初期のタイムシェアリングシステムに戻るまで、私たちのシステムは、ユーザーとユーザーが作成したコードを、私たちとお互いの致命的な敵と見なしていました。  
–ロジャーニーダム  
偽りの顔は、偽りの心が知っていることを隠さなければならない– MACBETH  
  
イデオローグは望みどおりに世界を扱いますが、エンジニアは世界をそのまま扱います。  
コンピューティングの初期の頃は、ほとんどの場合本当の敵はいませんでした。銀行と軍隊はシステムを保護する必要がありましたが、他のほとんどの人は実際には気にしませんでした。  
学生はシステムをハッキングしてより多くのリソースを取得しようとする可能性があり、システム管理者はそれらを阻止しようと試みますが、それは主にゲームでした。  
初期のインターネットは友好的な場所であり、学者、テクノロジー企業のエンジニア、そして何人かの趣味家が住んでいました。  
（それでも、実験室から脱出した学生の実験でした。セクション21.3.2で話をします。）  
1990年代半ばに最初のスパムが発見され、1990年代後半に最初の分散型サービス拒否攻撃が発生し、ドットコムブームにおける通信販売ビジネスの爆発的な増加により、クレジットカード詐欺が発生しました。  
アンダーグラウンド市場の出現により、2000年代半ばに状況は変化しました。  
これにより、18世紀後半に製造業が行ったように、彼らは仕事で上手になり、スケールアップし、グローバル化することができました。  
 –データを大規模に収集し、Googleと同じようにインデックスを付けて、アナリストが利用できるようにする方法を検討します。  
そしてもちろん、誰もがオンラインになると、これにはスパイや詐欺師だけでなく、ジャーク、ゾッと、人種差別主義者、いじめも含まれます。  
それについてもかなり知っています。  
サイバー犯罪についてはよく知っています。現在、オンライン犯罪は、量的および金額的に、すべての犯罪の約半分を占めています。  
多くの伝統的な犯罪がオンラインになり、典型的な企業は外部の詐欺師だけでなく、不正な内部関係者も心配する必要があります。  
選出された政治家への嫌がらせを通じて、学校でサイバーいじめに苦しむ子供から、以前のパートナーに忍び寄る人々まで、多くの人々がオンラインの敵意に対処しなければなりません。  
新しい問題に取り組むときにセキュリティエンジニアが最初に行う必要があることの1つは、可能性のある敵を特定することです。  
 すべての合理的な逆境に対抗するために、同じことは複雑な現実のシステムにはあまり当てはまりません。  
では、敵はどのような能力を持ち、どのような動機があるのでしょうか？  
 この章では、動機に応じてオンラインと電子の脅威を分類します。  
次に、主に金銭を動機とする犯罪者を扱います。  
最後に、ネット上のいじめからストーカーに至るまで、主に個人的なものであり、主にその人物に対して犯罪を犯している悪役について説明します。  
ほとんどの企業とほとんどの個人は、それらの一部にのみ関心があります。  
  
政府は、ネットワークの受動的監視とコンピュータシステムへの能動的攻撃の両方のためのさまざまなツールを備えています。  
ただし、規模、目的、能力については政府間で大きな違いがあります。  
スパイが今日の脅威モデルに含まれていない場合でも、彼らが使用するツールは、遅かれ早かれ、多くの場合、詐欺師の手に渡ることになります。  
2.2.1 5つの目  
  
私はカリフォルニア州パロアルトのホテルで、2011年に科学的訪問者としてGoogleに定期的に訪問する前にガーディアンをオンラインで読み、Androidフォンの非接触型決済の開発を手伝いました。  
朝食後、Googleplexに車で行ったところ、以前の同僚も私と同じように困惑していることがわかりました。  
gmailチームもしませんでした。  
 エリックシュミットに注文があった場合、もしそうであれば、メールチームとセキュリティチームに知らされずに、それをどのように実装できたでしょうか。  
Prismは、保証された盗聴を行うためにFBIに提供されたアクセスチャネルの内部NSAコードネームであることが判明しました。  
したがって、私のような外国のターゲットの場合、NSAインテリジェンスアナリストがしなければならないことは、タブをクリックして、私が米国外の人物であると信じていたということです。  
記事によると、このプログラムは2007年にマイクロソフトで開始されました。 Yahooはそれを法廷で戦ったが、敗北し、2008年後半に参加した。 GoogleとFacebookは2009年に追加され、Appleは最後に2012年に追加されました。翌日、話の出所は、笛を吹くことにしたNSAのシステム管理者であるEdward Snowdenであることを知りました。  
彼は6月21日にラテンアメリカに逃亡しようとしましたが、米国政府がパスポートをキャンセルした後、彼はモスクワで行き詰まり、最終的にはロシアで亡命しました。  
リークされたドキュメントに基づく最初のストーリーは、実際にはプリズムストーリーの2日前に現れました。それはFISA裁判所がVerizonにすべての通話データレコード（CDR）を引き渡すように命じた方法に関するものでした  
とにかく機関がそうすることを知っていたので、これはセキュリティ専門家からそれほど注目されませんでした。  
そして、従うべきものはすべてを変えました。  
2.2.1.2テンポラ  
これは完全な驚きではありませんでした。ジャーナリストのダンカンキャンベルは、1988年にIntelsat衛星ネットワークを利用してエキロンと呼ばれるシステムを記述し、アナリストが関心のある電話番号へのトラフィックまたはそこからのトラフィックを選択できるように、メタデータを検索に利用できるようにしながら音声通話をテープに保存しました[373、374] （セクション26.2.6でより歴史的な背景を説明します）  
スノーデンは私たちにテクノロジーの最新情報を提供してくれました。  
これらのそれぞれが10Gb / sを伝送するので、総データ量は1日21Pbにもなる可能性があるため、着信データフィードは大幅なボリューム削減を受け、ビデオやニュースなどが破棄されます。  
Temporaプログラムは、以前のエシェロンと同様に、英国に深く関わっています。  
したがって、英国の主要な情報資産の1つは、19世紀の帝国を制御するために構築された通信インフラストラクチャの遺産であることが判明しました。  
1SIGINT（シグナルインテリジェンス）  
2.2.1.3筋肉  
10月30日に明らかになったこのデータは、YahooやGoogle [2016]などの大規模サービス会社のデータセンター間を流れるデータを収集したものです。  
「Google Cloud Exploitation」に関するNSA PowerPointスライドがワシントンポストで発行された後–図2.1を参照–企業は、ネットワーク上のすべてを暗号化するためにスクランブルをかけました。  
それは、あなたが令状を順守したとしても、可能であればスプークもあなたをハッキングすることを業界の人々に思い出させました。  
 重大なプライバシー侵害でした。  
 AkamaiやCloud ﬂ areなど。 Webトラフィックは、ユーザーのラップトップまたは電話からISPのCDNの存在場所まで暗号化されますが、追加料金を支払わない限り、バックホールでは暗号化されません。ほとんどの場合はそうではありません[86]。  
  
NSAとCIAは共同でSpecial Collection Service（SCS）を運営しています  
。  
これには、スピーチや電子通信を監視するバグの配置から標的組織でのほくろの募集、標的国でのアンテナの秘密の配備から内部のマイクロ波リンクを利用するまで、古典的なスパイのトレードクラフトが関係する可能性があります。  
接近アクセス操作には、テンペストモニタリングが含まれます。19.3.2で説明されているように、コンピュータモニタや他の機器からの電磁放射によって漏れる情報の収集です。  
  
