HP WOLF SECURITY

サイバー犯罪の進化：ダークウェブが脅威の現状を急激に悪化させている理由とその対策

AN HP WOLF SECURITY レポート

コンテンツ

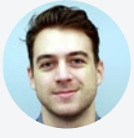
レポート寄稿者

アレックス・ホランド（Alex Holland）
HP Wolf Securityレポート作成者、HPシニアマルウェアアナリスト

ジョアンナ・バーキー（Joanna Burkey）
HP最高情報セキュリティ責任者（CISO）

Dr. イアン・プラット（Ian Pratt）
HPパーソナルシステムズ事業セキュリティ部門グローバル責任者

ボリス・バラシェフ（Boris Balacheff）
HP Labsセキュリティリサーチ / イノベーション担当チーフテクノロジスト



パトリック・シュレイファー（Patrick Schläpfer）
HPマルウェアアナリスト

マイケル・カルセ（Michael Calce）氏
「MafiaBoy」として知られる元ブラックハットハッカー、HPセキュリティアドバイザリーボード・チェアマン、Decentraweb CEO、Optimal Secure社長

マイク・マクガイア（Mike McGuire）博士
英国サリー大学犯罪学上級講師、サイバーセキュリティに関する専門著作者

ロバート・マッセ（Robert Masse）氏
HPセキュリティアドバイザリーボードメンバー、Deloitteのパートナー

ジャスティン・ボーン（Justine Bone）氏
HPセキュリティアドバイザリーボードメンバー、MedSec CEO

エグゼクティブサマリー

ダークウェブはかつてないほどサイバー犯罪経済を加速させた

サイバー犯罪者が協力し、組織化し、技術を磨き、不正な店舗を設立できる匿名のオンライン環境を提供することで、ダークウェブはサイバー犯罪を多様で評判の影響を受けやすいサービス産業へと進化させることを可能にしました。

本レポートは、HP Wolf SecurityがForensic Pathways[1]と共同で、産学のセキュリティ専門家の協力を得て作成したもので、簡単に導入できるマルウェアやランサムウェア攻撃が “Software as a Service（サービスとしてのソフトウェア）” ベースで提供されるようになったことで、今日のサイバー犯罪者がいかにプロフェッショナルな基盤を利用して活動するようになっているかを明らかにしています。その結果、初歩的なITスキルしか持たない人々でさえ、自分の選んだ対象に対して標的型サイバー攻撃を仕掛けることができるようになっています。

「デジタルトランスフォーメーションは、例えば、"as a service（サービスとしての提供）"に見られるように、攻撃と防御の両側面を強化するものです。これは、持続的標的型攻撃（APT）グループの専売特許であった高度な知識とリソースを必要とする複雑な攻撃が、より多くの脅威アクターがアクセスできるようにすることで、悪意ある活動を民主化しています」とHP Wolf Securityの脅威リサーチチームのシニアマルウェアアナリストで、本レポートの著者であるアレックス・ホランド（Alex Holland）は語っています。

このような複雑な攻撃は、何十億もの個人情報をダークウェブ市場でわずかな金額で入手できるようにしたデータ流出事件によっても促進されています。 ランサムウェアやデータ強奪攻撃で使用されるマルウェアの亜種やエクスプロイトの多くは、10ドル未満で販売されています。FBIの推計によると、2021年に米国で発生したサイバー犯罪の被害額だけで69億ドルという驚異的な数字になっているのも不思議ではないでしょう。[2]

「デジタルトランスフォーメーションは攻撃と防御の両側面を強化するものです」

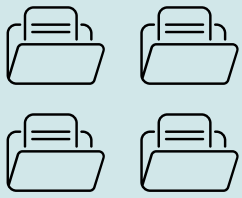
アレックス・ホランド（Alex Holland）
HPシニアマルウェアアナリスト

しかし、サイバー防御者に不利な状況にあるように感じられるかもしれませんが、防御力を改善する大きな機会があります。多くの場合、それは単に基本をマスターすることに他なりません。サイバー攻撃の影響が大きくなり、ツールやテクニックが進化した一方で、主要な攻撃経路は比較的変わっていません。 このことは、防御者があらゆる種類の脅威に挑戦し、レジリエンスを強化する機会を提供することになります。

サイバー犯罪の5つの事実

110億件

今日、ある情報漏えい通知サイトには110億を超える件数が記録[3]



3/4

を超えるマルウェア広告が$10未満

カスタムエクスプロイトの価格

$1,000-$4,000

92%

のサイバー犯罪者向けマーケットプレイスがトラブル解決サービスを提供し、買い手と売り手がレビューを残すことが可能

91%

のマーケットプレイスがエクスプロイトを$10以下で広告

セクション01

サイバーホビイストからサイバーシンジケートへ
金銭的動機によるサイバー犯罪の進化

サイバー犯罪コミュニティの原型が創られる

1990 年代半ばには、ハッカーのサブカルチャーが盛んになり、インターネット・リレー・チャット (IRC) [4] を通じて世界的な通信が行われるようになりました。当初、ハッカーは自分の技術力を自慢するために集まっていました。しかし、ドットコム・ブームが起きると、多くの人が真剣にお金を稼ぐことができるかもしれないと気づきました。

「昔は自分で考えて、技術的にできることをアピールしないと注目されませんでした。現在では、本当にコードを書くサイバー犯罪者はごく少数で、ほとんどはお金のためです。また、参入障壁が非常に低いため、ほとんど誰でも脅威アクターとなることができます。これは企業にとって悪いニュースです」

