私たちは暴力的なスラム街の警察のようでした。  
1はじめにIdeologueは希望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。銀行や軍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本当に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場合があり、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、ハイテク企業のエンジニア、そして何人かの趣味家が住んでいました。  
 （それも研究室から脱出した学生の実験でした。セクション21で話をします。  
2。  
 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、ドットコムブームでの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。  
1。  
 2000年代半ばにアンダーグラウンドマーケットが出現し、状況は変化しました。  
 これにより、製造業が18世紀後半に行ったように、彼らの仕事がうまくなり、スケールアップし、グローバル化することができました。  
また、ソーシャルネットワークの登場により、手作りのウェブページを作成するスキルを持ったオタクだけでなく、誰もがインターネットを利用できるようになりました。  
過去10年間、この脅威の状況は安定しています。  
 Ed Snowdenや他の内部告発者のおかげで、西側の諜報機関の機能と方法について多くのことを知っています。また、中国、ロシア、その他の国家国家の脅威行為者についても多くのことを学びました。  
 マルウェアとボットネットに基づく相当な犯罪インフラストラクチャがあり、私たちが絶えず取り組んでいます。詐欺の大規模な生態系もあります。  
一部の企業は敵対的な政府、一部の企業は他の企業、そして一部は活動家について心配する必要があります。  
 そして、私たちの政治は、オンライン過激主義のダイナミクスにより、さらに二極化するかもしれません。  
 特定のシステムコンポーネント（暗号化など）を設計して、すべての妥当な敵に対抗することもできますが、複雑な現実のシステムでは同じことがはるかに当てはまりません。  
 では、敵対者にはどのような能力があり、どのような動機があるでしょうか？この評価をどの程度確信していますか。また、システムの存続期間中にどのように変化する可能性がありますか？この章では、動機に応じてオンラインおよび電子的な脅威を分類します。  
 次に、動機が主に金銭である犯罪者を扱います。  
 最後に、個人的な理由があり、ネットいじめからストーカーまで、主にその人物に対して犯罪を犯している不正行為者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わっています。  
セキュリティエンジニアリング36ロスアンダーソン2。  
 THE SPOOKS2。  
 何百もの企業が、盗聴、無線傍受、およびさまざまな脆弱性を利用してコンピュータ、電話、その他のデジタル機器を乗っ取る機器を販売しています。  
 潜在的な対戦相手の観点から、4つの代表的なカテゴリ（米国とその同盟国、中国、ロシア、アラブ世界）について説明します。  
2。  
1ファイブアイズジョンレノンが撃たれたときの特定の年齢層の誰もが彼らがどこにいたか覚えているように、2013年以来私たちの貿易に参加しているすべての人は、その年の6月7日金曜日にスノーデンの啓示を知ったときの彼らがどこにいたか覚えています。  
2。  
1PrismIはカリフォルニア州パロアルトのホテルにいて、2011年に科学的訪問者としてGoogleに予定していた訪問の前にGuardianをオンラインで読み、Androidスマートフォンの非接触型決済の開発を手伝いました。  
 朝食後、グーグルプレックスまで車で行ったところ、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。  
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、Iwaが米国人ではないと信じていると言ってタブをクリックすることでした。  
 記事によると、このプログラムは2007年にMicrosoftで開始されました。 Yahooはそれを法廷で戦ったが、敗北し、2008年後半に加わった。 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。2。  
翌日、話の出所が、笛を吹くことにしたNSAシステム管理者のエドワードスノーデン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、米国政府が彼の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逃亡しました。  
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日前に登場しました。それは、FISA裁判所がその年の2月にNSAにすべての通話データレコード（CDR）を引き渡すようにVerizonに命じた方法に関するものでした[814]。  
 しかし、プライバシー法学者会議で破り、NSAがアメリカ人の国内通信を「うっかり」収集していることをNSAがアメリカ人の国内通信を収集していることを証明したときに議会に嘘をついたことを示したため、それは弁護士や政治家の注目を確実に集めました。 '。  
2。  
1。  
 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Echa-lon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との間で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オンにしました[373、374] （セクション26で、より歴史的な背景を説明します。  
6）。  
 コーンウォールだけでも、200本の大西洋横断ファイバーが取り出され、一度に46本が収集されました。  
 次に、電話番号だけでなくIPアドレスなどのより一般的な検索語句をセレクターを使用して選択し、興味があることが判明した場合に備えて30日間保存しました。  
英国はインターネットのバックボーンの約4分の1に物理的にアクセスできます。現代のケーブルは、以前の電話ケーブルの場所に行く傾向があり、19世紀の電信ケーブルと同じエンドステーションの間に敷設されることがよくありました。  
そして資産は確かに重要です。2012年までに、GCHQの300人のアナリストとNSAの250人のアナリストがデータをふるいにかけ、それぞれ40,000と31,000のセレクターを使用して、毎日600mの「電話イベント」をふるいにかけました。  
2。  
2。  
Tempora上で実行されているアプリケーションの1つはMuscularでした。  
 メールはサービスのフロントエンドに向かう途中でSSLを使用して暗号化されている可能性がありますが、その後、各会社のデータセンター間をクリアラインで流れます。  
1 –企業は、ネットワーク上のすべてのものを暗号化するためにスクランブルをかけました。  
それは、あなたが令状を遵守したとしても、可能であればスパイ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。  
図2。  
 そのため、お客様はリンクが暗号化されていると考えており、偶発的なスヌーピングから保護されていますが、バックボーントラフィックを読み取ることができる国や企業からは保護されていません。  
2。  
4特別収集NSAとCIAは共同で特別収集サービス（SCS）を運営しており、その最も目に見える活動は、米国の屋根の近くのプラスチックパネルおよび関連するセキュリティエンジニアリング39ロスアンダーソンです2。  
 世界中の大使館。これらは、セルラー通信（「ステートルーム」として知られているプログラム）を掃除するためのアンテナを隠します。  
 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から、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で説明されているように、コンピューターモニターや他の機器からの電磁放射によって漏洩した情報の収集です。  
2。  
2。  
2。  
5BullrunおよびEdgehillSpecialコレクションでは、サプライチェーンの改ざんがますます増えています。  
 そして、極度のサプライチェーン改ざんの形は、NSAがスイスの会社であるCrypto AGを買収したときでした。この会社は、冷戦中に非同盟国に暗号化機器の主要サプライヤーでした。ストーリーについては、セクション26で詳しく説明します。  
7。  
BullrunはNSAコードネームで、EdgehillはGCHQコードネームで、「暗号化」、つまりスタックのすべてのレベルで供給とサプライヤーを改ざんする年間1億ドルのプログラムです。  
 1つの壮大な事件は、デュアルEC\_DRBGの失敗でした。NISTは、NSAバックドアを含むことが判明した楕円曲線に基づいて乱数ジェネレータを標準化しました。  
