

The screenshot shows the FireEye website with a red header bar containing the FireEye logo and navigation links: Products, Services, Solutions, Partners, Support, Resources (which is highlighted in red), and Company.

Threat Intelligence: Attack Groups

- Red Line Drawn: China recalculates its use of cyber espionage**
- Report that details recent Chinese cyber operation findings despite the September 2015 agreement between President Barack Obama and Chinese President Xi Jinping.

Follow the Money: Dissecting the operations of the cyber crime group FIN6

Download the report to learn about FIN6's operations to steal payment card data and sell that information to an underground card shop.

Pinpointing Targets: Exploiting web analytics to ensnare victims

Threat intelligence on how attackers alter websites and redirect visitors to a profiling script called WITCHCOVEN.

HAMMERTOSS: Stealthy tactics define a Russian cyber threat group

Threat intelligence on the history, targets, and methodology of the Russian APT29 group that created the elusive malware backdoor HAMMERTOSS.

Threat Intelligence: Technologies

- Overload: Critical lessons from 15 years of ICS vulnerabilities**
- Download this threat intelligence report for trends in Industrial Control Systems (ICS) vulnerability disclosure and outlook and recommendations for ICS asset owners.

Connected Cars: The open road for hackers

Find out the top 5 risks posed to interior and exterior vehicle systems.

Matryoshka Mining: Lessons from Operation RussianDoll

Get tools and techniques to help security professionals recognize and conduct enhanced malware analysis.

FireEye Labs Report: 2015 holiday season email campaigns

FireEye Labs collected data on the six most prominent malware families delivered during the 2015 holiday season.

SYNful Knock: A Cisco implant

Insight into how attackers use Cisco routers as a threat vector to establish a foothold and compromise data.

FireEyeのような研究者が組織犯罪や国家的アクターの活動を報告しています。
(スクリーンショットはfireeye.comの許可を得て使用)

国家的アクターは、資金を提供したり保護してくれる政府、軍、またはセキュリティサービスの手の届く場所で活動し、「もっともらしい否認」を維持します。国家的アクターは、独立したグループやハクティビストを装います。彼らは、他の国家を巻き込むうとする偽旗作戦キャンペーンを実行することもあります(media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/11/20151759/KSB2019_APT-predictions-2020_web.pdf)。

犯罪シンジケートと競合企業

多くの国で、サイバー犯罪のインシデント数と損失額が、物理的犯罪を上回っています。犯罪シンジケートは、被害者と異なる裁判管轄権からインターネットを介してサイバー犯罪を行ったため、告発する場合の手続きの複雑さが増大しています。シンジケートは、犯罪により利益を得る機会を探していますが、彼らの典型的な活動は金融詐欺（個人および企業が対象）と恐喝です。

競合企業によるスパイ行為の多くに国家的アクターが関わっていると考えられていますが、犯罪ビジネスが競合企業に対してサイバースパイ行為を行っている可能性も考えられなくありません。こういった攻撃は、窃盗や、競合企業の事業を混乱させたり評判を傷つけることを目的としている可能性があります。競合企業による攻撃は、最近転職してきた従業員がインサイダー情報を持ち込むことで簡単に実行される可能性があります。

インサイダー脅威アクター

脅威アクターの多くは、標的とするネットワークの外部から操作を行います。その場合、外部脅威アクターは、合法な許可を得ることなくシステムに侵入する必要があります。インサイダー脅威は、組織によって認められ、何らかのアクセス許可を得ている脅威アクターによって行われます。内部の脅威グループは、従業員など永久的特権を持つインサイダーと、契約社員や訪問者など一時的特権を持つインサイダーに区別できます。カーネギーメロン大学のコンピューター緊急対応チーム(CERT)は、悪意のあるインサイダーを次のように定義しています。

組織のネットワーク、システム、またはデータへのアクセス権を現在所有しているまたは以前所有していたことがあり、組織の情報または情報システムの機密性、完全性、または可用性に悪影響を及ぼす方法で、そのアクセス権を意図的に超えて、または誤って使用する、現在または以前の従業員、契約社員、またはビジネスパートナー。[\(insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html\)](https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html)



元インサイダーには、現在他社で働いている元従業員や、解雇され不満を抱いている元従業員など、曖昧なケースもあります。これらは、効果的なオフボーディング管理が行われていない場合、内部脅威や、インサイダーの知識を持つ外部脅威として分類され、場合によっては残存する権限も持つことになります。

CERTは、悪意のあるインサイダー脅威の主な動機を妨害行為、金銭的利益、ビジネスの優位性として識別します。外部の脅威と同様に、インサイダー脅威は、日和見型または標的型のいずれかである可能性があります。また、ここでの主要ポイントは、例えば不満を抱いていたり、詐欺を犯す可能性のある従業員というように、動機を特定することです。請求書の改竄や資金の流用といったキャンペーンを計画し実行する従業員は、構造的攻撃を行っていることになり、給料のデータベースで何度もパスワードを推測しているうちにネットワークでファイル入手できることに気づいた従業員は、日和見型攻撃を行っていることになります。インサイダー脅威が外部脅威アクターまたはグループと協力して活動している可能性も評価しなくてはなりません。

インサイダー脅威は、「意図的ではない」可能性があります。意図的ではないまたは不注意から発生するインサイダー脅威は、独立した脅威アクターではなく、外部脅威アクターまたは別の「悪意のある」内部脅威アクターがエクスプロイトするためのベクトルです。ユーザーのパスワード管理が不十分であるなど、意図しない脅威は通常、認識の欠如や不注意が原因で発生します。意図しないインサイダー脅威のもう一つの例は、**シャドーIT**の概念で、IT部門の許可を取ったり、調達とセキュリティ分析プロセスを経ることなくユーザーがコンピューターハードウェアやソフトウェアを購入したり、職場に持ち込んだ場合がそれに該当します。シャドーITの問題は、ユーザーが容易に入手できるクラウドサービスやモバイルデバイスが急増することによって悪化しています。シャドーITによって監視されていない攻撃対象領域が新たに出来てしまい、悪意のある敵対者にエクスプロイトされる危険が生じます。