特別な収集はますますサプライチェーンの改ざんを伴います。  
そして、NSAが極度の形態のサプライチェーン改ざんをしたのは、NSAが冷戦中に非同盟国に暗号化機器の主要サプライヤーであったスイスの会社であるCrypto AGをひそかに買収したときでした。後で詳しく説明します。  
これは、学術研究を指揮する、または誤解させる試みから始まります3。信頼できる人々を標準委員会に配置し、NISTの影響力を利用して弱い標準を採用することを続けました。  
ただし、実際の被害のほとんどは、暗号鍵の長さの制限によるものであり、輸出管理を強制するための同盟国に対する外交圧力と相まって、輸出ライセンスを必要とする企業は、「適切な」標準を使用するために腕をねじることができました。暗号戦争に巻き込まれた（セクション26.2.7で説明）  
その結果、現在使用されているシステムの多くは脆弱な暗号化を使用せざるを得なくなり、ホテルや車のドアのロックからVPNまで、あらゆるものに脆弱性が生じました。  
監視ポリシーと暗号化ポリシーに起因する脆弱性が1つに見られます。コンピュータにソフトウェアを埋め込むことができないため、NSAがあなたに対してハイテクコレクションを使用する必要がある場合、それは褒め言葉かもしれません。 31990年代に、ケンブリッジ大学のアイザックニュートン研究所でコーディング理論、暗号化、およびコンピューターセキュリティの研究プログラムを実行するように入札したとき、GCHQの上級幹部は、先に進めないように研究所に50,000ポンドの寄付を提供しました。暗号で興味深い出来事があり、女王陛下の政府はこの状況が続くことを望んでいます。」次々に章を読み、本のパート3に戻って、ポリシーの履歴について詳しく説明します。  
2.2.1.6 Xkeyscore  
ファイブアイズは、アナリストが収集したデータをリモートで検索して結果を収集できる分散データベースであるXkeyscoreを使用してコンピューターデータを検索します。  
2008年のトレーニング資料の例には、「私のターゲットはドイツ語を話しますが、パキスタンにいます。  
「イランの暗号化されたすべてのWordドキュメントを表示」および「イランでのすべてのPGP使用状況を表示」。  
 より一般的なコレクション。  
そのコンポーネントは収集ポイントで情報をバッファリングします– 2008年には、150のサイトに700のサーバーがあります。  
必要な唯一の司法承認は、アナリストが会話の当事者の1人が米国に居住していないと信じる理由を入力するプロンプトです。  
タスクされたアイテムが抽出され、リクエストした人に送信されます。通知システムがあります（Trafficthief）  
抽出はフィンガープリントまたはプラグインに基づいて行われます–後者は、ステガノグラフィや自作の暗号化などの新しい課題に対応するために、アナリストが検出器ですばやく対応できるようにします。  
。  
 何億もの携帯電話からのトラフィック[1658]。  
2014年のスノーデンとのインタビューによると、Xkeyscoreはアナリストがターゲットのオンラインアクティビティのフィンガープリントを作成し、世界中を自動的に追跡できるようにします。  
Xkeyscoreにはデッキのコレクションがあり、Morgan Marquis-Boire、Glenn Greenwald、Micah Lee [1230]による調査があります。デッキを注意深く読むことは、Snowdenの倉庫を探索するための良い出発点となります。  
2.2.1.7長距離  
Xkeyscoreトレーニング資料には例が示されています。「X国のすべてのVPNスタートアップを表示し、ユーザーを解読してユーザーを発見できるようにデータを提供してください」。  
暗号解読技術の詳細な説明は、Extremely Compartmented Information（ECI）として保持されています。  
これらは何でしょうか？  
他の人たちは、関連する規格へのNSA暗号学者の関与を指摘し、プロトコルフローは後で発見されました。さらに、数論やプロトコルのエクスプロイトが進歩したとしても、NSAには1024ビットのDiffie-Hellmanをブルートフォースで破壊するだけの十分な資金があることを指摘する人もいます。 –彼らが行うこと[853]。  
  
プロトコルに対する攻撃には長い歴史があり、さまざまな方法でなりすまし、再生、操作が可能です。  
 インターネットトラフィックに対する最も文書化されたNSA攻撃は、Quantumのコードネームの下で行われ、通信エンドポイントの1つを動的に利用します。  
さまざまな風味があります。 「Quantuminsert」では、挿入されたパケットがブラウザを「Foxacid」攻撃サーバーにリダイレクトします。  
  
コンピューターとネットワークの悪用（CNE）  
Operation Socialistは、2010–11年にベルギーの主要な電話会社Belgacom5をハッキングしたGCHQコードネームでした。  
その後、攻撃者はシステム管理者権限を使用してマルウェアをインストールしました4https：//www.edwardsnowden.comには、コレクションの検索エンジンもあります。  
さらなるアクセスを活用するための認証サーバー、追跡サーバーをカバーできるように課金サーバー、会社のコアシスコルーターなど、数十台のサーバー[734]。  
NATOとEUのある加盟国が別のNATOの重要なインフラストラクチャにサイバー攻撃を行うという考えは、多くの人を驚かせました。  
これらの機関が英国およびその他の加盟国に対して多くの法律を制定していることを考えると、これはまるで米国の州知事が国の部隊にAT＆Tをハッキングさせて議会とホワイトハウスを盗聴できるかのようでした。  
物語は2013年9月に公開され、ドイツのニュース雑誌Der Spiegelは、GCHQが責任を負っていることを示すSnowdenの文書を発行しました。  
 助けることを拒否した。  
Europolは後に、「犯罪の起源が疑われる」ハッキングの調査に役立つという方針を採用しました。政府によるハッキングについては言うまでもありません。  
 暗号;常に「英国の否認可能」でなければならないこと。また、通信の低下や「過激なWebサイトでのユーザーのパスワードの変更」[735]などの「影響」にも使用できます。  
電話会社のある幹部が説明したように、「MNOは当時、ネットワークセキュリティについて無知でした。NSAとその同盟国によって使用されているハッキングツールと手法は、今ではかなりよく理解されています。一部は法執行機関と共有されています。  
 は、NSAのTailored Access Operationsチームのハッカーが攻撃を仕掛けるために使用した実際のNSAマルウェアサンプルをいくつか公開しました[238]。  
 すべての中で最も優れたドキュメントはおそらく、CIAが使用する別のグッズストアに関するものであり、2017年の「Vault 7」のリークでウィキリークスにある程度詳しく開示されています。  
、オーディオ、ビデオ。サムドライブに感染してエアギャップをジャンプするツール。 Wi-Fiルーターに感染して中間者攻撃を実行するためのツール。また、文書に透かしを入れるためのツールでさえ、それらを漏らす内部告発者を追跡することができます。  
TVやIoTデバイスをハッキングするツールや、法医学的調査を妨害するツールもあります。  
そのようなツールの法執行機関による使用の例として、2020年6月にリールのフランス警察が2018年以降、犯罪者が好む暗号化されたメッセージングシステムであるEncroChatを実行している数千のAndroidフォンにマルウェアをインストールし、フランス、オランダ、イギリスなどの800人の犯罪容疑者、ならびに汚職および数トンの麻薬の押収による数人の警官の逮捕[1332]。  
彼らが組織の主要人物を見つけようとしている場合-重要な決定について助言する政策立案者であれ、寡頭政治家の利益の洗浄に関与している弁護士であれ-彼らはXkeyscoreのトラフィックデータを使用して連絡先ネットワークをマッピングできます。  
サイバー犯罪に関する私たち自身の調査から、このプロセスについていくらか洞察を得て、地下のフォーラムから数千万のメッセージをこすり取り、それらを分析して新旧の犯罪タイプを理解しています。  
Web検索を行うときにアダプティブテキストマイニングを使用するのと同じように、検索結果のサンプルに基づいて検索用語を常に絞り込み、メッセージマイニングにはメタデータも用意されているため、スレッドをたどり、フォーラム全体で俳優を追跡し、クラスター分析を行うことができます。そして、他のさまざまなトリックを使用して、「このようなメッセージをさらに見つけます」。  
アナリストがハンティングフェーズからギャザリングフェーズに移行すると、プリズムを使用してFacebook、Google、およびマイクロソフトのターゲットのアカウントを確認できます。Xkeyscoreを使用すると、アクセスしたWebサイトを確認できます。  
代理店は、WhatsAppなどのエンドツーエンドのメッセージングシステムへのアクセスを求めています。英国、オーストラリア、中国などの国では、立法府はすでにこれを承認していますが、どの米国企業が準拠する可能性があるかはまったく明確ではありません（ポリシーについては第26章で説明します）。  
価値の高いターゲットを考えると、アナリストがラップトップまたは携帯電話に直接インストールできる大きなツールバッグがあります。  
彼らは6Seeをダウンロードして、たとえばこれを測定するために現代のスマートホームを盗聴したHillとMattuをダウンロードできます[900]  
一方、アナリストはメッセージングアプリにバグを犯し、復号化された通話内容を収集することで、エンドツーエンドの暗号化を打ち破ることができます。  
報道はかなり完全です。  
エド・スノーデンが彼にインタビューしているジャーナリストが彼らの電話を冷蔵庫に入れると主張したことは少し不思議ではない！最後に、アナリストにはプロキシを使用して、インターネットに不正にアクセスすることもできます。通常はボットネット上のマシンです。  
2.2.1.11攻撃作戦NSA局長はまた、2009年から米国国防総省の10の統一指揮官の1つである米国サイバー司令部を率いている。  
これは、機械的損傷を引き起こすように設計されたパターンで、イラン濃縮ウランを高速化および低速化することによって損傷するように設計されたワームであり、米国とイスラエルが共同で開発しました[325、826]。  
USBドライブを使用してエアギャップをイランのシステムに橋渡しするように導入されたようで、コピーが中央アジアとインドネシアに何らかの形で広まった後、2010年に明らかになりました。  
 その後、同様のトリックと共通のコードを使用して発見され、中東および南アジアの多くの企業で監視を行いました。最近のコード分析ツールは、2002年に遡るマルウェアの系統を追跡しました（Flowershop）  
 [2068]。  
ああ、そしてゼロデイ脆弱性の価格は急上昇しました。1つの携帯電話をタップするのは難しいです。  
または、偽のベースステーションを使用して背後を運転し、信号が本物の信号よりも大きいので、彼の電話がローミングしてくれることを期待できます。ただし、電子的検出のリスクもあります。  
パリ中心部の誰かを頻繁に盗聴したいのなら、なぜ皆を盗聴しないのですか？  
フランスのすべての人をハックしたい場合は、おそらく使用している機器を破壊することによって、電話会社をハックしてください。  
ファイブアイズ戦略は本質的に世界のすべてを集めることです。インフラストラクチャの構築と維持に数十億ドルかかるかもしれませんが、それができればすべてが揃います。  
戦時中は、コマンドを送信して敵のレーダー基地を爆破することができます。しかし、それを1回または2回以上行うと、若者は多くの歩哨に遭遇し始めます。  
 何千ものドローン。  
 ファイブアイズのアプローチはこれです。  
したがって、競合他社の状態に関する重要な問題は、一般にファイブアイズの立ち入り禁止である電子空間をどれだけ作成できるかだけではありません。  
私たちがオンラインで目にするスキャンとプローブの数は、NSAだけがスケールするサイバー兵器の構築を試みているわけではないことを示しています。  
これにより、多数のポリシー問題が発生します。この問題については、パート3で取り上げます。  
  
