サイバー攻撃とマルウェア

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
基盤ネットワーク研究グループ
嶋田 創

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

目的から考えるサイバー攻撃の分類

- 以下の4パターンで分類すると事後対応を考えやすい
  - もちろん、例外や攻撃成功後の目的の移行なども考える

	金銭目的	金銭目的でない
無差別な攻撃	• バラマキ型ウィルスの利用 ✓ PCなどを乗っ取って悪用する(時間貸し) ✓ 最近だとランサムウェアも • 最近では、ネット接続端末が増えていて防衛が大変	• 技術力の誇示や愉快犯 ✓ 昔のコンピュータウィルスやワーム ✓ コンピュータ制御されている機器を誤動作させる
標的を絞った攻撃	• 企業や組織を狙った標的型攻撃 ✓ 機密/個人情報などの窃取 ✓ 業務妨害と脅迫の組み合わせ(ランサムウェアも)	• ハクティビスト(政治的主張などを目的とした攻撃) ✓ Webサイトへのサービス不能攻撃 ✓ Webサイト書き換え(主張を入れ込む)

攻撃の例

- 無差別なもの
  - RAT(後述)でボットネットを作って利用権を売る
  - キーロガーでクレジットカード情報などの決済情報を得る
  - ランサムウェアでデータを暗号化(+一部暴露)して身代金要求(脅迫)
- 標的を絞ったもの
  - (D)DoS攻撃(後述)で業務妨害しつつ脅迫
    - 業務妨害自体が目的のこともある
  - RAT(Remote Administration Trojan)を送り込んで機密情報の窃取
  - 特定の産業システムの破壊を目的とした攻撃
    - 特に電力などのインフラ系
  - 金銭取扱システム(POS, ATM)へのマルウェア感染目的の攻撃
    - 利用者のクレジットカード情報の窃取

参考: 金になる情報@ブラックマーケット(2017頃の情報)

- クレジットカード情報: $4-$20
  - どこで発行されたかによって価値が違う
- 本人認証に使われる情報: $1-$3
  - 社会保障番号、生年月日、など
- RATソフトウェア一式: $20-$50
- Webサーバ乗っ取り: $100-$200
- DDoS攻撃: $60-$90 / day
- 感染して乗っ取ったコンピュータ: $120-$200 / 1000台

主な攻撃者の種類分け

- 金銭目的の犯罪を行なうグループもしくは個人
  - 非常に数が多い
  - あまりにも活発な所は外部から名称が付けられることも
    - 有名どころはAPT28(別名 fancy bear, Sednit, など)
- ハクティビスト
  - サイバー攻撃で政治的主張をしたい人
    - Anonymousや某過激派が代表格
  - 反捕鯨関係がよくDoSをかけていた(OpKillingbay、OpWhales、OpSeaWolrd、など)
- スクリプトキディ(とその亜種)
  - 基本的にネットに転がっているツールを使うだけ
  - たいていはツールを使うだけだが、勉強熱心で成長性の高い人も
    - 個人的には、ツールを適切に使いわけて目的を達成できるようになればスクリプトキディを卒業していると思う

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

マルウェアとは

- MALicious softWARE(悪意のあるソフトウェア)の略
- かつてはよくコンピュータウイルスと呼ばれていたが、最近はマルウェアと称すことが多い
- 「コンピュータウイルス」の時代との違い
  - 愉快犯や技術誇示から犯罪の道具へ
  - おおっぴらに感染/拡散しない
    - 特定のグループ/ネットワークのコンピュータにのみ感染
    - そもそも、あまりばらまくと発見される可能性が高くなる
  - おおっぴらに怪しい通信したりしない
    - 他の通信(最近はHTTP(S)通信/Webアプリ)にまぎれて通信したりします
  - おおっぴらに破壊活動をしたりしない
    - ただし、発見されると証拠隠滅に動くこともあります

最近のマルウェアの傾向

- 年あたりの新種マルウェアの個数は億を超える[1]
  - すでに悪い人の間ではマルウェア作成ツールの利用は広がっている
    - 新規マルウェアを作るコストは下がっている
    - 「検知の可能性がある使い回しより、毎回新規に作った方がいいんじゃね?」と考えていると想像
  - 「動作は前にあるものと同じだが、本体のファイルのハッシュ値が違うから」レベルで別物扱いされている物も含まれているだろうが…
- (1,2日レベルの差で)アンチウイルスソフトウェアによって検知されたりされなかったり
  - アンチウイルスソフトウェア会社も献体をあつめるのが大変?
  - 「怪しい」と思ったら、いくつかのアンチウイルスソフトウェア(無償版など)でスキャンをかけてみるのもあり
    - ちゃんと最新の検知情報定義ファイルに更新してからスキャンすること
  - VirusTotalなど検体を集めているサイトもある(機密誤アップ注意)

[1] https://japan.zdnet.com/article/35116774/

マルウェアの分類(1/3)

複数の機能を持っているマルウェアは珍しくない点に注意

- ドロッパ(ダウンローダ)
  - より高度なマルウェアを送り込む
  - 他のファイル形式の脆弱性を利用した実行ファイルのカプセル化
- スパイウェア(トロイの木馬)
  - 金融関係情報や各種サービス用ユーザ名/パスワードの窃取
  - ファイル送出、キー入力の記録、スクリーンショット取得などの機能
- バックドア作成
  - 遠隔で司令を受けて動作可能な口をインターネットに向けて開く
  - 他にも悪用に便利なツールセットをまとめて導入も →ルートキット
- ボットネットクライアント
  - 司令を受けての一斉の外部攻撃などの動作を目的としたマルウェア

マルウェアの分類(2/3)

- RAT(Remote Administration Trojan)
  - トロイの木馬、バックドア作成、ボットネットクライアントの発展
- ランサムウェア
  - ファイルを暗号化した上で、「暗号化解除して欲しければ…」と脅迫
  - 最近だと、暗号化と平行してファイルを窃取して、窃取したファイルの公開(一部を公開)しての脅迫も行う
    - 機微な個人情報を扱う所は公開の方が怖い
- マイニングマルウェア
  - マルウェアをばらまいた者に収益が入る形で仮想通貨を採掘
  - Webページ側に設置して特定Web閲覧時のみJavaScriptを走らせて採掘する物は、個人的には、悪質さは無いと考える
    - むしろ、悪質なWeb広告の方がはるかに有害

マルウェアの分類(3/3)

- フリースウェア(fleece + software)
  - アプリ削除後も課金を続ける悪質なサブスクリプション型アプリ
- スケアウェア(scare + software)
  - 「ウィルスが検出された」とかポップアップを出して金を巻き上げる
    - よくあるパターン: 全く役に立たないソフトウェアを売りつけられる
  - 最近は、スケアウェア起動後に「遠隔サポート」と称して、遠隔でいろいろ(マルウェア埋め込みなど)操作された上で高額請求される事例も
    - けっこう美味しいのか、2024年頃かはすごく増えている

- (昔ながらのコンピュータウィルス)
  - ワーム: ひたすら他PCに感染して増殖(Denial of Serviceにつながることも)
  - ウイルス: PCに何らかの異常を発生させる(デモ画面を出すなど)

Potentially Unwanted Application (PUA)

明示的な金銭的被害等は生じない(端末のリソースは消費する)が、利用者に益することなはないソフトウェア

- アドウェア
  - 広告を大量に表示(アクセス)させることで(アフィリエイトなどで)収益につなげる
  - ソフトウェアインストール時に付属ソフトウェアとして入る事例も多い
- 必要以上の権限を要求するアプリ
  - 必要以上に要求した権限で個人の行動を窃取してターゲティング広告につなげたりすることで収益をあげたりとか
  - (対策の動きとして、)GoogleのChrome Webストアは「最もアクセスするデータが少ない権限を利用すること」が方針となっている[1]
    - でも、Google自体はFLoCという広告ターゲティングを新たも作ったり…
    - Chrome系(Edge含む)のシェア独占化でプライバシー面対応で少し不安

