ネットワークを介したマルウェアの活動

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部門
嶋田 創

概要

- マルウェアの概要
  - マルウェアの種類
  - マルウェアの識別
- ネットワークを介したマルウェアの送り込みとその検知
  - メールベースの送り込み
  - Webベースの送り込み
- ネットワークを介したマルウェアの活動とその検知
- 標的型攻撃とマルウェア

最近のマルウェアの傾向(1/2)

- 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?」と思っているのかもしれない
  - 「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…
- (数日レベルの差で)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することもある
  - 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をダウンロードしてからスキャンすること

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

最近のマルウェアの傾向(2/2)

- パッキングや難読化がされているマルウェアが多い
- 耐解析ルーチンを備えていて、自己消去とか行う
  - VMらしきインタフェースが見えたら停止
  - 動作中プロセスを見てデバッグツール関係を探す
  - その他、解析環境の可能性を探る(タイマーの動きとか)
- 裏でオペレータがきっちり待機している攻撃グループも最近は増えている
  - ランサムウェア被害者をオペレータが効果的に揺さぶったり
  - 攻撃対応に応じて、攻撃対応への嫌がらせをやったり

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
  - 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
  - 他にも悪性活動に便利なツールセット(rootkit)をまとめて導入も
- 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)
  - スパイウェア、バックドア作成、ボットネットクライアントの発展
  - インストールされているアプリの管理(動作停止)とか開いているウィンドウの管理(警告ウィンドウを閉じる)とか検知逃れに使える機能も
- 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、「全データをインターネット上で一般公開されたくなければ」とかの亜種もある
- 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、偽セキュリティソフトを売りつけたりする
  - 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
- 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(ネットワークに対するDoS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
  - アプリなどの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]

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

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

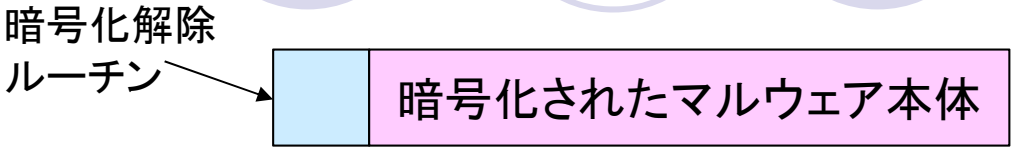
- シグネチャ検知
  - 特徴的なコードや動作を目印として検知
  - 誤検知は少ないが、未知攻撃の検知はまず無い
- ふるまい検知
  - 例: 怪しい動作やコードパターンをいくつか定義し、その観測数がしきい値を越えたら検知
    - いろいろやり方があり、それらをさらに複合させることも多い
  - 未知攻撃を検知できる可能性はあるが、誤検知も起こす
  - 最近では、検知方法の生成に機械学習や深層学習の応用が多い
  - サンドボックスと呼ばれる隔離実行環境を一時的に作ってファイルを実行する物も

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り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

→ニュース等で見た名前と手元の検知が違うことはありうる

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

VirusTotalでマルウェアの識別

- ファイルに対して様々なアンチウィルスの結果を見ることができるサイト
  - マルウェアらしき物をアップロードして結果を見たり
  - 検体はサンプルとして利用されるので、間違って重要ファイルをアップロードしない
- 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
- ハッシュ値、ドメイン、IPアドレスなどからの汎用検索も可能

VirusTotalにマルウェアを上げた例

SHA256: 9b3a7ac1138a8b2f35167a2c1dd9eba4152885ed4142f5cba6ad5cddc80c0bcb

ファイル名: TBUpdate.dll

検出率: 34 / 66

分析日時: 2018-07-24 00:26:10 UTC (2 時間, 15 分前)

