2022年
BrightCloud® 脅威レポート

BrightCloud®
Threat Intelligence

目次

予想通り、昨年はサイバー犯罪者とセキュリティ専門家の双方で新しい動きが目立ちました。

はじめに

デビッド・デュフォー (David Dufour)
エンジニアリングおよびサイバーセキュリティ担当副社長

多くのサイバーセキュリティインシデントが発生した2021年、専門家は困惑し、企業や警察、政府関係者は対応に追われました。

サプライチェーンへの攻撃は言うまでもなく、Emotetボットネットの撲滅と復活もありました。また、デバイスで検出されにくいようマルウェアが高度化したことは間違いなく、大規模なインフラ攻撃で米国やベルギーなど広い範囲に大混乱を招きました。

リモートおよびハイブリッド作業環境はこの1年間進化を続けており、私たちの働き方や人との関わり方はさらに変わっていくでしょう。こうした新しい現実により、悪意のある人物がより簡単に多くの収益を得る手段は広がりましたが、電子メール、テキストメッセージ、その他の通信プラットフォームでのフィッシング攻撃が侵入の最初のステップであることは変わりありません。

悪意のあるURLが急増しています。ブラウザーベースのクリプトジャッキングは事実上見られなくなった代わりに、クリプトマイニングマルウェアが主流になりつつあります。サイバー犯罪者は、私たちのデータや個人情報を脅かす手口を次々と考え出します。

サイバー犯罪者が組織を危険にさらすためのステルスアプローチを前進させる中、サイバーセキュリティアナリストと脅威研究者はリスクの特定と拡散防止を続けました。極めて困難な課題となることもありますが、どの業界や分野でも取り組み続けるしかありません。

個人や企業がサイバー犯罪から完全に解放されることはありえません。中堅・中小企業(SMB)は、ランサムウェア攻撃に対して特に脆弱なままです。ランサムウェアの支払いが2021年に急増し、REvilなどのランサムウェア攻撃集団の活動を阻止すべく各国が団結しましたが、Apple、Microsoft、Googleといった一流企業は、疑いを持たないユーザーを誘うための餌としてフィッシングに引き続き利用され、製造業は攻撃の主要な標的であり続けています。

今年のBrightCloud® 脅威レポートでは、大小の企業に影響を与えている新しい事実と、そうした変化が企業と個人にとって何を意味するのかを考察し、詳細な分析を通じて今年の展望、傾向分析、予測を提供します。

本稿が対策と復旧戦略の策定、さらには将来の安全確保に役立つことを願っています。

脅威インテリジェンスの概要

『2022年BrightCloud® 脅威レポート』で示された脅威インテリジェンス、傾向と詳細は、BrightCloud® プラットフォームにより継続的かつ自動的に取り込まれたデータに基づいています。BrightCloud® プラットフォームは、すべてのWebroot保護とBrightCloudサービスを強化する独自のマシンラーニングベースのアーキテクチャです。このデータは、9,500万を超える実世界のエンドポイントとセンサー、特殊なサードパーティデータベース、およびテクノロジーパートナーによって保護されているエンドユーザーからのインテリジェンスから取得されます。当社の脅威研究チームは、高度なマシンラーニングとAIの技術を使用してデータを分析および解釈します。

本稿では、さまざまな脅威の活動の分析と観察した傾向についての洞察を提供した上で、業界、地域、企業、人々など広範囲にわたる影響について説明し、来る年に脅威の専門家が期待することを明らかにします。

9,500万+

実世界センサー

7,800万+

テクノロジーパートナーを通じて保護されたエンドユーザー

10億+

分類されたドメイン

430億+

評価対象のURL

43億9,000万+

IP – すべてのIPv4と使用中のIPv6

380億+

ファイル動作記録

3,700万+

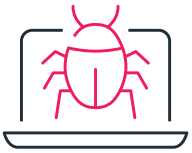
アクティブなモバイルアプリ

マルウェア

Webrootで保護されたWindowsエンドポイントに到達するマルウェアファイルの数は、2020年から2021年にかけて58%減少しました。信じられないほどの変化です。本稿の各セクションでは、Emotet、DarkSide、REvilの活動停止、Windows 7から新しいWindowsバージョンへの継続的な移行、BrightCloudテクノロジーによるアップストリームマルウェア検出機能の強化など、この大幅な減少をもたらしたいくつかの要因について見ていきます。

減少のもう1つの大きな要因は攻撃者の行動です。彼らは、独自のマルウェアアプリケーションをエンドポイントに転送するのではなく、Living off the Land Binaries(環境寄生バイナリ、通称「LOLBins」)を使用し、エンドポイントに既存の無害なアプリケーションを使用して検出を回避することが増えています。とはいえ、マルウェアがもはや大きな脅威ではないと思ってはいけません。2021年、Webrootで保護されたWindowsエンドポイントでは、1日あたり平均100万を超える新しいマルウェアとWindowsアプリケーションファイルが見つかりました。

世界で1台のPCでしか検出されないWindowsマルウェアの割合も追跡したところ、今年はマルウェアの86.3%が1台のPCにしか存在しないユニークなものでした。2020年の86.1%、2019年の86.2%とほぼ変わっていないことから、攻撃者が検出を回避するために一貫して使用されてきた手法と言えます。



今年は、マルウェアの86.3%が1台のPCにしか存在しないユニークなものでした。

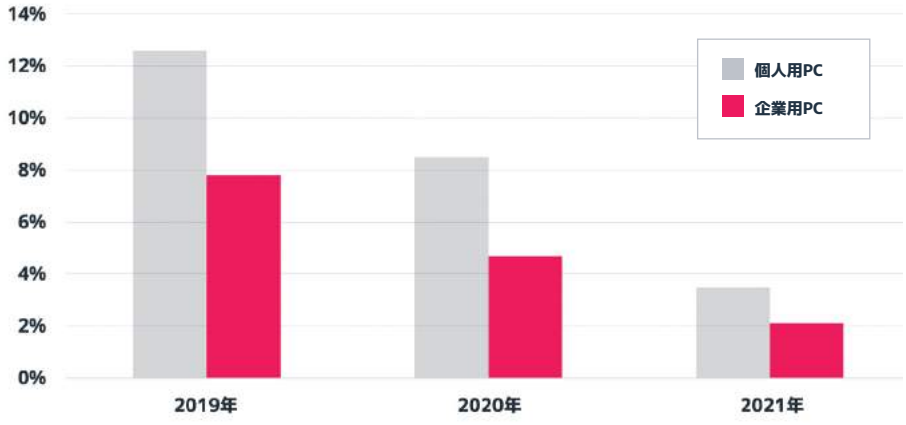
また、エンドポイントごとのテレメトリでアンチウイルステクノロジーを使用することの重要性も明らかです。

感染した個人および企業用PC

近年続いているもう1つの傾向は、個人および企業用PCの感染率の低下でした。2019年には、個人用PCの12.6%と企業用PCの7.8%が1回以上のマルウェア感染を経験しましたが、2020年には、感染率は個人用PCで8.5%、企業用PCで4.7%に低下。2021年にはさらに急激に下がり、個人用PCは3.5%、企業用PCは2.1%になりました。

感染率の低下は前向きな動きですが、個人用PCの感染率は依然として企業用PCのほぼ2倍です。つまり、企業は個人用PCを業務に使用しているリモートワーカーを保護する必要に迫られているということです。

感染減少の理由の1つは、多層防御の浸透です。より多くの防止策が講じられるようになり、エンドポイントに到達するマルウェアは減りました。もう1つの大きな理由は、Windows 7からWindows 10およびWindows 11への継続的な移行です。これらの新しいバージョンではセキュリティ機能が強化されているため、感染の可能性が低くなっています。



図表1:企業用および個人用PCの感染率

脅威への認識が広まるにつれ、組織化されたサイバー犯罪に対するより積極的かつ攻撃的な対策が具体化しつつあります。

感染率の調査に加え、再感染率、つまり1年間にPCが感染した回数も調べました。感染した個人用PCのうち、53%が2回以上、19%が6回以上感染。感染した企業用PCのうち、45%が2回以上、12%が6回以上感染しました。これらの割合は2020年とほぼ同じです。こうした再感染率から、特に侵入発生後のユーザー教育が重要であることがわかります。

感染した個人用PCに占める割合

53%が2回以上感染

19%が6回以上感染

ライセンス数別の感染率

今年のレポートでは、ライセンスが付与された企業用PCの台数別に感染率の分析を新たに行いました。ライセンス付与されたPCが20台以下の小規模組織では、今年いずれかのPCで感染を経験した割合は8.3%にとどまり、感染台数は平均6台でした。中規模組織(ライセンス付与されたPCが21～100台)を見ると、感染率は一気に34.1%に増え、感染台数は平均9台になりました。ライセンス付与されたPCが101～500台の組織では感染率がさらに上がり65.1%、500台を超える組織では89.7%でした。ご想像のとおり、企業の規模が大きくなるほど、感染のリスクは高まります。

PCのライセンス数に基づく企業規模	感染した企業の割合	感染した企業ごとの平均感染回数
1～20: 小規模	8.3%	6
21～100: 中規模	34.1%	9
101～500: 大規模	65.1%	23
501～: 超大規模	89.7%	86

図表2:企業規模別のPC感染率

さらに見逃せないのは、規模の小さい企業と大きい企業に対する感染の相対的な影響の違いです。小規模企業が感染を経験すると、通常、社内の感染PC台数の割合は大企業の場合よりはるかに大きくなります。小規模企業の感染率はるかに低いにもかかわらず、感染の影響はより大きくなる可能性があるのです。小規模企業は、IT専門家や高度な訓練を受けたサイバーセキュリティの専門家がいないことから、脆弱な立場に置かれています。

Windows 7とWindows 10

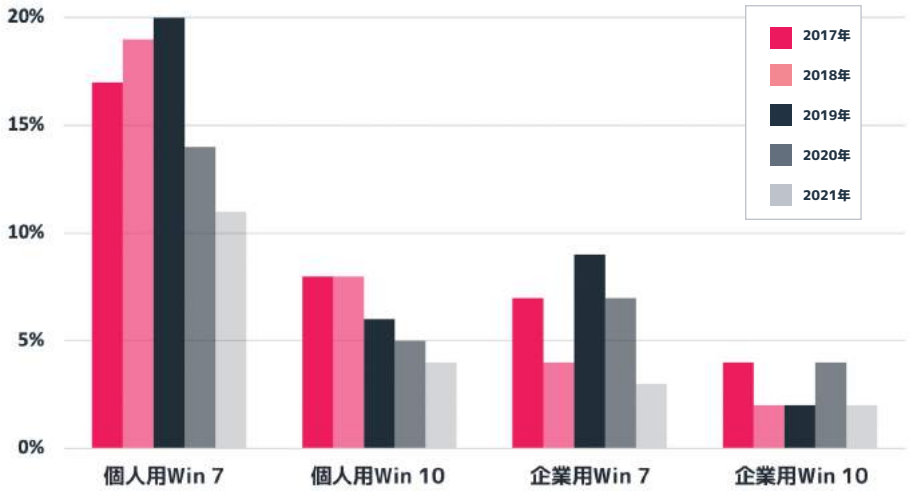
当社ではWindows 7およびWindows 10 PCの感染率を数年間監視してきましたが、Windows 7の感染率は一貫してWindows 10よりもかなり高く、その傾向は今年も続いています。2021年の感染率は、Windows 7 PCが1台あたり0.06回であったのに対し、Windows 10 PCは平均わずか0.03回とWindows 7の半分でした。

使用されているWindows 7デバイス数の減少に伴い、Windows 7に関連する感染の数は今後減り続けるはずです。Microsoftは、Windows 7のサポートが終了した2020年の初めに、Windows 7のパッチのリリースを終了しました。

当時、すべてのPCの約16%でまだWindows 7が稼働されていましたが、2021年の終わりには5%に急落し、Windows 10の使用率が86%になりました。Windows 11も利用され始めているため、Windows 7の数はさらに減少すると思われます。

個人用PCと企業用PCを区別すると、Windows 7とWindows 10の間にはさらに劇的な違いが見られました。まず、企業用PCはWindows 7からの移行において個人用PCに遅れをとっており、2021年末時点で、依然としてWindows 7を使用している割合は、企業用PCの6%に対し個人用PCはわずか4%でした。一方、圧倒的に多くのユーザーが使用するWindows 10は、個人用PCの88%で実行されているのに対し企業用PCでは84%でした。