2。  
 その結果、今日使用されているシステムの多くは弱い暗号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2NSAがコンピューターにソフトウェアを埋め込むことができないため、NSAがユーザー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、それは賛辞となる可能性があります！ケンブリッジ大学のアイザックニュートンインスティテュート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し、GCHQの上級幹部が50,000ポンドの寄付を募り、「暗号化には興味深いことは何も起こっていません。陛下の政府はこのa↵airsの状態が続くことを望みます。  
セキュリティエンジニアリング40ロスアンダーソン2。  
 THE SPOOKSchapterを次々に読み、本のパート3に戻って、ポリシー履歴についてさらに詳しく説明します。  
2。  
6Xkeyscoreこのような膨大なデータのコレクションでは、それを検索するための優れたツールが必要です。  
2013年7月31日に公開されたNSA文書は、それをインテリジェンスを開発するための「最も広範囲に及ぶ」システムとして説明しています。アナリストは、電子メール、SMS、チャット、アドレス帳のエントリ、および閲覧履歴を検索できます[815]。  
 どうすれば彼を見つけることができますか？」 「イランの暗号化されたすべてのWord文書を表示」および「イランでのすべてのPGP使用を表示」。  
Xkeyscoreは、1つのクエリがすべてのサイトをスキャンする連合システムです。  
一部は海外でハッキングされたシステムのように見え、そこからNSAマルウェアは送信されたクエリに一致するデータを漏らすことができます。  
 ボリュームは、トラフィックデータが30日間保持されるが、コンテンツは3〜5日間のみであるボリュームです。  
 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います。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して、分析者が検出器ですばやく対応できるようにします。  
 たとえば、GCHQとNSAが2015年に発表した、SIMカードの世界有数のプロバイダーであるフランコオランダの会社Gemaltoをハッキングして、数百からのトラフィックを傍受する（必要に応じて偽装する）ために必要なキーを侵害した何百万もの携帯電話[1658]。  
 2014年のスノーデンへのインタビューによると、Xkeyscoreを使用すると、アナリストは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て、世界中を自動的に追跡することができます。  
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セキュリティエンジニアリング41ロスアンダーソン2。  
 SPOOKScanは、Snowdenの貯蔵庫を探索するための良い出発点になります4。  
2。  
7LonghaulBulkによるキーの盗難とサプライチェーンの改ざんだけが、暗号を破る方法ではありません。  
VPNは簡単に破られるようです。 Longhaulと呼ばれる復号化サービスは、暗号文を取り込み、プレーンテキストを返します。  
 これらは何でしょうか？リークは、VPN暗号化のセットアップに使用されたプロトコルメッセージの勤勉な収集を示しているため、一部の暗号学者は2015年に「Logjam攻撃」の一部の変種が、国の攻撃者が使用する1024ビットプライムに対して実行可能であると示唆していますほとんどのVPNと、Di-e-Hellmanキー交換を使用した多くのTLS接続[26]。  
 暗号解読については、第5章で詳しく説明します。  
2。  
8Quantumプロトコルへの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。  
2。  
1。  
Operation Socialistは、2010年から11年にかけてベルギーの主要電話会社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にコレクションの検索エンジンもあります。  
com。  
セキュリティエンジニアリング42ロスアンダーソン2。  
 数十のサーバーにアクセスできます。認証サーバーを含め、さらにアクセスを利用して、サーバーを追跡できるように請求サーバーと会社のコアCiscorouter [734]をカバーできます。  
 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や他の加盟国の法律を数多く作成していることを考えると、これはまるで米国の州知事が州の警官にAT＆Tをハッキングさせ、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月に公表され、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スノーデンのドキュメントを発行しました。  
 通信の責任者であるベルギーの大臣、アレクサンダーデクルーは、ベルギー自身の諜報機関が非公式に作戦を許可したかもしれないと示唆さえしました[735]。  
CNEのGCHQスライドデッキは、トラフィックをリダイレクトすることと、暗号化を「有効にする」（破壊する）ことの両方によって従来型の信号をサポートするために使用され、常に「英国で拒否可能」でなければならないことを説明しています。また、通信の低下や「過激派ウェブ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、「当時、MNOはネットワークセキュリティについて無知でした。  
NSAとその同盟国が使用す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。  
（これらのツールのいくつかは、後で説明するように、NotPetyawormを起動するためにロシア人によって、およびWannacryの北朝鮮人によって再利用されました。  
 これらには、リモートアクセスTrojanSecurity Engineering43Ross Anderson2のインストールに使用できるツールのマニュアルが含まれています。  
 マシン上のスポーク。マシンを地理的に配置し、ファイル（SSH資格情報を含む）、オーディオ、ビデオを抽出するためのコンポーネントを備えています。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。文書に透かしを入れるためのツールでさえ、内部告発者が文書を丸ごと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。  
 こ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の警察が2018年以降、犯罪者が好む暗号化メッセージングシステムであるEncroChatを実行する数千のAndroidフォンにマルウェアをインストールし、800人の犯罪容疑者の逮捕につながったことが明らかになりましたフランス、オランダ、イギリス、その他の地域での不正行為、およびいくつかの警察による汚職と数トンの麻薬の押収[1332]。  
2。  
10アナリストの視点インテリジェンスアナリストには、大きなツールのバッグがあります。  
 一緒に旅行した携帯電話を追跡する「Cotraveler」など、さまざまな便利なツールがあります。  
 このプロセスを「アダプティブメッセージマイニング」と表現するかもしれません。  
 個々のメッセージを読んで得られる詳細ビューと、大量のコレクションを分析することで得られる統計ビューを切り替える機能は、非常に強力です。  
 トラフィックのデータ分析により、さらに多くのことが実現します。暗号化の使用が増加しているにもかかわらず、家との通信により、いつどのくらいの期間、どのアプリまたはデバイスが使用されているかがわかります6。  
価値の高いターゲットを考えると、アナリストがノートパソコンや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。  
たとえば、現代のスマートホームを盗聴してこれを測定したHillとMattuをダウンロードできます[900]。  
2。  
 一方、アナリストはバグメッセージングアプリを使用して、復号化されたコールコンテンツを収集することにより、エンドツーエンドの暗号化を打ち破ります。  
報道はかなり完全です。  
 Ed Snowdenが、彼にインタビューしているジャーナリストが自分の電話を冷蔵庫に入れると言ったのも不思議ではありません。最後に、アナリストはインターネットに不正にアクセスできるプロキシ（通常はボットネット上のマシン）も持っています。  
2。  
1。  
それは、攻撃的なサイバー運用を担当し、その中で真の違いをもたらしたのはStuxnetでした。  