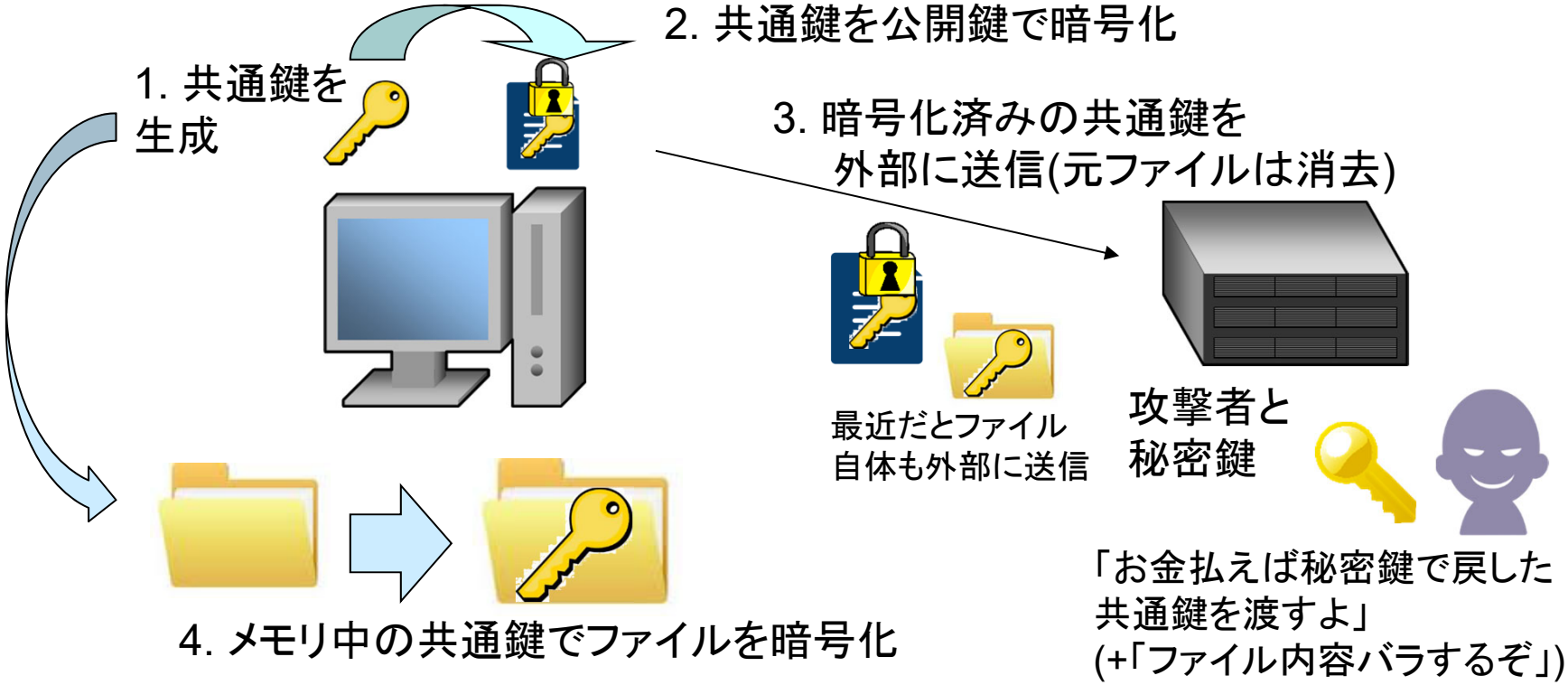
[1] https://it.srad.jp/story/19/06/06/0436222/

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

ランサムウェアの動作

- 共通鍵は暗号化した状態でしかファイルに残らない
  - メモリの上のみに残して実行終了や電源断で消滅
- 稀に復号ツールが出ることがある
  - メモリ上の共通鍵を抽出、悪人が秘密鍵を公開した、など

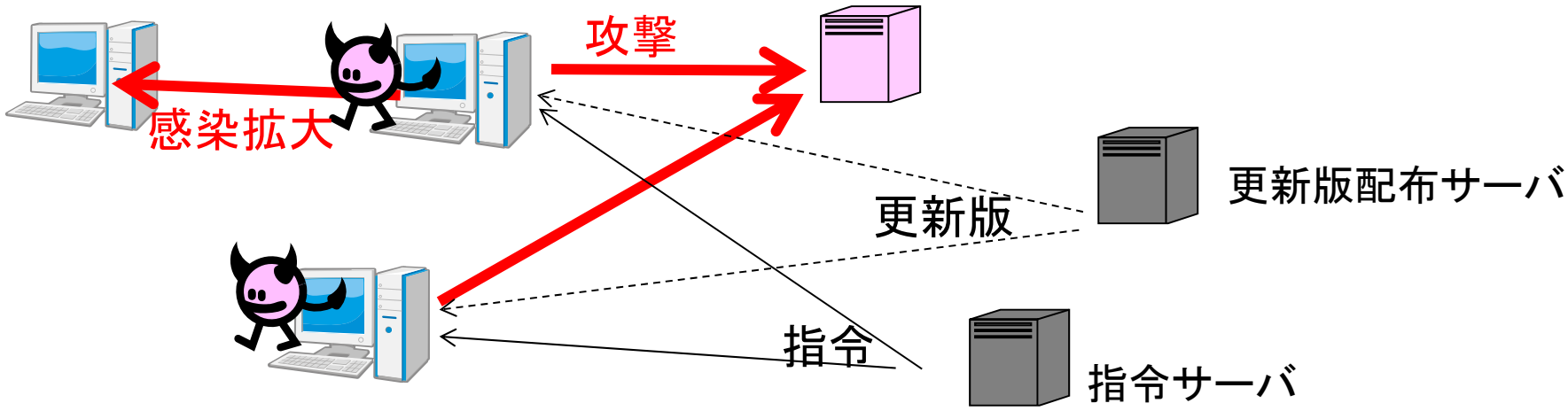


兵器化されるランサムウェア

- 2018年頃からどんどんランサムウェア攻撃が高度化中
  - 効果的に金銭窃取できる攻撃と攻撃者が認識してどんどん改良
  - 脅迫金額も組織を狙った物相当にアップした上で組織を狙ったり
  - 感染後に遠隔オペレータにつないで被害者を効果的にゆさぶったり
- ランサムウェアで狙われる傾向にある組織
  - 病院: 電子カルテその他の医療機器に患者の命がかかっている
  - 行政: 行政の電子システムが止まると社会も止まる
  - 社会インフラ: インフラ制御システムが止まると社会も止まる
- セキュリティアップデートをやりにくい組み込みシステムが感染すると大変
  - 病院の電子カルテ系、工場の産業機械、など
  - ネット接続切っても、更新を適用するためのメンテナンス用PCやアップデートデータを入れたUSBメモリから感染することも多い

RAT(Remote Administration Trojan)

- トロイの木馬、バックドア、ボットネットクライアントの発展
- 指令を受け取って様々動作を取る
  - 侵入した端末の周りの偵察や(指示を受けての)感染拡大
  - 自分自身の更新やおとりマルウェアの導入
  - 外部への攻撃
- 最近は司令通信の隠蔽が進んでいる(TwitterやSlackなどのWebサービス利用の事例も)



RATの代表的な機能

- スクリーンショット、音声、Webカメラの画像の取得
- キー入力操作情報の収集
- 開いているウィンドウの管理
- パスワードの管理
- レジストリ、プロセス、サービス、デバイス、インストールされているアプリケーションの管理
- ファイル検索、同時に多数のファイル移動の実行
- リモートシェルの実行
- サーバの共有化
- 自身の更新、再起動、終了
- (ランサムウェア機能?)