また、個人用PCは企業用PCよりも感染率がはるかに高いこともわかりました。Windows 7を実行しているPCの感染は、個人用PCでは1台あたり0.11回あり、企業用PCの0.03回の3倍を上回っています。Windows 10の場合は、個人用PCと企業用PCの違いはそれほど顕著ではなく、それぞれ0.04回と0.02回です。



図表3:企業用および個人用PCでのOS別感染率

それでも、感染率は総じて数年前よりも大幅に改善されています。これらの調査結果は、マルウェアからのエンドポイントの保護が改善されたことを示していますが、個人用PCが企業用PCよりも今なおはるかに大きなリスクにさらされていることは明らかです。

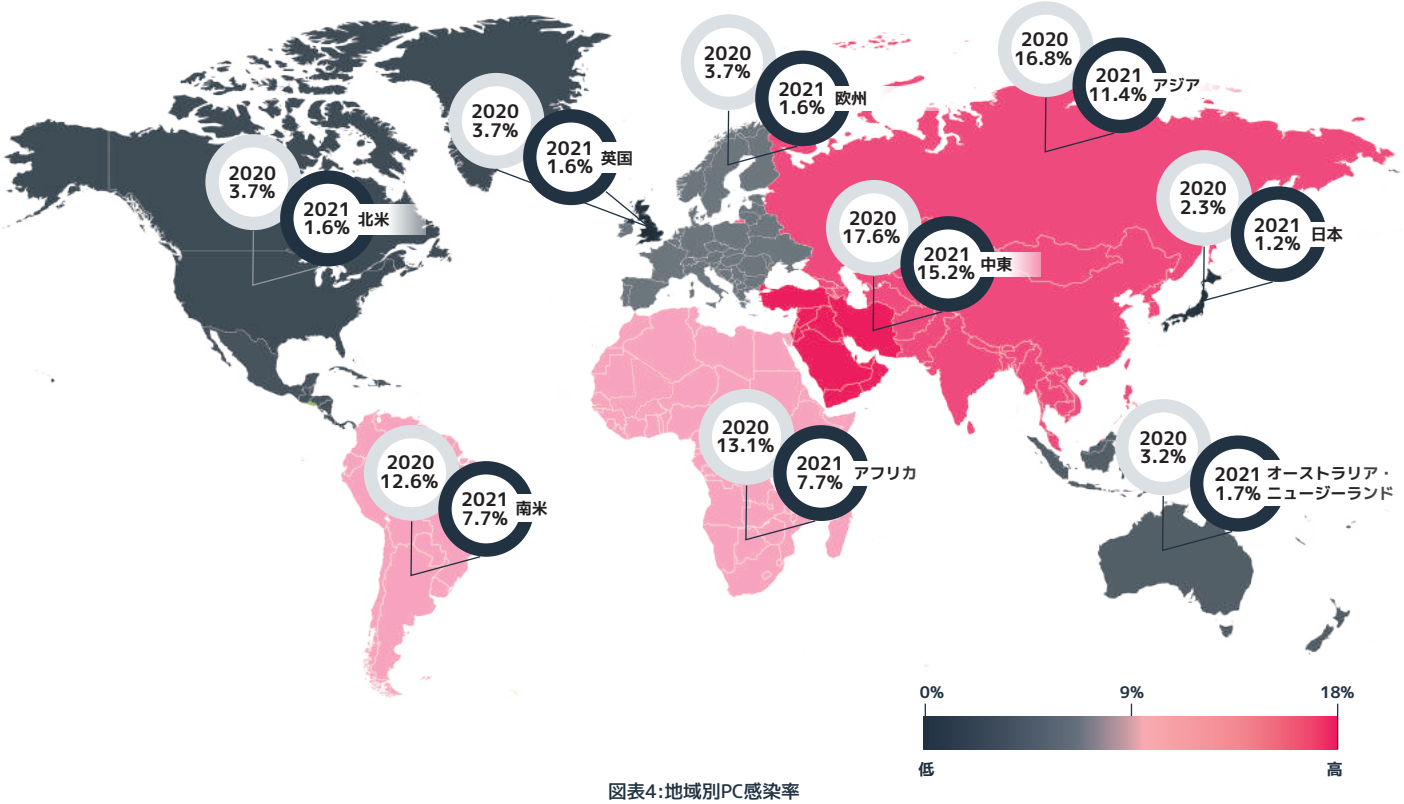
地域別感染率

Windows 10およびWindows 7 PCの感染率は、世界のどこにPCがあるかによっても大きく異なります。感染率を地域ごとに分けると、地域間の差異がわかります。日本と英国のWindows PCの感染率は中東の10分の1未満です。この差は、日本の感染率が中東の約7分の1であった2020年から拡大しています。

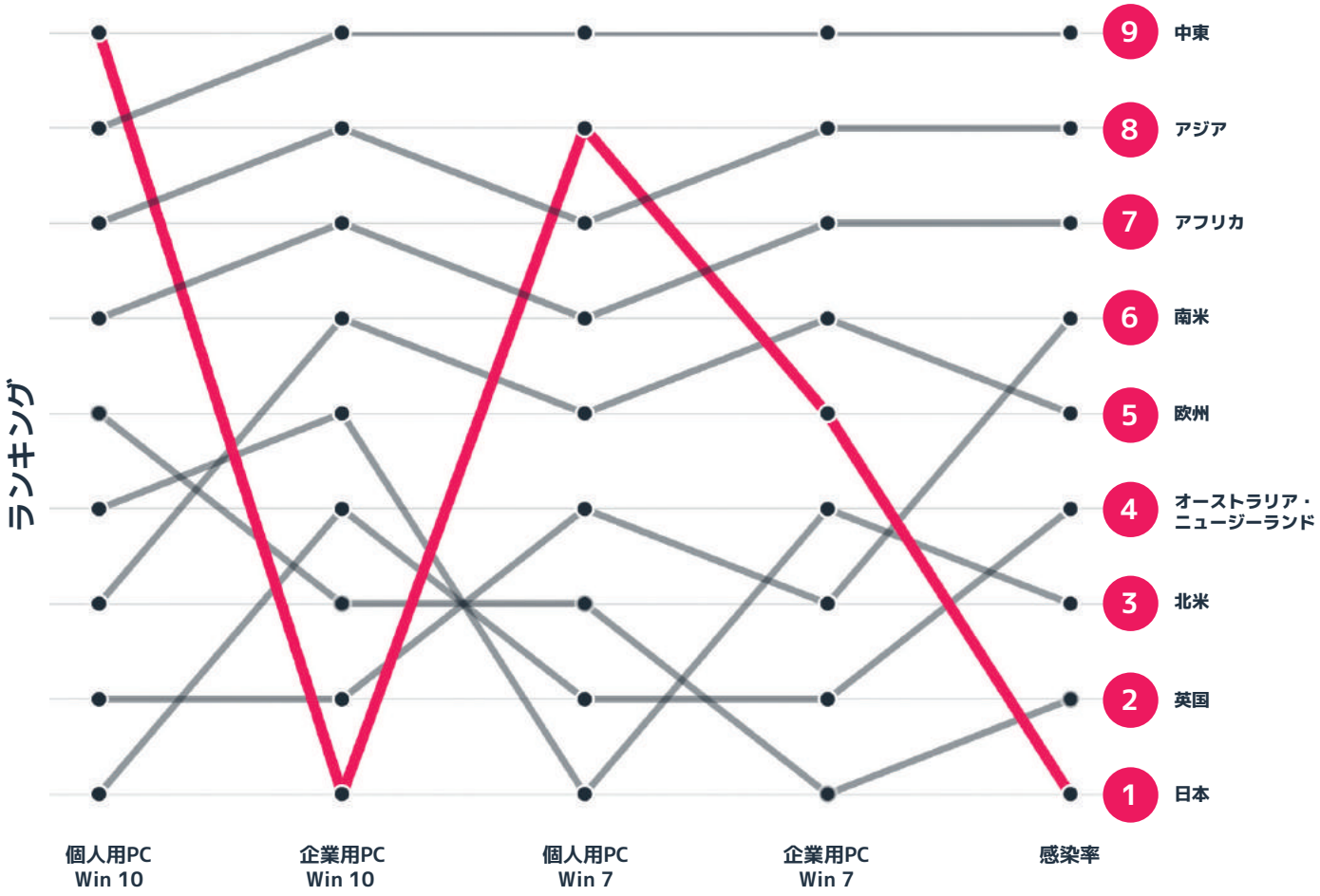
感染率が最も低い4つの地域(日本、英国、北米、オーストラリア・ニュージーランド)では、2020年から2021年にかけて平均51%下がり、4地域全体で1.4%になりました。一方、他の地域では、前年比で33%の減少にとどまり、平均9.2%になりました。

これらの感染率をWindows 7とWindows 10で区別すると、話はやや複雑になります。感染率が最も高い5つの地域では、個人用PCの16.7%と企業用PCの14.3%で今もWindows 7が実行されていますが、日本では、個人用PCの21.7%と企業用PCの9.2%でWindows 7が実行されているにもかかわらず感染率は1.2%でした。つまり、Windows 7 PCの割合が高い地域では感染率が高くなる傾向がある中、日本は明らかな例外です。

世界全体では、Windows 10の導入は2020年から2021年に11.2%増加しました。北米を除くすべての地域では9%以上増加したのに対し、北米では増加が比較的緩やかでした。さらに目を引くのは、全地域でのWindows 7からの大規模な移行です。下は中東の23.5%、アジアの26.5%から、上は北米の49.0%、英国の50.1%まで、Windows 7の減少が見られます。

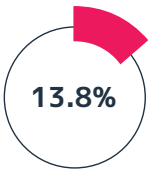


図表4:地域別PC感染率

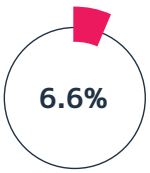


図表5:個人用/企業用PCでのWindows 7/10の導入および感染率のランキング

Windows 10の使用増加



世界中の企業用PC



世界中の個人用PC

昨年のWindows 7からWindows 10への移行は、ほとんどの地域で、主に企業用PCによるものでした。

Windows 10の使用増加は、企業用PCでは世界全体で13.8%でしたが、個人用PCでは6.6%にとどまりました。同様に、Windows 7の使用減少も主に企業用PCによるもので、前年比で42.1%減少しました。個人用PCでの減少は29.3%とやや控えめでした。

別の角度でデータを見るために、個人用および企業用PCでのWindows 7とWindows 10の導入ならびに感染率の観点から9つの地域を1 (最高)から9 (最低)にランク付けしました。地域ごとにデータをランク付けすると、日本と世界の他の地域との違いがわかります。日本は、企業用PCでのWindows 10の導入は1位ですが、個人用PCでのWindows 10の導入は最下位となっています。

Windows 7の使用については、企業用PCでは全地域の中間、個人用PCでは下から2番目に位置しています。ただどういうわけか、感染率は最も低くなっています。ほとんどの国では、感染率を含め、カテゴリによるランキングの差はそれほど大きくありません。

感染率の地域差の要因としては、マルウェアがエンドポイントに到達するのを防ぐ多層防御の効果や、ソーシャルエンジニアリング攻撃によってユーザーのPCが知らないうちに感染するのを防ぐためのセキュリティ意識向上のためのトレーニングの効果などが考えられます。