 4つのゼロデイエクスプロイトと2つの盗まれたコード署名証明書を使用してWindows PCを無差別に拡散し、イランのNatanzエンリッチメントプラントで使用されているタイプのSiemensプログラマブルロジックコントローラーが見つかるまで、技術的に洗練されていました。 PCはオペレーターにすべてがきちんと整っていることを保証しながら、破壊的なコマンド。  
 他の2種類のマルウェア（FlameとDuqu）は、類似のトリックと共通のコードを使用して発見され、中東と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には、2002年（Flowershop）にまで遡るマルウェアの痕跡があり、2016年まで動作し続けました（方程式グループツールを使用）[2068]。ああ、そしてゼロデイ脆弱性の価格は急激に上昇しました。  
2。  
12攻撃のスケーリングコンピュータ科学者はアルゴリズムのスケーリング方法の重要性を知っており、攻撃についてもまったく同じです。  
 容疑者の後ろを車の中でラジオと暗号解読装置を使って運転し、リスクを発見して、容疑者の信号をあるセルから別のセルに移動する際にうまく捕まえることを期待している。  
2。  
 どちらも高度なスキルを必要とする作業であり、歩留まりは低くなります。信号を失うのはおそらく4分の1の時間です。  
 フランスのすべての人をハックしたい場合は、おそらくそれが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可能性がありますが、それができればすべてが揃います。  
 戦時中は、敵のレーダー基地を爆破するためにコマンドを送信できますが、1回または2回以上実行すると、若者は多くの歩哨に遭遇し始めます。  
 では、サイバー攻撃をどのように拡大して、1つの発電所だけでなく、対戦相手の電力網全体を破壊するのでしょうか。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、FiveEyesの一般的な制限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だけが拡張可能なサイバー兵器の構築を試みているのではないことを示しています。  
 これにより、多く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。  
2。  
2ChinaChinaは現在、米国の主要な競争相手であり、GDPの点だけでなく、技術の大国としても2番目です。  
ただし、中国国内では、ローカルデータへの無制限のアクセスが要求されます。  
Yahooのシステムが2002年に反体制派のWang Xiaoningをトラップするために使用された後、Alibabaは2005年にYahooの中国事業を引き継ぎました。しかし、王の妻が2007年に米国の裁判所でYahooを訴えたときはまだ騒ぎがあり、Yahooがこの問題について議会を混乱させたことを示した[1760]。  
2。  
セキュリティエンジニアリング46ロスアンダーソン2。  
 THE SPOOKSserver in China [1959]。  
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への批判をすでに破っていて、そして数ヶ月後に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。  
 米国の対外軍事研究局（FMSO）による2004年の調査によると、中国の軍事法理は国を西側との戦争状態にあると見なしています。我々は中国を攻撃して冷戦を続け、破壊的なアイデアをインターネットを通じて輸出することで共産主義体制を打倒しようとしている[1881]。  
したがって、YahooとGoogleはロッキードマーティンやBAeと同様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ヒソの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、中国、チベットの航空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つの機関の近くにあるIPアドレスにサイフォンで送られていました。  
この手法はフィッシングと呼ばれ、誰かが噛み付いたルアーを提供することで機能します。特定の個人を対象とする場合（この場合のように）はスピアフィッシングと呼ばれます。  
PDFファイルを別のファイルに送信すると、埋め込まれた攻撃で到着します。  
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賃貸しているサーバーに突然感染しました。  
 それが出てからしばらくの間、私たちの機器への攻撃と、政府に攻撃を起因する証拠はないと主張した中国人による会議での対処に対処する必要がありました。  
2。  
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ついての映画を見せた[1898]から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。  
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兵器システムを盗んだという国防総省からの漏洩報告でした[1379]。オバマ政権は、窃盗の秘密の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で起訴されました。  
 10代の麻薬使用から閉鎖された同性愛者関係まで、それらを脅迫するために使用される可能性のある情報を漏らすように命じられたSta↵は、トップシークレットクリアランスを申請します。  
 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ことも想定していました。  
中国人が敏感な政府の仕事で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、「IPtheft」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望んでいた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。  
2。  
 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。  
 ウイグル人の携帯電話をハッキングするためのカムペーンは、侵害されたウイグル人のウェブサイト[393]を介して配信された複数のゼロデイ攻撃を含みました。これは、中国のウイグル人だけでなく、ディアスポラも標的にしました。  
 別のアプローチは、ソフトウェアのサプライチェーンを攻撃することでした。 Wicked PandaまたはBariumと呼ばれる中国のグループは、コンピューターメーカーのAsusからのソフトウェアの更新、PCクリーンアップツール、Koreanremote管理ツール、および3つの人気のあるコンピューターゲームを悪用して、数百万台のマシンにマルウェアをインストールしました。バンキング型トロイの木馬ランサムウェアを起動するのではなく、スパイ活動に使用されました[810]。  
 そして中国も社会主義ゲームをプレイしていた：誰かが過去7年間に少なくとも10の西側の携帯電話会社をハッキングし、通話データレコードを濾過したこと、そして加害者は中国軍にリンクされたAPT10ギャングであるように見えた[2017 ]。  
 以前、別の中国企業ZTEを上回っていました。 2018年にGCHQは、ZTE機器が「効果的または実用的に軽減することができない英国の国家安全保障にリスクをもたらす」と警告した[1475]。  
セキュリティ制御ルートはHuaweiで試されました。Huaweiは2010年にオックスフォードシャー州にセンターを設置し、GCHQは同社が英国での販売を許可されている条件としてソフトウェアを調査することができました。  
 Huaweiは多くのコードをコピーしており、理解できないことを把握できず、長年の約束にもかかわらず、多くの問題への取り組みが進展していませんでした。  
中国はHuaweiシステムをハッキングするだけでなく、誰もがそうでした。  
10実際にそのコードで悪意のあるバックドアに巻き込まれた唯一のルーターベンダーは、NSAのDual-ECバックドアを使用してVPNトラフィックを悪用可能にするだけでなく、他のユーザーが悪用できるような不器用な方法でそれを行った米国企業Juniperですそれも–そして少なくとも1つの他の党がそうした[413]。  
セキュリティエンジニアリング49ロスアンダーソン2。  
 英国のバックボーンルーターや盗聴に使用されたシステムから数年。  
 オーストラリアやニュージーランドを含む多数の国々がHuaweiequipmentを全面的に禁止し、2019年にカナダはHuaweiと企業との関係について詐欺を企てたグローバルバンクの詐欺を企てたとして米国を要請したHuaweiのCFO（創設者の娘でもあります）を逮捕しましたイランでの操作。  
 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多くを支援してネットワークを近代化しており、このアクセスにより、5つの目との競争に対抗できる可能性があります。  
