

はじめに

2018年上半期のセキュリティに関する重要ポイントの1つは、コンピュータシステムを完全にセキュアにすることはできず、また基盤となるハードウェアも、その上で動作するソフトウェアと同様に、悪用される可能性のある欠陥による影響を受けやすいということです。MeltdownとSpectreの2つの新たな脆弱性が、CPUを搭載したほぼすべてのデバイスに影響を及ぼし、コンピュータセキュリティ史上おそらく最悪の上半期となりました。これまでで最も深刻な脆弱性ではないとは言え、この2つの脆弱性は、今日のプロセッサのプライベートメモリの隔離方法にある欠陥につけ込むというその性質から、コンピュータエコシステム全体に打撃を与えました。修正が行われるまで、ログイン認証情報などの個人データが不正アクセスにさらされるという状態が続きました。その上、MeltdownとSpectreは発見されるまで20年にもわたって存在しており、他にも多くのバグが潜んでいることは間違いありません。

こうした騒動の中には、前向きな発見もありました。業界が総力を挙げてMeltdownとSpectreの対応に取り組んだ結果、協力とコミュニケーションにおけるポジティブな傾向が明らかになったのです。1つ目は、脆弱性がホワイトハットハッカーによって発見されたことです。Microsoft、Appleのバグバウンティプログラム（バグ発見報奨金制度）に加え、GoogleのProject Zeroなどが機能しているということに他ありません。こうした制度は、脆弱性を発見したユーザーが、その情報を一般に公開する前に、その問題を解決できる当事者に報告するよう奨励するためのものです。2つ目は、この2つの脆弱性の存在が嚴重に守られたという点です。これによりOSメーカーは、修正プログラムを開発するために必要な時間を確保することができました。競合企業同士が情報を共有し、ハードウェア問題に対するソフトウェアソリューションを開発しようと足並みを揃えて取り組みました。

しかし、この様子をサイバー犯罪者がただ指をくわえて見ているわけではありません。サイバー犯罪者は、常に新しい手法やテクニック、回避方法を取り入れることで、Emotet、TrickBot、Zeus Pandaなど他のマルウェアをより執拗で検出の難しいものへと進化させています。ランサムウェアからクリプトジャッキングに手口を切り替えているのです。ますます精巧になるフィッシング攻撃を使ったログイン情報の盗取、マルウェアのダウンロード、スパイ行為などが行われています。犯罪者がこれまで以上に有益な情報源を見つけ出すようになったことから、フィッシング攻撃もターゲットを絞ったものになりつつあります。

ウェブルートの脅威研究チームでは、2018年上半期に当社のお客様ベースから得られたデータを分析しました。この中間脅威レポートでは、統計情報をご覧いただけるだけでなく、さまざまなニュースの背景についても説明しています。ウェブルートの調査からわかることは、貴重なデータやシステムを安全に保つには、堅牢で効果の高い多層型セキュリティ対策を絶えず進化させながら実施することが、これまでにないほど重要になっているということです。

最大の脅威

マルウェア、ランサムウェア、クリプトジャッキング、ボットネットが引き続き脅威の大半を占めています。2018年1月から6月にかけて、脅威の87%はマルウェア(ランサムウェアを含む)とクリプトジャッキングで、ボットネットが12%とその後が続いています。これらの脅威について1つずつ説明し、こうした数値からわかる背景についてウェブルートの所見をご紹介します。