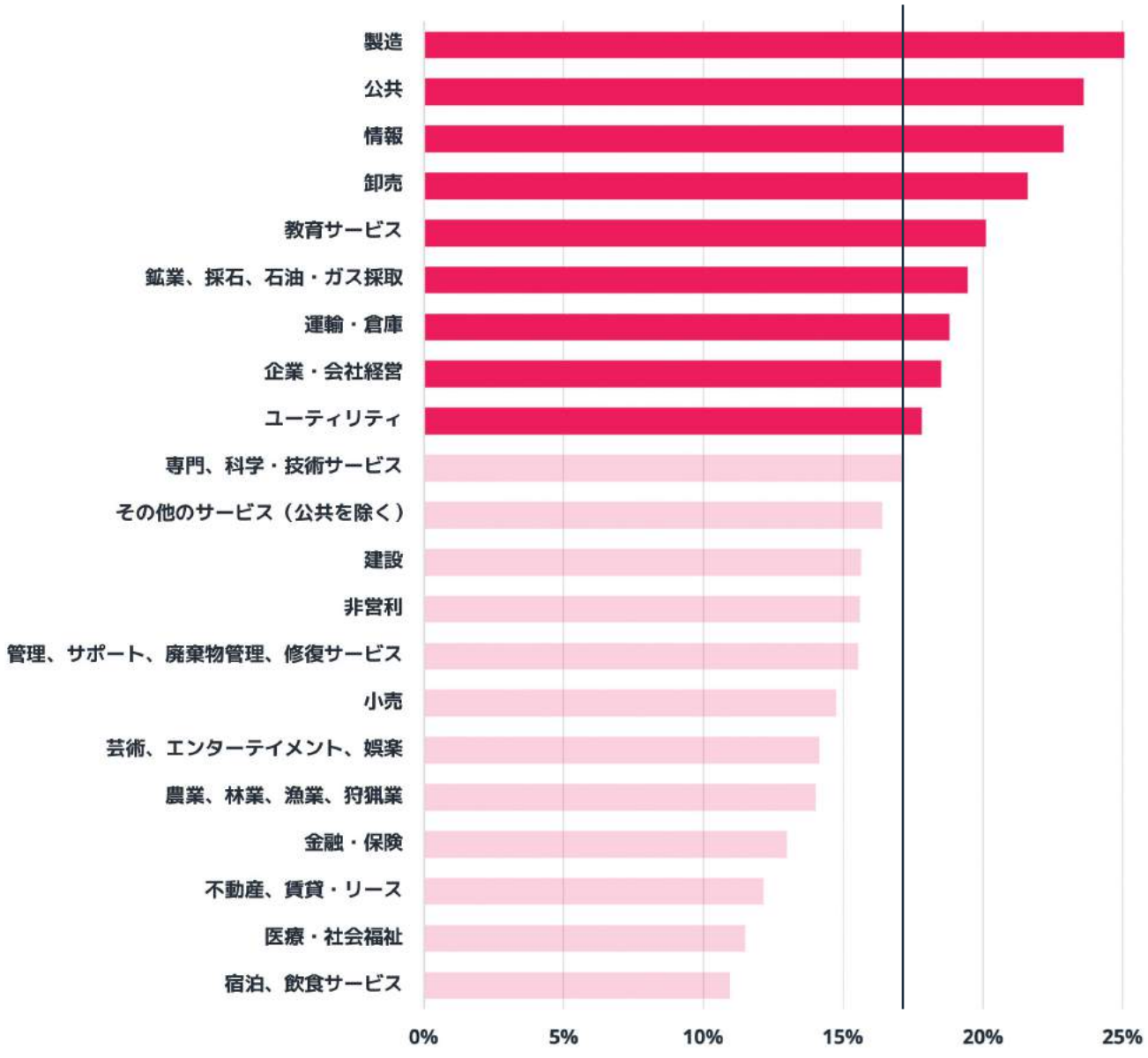
業種別感染率

当社はビジネス顧客の40%近くから業種に関するデータの提供を受けています。図表6は、昨年1回以上感染した企業の平均割合を業種別に示しています。グレーの直線は、これらの業種全体の平均感染率(16.8%)を示しています。このデータによると、感染率上位の業種は、製造(平均より54%上)、公共(同41%上)、情報(同37%上)となっており、卸売と教育サービスがそれに続きます。これら5業種のうち4業種は、2020年のトップ5にも含まれていました。

これらの数字は毎年変化しており、前年が3位であった製造業が今年最も感染率の高い業種となったことは驚くに値しません。2022年にはメーカーを標的とした攻撃が増えると予想されます。メーカーはサプライチェーンの混乱を回避するために身代金の支払いをいとわない可能性があるためです。

信頼できるソフトウェアサプライチェーンに対する攻撃は、間違いなく2021年の最大のサイバーセキュリティインシデントでした。SolarWinds、Kaseya、Log4jなどが被害を受け、世界中で話題になりました。こうした攻撃は、一度侵入すればソフトウェアが勝手に数千、数百万のシステムに送信されることから、サイバー犯罪者に好んで用いられます。製品やサービスにサードパーティソフトウェアが含まれる多くの企業では、サードパーティソフトウェアが引き続き攻撃者の標的にされることが予想されます。

感染率が低い方を見ると、宿泊・飲食サービス(平均より35%下)、医療・社会福祉(31%下)、不動産・賃貸・リース(27%下)、金融・保険(22%下)、農業、林業、漁業、狩猟業(16%下)などの業種が平均を大きく下回りました。



図表6:業界別の感染率と平均からの偏差

マルウェアが隠れる場所

当社はWindowsマルウェアが隠れている場所を追跡しています。マルウェアが潜む可能性のある場所はたくさんありますが、一部の場所がよく使用される傾向にあります。マルウェアがアクセスでき、他の多くのアプリケーションやファイルが格納されている場所です。

2020年には、マルウェア感染の83%が%temp% (28.4%)、%appdata% (26.1%)、%cache% (19.7%)、%desktop% (9.0%)の4つのパスのいずれかを使用していました。2021年も似通っており、感染の83%が同じ4つのパスを使用していますが、%temp% (33%増加して37.8%に)および%desktop% (40%増加して12.6%に)の使用が大きく増え、%appdata% (46%減少して14.2%に)の使用は減りました。%cache% (5%減少して18.7%に)は他と比較してあまり変化が見られませんでした。

また、個人用PCと企業用PCではマルウェアの隠れ場所に大きな違いが見られました。個人用PCで上位を占めるのは、%temp% (33.8%)、%cache% (21.9%)、%desktop% (15.0%)、%appdata% (12.5%)の4カ所です。全Windows PCでも上位は同じ4つで、割合も同様です。2020年との特筆すべき違いは、%desktop%が使用されることがかなり多くなり、%appdata%の使用が急激に減ったことです。

企業用PCでは個人用PCと少し異なり、上位は%temp% (50.9%)、%appdata% (19.7%)、%cache% (8.4%)、%windir% (5.6%)の4つが占めています。

企業用PCでは、マルウェアが隠れる可能性のあるすべての場所のうち、%temp%の使用時間が半分を超えていることになります。

2020年には企業用PCのマルウェアによる%temp%の使用率は21.7%であったことから、これは大きな変化です。2020年の1位の場所は%appdata% (41.0%)でしたが、こちらは1年間で半分以上減少しています。興味深いことに、2019年の%temp%と%appdata%の割合は、2021年の数値にかなり近く、2021年はそれぞれ54.4%と16.7%でした。

スポットライト:Cobalt Strike

2021年に注目を集めた攻撃はすべてCobalt Strikeを利用していたようです。Cobalt Strikeは元来、ホワイトハッカーとレッドチームと呼ばれる脆弱性診断チームが侵入テストに使用するためのものでした。極めて高度なハッキングツールが単一のパッケージに統合されており、使いやすく、必要な技術的知識のレベルも他の多くのツールほど高くありません。それらのハッキングツールは、Cobalt Strike自体を隠しながら脆弱性を特定し、横方向に広がって、特権エスカレーションや暗証番号とハッシュの収集を実行するように設計されています。また、侵入したシステム内に痕跡をほとんど、またはまったく残しません。

こうした魅力的な特性を持つCobalt Strikeを攻撃者が利用しないわけがありません。Cobalt Strikeを改造して利用できるようにし、アフィリエイトに販売するために独自のバージョンを作成した攻撃者は、2021年にそれらのバージョンの強化に力を注ぎ、2021年半ばには、Linuxポートまで発見されました。

攻撃者は特にエンドポイントへのリモートアクセスと制御、ランサムウェアの配布と制御、コマンドおよび制御機能を必要とするその他の行動の実行にCobalt Strikeを好んで使用します。2022年もCobalt Strikeは攻撃者に多用されると考えて間違いありません。

「今年は感染率の改善が見られるとはいえ、個人用PCの感染率が企業用PCより高いことに変わりはありません。Windows 11の導入にともない、攻撃者はこれまでにない新機能を活用する斬新かつ危険なエクスプロイトを躊躇なく実行することでしょう。」

グレイソン・メルボルン(Grayson Milbourne)、
セキュリティインテリジェンスディレクター

ランサムウェア

ランサムウェアは、今なお中堅・中小企業にとって最大のサイバー脅威です。中堅・中小企業の感染要因は、トップがリモートデスクトッププロトコル(RDP)、続いて電子メールフィッシングとなっています。2021年には、ランサムウェア攻撃の82%が従業員数1,000人未満の組織を標的にし、従業員が100人以下の小規模組織は、ランサムウェアの被害者の44%を占めていました。また、すべてのランサムウェア攻撃の84%にデータ侵害の脅威が含まれており、前年からわずかに増加しています。[i]

2021年、ほとんどのランサムウェア攻撃で、多くのコンピューターが使用不能になり機密データが盗まれ、期限内に暗号通貨の身代金を支払わない限りデータを開示すると組織が脅迫を受けました。RaaS (サービスとしてのランサムウェア)モデルが一般的になる前であれば、組織はデータを復元し、身代金の支払いを回避することができました。

今、被害組織はより厳しい選択を迫られます。身代金の支払いを拒否して修復に集中するか、身代金を支払って攻撃者が約束を守ることを祈るかです。また、攻撃者が約束を守った場合に、データプライバシー法に従って、攻撃者によるデータアクセス時に発生していたデータ侵害を開示するかどうかも選択することになります。

攻撃者側も、標的とする組織をより入念に選択するようになりつつあります。中堅・中小企業にとっては迷惑な話です。攻撃者は、Colonial Pipelineのような有名企業をあえて狙おうとはしません。そのような攻撃は、阻止され逮捕されて終わるからです。[ii]

そのため、リスクが少ない小規模な組織を狙うことが増えています。また、攻撃者が要求し手にする身代金の金額も上がる一方です。[iii] 身代金金額の増加は、米ドルの価値の下落や、EU一般データ保護規則(GDPR)違反に対する罰金の引き上げが原因と考えられます。

2022年に何が起こるかは誰にもわかりません。ランサムウェア攻撃集団の起訴が進み、最終的にフィッシングの減少につながるのでしょうか。

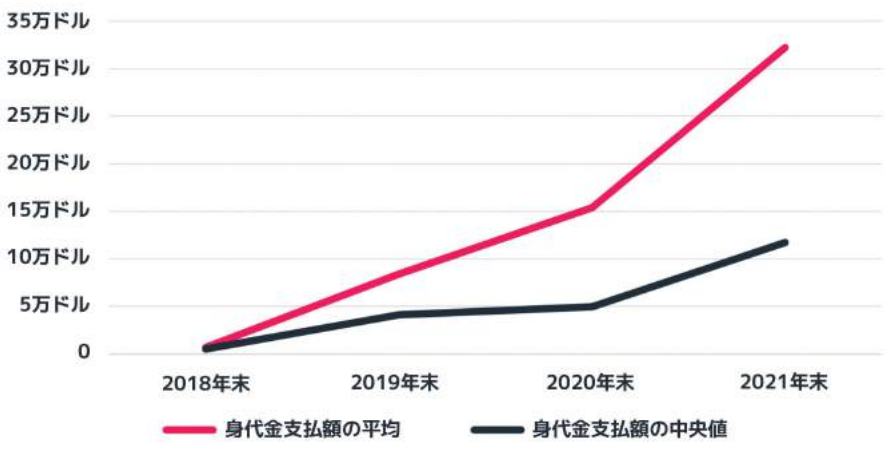
それともランサムウェア攻撃集団が、さらに高い身代金の支払いをターゲットに強要するための斬新な方法を思い付くでしょうか。

2021年の傾向と、これが1年先に何を意味するかを詳しく見てみましょう。

身代金金額の上昇

2021年、身代金の平均支払い額は、これまでにない驚くべき速度で増加しました。2018年末の時点で、身代金の平均支払い額はわずか6,733ドルでした。[iv] 1年後、それは84,116ドルになり、[v] 2020年の終わりには、平均154,108ドルになりました。[vi] 1年あたり約73,500ドル増えたことになります。2021年末の平均は、2020年の平均の2倍以上になり、322,168ドルに達しました。

身代金金額の中央値も2020年以降2倍以上になり、49,450ドルから117,116ドルに増加しています。[vii] この数年間の傾向とインフレを考え合わせると、2022年も身代金金額は増加し続けると予想されます。



図表7:通年の身代金支払額の平均および中央値

2021年に発生した最大級の身代金要求の例

7,000万ドルの身代金

注目を集めるサプライチェーン攻撃で、REvilランサムウェア攻撃集団がKaseyaのIT管理ソフトウェアに侵入。そのソフトウェアを使用している企業だけでなく、その顧客である推定800～1,500社の中堅・中小企業にも感染を広げました。REvilは身代金として7,000万ドルを要求しました。[viii]

