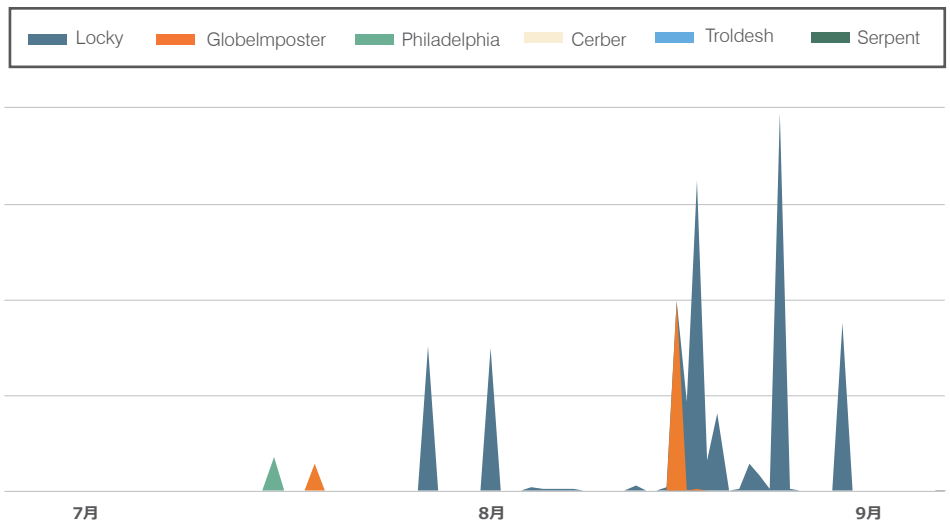

図6：上位のランサムウェアの型の一日あたりのメッセージ量、インデックス付き、2017年7月～9月

ランサムウェア
このタイプのマルウェアは、被害者のデータを暗号してロックし、復号鍵でロック解除するために「身代金」を要求します。

昨年は**ランサムウェア**の新しい型が急増しましたが、これがようやく少し減速しているようです。ただし、脅威が減ったためではありません。

平均して1日あたり1.4のランサムウェアの新しい型が出現しています。前四半期の1日あたり1.8の新型から、減少しています。この減少は、前四半期の合計数を増加させていた多数の「小規模プロジェクト」、概念実証、実験的、および「スクリプトキディ」のランサムウェアの型が減少したためと考えられます。

つまり、この減少は、ランサムウェアの脅威が減ったことを示している訳ではありません。そうではなく、攻撃者がランサムウェアを新しい方法で使用してさらに高度化し、少数のさらに効果的な型を統合していることを示唆しています（図7）。

新たに報告された型

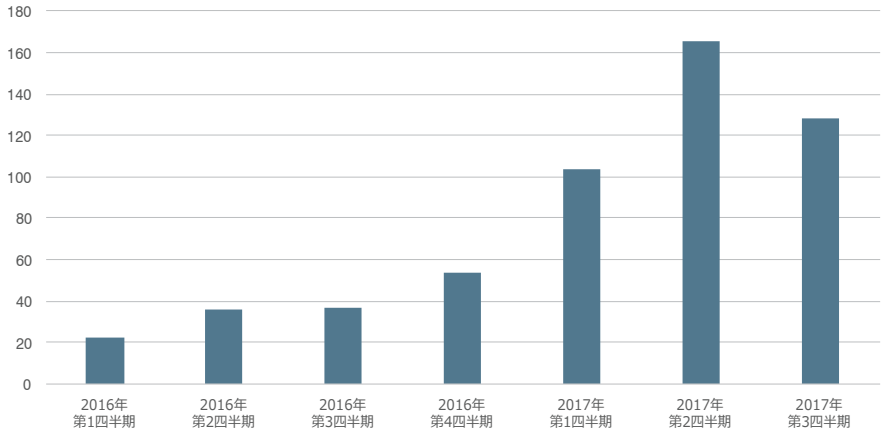

図7：新たに報告されたランサムウェアの型、四半期ごと、2016年～2017年現在まで

コインマイナーマニア

仮想通貨発掘者、つまり「コインマイナー」は、感染したマシンのシステムリソースを使用して脅威攻撃者に対して電子キャッシュを生成するマルウェアの型です。ビットコインやライトコインなどの仮想通貨は、希少性を生成して通貨の価値を確保するためのメカニズムが組み込まれています。このメカニズムにより、新しい通貨ユニットを「発掘」するために必要となる計算の実行がかつてないほど難しくなっています。最も人気のある主流の仮想通貨であるビットコインは、現在、発掘するにはスーパーコンピュータ並みの計算能力が必要です。ただし、ライトコインやMoneroなどのその他の仮想通貨はいまだにデスクトップクラスのコンピュータで発掘でき、多数のクライアントシステムのCPUサイクルを盗んで発掘することも可能です。