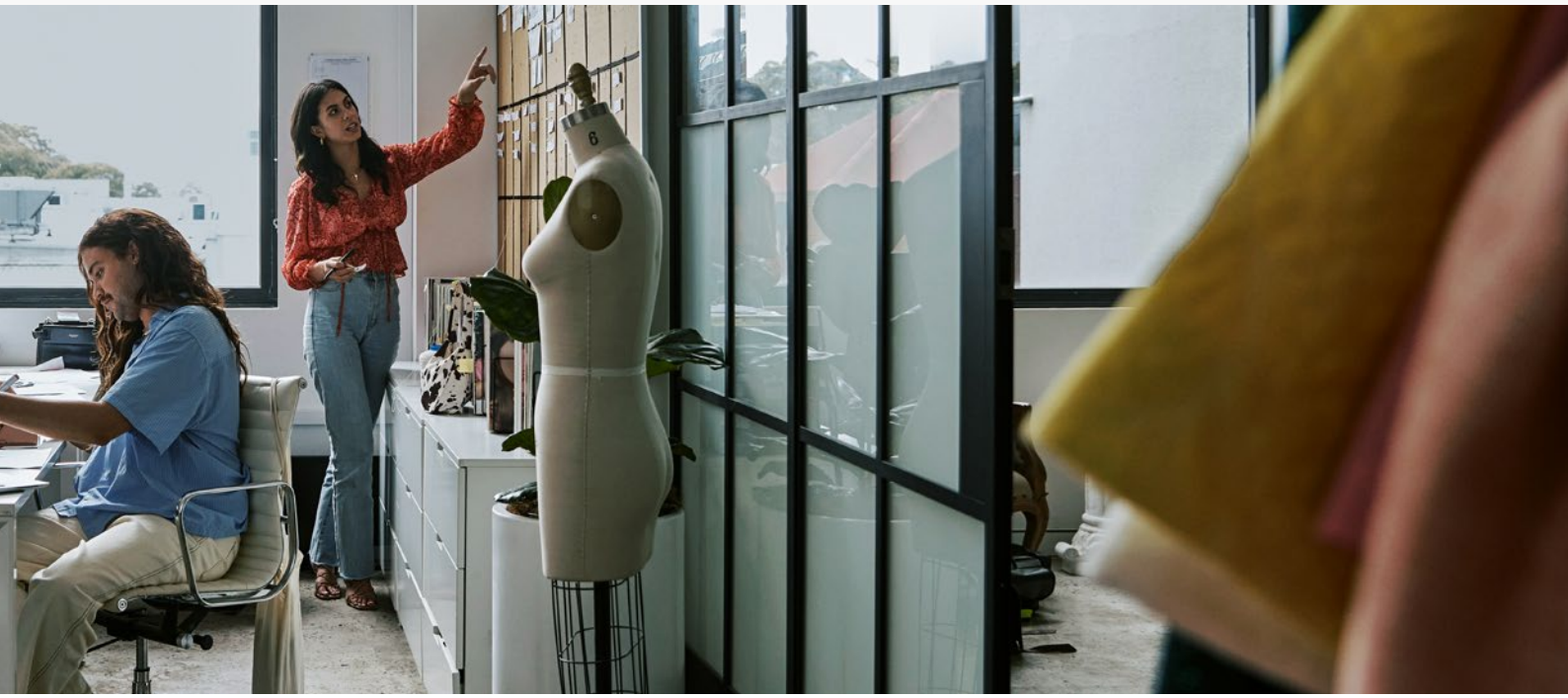
マイケル・カルセ (Michael Calce) 氏、HPセキュリティアドバイザリーボード・チェアマン、元ハッカー「MafiaBoy」

キーポイント

グローバルなハッカーコミュニティが形成、エクスプロイトや攻撃テクニックを共有し始める。

グループや個人が称賛しあい、技術力の高さをアピールしあう。

攻撃は通常、金銭的な動機によるものではなかった。



DIYサイバー犯罪キットがサイバー犯罪マーケットプレイスを開く

マルウェアキットの発売により、必要なスキルのレベルは低下し始めました。しかし、こうした「個人事業主」の詐欺師たちは、協力し合ってスキルをプールするようになるまでは、事業をスケールするための力をほとんど持ちませんでした。こうして、ハッカーは、システムへの侵入、マルウェアの開発、盗難金や暗号通貨の洗浄など、攻撃チェーンのさまざまな部分の完成度を高めることに特化するようになったのです。

キーポイント

コモディティ化したマルウェアキットにより参入障壁が低くなった。

サイバー犯罪者は特定分野に特化した新しいネットワークに強みをプールし始めた。

マネタイズは詐欺に焦点を当て、事業ではなくオンラインバンキングのユーザーをターゲットにした。

フォーカス

ZeuS と SpyEye

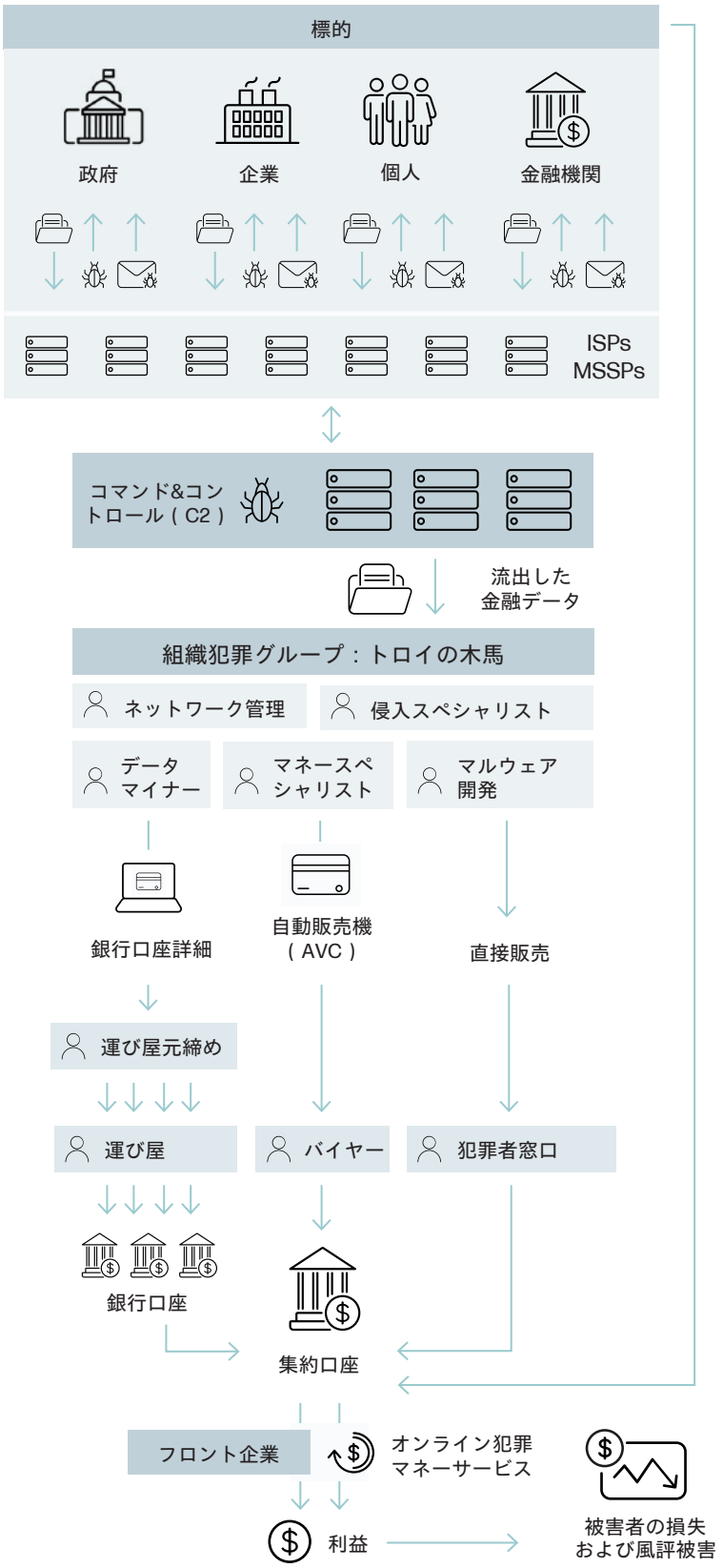
DIYバンキング型トロイの木馬キットZeuSは感染したコンピュータとのネットワークを構築、管理、制御することを可能にするボットネットを実現します。これによって、多くのオンライン銀行口座から現金を不正に引き出したり、クレジットカード番号を取得したりすることができます。[5]

ZeuSは8,000ドル[6]で販売されていましたが、2009年には、1,000ドルのSpyEye[7]と競合することになりました。SpyEyeは低価格であることに加え、ライバルZeuSが感染PCにあった場合にアンインストールする"kill ZeuS" 機能[8]が搭載されていました。