5,000万ドルの身代金

Quanta ComputerもREvilの標的になりました。REvilは、QuantaがApple向けに製造したコンピューターコンポーネントの設計図を盗んだと主張し、その証拠としていくつかのファイルを公開しました。彼らは5,000万ドルの身代金をQuantaではなくAppleに要求し、Appleが数日のうちに支払いに応じなかった場合、身代金を1億ドルに増額すると言いました。[IX]

4,000万ドルの身代金

CNA Financialは、Phoenixランサムウェアに感染し、CNAのウェブサイト、電子メール、その他のシステムが停止しただけでなく、従業員と顧客に関する大量の機密情報が漏洩しました。2週間の復旧作業の後、CNAは、システムとデータへのアクセス復元のために4,000万ドルの身代金を支払うことを決めました。[X]

当然のことながら、保険会社はサイバー保険の料率を引き上げつつあります。また、サイバー保険の加入条件を厳しくしています。たとえば、一連の技術的管理の実施を要求する場合があります。このような管理は複雑でコストがかかるため、中堅・中小企業にとっては特に難しい場合があります。[xi]

その結果、多くの組織は、ランサムウェア攻撃に対するレジリエンスを高めるために、サイバー保険への依存から多層防御の強化へと移行しています。

ランサムウェア攻撃集団

2021年は、警察がランサムウェア攻撃集団に反撃を開始した年でした。2022年の初めには、ロシア当局はREvilという攻撃集団のメンバーを逮捕し、彼らのコンピューターなどの資産を押収しました。[xii]

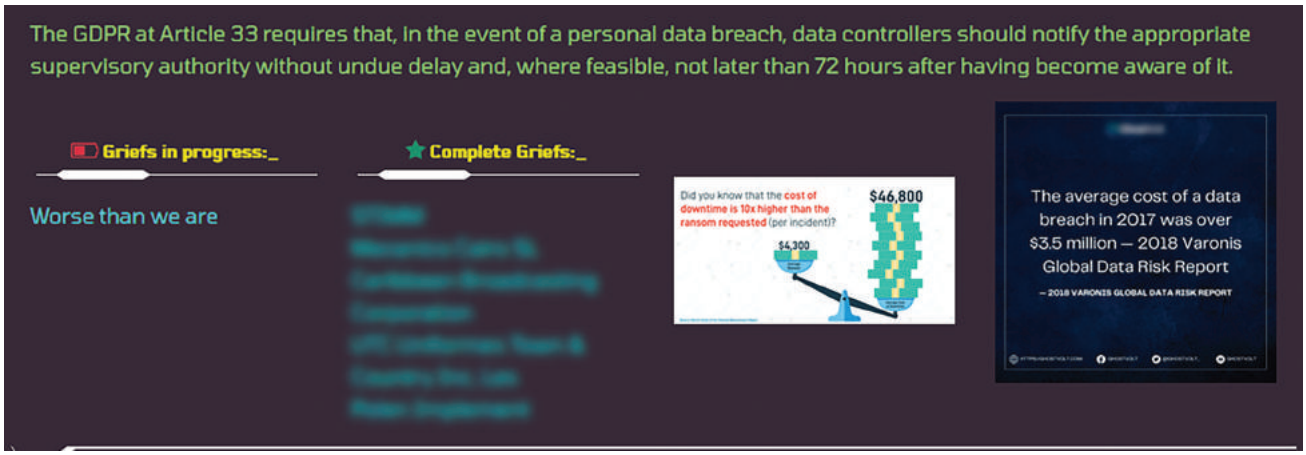
これは、米国とロシアの当局間の前例のない協力や、アフィリエイトではなくランサムウェア攻撃集団のメンバーが逮捕されるなど、いくつかの理由で注目に値します。ランサムウェア攻撃集団を逮捕、起訴、収監するための警察の力が高まり、2022年のREvilの押さえ込みに向け明るい兆しが見えています。

これは朗報です。ただ残念ながら、RaaSビジネスモデルは勢いを保っています。DarkSideやREvilなどのランサムウェア攻撃集団はいったん活動を停止しましたが、後日縮小したり名前を変えたりして再度姿を現しました。ランサムウェアから得られる収益は非常に大きいことから、捕まる危険を承知で儲けようとする人が後を絶ちません。RaaSモデルは、ランサムウェア攻撃集団を首謀するランサムウェアの作成者やリーダーのリスクも軽減します。そうした個人はまだ逮捕や起訴に至っておらず、捕まるのはランサムウェアの配布者とアフィリエイトだけです。

とはいえ希望はあります。2021年11月に米国務省がDarkSideランサムウェア攻撃集団の首謀者に関する情報に対して最大1,000万ドルの報奨金を提供すると発表したのです。[xiii]

ランサムウェア攻撃集団の側も、身代金の支払いを強要するための新しい戦術を使用しています。たとえば、盗まれたデータに個人情報が含まれている場合、組織はそれを報告し、GDPRおよびその他の法規制に基づいて罰金の支払いを求められる場合があるのですが、ランサムウェア攻撃集団は、被害者への恐喝戦術でこれを利用し、身代金を支払わないと、GDPR違反者のリストに加えられ評判が損なわれると伝えます。つまり、GDPRは、組織にセキュリティ対策の改善を促す仕組みではなく、組織に身代金の支払いを促すために利用されているのです。

被害者が身代金を支払うと、攻撃者はランサムウェアを使い続け、身代金の要求を引き上げるようになります。多くの公的機関は、支払われる身代金の数を減らすために、組織にすべてのランサムウェアの支払いを開示するように要求するか、身代金の支払いを違法にする必要に迫られています。そうすれば、ランサムウェアの収益性は低下し、ランサムウェア活動は減速するでしょう。[xiv]



これは「Grief」としてリブランドしたランサムウェアグループ(別名Doppelpaymer/BitPaymer)のダークウェブ上の恐喝ページです。
GDPRコードとマーケティング資料を使用して、侵入を内密にするためにお金を払うよう圧力をかけています

ただし、たとえ身代金の支払いが違法になっても、一部の組織が早期復旧と悪評回避のため身代金を支払うことは避けられないと思われます。公的機関がそのような法律違反を特定するのは非常に困難です。

公的機関もサイバーセキュリティ情報共有の改善に取り組んでいます。たとえば、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁は、サイバー情報共有・連携プログラム(CISCP)を立ち上げました。最も必要としている人々と有益な情報やその他のリソースを共有することは、ランサムウェア犯罪を高リスク・低収益にするための大きな一歩になる可能性があります。

ランサムウェアの手法

ランサムウェアは、主に多段階マルウェア攻撃を通じて拡散し続けています。第1段階のフィッシング攻撃では、ユーザーをだまして悪意のある添付ファイルやリンクをクリックさせます。ほとんどの場合、これは言葉巧みにユーザーにマクロの有効化を求める文書です。マクロを有効化すると、ボットネットクライアントがコンピューターに感染し、攻撃者がコンピューターに対するコマンドおよび制御機能を利用できるようになります。

第2段階では、攻撃者はボットネットクライアントを使用してTrickbotやCobalt Strikeなどのマルウェアをインストールし、組織内で偵察を開始してシステムからシステムへと横方向に移動しながら暗証番号を盗みます。最後に、攻撃者はインストール済みのマルウェアを使用してランサムウェアをダウンロードし、組織のシステムに感染させます。

2021年、警察は、多くのランサムウェア攻撃が依存しているコンポーネントの一部を停止するための措置を講じました。代表的な例はEmotetです。ボットネットのコマンドおよび制御機能と、ランサムウェアやその他のマルウェアを組織内に配布する機能を持つことから広く使用されているこのトロイの木馬は、警察組織が連携した大規模な取り組みにより、2021年初頭にテイクダウンされました。

残念ながら、Emotetは2021年後半に復活しました。[xv] 一旦は撲滅させたと思っていたのですが攻撃者の活動を一時的に難しくしたにすぎず、終息には至りませんでした。

ランサムウェア攻撃者は、検出を回避しようと、マルウェアコンポーネントだけに依存するのではなく、多段階攻撃の一環としてLiving off the Land Binaries(環境寄生バイナリ、通称「LOLBins」)戦術を使用することが増えています。

たとえば、Microsoftのリモートアクセスシステムであるの悪用が広がっており、2021年には、ランサムウェア拡散のためにフィッシングと同じくらい頻繁にRDPが使用されました。RDPは数年前からよく標的になっていましたが、2020年のリモートワークへの突然の大規模移行以来、RDP攻撃が急増しています。

ランサムウェア攻撃は、コマンドおよび制御機能を提供するために、通常1つ以上のマルウェアコンポーネントに依存しています。

多段階のマルウェア攻撃が好まれる傾向は変わりませんが、2021年には単一段階の攻撃が増加しました。攻撃者は、巧妙なフィッシングメールの添付ファイルをはじめとする手段でランサムウェアの実行可能ファイルをユーザーに直接配布しました。[xvi] 単一段階攻撃には、多段階攻撃よりも迅速で、組織が検出して停止する可能性のあるマルウェアコンポーネントが少ないという利点があります。ただし、単一段階攻撃では、多段階攻撃のように組織内の可視性とアクセス性を攻撃者に提供できません。

2022年に目を光らせておくべきランサムウェア手法の傾向として最後に挙げられるのがクリプトマイニングです。一部の攻撃者は、ランサムウェアに代え、攻撃者に利益をもたらしながら被害組織のリソースを消費するクリプトマイニングソフトウェアを展開しています。これについては、本稿の暗号通貨のセクションで詳しく説明します。

サイバーレジリエンスによるランサムウェアの阻止

ランサムウェアは、フィッシングメール、悪意のあるリンク、セキュリティ保護されていないRDPなど、さまざまな方法でシステムに侵入して感染させます。多くの組織、特に中堅・中小企業では、今日の脅威への対応に必要な予算もスタッフのスキルも不足しています。また残念なことに、どのような予防策を講じても、組織内のどこかでランサムウェア感染が発生することは避けられません。

必要なのは、ランサムウェアやその他のサイバー脅威に対抗し、脅威が成功した場合に復旧するための戦略です。その戦略がサイバーレジリエンスです。サイバーレジリエンスは、人材のトレーニング、脅威の阻止、デバイスとネットワークの保護、データのバックアップ、およびデータ損失からの迅速な復旧に的を絞った多層防御戦略を立てることで機能します。

ランサムウェアを阻止するための多層アプローチは不可欠です。1つで100%の効果を発揮する防御策などありません。ただ、すべての受信メールにマルウェアがないか調べ、PCへのパッチ適用を万全にし、すべてのPCでアンチウイルスソフトウェアとエンドポイント保護ツールを使用し、フィッシング攻撃やさまざまなソーシャルエンジニアリングを回避する方法についてユーザーを教育するなどして防御策を組み合わせれば、攻撃の成功率を下げることができます。ある防御策では見逃された攻撃があっても、別の防御策がそれをブロックします。

サイバーレジリエンスは、ランサムウェア攻撃がこれらの防御策をすり抜けてシステムの感染に成功した場合でも対処できるよう準備を整えることでもあります。これには、インシデント対応機能を常に使用できる状態にし、回復力計画を定期的にテストすることも含まれます。組織の基幹システムとデータのバックアップおよび復元機能の準備はとりわけ重要です。準備ができていれば、より迅速に行動して、ランサムウェアインシデントの拡散を阻止し、重大なデータ侵害の可能性を最小限に抑え、業務を復旧することができます。

スポットライト:
「ステルス」型ランサムウェア攻撃の未来

2022年には、「ステルス」型のランサムウェア攻撃が発生するでしょう。身代金の迅速な支払いを促すために、ランサムウェア攻撃集団は、データが暗号化されて盗み出される「前」に身代金を支払うオプションを被害者に提供します。

彼らは、高度なフェイルセーフ自動暗号化および抜き取りルーチンを設定して、ターゲットに複数の強力な足場を確保しておきます。埋め込まれたマルウェアをターゲットが削除またはブロックしようとすると起動する仕組みになっています。すべての重要データとバックアップが暗号化されて主要データが盗み出される前に、非常に短い身代金支払い期間が設けられます。ターゲットは、暗号化されたデータを復元して業務を復旧するために必要な作業は言うまでもなく、本格的な攻撃の発生についての公表や、コンプライアンスの罰金やメディアの否定的な注目を回避するために、指定された早い段階で支払おうという気になります。