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

マルウェアの送り込みパターン(1/3)

- 昔ながらのメール
  - メールボックス内メールに返信の形で出すEmotetがちらほら活動
  - 本体に添付することは減ってきてWebからのダウンロードが中心に
    - JavaScriptを実行させてダウンロードと実行
    - Windows PowerShellを立ち上げてダウンロードと実行
      - 最近はこれを手動で実行されるClickFixが大きな問題に(リテラシ回参照)
    - Microsoft Officeのマクロを実行させてダウンロードと実行
  - 標的化: ビジネス等でやりとりのある相手を装ってメールで送り込み
- アプリストアに紛れ込ませる
  - 有名アプリと似た名前や似た提供者名でマルウェアをパックした物をアプリストアに設置
  - ニュースで話題になった物に対して、直後に多く発生したりする
    - オンライン会議で話題になったZoom(@2020年)とかChatGPT(@2023年)とか

マルウェアの送り込みパターン(2/3)

- Webからのダウンロード
  - 攻略されたWebサイトから配布orWeb広告にまぎれて配布
    - 特に広告(malvertizing = malware + advertising)は増える傾向にある
      - 偽マルウェア警告からダウンロードさせたり、ClickFixにつなげたり
    - プラグインの脆弱性利用も多い(例: Java)
  - 偽Webサイトに誘導して(本来のWebサイトのアプリを装って)配布
    - 家庭用ブロードバンドルータの脆弱性を突かれて設定された事例も
  - 標的化: 水飲み場型攻撃
    - 特定のユーザがよく見るWebサイトにマルウェアをしかける
- 端末に接続したデバイス経由
  - USBメモリにマルウェアを入れてAutorunさせるのは古典的な方法
  - 接続機器用のドライバやファームウェアを狙う物もある
  - 接続ケーブル内に収まるチップ経由で攻撃も起こりうる[1]

[1] https://jp.techcrunch.com/2019/08/13/2019-08-12-iphone-charging-cable-hack-computer-def-con/

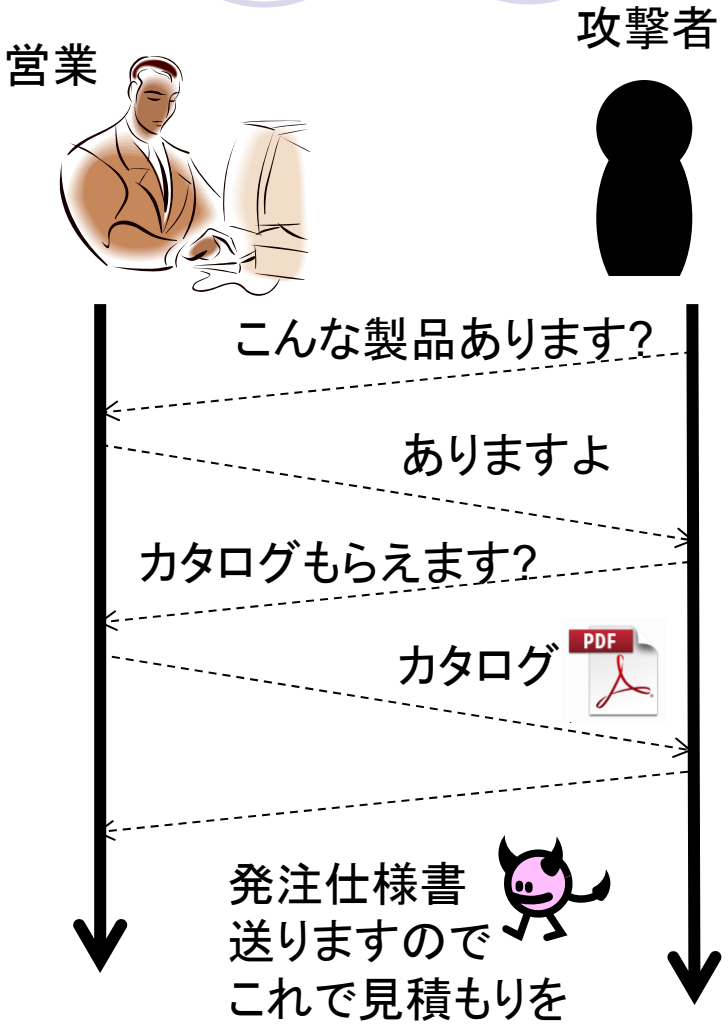
マルウェアの送り込みパターン(3/3)

- アプリやWebブラウザ拡張やアプリ用プラグインの悪性化
  - 最近、特に増えてきている印象
  - 昔はマイナー物がやられることが多かったが利用者が多い物も[1]
  - アプリ開発者へ高額での買い取りや情報収集機能追加依頼は昔から続いている[2]
- (AIを利用した悪性スクリプトの現地生成?)
  - (まだ特に明確に被害が出ているではないが、これから起きるかも?)
  - 後で述べるいわゆる生成系AIの有害情報出力回避を利用して、悪性スクリプトを生成して実行させる物は容易に作れそう
    - ClickFixさせたりAIエージェントに直接実行させたり

[1] https://gigazine.net/news/20251204-browser-extension-malware/
[2] https://gigazine.net/news/20230810-open-source-takeover-offer/

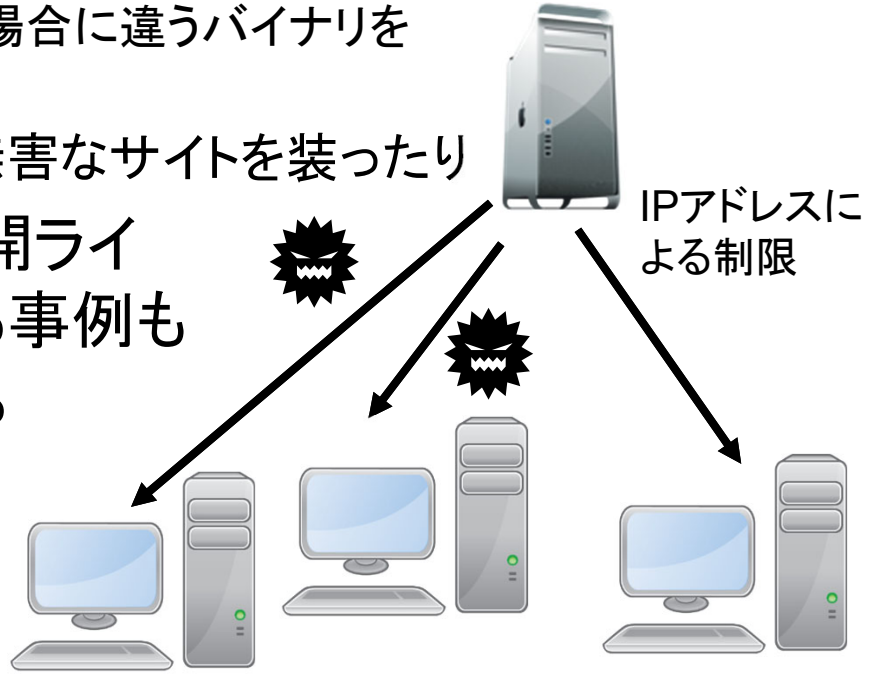
マルウェア送り込みのテクニック: やりとり攻撃

- 複数回のメールのやりとりの後にマルウェア送付
- 例: 営業部へのやりとり攻撃
  - 営業の業務フローを利用して送り込む
  - 営業部から開発部などの機密情報を持ちそうな所へ浸潤
- 最近だと、無差別型でも領収書とか営業が反応しそうなキーワードが含まれたメールが多い
  - 営業は狙いやすいと思われている?
- サプライチェーン(子会社、委託先)経由の攻撃の脅威は続いている