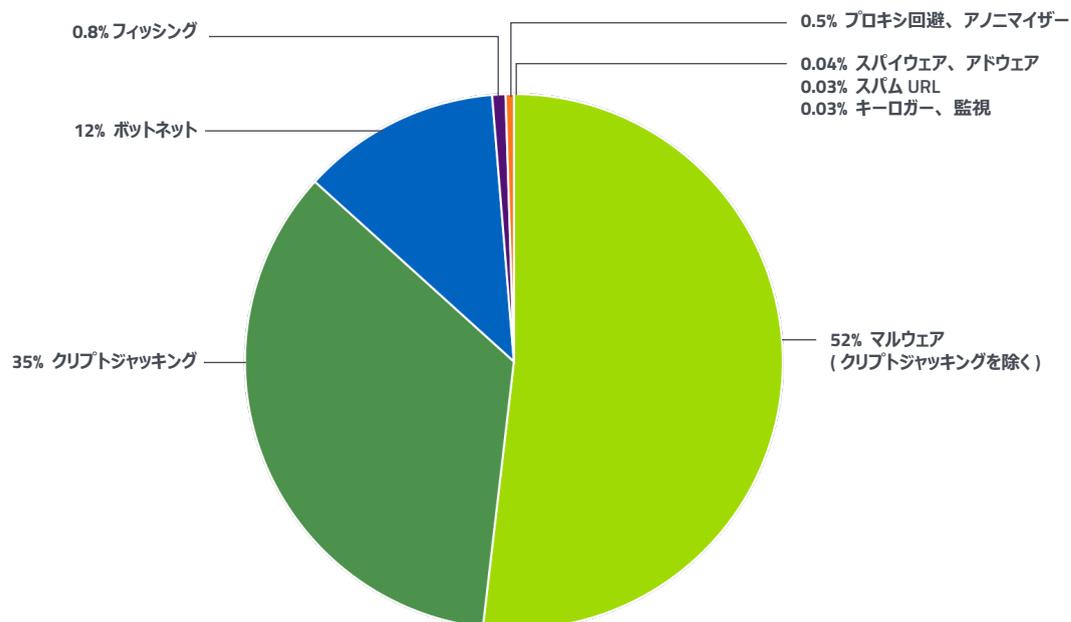


図 1: 現在の脅威情勢

ランサムウェアが新たなビジネスモデルを採用

昨年ランサムウェアは猛威を奮い、被害者たちをパニックに陥れました。多くの企業がミッションクリティカルなデータを守ろうと慌てふためきましたが、その多くは要求に屈し、暗号通貨を通じて身代金を支払うことになりました。暗号通貨自体も価値が急高騰したため、身代金の額も膨れ上がる一方でした。しかし最近では、ランサムウェア キャンペーンを成功させることの難しさに加え、以前のバージョンも保存するクラウド バックアップなどの優れたバックアップの利用が増えていることから、ランサムウェアを作成しても、データを復旧するための身代金を支払うようにユーザーを追い込むことができなくなっています。

Windows 10 に移行するユーザーが増えるにしたがって、ランサムウェアの脅威はさらに衰えつつあります。ウェブルートの調べによると、今年半ばまでに消費者の 75% と企業の 40% が、セキュリティ機能が強化されたこのオペレーティング システムに移行しています。

しかし、ランサムウェアがなくなったわけではありません。なくなったのではなく、セキュリティで保護されていないリモート デスクトップ プロトコル (RDP) 接続を攻撃経路として狙う、よりターゲットを絞ったビジネス モデルに形を変えたのです。Shodan などのツールを使うと、適切な RDP 設定を作成せず、システムを無防備な状態のままにしている多くの企業をあぶり出すことができます。高度な技術を持たないサイバー犯罪者でも、ダーク ウェブに行けば、すでにハッキング済みのマシンへの RDP アクセスを購入できます。特定のシステムにアクセスできるようになれば、そのシステムや共有ドライブ上のあらゆるデータを閲覧し、その価値を査定したり、ランサムウェアや他のマルウェアを展開したりすることが可能になります。ほんの数分でもエンドポイント保護を無効にすることができれば、悪質なペイロードを正常に実行できることを、犯罪者たちは知っています。

適切に設定されていない RDP を狙ったキャンペーンにより、SamSam Ransomware グループは、暗号通貨を通じて何百万ドルもの利益を上げ、アトランタ州とコロラド州の政府部門や医療検査大手の LabCorp を閉鎖させたことで、ニュースにも大きく取り上げられました。しかし犯罪者にとって、今や RDP 攻撃で実行可能なペイロードのオプションは 1 つだけではありません。インストールされているすべてのハードウェアを確認できるため、インストールされている CPU や GPU を使って暗号通貨を採掘すると、単純にランサムウェアに感染させるのと、どちらが儲けが大きいかを簡単に判断できるのです。