ZeuSとSpyEyeのプロジェクトは後に統合[9]されましたが、その後すぐにZeuSのソースコードが流出したことによりサイバー犯罪の競争が激化し、バンキング型トロイの木馬ICE IX、Citadel、KINSなど、多くのZeuS亜種が攻撃で利用されました。[10][11][12]

ZeuS	$8,000
SpyEye “kill ZeuS” 機能付き	$1,000

閉鎖的グループによるバンキング型トロイの木馬運用。英国のナショナル・サイバー・セキュリティ・センター（NCSC）による組織的犯罪グループとサイバー犯罪のエコシステムに関する研究を基に作成された、マルウェアエンタープライズに関わる役割、インフラ、商品、サービスの関係を示した図。[13]



新たなマネタイズ手法がランサムウェアに拍車をかける

法執行機関や銀行のセキュリティ専門家が優勢になり、時にはサイバー犯罪者からボットネットの制御を奪い取るようになると、BitcoinやMoneroなどの暗号通貨が台頭してきました。これらの暗号通貨は、サイバー犯罪者に追跡困難な新しい方法を提供し、身代金を支払わなければ人々のデータを破壊する攻撃を収益化することを可能にしました。

この破壊型攻撃の成長期には、サイバー犯罪者の協力体制も強化され、異なる不正なスキルを持つ者が特殊な製品やサービスを販売する支援エコシステムが確立されました。言い換えると、サイバー犯罪者は、Malware as a Service (MaaS) を提供し始めました。

キーポイント

攻撃アクターは、詐欺からデータ拒否や破壊型攻撃へと移行した。

サイバー犯罪の世界でもデジタル化された "as a service "モデルが導入され攻撃が容易に行えるようになった。

ランサムウェアがマネタイズの手法の一つとして台頭し始めた。

フォーカス

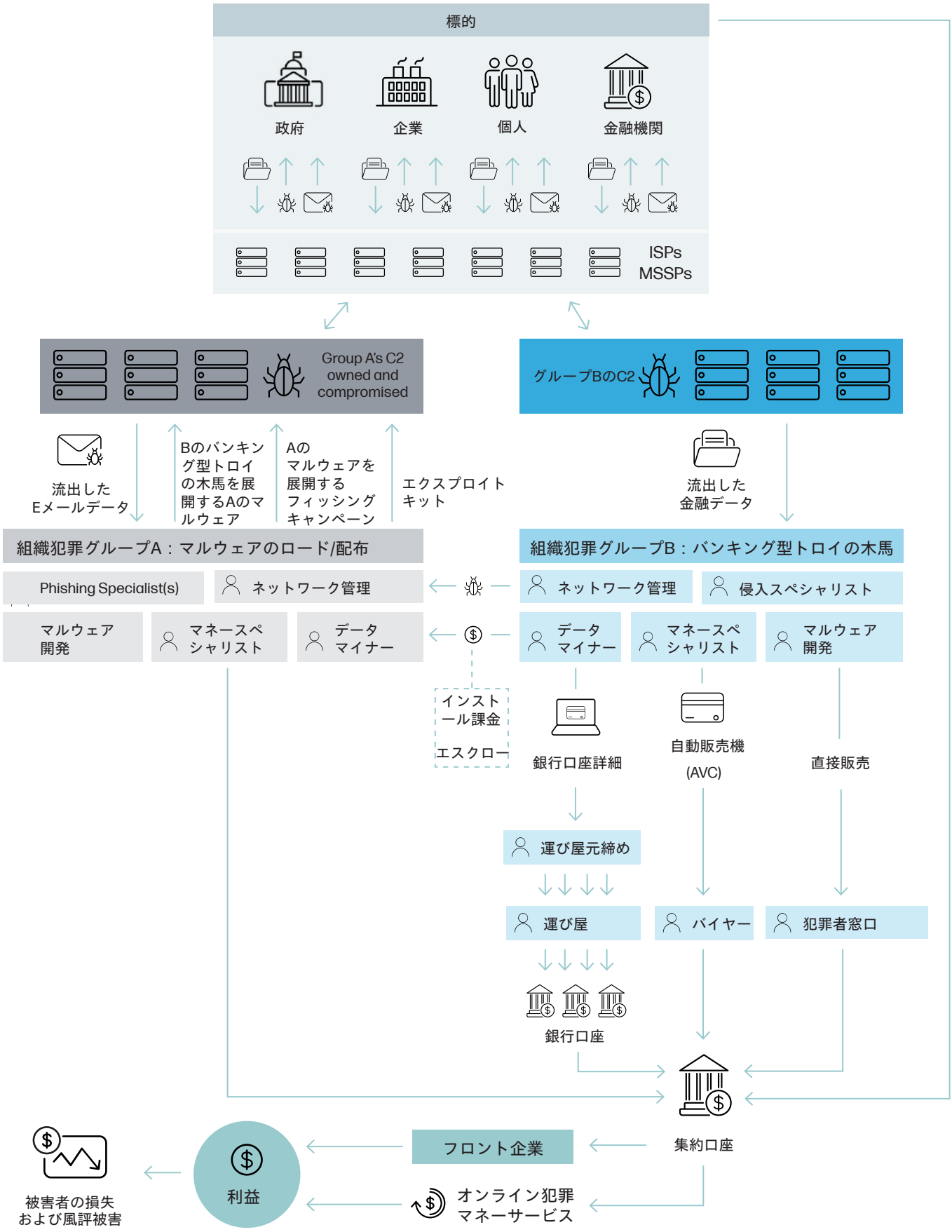
ランサムウェアの拡大

当初、CryptoLockerのようなランサムウェアの亜種は、ZeuS亜種Gameover ZeuSに依存し、すでに感染しているシステムをターゲットにしてマシンのデータ復号のために700ドルまたは同等のビットコインを要求する日和見攻撃を行っていました。[14]

WannaCryやNotPetyaのような攻撃は、破壊型手法で重要インフラを麻痺させることで、これを次のレベルに引き上げました。[15] [16]

Gameover ZeuSボットネットを経由して拡散したランサムウェア亜種CryptoLocker

マルウェアファミリーAが“access as a service（サービスとしてのアクセス）"としてBを配布する際の、マルウェア配布運用に関わるエンティティ、商品、サービスのマッピング図。[13]



支払いを最大化するために標的を定めた企業を狙う

2018年以降、サイバー犯罪はサービスおよびプラットフォームビジネスモデルへの移行を継続しており、脅威アクターは複雑なサプライチェーンを活用し、専門家の「プラグ&プレイ」コンポーネントを利用して攻撃を仕掛けています。

また、より組織化され標的が絞られてきています。犯罪者は、より大きな身代金の獲得や、インフラのより重要な部分の機能停止など、その影響を最大化するために、標的とするインフラの理解により多くの時間をかけています。.