マルウェア送り込みのテクニック: 水飲み場型攻撃

- 「ある仕事をしている人が頻繁に見るページにマルウェアを仕掛ける」ことによる特定業種の業社への標的型攻撃
- 例: あるソフトウェアの更新ページへの細工
  - 攻撃者がソフトウェア更新ページを乗っ取って悪用
    - 特定IPアドレスから更新が来た場合に違うバイナリを送る攻撃がしかけられていた
  - 逆にセキュリティ関係会社には無害なサイトを装ったり
- 管理が疎かなフリーウェア/公開ライブラリ/ブラウザ拡張を乗っ取る事例も
  - 昨年にはかなり広く使われている圧縮ライブラリxzにバックドアを仕掛けられた事件が(2024/3)[1]
    - かなり精巧にバックドアコードが隠蔽されていて大ニュースに



[1] https://forest.watch.impress.co.jp/docs/news/1580604.html

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

マルウェアの検知

大きく分けて2つの方法があり、組み合わせて使われる

- シグネチャ検知
  - 特徴的なコードや動作を目印として検知
  - 誤検知は少ないが、未知攻撃の検知はまず無い
- ふるまい検知
  - 例: 怪しい動作やコードパターンをいくつか定義し、その観測数がしきい値を越えたら検知
    - いろいろやり方があり、それらをさらに複合させることも多い
  - 未知攻撃を検知できる可能性はあるが、誤検知も起こす
  - 最近では、検知方法の生成に機械学習や深層学習の応用が多い
  - サンドボックスと呼ばれる隔離環境を一時的に作って実施する物も
    - RAT系を検知するために組織内におとり端末を設置する物も

マルウェア識別名の名付け

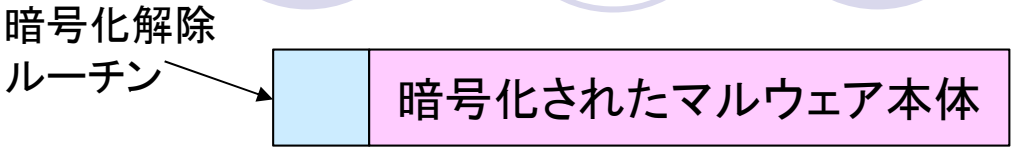
- マルウェアの特徴をもとに(マルウェアファミリに)識別
  - 基本的にすぐに亜種が出てくるので、マルウェアファミリとして識別
  - 特徴の例: バイナリ全体のハッシュ値、部分コード列との一致、埋め込みデータとの一致
- アンチウィルスソフトウェアごとに名付けが違ったファミリ分けも違ったり
  - 例1
    - Kaspersky: Trojan-Ransom.Win32.Agent
    - AVG: Trojan.Generic35
  - 例2
    - AVGは、Trojan.Win32.Agent、Trojan.CoinMiner.AKQ、Trojan.Dropper.Generic_r.AFの3種類に分類
    - Kasperskyは全部Trojan.Inject2.MDEに分類

VirusTotalによるマルウェアの識別

- 様々なアンチウィルスの検知結果を見ることができる
- 送ったファイルは検体として提供したことになる点に注意
  - Webサービス系の物はこういう規約は多い(著作権譲渡規約な物も)
- URL(Webサーバ)に対しても評価してくれる
  - というか、ちょこちょこ巡回しているらしい

https://www.virustotal.com/

マルウェアの隠蔽



- パッキング
  - 本体を暗号化した上で暗号化解除ルーチンを付与
  - 暗号化方法や暗号化解除ルーチンを変えて簡易な検知を回避
- 本体のダウンロード化
  - 最初に送り込むのは簡易なドロッパにして検知を回避
  - 単純にダウンロードさせるだけでなく、複数のサーバを経由させてみたり(Drive-by-Download)
  - 画像データなどの無害なデータに本体を埋め込んだり
- 難読化
  - わざと無駄な処理を入れたり、コードを超分割したり
  - マクロやスクリプト型のマルウェアで多用される
- ダミーマルウェアの同時送り込み

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

公開サーバのサーバ側への攻撃

- 認証の不備を狙うものは多い
  - 正規の遠隔操作(SSH, リモートデスクトップ, など)への認証ブルートフォース攻撃
  - Web認証ページへの認証ブルートフォース攻撃
  - 認証設定のうっかりミス系を狙うものもある
    - うっかりデフォルト設定(初期設定)のID/パスワードやテスト用ID/パスワードが動いていた
      - そもそも、不要なサービスを動かしていた
    - 設定変更時に間違った設定をした上、気づかずそのまま運用

  →認証の話とかぶる所も多い
- 大量データの送信により公開サーバを麻痺(DoS)
- Webサーバに対してのインジェクション系攻撃

公開サーバへのアクセス時にクライアント側で成立させる攻撃

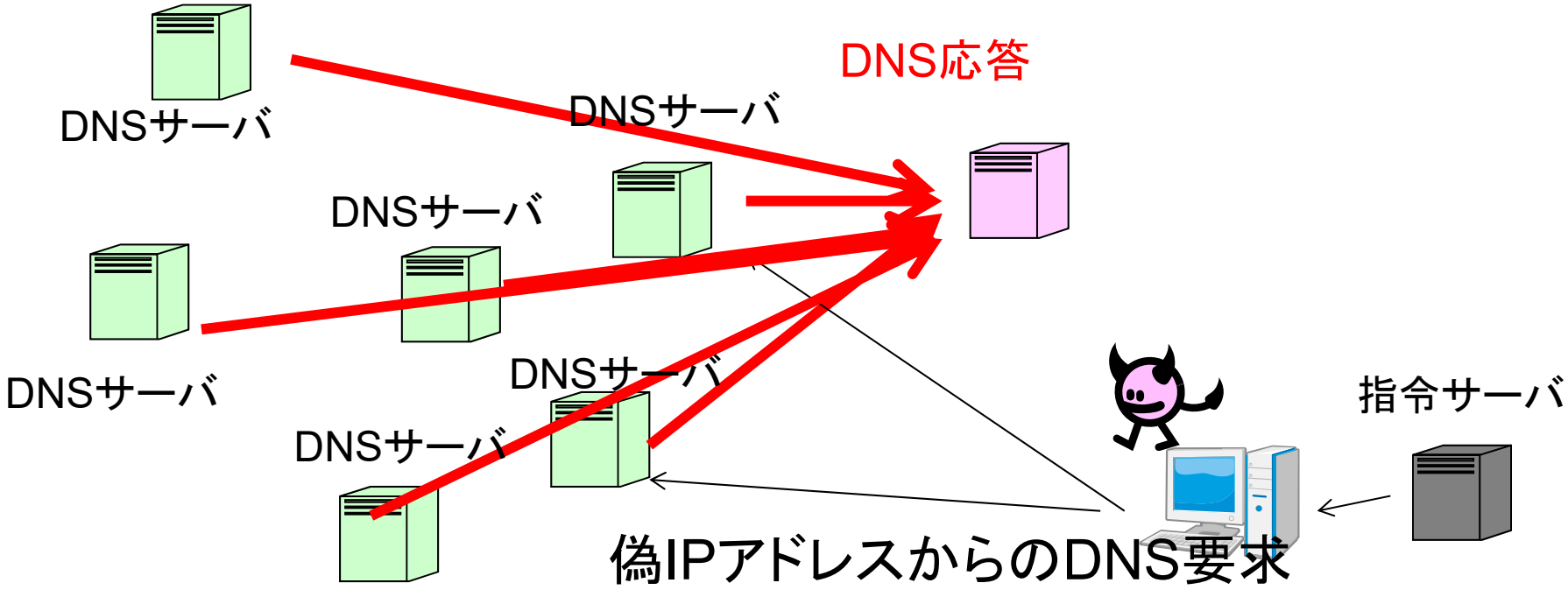
- ネットワークレベルでの偽サーバへの誘導
  - DNS、BGP、偽無線LANアクセスポイント
    (ネットワークサービスの回の講義資料にも一部説明あり)
  - 人の目視を騙して別URLへの誘導
- クロスサイトスクリプティングによるブラウザ上で悪意のあるJavaScriptの実行
  - 認証状態やセッション管理のCookie窃取
  - 偽パスワード入力画面のポップアップ
  - クロスサイトリクエスト強要によるWebサービスの設定変更