侵害から組織を守るには、適切な知識を身に付けることが重要な対策となります。多くの IT 部門が、デフォルトのポートを開きっぱなしにしたり、パスワード ポリシーを疎かにしたりなど、セキュリティの輪の中で最も脆弱な要素は従業員であるという現実を強調してしまっているのが現状です。

システムを構成し、回復性のベースラインを確立する方法に関するトレーニングは、多国籍企業にとっても従業員数 50 人の会社にとっても、同様に重要です。

クリプトマイニングがランサムウェアを退けて脅威の No.1 に

犯罪者の多くは、マルウェアを使用せずに暗号通貨から利益を得る、より簡単で速く、リスクの低い方法に移行しています。クリプトマイニングは、利益が非常に高いにもかかわらず、足がつきにくいという、あらゆるデバイスで行うことができます。コンピュータや電話だけでなく、ルーターやテレビなどの IoT デバイスにも有効です。ウェブサイト運営者の中には、目障りなバナー広告やサイドバー広告でサイト訪問者を辟易させることなく、サーバーにかかる費用を支払うための収益を簡単に得られるとして、自発的にクリプトマイニングに参加するケースもあります。しかし、その他のケースでは、ユーザーに断りなく採掘が行われています。

どちらのケースでも、採掘が行われていることはエンドユーザーにはほとんど見えておらず、電気代が多少上がったことにも気付かない可能性があります。ただし、企業となると話は別です。スケーリング(キーボードやマウスの使用時は CPU の負荷を最低限に抑えながら、使用時以外は 100% に引き上げる)が使用された場合は特に、電気代が急騰する可能性があります。

採掘に使用される電力は 6 か月ごとに倍増しており、2020 年までに全世界の消費電力の 3% はクリプトマイニングが占めることになると推定されています。

ビットコインは電力消費量が高いばかりでなく、回収した利益を浄化し、犯罪者の特定につながる足跡を難読化する必要があります。この理由から、最もよく採掘されている仮想通貨は Monero です。Monero は、どのような民生用ハードウェアでも実行することができ、匿名のブロックチェーンを持っているため、不正な利益を浄化する手間もかかりません。

マルウェアの進化

マルウェアは、2018 年上半期に確認された脅威の第 3 位に食い込んでいます。依然普及を続けているものの (2018 年の最初の 6 か月に見られたトラフィックの平均 1 % を占めているが、2017 年の 2% からの減少)、マルウェアの勢いは低下の傾向にあります。

この 50% の低下は、マルウェアを展開するよりも簡単に、リモートシステムから利益を上げる方法があることに大きく起因しています。クリプトジャッキングを行う JavaScript をホストするウェブサイトを少数のユーザーが閲覧するだけで、犯罪者は元が取れるばかりか、利益まで簡単に得ることができます。

ボットネットはマルウェアの配信方法として最も主流であり、中でも Emotet は、ウェブルートがこれまで見てきた中で最も普及率が高く、最も執拗なボットネットです。Emotet のペイロードは目覚ましい速さで配信されます。このことから、キャンペーン運用の複数のステップが自動化されていることがわかります。Emotet は、スパム ボットネットのゾンビの数を増やすことを目標とし、特に認証情報の収集にその力を集中させています。その評判と効果は非常に高く、いくつかのメジャーなマルウェア キャンペーンで配信経路として使用されているほどです。

今や Emonet には、ボットネットの中に追加の層を作成し、ボットネットの回復性を高めるオプションすらあります。最近では、被害者のルーターをコマンド&コントロール (C2) インフラのプロキシノードに変えることのできる、ユニバーサル プラグ アンド プレイ (UPnP) モジュールが開発されています。ほとんどの家庭用ルーターは、Linux ベースでアンチウイルスを備えておらず、所有者からはただの黒い箱と見なされているような状態です。そのため適切なセットアップは進んで行われておらず、便利な UPnP が悪用され、ルーターに IoT デバイスが差し込まれても誰も気付かないこととなります。