そのため、これらの通貨を標的としたコイン発掘のマルウェアが増加しています。コイン発掘のマルウェアはエクスプロイトキットやソーシャルエンジニアリングスキームによって拡散され、EternalBlueのようなNSAエクスプロイトによっても拡散されています。Pirate Bayは閲覧者のCPUサイクルを使用してMonero通貨を発掘したため、最近トップニュースになりました。

脅威は多面的です。サーバー側のWeb脆弱性を標的とし、アクセスしているブラウザのCPUリソースを使用するようコインマイナーを取り込む、スクリプトを埋め込む攻撃もあります。また、フィッシングを使用して、トレンドとして広範に渡って急成長している、ユーザーの仮想通貨ウォレットの認証情報を盗む攻撃もあります。この攻撃でも、被害者のPCをコインマイナーにするためにマルウェアが使用されています。

使用する手法に関係なく、脅威攻撃者は、発掘のために被害者のPCを悪用する新たな手段を検討している可能性が高いです。より少額の通貨がビットコインの飽和レベルに達するまで、見通しは非常に利益の多いものとなっています。脅威攻撃者は、時期と「マネーを追いかける」意欲を示しています。

仮想通貨
セキュアかつ匿名性を確保するように設計された一種のデジタルマネー。この通貨を商品の売買に使用でき、政府発行の通貨に交換することも可能です。コンピュータ処理能力を使用して複雑な計算問題を解決する「マイニング」プロセスによって生成されます。

ドメインなりすまし
ドメインなりすましとは、攻撃者のメールを正規の期待されるアドレスから送信されたように見せて、信頼できる同僚や連絡先になりすますことです。実際のドメイン名のように見える、よく似たドメイン名を使用したドメインなりすましもあります。

メール詐欺の増加と攻撃者による手法の巧妙化

基本統計：当社のグローバルな顧客ベース全体で、メール詐欺攻撃が前四半期より29%増加。

メール詐欺攻撃の総数が増加するにつれ、標的となった組織に対する攻撃の頻度も増加しています。メール詐欺攻撃は前四半期より12%、前年の同四半期より32%増加しました。

一般的なメール詐欺手法であるドメインなりすましも、さらに増加しました。このタイプの攻撃は、メール認証を使用すると完全に阻止できます。依然として、89%もの組織がこの四半期に少なくとも1回のドメインなりすましに遭っています。

標的になった業種

すべての業種が引き続き、メール詐欺の標的になりました。ただし、過去の四半期と同様に、攻撃者はより複雑なサプライチェーンを擁する組織を標的としたようです。たとえば、メーカーは引き続き、ほかの業種よりも標的になる頻度が高くなっています。図8は、標的になる相対頻度を業種別で示しています。この図は、2017年の第3四半期、2017年の第2四半期、および前年の同四半期を比較したもので、いずれの四半期でも同様の相関関係が示されています。