攻撃対象領域と攻撃ベクトル

攻撃対象領域とは、悪意のある脅威アクターが脆弱性のエクスプロイトを試みる可能性のあるすべてのポイントが該当します。攻撃対象領域を評価する際は、脅威アクターのタイプを考慮する必要があります。外部脅威アクターに対する攻撃対象領域は、インサイダー脅威に対する攻撃対象領域よりかなり小さい（あるいは小さいはずである）という特徴を備えています。ネットワークの攻撃対象領域がすべてであると考がちですが、個人のソフトウェアアプリケーションの攻撃対象領域についても分析が行われます。攻撃対象領域を最も小さくするには、アクセスを制限することになります。すなわちいくつかの既知のエンドポイント、プロトコル/ポート、サービス/方法だけを許可します。それぞれの脆弱性について評価する必要があります。

脅威アクターの観点から見ると、攻撃対象領域の様々な部分が潜在的な攻撃ベクトルに該当します。攻撃ベクトルとは、脅威アクターが安全なシステムに対するアクセス権を得るために使用する経路です。多くの場合、アクセス権を得ることで、ターゲット上で悪意のあるコードを実行することができるようになります。

- ダイレクトアクセス — これは物理的、または局所タイプの攻撃です。脅威アクターは、例えばロックされていないワークステーションをエクスプロイトしたり、ブートディスクを使用して悪意のあるツールのインストールを試みたり、デバイスを盗んだりする可能性があります。
- リムーバブルメディア — 攻撃者は、USBメモリやメモリカードにマルウェアを仕込んだり、従業員をだましてPC、ラップトップ、スマートフォンに媒体を接続するように仕向けたりします。エクスプロイトの中には、単に媒体に接続するだけで、マルウェアを実行してしまうものもあります。多くの場合、攻撃者にとって必要なのは、従業員が脆弱なアプリケーションでファイルを開くか、設定プログラムを実行してくれることです。

- 電子メール — 攻撃者は、電子メールまたは添付が可能なその他の通信システムを介して悪意のあるファイルを送信します。ユーザーが添付を開くよう仕向ける際、攻撃者は、ソーシャルエンジニアリング技術を使用する必要があります。
- リモートおよびワイヤレス — 攻撃者は、リモートアクセスやネットワークへのワイヤレス接続のための認証情報を入手するか、認証に使用するセキュリティプロトコルを破ります。あるいは、アクセスポイントのような信頼できるリソースをスプーフィングし、そのリソースを使って認証情報を収集し、盗んだアカウント情報を使ってネットワークにアクセスします。
- **サプライチェーン攻撃** — 脅威アクターは、直接ターゲットを攻撃するのではなく、サプライチェーンに連なる企業を介してターゲットに侵入する方法を探します。このうち注目を集めた例は、企業のHVACサプライヤーを介して行われたターゲットデータ侵害です (krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company)。
- ウェブとソーシャルメディア — マルウェアには、投稿に添付されたファイルや、ダウンロードを介して感染します。攻撃者は、サイトを侵害することもできるため、脆弱なブラウザソフトウェアはそれによって自動的に感染します（ドライブバイダウンロード）。ソーシャルメディアは、ソーシャルエンジニアリングキャンペーンを強化したり、トロイの木馬を仕込むために、こっそりと利用されることもあります。
- クラウド — 現在多くの企業が、インターネットでアクセスできるクラウドを介して自社のネットワークサービスの一部または全部を運営しています。攻撃者は、認証が脆弱なアカウント、サービスまたはホストを見つけるだけで、アクセス権を得ることができます。攻撃者は多くの場合、クラウドにおけるサービス開発やクラウドシステム管理に使用するアカウントをターゲットにします。同様に、被害者のシステムにアクセスする方法として、クラウドサービスプロバイダー (CSP) の攻撃を試みる場合もあります。

巧妙な脅威アクターは、複数のベクトルを利用します。彼らは多くの場合、「ショーウィンドウ破り（スマッシュアンドグラブ）」タイプの単一攻撃ではなく、複数段階のキャンペーンを計画します。

レビューアク ティビティ：

脅威アクターのタイプと攻撃ベクトル

次の質問にお答えください。

1. 次の脆弱性、脅威、リスクのうち、可能性や影響があると評価されるのはどれですか？
2. 次の記述は正しいですか、誤りですか？国家的アクターは主に他の国に対してのみリスクをもたらします。
3. あなたは、所有するアプリケーションサーバーの一つで、コマンドプロンプトを表示するスクリーンショット付きの電子メールを受取ります。電子メールは、脆弱性を修正するために、ハッカーに1日だけコンサルティングを依頼することを提案しています。この脅威はどのように分類しますか？
4. 主に社会の変革を望むことが動機となるのはどのタイプの脅威アクターですか？
5. 多くの資金力を持つ可能性が高い3つの脅威アクターのタイプは何ですか？
6. あなたは、小企業の攻撃対象領域評価レポートの作成をサポートしています。CompTIAのシラバスに従うとすると、次の報告書の見出しから省略されている2つの潜在的な攻撃ベクトルは何ですか。直接アクセス、電子メール、リモートおよびワイヤレス、ウェブおよびソーシャルメディア、クラウド。