他の主要なマルウェア群を見ても、犯罪者たちがマルウェアの回復性を強化し、検出しにくく、長続きさせることに力を入れていることは明白です。セキュリティ防御に対応すべく手口を変える犯罪者たちとの戦いは、絶えずその背景が変化します。Trickbot は、レベル 1 の C2 インフラに Tor サーバーが追加されたことで、攻撃モジュールや Web インジェクションの拡散に使用されるサーバーが長期間にわたってアクティブな状態を維持できるようになりました。Zeus Panda (Panda Banker) は未だ流行を続けており、ここ数か月でさらに世界中の地域にターゲットを広げ始めています。内部の保護機構に変化を加えることで、ペイロードのリバース エンジニアリングと検出が困難な状態を維持しようとする、犯罪者たちの全体的な動きが見てとれます。

フィッシング：勢いの衰えない攻撃

フィッシングに加え、ターゲットを絞ったソーシャルエンジニアリング攻撃が増加の傾向を見せており、ウェブルートの調べによると、フィッシング攻撃は1月から6月にかけて60%以上増えています。

フィッシングは、企業ネットワークに侵入する方法として依然効果的です。1人を騙すことさえできれば、認証情報を入手してRDP攻撃を仕掛けることができます。これはランサムウェアのセクションで説明したとおりです。

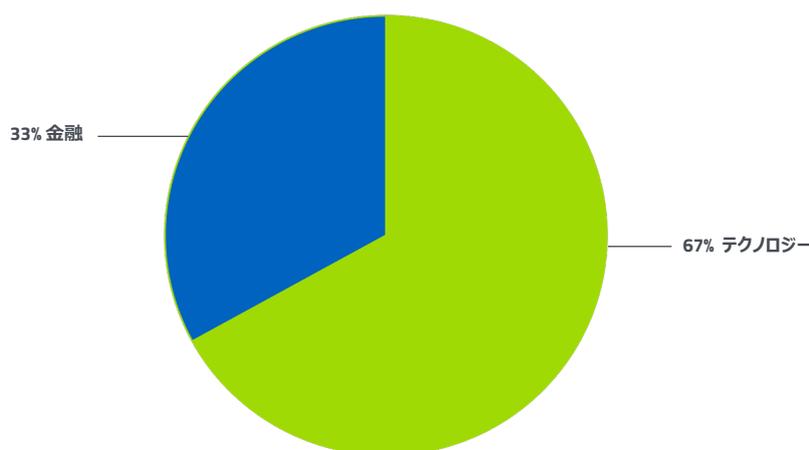


図 2: 2018 年上半期にフィッシングによる偽装被害に遭ったウェブサイト上位

犯罪者たちは、どの攻撃の成功率や利益率が高いかを知ることで、ターゲットを変え、微調整を繰り返します。過去3年のメインターゲットであった Google でしたが、2018 年上半期はその座を Dropbox (攻撃の17%) に譲っています (Google は15%)。

犯罪者があるユーザーの Gmail アカウントに侵入した場合、その報酬として、1人のユーザーのデータしか手に入らない可能性があります。しかし Dropbox の場合、個人ユーザーや企業が、税務や財務にかかわる情報や個人情報、ビジネス情報を Dropbox に保管しているため、見返りがはるかに大きい可能性があります。Dropbox の企業アカウントがますます普及するとともに、見返りも飛躍的に大きくなります。Dropbox の企業アカウントにアクセスすることができれば、暗号鍵が手に入る可能性もあります。暗号鍵があれば、膨大な量のミッションクリティカルなデータや機密性の高いデータの入手につながります。