身代金要求のサイバー犯罪者は、特定のシステムを暗号化するか、ターゲットのネットワークとシステムに深く侵入したという強力な証拠を示すと申し出ます。支払いが迅速に行われない場合、サイバー犯罪者は最初の説得の段階でDDoS攻撃を使用します。実際よりもはるかに深く侵入したと主張し、標的を絞ったDDoS攻撃を使用して、ウェブサイトやその他の重要なシステムに侵入したように見せかける攻撃者もいます。

国際法の監視が厳しくなる中、サイバー犯罪者は不必要な注意を引くことは避けたいと考えています。この「ステルス」型のアプローチでは、目立つことなく、より迅速に支払いを受けやすくなります。また、2022年に一部の国や州で施行される可能性のあるランサムウェア攻撃の支払いを禁止する法律を回避しやすくなる可能性もあります。

「侵入からランサムウェア展開までの時間は今後さらに短くなります。また、特定されにくくなるよう、攻撃者がリブランドを行うこともあるでしょう。攻撃者がより戦略的に標的を選ぶようになると、中堅・中小企業は格好の餌食となります。保護策をほとんど講じていないこの種の企業なら身代金の要求に応じやすいと攻撃者は考えているのです。」

マット・アルドリッジ(Matt Aldridge)、
プリンシパルソリューションコンサルタント

暗号通貨

2021年には、暗号通貨への攻撃に大きな変化が見られました。まず、ブラウザーベースのクリプトジャッキングの終焉を目の当たりにしました。この形式の攻撃は、JavaScriptが悪意を持って注入されたウェブサイトで無防備な訪問者をだますことに依存しています。このようなサイトにアクセスすると、ユーザーの知らないうちにユーザーのブラウザーからクリプトマイニングスクリプトが実行されます。ブラウザーベースのクリプトジャッキングは2021年以前から衰退していましたが、今年ほとんど姿を消しました。

残念ながら、クリプトジャッキングは、ウェブサイトのトラフィックに依存せず効果の高い別のクリプトマイニングのアプローチに置き換えられました。攻撃者は、フィッシング攻撃によってクリプトマイニング実行可能ファイルを拡散し、ソフトウェアの脆弱性を悪用しています。最新のクリプトマイニングマルウェアの代表的な例はLemonDuckです。LemonDuckは、多くの技術を使用してシステムに感染し、感染したシステムから他のシステムに自らを拡散させます。[xvii]

クロスプラットフォームのマルウェアとして、LemonDuckはWindowsとLinuxの両方のコンピューターに感染することができます。安全性の低いプラットフォームへの拡大により、LemonDuckはより迅速に拡散し、マイニング数と収益を増やしています。また、脆弱性にパッチを適用したり、他のマルウェアの亜種を削除したりすることで、感染したプラットフォームを「保護」します。

これは、十分な実行時間を確保して成果を挙げるためには、クリプトマイニングマルウェアの検出を長期間(通常は数週間または数か月間)回避する必要があるためです。

暗号通貨の価値と人気が高まるにつれ、暗号通貨自体を盗むために詐欺を働く攻撃者も出てきました。

こうした詐欺では、フィッシングによって暗号通貨を攻撃者の管理口座に預けさせるといった従来の方法が常套手段というわけではありません。攻撃者は、偽のモバイルウォレットの配布から、見た目はそっくりの悪意のある交換サイトに被害者をリダイレクトするDNSポイズニング攻撃の使用まで、あらゆることを行います。クリップボード上のアドレスを攻撃者が選択したアドレスに置き換えるスキマーを含むマルウェアも見られます。

暗号通貨のマネーロンダリングへの関心も高まっています。ランサムウェアで多額の身代金を集めたり、詐欺を働いて暗号通貨を盗んだりする攻撃者は、検出や起訴を避けるために、通常暗号通貨のソースを隠す必要があります。警察は暗号通貨ロンダリングを厳しく取り締まっています。また、米国司法省は2021年後半に国家暗号通貨執行チーム(NCET)を設立しました。NCETは暗号通貨関連の犯罪を調査して起訴すると同時に、被害者の資金回収を支援します。[xviii]

これがこの種の犯罪の減少につながるかどうかはまだわかりませんが、2022年2月、盗まれた36億ドルの暗号通貨の押収と容疑者逮捕を司法省が発表しました。この暗号通貨は数年前に盗まれ捜査当局が追跡していたものですが、見事に挽回しました。[xix] うまくすれば今後はさらに多くの暗号通貨の押収と逮捕が見込まれます。

「新たに出現した脅威アクターは、長期的マイニングと短期的マイニングの費用対効果分析を行い、ソーシャルメディアプラットフォームを利用して価格を操作しようとする可能性があります。彼らはより入念に計画を練ることで、もうけを最大限に増やそうとするでしょう。」

ケルビン・マレー(Kelvin Murray)、
シニア脅威リサーチアナリスト

高リスクURL

悪意のあるURLや疑わしいURLなどの高リスクURLは、以下のように分類されます。

- ボットネット
- キーロガーと監視
- マルウェアサイト
- フィッシングとその他の詐欺行為
- プロキシ回避と匿名化
- スパム、スパイウェア、およびアドウェア

BrightCloud® Web Classification Serviceは、ウェブサイトの動作、履歴、年齢、人気、場所、ネットワーク、リンク、およびリアルタイムのパフォーマンスに基づいてURLを分類するために1日平均45億件を超えるリクエストを行います。常に分類を更新して、リスクの高いURLと、各URLに関連付けられている不正な動作を特定しています。

当社が毎年注意深く監視している傾向の1つは、悪意のない(信頼できる)ドメインでホストされている悪意のあるURLの数です。この割合は、脆弱性を悪用してウェブサーバーに侵入し、フィッシングサイトのホスティングに使用するなど、他の点では害のないサーバーに悪意のあるウェブサイトを攻撃者がセットアップした頻度を示します。数年前、その割合は25%から40%の間を上下していましたが、2020年には8%に下がりました。その大幅な減少が、パンデミック、ウェブサーバーとウェブサイトのセキュリティ対策の改善、または当社の脅威データ収集方法の一部変更に関連しているかどうかは当時わかりませんでした。

ただ、今は答えられます。2021年に、その割合は悪意のあるURLの16%にまで跳ね上がりました。2020年の一時的な落ち込みは、主にパンデミックに関連していたと考えていいでしょう。

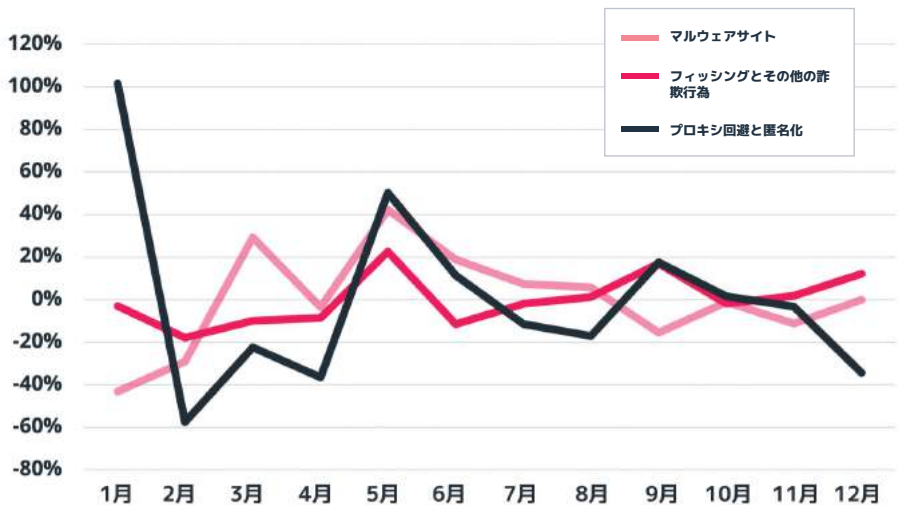
組織がウェブサーバーなどの外部からアクセス可能なリソースの保護に多くのリソースを集中させたか、攻撃者が計画を変更した可能性があります。

URLの分類

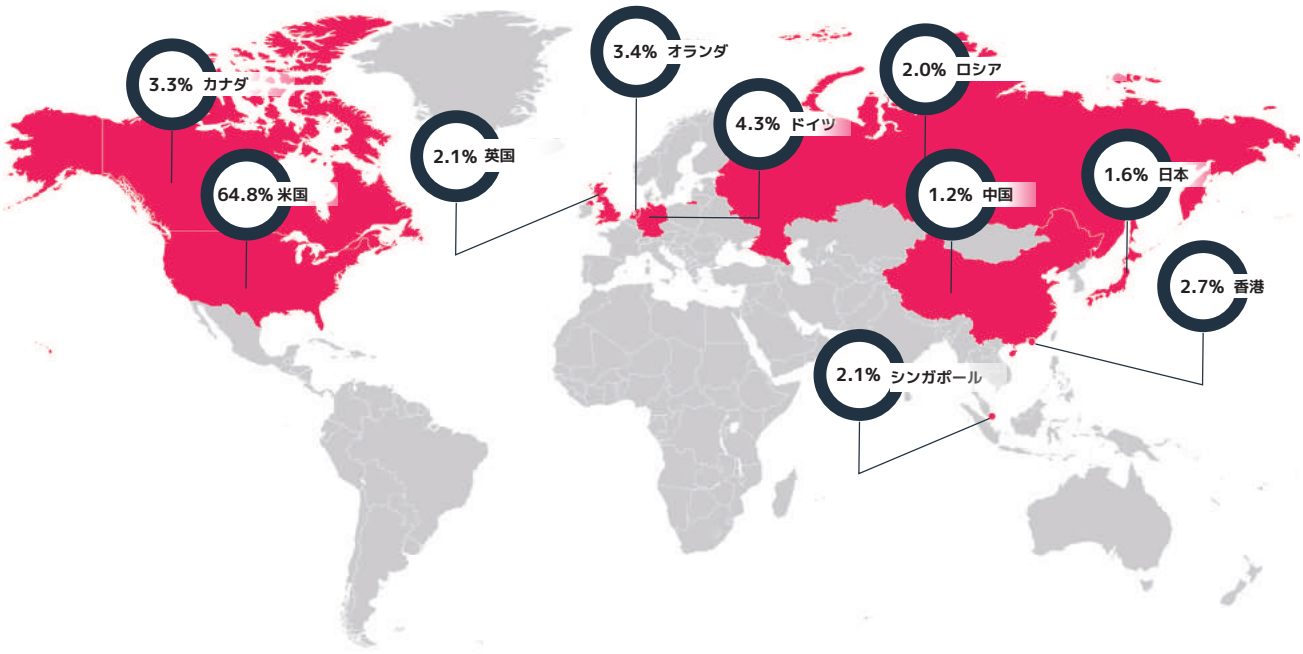
2021年に400万を超える新しい高リスクURLを発見し、そのほぼ3分の2がフィッシングに関係していました。

これは高い割合ですが、高リスクURLの81%がフィッシング用であった2020年から大幅に減少しています。ほとんどの高リスクURLは、フィッシング、マルウェアサイト、プロキシ回避と匿名化用であり、本稿ではこれら3つのタイプに焦点を当てています。

グラフは、各タイプの2021年の月ごとの変動を表すものです。その年の平均を0%とし、実際の数がそれをどれだけ上回ったか下回ったかを示しています。興味深いことに、このグラフから、年間を通じてフィッシングURLの数の変動が比較的少なく、振れ幅は最大で平均の上下約20%であることがわかります。マルウェアサイトはより動的で、振れ幅は平均の上下40%を超えています。



図表8:高リスクURL分類の傾向



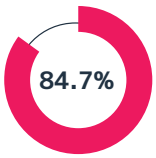
図表9:2021年に高リスクURLの大半をホストしていた上位10か国

圧倒的に大きな変化が見られたのは、プロキシ回避と匿名化です。1月の値は平均を100%以上上回っていたにもかかわらず、2月には平均を60%近く下回るまで急落。また5月に平均を50%上回りました。最も注目すべきは、5月には3種類の高リスクURLすべてが急増したことです。

これらすべての変動を引き起こしたであろう出来事は特定できません。ただ、これらの傾向を何年にもわたって監視してきた当社の経験から、新しい脆弱性、最新の社会情勢、ユーザーの習慣の変化といった要因を活かして成功につなげるために攻撃者が手口を次々と変えることはわかっています。

地理的分布

当社では、新しい高リスクURLを見つけるたびに、それをホストしている国の特定を試みます。2021年当時、新しい高リスクURLの約48.5%は、URLの発信元を特定しにくくするプロキシやTorのような匿名化ツールの背後に隠れていました。マルウェアサイトのURLの場合、プロキシまたは匿名化ツールの背後に隠れていたサイトは84.7%に上りました。