トピック2B

脅威インテリジェンスの情報源を説明する



対象試験範囲

1.5 さまざまな脅威アクター、ベクトル、インテリジェンスの情報源を説明することができる

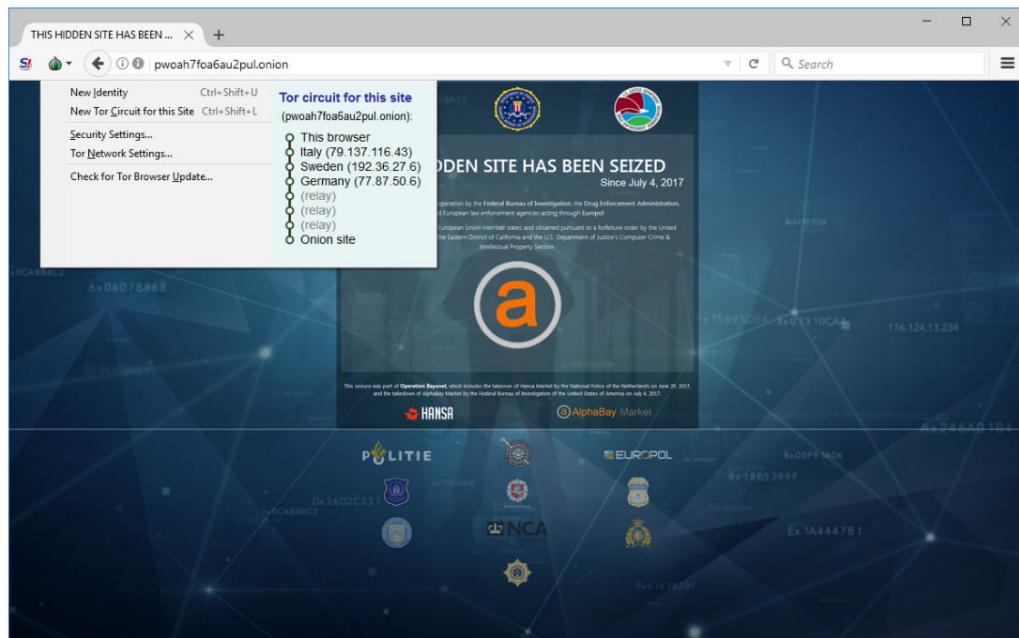
セキュリティの専門家であるならば、セキュリティ技術と実践、および敵対者の戦術と技術の、両方の知識を継続的に更新し広げる必要があります。また、個人レベルで最新の知識を維持するだけでなく、脅威インテリジェンスプラットフォームを選択しデプロイする必要があります。同様に、脅威インテリジェンスと脅威リサーチソースを特定して評価し、セキュリティ管理を強化するためにそのリソースを使用できる必要があります。

脅威リサーチソース

脅威リサーチとは、情報収集に努める敵対情報活動のことであり、セキュリティ関連企業と研究者が最新のサイバー敵対者の戦術、技術、手順(TTP)の発見を試みます。サイバーセキュリティリサーチには、主に多くの企業や大学研究機関が携わっています。ファイアウォールやマルチウェア対策プラットフォームを使用するセキュリティソリューションプロバイダーは、顧客のネットワークから大量のデータを抽出します。彼らは、顧客のサイバーセキュリティオペレーションをサポートしているため、TTPや顧客の指標を分析し公表することができます。またこれらの組織は、ハッカーが脆弱なシステムをどのように扱うかを観察するために、ハニーネットを使用することもあります。

脅威インテリジェンスのもう一つの主な情報源は**ダークウェブ**です。ディープウェブはWorld Wide Webの一部で、サーチエンジンによる索引付けはされていません。ディープウェブには、登録が必要なページ、検索による索引付けをブロックするページ、リンクされていないページ、非標準のDNSを使用するページ、標準化されていない方法で符号化されたコンテンツが含まれます。ディープウェブ内には、「通常の」ブラウザアクセスでは見えない領域があります。

- **ダークネット** — 使用を匿名化し、ネットワークの存在がサードパーティに知られたりネットワークに対して実行するアクティビティが分析されたりしないように動作するオニオンルーター (TOR)、Freenet、またはI2Pのようなソフトウェアによって、インターネットインフラストラクチャを覆うように設定されたネットワークです。オニオンルーティングは、例えばこの匿名化の実現のために、複数の暗号化層やノード間のリレーを使用します。
- **ダークウェブ** — ダークネットのみを介してアクセスできるサイト、コンテンツ、およびサービスです。ダークウェブのサーチエンジンも存在しますが、多くのサイトは隠されています。URLを介したダークウェブサイトへは、多くの場合、「word of mouth」という掲示版を介してのみアクセスできます。



TORブラウザを使用して、現在は法執行機関によりクローズされているAlphaBayマーケットを閲覧する。
(スクリーンショットはSecurity Onionから許可を得て使用)

こういったダークウェブサイトやメッセージボードの調査は、敵対情報活動の有益な情報源です。ダークウェブサービスの匿名性のおかげで、調査員は、盗まれたデータとハッキングツールの交換のために設定されたフォーラムやウェブストアに簡単に侵入できます。敵対者はこれに反応して、新しいネットワークや法執行機関の侵入を特定する方法を設定しています。つまり、ダークネットやダークウェブは絶えず変化し続けているのです。

脅威インテリジェンスプロバイダー

セキュリティソリューションプロバイダーと研究機関によって行われるリサーチの結果は主に次の3つの形式を取ります。

- **行動脅威リサーチ** — 主なりサーチソースから収集した攻撃とTTPの例をナレーションを使って説明します。
- **レビューーション脅威インテリジェンス** — 悪意のある行動に関するIPアドレスやドメインのリストと、既知のファイルベースマルウェアのシグネチャです。
- **脅威データ** — 既知のTTPと脅威アクターのインジケーターを使って、顧客が所有するネットワークとログで観測したイベントの関連性を特定できるコンピューターデータです。

脅威データは、セキュリティ情報イベント管理(SIEM)プラットフォームで統合したフィードとして、パッケージ化することができます。これらのフィードは通常、**サイバー脅威インテリジェンス(CTI)**データと呼ばれます。しかし、CTIのデータはそれ自体では完璧なセキュリティソリューションではありません。実行可能なインテリジェンスを作成するには、脅威データを顧客のネットワークから入手した観察用のデータと相互に関連付ける必要があります。多くの場合、SIEMの**人工知能(AI)**機能で、このタイプの分析を行います。

脅威インテリジェンスのプラットフォームとフィードは、3種類の異なるコマーシャルモデルのひとつとして供給されます。

- **クローズド/プライエタリ** — 脅威リサーチとCTIデータは、有料のサブスクリプション契約を行うと、商用の脅威インテリジェンスプラットフォームで使用できるようになります。またセキュリティソリューションプロバイダーは、ブログ、ホワイトペーパー、ウェビナーなどの形式でプラットフォームの契約者に有益なリサーチを早く提供することもできます。このプラットフォームの例には次のようなものがあります。

- IBM X-Force Exchange (exchange.xforce.ibmcloud.com)
- FireEye (fireeye.com/solutions/cyber-threat-intelligence/threat-intelligence-subscriptions.html)
- Recorded Future (recordedfuture.com/solutions/threat-intelligence-feeds)

IBM X-Force Exchange脅威インテリジェンスポータル
(画像著作権 2019 IBM Security exchange.xforce.ibmcloud.com.)