標的となった業種—2017年第3四半期、2017年第2四半期、2016年第3四半期の比較

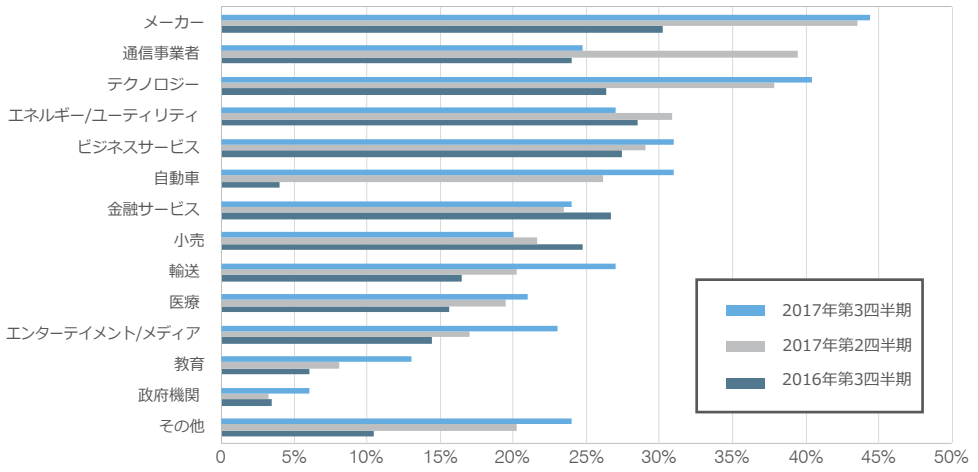

図8：標的にされた業種別の、企業あたりのメール詐欺攻撃の平均数、2017年第3四半期、2017年第2四半期、2016年第3四半期の比較

メール詐欺

メール詐欺攻撃では、幹部トップから送信されたと称するメールによって、送金するか機密情報を送るように受信者が求められます。添付ファイルやURLは使用されないため、検出して阻止するのが難しい可能性があります。

メール詐欺に関する当社の分析により、企業の規模とメール詐欺攻撃の頻度に相関関係はないことが分かりました。第2四半期には、サイバー犯罪者が大規模な組織を優先させる兆候が多少ありましたが、統計的にそれほど大きなレベルではありませんでした。この四半期では、明白な相関関係は全くなくなりました。あらゆる規模の企業が一様に標的になりました。

個人標的設定が精緻に

本質的に、メール詐欺は完全に標的型です。この事実は、攻撃者が組織あたりでさらに多くの身元になりすまし、さらに多くの従業員を標的にしていることから、かつてないほど明白になりました。標的となった組織のほぼ4分の3で、2人以上の身元がなりすまされて、2人以上の従業員が標的になりました。「ホエーリング」と呼ばれる、経営幹部レベルのエグゼクティブのなりすましメールを使用して、別の経営幹部レベルのエグゼクティブを標的にする攻撃が、引き続きよく発生しています（このタイプの攻撃は、図9に「1対1」攻撃と示されています）。ただし、サイバー犯罪者は範囲を広げており、同じ組織内のさらに多くの人々を標的にしています。

標的にされたスタッフ数別のなりすましに遭った身元数、2017年第3四半期、2017年第2四半期、2016年第3四半期の比較

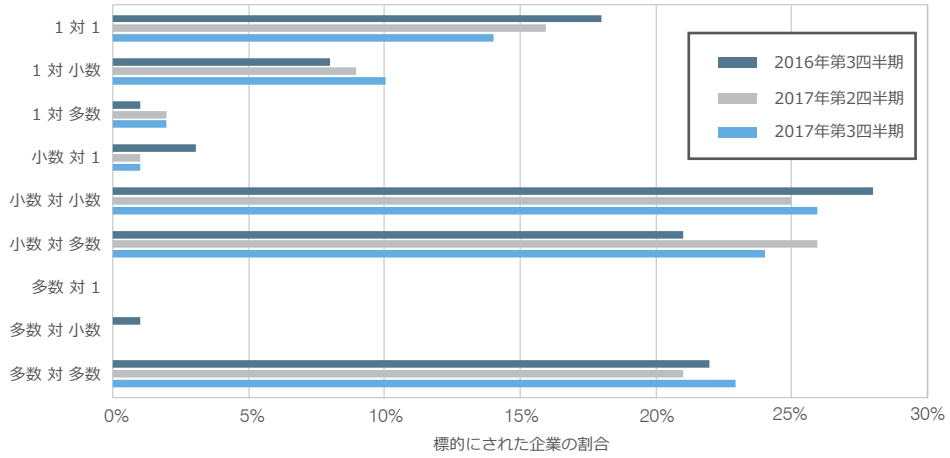

図9：なりすましに遭った幹部の身元数に対する、標的とされた個人数別の攻撃タイプ。例えば、メール詐欺攻撃を受けた企業で、4名の幹部の身元がなりすまされ、かつ10名の財務部門の人員が標的になった場合、「少数 対 多数」の攻撃に分類される。

また、攻撃者は引き続き、偽のチェーンメールを使用して攻撃者のメールがより信用されるようにしています。第3四半期には、全メール詐欺の約10%でこの戦術が使用されました。