中国は現在、米国の主要な競争相手であり、GDPだけでなく、テクノロジーの強国としても2番目です。  
。  
一部の米国のサービス会社は以前はそこで営業していたが、トラブルが続いた。  
2008年に、中国で利用可能なSkypeのバージョンが変更され、メッセージが機密性の高いキーワードでスキャンされ、見つかった場合、ユーザーのテキストが7にアップロードされました。これらのデバイスは、米国ではStingrayおよびIMSIキャッチャーとしてのヨーロッパ。彼らは、セクション22.2.1で詳細に説明する種類の中間者攻撃を行います。  
2009年12月、グーグルは企業インフラストラクチャに対する中国の攻撃を発見しました。これはオペレーションオーロラとして知られるようになりました。中国のエージェントがFBIの盗聴に使用されたGoogleシステムにハッキングした（上記のプリズムを参照）  
グーグルは中国のユーザーのために彼らの検索エンジンの検閲されたバージョンを操作することに対する批判に既に苦しんでいて、そして数ヶ月後、彼らは中国から撤退した。  
中国の戦略は、海外でのこれまで以上に積極的なコレクションによって増強された、完全な国内統制の出現でした。  
米国外軍事研究局（FMSO）による2004年の調査によると  
中国の指導者は、米国のサービス会社、ニュースWebサイト、Torなどの匿名ツール（国務省が中国や他の人々が検閲に打ち勝つことができるように資金を提供）を目にしています  
したがって、YahooとGoogleは、ロッキードマーティンとBAeのように公正なゲームと見なされていました。  
その年の北京オリンピックに向けて中国人がオフィスシステムをハッキングしたことを知っていたダライラマから助けを求められました。  
彼は、チベット亡命政府のオフィスにある50台のPCのうち約35台がハッキングされていることを発見しました。情報は、チベット問題のさまざまな側面を担当する中国の国家安全保障機関の3つの組織の近くにあるIPアドレスに転送されていました。  
この手法は、誰かが噛むルアーを提供することで機能するため、フィッシングと呼ばれます。特定の個人を対象とする場合（この場合のように）  
その後、チベット人のメールサーバーを危険にさらしたため、オフィスの人が.pdfファイルを別の人に送信するたびに、埋め込まれた攻撃が行われました。  
これについて考えるのをやめると、これはかなり冷静です。  
そして、あなたのマシンは、友好的な国で1万マイル離れたところに借りているサーバーに突然感染しました。  
それが出た後、私たちはしばらくの間、私たちの機器への攻撃に対処しなければならなかった、そして私たちが攻撃を彼らの政府に帰する証拠がないと主張した中国人による会議での口論。  
2009年に鉄鉱石の価格を巡るリオティントとの複雑な論争と同じ年にメルボルン国際映画祭のハッキングがウイグルの指導者に関する映画を上映したときの中国の国家ハッキングに関する一連のさらなる報告が続きました[ 1898]。  
フラッシュバルブの最初の瞬間は、中国のハッカーがF35ジョイントストライクファイターの秘密の一部と他の一連の武器システムを盗んだという国防総省の漏えいした2013年の報告でした[1379]。オバマ政権は、営業秘密の盗難に関する調査と訴追を最優先事項とすることを誓約し、翌年、人民解放軍の5人のメンバーが欠席したとして起訴された。  
指紋やセキュリティクリアランスのインタビューからの機密情報に至るまで、2200万人の現在および元の連邦従業員の非常に個人的なデータにアクセスできます。  
過去5年間のすべての性的パートナーは、通常の最高機密のクリアランスのために宣言されなければなりません。ストラップクリアランス用（信号インテリジェンス資料を処理するため）  
したがって、この漏えいは、わずか2,200万人以上に影響を与えました。  
（シニクスは、内部告発者が信用されないようにするためにもそうだと考えていました。）  
中国人が政府の敏感な仕事をしているすべてのアメリカ人に関するすべての妥協する情報を入手することは驚きました。  
 その年の9月の首脳会談で、オバマ大統領とXi大統領はコンピューターによる知的財産の商業的利益のための盗難を控えることに同意した8。  
2000年代の中国の攻撃は、賢い人々とシンプルなツールを使用しました。チベット人への攻撃は、リモートアクセストロイの木馬としてロシアのクライムウェアを使用しました。  
英国の警察および治安機関は2007年に英国の企業に警告した。  
いずれにせよ、「IPの盗難」というフレーズは常に簡略化されたものであり、分類された情報防御請負業者の盗難を、中国市場へのアクセスと偽造の副問題を必要とする他の企業による強制的な技術移転のより大きな問題に追いやるために使用されました。  
チベットの攻撃と同様に、これらは通常粗雑なツールを使用し、操作のセキュリティが非常に低いため、どこから来たのかはかなり明らかでした。  
 脅威インテリジェンス企業によって追跡されます。  
中国は産業および商業スパイ活動も行っており、西側の機関はマネージドサービスプロバイダーを利用していると主張しています9。  
GCHQの作戦社会主義と同様に、このような間接的な戦略は、あなたが主権者ではない地域で攻撃を拡大する方法を提供します。  
2018年以降、トランプ政権が2019年5月にHuaweiをブラックリストに載せることで、中国企業がNATO諸国でルーターと5gネットワークハードウェアを販売することを許可すべきかどうかについて政治的な議論がありました。  
トランプ大統領は、北朝鮮とイランへの制裁を破ったことでZTEを禁止しましたが、その設備を容認し、安全管理の対象として米国に戻すことを許可しました11。  
アナリストはバックドアを発見しませんでしたが、彼らの2019年のレポートは、Huaweiのソフトウェアエンジニアリングプラクティスに対するいくつかの厳しい批判を表面化しました[931]。  
既知の脆弱性がありサポートされていないバージョンを含む、管理できない数のOpenSSLのバージョンがありました：4つの異なるOpenSSLバージョンの70のフルコピー、および14バージョンの304の部分コピー。  
彼らの機器は9で除外されていました。これは、ウィプロをハッキングして顧客を危険にさらすためにこれを使用したという主張で2019年に公開されました[1093]。しかし後になって、ウィプロが利益のために活動している犯罪組織によってハッキングされたことが明らかになりました。  
11これは、大統領が刑事訴追に干渉することを「恐れた」と宣言した元国家安全保障顧問のジョンボルトンによると、Xi大統領への好意として行われた[156]。  
英国は、信頼を置く前に、「複数のバージョンと複数の製品範囲にわたる改善の持続的な証拠」を要求しました。  
 ファーウェイとイランで事業を行っている会社との関係について、世界の銀行を詐欺するために共謀したことで彼女を引き渡そうとする米国の要求に続いて。  
米国は、Huaweiにチップ、ソフトウェア、またはサポートを販売する米国のサプライヤーを禁止しました。  
一方、中国は後発開発途上国のネットワークの近代化を支援しており、このアクセスにより、やがてファイブアイズの範囲に匹敵する可能性があります。  
戦略的には、問題は中国がHuaweiルーターを使用して他の国々を大規模に盗聴できるかどうかだけでなく、緊張時にそれを使用してBGPルーティングを破壊することによりインターネットを破壊するDDoS攻撃を開始できるかどうかということではないかもしれません。  
長年にわたり、中国の「平和的台頭」の教義は、他の主要な勢力と十分に強くなるまで対立しないようにすることを意味していました。彼らはオンライン操作を伴うこともある様々な方法で他の国をいじめ始めています。  
2020年、EUは中国がコロナウイルスのパンデミックに関する破壊的な偽のニュースを広めたとして非難し[1577]、オーストラリアはパンデミックの起源に関する国際的な調査を求めて以来発生したサイバー攻撃を非難しました[935]。  
外交評論家は、中国の通商政策は攻撃的ではあるが1970年代の日本と同じであり、アメリカほど積極的ではないと指摘している。新しい冷戦は見当違いであり、前回と同じように無駄で危険である可能性が高いこと。中国は依然としてそれを混乱させる以上に国際秩序を支持している。そして、それはアメリカが第二次世界大戦以来行ってきたよりも一貫してそれを支持している[704]。  
  