戦略的に、問題は中国がHuaweirouterを使用して他の国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ではありません。2。  
 何年もの間、中国の「平和の台頭」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。  
 彼らは時々オンライン操作を伴う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ついての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、中国の貿易政策は攻撃的ではあるが、1970年代の日本との違いはなく、アメリカほど攻撃的ではないと指摘している。新しい冷戦は誤解を招き、最後の冷戦と同じくらい無駄で危険である可能性が高いこと。中国はそれを混乱させる以上に国際秩序を支持している。そしてそれはそれが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]。  
セキュリティエンジニアリング50ロスアンダーソン2。  
 THE SPOOKS2。  
3ロシア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やマルウェアを使用するハッキングチームを補っています。  
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、彼の寡頭政治、正統派キリスト教、同性愛恐怖症、およびファシストのイデオログIvanIlyinの抱擁について、特に2012年の不正選挙以来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、中国の4つの点とは異なります。  
 第2に、ロシアは中国と同様に閉鎖されようとしているが、国内の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め、西側諸国と絡み合っている[605]。  
 これらの介入には、サイバー攻撃と「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）の混合戦略と、拒否の政治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、そしてイタリア、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に見えます。  
 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であり、エストニア人が米国のサービスプロバイダーのように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の電子情報戦争に関する章で詳しく説明します。  
 ロシアとジョージアの間の短い戦争の勃発後の翌年、ロシアのハッカーは、ロシアの愛国者が攻撃するためにジョージアの標的のリストを備えたウェブサイトを開設しました[1990]。  
 親ロシア大統領ヤヌコビッチに対するキエフのマイダン広場での悪党デモ、および約100人のデモ参加者を撃ったロシアの傭兵による2014年2月の介入、ヤヌコビッチは賛成した。  
 彼らの戦術は、ロシアのspe-Security Engineering51Ross Anderson2を組み合わせたものです。  
 平服の制服部隊、ロシア語を話すウクライナ人やロシアによる反乱のプロパガンダ主張の多く、同性愛者やユダヤ人に対してロシアの純粋さを守るために人々を守るのを助けている;これらすべてはさまざまなサイバー攻撃と協調している。  
翌年、紛争が続いたため、ロシアは3つの異なる配電システムで30の変電所を互いに30分以内に停電させ、23万人が数時間電力を失っていました。  
 この攻撃は、マレーシア航空の旅客機の撃ち落としによる乗組員全員の喪失を含む、他の紛争の影響と比較してまだわずかでした。しかし、それは幹線電力を破壊する最初のサイバー攻撃でした。  
NotPetyaワームは、ウクライナのビジネスの大多数が使用する会計ソフトウェアであるMeDocの更新サービスを使用して最初に配布されました。  
 2016年3月から、中国のギャングがベトナム、香港、フィリピンのターゲットに対してこの攻撃を使用し始めました。これはおそらく、サイバー兵器を見つけてリバースエンジニアリングを行った結果です（サイバー兵器を起動せず、共有していると言われています）。NotPetyaワームは、Windowsメモリからパスワードを回復するMimikatzツールとともに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の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攻撃により、銀行、通信会社、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国民投票と米国でのトランプ大統領の選挙によってマークされました。どちらもかなりのロシアの干渉がありました。  
2。  
 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非難された。  
 一部のトランプ関連団体は、さまざまな罪で刑務所に行きました。  
4。  
 一方では、プーチン大統領が権力を掌握して以来、民主主義国家の影響力とルールに基づいた国際秩序を弱体化させ、権威主義的な政府を促進するために、米国上院の対外関係委員会への報告は、ロシアの持続的な政策の物語を示しています左右両方、それができる場所でトラブル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、トランプ氏の選挙はすべてロシアの責任だと信じて警告している。政治エリートとのポピュラーな差別のルーツははるかに古く、より深い[227]。  
8。  
 ティモシー・スナイダーはこれをすべて現代ロシアの歴史と政治の文脈に置いています[1798]。彼の分析はまた、民主主義に対する破壊的な情報戦争のための脚本を概説しています。  
 プーチンは柔道選手です。柔道は相手の強さと勢いを使ってつまずきます。  
2。  
 中東政府はアラブの春の反乱にひどく揺れ動いており、2010年4月から7月にかけてのリビアのように、反乱軍がGoogleマップを使用して米国、英国、フランスの戦闘機のターゲットファイルを生成していたときなど、一部の人々はインターネットをしばらく利用していませんでした。  
アラブ首長国連邦の作戦は、2019年、whistleblower、Lori Stroud [247]によって説明されました。  
UAEの主な手法はWindowsマルウェアのスピアフィッシングでしたが、Karmaと呼ばれる最も効果的なツールを使用して、iPhoneの犯罪者や地元の反体制派をハッキングすることができました。  
2。  
 あるケースでは、英国の大学院生をソーシャルエンジニアリングして、自分のPCにスパイウェアをインストールし、彼のコミュニケーションを追跡しにくくする口実をつけました。  
 UAE政府によるiPhoneマルウェアの使用は、独立した観察者によって文書化されました[1219]。  
 ポストは、サウジアラビアの皇太子モハメッドビンサルマンを命令した人物として露出するようにキャンペーンし、2019年1月に、国家検察官は、ポストの所有者イエズベゾスが浮気をしていることを示すテキストを含む特別版を発行しました。  
 Enquirerhadは、Bezosが入手したいくつかの写真を脅迫しようとしました。彼と捜査官の両方に、この紙が「ニュース収集プロセスにおける電子的な盗聴やハッキングのいかなる形式」にも依拠していないことを宣言することを望みました。  
 捜査官によると、彼のiPhoneはサウジアラビア政府によってハッキングされた[199]。ダメージを与えた悪意のあるWhat-sAppメッセージはCrown Princehimselfの電話から送信されました[1053]。  
さらに不愉快な例はシリアであり、残虐行為の工業化は情報収集を拡大するための3番目のアプローチです。  
 内戦が始まると、容疑者を逮捕していた警察は、容疑者がメールやソーシャルメディアのパスワードを開示しない限り、その場で女性の家族を強姦すると脅迫します。  
攻撃のスケーリングに対するこの被害者ベースのアプローチは、シリアだけでなくアメリカやヨーロッパでも多くのマシンの妥協をもたらしました。  
トロントのJohn Scott-Railtonと同僚のおかげで、私たちは、反体制派を標的にするために使用されているオンライン監視、コンピュータマルウェア、および電話エクスプロイトのさらに多くの文書化された例を持っています。多くは中東とアフリカの国々だけでなく、メキシコやハンガリーにもあります[1219]。これらのツールは、携帯電話のマルウェアから、独自のネットワークで独自の反体制派に対して使用する大量監視ツールですが、信号システムを悪用することで海外の携帯電話を追跡および盗聴できるツールにまで及びます[488]。  
NGOはこのサイバー兵器取引を押し戻そうと試みました。  