エクスプロイトキット：減少したが、なくなった訳ではない

RIG EK

RIGは、2016年6月にAnglerのオペレータが逮捕された後、Anglerの消滅のすぐ後に最も有名なEKとなりました。

基本統計：第3四半期の全エクスプロイトアクティビティの73%にRIG EKが関与。

エクスプロイトキットは、2016年初めにピークを迎えた後で、広く報道されているように大幅に減少しました。アクティビティは2016年のレベルのわずか10%程度で低迷していますが、EKは引き続き、脅威状況の重要な部分になっています。このことは、高レベルのソフトウェア不正コピーが定期的なパッチ適用の妨げとなっている地域で、特に当てはまります。

また、新しいソーシャルエンジニアリングスキームがEKに使用されており、攻撃者は最新のエクスプロイトを使用しなくても攻撃を行えます。ただし、エクスプロイトキットのランディングページにトラフィックを誘導することを目的とした、「traffer」ネットワークによるアクティビティが増加していることが確認されています。この変化は、今後数か月間にエクスプロイトキット（EK）アクティビティが再開される可能性があることを示唆しています。

現在のところ、RIG EKは引き続き主流のエクスプロイトキットとなっており、この四半期に確認されたEKトラフィック全体の73%を占めています。この四半期末までに、すでに弱まっていたAngler EK関連のトラフィックはほとんど見られなくなりました。この四半期の若干の期間、トップの座をRIGと争っていたNeutrinoも、この四半期末にはほぼ完全にRIGにトップを明け渡しました。図10は、上位のエクスプロイトキットのトラフィックを示しています。

エクスプロイトキットアクティビティー2017年第3四半期に収集されたサンプルのシェア

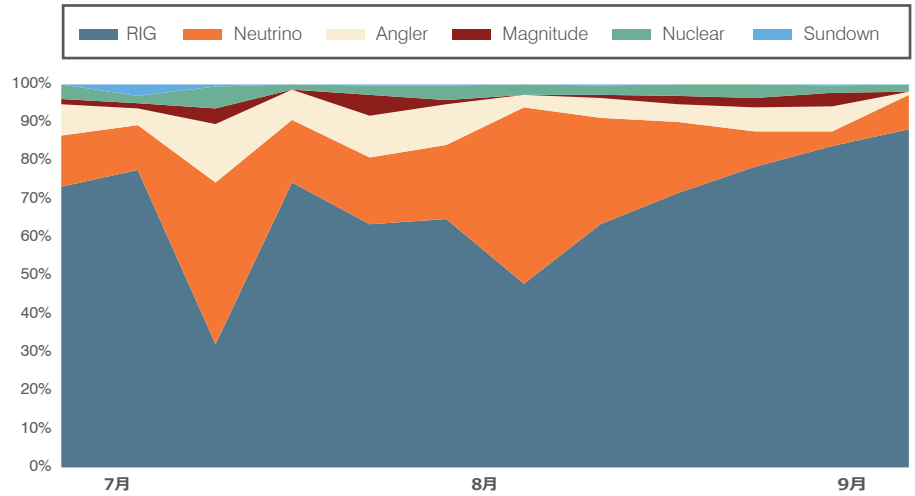

図10：全体における比率での、上位のエクスプロイトキットトラフィック、2017年4月～5月

ドメインの傾向

基本統計：疑わしいドメイン登録の数が防御的な登録の20倍になり、ブランドを保護しようとする企業とブランドを悪用しようとする攻撃者のギャップが広がった。

タイポスクワッティング
詐欺者は、正規のドメインのスペルミスのドメインまたは異なる表現のドメインを登録し、URLを間違って入力したユーザーやメールヘッダーを詳しく確認しないユーザーをだまします。

第3四半期に当社は、Fortune 50企業を対象として「疑わしいドメイン」の登録を調べるように調査を拡大しました。疑わしいドメインとは、**タイポスクワッティング**やなりすましに使用される可能性が高いドメインのことです。

2015年初めから2017年8月まで、ブランド所有の防御的なドメインが減少する一方で、ブランド以外の第三者によって登録された疑わしいドメインが増加しています（図11）。2017年1月から8月までの期間に、前年の同期間と比較し、ブランド所有の防御的な登録が前年の20%減少したのに対して、疑わしいドメイン登録が20%増加しました。