ロシアは中国と同様に、アメリカのプラットフォームの利点を欠いており、スピアフィッシングとマルウェアを使用するハッキングチームで補っています。  
歴史家ティモシースナイダーは、プーチンの権力の台頭と、特に2012年の不正選挙以来の、プーチンの寡頭政治、正統派キリスト教、同性愛嫌悪、ファシストのイデオローグイヴァンイリンの抱擁について説明しています。  
オンラインでの戦略的な姿勢は、中国とは4つの点で異なります。  
第二に、ロシアは中国のようにより閉鎖されようとしているが、その国内インターネットは比較的オープンであり、VKやYandexなどの主要なサービス会社を含む西側諸国と絡み合っている[605]。  
これらの介入には、サイバー攻撃に加えて「リトルグリーンメン」（ユニフォームにロシアの記章がない軍隊）と、拒否の政治戦略を組み合わせた戦略が含まれています。  
2005年頃から、その目標は、米国とEUを弱体化させ、ルールに基づく国際秩序の代替として権威主義とナショナリズムを促進することでした。  
Brexit、ハンガリー、トルコ、ポーランドの権威主義政府の出現、およびイタリア、スロバキア、オーストリアの連合政府の権威主義者の存在により、この戦略は成功しているようです。  
政府機関、銀行、メディア企業に対するDDoS攻撃により、エストニアは外部インターネットアクセスを数週間にわたってレート制限する必要がありました[692]。  
懐疑論者は、攻撃はアマチュアの仕事のように見え、米国のサービスプロバイダーのようにシステムがシステムを強化していなかったためにうまくいったと述べました。  
これについては、セクション23.8の電子情報戦争に関する章で詳しく説明します。  
エストニアとジョージアはウクライナのウォームアップに過ぎませんでした。  
ロシア人は2月24日にウクライナを侵略し、クリミア半島を併合し、ウクライナ東部のドンバス地域に2つの人形国家を設立しました。  
たとえば、5月にロシア人はウクライナの選挙委員会のウェブサイトをハッキングして、投票の1％未満しか獲得しなかった民族主義者が勝ったというメッセージを表示するように仕掛けました。これは発見されブロックされましたが、ロシアのメディアはとにかく偽の結果を発表しました[1798]。  
彼らは、数か月にわたって埋め込まれた複数の異なる攻撃ベクトルを含み、クリミアの配電に対するウクライナの攻撃に続いて-そして代わりにそれらを破壊する可能性があるときに機器をオフにした-警告として意図されたように思われた[ 2067]。  
2017年6月27日、ついにNotPetya攻撃が発生しました。これまでで最も被害の大きいサイバー攻撃です[813]。  
その後、興味深い履歴を持つNSAエクスプロイトであるEternalBlue脆弱性を使用して、Windowsファイル共有全体の組織に横方向に広がりました。  
。  
NotPetyaワームは、Windowsメモリからパスワードを回復するMimikatzツールと共にEternalBlueを使用しました。  
しかし、身代金を支払ったコンピューター所有者のファイルを解読するメカニズムがなかったので、それは本当に破壊的なサービス拒否ワームでした。  
NotPetyaの攻撃により、銀行、電話会社、さらには旧チェルノブイリ原子力発電所の放射線監視システムさえも破壊されました。  
世界最大のコンテナ輸送会社であるマースクは、3億ドルのコストで、ほとんどのコンピューターを置き換え、遅延した出荷を顧客に補償する必要がありました。 FedExも3億ドルを失い、Mondelezは1億ドルを失いました。  
2016年は英国のBrexit国民投票と米国のトランプ大統領の選挙によって特徴付けられましたが、どちらもロシアの干渉がありました。後者では、キャンペーン中にロシアの干渉がオバマ大統領によって非難され、新たな経済制裁に至り、その後、米国の諜報機関によっても非難された。  
一部のトランプ関連団体は、さまざまな犯罪で刑務所に行きました。  
一方では、プーチン大統領が政権を握って以来、民主主義国家の影響力とルールに基づく国際秩序を弱体化させ、権威主義を促進するために、米国上院の外交委員会への報告は、ロシアの持続的な政策の物語を述べています。左と右の両方の政府、そしてそれができるところで問題を引き起こしています。  
一方、ヨチャイベンクラー氏は民主党に対し、トランプ氏の選挙がすべてロシアの過失だと信じ込まないよう警告している。政治エリートに対する大衆の不満のルーツははるかに古く、より深い[227]。  
。  
それは変電所をハッキングすることだけでなく、有権者の心をハッキングすることでもあります。制度や事実さえも信頼を損なうこと、ソーシャルメディアを利用すること、政治をショービジネスとして作り直すことについて。  
  