 GCHQは、アサド大統領のネットワークに大量の監視機器が存在する場合、セキュリティエンジニアリング54ロスアンダーソン2ではなく、英国のデバイスである必要があると判断しました。  
 THE SPOOKSUウクライナのもの。  
2。  
）したがって、従来の武器販売を巡る倫理的問題は、サイバーの時代でも続いています。実際、これらのツールはアメリカ人、イギリス人、家に座っているが不幸な政府の連絡先リストに載るほど不運な人たちに対しては使用されていないため、さらに悪化する可能性があります。  
制裁によって何年も隔離されてきたイランは、地元のハッカーフォーラムを利用して、独自のサイバー機能を開発してきました。  
 これは米国およびその他の攻撃の標的にもなっていますが、最もよく知られているのはStuxnetでした。その後、CIAの秘密の通信ネットワークを追跡し、多数のエージェントを切り上げました[578]。  
 元の例としては、オランダのDiginotar CAをハッキングして反体制派のGmailを監視することができました。そのShamoonマルウェアは、サウジアラビアの国営石油会社であるAramcoで数千台のPCを損傷しました。  
最近では、2020年4月にイスラエルの水処理プラントを攻撃しました。イスラエルは翌月、イランのバンダルアッバス港を攻撃して対応した[229]。  
 2014年、ソニーピクチャーズが北朝鮮の指導者を暗殺する計画についてのコメディに取り組み始めた後、ハッカーグループはソニーのインフラストラクチャの大部分を破壊し、トップフィルムエグゼクティブのエイミーパスカルを辞任させ、未公開の映画をいくつか漏らしました。  
 同社はこの映画を限定公開にしたが、オバマ大統領が北朝鮮の脅迫をあきらめたとして非難したとき、代わりに完全公開にした。  
 NotPetyaのようなNSA Eternal-Blueの脆弱性を利用していましたが、マルウェアの研究者が強制終了のスイッチを発見したため、阻止されました。  
 2018年、米国司法省は北朝鮮政府のハッカーの両方の事件、および一連の電子銀行強盗（バンコフバングラデシュからの8100万ドルを含む）に対する起訴を解除しました[1653]。  
2。  
5属性属性は難しいため、サイバーは異なるとよく言われます。  
セキュリティエンジニアリング55ロスアンダーソン2。  
 CROOKSE賢い人々は運用上のセキュリティにミスを犯し、それを与えることになります。脅威インテリジェンス企業は、多くの場合、妥当な確率で誤ったフラグ操作さえも属性付けできるようにする多くのデータを収集しています[180]。  
 2009年の気候変動に関するコペンハーゲンサミットの数週間前に、何千人もの電子メールが公開され、そのほとんどはイギリスのイーストアングリア大学の4気候の科学者との間で送受信されました。  
 後に行われた公式調査の結果、メールは文脈から引用されたものであることが判明しましたが、被害は発生しています。  
 しかし、より説得力のある分析の1つは、それが内部リークまたは事故でさえあったことを示唆しています。 1つのアーカイブファイルとそのファイル名（FOIA2009。  
 ここで本当に興味深いのは、電子メールがどのように陰謀論にまとめられたかです。  
 最初の話は、2017年3月8日、ApacheがApache Strutsの脆弱性について警告し、パッチを発行したというものでした。 2日後、ギャングは脆弱なシステムを探し始めました。5月13日、彼らはEquifaxの紛争ポータルにパッチが適用されていないことを発見し、侵入しました。  
 いずれにせよ、違反は回避可能でした。侵入者は、51の内部データベースシステムへのアクセスを許可する平文のパスワードファイルを見つけ、76日を費やして少なくとも145の個人情報を入手しました。  
 幹部らは、9月7日に公衆に通知する前に株を売却した。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目的で使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捜索し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人のメンバーが起訴された[552]。サイバー犯罪者に目を向けます。  
3CrooksCyber​​crimeは、少なくとも先進国では現在、量と金額の両方で、すべての犯罪の約半分です。  
 それでも、世界の法執行機関は通常、予算の1％未満を費やしてそれを費やしています。  
3。  
 その結果、他のすべてと同様に、犯罪がオンラインになったときに、オンラインコンポーネントはカウントされず、犯罪は減少したように見えました。  
同僚と私はケンブリッジサイバー犯罪センターを運営しています。そこでは、スパムやフィッシングマルウェア、ボットネットのコマンドアンドコントロールトラフィックから地下犯罪フォーラムへの投稿のコレクションに至るまで、他の研究者が使用するデータを収集して整理しています。  
コンピュータ詐欺は1960年代から存在しており、注目に値する初期のケースは、1964年から72年にかけて60,000を超える偽のポリシーを作成し、再保険会社に販売し、それらすべてを追跡する特別なコンピュータシステムを作成したことです。  
 しかし、初期の詐欺はほとんどが家内工業であり、個人または小グループがクレジットカード番号を収集し、次に偽造カードを店で使用したり、カード番号を使用して通信販売商品を入手した。  
サイバー犯罪を理解するには、共有インフラストラクチャー構造を最初に検討し、次に利益を上げるために行われる主要なタイプのサイバー犯罪を検討するのが便利です。  
2。  
1犯罪インフラ2005年以降、アンダーグラウンドマーケットの出現により、ボットネットの遊牧民、マルウェアの作成者、スパムの送信者、キャッシュアウトオペレーターなど、犯罪インフラのプロバイダーとしての専門性が高まっています。  
3;このセクションでは、私の焦点は、俳優と彼らが活動する生態系にあります。  
サイバー犯罪が産業化された今、「職務」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む、カスタマーサポートやシステム管理などの役割を担っています[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。  
3。  
3。  
1ボットネットの飼い主最初のボットネット–侵害されたコンピューターのネットワーク–は、1996年にニューヨークのISP Panixを攻撃し、病院内の侵害されたUnixマシンを使用してSYNフラッド攻撃を行った[368]。  
 サイバー犯罪者が組織化し始めると、大幅なスケールアップがありました。  
 ボットは最初にコマンドアンドコントロールサーバーに指示を求めて連絡します。これらは、感染マシンを監視し、それらのリストをISPや企業に提供するために悪用穴を使用するために、脅威インテリジェンス企業に引き継がれるか、引き継がれます  
 2007年、ストームはWindowsマルウェア全体の8％を占めるまでに急増しました。ほとんどの場合、電子メールの添付ファイルにあるマルウェアによってマシンに感染し、eDonkeyピアツーピアネットワークを使用して他の感染マシンを見つけました。  
 Defenderは、ボットアドレスのリストを収集するためにこのネットワークに参加する多くのピアを取得したため、ボットをクリーンアップでき、2008年後半までにStormはサイズの10分の1に削減されました。  
次の犯罪の革新は、コンフィッカーボットネットであるドメイン生成アルゴリズム（DGA）によってもたらされました。  
 防御側はドメインを購入することから始めましたが、後の変種は1日あたり50,000ドメインを生成し、業界ワーキンググループはこれらのドメインを単に使用するだけではない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できます。  
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企業はツールを利用可能にし、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。  
 2019年までに、セキュリティエンジニアリング58ロスアンダーソン2。  
 人々は今、wifiにあらゆる種類のデバイスを持っているため、あまり一般的ではなくなり、その多くはユーザーインターフェイスを備えていません。人間のユーザーとのコミュニケーションが難しくなっています。  
 歩兵をいくつかの小さなボットネットに断片化すると、防御ノードがそれらすべてを潜入することが難しくなりますが、制御ノードは、防御ノードが到達しにくい場所に配置される場合があります。2016年10月以降の最新のイノベーションは、IoTデバイスを悪用するボットネットのファミリーであるMiraiです。  
 Miraiボットネットは、インターネットのIPv4アドレススペースをスキャンして、通常、電源投入から数分以内に感染する他の脆弱なデバイスを探します。  
 それ以来、1000以上のバリアントがあり、研究者はこれらを調査して、何が変更されたかを判断し、どのような対策を使用するかを考え出しました。  
 たとえば、Miraioperatorsは、数十人が関与している可能性がある2つまたは3つのグループのようです。  
3。  