マルウェアサイトURLの84.7%がプロキシまたは匿名化ツールの背後に隠れていました。

図表9は、高リスクURLをホストしていると特定されたことが特に多い10か国を示しています。これらの国のほとんどでは、2020年から2021年にかけて順位と割合の変化があまり見られません。米国は、特にフィッシングサイト向けに高リスクURLの大部分をホストしており、そのシェアは2020年以降さらに増加しています。同じ期間に、ドイツのシェアは2倍以上、カナダのシェアは3倍以上になりました。デンマークと韓国はトップ10から脱落し、中国と英国に取って代わられました。

発信元を追跡できるマルウェアサイトのURLについては、米国(44.3%)が他を引き離し1位に、それに続くトップ5は中国(10.5%)、香港(9.1%)、シンガポール(5.7%)、ロシア(5.4%)となりました。これらを合わせると、2021年に見つかった発信元がわかるすべてのマルウェアサイトのURLの75%が上位5か国でホストされていたことになります。

米国は、フィッシングURLのホスティングでも世界トップで、発信元を追跡できるすべてのフィッシングURLの59.6%を占めています。これに続くトップ5はドイツ(5.3%)、カナダ(4.5%)、オランダ(4.3%)、香港(2.7%)で、上位5か国でのホスティングを合わせると、発信元がわかるすべてのフィッシングURLの76.4%に上ります。

「存在する高リスクURLの割合は今後も増えると予測していますが、攻撃者は年間を通して各時点の状況に基づき戦略的にこれらのURLを使用します。ホリデーシーズンが始まる前であっても、納税後や選挙前であっても、攻撃者は、無警戒なユーザーをだましてクリックさせようと、攻撃のタイミングを計っていると考えられます。これは企業と消費者により大きなリスクをもたらすでしょう。」

グレイソン・ミルボーン(Grayson Milbourne)
セキュリティインテリジェンスディレクター

フィッシング攻撃

電子メール、テキストメッセージ、その他の通信プラットフォームを介したフィッシング攻撃は、今も他の多くの攻撃の最初のステップになっています。高リスクURLのセクションで説明したように、当社が2021年に検出した新しい高リスクURLのほぼ3分の2は、フィッシング攻撃用でした。マルウェアやランサムウェアによる攻撃、暗号通貨詐欺はすべて、フィッシングを広く利用しています。

フィッシングメッセージやウェブサイトはどんどん巧妙化するため、ユーザーが気付きにくくなっています。CAPTCHAをフィッシングサイトに追加して、よりリアルに見せる攻撃者もいます。[xx]

ユーザー向けにセキュリティ意識向上のためのトレーニングを行うと同時にフィッシング対策テクノロジーを用いることで、これらの脅威を検出して阻止することが、これまで以上に重要になっています。

フィッシング件数

図表10は、2021年の各月に検出されたフィッシングメッセージの件数を示しています。例年どおり、年初からしばらくの間はフィッシングが少なく、最初の4か月のフィッシング活動の合計は年間の9%に過ぎませんでした。

その後、4月までの平均と比較して**5月に770%増加**しました。

米国では、フィッシング活動が所得税の申告時期あたりに急に活発化することがよくあります。攻撃者が税金の還付を受けた消費者から搾取しようとすることもその一因かもしれません。

「サイバー犯罪者は、スピアフィッシングやスプーフィングなどの攻撃を実行する機会として納税時期を利用することを好みます。暗証番号を解除したり、納税申告内容や還付資格を確認したりするために個人情報を提供させようとする不審な電子メールに注意してください。企業も個人も簡単にそうした罠にはまる可能性があります。受信メールが正当な発信元からのものであることを常に確認し、個人情報の提供を求める迷惑メールには決して返信しないでください。」

グレイソン・ミルボーン
(Grayson Milbourne)
セキュリティインテリジェンス
ディレクター

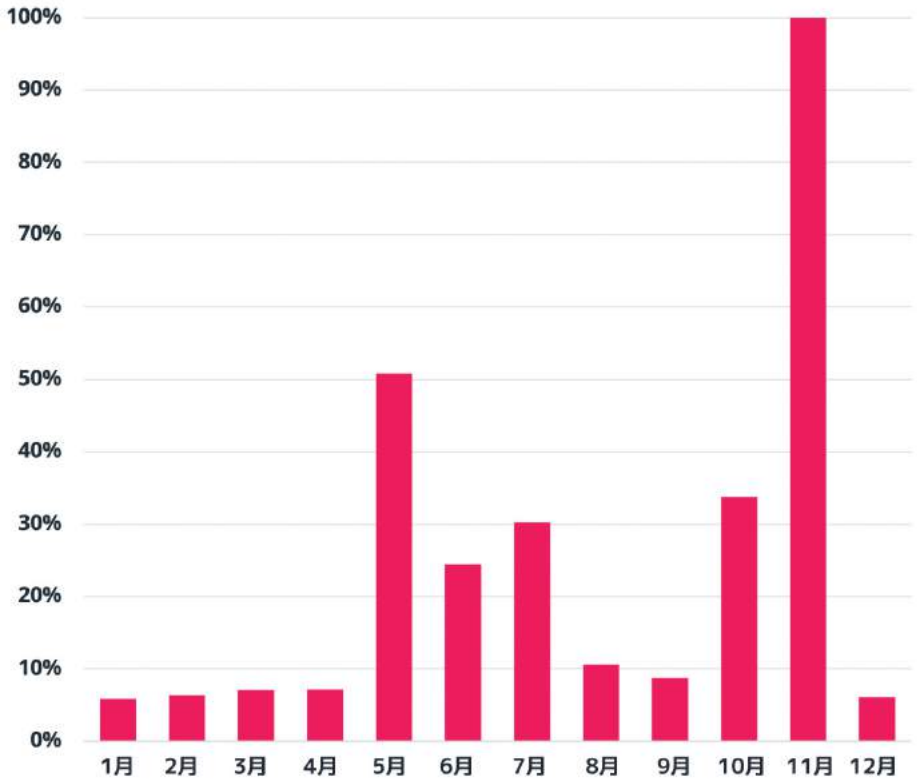
セキュリティ意識向上のためのトレーニングを受けると、クリックする前にURLについて調べることの重要性をユーザーが理解するようになります。これに対抗するために、一部のフィッシング攻撃では、bit.ly、tinyurl.com、is.gdなどのURL短縮サービスを使用して、フィッシングURLにリダイレクトする一見正当なURLを生成しています。これらの短縮サービスは合法的な目的で広く使用されているため、ほとんどの組織はブロックできません。[xxi]

このようなフィッシング攻撃を阻止するには、ユーザーが短縮URLを認識してクリック前にリダイレクト先を探す訓練を受ける必要があります。たとえば、bit.lyまたはtinyurl.comのURLの末尾にプラス記号を追加すると、短縮URLの作成日時とリダイレクト先URLを示す安全なページに移動します。短縮URLを入力するとリダイレクト情報を取得できるウェブサイトもあります。短縮URLを認識してそれらを処理する方法をユーザーは身につける必要があります。

2021年には、年間のフィッシング活動の17.5%が5月に発生しました。

20%に迫る割合です。6月と7月にもかなりのフィッシング活動が発生した後、8月と9月は急減しました。フィッシング活動が例年少ないこの期間は「ハッカーホリデー」と呼ばれています。おそらく犯罪者が休暇を取っているのでしょう。

例年フィッシングが活発化する10月と11月に今年も急増が見られました。フィッシングが群を抜いて活発になる11月は年間の全活動の34.3%を占め、10月は11.6%でした。10月と11月にフィッシングが活発になるのは、ホリデーショッピングシーズンが近づくためです。また、米国で選挙の二極化が進み関心が高まると、攻撃者はフィッシングメッセージやウェブサイトに選挙を利用しました。主に5月と6月に行われた予備選挙、および11月初旬の総選挙の時期がこれに当たります。



図表10:月ごとのフィッシング攻撃

HTTPおよびHTTPSの使用

フィッシングURLを検出した場合、HTTPとHTTPSのどちらを使用しているかも追跡します。多くのユーザーは、ブラウザーでHTTPSに「安全」を意味する鍵マークがついているのを目にすることから、鍵マークが表示されていれば正当なサイトだと誤って判断します。当然攻撃者はこれを理解しているため、ドメインを登録し、証明書を取得して、その証明書を使用するウェブサイトを作成します。

2021年に検出されたすべてのフィッシングURLのうち、32%はHTTPSを使用していました。ドメイン登録機関と証明機関が犯罪者によるサービスの利用を阻止しようとしなかったり、証明書のレピュテーションが脅威インテリジェンスの一部として追跡されなかったりすると、この割合ははるかに高くなるでしょう。

図表11:月ごとのフィッシング攻撃でのHTTP/HTTPS使用

最もなりすましの多い企業

通常、フィッシング攻撃で偽装される企業は、順位の変動は多少あるものの、顔ぶれはいつも同じです。2021年に標的にされた上位5ブランドは、検出されたフィッシングURLの54%以上を占めました。Apple (13.0%)、Facebook (12.1%)、YouTube (11.8%)、Microsoft (9.1%)、Google (9.1%)がフィッシング攻撃でおとりとしてよく使用され、2020年にもYouTube以外はすべてトップ5に入っていました。YouTubeの順位が上がったのは、同じくAlphabet傘下にあるGoogleにアカウントがリンクされていることが原因であると思われます。

最もなりすましの多い企業のトップ5から今年姿を消したのは、2020年に1位となったeBayです。eBayは、パンデミックに伴う商品不足が深刻になる中、必要な商品を探す消費者がサイトに押し寄せた2020年の初めに特に頻繁に偽装されました。

「サイバー犯罪者が戦術を進歩させ、より巧妙で検出されにくくなるにつれ、ソーシャルエンジニアリングの戦術はより複雑になると予想しています。ビジネスメール詐欺(BEC)がより一般的になるでしょう。ディープフェイク技術は虚偽・誇大広告に興味を引くための強力なツールとして発展を続け、特に選挙や政治情勢に関する偽情報を広めるのに利用されるでしょう。」

タイラー・モフィット(Tyler Moffitt)、
シニアセキュリティアナリスト

2019年のトップ10		2020年のトップ10		2021年のトップ10	
Facebook	12.8%	eBay	13.2%	Apple	13.0%
Microsoft	10.6%	Apple	10.2%	Facebook	12.1%
Apple	8.4%	Microsoft	9.5%	YouTube	11.8%
Google	7.7%	Facebook	8.8%	Microsoft	9.1%
PayPal	6.2%	Google	8.6%	Google	9.1%
Dropbox	3.2%	Steam	7.9%	Amazon	8.9%
Chase	3.1%	Yahoo	5.4%	PayPal	3.3%
Yahoo	2.9%	Amazon	4.7%	La Banque Postal	2.7%
Adobe	2.8%	Netflix	3.0%	Target	2.5%
Wells Fargo	2.8%	PayPal	3.0%	Instagram	1.9%