その他の世界の政府は、さまざまなサイバー機能を備えていますが、ツールの性質や出所など、共通のテーマがあります。  
それ以来、アラブ諸国はスパイウェアとハ​​イプロファイルターゲットに対するハッキングを組み合わせた戦略を発展させてきました。トロールファームは、公共の場で虐待的なコメントを送り出し、物理的な強制を行っています。  
NSAのアナリストとエドスノーデンの元上司である彼女は、2014年にメリーランドの請負業者に雇われ、傭兵としてドバイで働くようになりましたが、UAEの作戦がアメリカ人を対象にし始めた後に去りました。  
彼らはまた、政権に批判的な外国人を標的とした。  
諜報チームは、ドバイの大きな別荘にいる傭兵とエミラティスの両方の数十人で構成されていました。  
2018年、サウジアラビア政府はワシントンポストのジャーナリスト、ジャマルカショギをイスタンブールの領事館で殺害しました。  
ベゾスは、彼と彼の妻が離婚していることを発表することによって調査者を先取りし、漏洩の原因を見つけるために調査員を雇いました。  
代わりにベゾスは公開されました。  
米国司法省はその後、政府を批判した人々の個人アカウント情報をサウジアラビア人に開示することにより、2人の元Twitter従業員をスパイ行為で告発した[1500]。  
反体制派に対するマルウェアの攻撃は2012年から報告されており、当初はさまざまなスピアフィッシングルアーを使用していました。  
その後、バンで拷問室に連れて行かれる間、彼らは彼のすべての接触をスピアフィッシングしました。  
戦争が進むにつれてキャンペーンは着実に巧妙になり、偽旗攻撃がありましたが、斬首のビデオを表示するいくつかのツールで残酷なエッジを維持しました[737]。  
ここでの本当の問題は、主に米国、ヨーロッパ、イスラエルにある企業のエコシステムであり、不快な国家にハッキングツールを提供しています。  
これらのツールは、独裁者がアメリカとヨーロッパの敵を追跡および監視するために使用されます。  
あるケースでは、NGOは、シリア企業が英国企業のドイツ子会社から大量監視機器を購入する能力は輸出規制の対象とすべきであると主張しましたが、英国当局はそれをブロックすることに消極的でした。  
（これについては、セクション26.2.9で詳しく説明します。）  
昔は、遠く離れた独裁者に武器を売っても、居住者に害を及ぼすことはありませんでした。しかし、サイバー兵器は世界的な影響を与える可能性があります。  
シリアと同様に、その主な焦点は、特に国内外の反体制派イラン人に対する諜報活動にあります。  
それは海外でのスパイ活動と独自の攻撃の両方を開始しました。  
イランのサイバー機能の歴史はCollin AndersonとKarim Sadjadpour [49]によって伝えられています。  
最後に、北朝鮮について言及する価値があります。  
その後、コメディが一般公開された場合、映画館に対するテロ攻撃の脅威が続きました。  
2017年、北朝鮮はWannacryワームが世界中で200,000台を超えるコンピューターに感染し、データを暗号化してビットコインの身代金を要求した後に再び注目を集めました。NotPetyaのように、選択的な復号化の手段がなかったため、破壊的なワームでした。  
その間、それは自動車メーカーである日産とル​​ノー、および台湾のチップファウンドリTSMCでの生産を混乱させ、英国の国立保健局のいくつかの病院に事故および緊急ユニットを閉鎖させました。2019年、北朝鮮のエージェントは、漏洩した国連の報告書で、暗号通貨取引所からの10億ドル以上の盗難でさらに非難されました[346]。  
2.2.5帰属  
一般的な命題としてこれは正しくありません。オンラインでの匿名性は、あなたが思っているよりもはるかに困難です。  
しかし、それが真実である場合もあり、人々は依然としてクライメートゲート事件を指摘しています。  
気候懐疑論者は、地球温暖化の証拠を地球規模の陰謀の証拠として最もよく提示する方法を議論した彼らの何人かを捕らえました。  
人々は、加害者がロシア人であるかサウジアラビア人であるか、あるいはエネルギー会社でさえあり得たかどうか疑問に思います。  
 いずれにせよ、情報公開の準備ができていた可能性があることを示唆している。  
別の可能な州の行動は、Equifaxハックでした。  
訴訟における後の話は、Equifaxがポータルのデフォルトのユーザー名とパスワード「admin」を使用していたことでした[358]。  
役員は、9月7日に一般に通知する前に株を売却しました。議会は激怒し、CEOのリック・スミスは解雇された。  
しかし、盗まれた情報が犯罪的に利用されることはありませんでした。そのため、当時のアナリストは、加害者がアメリカ人の個人データを大規模に求めている国家国家の行為者であると疑っていました[1444]。やがて、中国軍の4人のメンバーがそのために起訴された[552]。  
次にサイバー犯罪に移ります。  
2.3詐欺師  
それが半分より少し多いか少ないかは、定義に依存します（税務申告がオンラインで提出されるようになりましたか？  
 そして、あなたが尋ねる質問について（嫌がらせやネットいじめを数えますか？  
 –しかし、定義が狭くても、それはまだほぼ半分です。  
最近まで、ほとんどの管轄区域の警察はそれを無視するために最善を尽くしていました。アメリカでは「個人情報の盗難」として却下され、個別にカウントされましたが、イギリスでは被害者は2005年から15年にかけて警察ではなく銀行に訴えるように言われました。  
しかし、最終的には、定期的な被害者調査で不正行為について質問し始めた国々で真実が明らかになりました12。  
このセクションでは、2019年に実施したサイバー犯罪のコストに関する調査と、それらが時間の経過とともにどのように変化しているかを取り上げています[91]。  
支払いシステムに対する電子詐欺は1980年代から存在しており、1990年代にインターネットが開かれたときにスパムが届きました。  
現代のサイバー犯罪はおそらく、産業革命の実体経済で起こったのと同じように、詐欺師が彼らの仕事に特化し、上手になることを可能にする地下市場が出現した2003年から5年にさかのぼることができます。  
前のセクションで検討した州が犯した犯罪と、次の調査で検討する他の個人に対して個人が犯した犯罪には、かなりの重複があります。しかし、俳優の動機は有用な主要なフィルターです。  
2.3.1犯罪インフラ  
技術についてはセクション21.3で詳しく説明します。このセクションでは、アクターとそれらが動作するエコシステムに焦点を当てています。  
サイバー犯罪が産業化された今、「仕事」の大部分は、法執行機関の削除の回避に関連するすべての面倒なセットアップ作業を含め、カスタマーサポートやシステム管理などの退屈な役割になっています[453]。  
（さらに、サイバー犯罪業界はコロナウイルスのパンデミックの間に急成長しています。）  
2.3.1.1ボットネット遊牧民  
次の使用はスパムであり、2000年までにEarthlinkスパマーは100万を超えるフィッシングメールを送信しました。その著者はEarthlinkに訴えられました。  
スパマー、フィッシャーマンなど、悪意のあるユーザーが貸し出すことができる専門的に構築され維持されているボットネットを目にするようになりました。 2007年までに、Cutwailボットネットは100万台を超える感染マシンから1分間に5000万件を超えるスパムを送信していました[1832]。  
スパマーの最初の対応はピアツーピアボットネットでした。  
スパムだけでなく、DDoS、ポンプアンドダンプの株式詐欺、銀行の認証情報の収集にも使用されました。  
その後、ビットコインも盗んだ同様のボットネットであるKelihosが続きました。その作成者であるロシア国民は、2017年のスペインでの休暇中に逮捕され、2018年に有罪を認めた米国に移送された[661]。。  
防御側はドメインを購入することから始めましたが、後の亜種は1日あたり50,000ドメインを生成し、業界のワーキンググループは、これらのドメインが単に使用されなくなるとレジストラと合意しました。  
ストームと同様に、ランダム化の使用は両刃の剣であることが判明しました。防御側はドメインのサブセットに座り、感染したマシンのフィードを収集する可能性があります。  
コマンドアンドコントロールシステムを取り除くために何かができるかどうかに関係なく、ボットマスターを逮捕したり、技術的なトリックによって、ボットネット感染の一般的な修正は、感染したマシンをクリーンアップすることです。  
AV企業はツールを提供しており、マイクロソフトはパッチを提供していますが、多くの人々はそれらを使用していません。  
 しかし、帯域幅はISPに費用がかかるため、次のステップは、一部のISP、特にComcastなどのケーブル会社が感染したマシンを特定し、クリーンアップを約束するまでユーザーを「壁に囲まれた庭」に制限することでした。  
2020年には、数万台のマシンで多くのボットネットが見つかり、ほとんどのディフェンダーが対処するには小さすぎます。さらに、多層になる傾向があるいくつかの大きなボットネットがあり、通常は最下部にピアツーピアメカニズムがあり、フットソルジャーボットは、いくつかのコントロールノードと通信し、ドメイン生成アルゴリズムを使用してボットマスターを見つけます。  
2020年のそのようなボットネットの大金は、クリック詐欺のようです。  
最初のMiraiワームは、Xiaomiによって製造され、変更できない既知の工場出荷時のパスワードが設定されたCCTVカメラに感染しました。  
最初の攻撃はDynDNSに対するもので、米国東部海岸でTwitterを6時間ダウンさせました。  
いつでも、6ダースの大規模なボットネット遊牧民がいる可能性があります。  
  