サービス不能攻撃(DoS攻撃)

- Denial of Service攻撃
  - 攻撃元を分散させるとDDoS(Distributed DoS)攻撃
- 様々なネットワーク階層で実行可能
  - SYN Flood(L4)
  - UDP Flood(L4)
    - 最近のニュースでのDoS攻撃は主にこれ
  - HTTP GET flood(L5)
    - 要はWebページの再読込を多数送る
  - Slow HTTP DoS(L7)
    - わざとゆっくり処理を依頼することでWebサーバのセッション数を使い切る
- 基本的に、どこかで依頼を無視したり叩き落としたりするのが対策だが、正規利用者への影響も…

UDP Flood(1/2)

- 大抵は、以下に説明するリフレクション攻撃を併用
- いくつかのUDPプロトコルにおいて問い合わせ要求に対して応答の方がサイズが大きいことを利用
  - 要求に対して応答のサイズは数倍～数百倍(DNS/NTP悪用が有名)
  - 応答の方は多くのデータがあるので、データサイズは「応答>要求」



UDP Flood(2/2)

- 防衛の面では、UDPは送信/受信ともに同じポートを使うのがやっかい
  - 「リフレクション攻撃で送りつけられてきた応答」なのか「中から外に出した要求に対する応答」なのか分かりにくい
  - 例: NTPリクエストはNTPサーバのUDP 123ポートへ送信、応答はクライアントのUDP 123ポートへ返信
  - 対応1: 外から要求が来ることが考えられないプロトコルは落とす
  - 対応2: ステートフルファイアウォールを導入して、中から要求が出て行っていないはずの応答は落とす
- 最近だと1Tbps超UDP Floodで物理回線で埋まる攻撃も
  - 対応: インターネット上の途中のサブネットでブラックホールルーティングしてもらう
- 攻撃参加しないようにするのも大事
  - 要求に応答する範囲を制限する

認証へのブルートフォース攻撃(1/2)

- brute force: 力づくの、強引な
- 適当なID/パスワードをひたすら送って認証を突破しようとする力づくな方法
- 主な対象: Web(認証ページ), リモートデスクトップ, SSH
- 対策
  - パスワードの強度確保、他との共有の禁止
  - 接続元IPアドレスの制限
  - 単位時間あたりの認証回数の制限
  - 認証失敗回数に応じた短期の無効化(IPアドレス、ID)
    - IDを長期間無効化してしまうやり方は、正規の利用者への嫌がらせ(サービス妨害)ができてしまうので悪手

認証へのブルートフォース攻撃(2/2)

- 最近だと攻撃側も認証回数制限を考慮して攻撃してくる
  - 複数のIPアドレスから分散して攻撃
    - 例: A国のIPアドレスから認証試行n回、その後、B国のIPアドレスから認証試行n回、その後…
  - パスワードスプレー攻撃(認証の回の講義資料)で「1つのIDあたりの制限」を緩和
    - NATでサーバから見えるグローバルIPアドレスが同じになる場合への対応のため、IPアドレスあたりの認証回数制限は緩くせざるを得ない
      - NUWNET出口のIPアドレスなど、組織のネットワークの出口が同じグローバルIPアドレスになる事例は多い

偽サーバへの誘導(1/2)

- DNSに偽の名前解決を入れて偽サーバに接続させる
  - 偽DNSサーバを指定させたり、DNSサーバが上流DNSサーバに問い合わせた時に偽の応答を返したり
  - 対策としてDNSSECは提案されているが普及が微妙
  - HTTPSでDNSを実行して、ブラウザ内部で安全なDNSに接続させるDNS over HTTPの実装が急速に進んでいる(Firefox, Chromeなど)
    - 「この名前解決を行った」というプライバシーの範疇の情報を集中して集めることができるので、プライバシーとの兼ね合いが悩ましい
- 偽無線LANアクセスポイントを準備して誘導
- BGP(Border Gateway Protocol)への偽経路注入
  - 各サブネットを運営する組織はAutonomous System(AS)番号を与えられる
    - AS番号をネットに放流すると、経由ASの番号を追加しつつ流れる
    - 受け取った側からするとASの番号を列挙したものが経路となる

偽サーバへの誘導(2/2)

- HTMLでリンク先と表示文字を替える
  - http://www.example.jp/" と書いて、「http://www.example.jp/」に飛ぶと見せかける
- 偽URLの利用
  - 正規ドメインに似た文字をどこかのサブドメインとして設定(例: www.nagoya-u.ac.jp.example.com)
  - 多言語環境を利用して、英字アルファベットに似た文字を悪用
    - PunycodeでURLのFQDN部のエンコーディングができる
    - 例: ギリシア文字を使ってwww.nagoya-μ.ac.jp(μ: ミュー)
  - 参考: メールの宛先のタイプミスを狙ったドメインで重要メールを待ち構える事例も(例: gmali.com)
    - ドッペルゲンガードメインと呼ばれることも

クロスサイトスクリプティング(1/3)

- 主にユーザのブラウザ側で動くJavaScript言語で悪意のあるプログラムを実行するのに用いられる
  - あるWebサイト上で、そのWebサイト製作者が意図してないスクリプト(プログラム)が実行できる
  - 検証時は「<script>alart(1);</script>」という形で警告ポップアップウィンドウを作るJavaScriptを動かすのが一般的
- 実行されたJavaScriptでできること
  - 外部へデータ送信(セッションや認証状態をCookieとか)
  - 正規の入力欄におおいかぶさる形での偽入力欄作成 →情報窃取
- 略称はXSS
  - 英語ではCrossをX(棒がクロスしている文字)で略することはよくある
  - Web関係でCSSだとCascading Style Sheetが先にあったので

クロスサイトスクリプティング(2/3)

- よくあるパターン: フォーム等への入力結果が表示されるWebサイトで、特定の入力をするとXSS成立
  - 会員登録などで「個人情報入力」→「確認用入力結果表示」とか
- 基本的に、「入力の一部でタグを途中で終了させ、その後にスクリプトを挿入」の形 (HTMLの構文については4/26講義資料)
  - 例: http://..../hoge.cgi?initdata=hogeと入力すると<input initdata="hoge">となるHTMLを動的生成におけるJavaScript挿入
  - 入力例: http://..../hoge.cgi?initdata="><script>alart(1);</script>"<input initdata="
  - 出力例: <input initdata=""><script>alart(1);</script>"<input initdata="">
- 対策: 入力データをエスケープで無害化
  - < → < > →> " → " ' → $#39; & → &