Webroot BrightCloud® リアルタイム フィッシング対策サービスによってフィードされる Webroot SecureAnywhere® などのエンドポイントセキュリティ製品を利用することは、損害が起きる前にこうした攻撃を阻止するうえで重要な役割を果たしますが、人的要因への対処が依然として必要とされています。幸いにも、Webroot® Security Awareness Training で提供されるような、エンドユーザーを対象としたサイバーセキュリティ教育やフィッシングシミュレーションを利用することで、従業員がフィッシング攻撃をうまく回避できる可能性を高められるということがますます証明されています。

Web ベースの脅威

2018 年上半期に見られた数千万の悪質な URL は、主に 4 つのカテゴリーに分布していました。87% はマルウェア、クリプトジャッキング、ランサムウェアで、続いて 12% がボットネット、フィッシングが 1% 未満、プロキシ回避とアノニマイザーが 1% 未満という結果です。残りの 0.2% には、スパム URL、スパイウェア、アドウェア、キーロガーおよび監視が含まれています。

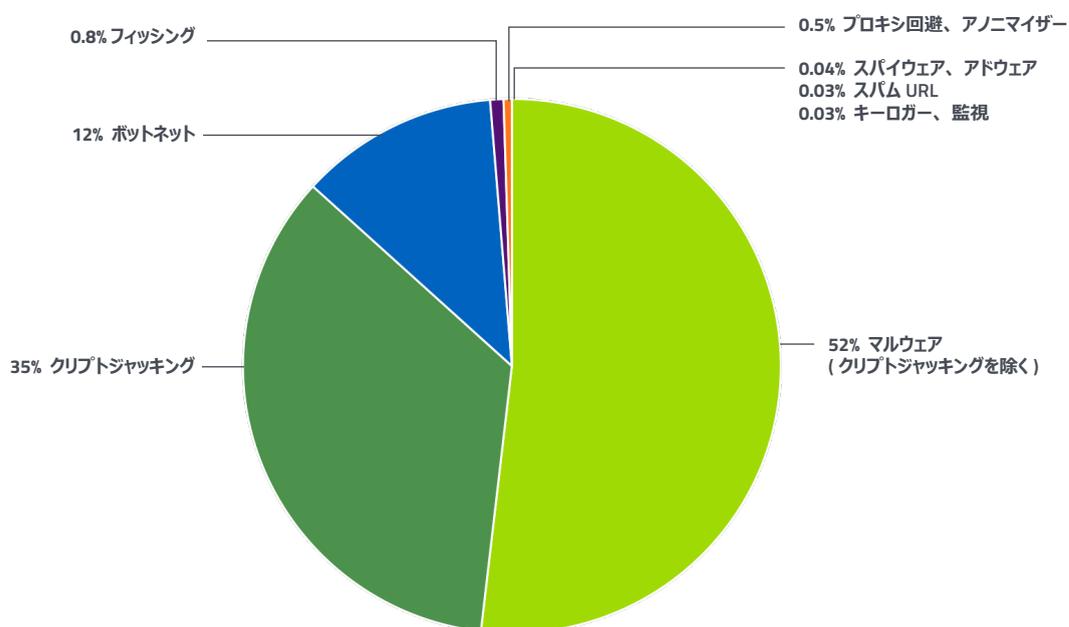


図 3: Web ベースの脅威の上位

Webroot SecureAnywhere® DNS プロテクションでは、毎日新しいフィッシングドメインやボットネットが検出されます。DNS プロテクションをご利用のお客様から得られた 2018 年 4 月から 6 月にかけての結果では、同製品によってブロックされるリスクカテゴリーの検出が数十万件にも上りました。