図表12:フィッシング攻撃で最もなりすまし対象となった企業

2021年には、検出されたすべてのフィッシングURLのうち、上位10ブランドが72%近くを占めました。

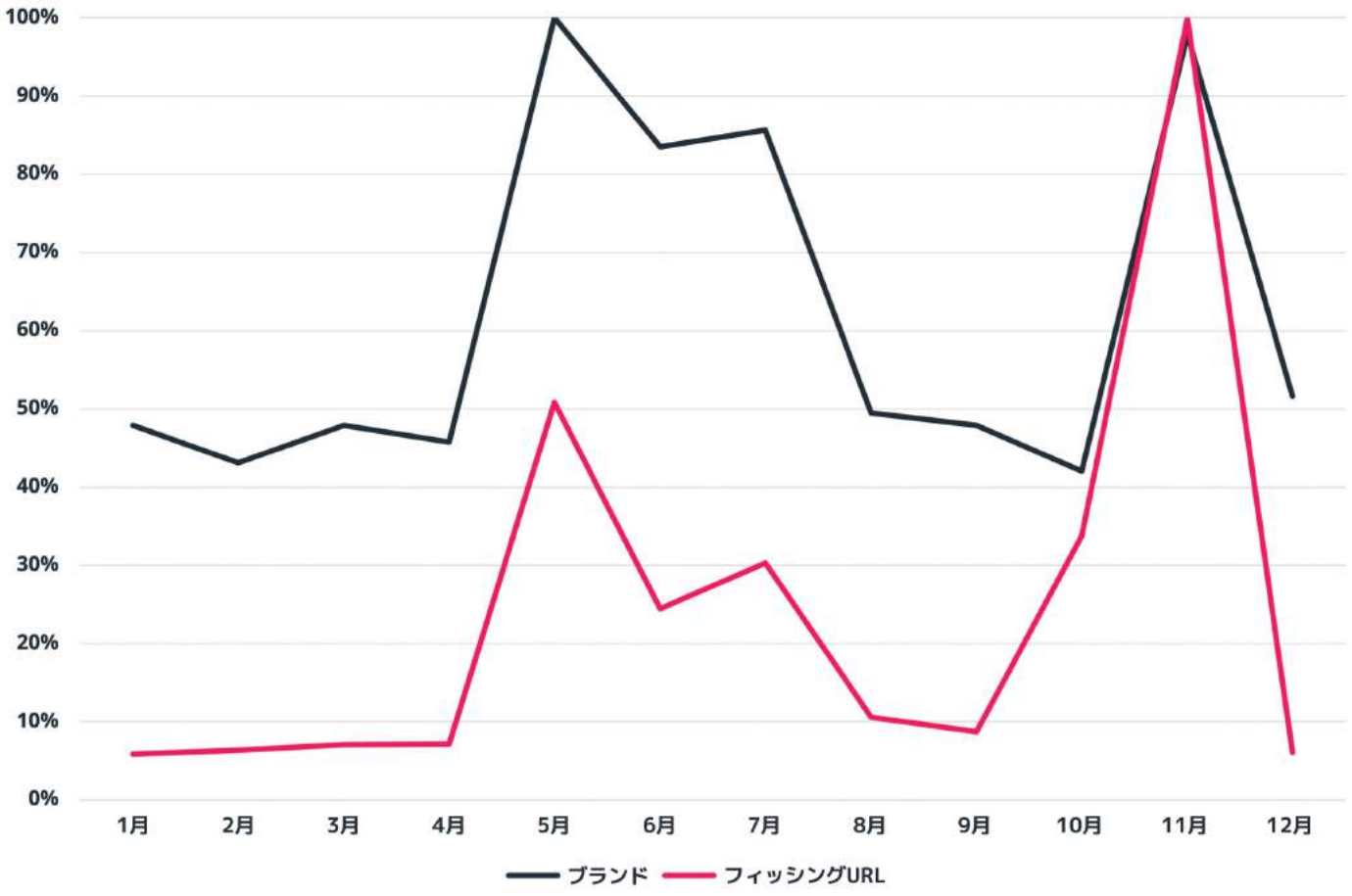
最悪の商品不足が終わると、フィッシング詐欺師はeBayから離れていき、今年eBayはかろうじてトップ20に入りました。これは、最新の社会情勢に応じて攻撃者の行動が変化することを示す代表的な例です。

2021年には、検出されたすべてのフィッシングURLのうち、上位10ブランドが72%近くを占めました。ただし、毎年何百もの他のブランドを利用したフィッシング攻撃を検出しており、多くの場合、年間を通じて1つのブランドで1つのフィッシングURLが使用されています。また、任意の時点で見ると、偽装される企業は実にさまざまです。

図表13は、偽装されたブランドの月ごとの相対数を表しています。測定した月のうち5月が最高でした。

11月は5月とほぼ同じ数のブランドが偽装され、6月と7月も高い値となりました。比較のために、グラフには、各月に検出されたフィッシングURLの相対数も示されています。11月には、ブランドの多様性とフィッシング件数のどちらも高かったことがわかります。5月は、フィッシング件数は同じでしたが、偽装されたブランド数は半分しかありませんでした。

2つの線をより厳密に比較すると、10月と11月を除き、年間を通じて似たような推移の仕方をしています。10月と11月には、偽装されたブランドの数が急増し、12月に通常のレベルに戻ったようです。その理由として最も可能性が高いのはホリデーショッピングシーズンです。



図表13:なりすまし対象となったブランド数(月別)

悪意のあるIPアドレス

BrightCloudは、関連付けられたIPアドレスによって悪意のある行動を追跡して、犯罪常習者をブロックし、攻撃がエンドポイントに到達するのを防ぎます。2021年のある時点での悪意のあるIPの平均数は400万近くでした。この数は過去数年間変化がなく、悪意のあるIPの活動が停滞している可能性を示しています。

悪意のあるIP追跡の一環として、BrightCloudは各アドレスから行われる不正な活動の種類を監視します。当社では悪意のある行動が検出された場合、そのインスタンスを「有罪」と呼びます。本稿では、年間で最も有罪となった5万件の悪意のあるIPについて詳しく考察します。2021年の上位5万件は、1,160万件の有罪判定を受けており、2020年の有罪判定より10%増加しています。

複数の悪意のある行動を実行

悪意のあるIPの悪意のある行動には、スキャナー、スパムソース、Windowsエクスプロイト、ボットネット、Torプロキシ、その他のプロキシ、ウェブ攻撃、フィッシング、プロキシ、モバイル脅威などさまざまなソースが利用されています。2021年の上位5万件の悪意のあるIPを見ると、どのIPも年間を通じてこれらのカテゴリの2つ以上で有罪と判定されました。またこのうち96.5%が3つまたは4つのカテゴリで有罪と判定されました。

これは、最も活発な悪意のあるIPは、複数の悪意のある行動に使用されるという永続的な傾向を示しています。

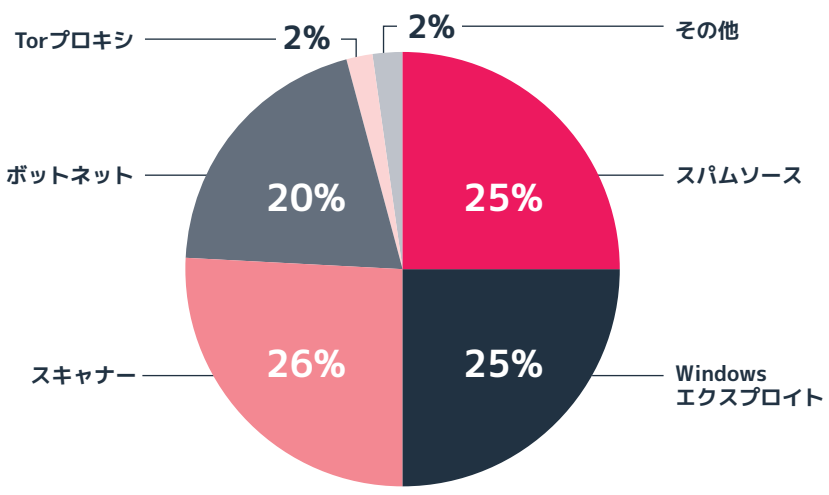
ただし、5つ以上のカテゴリに該当する悪意のあるIPを見た場合、この有罪傾向は弱まり、上位5万件の3.5%にまで下がります。この割合は前年までよりも低下しており、攻撃者が1カ所から実行する悪意のある行動の種類を減らして検出を回避しようとしている可能性があることがわかります。

図表14は、上位5万件の悪意のあるIPのカテゴリ別有罪判定数を反映しています。4つのカテゴリが他のカテゴリよりもはるかに高い割合となっています。

最大のカテゴリのスキャナーは26%、次にスパムソースとWindowsエクスプロイトがそれぞれ25%、ボットネットが20%と続いています。これらの4つのカテゴリは、すべての有罪判定の96%を占めており、これは2020年の調査結果と類似しています。

BrightCloudではTorネットワークの出口ノードも追跡しています。攻撃のソースを隠すためにTorプロキシがよく使用されるためです。検出されたTor出口ノードの数は、2020年から2021年にかけて約40%増加しました。

2021年の合計は2019年に観察されたもののほぼ3倍です。右肩上がりが続いているのは、リモートおよびハイブリッドワークへの移行とプライバシーに関する懸念の高まりからTorネットワークの使用が増加していることを示しています。



図表14:上位5万件の悪意のあるIPアドレスのカテゴリ別有罪判定数

有罪判定の頻度

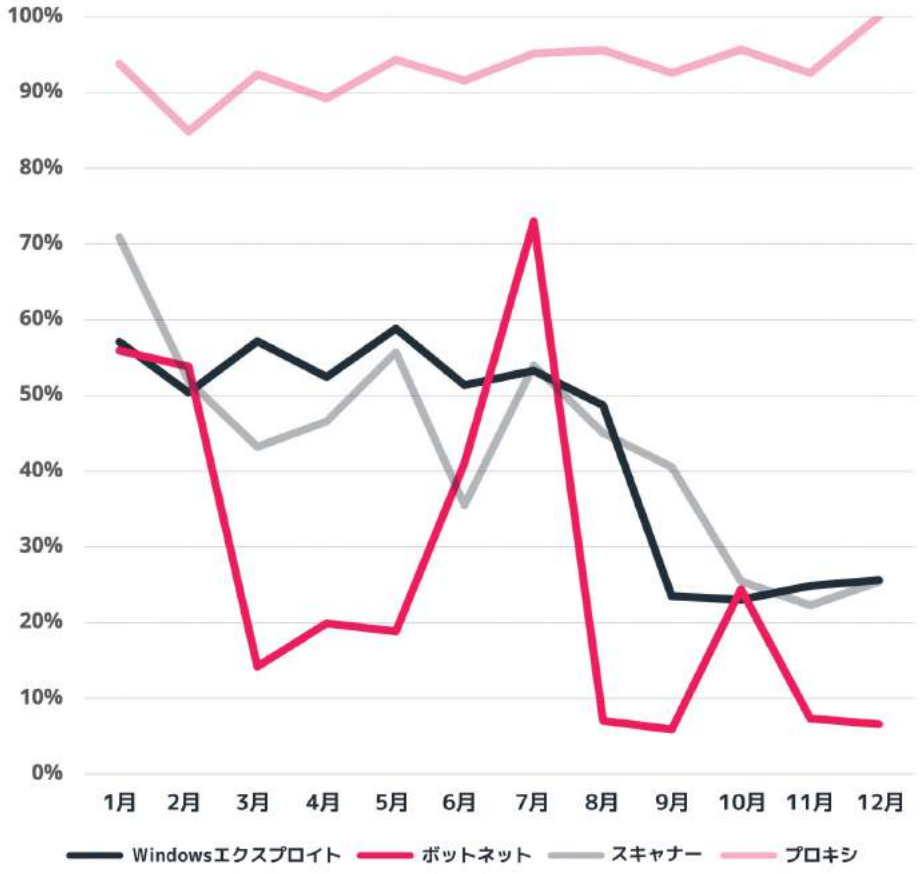
これまで見てきた有罪判定数は、それぞれの行動の発生頻度を示すものではありません。もう少し深く掘り下げて、上位5万件の悪意のあるIPアドレスのそれぞれが悪意のある行動を実行した頻度を見てみましょう。

2021年どの月にも悪意のある行動が観察されたのは上位5万件の6.0%のみでした。有罪判定の34%近くを上位5万件が占めていたにもかかわらずです。IPは、悪意のある目的で短期間使用された後、数か月のブランクを経て使用が再開することがよくあります。この流動的な戦略により、攻撃者はブロックされるのを回避するとともに、攻撃再開前にブロックリストから削除されるよう十分な時間を確保することができます。

上位5万件のうち、54.1%は2021年の活動期間は3か月以下でした。

有罪のカテゴリとして最もよく見られるスパムは、昨年全体の86.3%を占めました。これは、2020年と2019年の割合(それぞれ87.0%と87.6%)とほぼ同じです。スパムの割合は1年を通して比較的一貫していました。

残りの有罪判定データの変化がわかりやすいよう、スパムのデータを除いてみました。図表15は、上位5万件の上位カテゴリ(スパムを除く)であるプロキシ、Windowsエクスプロイト、スキャナー、ボットネットの月別有罪判定数を示しています。プロキシは年間を通じてほぼ一定していましたが、他のカテゴリ、特にボットネットには大きな変化が見られ、7月にはボットネットの有罪判定が急増しました。その理由としては、その時点で1つ以上の大規模なDDoS攻撃が実行され、何か月も静かだったボットネットのメンバーが突然活発化し、一斉に検出されたことが考えられます。



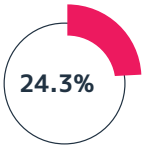
図表15:上位5万件の悪意のあるIPアドレスのカテゴリごとの月別有罪判定数(スパムを除く)