- ベンダーのウェブサイト — プロプライエタリ脅威インテリジェンスは、常に有料で提供されるわけではありません。セキュリティ、ハードウェア、ソフトウェアなどあらゆるタイプのベンダーは、大量の脅威リサーチを彼らのウェブサイトを介して一般的な利点として顧客が容易に入手できようしています。その一例がMicrosoftのセキュリティインテリジェンスブログです(microsoft.com/security/blog/microsoft-security-intelligence)。
- パブリック/プライベート情報共有センター — 多くの重要な産業で、**Information Sharing and Analysis Centers (ISAC)**が、脅威インテリジェンスの共有とベストプラクティスの推進のための体制を確立しています(nationalisacs.org/member-isacs)。これに該当するのは、電力供給、金融マーケット、航空機産業などの重要な産業に携わる企業や機関などの分野に特化したリソースです。ISACの対象範囲でない場合、地域の産業グループや業界団体が協力して、相互サポートを提供している場合があります。
- オープンソースインテリジェンス(OSINT) — 企業の中には、オープンソースベースで脅威インテリジェンスサービスを運営し、プラットフォームや研究活動から直接ではなく、コンサルタント業から収入を得ているところもあります。次はその例です。
 - AT&T Security, previously Alien Vault Open Threat Exchange (OTX) (otx.alienvault.com)
 - Malware Information Sharing Project (MISP) (misp-project.org/feeds)
 - Spamhaus (spamhaus.org/organization)
 - VirusTotal (virustotal.com)



OSINTは、オープンソース脅威リサーチプロバイダを指すだけでなく、一般に公開されている情報から入手できるインテリジェンスを意味します。OSINTとは、攻撃者が、攻撃ベクトルの識別を支援するドメイン、IPアドレス範囲、従業員、およびその他のデータを収集するための一般的な偵察技術です。また企業は、攻撃計画の兆候（フォーラム上のチャット）や侵害の兆候（オンラインフォーラムに投稿された機密情報またはアカウントの認証情報）などをネットワーク上で監視しなくてはなりません。多くの商用プロバイダーが、ダークWebソースを含む可能性のある監視サービスを提供しています。

その他の脅威インテリジェンスリサーチソース

脅威インテリジェンスプラットフォーム以外にもベストプラクティスのアドバイスや新しいリサーチソースが多く存在します。

- 学術誌 — IEEEなどの研究機関の研究者、業界の非営利組織や協会による発行物で、紙面の刊行物として発行されています。これらの文献は通常、定期購読することにより入手できます。無料のソースとしては、arXiv preprint repositoryがあります(arxiv.org/list/cs.CR/recent)。Preprintは、出版されたり同業者の審査を受けることはありません。
- カンファレンス — セキュリティカンファレンスは、様々な機関が主催・支援し、最新の脅威や技術に関して発表する機会が提供されます。
- Request for Comments (RFC) — 新しい技術がウェブの標準として承認されると、W3CによってRFCとして発行されます(rfc-editor.org)。また、セキュリティに関する多くの検討事項やベストプラクティスを網羅したRFCの情報もあります。
- ソーシャルメディア — 企業や個人の研究者や専門家は、ブログやソーシャルメディアのフィードで情報提供を行います。有益なブログやディスカッションソースは、数が多すぎるため、ここに記載することはできませんが、Digital Guardianがまとめたリストが参考になります(digitalguardian.com/blog/top-50-infosec-blogs-you-should-be-reading)。



情報源であるのと同様に、ソーシャルメディアでは脅威データを監視しなくてはなりません (trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter)。

戦術、技術、手順と侵害インジケーター

戦略、技術、または手順(TTP)は、敵対者の行動の一般的な記述です。専門用語は、米軍の教義から採択されます(mwi.usma.edu/what-is-army-doctrine)。TTPは、キャンペーンの戦略とアプローチ（戦術）、汎用の攻撃ベクトル（技術）、特定の侵入ツールと方法（手順）の観点から行動を分類します。

侵害インジケーター (indicator of compromise、IoC) は、資産またはネットワークに対する攻撃が成功したことがある、または現在攻撃が続いているという、今も残っている証拠のことです。別の言い方をすれば、IoCはTTPの証拠です。

TTPは、敵対者がどのようなアクションを取ったかを示し、インジケーターは、これらのアクションがどのように見えるか認識する方法を示します。stixproject.github.io/documentation/concepts/ttp-vs-indicator

攻撃のターゲットやベクトルには多くの種類があるため、IoCにも様々な可能性があります。次は、遭遇する可能性のあるIoCのリストです。

- 権限のないソフトウェアやファイル
- 信用できない電子メール
- 信用できないレジストリやファイルシステムの変更
- 未知のポートやプロトコルの使用
- 帯域幅の超過使用
- 認可されていないハードウェア
- サービスの中止や改竄
- 信頼できない、または権限のないアカウントの使用

IoCは、マルウェアのシグネチャのように明白で客観的に特定できるものもありますが、多くの場合、大量のデータポイントの相関関係によってのみ確実に説明できます。これらのIoCは、しばしば単一イベントではなく変則的な活動パターンによって特定され、様々な解釈ができるため、診断に時間がかかります。したがって脅威インテリジェンスプラットフォームは、誤検知が生じて分析時間が足りなくなることのないように、AI支援分析を使用して検出スピードをアップさせます。