2マルウェア開発者世界の諜報機関や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）。  
 一部は、脆弱性をエクスプロイトに変換することに集中しています。これは、スタックカナリア、ASLR、およびセクション6で後述するその他の手法を使用する最新のオペレーティングシステムでは重要なタスクです。  
1。  
 最も価値の高い操作は、ウイルス対策会社からの最新の対策に対処するために一定のアップグレードで維持されるプラットフォームのようです。  
 一部のプロバイダーは、ロシアのように国民を引き渡さない管轄区域に拠点を置いており、ロシアのクライムウェアは、ロシアの国家主体だけでなく他の主体によっても使用されています。  
 中国および中古の古い電話が多い国では、これはセキュリティエンジニアリング59ロスアンダーソン2を使用するソフトウェアである可能性があります。  
 Androidフォンをルート化するCROOKSunpatchedの脆弱性。米国とヨーロッパにはパッチが適用されていない電話がたくさんあります（多くのOEMは電話が販売されなくなるとパッチの提供を停止するため）が、銀行取引の認証に使用されるSMSを盗むなど、多くの場合、悪いことをするアプリにすぎません。  
3。  
3スパムの送信者1990年代半ばにインターネットが一般に公開されたとき、スパムは小規模に届きました。2000年までに、Earthlinkのスパマーが数百万のフィッシングメールを送信しているのを目にしました。  
 主な受益者は、Yahoo、Hotmail、GmailなどのWebメールサービスだった可能性があります。 2010年代には、数億人がサービスの利用に切り替えました。  
 ランサムウェアをインストールするためにスパムを使用したい場合は、ゼロからすべてを学ぶよりも、既存のサービスを支払うほうがよいでしょう。  
Yahooが大規模な妥協の後にVerizonに売却された8bnprice [771]。  
3。  
4アカウントの一括侵害一部のボットネットは、パスワードやパスワード回復の質問を推測することで、常に電子メールやその他のオンラインアカウントに侵入しようとしています。  
ピークがあり、通常、ハッカーが1つのWebサイトで数百万のメールアドレスとパスワードを侵害し、他のすべてのWebサイトでそれらを試します。  
 侵害されたアカウントは、さまざまな方法でそれらを悪用するトポピートで販売されます。  
 これらは、立ち往生した旅行者などの詐欺にも使用できます。被害者は、外国で強盗され、ホテル代金を支払うための緊急の経済的支援を求めていることを友人全員にメールで送信します。  
テーマの変種は、ペイパーインストールサービスで、電話またはPCにマルウェアを埋め込んで注文し、大規模に提供します。  
 ドライブバイダウンロードなどのより技術的な手段を使用することもできます。  
セキュリティエンジニアリング60ロスアンダーソン2。  
 CROOKS2。  
1。  
 彼らはターゲットを調査し、複数のスピアフィッシングの試みを行い、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。  
 JohnScott-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の仕組みを明らかにし、中立性の擁護者もネットで追跡して、インドの会社を追跡しました[1692]。  
3。  
2。  
1。  
 今日では、侵害された銀行の信用証明書を地下市場で購入して悪用する専門家がいます。  
キャッシュアウトの手法は数年ごとに変化します。パスは世界のマネーロンダリング管理を通じて発見され、規制はそれらをブロックするように調整されます。  
 2000年代の半ばに戻って、ラバは店に行って盗まれたクレジットカードで商品を購入するドラッグユーザーである可能性があります。その後、外国企業を代表する「エージェント」に大きな収益を約束する広告によって、知らないうちにラバが採用されたが、彼らは個人の銀行口座を通じて盗まれた資金を送金するために使用された時期があった。その後、コスタリカに本拠を置く無認可のデジタル通貨であるLibertyReserveは、それが閉鎖され、その創設者が2013年に逮捕されるまでのすべての準備期間でした。  
スパムと同様に、キャッシュアウトは常に進化している攻撃防御ゲームです。  
 また、深刻な法執行機関の注意を引くのに十分な規模になるまで、規模を拡大できるギャングを支持しているようです。2020年に、1人のSergey Medvedevが2010–15の期間に実際の損失に5億6,800万ドル以上の損害を与えたとして有罪を認めました[1928]。  
3。  
3。  
7ランサムウェア暗号通貨の減少の理由の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、ランサムウェアサービスとしてのプラットフォームを目にしてきました。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、解読することができません。  
 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を起こしました[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。  
2。  
2銀行および決済システムへの攻撃カード決済システムへの攻撃は、カードの紛失および盗難から始まり、1980年代に偽造スケールが登場しました。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。犯罪者が盗まれたカード番号や関連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を生み出したのはカード詐欺でした。  
 「なりすまし」は括弧で囲んで書いていますが、これは実際にはなりすましの昔ながらの存在です。  
 21世紀初頭、銀行はお金ではなく、あなたの身元が盗まれたと主張するようになりました[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。影響を受ける顧客に通知し、再発行されたカードに対して銀行に払い戻しを行うと、小売業者にとって非常に高額になる可能性があります。  
セキュリティエンジニアリング62ロスアンダーソン2。  
 オンラインバンキングの攻撃は、2005年に大規模なフィッシング攻撃の到来とともに増加しました。銀行から送信されたように見える電子メールは、パスワードを盗んだ銀行のWebサイトを模倣するように顧客を誘導しました。  
 Zeusとそれ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aPC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「ブラウザ内攻撃」。  
）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月に米国の捜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、acrookはビジネスメールアカウントを侵害し、銀行口座番号が変更されたことを顧客に知らせます。または、詐欺師がCEOになりすまして、財務コントローラーに支払いを注文する場合。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に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、および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。  
2。  
3セクター別サイバー犯罪エコシステム銀行以外の多くのセクターには、独自のサイバー犯罪が確立されています。  
 航空券を不正に入手した人々の生態系全体が存在します。航空券は、盗まれたクレジットカード番号で単に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、これらの企業での腐敗者によって予約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公共。  
 それらを使用する乗客のなかには疑わしいことを知っている人もいれば、だまされている人もいます。搭乗口で人を逮捕するだけでは問題に対処するのが困難です。  
）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。セキュリティエンジニアリング63ロスアンダーソン2。  
 CROOKS2。  
4内部攻撃企業が人を雇い始めて以来、インサイダーによる詐欺が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the Big Fourの会計事務所によって推進されており、監査クライアントが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ています。  
 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。  
3。  