DNS プロテクション経由で確認されたトラフィックのおよそ 0.5% は悪質なものでした。

Web ベースの脅威をさらに詳しく見てみると、クリプトマイニングとクリプトジャッキングが一般化していることがわかります。1 日に見られる数百万件の URL リクエストのうち、お客様がクリプトマイニングの скриプトが入ったサイトを訪問したのは約 3% の確率で、こうした訪問のうち 5 件に 1 つが coinhive.com とそのサブドメイン（クリプトマイニング リレーの接続先ノード）へのアクセスでした。Coinhive の創設者は、ウェブサイトの所有者が広告を配信することなくサイトから収益を得るための正当な方法としてマイニング スクリプトを開発したと主張しています。また Coinhive は、そうした収益の 30% を手数料として受け取るという形を取っています。Coinhive のスクリプトを意図的に使用するサイト（主にポルノ、トレント、ストリーミングなどのサイト）は、採掘を行っていることを訪問者に知らせる場合もあれば、知らせない場合もあります。Coinhive はこれまで、ユーザーが承知のうえで CPU パワーの使用許可に同意するオプトイン方式のスクリプトを義務付けようと何度も試みてきましたが、ホストされている Coinhive スクリプトの圧倒的多数は、オプトインを要求していません。他のサイトでは、悪質なユーザーがサイトの所有者の知らないうちに勝手にサイトを変更し、クリプトマイニングを行うように仕組むことで、リダイレクトを Coinhive へと送り、Monero の採掘を行っている場合もあります。そうしたケースでは、アクティビティが検出されて削除されるため、下記に挙げられる主ドメインよりもカウントははるかに低くなります。

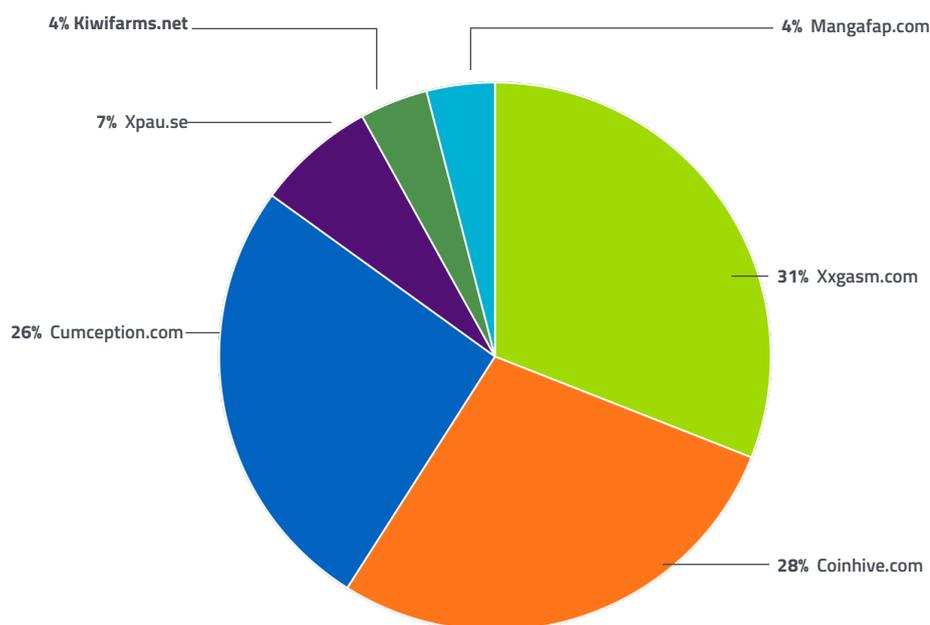


図 4: クリプトマイニングドメイン上位

セキュリティ意識向上トレーニング：戦力の増強

2018 年に見られた大量のサイバーセキュリティ脅威がもたらした前向きな結果として、従業員のセキュリティ意識が多くの組織のセキュリティ戦略にとって重要な要素になりつつあるということが挙げられます。

侵害の 93% がフィッシング攻撃から始まっており、従業員の 22% がここ 1 年間でフィッシングのリンクを少なくとも 1 つクリックしています。¹

リスクを低減するための鍵は、メールやリンクがフィッシング攻撃であると見分けるための重要なポイントに焦点を当てたトレーニングです。また従業員やデータを保護するためのセキュリティ意識向上トレーニングには、企業の罰金回避や SEC、FINRA、HIPAA、GDPR などの規制への準拠を支援するという効果もあります。

From: "microsoft@helpdesk-notification.com" <microsoft@helpdesk-notification.com>

Date: Wednesday, September 12, 2018 at 4:07 PM

To: <Recipient>

Subject: Your Microsoft Account Password Has Been Changed

Microsoft account

Your password changed

The password for the Microsoft account <recipient email> was just changed.