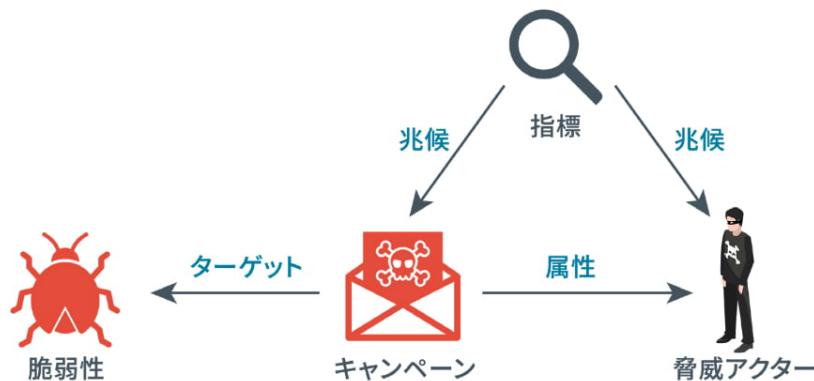
 厳密に言えばIoCは、攻撃が成功した証拠です。用語*indicator of attack (IoA)*は、時には侵入の企てが進行している証拠にも使用されます。

脅威データフィード

サイバー脅威インテリジェンス(CTI)プラットフォームを使用する場合、**脅威データフィード**のサブスクリプションを契約します。脅威データ内の情報は、ネットワークやシステムログのイベントデータと組み合わせることができます。分析プラットフォームは、IoCを検出するために、データの相関を取ります。脅威データフィードの実装には様々な方法があります。

脅威情報構造化記述形式 (Structured Threat Information eXpression、STIX)

OASIS CTIフレームワーク(oasis-open.github.io/cti-documentation)は、組織がCTIを共有できるように、自動フィードタイプの形式を提供するよう設計されています。フレームワークの**脅威情報構造化記述形式 (STIX)** 部分には、IOCの標準的な用語とそれらの関係性を示す方法が記載されています。



STIX 2の関係の例。(アイコンの画像©著作権2016 Bret Jordan。Creative Commons Attribution-ShareAlike (CC BY-SA) License, Version 4.0に基づいてライセンスを取得 (freetaxii.github.io/stix2-icons.html)

STIXはCTIを記述する形式を提供しますが、**検知指標情報自動交換手順 (Trusted Automated eXchange of Indicator Information、TAXII)** プロトコルは、サーバーとクライアントの間でCTIを送信する手段を提供します。例えば、CTIサービスプロバイダーは、CTIデータのレポジトリを保持します。サービスのサブスクリプション契約者は、TAXIIを介して分析ツールにロードされるデータの更新版を入手します。このデータは、クライアントがリクエストすることができ(収集と呼ぶ)、あるいはデータをサブスクリプション契約者に送ります(チャネルと呼ぶ)。

Automated Indicator Sharing (AIS)

Automated Indicator Sharing (AIS)は、脅威インテリジェンスの共有に参加する企業に対して、米国の国土安全保障省(DHS)が提供するサービスです(us-cert.gov/ais)。これは本来ISACを対象としていますが、民間企業も参加することができます。AISは、STIXおよびTAXIIの標準とプロトコルに基づきます。

脅威マップ

脅威マップは、CTIプラットフォームによって検出された攻撃のソース、ターゲット、タイプを示すアニメーショングラフィックスです。セキュリティソリューションプロバイダーは、顧客のシステムに対するグローバルな攻撃を示す、このようなマップを発行します(fortinet.com/fortiguard/threat-intelligence/threat-map)。

ファイル/コードレポジトリ

virustotal.comのようなファイル/コードレポジトリは、既知のマルウェアコードのシグネチャを保持します。コードサンプルは、顧客の実際のシステムやサブスクリプション契約者がアップロードした(公開レポジトリ)ファイルから抽出します。

脆弱性データベースと脆弱性フィード

敵対者の分析ツールや分析行動だけでなく、脅威インテリジェンスの別のソースが、OS、ソフトウェアアプリケーション、ファームウェアコードの脆弱性を識別しています。セキュリティの研究者が脆弱性を探すのは、多くの場合、ベンダーが提供するバグバウンティの報酬を得るためにです。脆弱性のリストは、Mitreが運営する**共通脆弱性識別子 (Common Vulnerabilities and Exposures、CVE)** のようなデータベースに保存されています(cve.mitre.org)。脆弱性に関する情報は、自動化された脆弱性スキャンソフトにフィードとして供給することができるシグネチャやスキャンスクリプトとして体系化されます。

人工知能と予測分析

脅威データフィードが、自動的に脅威インテリジェンスを作成することはありません。セキュリティインテリジェンスとCTIデータを組み合わせて処理、相関解析、分析することによって、セキュリティに関する問題の識別をサポートする実用的なインサイトが得られます。例えば、セキュリティインテリジェンスは、ログやネットワークのトラフィックデータを収集することによって、あるIPアドレスの範囲からウェブサービスに対してDDoS攻撃が実行されたことを明らかにします。脅威インテリジェンスは、これらのIPアドレスとハクティビストグループを関連付けます。2つのインテリジェンスソースが関連付けられると、このグループが関係している標的と戦術を識別し、さらなる攻撃を緩和するよう制御することができます。多くの脅威インテリジェンスプラットフォームが相関分析の実施に人工知能(AI)の類を使用しています。

AIと機械学習

AIは、人間の能力と類似する汎用性のあるインテリジェンス能力をシミュレートし実証することができる機械システムを作成する科学技術です。初期のAI（エキスパートシステム）はif-thenルールを使用して、ナレッジベースと呼ばれる限られたデータセットから推論を描きます。**機械学習(ML)**は、アルゴリズムを使用して入力データを解析し、例えば対象があるタイプに類別したり、ゲームで次のベストな動きを考案したりするなど、そのデータを使用するための戦略を開発します。機械学習はエキスパートシステムとは異なり、データの解析や戦略の開発に使用するアルゴリズムを修正することができます。また、意思決定プロセスを段階的に改良することができます。この学習プロセスを推進する構造を人工ニューラルネットワーク(ANN)と呼びます。ニューラルネットワークのノードは、ノード間の複雑なフィードバックループを使用して、入力を取得した後に出力を導出します。MLシステムは、目標とエラーステートを持ち、エラーの数を減らして目標を最適化できるようニューラルネットワークを調整します。