 セクション24で説明するように、1990年代以降、プリンターベンダーは暗号化を使用して、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しています。  
 ゲーム機メーカーはアフターマーケットベンダーとまったく同じゲームをプレイしています。  
 多くの顧客はこの厄介なものを見つけ、コントロールを回避しようとします。  
 そのため、現職者は、製品をロックするために見つけることができる最高の暗号技術者を雇うことができ、チャレンジャーは、ロックを解除するために見つけることができる最高の暗号分析者を雇うことができます。顧客は、あらゆる方法でハッキングできます。  
国家関係者と同様に、企業は複数の博士号、数百万ドルの資金調達、および電子顕微鏡などの資本資産を備えたチームを編成する場合があります13。  
6。  
 おそらく、最もよく知られている秘密のハッキングは、EUと米国の排出量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;車で販売されているディーゼルエンジンは、標準の排出量試験条件を検出した場合にクリーンに、そしてそれ以外の場合は効率的に実行するようにプログラムされています。  
VWhasは、刑事上および民事上の罰金と補償をカバーするためにe250bnを確保しました。  
4つの政府機関による50億ドルに加え、7億ドルの集団訴訟[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。たとえば、第12章で後述するオーバーレイSIMカードです。  
セキュリティエンジニアリング64ロスアンダーソン2。  
 CROOKSは、中国の人々が2010年代初頭の高いローミング料金を打破できるように設計されています。  
 副次的な影響として、このようなSIMにより、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。  
 明白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。  
3。  
 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、銀行で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に命じられました[698]。  
 多くの人が正しいことをしようとしています。たとえば、サプライヤーから賄賂を受け取っているマネージャーや性的嫌がらせ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では、犯罪を地域ごとに報告するメカニズムを備えていますが、管理上の決定に関する倫理的懸念を提起するための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、潜在的な漏洩者に監視リスクまたはそれらに対抗する可能性がある運用上のセキュリティ対策について常に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わかります。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かどうかです。  
4。  
 たとえば、彼らは今までに別の仕事を得るでしょうか？これは、正式な法的保護の問題だけでなく、文化の問題でもあります。  
しかし、匿名性が役に立った例は、2008–9年の英国議会支出スキャンダルでした。  
 同紙は、国会議員が議会のウェブサイトで多くをあきらめて発表した5月から6月にかけて、割賦のジューシーな部分を公開しました。  
 内部告発者は技術的に犯罪を犯した可能性がありますが、彼らの行動は明らかに公益のためでした。今や議会の経費はすべて公的であるはずです。  
 しかし、彼は以前の内部告発者であるビルビニーが逮捕され、それを試みた後に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、あなたの立場の1つがあなたのお金を盗んでいて、もう1人がそれについてあなたに伝え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。4Geeks攻撃者の3番目のカテゴリは、私のような人々です–脆弱性を調査し、修正できるように報告する研究者。  
セキュリティ企業で働く研究者は、ニュース価値のあるエクスプロイトも探します。BlackHatなどの会議での宣伝は、新しい顧客を獲得することができます。  
 法律の正しい側であろうとなかろうと、私たちは好奇心をそそる内向的な人であり、コントロールを感じる必要がありますが、課題を受け入れて「急ぐ」ことを求めます。  
 時には刺激から立ち直るので、私たちが所有しているものを固定するのを妨げる何かを回避することができます。時には利他主義の要素もあります  
 私たちはこれらのケースのいくつかを調査し、セキュリティエンジニアリング66ロスアンダーソン2を発見しました。  
 THE SWAMPチップおよびPINシステムに対するNo-PINおよびプレプレイ攻撃（バンキングの章で説明します（悪者はこれらの攻撃を実際に発見しましたが、私たちはそれらを複製して被害者の一部に正義を与えました）。  
 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、これは悪者がそれらをすぐに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、独立した研究者は脆弱性を売り込むことで深刻な金銭を稼ぐことができ、これを行うことで1人以上の熱心な研究者が100万ドル以上を稼いでいます。  
 それらが使用されると、広がり、最終的にリバースエンジニアリングおよび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。  
 会社は負けて、彼ら自身を馬鹿にして、彼らの車の不安を公表しました（技術的な詳細についてはセクション4で説明します）。  
1およびセクション27のポリシー。  
7。  
 最終的に、ソフトウェアがすべてに浸透するにつれて、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、その場合、確立された責任ある開示プロセスが呼び出される可能性を考慮しなければなりません。  
2。  
 これらは、学校でのネットいじめから、国の主催によるFacebookの広告キャンペーンに至るまで、人々を死の脅迫で議員たちに押し付けさせるものです。  
2。  
1ハクティビズムと憎悪のキャンペーンプロパガンダと抗議はテクノロジーのように進化した。  
 16世紀に印刷が普及したことで、セキュリティエンジニアリング67ロスアンダーソン2が生まれました。  
 沼地は第17の宗教戦争、第18の日刊新聞、そして第19のマスマーケット新聞である。  
インターネット時代の活動主義は、オンラインメディアを利用して、議員に手紙を書くなど、従来のロビー活動を動員することから始まりました。 2000年代には、IndymediaやAvaazなどの組織が専門知識を開発しました。  
4。  
 それ以来、政府は取り締まりを開始し、活動はオンラインのハットキャンペーンや急進主義にまで広がりました。  
 あなたが何百人もの人々に怒りメールやつぶやきを送るように動機づけることができるなら、受信側の会社や個人は面的な問題を抱えている可能性があります。  
活動家は、その目的、組織の一貫性、そして法律を破る範囲が異なります。  
 それから、立派な新聞に行く内部告発者、Twitterアカウントの穏やかな匿名性の背後にある人々に嫌がらせをする政治的パルチザン、標的の企業に侵入して彼らのウェブサイトを破壊するハッキング犯、あるいはそれらを攻撃するハッカーもいます。  
2。  
 トップエンドには、テロリストの罪で刑務所に入れられるハードコアタイプがあります。  
2。  
 霊長類を研究に使用するためにサルの家を建てる計画のために、動物解放戦線が私の大学を標的にした2003年にハクティビズムの終焉を迎えました。  
 私たちは彼らの電子メールアカウントを閉鎖することでそのオンライン攻撃に十分簡単に​​対処しました。  
 一部の指導者たちは、地元の製薬試験会社で駐屯地を襲撃し、医学研究者の車の下に爆弾を配置した後、テロ行為により投獄された[21]。  
 インシデントがバイラルになったときに自警団のフラッシュモブが形成されるなど、それは非常に自然発生的な場合があります。別の乗客が事件を撮影し、それをオンラインに置いた。数日のうちに、「犬のプーガール」は大学のコースを放棄して身を隠しました[418]。  
セキュリティエンジニアリング68ロスアンダーソン2。  
 THE SWAMP Twitterなどのプラットフォームの力がゲーマーゲートで明らかになり、2014年8月に元ボーイフレンドによって公然と公然と作られた女性のゲーム開発者についての虐待的なコメントによって引き起こされた嵐、およびゲーム業界における女性の異教徒批判の激流へとカスケード業界の男性が支配する文化を批判したフェミニスト。  
 嫌がらせは4Chanなどの匿名のメッセージボードで調整され、攻撃者は特定の標的に集まり、主流の保守的なジャーナリストからも批判されました[1130]。  