クロスサイトスクリプティング(3/3)

- 大多数の物は、外部サイトに設置した(ある程度規模の大きい)JavaScriptを読み込んで実行する
- クロスサイトスクリプティングフィルタもあることはあるが…
  - 明らかな有害なスクリプトをブロックするが、誤検出することもある
  - FirefoxではNoScript Security Suiteアドオンとか
- クロスサイトスクリプティング系の応用はけっこう多い
  - 例: Cross Site Request Forgery、SQLインジェクション、強制ブラウズ、書式文字列攻撃、リモートファイルインクルード、LDAPインジェクション、セッション固定攻撃、オープンリダイレクタ、ディレクトリトラバーサル、OSコマンドインジェクション、Xpathインジェクション、メモリ初期化ミスを利用したメモリリーク、HTTPヘッダインジェクション
  - 基本的に、「本来は実行対象として解釈されないはずのものが、実装ミスなどによって解釈されてしまう」ことに起因する

Cross Site Request Forgery(CSRF: クロスサイトリクエスト強要)

- XSSと似たようなものだが、「外部のWebサイトにリクエストを送る」という点がポイント
  - リクエストの例: Web掲示板の書き込み、Webサービスの設定変更、など
- 書き込みページなどを介さずにHTTP POSTやURLクエリでリクエストを受け付けるWebページ設計だと起こる
- パソコン遠隔操作事件で、被害者PCからWeb掲示板に犯行予告書き込みを強制させることにも使われた[1, 2]
- 対策: ちゃんとセッション管理して書き込みページや設定変更ページを経由しないリクエストは受け付けないようにする

[1] https://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6
[2] https://piyolog.hatenadiary.jp/entry/20121008/1349660951

ディレクトリトラバーサルによるファイル読み出し

- 本来は見れない範囲にあるデータを見られてしまう
- 多くのシステムでは".."は1つ上のディレクトリに移動を示す
  →入力にあったとしても処理しないようにシステムを組む
- が、何らかのミスで入力を処理してしまう脆弱性がありうる
  - 単純な設計ミス
  - 別の脆弱性から想定外のコードを実行される
- 本来は見れないパスワードやデータの閲覧が可能に
  - /var/www/htmlが外部公開の最上位のはずが、それより上のディレクトリも読まれる
  - 使っているソフトウェアが汎用の物ならば、パスワードを保存したファイルの位置はだいたい想像できる
- 対策: 正しく".."の無害化(除去)処理を入れる

OSコマンドインジェクション

- Webサーバ側でURLクエリを処理するアプリケーションの設計ミスなどでWebサーバ側でOSのコマンドを実行
  - WindowsサーバでもPowerShell経由で実行
- アプリケーション実装の中でOSコマンドを呼び出している所にインジェクションする事例が多い
  - 正規の処理の後に悪意のある動作を追加、など
- マルウェアをダウンロードして実行するコマンドのインジェクションが多い
  - テンポラリファイル置き場(どのプログラムも書き込み権限がある場所)にダウンロードして実行させる
- 対策:
  - XSSと同じくエスケープによる無害化
  - OSコマンド呼び出しを行わない実装を考える

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

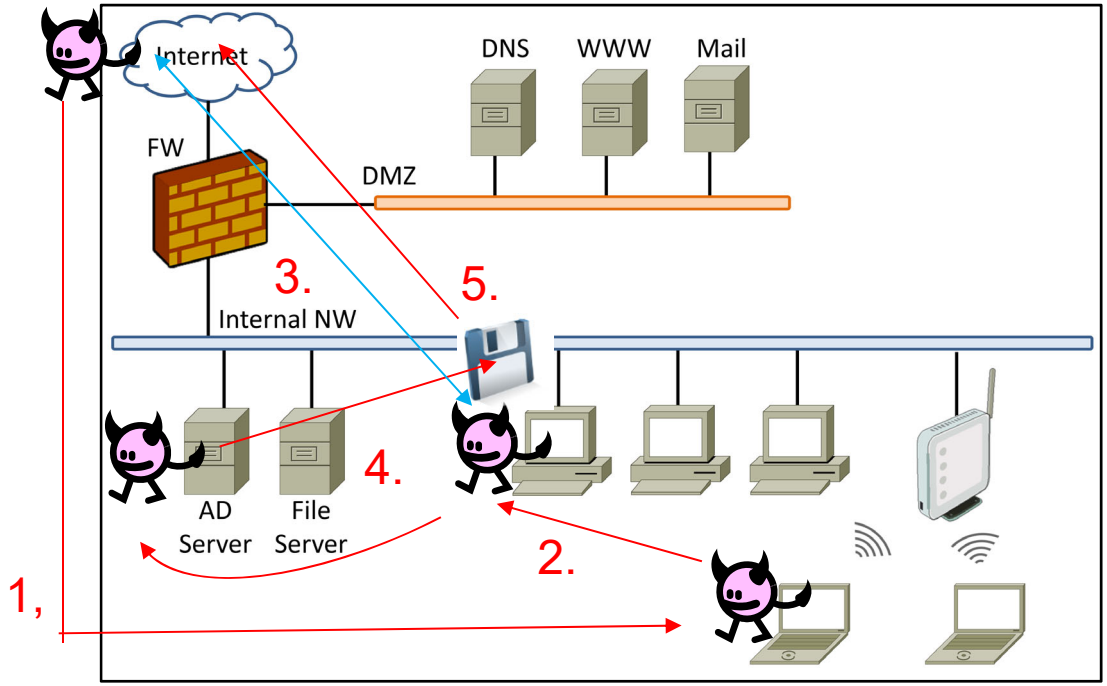
その他のサイバー攻撃など

- 標的型攻撃(目的達成までしつこく行われる攻撃)
- USB接続を利用した攻撃
  - 一般的なマルウェアの送り込み
  - OSを介さないファームウェアレベルの攻撃
  - 電気的な破壊
- サイドチャネル攻撃
- 機械学習/深層学習応用システムへの攻撃

一般的な標的型攻撃とその進行

- 英語ではAdvanced Persistent Threat(高度で執拗な脅威)
  - 失敗しても何度も攻撃を試みる
  - 複雑な組織内部の計算機システムに対しても浸潤するように攻撃
- 代表的な標的型攻撃の進行
  - 長いものだと攻撃に数ヶ月かけることもある

1. 組織内部潜入
2. 内部での拡散
3. 外部との通信基盤構築
4. 機密情報窃取
5. 情報送出



標的型攻撃の代表例(1/2)

三菱重工への標的型攻撃[1]

- 企業に対して大規模な標的型攻撃のリスクについて認識させた事例
- 2011/8にサーバが再起動を繰り返す原因追求中に発覚
  - 感染台数: サーバ 45台、従業員用PC 38台
  - 8種類のマルウェアを11の事業所から発見
- 発端:「原発のリスク整理」と名付けられた添付ファイルに見せかけたマルウェア
  - Adobe Flashの脆弱性を利用するマルウェア
  - 東日本大震災(2011/3)の直後かつ送信元は内閣府実在の人物の名前、メールアドレスを騙る

  →三菱重工は原発を作っている(いた)ので、受け取った人は疑いにくい

[1] https://piyolog.hatenadiary.jp/entry/20110919/1316393705

標的型攻撃の代表例(2/2)

日本年金機構への標的型攻撃[1, 2]