世界の諜報機関とその請負業者向けにマルウェアを作成する数百人のソフトウェアエンジニアに加えて、犯罪市場向けにマルウェアを作成する何百人もの人々がいる可能性があります。誰も本当に知りません（ただし、ハッカーフォーラムでトラフィックを監視して規模を推測することはできます）  
このコミュニティ内には専門家がいます。  
その他は、エクスプロイトがインストールするリモートアクセストロイの木馬を専門としています。他の企業は、回復力のあるコマンドアンドコントロール通信用のピアツーピアおよびDGAソフトウェアを構築しています。さらに、銀行詐欺に特化したペイロードを設計する人もいます。  
各スペシャリスト市場セグメント内には、通常、少数のオペレーターがいるため、そのうちの1人を逮捕すると、しばらくの間、違いが生じます。  
Androidが最も頻繁に使用されているオペレーティングシステムであるWindowsを引き継いでいるため、Androidマルウェアが増加しています。  
 しかし、銀行取引の認証に使用されるSMSを盗むなど、多くの場合、悪いことをするのは単なるアプリです。  
2.3.1.3スパム送信者  
2010年までに、スパムは世界のISPとテクノロジー企業に1年あたり約10億ドルの対抗策としてコストをかけましたが、その事業者はおそらくその1％を獲得しました。  
現在のスパムフィルターを通過するには、絶えず変化するトリックのツールボックス全体が必要であるため、スパムは非常に専門的なビジネスになりました。  
一部のスパムには産業規模の電子メールの侵害が含まれており、被害者にとって費用がかかる可能性があります。約3億5000万ドルは、Yahooが大規模な妥協の後でVerizonに売却された48億ドルの価格から打ち消されました[771]。  
2.3.1.4アカウントの一括侵害  
大規模な電子メールサービスプロバイダーは、毎日数万のアカウントを回復している可能性があります。  
2019年には、この認証情報の詰め込みは、アカウントの侵害が試みられたボリュームの最大数を占めています[1882]。  
プライマリ電子メールアカウントには、攻撃者が運がよければ銀行口座など、他のアカウントの復旧情報が含まれていることがよくあります。  
他のすべてが失敗した場合、侵害された電子メールアカウントを使用してスパムを送信できます。  
これには、特別なビューアをインストールするように要求する無料のポルノサイトから、スポーツ用品の提供や話題のイベントに関するニュースまで、さまざまな状況でのフィッシングルアーが含まれます。  
このようなサービスは、ボットネットによって提供されることが多く、ボットネットは自分の番号を維持する必要があります。彼らは米国とヨーロッパで感染したマシン1,000台あたり10〜15ドル、そしておそらくアジアでは3ドルをサードパーティの顧客に請求するかもしれません。2.3.1.5標的型攻撃者  
彼らはターゲットを調査し、複数のスピアフィッシングを試み、パスワードの回復手順を試み、関連するアカウントに侵入できるかどうかを確認します。  
John Scott-Railtonと同僚は、ExxonMobilの批評家をターゲットにしたハックフォーハイヤー会社であるDark Ba​​sinのしくみを明らかにし、ネットの中立性の擁護者もインドの会社まで追跡しました[1692]。  
  
20世紀に戻ると、クレジットカード番号を盗んだ人々は、商品を購入してからお金を手に入れるためにそれらを売るという問題に行かなければなりませんでした。  
価格は、真の価値が犯罪の連鎖のどこにあるかを明らかにします。クレジットカード番号と有効期限の組み合わせは1ドル未満で販売され、1ドルを獲得するには、CVV、カード所有者の名前と住所などが必要です。  
いくつかのキャッシュアウト企業は、彼らがリスクの一部を移すラバの軍隊を組織しています。  
次に、洗濯屋はラトビアのロシアの銀行を利用し、ロシアのラバが現金を引き出すことになった。  
ビットコインはしばらくの間引き継がれましたが、米国財務省がビットコイン取引所を顧客の特定に向けて一変させ始めたため、価格が変動しやすくなるにつれて、サイバー犯罪コミュニティーでの人気は停滞しました。  
私たちはそれを監視し、サイバー犯罪者がキャッシュアウトを含むサービスを売買するアンダーグラウンドハッカーフォーラムで数千万の投稿から集めたデータベースであるCrimeBBを使用して傾向を分析します[1499]。  
  
暗号通貨が減少した理由の1つは、ランサムウェアの増加であり、これに関与するギャングが被害者にとって使いやすい支払い方法に切り替わったためです。  
2017年以降、ランサムウェアアズアサービスプラットフォームが登場しています。これらのプラットフォームを使用するオペレーターは、多くの場合アマチュアであり、たとえあなたが支払う意思があるとしても、解読することはできません。  
これは2019年から20年にかけて急速に拡大しており、米国で最も注目度の高いランサムウェアの被害者は公的機関です。数百の地方自治体と少数の病院がサービス障害に苦しんでいる[358]。  
しかし、それは国際的な現象であり、多くの民間企業も犠牲になります。  
  
カード決済システムへの攻撃は、カードの紛失や盗難から始まり、1980年代に大規模な偽造が登場しました。多くの企業が詐欺を検出する方法についてほとんど考えずにオンラインで販売を始めたので、ドットコムブームはさらに1990年代に物事を加速させました。犯罪者が盗んだカード番号や関連する機器やサービスを売買する方法を模索したため、2000年代半ばに地下市場が生まれたのはカード詐欺でした。  
「個人情報の盗難」は括弧で囲んで書いていますが、これは実際には昔ながらのなりすましの罪にすぎません。  
21世紀初頭、銀行はお金ではなく、個人情報が盗まれたと主張しました[1727]。  
カード詐欺のエコシステムは現在、かなり安定しています。  
多くのカード番号は、小売業者に対するハッキング攻撃で収集されます。影響を受けた顧客に通知して銀行に払い戻しを行い、再発行されたカードを支払うと、小売業者にとって非常に高額になる可能性があります。  
オンラインバンキングへの攻撃は2005年に増加し、大規模なフィッシング攻撃が登場しました。銀行から送信されたと思われる電子メールは、パスワードを盗んだ銀行の偽のWebサイトに顧客を誘導しました。  
Zeus以降のトロイの木馬は、ユーザーがWebサイトを認識する銀行にログオンするまでPCに潜んでいます。その後、ラバのアカウントに支払いを行い、その活動をユーザーから隠します。いわゆる「ブラウザ内での攻撃」です。  
 Zeusの背後にある詐欺師、および後にDridexバンキングマルウェアは、2019年12月に米国の調査官によって指名され、起訴され、約1億ドルを盗んだと非難されましたが、ロシアでは依然として自由です[795]。  
企業はビジネスメールの侵害にも注意を払う必要があります。この場合、詐欺師はビジネスメールアカウントを侵害し、顧客に銀行口座番号が変更されたことを知らせます。または、詐欺師がCEOになりすまして財務管理者に支払いを行うように命令する場合。そして、あなたの銀行から来たふりをして、支払いを承認するためのコードをリリースするよう仕向ける人々によるソーシャルエンジニアリング攻撃。そのような詐欺の専門性については、銀行、その規制当局、小売顧客のみに直接影響を与える犯罪の増加とともに、第12章で説明します。  
  
銀行以外の多くのセクターには、独自のサイバー犯罪シーンがあります。  
不正に入手した航空券を販売する人々のエコシステム全体があります。これらのチケットは、盗まれたクレジットカード番号で購入されることもあれば、旅行会社や航空会社のシステムを操作またはハッキングすることによって直接入手されることもあります。彼らの飛行距離を盗むことによって直接大衆から詐欺しました。  
それらを疑わしいと知っている乗客の一部は、彼らが疑わしいことを知っていますが、他の人はだまされているため、搭乗口で人々を逮捕するだけでは問題に対処することが困難になります。  
 旅行詐欺の説明と分析については、Hutchings [936]を参照してください。  
  