家庭や職場で使用するものから私たちが持ち運ぶものまで、IoTデバイスの数は今後も増え続けます。消費者が日常的に使用する多くのIoTデバイスには、他のデバイスに共通するセキュリティ機能が不足しており、[xxii] それらが安全な状態で展開されることや、ましてや維持されることなどめったにありません。消費者向けIoTデバイスは、多くの処理機能と帯域幅を利用できるため、格好の標的となっています。

消費者向けIoTデバイスは、攻撃者がボットネットと組み合わせてDDoS攻撃を実行する際の悪用と侵入の道具として最適です。また、同時に実行されている他の攻撃を隠すトラフィックを生成するために使用されることもあります。ボットネットのIP数は2022年に増加すると予想されますが、2021年と同様の変動があるでしょう。

地理的内訳

上位5万件のIPアドレスは175か国からのものです。ただし、大多数にあたる80%は20か国を発信元としていました。最も目を引いたのは、上位5万件の半分以上がわずか5か国、すなわち中国(17.6%)、米国(15.0%)、インド(8.6%)、ベトナム(6.7%)、ロシア(3.9%)にあったことです。



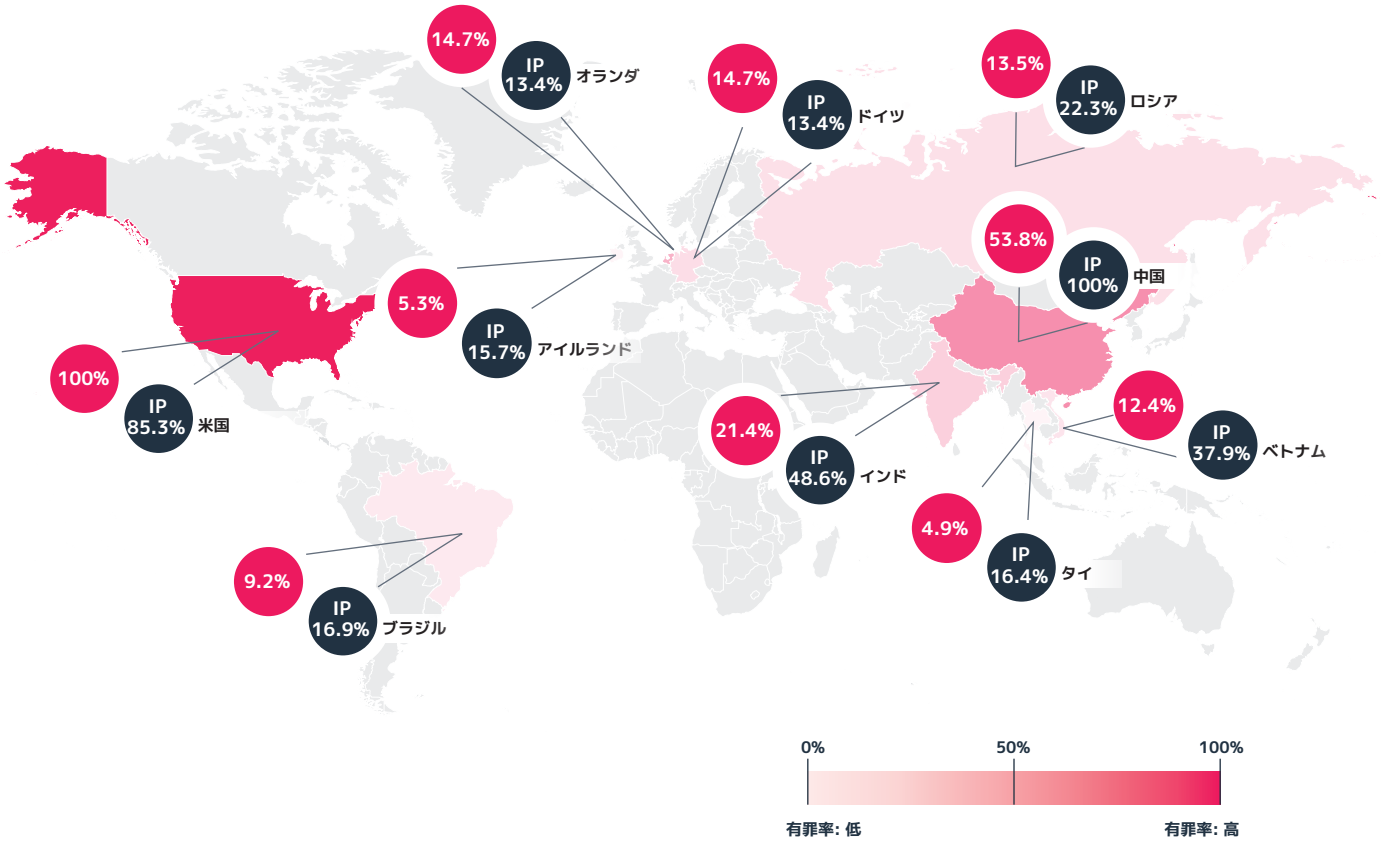
米国は2021年に最も多くの有罪判定を受けました。

図表16は、上位10か国から発信された上位5万件のIPアドレスの相対的なシェアを示しています。中国のシェアは1位であるため100%と表されています。このチャートは、各国の有罪判定数も示しています。米国は2021年に最も多くの有罪判定を受け、上位5万件の24.3%を占めました。これは2020年から25%の増加です。

2021年の上位5か国の残りは、中国(13.1%)、オランダ(8.2%)、インド(5.2%)、ドイツ(3.6%)でした。これら5か国を合わせると、有罪判定では54%を超えますが、上位5万件のIPアドレスでは47%にとどまり、圧倒的なシェアというほどではありませんでした。

上位5か国のうち、悪意のあるIPアドレスあたりの有罪判定数はオランダが最も多く、平均526件でした。これは、オランダの悪意のあるIPアドレスのそれぞれが、他の国を平均した悪意のあるIPアドレスよりも、平均して多く悪意のある行動を実行したことを意味します。

2位は375件の米国、3位は350件のドイツとなりました。上位5万件全体では、IPアドレスあたりの有罪判定の平均数は241件でした。



図表16:悪意のあるIP上位5万件について、発信元の国別に見た悪意のあるIPアドレス数と有罪判定数

セキュリティ意識向上のためのトレーニング

脅威を阻止するには、多層防御が必要不可欠です。攻撃はますます巧妙化し、結果的に攻撃者は身代金や暗号通貨の盗難によって過去最高の利益を確保しています。最善の防御策は、補完し合う防御策をいくつか重ね合わせることで成り立ちます。セキュリティ意識向上のためのトレーニングは、ユーザーの行動を変化させることに重点を置く唯一無二の防御策です。

セキュリティ意識向上のためのトレーニングを通じてユーザーが適切な訓練を受けると、マルウェアに感染するデバイスが大幅に減少します。Webroot® Security Awareness Trainingを導入すると、Webroot® Business Endpoint Protectionのみを使用するよりも、デバイスのマルウェア感染が10%減少します。また、Webroot® DNS ProtectionとWebroot® Security Awareness Trainingを併用すると、15%減少します。Webroot® Security Awareness Trainingは、今なお頻発するBEC攻撃に関するユーザー教育も行えます。

BEC攻撃にはマルウェアの要素が含まれているとは限らないため、BEC攻撃を発見して阻止するには、ユーザー教育が特に重要です。

データ損失のインシデントの多くは、1人のユーザーによる1回のミスから始まります。デバイスの感染を15%削減すると、特に中堅・中小企業にとって大きな違いが生まれます。ユーザーがフィッシング攻撃やその他のソーシャルエンジニアリング戦術にだまされないという保証はありませんが、適切なトレーニングを行うことで、それらを検出して成功を阻むことが容易になります。

ユーザーはフィッシングの最新の傾向、特に選挙や主要なスポーツイベントなどのトピックに関係する情報を頻繁に確認する必要があります。また、ソーシャルメディア上の偽のペルソナやディープフェイクの使用など、ユーザーをだますために使用される他の脅威についても知る必要があります。ユーザーの教育水準が高いほど、組織の保護にユーザーが積極的に参加できるようになります。

結論

2021年を振り返ると、セキュリティ関連の問題は考え得る限りすべての問題が発生した年でした。今年はどうでしょうか。

残念ながら、同様の状況が続くものと推測されます。広く分散した人材がハイブリッド型の作業環境で働くという現状が変わらない中、悪意のある攻撃者は戦略を練って攻撃計画を実行に移し続けます。リモートで動作するデバイスが増えるにつれ、エンドポイント保護とセキュリティ意識向上のためのトレーニングは、保護と攻撃防止に不可欠となり、また、悪意のある攻撃者は手口を巧妙化し続けるため、ますます重要になっていきます。さらに悪いことに、悪意のある攻撃者が手を組んでより大きな犯罪組織を作り、ランサムウェア、暗号通貨の盗難、盗んだデータの販売などによって今後も大きな利益を生み出そうとすることは間違いないでしょう。サプライチェーン攻撃、重要なインフラストラクチャに対する攻撃、テイクダウンされたボットネットの再生は今後の動向を示唆しています。2022年も私たちにとって困難の多い年になるでしょう。

テクノロジー、プロセス、人材にサイバーレジリエンスを組み込み対応することで、これらの脅威に備えて回復する能力が生まれます。侵入をゼロにすることは不可能であるため、計画を立て、発生したら迅速に回復できるよう準備する必要があります。

侵入の可能性を減らし、通常の業務を迅速に復旧する能力を確立するには、強力な多層防御策を導入する必要があります。これには、業界をリードする脅威インテリジェンスとマシンラーニングに裏打ちされたソリューションを使用して、マルウェアやネットワーク層の攻撃を防ぐことも含まれます。すべてのシステムとファイルをバックアップして、必要な時に必要な場所でデータを常に利用できるようにするとともに、攻撃シナリオをシミュレーションして復元機能をテストすることも必要です。また、ユーザーがフィッシング攻撃や詐欺を特定して回避できるように、頻繁にトレーニングを行うことも重要です。これらを統合した対策が、サイバーレジリエンスの中核になります。

サイバーレジリエンス戦略を導入すれば、攻撃に備え、攻撃を受けても回復することができます。多層防御アプローチにより、悪意のある脅威の拡散を阻止し、重大なデータ侵害の可能性を最小限に抑え、業務を復旧させるために、より迅速に行動できます。サイバー犯罪との戦いを前進させることができるのは、サイバーレジリエンスだけです。

出典

i https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021
ii https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/
iii https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021
iv https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases
v https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
vi https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
vii https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021
viii https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/
ix https://www.wired.com/story/apple-ransomware-attack-quanta-computer/
x https://www.zdnet.com/article/us-insurance-giant-cna-financial-paid-40-million-ransom-to-wrestle-back-control-of-systems/
xi https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/22/with-rising-cyber-insurance-costs-and-requirements-consider-new-alternatives-to-fight-ransomware/?sh=8eef096e140e
xii https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/
xiii https://www.reuters.com/technology/us-offers-reward-up-10-mln-information-darkside-cybercrime-group-2021-11-04/
xiv https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
xv https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/
xvi https://zix.com/resources/threat-report
xvii https://www.zdnet.com/article/microsoft-warns-over-this-unusual-malware-that-targets-windows-and-linux/
xviii https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
xix https://www.wsj.com/articles/justice-department-says-it-seized-3-6-billion-in-stolen-cryptocurrency-exchange-hack-11644339381
xx https://zix.com/resources/threat-report
xxi https://zix.com/resources/threat-report
xxii https://doi.org/10.6028/NIST.IR.8267-draft

BrightCloud® Threat Intelligenceについて

BrightCloudは、ゼロデイ脅威をリアルタイムで阻止するためにクラウドおよびAI (人工知能)を取り入れた初めての脅威インテリジェンスプラットフォームです。このプラットフォームは、エンドポイントおよびネットワークの保護と脅威インテリジェンスにより世界中の企業と製品を保護するために使用されます。業界で最も堅牢なインターネット脅威データベースの構築と分析に10年以上の経験を持つBrightCloudには、対象範囲がきわめて広いモデルを使用するほか、分類されないオブジェクトの数は少なく、履歴レコードの数は非常に多いという他ではまねができない特長があります。

2019年、BrightCloudはエンタープライズ情報管理のグローバルリーダーであるOpenTextに買収されました。組織全体で、サイバーレジリエンス分野のマーケットリーダーとして、あらゆる規模のビジネスに総合的なエンドポイントプロテクションと災害復旧を提供しています。

brightcloud.com

BrightCloud®
Threat Intelligence