「前世紀、経済は個人事業主から大量生産、サービスモデル、そしてAmazonのようなプラットフォームに移行しました」と、英国Surrey大学犯罪学上級講師のマイク・マクガイア（Mike McGuire）博士は述べてます。「サイバー犯罪経済は、これを25年足らずで実現したのです」

キーポイント

サイバー犯罪者は、複雑なサプライチェーンにおいて専門的サービスを提供している。

「プラグ&プレイ」のサービスやソリューションを使いキャンペーンを迅速に開始することができる。

影響を最大化し支払いを増加させるために標的を定めた企業が狙われる。

フォーカス

ランサムウェアの役割分担

ランサムウェアは現在、サイバー犯罪のマネタイズ方法として最適な選択で、犯罪者は直接・間接的に高いレベルで協力しながらプロとして運営しています。彼らは一般的に、以下のような専門的な役割に分類されます。

ディストリビューター
Eメールやエクスプロイトキットなどでマルウェアを配布する担当者。

アクセスブローカー
手に入れた不正アクセスを他の犯罪者に売る人。.

侵入スペシャリスト
レッドチームとも呼ばれる侵入テストに熟練した者。ネットワーク内の貴重なデータを特定・窃取し、ランサムウェアを展開できるポイントまで侵入を拡大し、最大限の被害を与える役割を担う。

マネタイザー
支払金の取り扱いや現金化に特化した脅威アクター。

セクション02

サイバー犯罪のコラボレーション - 今日のサイバー犯罪工場に潜入

サイバー犯罪の歴史を振り返ると、脅威アクターが知恵とリソースをプールすることで、攻撃がより巧妙になり被害が拡大することは明らかです。それを可能にする鍵となるのが、成熟したマーケットプレイスです。フォーラムやチャットルームでは、信頼に基づく交流が促進され、不正行為には罰則が適用されます。

我々は、ダークウェブやハッキングフォーラムを掘り下げ、これらの場がどのように運営され、サイバー犯罪者が攻撃の売買や議論にどのように利用しているかを理解したいと考えています。そのために、Forensic Pathways はTorネットワーク上のコンテンツを監視する自動クローラーを使用し、ダークウェブ・マーケットプレイスのリストを収集しました。3,500万以上のURLがインデックス化され、5,502のフォーラムと6,529のマーケットプレイスを含む、約33,000のアクティブなウェブサイトが見つかりました。

キーポイント

最も重要なのはアクセスとコントロール。

コモディティ化が参入障壁を下げる。

窃盗犯の「名誉」という皮肉 - なぜダークウェブでは評判が重視されるのか。

採用とコラボレーションのためのサイバー水飲み場。

企業が注目すべき4つの重要な調査結果

1. 最も重要なのはアクセスとコントロール

すべての侵入は、被害者のネットワークへの侵入ポイントを必要とし、アクセスとコントロールはサイバー犯罪の聖杯となっています。ソーシャルエンジニアリングは、システムへの侵入方法として最も好まれるものの1つです。2022年の第1四半期にHP Wolf Securityが隔離したマルウェアの69%は、無害なビジネス文書を装ったメッセージで、Eメール経由で送信されていました。[17]

また、ダークウェブから盗まれたユーザー名やパスワードを使って侵入する方法もあります。我々の調査によると、ダークウェブで販売されているリモートデスクトッププロトコル認証情報の平均価格は$5であることが分かっています。また、企業の情報漏えい事件で失われた情報を収集しているあるサイトには、110億件もの認証情報が掲載されています。[2]

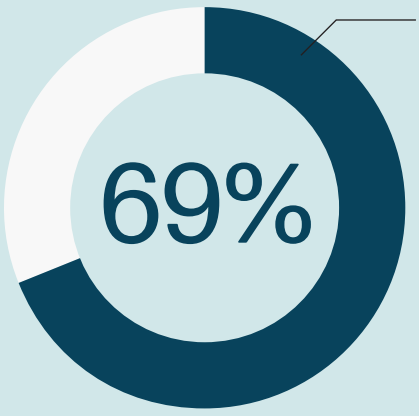
また、ソフトウェアのセキュリティ上の欠陥や弱点をエクスプロイトする方法もあります。我々の調査では、ダークウェブ上で議論されているこのような脆弱性が130件見つかり、最も深刻かつ実行が容易なものに焦点が当てられていました。

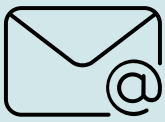
公開された欠陥には、Common Vulnerabilities and Exposures (CVE) 識別子が付与され、業界全体のCommon Vulnerabilities and Exposures Databaseで追跡されます。[18] CVEには、Common Vulnerability Scoring System（共通脆弱性評価システム）と呼ばれる、深刻度に関する10段階のスコアが設定されています。ダークウェブで議論されている平均レベルは7.4であることが分かっています。

最も人気のあるターゲットはWindows OS、Microsoft Office、Webコンテンツ管理システム、 Webサーバー、メールサーバーでした。脅威アクターは、ネットワークへの初期アクセスやシステムのコントロールを可能にする脆弱性に着目しています。

セキュリティ上の欠陥を修正するためにベンダーが発行するパッチでさえ、犯罪者の手助けになることがあります。HPパーソナルシステムズ事業セキュリティ部門グローバル責任者であるDr. イアン・プラット（Ian Pratt）は、「一部のサイバー犯罪者は、多くの組織がパッチの展開に手間取ることを知っており、新しい脆弱性の発見にリソースを投入するよりも、ベンダーの新しいパッチを注視し、脆弱性を理解しエクスプロイトを作成するために、リバースエンジニアリングを行っています」と述べています。

2022年Q1：





HP Wolf Securityが隔離したマルウェアのうち、Eメール経由で送信されたものの割合。[17]

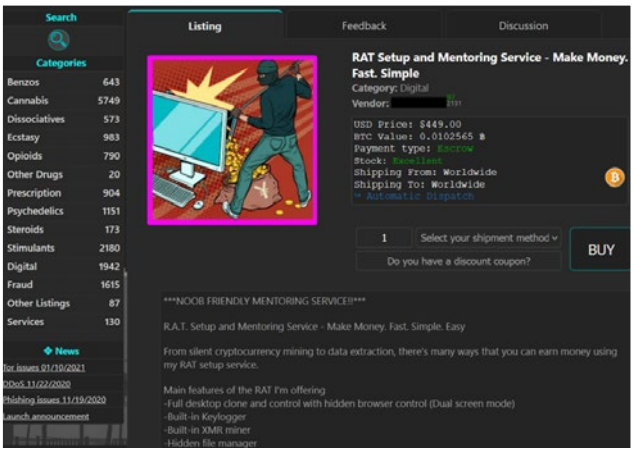
企業のデータ漏洩で失われた情報を収集する、あるサイトに含まれていた認証情報[2]は

110億件

2. コモディティ化が参入障壁を下げる

エクスプロイトやマルウェアが安価なコモディティとなった今、新たな金儲けの方法が生まれつつあります。サイバー犯罪者は、必要な攻撃ソフトウェアをレンタルし、マルウェアのベンダーに手数料を支払うことで、ランサムウェアの成果を共有することができるようになりました。マルウェアの作者は、ユーザーに助言サービスや必要な知識を説明した詳細な「プレイブック」へのアクセスを提供することで、自社製品の差別化を図っているほどです。