企業が人を雇い始めて以来、インサイダーによる詐欺は問題となっています。  
主な防御は簿記です。  
このエコシステム全体は、テクノロジーと同様に進化しており、その設計は、監査クライアントに要求を出すBig Fourの会計事務所によって推進され、会計事務所は、会計ソフトウェアとサポートするセキュリティメカニズムの開発を推進します。  
内部告発を含む内部攻撃もあります。これについては以下で説明します。  
2.3.5 CEOの犯罪  
1990年代から、セクション24.6で説明するように、プリンターベンダーは独自のインクカートリッジを使用するように顧客を固定するために暗号化を使用していますが、リフィルを販売する企業は暗号を破っています。  
付属品の制御に暗号を使用することは今や広く行き渡っており、冷蔵庫の水フィルターカートリッジにも見られます[1071]。  
米国の裁判所は、LexmarkとSCCの訴訟でこれは罰金であると決定しました。プリンターベンダーのLexmarkは、セキュリティチップのクローンを独立したインクベンダーに販売したSCCを訴えましたが、敗訴しました。  
ここでは、紛争は合法でオープンです。  
これについては、セクション24.6で詳しく説明します。  
おそらく、最もよく知られている秘密のハッキングは、EUと米国の排出ガス試験スキームに関するフォルクスワーゲンによるものでした。自動車で販売されているディーゼルエンジンは、標準の排出ガス試験条件が検出された場合は問題なく作動し、それ以外の場合は効率的に作動するようにプログラムされています。  
アウディの最高経営責任者はドイツで解雇され、投獄された[1084]。  
他の自動車メーカーも浮気していました。ダイムラーは、2019年にヨーロッパでe860mを確定し[1466]、2020年には4つの政府機関からの15億ドルの罰金と7億ドルの集団訴訟で構成される米国の和解に達しました[1856]。  
製品は、保護システムのクラス全体を破壊するように設計されている場合があります。その例として、第12章で後述するオーバーレイSIMカードがあります。  
中国の人々が2010年代初頭の高いローミング料金を打ち破ることを可能にするように設計されています。  
副作用として、このようなSIMを使用すると、ある種の銀行詐欺を非常に簡単に実行できるようになります。  
明らかな攻撃には産業スパイが含まれますが、今日ではそれよりもはるかに複雑になっています。  
2.3.6内部告発者  
しかし、2018年、バークレイズ銀行のCEOは642,000ポンドの罰金を科され、銀行の内部告発者を追跡しようとしたために彼のボーナスの500,000ポンドを返済するよう命じられました[698]。  
多くの人が、サプライヤから賄賂を受け取っているマネージャーや、スタッフにセクハラをしているマネージャーを報告するなど、かなり平凡なレベルで正しいことをしようとしています。  
それでも、力の不均衡のために彼らはしばしば失います。彼らは発砲し、問題は継続します。  
銀行、警察、オンラインサービスなどの一部の組織には、スタッフが犯罪を報告するためのメカニズムがありますが、管理上の決定に関する倫理的懸念を提起する効果的なプロセスはありません14。  
外部メカニズムは少し良いかもしれません。  
技術に精通したリーク担当者がそのようなサービスを使用することはありません。  
しかし、メカニズムは不格好である傾向があり、それらを促進するWebページは常に、監視リスク、またはそれらに対抗する可能性のある運用セキュリティ対策のいずれかについて潜在的な漏洩者を教育するわけではありません。  
これは主に技術的な問題ではなく、ポリシーの問題です。  
ほとんどの場合、内部告発者が誰であるかはすぐに明らかです。そのため、重要な要素は、内部告発者がセクハラスキャンダルの取り扱いについて2018年にストライキを続けたのかどうかです。たとえば、彼らは今までに別の仕事を得るでしょうか？  
たとえば、ハーベイワインスタインのレイプの有罪判決により、多くの女性がセクハラや差別に抗議することができました。うまくいけば、Black Lives Matterの抗議が同様に色の人々に力を与えるでしょう[31]。  
国民が国会議員の経費請求にアクセスできるかどうかについての長い裁判中に、誰かが記録が保存されているPCに行き、それらをDVDにコピーして、ロットをDaily Telegraphに売りました。  
半ダースの大臣が辞任した。 7人の国会議員と仲間が刑務所に行った。次の選挙で数十人の国会議員が立候補したか議席を失った。そして、納税者に課された事柄のいくつかには、怒りと怒りの両方がありました。  
国の議員が最後まで手を差し伸べているなら、他に何がシステムをきれいにするでしょうか？  
しかし、彼は以前の内部告発者、ビル・ビニーがそれを行おうとした後に逮捕され、嫌がらせを受けたことを知っていました。  
商業企業のそれほど高くないレベルで、あなたのスタッフの1人があなたのお金を盗んでいて、別の人がそれについてあなたに話したいと思っているなら、あなたはその仕事をするほうがよいでしょう。  
2.4オタク  
学者は好奇心から新しい攻撃を探し、専門家から高い評価を得ます。これは、教授の昇進や、私たちを支援する学生の仕事につながります。  
人々が山を登ったりチェスをしたりするのと同じように、趣味のハッカーは挑戦として物事に侵入します。ハクティビストは、邪悪であると考える会社を困らせるためにそれを行います。  
私たちの報酬は、学術出版物、セキュリティコンサルティングビジネスの顧客獲得、学会や政府機関からのメダル獲得、ソーシャルメディアなど、有名です。  
たとえば、過去に人々が私たちのところに来て、自分の銀行カードが盗まれて品物を購入したため、PINが使用されていなかったはずであると銀行が払い戻しをしないと不満を述べたことがあります。  
。  
そのため、一部の研究者はメーリングリストで匿名でバグを公開しました。しかし、これは悪者がすぐにそれらを使用できることを意味しました。  
多くの企業は、脆弱性に対する報酬を提供するバグ報奨金プログラムを運営しています。その結果、独立した研究者が脆弱性を売り込むことで深刻な金銭を稼ぐことができるようになり、これを行うことで1人以上の精力的な研究者が100万ドル以上を稼いだ。  
いったん使用されると、広がり、最終的にはリバースエンジニアリングされてパッチが適用されます。  
いくつかのより伝統的なセクターは、責任ある開示をまだ採用していません。  
会社は負け、馬鹿になり、車の安全性を公表しました（セクション4.3.1の技術的な詳細とセクション27.5.7.2のポリシーについて説明します）  
最終的に、ソフトウェアがすべてに浸透すると、ソフトウェア業界の作業方法もより広く普及するようになります。  
顧客に害を及ぼす問題を隠蔽している企業は、内部の内部告発者または外部のセキュリティ研究者が何が起こっているのかを突き止め、それが発生した場合、多くの場合確立された責任ある開示プロセスが存在する可能性を考慮しなければなりません。呼び出す。  
  
私たちの4番目のカテゴリーは虐待であり、これは通常、財産ではなく人に対する犯罪を意味します。  
最初に、政治的嫌がらせや児童の性的虐待の素材など、規模に応じた犯罪を扱い、次に、学校のいじめから親密なパートナーの虐待に至るまで、そうでない犯罪を扱います。  
2.5.1ハクティビズムとヘイトキャンペーン  
古代の社会は壮大な詩と関係がありました。都市は人々がフォーラムでスピーチをすることにより、直接何百人もの人々とコミュニケーションをとることを可能にしました。書き込みの発明により、さらなるスケールアップが可能になりました。  
活動家たちはマスコミで注目を集めるために競争することを学び、ラジオやテレビが登場するにつれてスキルを磨きました。  
2011年、ワエルゴニムなどの活動家はソーシャルメディアを使用してアラブの春を引き起こしました。これについては、セクション26.4.1で詳しく説明します。  
ヘイトキャンペーンの多くは政府や野党によってひそかに資金提供されていますが、決してすべてではありません。単一問題のキャンペーングループもプレイヤーです。  
DoS攻撃は、実際のブランドのダメージを与えるだけでなく、役員やスタッフに苦痛を与える一方で、サービス拒否攻撃は運用を妨害する可能性があります。支持者に国会議員にメールを送信する完全に法律を順守するNGOから、ボットにニュースストーリーをクリックしてニュースを操作し、メディア分析をプレイして編集者にもっと注意を向けさせる、少しエッジの効いたNGOまで、さまざまな要素があります。問題。  
上記2.2.5で説明されているClimategateスキャンダルは、ハクティビストによる中傷の一例です。  
1990年代、私は楽しくメールとUsenetを使用して、英国議会を通過する監視法案に対して人々を動員しました。これについては、後でセクション26.2.7で説明します。  
オンラインコンポーネントは、スタッフのメンバーに送信された何千もの電子メールで構成されており、頭の中にワイヤーがあるサルの悲惨な画像が含まれています。これは、何百人もの人々が1つのターゲットをオンラインで団結させる「旅団」の初期の例でした。  
しかし、彼らは肉体的なデモンストレーションとメディアへの嫌がらせを続けた。私たちの副首相は彼女の損失を削減することを決め、そして猿の家は代わりにオックスフォードに行きました。  
オンラインシェイミングは抗議の手段として人気が高まっています。  
最初の例は2005年に、ソウルの若い女性が犬が地下鉄の車両で排便した後に片付けができなかったときに起こりました。  
それ以来、他にも多くの事件があった。  
多くの人々が自宅からドックス、SWAT、または猟犬をかけられた[1932]。  
運動はリーダーレスのように見え、絶えず進化しました。1つの継続的なテーマは「社会的司法戦士」に対する不満です。  
怒っているオンライン暴徒の力への認識が高まっているため、地方政治家からライバルを弱体化させようとしている国民国家から、ライバル国の選挙を振り回そうとしている国家まで、あらゆるレベルの政治家が彼らをかき立てています。  
。  
一方、ソーシャルメディア企業はオンラインコンテンツを検閲する必要に迫られており、AIプログラムがジョーク、虐待、陰謀論、外国政府による情報戦争の違いを見分けるのは難しいため、最終的にはもっと雇わなければならないその他のモデレーター。  
  