これらの防御的な登録を行っても、疑わしいドメインはブランド所有のドメインを歴史的にはるかに上回ってきました。2016年に行われた防御的な登録すべてに対して、当社は第三者による10件の疑わしいよく似た登録を確認しました。今年は、疑わしい登録が防御的な登録の20倍になっています。

また、防御的な登録の増加は通常、現行の防御ではなく、新製品発売などのブランド関連の主要イベントに関係しています。

インデックス付き、攻撃タイプ別、悪意のあるメッセージの一日あたりの量、2017年現在まで

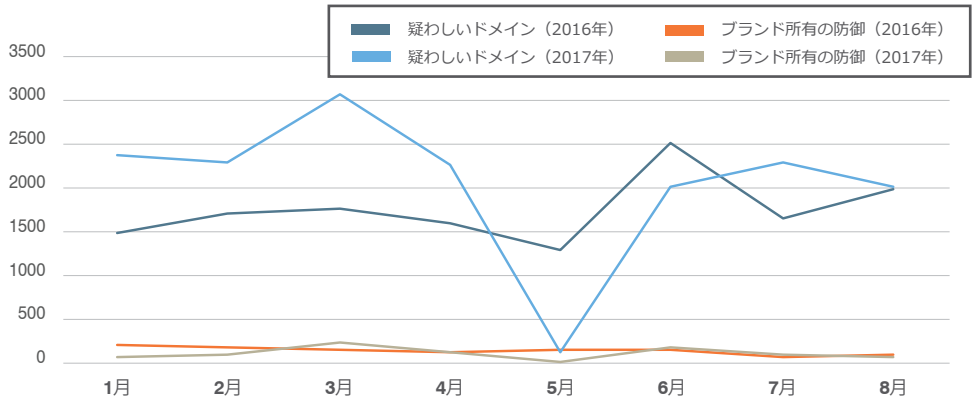

図11：Fortune 50社における疑わしいドメイン登録とブランド所有の防御的登録の前年同期比較（2016年第1四半期～第3四半期と2017年第1四半期～第3四半期）

ソーシャルメディアの傾向

基本統計：不正なカスタマサポートアカウントが前年の同四半期の2倍に増加。

ソーシャルメディアの脅威は、マルウェアの拡散から詐欺まで多種多様であり、非常に多くなっています。当社では、以下の2つの主要カテゴリを追跡しています。

- 「Anglerフィッシング」に使用される不正なサポートアカウント
- 認証情報や個人情報を盗むページにユーザーを誘導する、より従来型のフィッシングリンク

偽のカスタマサポートアカウントの数は前四半期より5%増加し、前年の同四半期の2倍に増加しました。ブランドのソーシャルメディアアカウントのフィッシングリンクは、前四半期より10%増加し（図12）、前年の同四半期からほぼ横ばいになっています。

これらの情報から、ソーシャルメディアの攻撃が大きく変化していることが分かります。攻撃者は、イベントや季節的な傾向には従来型のフィッシングで対処しながら、利益の多いAnglerフィッシングに注意を向けています。

ソーシャルメディアによる標準的な認証情報フィッシングがさらに簡単になる可能性があります。ただし、標的型のAnglerフィッシングは、ブランドのソーシャルメディアページのコメントに投稿されるランダムなリンクよりもかなり人間的であり、被害者にとって正規のように見えるため、成功する可能性がより高くなっています。