分析結果 | ファイルの詳細 | 関連 | 追加情報 | コメント 1 | 投票

ウイルス対策ソフト	結果	更新日
AhnLab-V3	PUP/Win32.Agent.C1730310	20180723
Antiy-AVL	Trojan/Win32.TSGeneric	20180724
Arcabit	PUP.Adware.ClientConnect	20180723
Avast	Win32:Adware-gen [Adw]	20180723
AVG	Win32:Adware-gen [Adw]	20180723
AVware	Conduit (fs)	20180723
Bkav	W32.HfsAdware.A5D5	20180723
CAT-QuickHeal	PUA.Clientconn1.Gen	20180723
ClamAV	Win.Adware.Opencandy-37	20180723
Comodo	ApplicUnwnt	20180723

VirusTotalでIPアドレスを評価した例 (1/3)

virustotal

[redacted] IP アドレス情報

Geolocation

Country	US
Autonomous System	13335 (CloudFlare, Inc.)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2018-07-23	artribune.com
2018-07-23	positivemed.com
2018-07-23	ajtmh.org
2018-07-23	www.ajtmh.org
2018-07-22	www.aminus3.com
2018-07-22	www.divinecosmos.com
2018-07-22	divinecosmos.com
2018-07-22	wordpress.divinecosmos.com
2018-07-22	www.artribune.com
2018-07-21	controradio.it

続き

VirusTotalでIPアドレスを評価した例 (2/3)

⚠ Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

1/66	2017-12-01 01:26:34	http://www.controradio.it/
2/64	2017-09-07 12:11:06	http://sbotogel.com/DL/sboapps.apk
2/65	2017-07-30 07:25:38	http://clouda.chromeinform.com/
1/65	2017-07-28 08:28:49	http://cloud.chromeinform.com/
3/66	2017-07-27 13:22:57	http://cs.chromeinform.com/
2/66	2017-07-22 10:51:54	http://chromeinform.com/
3/65	2017-07-08 03:55:53	http://cs.chromeinform.com/v4/report/ST1000LM014-1EJ164_W772S5VRXXXXW772S5VR?action0=dll.57
3/65	2017-06-21 09:29:40	http://cs.chromeinform.com/v4/report/HitachiXHTS545050A7E380_TMA55DTF0TRN2P0TRN2PX/
3/65	2017-06-19 01:10:24	http://cs.chromeinform.com/v4/report/HitachiXHTS545050A7E380_TMA55DTF0TRN2P0TRN2PX?action=
2/64	2017-05-29 19:39:36	http://cs.chromeinform.com/v4/report/WDCXWD2500BEVT-75ZCT2_WD-WXE908UKJ178KJ178?action0=

続き

Latest detected files that were downloaded from this IP address

Latest files that are **detected by at least one antivirus solution and were downloaded by VirusTotal from the IP address provided**.

7/61	2017-09-07 12:11:13	88819fda9664070cb0f01f3a1a584e8a3a55a89670a228abba30845e33ef2b19

VirusTotalでIPアドレスを評価した例 (3/3)

Latest undetected files that were downloaded from this IP address

Latest files that are **not detected by any antivirus solution and were downloaded by VirusTotal from the IP address provided**.

0/58	2018-05-26 18:00:24	3550474f9a466ace7857064d81db50a25ba7c81de043bc9df8289bd90e32e411
0/60	2018-04-03 20:01:35	224546ee41f8aacc21cb2067284a16ce5fffd04bbf79a5e4fc04c810dfe6ce67
0/57	2018-01-01 11:31:50	35e4356acfafa075498d87f41081210360dcc725691c54d9f03afdf48f6903f0
0/56	2017-12-13 13:22:18	efaea528fbbeb0987dd3ee02c095923fa2d4980c3870d534966a88206eff9212
0/56	2017-12-13 13:22:15	cd4e1ddede59740b607ccf3def3db28fdb638c34dc9171af80dc37d10a9a021b
0/60	2017-10-17 02:00:05	5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9
0/57	2017-08-02 21:47:14	e5cc9085538db5f3564674fbaafb0195fe04f89a11b76950e2af61ed745a39bc
0/56	2017-05-29 19:39:39	4f8ba43c1ee127eb3011f2b5fe3b754ceb566b000b558d252bbb4c87834de9a8
0/54	2017-05-11 10:42:29	8b5cc4df7eec7d32a7814eca4af047ae33b2d52342667715682e19c25b0b9faa
0/56	2017-04-11 13:49:29	c12f6098e641aaca96c60215800f18f5671039aecf812217fab3c0d152f6adb4

続き

Latest undetected files that communicate with this IP address

Latest files submitted to VirusTotal that are **not detected by any antivirus solution and communicate with the IP address provided** when executed in a sandboxed environment.