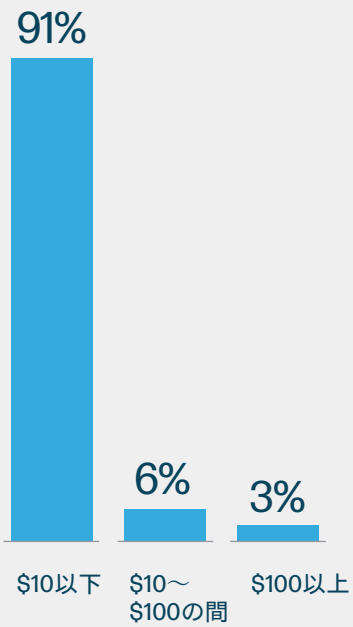
このような動きは、多くのサイバー犯罪者が、もはやマルウェア・ツールを販売するのではなく、新たなサービス主導型経済において、自らの専門知識やスキルを販売する方向へとシフトしていることを示しています。



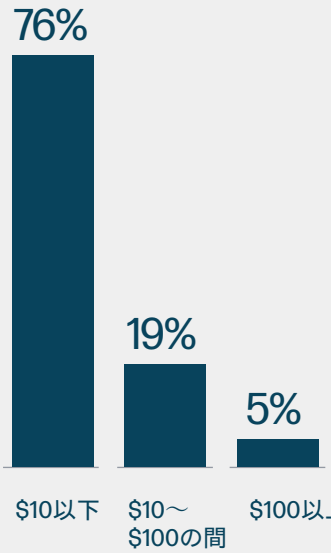
マルウェア助言サービスの販売

サイバー犯罪の低コスト化

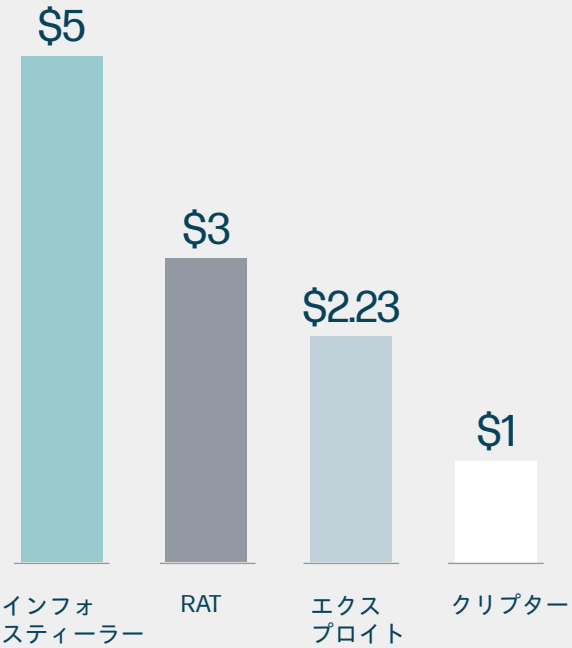
ダークウェブで宣伝されている174個のエクスプロイトのうち：



1,653個のマルウェア広告のうち：



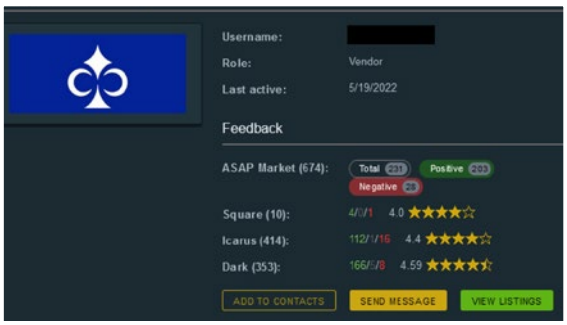
サイバー犯罪マーケットプレイスにおけるマルウェアの平均価格



3. 窃盗犯の「名誉」という皮肉 - なぜダークウェブでは評判が重視されるのか

サイバー犯罪者のマーケットプレイスでは、信頼が不可欠であるため、ベンダーとバイヤーのレピュテーションスコアやカスタマーレビューなど、公正な取引を促す高度なメカニズムが開発されました。

また、匿名のTorネットワーク上のWebサイトの平均寿命はわずか55日であるため、マーケットプレイスはセラーのフィードバックを記録する方法を開発し、マーケットが閉鎖または停止された場合でも失われないようにしました。



他のマーケットからのベンダー評価スコアを表示するマーケットプレイスのリスト

4. 勧誘とコラボレーションのためのサイバー水飲み場

潜在的な顧客、パートナー、従業員と簡単につながることができることは、サイバー犯罪のエコシステムにとって不可欠な要素です。フォーラム、専門家のチャットグループ、暗号化された閉じたネットワークは、サイバー犯罪者がつながりを作り、パートナーを勧誘するためのハブを提供しています。

「ダークウェブは、最先端の顧客サービスを提供するサイバー犯罪者の最前線であり、エスクロー決済などの機能が、過密な市場においてセラーを差別化しています」とマイク・マクガイア（Mike McGuire）博士は述べています。

「しかし、その背後には、一握りの強力な集団がトップから糸を引いて、情報共有や勧誘を行い、最大限の成果を上げるため、あるいは慎重に選んだ標的を破壊するための多国籍サイバーシンジケートを運営する、秘密の「見えないネット」が存在します。」

ベンダーのレピュテーション管理に関するダークウェブ調査結果

100%

のサイバー犯罪マーケットプレイスにはベンダーのフィードバックスコアがある。

77%のサイバー犯罪マーケットプレイスは、「ベンダーボンド」（販売許可証）を要求しており、その費用は最大で3,000ドル。

92%のサイバー犯罪マーケットプレイスが第三者によるトラブル解決サービスを提供。

85%

がエスクロー決済を利用。 - バイヤーが合意した製品またはサービスを受け取ってから、セラーは支払いを受け取る。

セクション03

ホライゾン・スキャニング - 今後5〜10年でサイバー犯罪はどう変わるか？

コラボレーション、専門化、プロフェッショナル化が進む中で、今大きな問題となっているのは「脅威の環境は今後どのように進化していくのか?」ということです。ホライゾン・スキャニング手法により、我々はITセキュリティのプロフェッショナルが認識すべき4つの主要な予測を特定しました。