 それは2年後の2016年の選挙に影響を与えたオルタナティブライトムーブメントの発展に貢献したようです。  
 怒っている暴徒は先進国の現代政治の不愉快な特徴です。それほど発展していない国では、インドなどの国々で実際のリンチが行われているため、事態はさらに悪化します（与党のBJP党は、少なくとも2011年以来、政治的反対者や市民社会の批評家に嫌がらせをするためにトロール軍を構築しています[1637]）。  
 一方、ソーシャルメディア企業はオンラインコンテンツの検閲を迫られており、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語るのは難しいため、結局はますます雇わなければならないモデレーター。  
4以下。  
5。  
 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ついてはほとんどデータがありません。  
 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るようです。  
最も悪名高い法医学上の失敗は英国の作戦鉱石で、26で詳しく説明しています。  
3。  
 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およびセキュリティエンジニアリングの69ロスアンダーソン2）の下で運営されている規制機関の独占です。  
 THE SWAMPthe UK）、数日から数週間かかります。政府が銀行がフィッシングサイトへの対処に使用する民間の請負業者を利用する場合、事態はより迅速に進むでしょう[938]。  
これは、通常の虐待チャネルを使用してそのようなコンテンツを処理することを困難にするだけでなく、それを武器にすることも可能にします。抗議者はそれを標的に送信し、警察に報告することができます。  
 技術を理解せずにタフな話をしたい議員が原因で、全体が混乱しています。  
）ティーンエイジャーの間でセクシングの人気が高まるにつれて、法律と規範のギャップが生じています。  
 これは、ブダペスト条約からわずか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、最終的な結果は実害です。  
 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行為をしているので、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。  
2。  
3学校や職場でのいじめオンラインでの嫌がらせやいじめは、現代社会では学校だけでなく、職場でも日常的に行われています。  
 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（13％が口頭、5％がサイバー、3％が肉体的）一方で、約半分がいじめられている（それぞれ24％、8％、9％）[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200万件の脅迫行為が報告されており、7％がソーシャルネットワークで、さらに9％が電話で行われました。  
それでも、一部のコメンテーターがソーシャルメディアの使用にリンクしている、10代の自殺の増加についてのメディアでの話があります。  
5。  
2。  
4親密な関係の乱用内部告発者（企業に対する内部者の脅威）について説明して最後のセクションを終了したのと同じように、親密な関係の乱用、家族や個人に対する内部の脅威でこのセクションを終了します。親密なパートナーによる虐待は、女性の27％、男性の11％によって引き起こされています。  
 特に有名人は、ジョンレノンの場合のように、一度も会ったことのない人々にストーキングされる可能性があります。  
 テクノロジーによって被害者の窮状はさらに悪化しています。  
 彼女のメッセージは、2015年以来、被害者からのそのような材料の要求を取り下げてきた大手サービス会社に伝わりました[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、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物理的な制御フェーズです。新しい家、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、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、別居段階。  
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、ストレスが高く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。彼らはあなたの歴史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;彼らは、2要素認証、異常なアクティビティの通知、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。  
6。  
 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よう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可能性は、世界中のAppleとGoogleに対する抗議につながっていますが、2020年の時点ではまだ存在しています。  
 多くの関係は大部分は有益ですが、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、偶然から深刻な虐待に至るまで、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。  
2。  
 あなたを攻撃する可能性のある人と方法を理解することが重要です。また、あなたがどのように攻撃されたのか、誰が攻撃したのかを把握できることも重要です。  
この章では、敵を4つのテーマに分けました。スプーク、クルック、ハッカー、沼です。  
 （もちろん、「私たちの」スパイは良いと考えられていますが、「彼ら」は悪いです。道徳的価値観は、公共の利益と私的な利益に依存しています。  
 詐欺師も詐欺師もマルウェアを使用して、インフラストラクチャとしてボットネットを確立しています。  
 特定のビジネスセクターに接続されたサイバー犯罪エコシステムもあります。基本的に、犯罪はそれが拡大できる場所で進化します。  
7。  
 虐待を拡大する方法はたくさんあります。システムを設計するときは、それに対する犯罪やそれを使用する虐待がどのように拡大するかを理解する必要があります。  
個人的な虐待も重要です。  
 これはセキュリティ研究コミュニティでは無視されています。おそらく私たちが主に利口な白人またはアジア地域の安定した家族の男の子であるからです。  
 したがって、パッチ適用やウイルス対策に依存するだけでは不十分です。  
 インシデントに対応するための計画を立て、法医学捜査を誰に依頼すればよいかを知っておく必要があります。そのため、CEOがテレビカメラの前で上陸した魚のように息を切らさないでください。  
 大企業に助言している場合、彼らはすでにこれの多くを持っているはずであり、それが中小企業である場合、彼らが十分にそれを行う方法を考え出すのを助ける必要がある。  
2。  
 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年以降、CambridgeCyber​​crime Centreを設置して、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向けの共有リソースとして収集することで、この問題の修正に努めています。  
 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のあるレガシーシンクタンクは1つもないようです。  
サイバー虐待の研究に関しては、いくつかの研究がありますが、技術学者、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。  
 WeSecurity Engineering73Ross Anderson2。  
 さらに読む公共政策の問題にもっと多くの技術者を巻き込み、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。  
2。  
 スノーデンの啓示の出発点は、グレングリーンウォルドの本「隠れるべき場所なし」[816]かもしれません。ロシアの戦略と戦術の説明については、米国上院の対外関係委員会への2018年の報告書[385]を参照してください。そして、プロパガンダの歴史への素晴らしい紹介については、Tim Wuの「The Attention Merchants」[2050]を参照してください。  
 BillChamblissなどの犯罪学者は、前世紀の海賊行為や奴隷制から、最近の諜報機関による薬物や武器の拷問や暗殺まで、国家組織犯罪を研究してきました。これにより、違法な監視を評価するためのより広いコンテキストが得られます。  
 最後に、Wannacryを止めたマルウェアの専門家であるMarcus Hutchingsの話は[811]にあります。