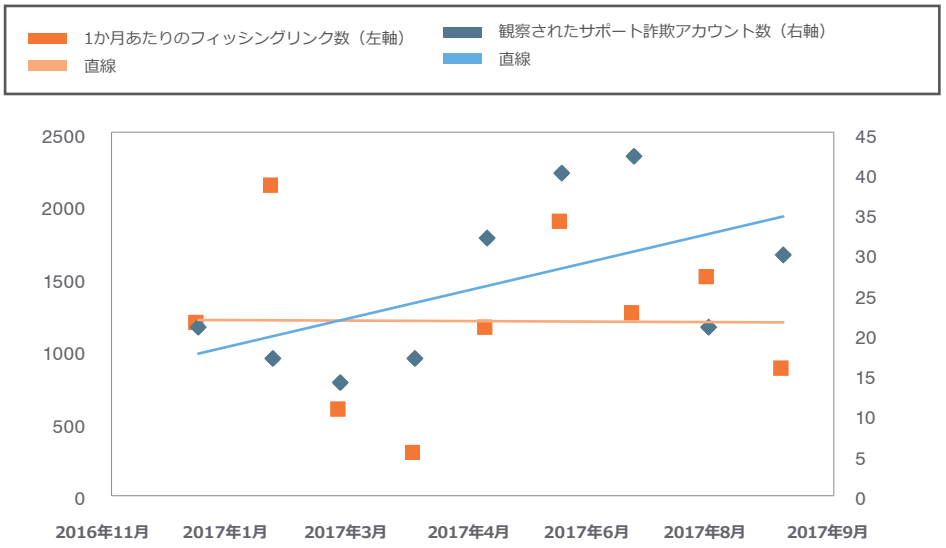

図12：ソーシャルメディア経由と不正なサポートアカウント経由を比較したフィッシングリンク配布における相対的な月別アクティビティ

推奨

このレポートは、脅威状況の変化に関するインサイトを提供しており、企業のサイバーセキュリティ戦略に活用できます。企業のデータ、従業員、ブランドを今後の数か月に渡って保護する方法の主な推奨項目はこちらです。

Web上のタイポスクワッティングに対処する
防御的なドメイン登録は、メール詐欺や認証情報フィッシングに使用されるよく似たドメインを攻撃者に作成させないための、簡単かつコスト効率の高い戦術です。ビジネスリーダーと連携し、登録される可能性があるよく似たドメインのリストを定義します。標的となる頻度が高い、会議やマーケティングキャンペーンのWebサイトを含めます。

メール詐欺に使用されるドメインなりすまし手法を阻止するため、メール認証を導入する
DMARC（Domain-based Message Authentication, Reporting & Conformance）などのプロトコルを使用すると、詐欺者がメールドメインを使用するのを阻止できます。よく似たドメインを使用したメール攻撃に対しては、自社のドメインと誤解される可能性があるドメインを特定し、サードパーティサービスを使用してそれらのドメインを削除できる必要があります。

あらゆるタイプのメール攻撃からユーザーを保護する
マルウェア添付ファイル、悪意のあるURL、ソーシャルエンジニアリングのメール詐欺のいずれの場合でも、メール防御によって広範囲のメールベース脅威に対応する必要があります。強力な保護には、疑わしいURLや添付ファイルを先制的に特定してサンドボックス化するための、強力な分析機能が含まれます。この保護により、多段階のサンドボックス分析を使用して、悪意のある添付ファイルとURLを、配信時およびその後に従業員がクリックするときに特定する必要があります。また、メールなどの、従業員をだますマルウェア以外の脅威を特定して、詐欺師への送金や機密情報の送信を阻止する必要があります。

脅威インテリジェンスベンダーと連携する
小規模な標的型攻撃には、高度な脅威インテリジェンスが必要です。分析データと脅威インテリジェンスを1つに統合するソリューションを利用し、静的な手法と動的な手法を組み合わせて、新しい攻撃ツール、戦術、および標的を検出し、そこから学びます。分析結果を脅威インテリジェンスのフィードと相関付けて、検出が難しいこれらのメールをユーザーがクリックする前に捕まえます。

ソーシャルメディアで詐欺者からブランドを保護する
よく似たソーシャルメディアアカウント、特に、不正な「カスタマサポート」サービスを提供するアカウントに対して警告を発するセキュリティソリューションを検討します。ソリューションによって、侵害しているアカウントを検出するだけでなく、削除サービスと連携して顧客やパートナーへの詐欺行為を阻止する必要があります。

最新の脅威インテリジェンスおよびインサイトについては、
Proofpoint Threat Insightブログ（**proofpoint.com/jp/threat-insight**）を**参照してください。**

PROOFPOINTについて

Proofpoint, Inc.（NASDAQ:PFPT）は、高度な脅威やコンプライアンス違反のリスクから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、メール、モバイルアプリ、ソーシャルメディア経由で自社のユーザーを狙う高度な標的型攻撃を阻止し、社内の機密情報を保護できるようにサイバーセキュリティの担当者をサポートします。また、問題が発生した場合に迅速に対応できるように、適切な情報とツールを提供します。Proofpointのソリューションは、Fortune 100企業の半数 以上を含む様々な規模の企業で採用されています。モバイル、ソーシャルを利用した現在のIT 環境に対応し、クラウドとビッグデータを駆使した分析で高度な脅威を阻止しています。

proofpoint.

www.proofpoint.co.jp