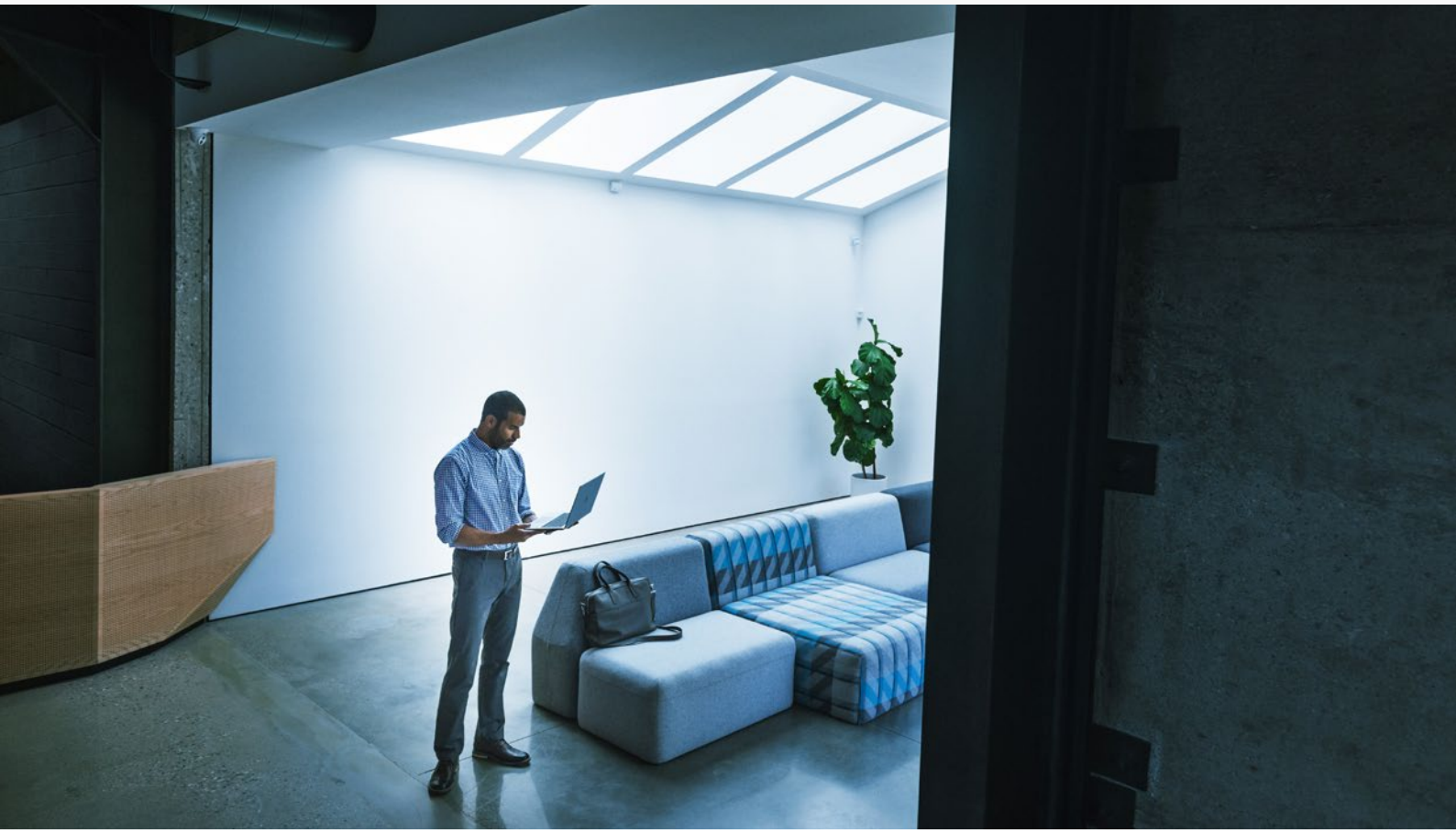
キーポイント

破壊的なデータ拒否攻撃の被害がさらに拡大する。

プロフェッショナル化が進み、標的型攻撃が増加する。

先端テクノロジーが武器にも盾にもなる。

攻撃者は投資収益率を高めるために効率化推進に注力する。



1. 破壊的なデータ拒否攻撃の被害がさらに拡大する

ハイブリッドワークとデジタルトランスフォーメーションの両方を取り入れる企業が増える中、攻撃者が広がり続けるアタックサーフェスを利用する可能性が高くなります。IoTデバイスとデータが止められず非常に重要な部門に対して、データ破壊の脅威を利用した恐喝攻撃が行われることが予想されます。

また、身代金を要求せずにデータを消去しシステムを無効化するマルウェア[19][20]によるShamoon（2012年）、Michelangelo（1991年）に続いて、2021年末から2022年にかけてのワイパー攻撃などの重要インフラへの破壊型攻撃も復活しています。

2. プロフェッショナル化が進み、標的型攻撃が増加する

サイバー犯罪の技術は、過去10年間で、北朝鮮が運営するものなどの、国家を基盤とする持続的標的型攻撃（APT）グループの技術に収斂されてきています。[21]これらのグループは、被害者のネットワークを深く理解した上で、人的操作を伴う攻撃を行うことを特徴としており、我々の調査では、この境界線の曖昧さは今後も継続することが示唆されています。

マイク・マクガイア（Mike McGuire）博士によると、北朝鮮はハッキンググループLazarusを通じてサイバー犯罪に投資し、金融制裁を回避するためにサイバー犯罪を利用する方法を先導しているという。「北朝鮮は、貧しい国々が経済を発展させるだけでなく、制裁を回避する可能性を示す道を示したことは間違いないでしょう。 賽は投げられました。 この4年間で、北朝鮮は決定的に変わりました」とマイク・マクガイア（Mike McGuire）博士は述べています。

3. 先端テクノロジーは武器にも盾にもなる

また、サイバー犯罪者は、新しい技術や発展途上の技術を利用した攻撃を導入することが予想されます。その中には、攻撃者がディープフェイクを使ってフェイクニュースを流し、AIの学習データを改ざんすることで組織に損害を与えるといった、人工知能（AI）によるデータの完全性に対する攻撃へのシフトが含まれる可能性があります。このことは、組織が変更できない強固な監査証跡を維持する必要性を強調しています。

Web3のような新しいプラットフォームは、ユーザーの個人データに対する新しいレベルの管理策を提供する可能性があります。サイバー犯罪者にとっては、サイバー犯罪を支援するレピュテーション・システムを構築し、複数のマーケットプレイスやフォーラムでレピュテーションを簡単に転送することでコラボレーションを拡大する新しい機会を意味する可能性があります。

さらなる警戒すべきリスクは、ハッカーがブルートフォース攻撃の高速化にクラウドの分散コンピューティングを利用する「クラウドクラッキング」拡大の可能性です。もし、これが量子コンピュータにまで拡大されれば、サイバーセキュリティに壊滅的な影響を及ぼす可能性があります。なぜなら、超高速コンピュータが、今日の電子商取引、銀行、通信を保護している古典的暗号アルゴリズムの解読に利用されるからです。[22]

4. 攻撃者は投資収益率を高めるために効率化推進に注力する

ダークウェブで攻撃者が議論しているのを見かけた脆弱性の多くは、数年前のものでした。2022年初めにHP Wolf Securityが隔離したトップ3のエクスプロイトも、少なくとも4年前のものでした。[17] 古い脆弱性を悪用する機会のウィンドウがこれほど大きいと、新しい脆弱性を武器化するための投資対効果は低くなります。 その代わりに、サイバー犯罪者は侵入のスピードと効率を高めることに注力する可能性が高くなります。

将来的には、例えば、攻撃者がAIや機械学習の技術を利用して、標的型スピアフィッシング攻撃を大規模に行えるようになる可能性があります。攻撃者は、AI機能を活用した攻撃ツールを導入することで、組織の重要人物にフィッシングメールをカスタマイズし、ネットワークへの最初の足掛かりを得た後の活動を加速することができます。

セクション04

基本をマスターし、レジリエンスを計画し、リスクを減らしゲームに勝つ可能性を高めるためにコラボレーションを行う

では、組織、企業、政府は、どのようにしてサイバー犯罪を招く可能性のレベルを下げればよいのでしょうか。専門家パネルによると、サイバーレジリエンスを向上させるには、3つの重要な方法があることがわかりました。