0/0	2018-03-26 00:45:10	a1fdaeee9a18b1f71dd5c9283656b172aa14fbafc994cbe5413a053c9df2643f

最近では、検体アップロード+解析用VMを備えたサービスも多い

- (VirusTotalサービスの成功を受けて、類似のサービスがいくつも出てきた?)
- 他のサービスでは、検知結果だけでなく、マルウェアの挙動データなども提示する+αがあったりする
- 中には、アップロードした検体を解析用VMで実行可能な
  - 単純に検体を実行できるだけでなく、実行時のプロセスやAPIの呼び出しの時系列を可視化するウィンドウも備えていたりする
  - ユーザ登録で無償枠が与えられるサービスもあるので、手元送りつけられてきた明らかに怪しい物を解析してみるのもあり
- アップロードした検体や解析結果は、サービス利用者の間で共有される
  - 他の人が検体を動作させた結果を見て勉強できる
  - 解析結果に追加したタグで検索もできる

解析用サンドボックスVMサービスの例(1/3)

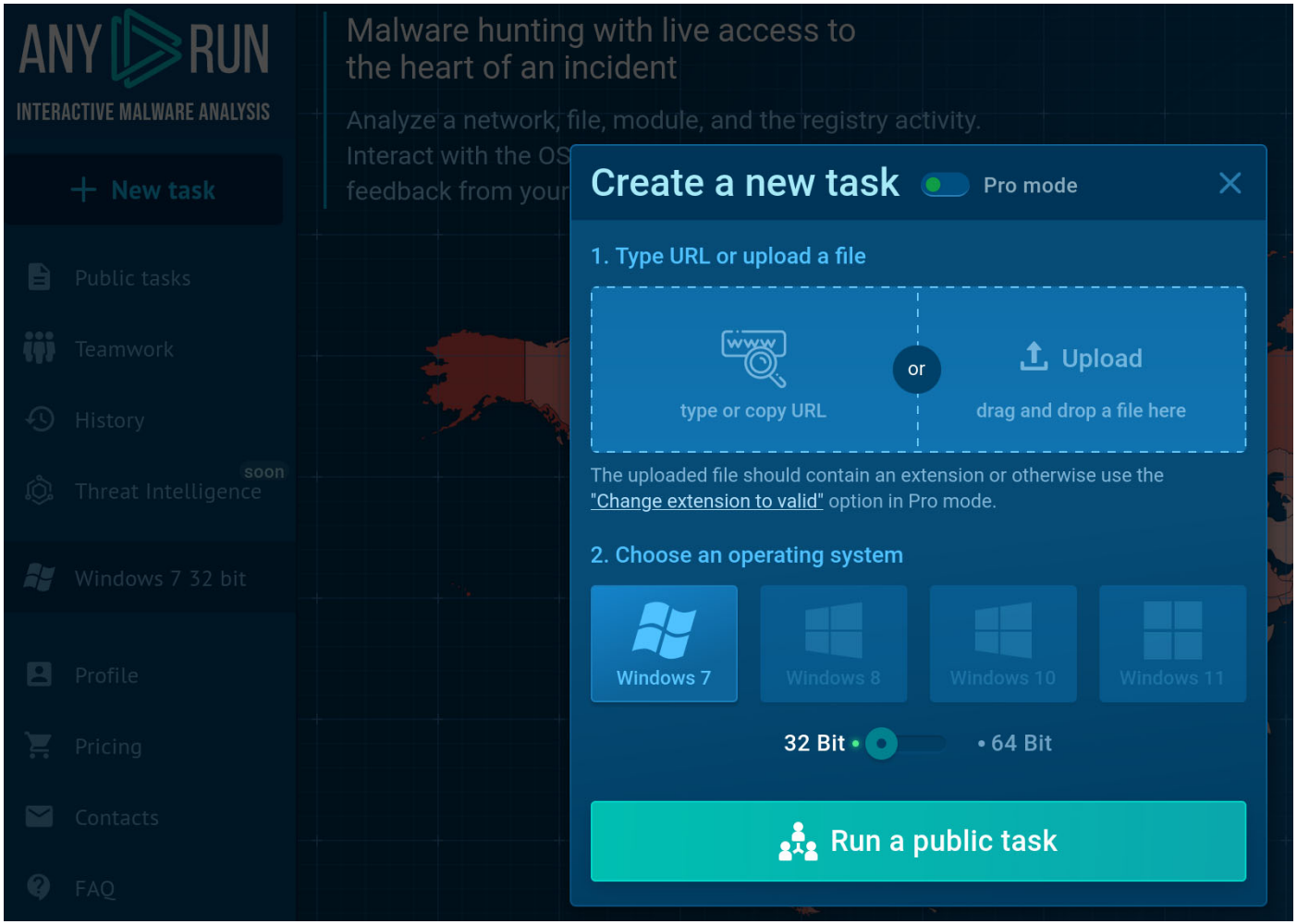
ANY.RUN: https://app.any.run/

- 実行ファイルを10秒間実行し、触った他のファイルや外部への通信の結果を見ることができる