脅威インテリジェンスの観点から言うと、AI支援分析は、アナリストがデータを手動で検証する場合に数十時間から数百時間かかる相関を正確に導出します。

予測分析

ネットワーク上の過去の攻撃の証拠の識別や、現在存在する攻撃ツールの識別は有益です。しかし、AI支援脅威インテリジェンスを使用する目的の一つは、予測分析や脅威の予測です。つまりシステムは、攻撃がはっきり認識される前に、特定の攻撃タイプを予想したり、脅威アクターの識別情報を推測できるということです。例えばシステムは、ダークウェブソース、Web検索、ソーシャルメディアへの投稿、フィッシングメールの企てなどから取り込んだデータを、会社名、関連IPアドレス、アカウント名などにタグ付けします。分析エンジンはこの「チャット」と、既知の敵対者グループと関係のあるIPアドレスを関連付けます。こうすることで、ターゲットは、攻撃が計画されているという警告メッセージを事前に受け取ることができるため、効果的な防御を準備する時間を確保できます。

執筆時点では、このように具体的な脅威予測機能は、市販の脅威インテリジェンスプラットフォームの機能として実証されていません。しかし予測分析は、侵害タイプイベントの発生可能性や影響（コスト）の正確かつ定量的な測定値を提供することによって、リスクの評価を通知できます。

レビューアク ティビティ：

脅威インテリジェンスの情報源

次の質問にお答えください。

1. あなたは、電子投票機を扱うサプライヤーの脅威インテリジェンスソリューションのコンサルタントをしています。低価格で最も関連のある情報を生成するのはどのタイプの脅威インテリジェンスの情報源ですか？
2. CEOは、自社の脅威インテリジェンスプラットフォームがOSINTを有効に活用しているかどうかを知りたがっています。OSINTとは何ですか？
3. あなたはAISに参加すべきかを評価しています。AISとは何ですか？また、AISのサーバーに接続するには、あなたのSIEMがどのプロトコルをサポートしている必要がありますか？

レッスン2

概要

意図と能力の観点から、外部と内部の脅威アクターのタイプを評価する方法を説明できる必要があります。また、脅威インテリジェンスプラットフォームとデータソースを実装するためのオプションを概説できる必要があります。

脅威アクターと脅威インテリジェンスを説明するためのガイドライン

脅威リサーチと分析の使用を評価する場合、次のガイドラインに従います。

- あなたのビジネスにとって最も脅威になり得る脅威アクタータイプのプロファイルを作成する。大企業へのサプライヤーとしてあなたが標的になる可能性があることを忘れてはならない。
- 特にあなたが携わる産業分野に直接関連する脅威リサーチの情報源を特定する。脅威の傾向やセキュリティのベストプラクティスに関して最新情報を維持し続けるための時間をとる。
- 脅威インテリジェンスプラットフォームの使用を評価し、プロプライエタリとオープンソースのオプションを検討する。
- 産業分野固有のデータが最も有用である可能性を考慮し、様々なプロプライエタリおよびオープンソースの脅威データフィードの利用を評価する。

レッスン3

セキュリティ評価を実施する

レッスン概要

セキュリティ評価とは、攻撃対象領域を評価するプロセスとツールを指します。敵対者の戦術と能力を知ることで、攻撃対象領域のポイントが潜在的に脆弱な攻撃ベクトルであるかどうかを評価することができます。評価の結果は、脆弱性が脅威者に悪用されるリスクを軽減するために、セキュリティ対策の導入、強化、再構成するための推奨事項となります。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- ネットワーク偵察ツールを使って組織のセキュリティを評価する。
- 一般的な脆弱性のタイプを用いてセキュリティに関する懸念事項を説明する。
- 脆弱性スキャン技術を要約する。
- ペネトレーションテストの概念を説明する。

トピック3A

ネットワーク偵察ツールを使って組織のセキュリティを評価する



対象試験範囲

4.1与えられたシナリオに基づいて、適切なツールを利用して組織のセキュリティを評価することができる。

偵察は、ネットワークを構築するノードや接続を識別することによって、潜在的な攻撃対象領域をマップするタイプの評価アクティビティです。スキャンの実行には多くの場合、コマンドラインとGUIのトポロジー発見ツールの両方を使用する必要があります。フィンガープリンティングツールを使用してホスト構成を報告し、ネットワークトラフィックをキャプチャし分析する必要があります。また、ホストに対するバックドア接続を操作したり、密かにデータを盗み出す際にツールをどのように使うのかを理解する必要もあります。

ipconfig、ping、およびarp

攻撃対象領域をマッピングするプロセスをネットワーク偵察および発見と呼びます。偵察技術を使用するのは脅威アクターだけではありません。セキュリティ評価や継続的監視の一環として、自分自身のセキュリティシステムのプローブやテストを行うために、セキュリティの専門家が使用することもあります。

トポロジー発見（または「フットプリント」）とは、ターゲットネットワークの構造をマッピングするために、ネットワーク間のホスト、IP範囲、経路をスキャンすることです。トポロジー発見は、資産データベースの構築や、権限のないホスト（認証されていないシステムの検出）またはネットワーク構成工の識別に使用することもできます。

基本のトポロジー発見タスクは、WindowsやLinuxに組み込まれたコマンドラインツールを使って実行できます。次のツールは、IP構成を報告したり、ローカルネットワークのセグメントまたはサブネットの接続性をテストします。

- **ipconfig** — ハードウェアまたはメディアアクセスコントロール(MAC)アドレス、IPv4アドレスとIPv6アドレス、デフォルトゲートウェイ、アドレスは静的かDHCPによる割り当てかなど、Windowsのネットワークインターフェイスに割り当てられている構成を表示します。アドレスがDHCPによって割り当てられた場合には、出力にはリースを提供したDHCPサーバーのアドレスも表示します。
- **ifconfig** — Linuxのネットワークインターフェイスに割り当てられた構成を表示します。
- **ping** — インターネット制御通知プロトコル(ICMP)を使用して特定のIPアドレスまたはホスト名でホストをプローブします。サブネット内の全IPアドレスのスイープを実行する場合、簡単なスクリプトでpingを使用することができます。次の例では、Windowsマシンの10.1.0.0/24サブネットをスキャンしています。

```
for /l %i in (1,1,255) do @ping -n 1 -w 100
10.1.0.%i | find /i "reply"
```

```
C:\Users\Admin>for /l %i in (<1,1,255>) do @ping -n 1 -w 100 10.1.0.%i | find /i "reply"
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.128: bytes=32 time<1ms TTL=128
Reply from 10.1.0.129: bytes=32 time<1ms TTL=128
Reply from 10.1.0.131: bytes=32 time<1ms TTL=128
Reply from 10.1.0.132: bytes=32 time=1ms TTL=128
Reply from 10.1.0.134: bytes=32 time<1ms TTL=128
C:\Users\Admin>_
```