キーポイント

基本をマスターしてサイバー犯罪の機会を減らす。

ゲームの勝利に集中する。

サイバー犯罪はチーム戦：サイバーセキュリティも同様。

1. 基本をマスターしてサイバー犯罪の機会を減らす

ベストプラクティスをフォローする

すべての組織は、多要素認証を確実に導入し、従業員がインストールできるソフトウェアを厳密に管理し、パッチのテスト、承認、導入、検証を迅速に行う必要があります。

アタックサーフェスを削減する

Eメール、Web 閲覧、ファイルのダウンロードなど、主要な攻撃経路からのリスクを軽減することに重点を置く。隔離技術のように、経路全体からリスクを除去しつつ、従業員のワークフローに支障をきたさないセキュリティ対策に投資する。

自己修復型ハードウェアを活用してレジリエンスを高める

侵入が起こることを考えれば、攻撃からできるだけ早く回復するために、レジリエンスのある自己修復型ハードウェアを使用することは理にかなっています。

「CISOは膨大な心配事のリストを持っています。セキュリティ機能を組み込むことで、そのリスト減らすことができれば、それに越したことはないでしょう。そして、結局は人間が最大の弱点です。」

「このため、組織はセキュリティをスタックとしてとらえ、テクノロジーを合理化し、ハードウェアからレジリエンスを構築してアタックサーフェスを削減し、個人から責任を取り除く必要があります」

マイケル・カルセ（Michael Calce）、HP セキュリティアドバイザリーボード・チェアマン、元ハッカー「MafiaBoy」

2. ゲームの勝利に集中する

最悪の事態に備える

防御だけでなく、攻撃された場合の事業継続性にも着目する。事前に準備を行い、攻撃者がどのような手口を使うかを予測することで、組織はより迅速に復旧することができます。

従業員やパートナーによるリスクを押さえる

あなたのゲームは、あなたのチームによってのみ強くなります。組織は、サプライヤーのセキュリティを吟味し、ソーシャルエンジニアリングについて従業員を教育するためのプロセスを整備する必要があります。

プロセスを重視しリアクションを練習する

攻撃への対応をリハーサルすることで、問題を特定し、改善し、より良い準備をすることができます。「我々は、統計データを監視することから脱却し、ゲームに勝つことにもっと集中する必要があります。優れた統計データを持ち、優秀な人材を擁するチームがあっても、重要なのは、肝心なときに勝てるかどうかです」とHPセキュリティアドバイザリーボードメンバーでDeloitteパートナー ロバート・マッセ（Robert Masse）氏は述べています。

「CISOにとって、これはあなたのチームは、攻撃が深刻化する前に、それを検知、予防、復旧することができるか？ということを意味します。定期的な模擬演習の実施、パフォーマンスのモニタリング、戦術や敵の潜在的作戦の検討など、これらは勝率を上げるために有効な手段です」

「最悪の事態が発生し、脅威アクターが防御を破った場合においても、インシデントレスポンス計画を始動するのが初めてという事であって欲しくないものです」

「誰もが自分の役割を理解し、従うべきプロセスに精通していることを確認することは、最悪の影響を抑え込むのに大いに役立つでしょう」

ジョアンナ・バーキー（Joanna Burkey）、HP最高情報セキュリティ責任者（CISO）

3. サイバー犯罪はチーム戦：サイバーセキュリティも同様

仲間に相談する

攻撃者は、これまで以上にコラボレーションをしています。防御側もそうあるべきです。脅威の情報をリアルタイムで同業他社と共有することがますます重要になっています。「セキュリティ対策により、一般的なマルウェアを阻止することができますが、最も危険なマルウェアは、アンダーグラウンドを捜索したときにのみ現れます」とHPセキュリティアドバイザリーボードメンバージャスティン・ボーン（Justine Bone）氏は述べています。「しかし、ほとんどの組織では、そのための時間やリソースを確保することができません。業界としてこの不透明な世界を理解するためにもっと投資し、その情報を仲間と共有することで、より効果的に防御し阻止することができるのです」

サードパーティセキュリティサービスを活用する

防御チームは、セキュリティ評価者や侵入テスト会社などのサードパーティを活用すべきです。これらは、弱点や対処が必要な重大なリスクを浮き彫りにすることができます。

脅威インテリジェンスを活用しホライゾン・スキャンを積極的に行う

アンダーグラウンド・フォーラムでの公開ディスカッションを監視することは、ネットワーク防御担当者にとって、組織が直面する脅威を理解し、防御策を検討する機会となります。「脅威を取り巻く環境を積極的に把握することが重要です。あまりに内向きになりすぎると、これから何が起こるかわからなくなります」とHP Labsセキュリティリサーチ担当チーフテクノロジストのボリス・バラシェフ（Boris Balacheff）は述べています。

「サイバーセキュリティ・コミュニティがその規模と共有への意欲において成長したことを目にすることが、希望を抱く最大の理由の一つです。敵対者と同じように、コラボレーションを行いと知識を共有することは、攻撃の激しい流れに対抗するために不可欠です」

「脅威の状況を積極的にスキャンし、洞察を仲間と共有することで、より安全で強靭なデジタル世界を共に構築することができます」

アレックス・ホランド（Alex Holland）
HPシニアマルウェアアナリスト

メソドロジー

HPは、ダークウェブ調査会社Forensic Pathwaysに委託して独立した調査を実施しました。

同社は、Torネットワーク上のコンテンツを監視する自動クローラーを使用して、ダークウェブマーケットプレイスのリストを収集しました。同社のダークサーチエンジン・ツールは、3,500万以上のURLのスクレイピングデータがインデックスされています。

収集されたデータは、Forensic Pathwayのアナリストによって調査、検証されました。このレポートでは、5,502のフォーラムと6,529のマーケットプレイスを含む、ダークウェブ全体で約33,000のアクティブなウェブサイトを分析しました。2022年2月から3月にかけて、Forensic Pathwaysは、Torネットワーク全体で最近アクティブになった17のサイバー犯罪マーケットプレイス、Torネットワークとウェブを横断する16のハッキングフォーラムとそのデータを含む関連リストを特定しました。

HP Wolf Security について

HP Wolf Security[α]はハードウェアで強化されたセキュリティとエンドポイントに特化したセキュリティサービスによる新しいタイプのHPのポートフォリオで、組織がサイバー犯罪者からPC、プリンター、そして人々を保護できるように設計されています。

HP Wolf Securityは、ハードウェアレベルから始まり、ソフトウェアやサービスに至る、包括的なエンドポイント保護とレジリエンスを提供します。https://jp.ext.hp.com/business-solution/wolf/をご覧ください。

[α] HP SecurityはHP Wolf Securityになりました。セキュリティ機能はプラットフォームによって異なりますので、詳細は製品データシートをご覧ください。

Forensic Pathwaysについて

Forensic Pathways Ltd. は、脅威インテリジェンス、サイバーセキュリティサービス、ダークウェブ監視、ソーシャルメディア調査を専門としています。

2016年 Forensic PathwaysはTorネットワークや隠しサービス（ダークウェブ）からのデータスクレイピングを開始しました。その「ダークサーチエンジン」は、ダークウェブを安全に検索し、関心のあるコンテンツを監視するために使用することができます。