- 有料プランで無い限り、実行結果は共有される
  - 他の利用者が実行した結果も見ることができる
  - 共有されている実行結果にタグ付け(マルウェアの種類、マルウェアファミリ名など)もされている
- 他同種のサービスとしてYOMI by YOROI (https://yomi.yoroi.company/)とか

次スライドからはANY.RUNでの実行の例

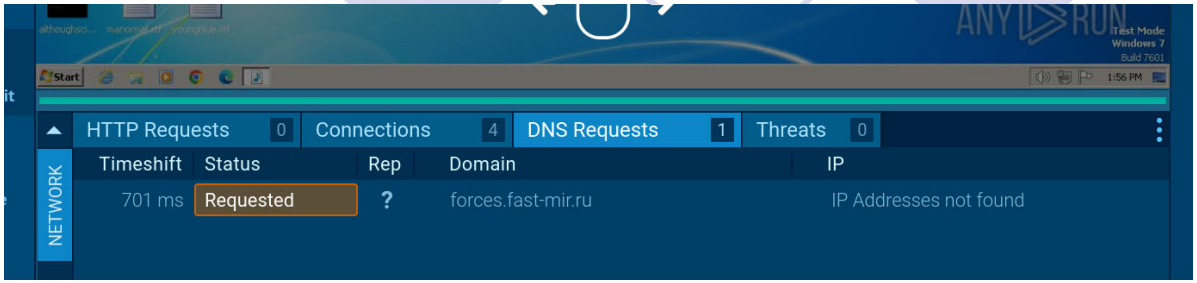
解析用サンドボックスVMサービスの例 (2/3)

- 解析用VMの種類を選択



解析用サンドボックスVMサービスの例 (3/3)

- 実行結果を見る



スパイウェア系(キーロガー系)

以下の物を窃取してネットワークを介して送出

- 認証に関わる入力
  - キー入力
  - 画面のスナップショット
    - ブラウザのどの欄に入力したか確認可能
    - マウスのクリックをトリガとしてスナップショットを取ることで、ソフトウェアキーボードなどのどこをクリックしたかを確認可能
- 独立したソフトウェアでなくブラウザ上で動作するJavaScriptキーロガーもある
- 直接認証情報を取ることも
  - アプリケーションの認証情報保存ファイル
  - 認証済みセッションのHTTP Cookie
  - ハッシュ化されたパスワード