WindowsでFor Loopでpingスイープを実行します—複数のオクテットの探索にはネステッドループが必要です。すべてのホストが ICMPプローブに応答するわけがないことにご注意ください。
(スクリーンショットはMicrosoftからの許可を得て使用。)

- arp — ローカルマシンのアドレス解決プロトコル(ARP)キャッシュを表示します。ARPキャッシュは、ローカルホストが最近通信を行った各IPアドレスに関するインターフェイスのMACアドレスを示します。これは、スプーフィング攻撃の疑いを調査している場合に有益です。例えば中間者攻撃のサインは、キャッシュにリストされたデフォルトゲートウェイIPのMACアドレスが正規ルーターのMACアドレスでない場合に発生します。



シンタックスを含むコマンドの使用についてさらに詳細な情報が必要な場合は、Windows用(docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands)またはLinux用(linux.die.net/man)オンラインリソースのコマンドの項目をご確認ください。

routeとtraceroute

次のツールは、リモートホストとネットワークのルーティング構成と接続性テストに使用できます。

- route** — ホストのローカルルーティングテーブルの表示および設定。ゲートウェイルーターを介してすべてのトラフィックをリモートネットワークに送信する場合、多くのエンドシステムはデフォルトルートを使用します。ホストがルーターでない場合、ルーティングテーブルにエントリーが追加された可能性が疑われます。

```
[centos@lx1 ~]$ route -n
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref    Use Iface
0.0.0.0          10.1.0.254      0.0.0.0        UG    100    0        0 eth0
10.1.0.0         0.0.0.0          255.255.255.0  U     100    0        0 eth0
```

Linuxホストのルートコマンドから出力です。多くのエンドポイントはこれに似たルーティングテーブルを保有します。これは、ネットワークインターフェイスeth0のデフォルトゲートウェイ(10.1.0.254)として設定されたホストを介したデフォルトルート(0.0.0.0/0)を示します。表の第2ラインは、ローカルトラフィックのサブネットを示します(10.1.0.0/24)。このネットワークが直接接続されていることは、0.0.0.0ゲートウェイで表現されています。

- tracert** — ICMPプローブを使用して、ローカルホストとリモートネットワーク上のホストの間に存在するホップのラウンドトリップタイム(RTT)を報告します。tracertは、このツールのWindows版です。
- traceroute** — Linuxホストからのルートを発見します。tracerouteは、デフォルトではICMPではなくUDPプローブを使用します。
- pathping** — 長い測定期間にわたり、ルートに沿ったレイテンシやパケット損失に関する統計データを提供します。pathpingはWindowsツールで、Linuxの同等ツールはmtrです。

セキュリティコンテキストにおいて、ベースラインと比較してデフォルトゲートウェイのレイテンシが高い場合、中間者攻撃が疑われます。他のホップのレイテンシが高い場合、DoS攻撃のサインである場合もあれば、ただ単にネットワークが混雑している場合もあります。



Linuxでは、*ifconfig*、*arp*、*route*、*traceroute*などのコマンドは推奨されていないため、ユーティリティは何年もアップデートされていません。ツールの*iproute2*スイートが、これらのコマンドの代替コマンドを提供しています(digitalocean.com/community/tutorials/how-to-use-iproute2-tools-to-manage-network-configuration-on-a-linux-vps)。

IPスキャナーとNmap

*ping*などのツールを使用したネットワークスキャンは、時間がかかり、ステルス性に欠け、詳細結果を入手することもできません。トポロジー発見は多くの場合、専用のIPスキャナーソールを使用して実行します。IPスキャナーは、ホストを発見し、インターネット内でのホスト同士がどのように接続されているかを識別します。監査用に、MicrosoftのSystem Center productのようなエンタープライズスイートがあります。こういったスイートは認証情報を提供して、**簡易ネットワーク管理プロトコル(SNMP)**のような管理プロトコルを介して許可されたスキャンを実行し、詳細なホスト情報を入手します。

Nmapセキュリティスキャナー (nmap.org)は、最も一般的なオープンソースIPスキャナーの一つです。Nmapは、様々なホスト発見の方法を使用できますが、その中には秘密裏に動作したり、ファイアウォールや侵入検知などのセキュリティメカニズムを無効にするものもあります。このツールはオープンソースソフトウェアのパッケージで、Windows、Linux、macOSのほとんどどのバージョンに使用できます。これはコマンドラインを用いたり、GUI (Zenmap)を介して操作できます。

Nmapコマンドの基本シンタックスは、スキャンすべきIPサブネット（またはIPホストアドレス）を与えることです。このようにスイッチを用いずに使用した時、Nmapのデフォルト動作はホストが存在するかを判断するために、*ping*とTCP ACK/パケットをポート80および443に送信します。ローカルネットワークセグメント上では、NmapはさらにARPと近隣探索(ND, Neighbor Discovery)スイープを実行します。ホストが検知されると、Nmapはホストに対してポートスキャンを実行し、どのサービスが動作中かを判断します。

```
C:\Program Files (x86)\Nmap>nmap 10.1.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:13 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:01:CA:AB (Microsoft)


```

Nmapデフォルトは、デフォルトの範囲内のオープンポートのリストをスキャンします。
(Nmap nmap.orgのスクリーンショット。)



このOSフィンガープリンティングは、IP範囲が広い場合は、時間を浪費する可能性があるだけでなく、ステルス性もありません。ホスト発見だけを実行したい場合は、Nmapを`-sn`スイッチ（または以前のバージョンの`-sP`スイッチ）と一緒に使用して、ポートスキャンを抑制することができます。