サイバー犯罪に関する主な用語集

持続的標的型攻撃 (APT) – 標的のネットワークに不正にアクセスし、長期間にわたって検知されないようにする、高度な能力を持つ脅威アクター。

防弾ホスティング(BPH) – マルウェアなどほとんどすべての種類のコンテンツのホスティングを許可し、顧客のプライバシーを確保するための措置を講じるウェブホスティングプロバイダー。

ダークウェブ – 検索エンジンにインデックスされていないインターネットの一部分。

DDOS (分散型サービス拒否攻撃) – 多くのシステムからの要求を殺到させることにより、システムやサービスを利用できなくする攻撃。

エスクロー・サービス – ある取引、およびその取引の一部として合意された条件が満たされると、第三者が資金の受払いを行う取り決め。

エクスプロイト – アプリケーションやシステムの脆弱性を利用して、意図しない動作や予期しない動作を引き起こすコード、データ、コマンド

エクスプロイト・ビルダー – ユーザーがコーディングせずにエクスプロイトを作成するためのツールで、サイバー犯罪者が脆弱性を持つシステムへのアクセスへのアクセスを得る際のハードルを下げる。

完全に検出不可(FUD) – マルウェアが検知を回避する能力。

モノのインターネット (IoT) – インターネットを通じてデータを送受信することができる、日用品に埋め込まれたコンピュータ。

マルウェア – コンピュータやネットワークに悪影響を与えるよう設計されたソフトウェア。例えば、コンピュータや ネットワークの 損傷、破壊、データの窃取など。

マルウェア・アズ・ア・サービス – サイバー犯罪者が売買する専門的なマルウェア商品とサービスのエコシステム。

パッカー – 実行ファイルを圧縮してサイズを小さくするツール。マルウェアの難読化に使われることが多い。

フィッシング – ソーシャルエンジニアリングのテクニックの一つで 攻撃者が被害者をだまして、機密情報を開示させたり、コンピュータをマルウェアに感染させるために、Eメールを使用する方法。

パープルチーミング – 組織のセキュリティを最大化するために、レッドチームとブルーチーム (防御的なサイバーセキュリティの専門家) が緊密に連携する方法論。

ランサムウェア – 金銭が支払われるまで、コンピュータ・システムへのアクセスを遮断するマルウェア。

リモートアクセス型トロイの木馬(RAT) – 攻撃者がコンピューターを遠隔操作できるようにするマルウェア。

レッドチーム – 組織のシステム、プロセス、人材にアプローチしセキュリティリスクを特定する、攻撃的なサイバーセキュリティの専門家集団。.

リモート デスクトップ プロトコル (RDP) – ネットワーク接続により、他のコンピュータにリモートで接続し、ディスプレイを見たり、デバイスにコマンドを入力したりすることができるプロトコル。

スピアフィッシング – 組織内の特定の個人やグループを狙ったフィッシングの一種。

インフォスティーラー – システムからユーザー名やパスワードなどの機密情報を収集するマルウェア。

TOR – The Onion Routerの略で、匿名通信を可能にする無料のオープンソースソフトウェア。

トロイの木馬 – 正規のソフトウェアに偽装したマルウェア。

ゼロデイ – 例えば、システムへの不正なアクセスなどの、攻撃者の悪意ある目標の達成に悪用することができる、これまでに発見されていないソフトウェアの脆弱性。

リファレンス

[1] Clarifyi. (2022). *The forensic approach to Threat Intelligence* [Online]. Available: https://clarifyi.com/

[2] Federal Bureau of Investigation. (2022). *Federal Bureau of Investigation Internet Crime Report 2021* [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[3] T. Hunt. (2022). *Have I Been Pwned* [Online]. Available: https://haveibeenpwned.com/

[4] Radware. (2022). *IRC (Internet Relay Chat)* [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/irc-internet-relay-chat/

[5] Trend Micro. (2015, Aug. 31). *A Brief History of Notable Online Banking Trojans* [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

[6] B. Acohido. (2014, Feb. 5). *Lessons from the capture of SpyEye's mastermind* [Online]. Available: https://eu.usatoday.com/story/cybertruth/2014/02/05/lessons-capture-spyeye-mastermind/5182697/

[7] Federal Bureau of Investigation. (2014, Jan. 28). *Botnet Bust: SpyEye Malware Mastermind Pleads Guilty* [Online]. Available: https://www.fbi.gov/news/stories/spyeye-malware-mastermind-pleads-guilty

[8] B. Krebs. (2010, Apr. 1). *SpyEye vs. ZeuS Rivalry* [Online]. Available: https://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/

[9] B. Krebs. (2010, Oct. 24). *SpyEye v. ZeuS Rivalry Ends in Quiet Merger* [Online]. Available: https://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

[10] D. Fisher. (2011, May 10). *Zeus Source Code Leaked* [Online]. Available: https://threatpost.com/zeus-source-code-leaked-051011/75217/

[11] A. K. Sood, R. J. Enbody, R. Bansal. (2012, Aug. 1). *Inside the ICE IX bot, descendent of Zeus* [Online]. Available: https://www.virusbulletin.com/virusbulletin/2012/08/inside-ice-ix-bot-descendent-zeus

[12] B. Krebs. (2013, Jul. 25). *Haunted by the Ghosts of ZeuS & DNSChanger* [Online]. Available: https://krebsonsecurity.com/2013/07/haunted-by-the-ghosts-of-zeus-dnschanger/

[13] National Cyber Security Centre. (2017, Apr. 9). Cyber crime – understanding the online business model [Online]. Available: https://www.ncsc.gov.uk/pdfs/news/ncsc-publishes-new-report-criminal-online-activity.pdf

[14] United States Department of Justice. (2014, Jun. 2). *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* [Online]. Available: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[15] BBC News. (2017, May 13). *Massive ransomware infection hits computers in 99 countries* [Online]. Available: https://www.bbc.co.uk/news/technology-39901382

[16] MITRE Corporation. (2022, Apr. 25). *NotPetya* [Online]. Available: https://attack.mitre.org/versions/v11/software/S0368/

[17] HP Wolf Security. (2022,年5月25日). *HP WOLF SECURITY脅威インサイトレポート　2022年Q1* [Online]. Available: https://jp.ext.hp.com/blog/security/product/hp-wolf-security-threat-insights-report-q1-2022/

[18] MITRE Corporation. (2022). *CVE* [Online]. Available: https://cve.mitre.org/

[19] MITRE Corporation. (2021, Feb. 9). *Shamoon* [Online]. Available: https://attack.mitre.org/versions/v11/software/S0140/

[20] Trend Micro. (2017, Mar. 6). *The Michelangelo Virus, 25 Years Later* [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-michelangelo-virus-25-years-later

[21] L. Constantin. (2019, Apr. 10). *Cybercrime groups raise the bar for security by borrowing APT techniques* [Online]. Available: https://www.csoonline.com/article/3387943/cybercrime-groups-raise-the-bar-for-security-teams-by-borrowing-apt-techniques.html

[22] J. Chu. (2016, Mar. 3). *The beginning of the end for encryption schemes?* [Online]. Available: https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303