- 大々的にニュースになって、一般的な人にも標的型攻撃について知らしめた事例
- 2015/5/23にシステム管理会社が不審な通信を報告して発覚
- 発端: マルウェア送り込みURL付きメールのURLクリック
  - 2015/5/8に最初の1名、数日おいて他にもう1名が
  - RAT型マルウェア(Emdivi)を送り込まれ、内部感染拡大が進行
    - 当時にアンチウイルスソフトウェアの検知をすり抜けた
  - 最終的に31台のPCに感染
    - 感染PC経由で共有ファイルサーバから情報窃取された

[1] https://www.mhlw.go.jp/stf/shingi2/0000095311.html
[2] https://piyolog.hatenadiary.jp/entry/20150601/1433166675

個人的に勉強になると思う標的型攻撃(高度で執拗な脅威)の報告書

- 産総研の情報システムに対する攻撃[1]
  - 研究所だけあって、50ページにも渡る詳細な報告書
    - よくぞここまで細かく公表してくれましたと感謝しかない
  - 弱いパスワードを設定したIDを外部公開システムで確認される
  - 内部システムにつながるサーバの攻略後、上記のIDを悪用される
- 海外拠点経由で侵入された三菱電機の事例[2, 3]
  - アンチウイルスソフトウェアのアップデート配信サーバの脆弱性を突いてマルウェア配布で感染拡大
    - アップデートハイジャックの亜種
  - PowerShellで組んだファイルレス型マルウェアを利用

[1] https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf
[2] https://piyolog.hatenadiary.jp/entry/2020/01/20/172436
[3] https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

標的型攻撃とランサムウェア

- 最近では、標的型攻撃にランサムウェアを複合してくるのが当たり前となってきている
- 理由(嶋田の個人的な主観)
  - 純粋な情報の窃取を目的とした標的型攻撃よりも、攻撃対象になる組織(お金につなげることができる攻撃対象)が大幅に増える
  - データの暗号化と窃取したデータの公開を合わせることで、身代金の支払いの確率があがることで、悪い人が味をしめた
    - ランサムウェアの項目でも説明したように、機微な個人情報を扱う所
    - 大手ランサムウェアactorは(Dark Webに)公開専用Webページを設置していたりする
- 標的型攻撃と同様に浸潤してからデータ暗号化などを行う
  - バックアップデータまでやられる事例が多い
    - オフラインのバックアップデータからの回復時も、ちゃんとランサムウェアが除去できてから実施するよう注意が必要

USBを利用した(物理的な)(セキュリティ)攻撃(1/2)

USBは色々とplug and playができて便利だが、本当にそのUSBデバイスつなげて大丈夫?

- そのUSBメモリの中にマルウェア入っていない?
  - (偽)ギフトにマルウェア入りUSBメモリが含まれていた事例[1]
- そのUSB接続で充電するデバイスは大丈夫?
  - USBで充電する電子タバコにマルウェアを送り込むファームウェアが入っていた事例[2]
- 正体不明のUSBメモリが置いてあったので、持ち主を探そうとして中身を見るためにPCに接続して大丈夫?
  - 放置USBメモリの半数以上がPCに接続されたという社会実験[3]

[1] https://piyolog.hatenadiary.jp/entry/2020/03/30/052613
[2] https://the01.jp/p0005410/
[3] https://internet.watch.impress.co.jp/docs/column/security/755865.html

USBを利用した(物理的な)(セキュリティ)攻撃(2/2)

- もっと怖いUSB経由攻撃デバイス
  - Killer USB: 内部にコンデンサと昇圧回路を持ち、過電圧によりPCを破壊
  - Bad USB: USBの認証用ファームウェアレベルで攻撃をしかける(OSまで処理が行く前に攻撃)
- USBと同じく汎用インタフェースのThunderboltにも脆弱性はあったりする[1]

- USB接続や充電が一般化したが、「そこに存在するUSBの口につないで大丈夫?」という意識は常に持った方が良い
  - 個人的に、最近増えている公共のUSB充電口はまず使わない
    - どうしても使うなら、一旦、モバイルバッテリに充電した上で使う

[1] https://pc.watch.impress.co.jp/docs/news/1251766.html

サイドチャネル攻撃

- チップに焼き込まれた暗号鍵などはすぐに変更できないので盗めると特に嬉しい

  →手間暇をかけた攻撃でも攻撃者にはメリットあり
- 暗号処理等によって他の部分に出る影響を調査して暗号鍵等を推測する手間暇かけた攻撃がよく行われる
  - 基本的に、非常に多くの試行と結果の統計処理が必要
  - 完全な暗号鍵を推測できなくても、鍵空間を狭めることができれば…
  - 例: 応答時間解析、電磁波解析、電力差分解析

応答時間解析

- 暗号鍵の数値によって演算時間が変わることがある
  - 例: 乗算において、0の桁があればその桁の処理は飛ばせる
- これを暗号鍵の推測に用いる
  - 計算が早ければ0の桁の多い暗号鍵では?
  - 比較用に作成したの暗号鍵の演算時間と比較
- 対策: 演算が簡単になる暗号鍵でも同じ演算時間になるように回路/プログラムを構成
  - 例: 0の桁があってもちゃんとその桁の加算処理を行う

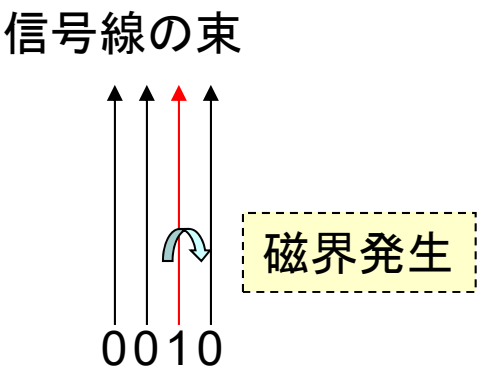
2進数乗算の桁処理飛ばし

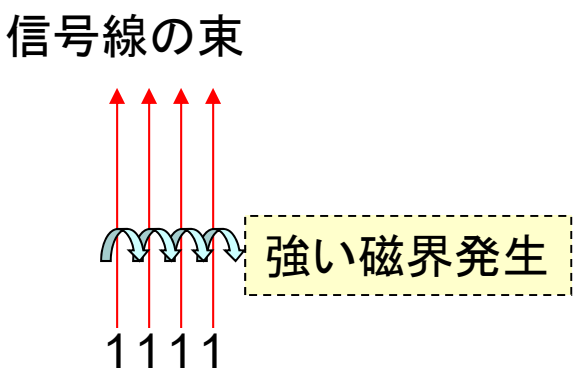
```
   0110          0110
 x 0101        x 0111
 ------        ------
   0110          0110
 0110          0110
 ------        ------
 011110        101010
```

電磁波解析

- チップ上で演算処理を行うと電磁波が発生します
  - 電流が流れると電界/磁界が発生します
- チップ上の複数の配線上に”0000”なデータと”1111”なデータが流れると差は出るか?