If it was you, then you can safely ignore this email.

If this wasn't you, your account has been compromised. Please follow these steps:

1. [Reset your password.](#)
2. Learn how to [make your account more secure.](#)

To opt out or change where you receive security notifications, [click here.](#)

Thanks,
The Microsoft account team

¹ Verizon. 「2018 年データ漏洩 / 侵害調査報告書」 (2018 年 4 月)

トレーニングを成功させるためには、従業員が会社に在籍している間、トレーニングを継続的に行う必要があります。下のグラフを見てもわかるように、2018年上半期の Webroot® セキュリティ意識向上トレーニングを利用するお客様ベースのデータでは、継続的な強化トレーニングの必要性が強調されています。

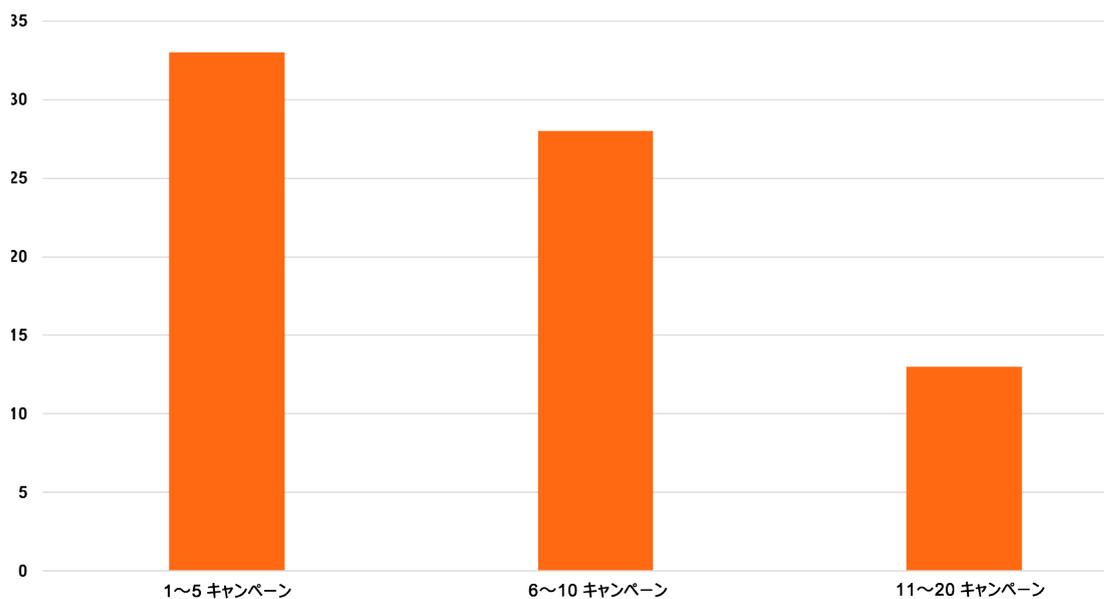


図 5: トレーニング キャンペーンを実施した回数が多いほど、フィッシングメールのクリック率が低下します。

ウェブルート独自のテストでは、セキュリティ意識向上トレーニングが行われる回数が増えるほど、従業員がリスクを見分け、回避できる可能性が高くなるといった具合に、リスクは比例して減少することがわかりました。

- 1) キャンペーンを 1 ~ 5 回実施した企業では、フィッシング クリック率は 33% でした。
- 2) キャンペーンを 6 ~ 10 回実施した企業では、クリック率が 28% まで下がりました。
- 3) キャンペーンを 11 回以上実施した企業では、クリック率が 13% まで下がりました。