1990年代にインターネットが政府の注目を集め、どうすればインターネットに対処できるかを疑問視したとき、規制されるべき最初のことは、児童の性的虐待（CSA）の画像でした。  
法的規制により、法執行機関の外部にいる者は調査を行うことが困難であるため、CSA資料の実際の普及率に関するデータはほとんどありません。  
確かに、オンラインの性犯罪に関する多くの法律は不適切に設計されており、被害者の数と被害者の被害を最小限に抑えることよりも、怒りを利用することによって推進されているようです。  
最も悪名高い法医学上の失敗は、イギリスの作戦鉱石でした。これは、26.5.3で詳しく説明します。  
何百人もの無実の男性が命を落としました。  
ほとんどの国では、CSAの削除は、警察または公共部門の規則（米国のNCMECおよび英国のIWF）の下で運営されている規制機関の独占です。  
公共部門の独占は、CSAの資料の所有を厳格責任違反とする多くの国の法律に起因しています。  
また、10代の若者がデートアプリを使用したり、離れた場所にいる関係で発生したインシデントに、親や教師が慎重に対処することも困難になります。  
（CSAの資料は現在、一部の議員のスタッフにとって大きな不快感を与えており、一部の新聞のジャーナリストは、電子メールアドレスを公開することに消極的です。）  
好むと好まざるとにかかわらず、親密な写真をパートナーに送信する（本物で意図したもの）  
これはブダペスト大会からわずか7年後のことでした。その署名者たちは、18歳未満の性的画像が虐待以外の何かであるとは想像していなかった可能性があります。  
10代の若者は、そのような写真を撮ったり共有したりしないように学校の先生からの講義を笑っていますが、最終結果は本当の害です。  
受信者は、たとえ無実であっても、携帯電話に写真を置くだけで犯罪を犯しているので、子供たちは他の子供を設定して非難することができます。  
  
オンラインの嫌がらせといじめは、学校だけでなく職場でも、現代社会では日常生活の事実です。  
英国の年次調査では、子供と若者の約4分の1が絶えずいじめられていることが明らかになっています（口頭で13％、サイバーで5％、身体で3％）。[565]。  
これは16,000世帯との対面インタビューに基づいており、2017年の調査では200万件の脅迫行動が報告され、7％がソーシャルネットワークで作成され、さらに9％が電話で行われました。  
 調査によると、ソーシャルメディアの使用が青年期の幸福度に及ぼす影響は微妙であり、せいぜい小さく、分析方法次第である[1473]。  
ありがたいことに、OECDの死亡率統計はこれも事実ではないことを示しています。15〜19歳の自殺は、1990〜2015年の間に10万人あたり約8名から約7名にわずかに減少しました[1477]。  
2.5.4親密な関係の虐待  
ゲーマーゲートはフラッシュバルブの例だったかもしれませんが、以前の親しいパートナーや他の家族からの保護は大規模に存在する本当の問題です。  
ストーキングはもちろん元パートナーに限定されません。  
しかし、以前のパートナーがそのほとんどを占めており、ほとんどの国の法執行機関は、歴史的に彼らに対して有効なことをすることに消極的でした。  
1つの副問題は、同意のない親密な画像（NCII）の公開です。  
彼女のメッセージは、2015年以降、被害者からの要求に応じてそのような資料を削除している大手サービス会社に届きました[1690]。  
虐待的で支配的な夫を離れる女性が直面する問題は、情報セキュリティの世界で最も困難なものの1つです。  
通常、3つのフェーズがあります。乱用者がデバイスにアクセスして、マルウェアをインストールしたり、デバイスを破壊したりする可能性がある物理的な制御フェーズです。新しい家や仕事などを見つけようとするハイリスク脱出フェーズ。嫌がらせを回避するために場所、電子メールアドレス、電話番号を保護する必要があり、生涯にわたる懸念がある可能性がある場合は、生涯のフェーズ。  
脱出後は、子供のオンライン活動を制限し、相互関係を断つ必要があります。子供に何かを投稿させると、学校の場所が漏洩し、虐待者が上向きになる可能性があります。  
このようなユーザーをサポートするために、責任ある設計者は、ストレスやリスクが高いときの使いやすさについて一生懸命考える必要があります。ユーザーが複数のアカウントを持つことを許可する必要があります。彼らはあなたの履歴をレビューしている誰かがあなたに何も削除されたことを教えてはならないように物事を設計するべきです; 2要素認証、異常なアクティビティ通知、およびシークレットモードをプッシュする必要があります。  
しかし、それは私たちが実際に見つけたものではありません。  
一部の国での大きな問題はストーカーウェアです。これは、パートナー、元パートナー、子供、または従業員を監視するために設計されたアプリです。  
さらに、Absherアプリがあり、サウジアラビアの男性が先進国では受け入れられない方法で女性をコントロールできるようになっています。アプリストアでの利用は、世界中のAppleとGoogleに対する抗議につながりましたが、2020年の時点でまだ存在しています。  
多くの関係は大部分は恩恵を受けていますが、いくつかの厳しい側面があり、参加者は多くの場合、どの側面に同意しません。  
テクノロジーは、偶発的なものから深刻な虐待まで、関係における複数のプライバシー侵害を容易にします。設計者は、世帯はユニットではなく、デバイスは個人ではなく、デバイスの購入者だけがユーザーではないことを認識する必要があります。  
  
構築または運用するシステムは、さまざまな敵から攻撃を受ける可能性があります。  
あなたのシステムは他人を攻撃するためにも使用される可能性があり、これについて事前に考えなければ、深刻な法的または政治的問題に直面する可能性があります。  
すべての脅威アクターが悪いわけではありません。多くのハッカーが責任を持ってバグを報告し、多くの内部告発者は公衆を元にしています。  
 諜報機関および法執行機関は、狩猟時に交通データ分析とコンテンツサンプリングを組み合わせて使用​​し、収集のためにターゲットを絞った収集を使用する場合があります。収集方法は、マルウェアによる法的強制から欺瞞にまで及びます。  
詐欺師は通常、大規模な攻撃には日和見的な収集を使用しますが、標的を絞った仕事には、スピアフィッシングが最適な武器です。諜報機関はより洗練されたツールを持っているかもしれませんが、同じ基本的な方法を使用しています。  
沼地に関しては、選択の武器は、現在、州、活動家グループ、さらには個人の雄弁家によって振られている怒っている暴徒です。使いやすさを考えるだけでは不十分です。あなたも虐待について考える必要があります。  
すべての警察官は、あなたを攻撃したり殺したりした人は通常見知らぬ人ではないことを知っていますが、あなたが知っている誰か-おそらくあなたの学校のクラスの別の男の子か、あなたの継父です。  
あらゆる規模の企業を防御している場合、ネットワーク上の十分な数のマシンが感染していることがわかり、それらがボットネットのゾンビだけなのか、標的型攻撃の一部なのかを知る必要があります。  
ネットワークを監視して十分なログを保持する必要があります。感染したマシンが発見されたときに、ボットネットを構築している子供なのか、視点の喪失に対応して別のボットネットを開発しようとしている攻撃者なのかを判断できます。  
ランサムウェアから回復するためのバックアップ、ビジネスメールの侵害をブロックするための支払い手順など、重要な制御について体系的に考える必要があります。  
この本の残りの部分で詳細を説明します。  
2.7研究の問題  
誰かがいくつかのデータを取得します-多くの場合、ウイルス対策会社からのNDAの下で-いくつかの統計を計算し、彼らの論文を書き、それから就職します。  
2015年以来、私たちはケンブリッジサイバー犯罪センターを設置することでこれを修正しようとしており、そこではスパム、フィッシング、ボットネット、マルウェアに関する大量のデータを研究者の共有リソースとして収集しています。  
サイバー犯罪について調査したい場合は、お電話ください。  
制御システムやその他の運用技術にマルウェアを埋め込もうとする人々は、国家の行為者か、国家に販売するサイバー兵器のベンダーである可能性が非常に高いです。  
しかし、何が起こっているのかを追跡することに関心を寄せているレガシーシンクタンクは1人もいないようです。  
サイバー虐待の研究に関しては、現在いくつかの研究がありますが、技術者、心理学者、犯罪学者、政治学者は十分に話し合っていません。  
より多くの技術者を公共政策の問題に関与させ、技術の現実についてより多くの政策担当者を教育する必要があります。  
  
この章で説明されているトピックに関する膨大な文献がありますが、かなり断片化されています。  
サイバー犯罪の調査については、2012年のペーパー「サイバー犯罪のコストの測定」[90]と2019年のフォローアップ「サイバー犯罪の変化するコストの測定」[91]を参照してください。  
ゲーマーゲートのストーリーは、ゾーイクインの「クラッシュオーバーライド」[1567]で語られています。