  →電界/磁界が合成され、電磁波の強度の差として出る
  - これを統計的に解析
- 対策: 0/1を反転させた(負論理)のデータを同時に流す、など





その他のサイドチャネル系の攻撃(1/2)

プロセッサ(CPU)の投機実行を利用した攻撃

- 投機実行: 近年のプロセッサで多用される「前の処理結果が出る前に次の処理を始める」高速化手法
  - 「前の処理結果で次の処理が変化」した場合、進めていた次の処理を破棄

  →「進めていた次の処理」の破棄がうまくいっていないことが

…

  - 特に「先行して読み込んでおいたデータ」まわり
- 2018/1に発表されたSpectreが有名
  - その後、MeltdownとかSpectre V2, V3, V4とかZombieLoad(2019/5)とかいろいろ見つけられて現在ホットな分野

その他のサイドチャネル系の攻撃(2/2)

物理手段で入力されたパスワードを推測

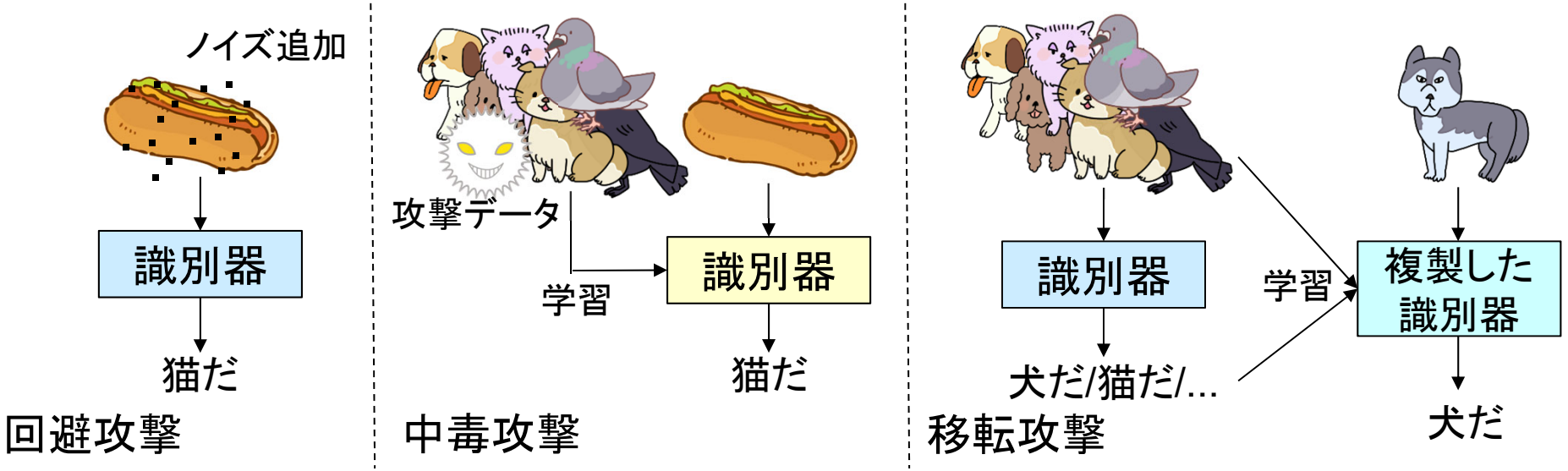
- (肩越しに)パスワードや暗証番号を入力される所を目視
  - ATMにバックミラーがついたりして一般人にも広く認識されているはず
- タッチパネルを触った後を赤外線カメラで記録
- キーボードの打鍵音から推測
  - 音は遠隔からでも取りやすい(音で振動する物を計測とか)からやっかい?
- スマホのタッチパネルのタッチ音(物理的な)で推測[1]
  - スマホ筐体内の電子部品の配置から物理的なタッチ音が微妙に変化
  - 同じスマホのタッチ音をConvolutional Neural Networkで学習して判別

[1] https://www.shizuoka.ac.jp/news/detail.html?CN=6370

機械学習/深層学習応用システムへの攻撃

機械学習/深層学習応用システム(いわゆるAI)への攻撃も

- 回避攻撃: 入力にノイズを加えて誤判定を起こさせる
- 中毒攻撃: 誤判定を誘発するデータ(攻撃データ)を学習データに紛れ込ませる
- 移転攻撃: 入力に対する出力の統計などをもとに識別器の内部パラメータや学習データの抽出(モデル抽出攻撃とも)



いわゆる生成系AIへの攻撃

- 主にプロンプト(指示文)を加工するプロンプトインジェクション
  - 一連のプロンプトで変な出力を誘発
  - プロンプトに人には理解できないsuffix(モデル内部の勾配情報などから作成)を追加して変な出力を誘発
- 回避攻撃系が良く試みられている
  - 安全制約を回避した有害情報の出力
  - 過去のプロンプトや学習データの出力
- 移転攻撃は識別器よりも容易(モデル蒸留とも呼ばれる)
- AIエージェントとかを組み込んだシステムへの攻撃も
  - 業務システムにAIエージェントが組み込まれてきている時代
    - 文書の文法等のチェックとか、到着したメールの要約とか

いわゆるAIのサイバー攻撃/防御利用

- AIを利用したアプリやWebサービスの脆弱性探査がいろいろできる時代である
  - そういうのに特化したAIモデルも出てきている
- 攻撃側がこれを攻撃に利用したら?
  - AIエージェントを利用して自動で脆弱性探査から攻撃までできる時代
  - 2026/2の防衛省サイバーコンテストをAIで攻略した話[1]
    - CTF(Capture The Flag)形式の大会を1時間以内で攻略
    - 異なるタイプのAIを準備して120並列で実行しFlag提出まで自動化
- 防御側も新たなAIを防御に活用しないといけない時代
  - ふるまい型検知(過去事例は無くても怪しいと判断したなら…)は20年近く前からAI(機械学習)の活用はされてたが、脆弱性探査も重要に
  - FirefoxがClaude Mythosを利用して1月前の前版から271件の脆弱性を修正[2]

[1] https://qiita.com/satoki/items/955302bf2615813bae5a
[2] https://japan.zdnet.com/article/35246770/

概要

- 目的から考えるサイバー攻撃の分類
  - 標的型/無差別型、金銭目的型か否か
- マルウェアを利用した攻撃
  - 様々なマルウェア
  - 特に近年話題となるマルウェア
  - マルウェアの送り込みパターン
  - マルウェアの検知
- 公開サーバ(Webサーバ)に対する攻撃
  - サービス不能(DoS: Denial of Service)攻撃
  - 不正リクエスト送付攻撃
- その他のサイバー攻撃
- サイバー攻撃およびマルウェア感染対策

基本的な事前対策

- OSやアプリケーションはちゃんとアップデートする
- アンチウィルスソフトウェアは利用する(検知パターンはちゃんと更新)
- データの定期的なバックアップ(2個所以上)
  - ランサムウェアにやられた時や怪しい時のクリーンインストールなど
- 怪しいURLへのアクセスやファイルの実行を避ける
  - と言いたい所だが、攻撃者の文面の工夫は日々向上しているので(最近だとAI応用も)、完全に0にすることは難しい
  - それでも、継続的な訓練メールでアクセス/実行の確率の低下は可能
- 重要情報にアクセスできる人/PC/ネットワークの適切な制限
- DoSはクライアント単独で根本的な対策は少ない
  - 最近は帯域を使い切る攻撃が多く、サーバ側で接続制御をしても…
  - 究極的には、上流ネットワークで対策してもらうことになる

基本的な事後対策

- 被害拡大の防止
  - 組織内部および組織外部の双方に対して
- 証拠保全(最近では特に重要度が高まっている)
  - 時間経過や電源断で記録が消える装置からは早期に証拠を保全
  - 電源断処理検知で証拠隠滅がありそうな場合は電源ケーブルを抜く
  - メモリ上のみにしか本体が存在しないファイルレスマルウェアは電源をつけっぱなしにする

  →名大のセキュリティガイドラインも「情報セキュリティ室の指示に従う」
- 証拠をベースとした追跡
  - 盗み出された物の同定
  - 実施された処理の同定
  - 組織内部などの拡散状況の同定
  - 侵入経路の同定(同一の経路を利用した他のPCなどは無いか?)