さらに、フィッシング シミュレーションやキャンペーンは、内容が最新で関連性が高い場合に最も効果がありました。

まとめ

年次脅威レポートに対するこの中間アップデートでは、ウェブルートの脅威研究チームの視点から、何百万人というウェブルートのお客様が体験した傾向と変化を明らかにしています。2018 年の上半期は、マルウェア制作者が絶えず検知を回避し、感染率を高め、ターゲット市場を拡大しようと新しい手法や手順を取り入れるにつれて、脅威情勢の拡大が続きました。

重要ポイント:

- » ランサムウェア攻撃は、ブルートフォースによるスパムやフィッシング攻撃の一步先に進み、RDP の脆弱性を利用して偵察を行い、価値の高いターゲットを特定するようになりました。
- » エンドユーザーや組織を犠牲にして犯罪者に利益をもたらす、クリプトマイニングとクリプトジャッキングへの大規模なシフトが見られました。
- » フィッシングは、メインターゲットを Dropbox に変更し、引き続き勢いを増しています。
- » 企業は、フィッシングメールやその他のリスクの見分け方について、エンドユーザーを教育するためのセキュリティ意識向上トレーニングの必要性を認識し始めています。

2018 年の下半期も、サイバー犯罪者たちは、防御側の一步先を行こうと新しい手法を取り入れつづけるであろうと予想されます。これは、RDP や UPnP、または新たな扉を開く今はまだ知られていない脆弱性など、道が 1 つ塞がればまた別の道を探すという、絶え間なく続いたちごっこです。サイバー犯罪者が世界中の新しい地域を狙いを定める中で、ターゲットの拡大も予想されます。2018 年の下半期は、クリプトジャッキングの事例が増えると見込まれます。これは、サイバー犯罪者が攻撃の意図を難読化し、さらには Coinhive を完全に迂回する可能性もあるためです。

セキュリティは完璧ではありません。そしてサイバー犯罪者が活動を止めることもありません。こうした犯罪者にとって、富を得るための新しい革新的な方法を絶えず模索することは、それだけ時間と労力を費やすだけの価値があることなのです。中には悪名を馳せたいがために、こうした活動を行うハッカーも存在します。

進化し続ける脅威に立ち向かう最善にして唯一の方法は、多層型のアプローチを取り入れることです。そのためには、あらゆる脅威ベクトルを網羅し、常に最新の状態に保たれた実績のあるセキュリティ技術に加え、エンドユーザー向けの高度な意識向上トレーニングを継続的に実施していく必要があります。

本中間アップデートは、ウェブルートの年次脅威レポートの延長として作成されたものです。年次脅威レポートでは、前年の新たな脅威やサイバー犯罪の傾向を分析し、今後の見通しや予測をご紹介します。ウェブルートの年次脅威レポートは、webroot.com/2018ThreatReport でご覧いただけます。

ウェブルートについて

ウェブルートは、サイバー脅威からの企業および個人ユーザーの保護にクラウドおよび AI（人工知能）を取り入れた初めてのサイバーセキュリティ会社です。ウェブルートでは、マネージド サービス プロバイダーや中小企業のお客様に向けて、エンドポイント プロテクション、ネットワーク プロテクション、セキュリティ意識向上トレーニングなど、最高のセキュリティ ソリューションを提供しています。Webroot BrightCloud® 脅威インテリジェンス サービスは、Cisco、F5 Networks、Citrix、Aruba、Palo Alto Networks、A10 Networks などの市場をリードする企業で採用されています。機械学習の力を活用して数百万にもものぼる企業および個人ユーザーを保護することで、ウェブルートはインターネットの安全に寄与しています。ウェブルートは米国コロラド州に本社を置き、北米、ヨーロッパ、アジア地域においてグローバルなビジネスを展開しています。Smarter Cybersecurity® ソリューションについては webroot.com をご覧ください。

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com

© 2018 Webroot Inc. All rights reserved. Webroot、BrightCloud、SecureAnywhere、FlowScape、Smarter Cybersecurity は、米国およびその他の国における Webroot Inc. の商標または登録商標です。他のすべての商標はそれぞれの所有者の所有物です。REP_092018_A4