サービス発見とNmap

ネットワーク上のアクティブなIPホストを識別して、ネットワークトポロジーのアイデア入手したら、ネットワーク偵察の次のステップで、どのオペレーティングシステムを使用しているのか、それぞれのホストはどのネットワークサービスを実行しているのか、さらに可能な場合は、これらのサービスはどのアプリケーションソフトがサポートしているのかなどを特定します。このプロセスは、**サービス発見**と呼ばれます。サービス発見は、潜在的な不正システムを調査し、未承認のネットワークサービスポートの存在を特定するために、防御的に使用することもできます。

Nmapを用いたサービス発見

ホスト発見スキャンを終了すると、Nmapは、範囲内のIPアドレスごとにスキャンした各ポートの状態を報告します。この時点で、一つ以上のアクティブなIPアドレスに対してさらにサービス発見スキャンを実行することができます。サービス発見スキャンの主なオプションには次のものがあります。

- TCP SYN (-sS) — これはハーフオープンスキャンとも呼ばれる迅速な技術で、スキャニングホストは確認応答を行うことなく接続をリクエストできます。スキャンのSYNパケットに対するターゲットの応答で、ポートの状態を識別します。
- UDPスキャン(-sU) — UDPポートをスキャンします。これらはACKを使用しないため、ポートの状態を判断する場合には、Nmapは応答またはタイムアウトを待つ必要があり、UDPスキャンには時間がかかります。UDPスキャンは、TCPスキャンと組み合わせることができます。
- ポートレンジ(-p) — デフォルトでは、Nmapは構成ファイルにリストされているとおり、一般に使用される1000個のポートをスキャンします。ポートの範囲指定には引数-pを使用します。

サービスとバージョン検知およびNmapを用いたOSフィンガープリンティング

特定のホストにおける詳細なサービス分析を、多くの場合**フィンガープリンティング**と呼びます。これは、ネットワークサービスをサポートする各OSまたはアプリケーションソフトウェアが、特有の方法でプローブに応答するためです。これによって、ホストに対するアクセス権限がない場合も、スキャンソフトウェアは、ソフトウェアの名前やバージョンで推測することができます。これはバナーグラブとも呼ばれ、その場合バナーとは、アプリケーションによって返される応答のヘッダーのことです。

サービスが発見された場合、-sVスイッチまたは-Aスイッチと共にNmapを使用すると、より集中的にホストをプローブし、次の情報を発見することができます。

- プロトコル — ポートは「よく知られた」アプリケーションプロトコルに使用されているのだと思い込んではいけません。Nmapはトラフィックをスキャンし、それが予測したシグチャと一致するかを確認することができます（HTTP、DNS、SMTPなど）。
- アプリケーション名とバージョン — Apache WebサーバーまたはInternet Information Services (IIS) Webサーバーなどのポートを操作するソフトウェア。
- OSタイプとバージョン — -oスイッチを使用すると、OSフィンガープリンティングが有効になります（OSフィンガープリンティングとバージョン発見の両方を行う場合は、-Aスイッチを使用）。
- デバイスタイプ — ネットワークデバイスのすべてがPCであるとは限りません。Nmapは、スイッチやルーター、またはNASボックス、プリンター、Webカメラなど、他のタイプのネットワーク接続したデバイスを特定できます。

```
C:\Program Files (x86)\Nmap>nmap 10.1.0.1 -A
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:41 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.000083s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
...
1 service unrecognized despite returning data. If you know the service/version, please sub
SF-Port53-TCP:V=7.70%I=7%D=1/6%Time=5E137F54%P=i686-pc-windows-windows%r(D
SF:NSVersionBindReqTCP,20,"\0\xle\0\x06\x81\x04\0\x01\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03");
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012 (98%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2016 (98%), Microsoft Windows Server 2012
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap フィンガーピンティングスキャンの結果。(Nmap nmap.org のスクリーンショット。)
```

Nmapには、Common Platform Enumeration (CPE)と呼ばれる標準構文で分類された、アプリケーションとバージョンのフィンガープリントシグチャのデータベースが付属しています。一致しない応答は、コミュニティによる分析を受けるためにウェブURLに提出します。

netstatとnslookup

基本サービス発見タスクは、WindowsやLinuxのオペレーティングシステムに組み込まれたツールを使用して実行することもできます。

- **netstat** — ローカルマシン上のTCP/UDPポートの状態を示します。WindowsとLinuxの両方で同じコマンドを使いますが、オプションのシンタックスが異なります。netstatを使用すると、サービスの構成ミスを確認できます（ユーザーが許可なくインストールしたウェブまたはFTPサーバーをホストが実行している可能性があります）。また、ローカルホスト上のサービスや、ホストからリモートIPアドレスへの疑わしいリモート接続を識別することもできます。マルウェアの識別を試みている場合、netstat出力は、どのプロセスがどのポートでリッスンしているかを示すのに最適です。

```
C:\Users\Administrator>netstat ! findstr "10.1.0"
  TCP  10.1.0.1:80          ROGUE:1415          TIME_WAIT
  TCP  10.1.0.1:80          GATEWAY:49161        ESTABLISHED
  TCP  10.1.0.1:135         ROGUE:1417          TIME_WAIT
  TCP  10.1.0.1:135         ROGUE:ms-sql-s        TIME_WAIT
  TCP  10.1.0.1:139         ROGUE:1418          TIME_WAIT
  TCP  10.1.0.1:445         10.1.0.134:49226    ESTABLISHED
  TCP  10.1.0.1:49154        ROGUE:1467          ESTABLISHED
  TCP  10.1.0.1:49155        ROGUE:1468          ESTABLISHED
  TCP  10.1.0.1:49158        ROGUE:1469          ESTABLISHED
  TCP  10.1.0.1:49159        ROGUE:1470          ESTABLISHED
  TCP  10.1.0.1:49163        ROGUE:1471          ESTABLISHED

C:\Users\Administrator>_
```

Windowsで動作するnetstatコマンドは、nmapスキャン中のアクティビティを示します。findstr関数は、出力結果をフィルタリングするために使われています（同じサブネット上のIPv4ホストからの接続のみを示す）。(スクリーンショットはMicrosoftからの許可を得て使用。)