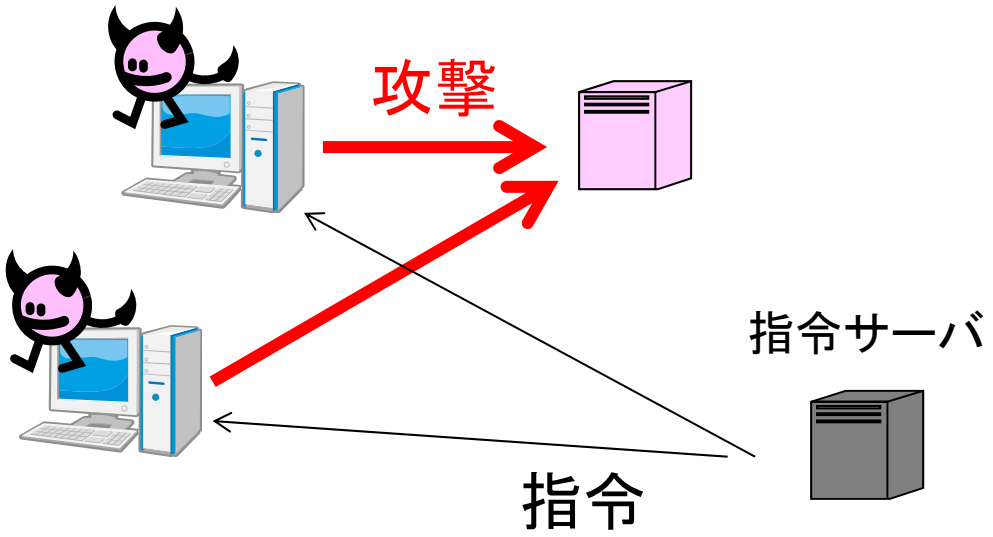
発展したスパイウェア

- 認証情報を取る(ファイルを取る)
  →様々なファイルを窃取するもの
- アンチウィルスソフトウェアの動作の妨害
  →動作中プロセスの制御機能を持つもの
- システム制御機能から発展してネットワーク設定変更など
  - 例: DNS設定を悪意のあるDNSに向ける

- ネットワーク上での検知: 外部への(大量の)送出通信の検知
  - ただし、高度な物だと細切れに送ったり他に紛れて送ったり

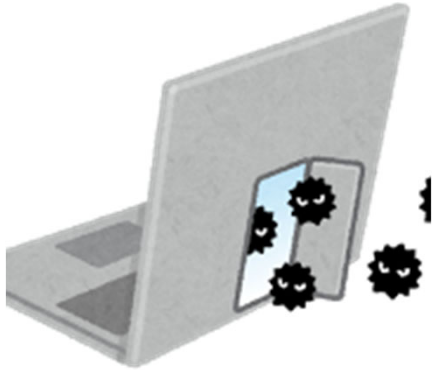
ボットネットクライアント系

- 指令を受け取って攻撃などの動作を取る
- 最近では、PCだけでなく組み込み系やIoT系のネットワークのクライアントも利用される
  - 2016年秋に話題となったMiraiとその亜種など
  - ブロードバンドルータとかはグローバルIPアドレスを持っている組み込み系なのでよく狙われる(アップデートしていますか?)
    - 新しめの製品に危険な脆弱性があってもアップデート提供しない会社も



バックドア系(トロイの木馬系)

- PC等を遠隔操作可能なように裏口を開ける
  - 正規に動いているSSHやRemote Desktop系を利用することも
  - 最近だとWebサイトにしかけるWebシェル(WebページにUNIXシェルのCUI)もよく使われる
- トロイの木馬(Trojan Horse)とも呼ばれる
- PC等をマルウェア配布サイトやボットネットの司令サーバなどにも悪用されることも
  - 悪事のクライアントにされるよりも、やっていることがさらによろしくないので、見つかった後の対応がめんどくさい
- 踏み台にしてさらなる悪さをすることも
  - どこぞから盗んだクレジットカードの悪用とか



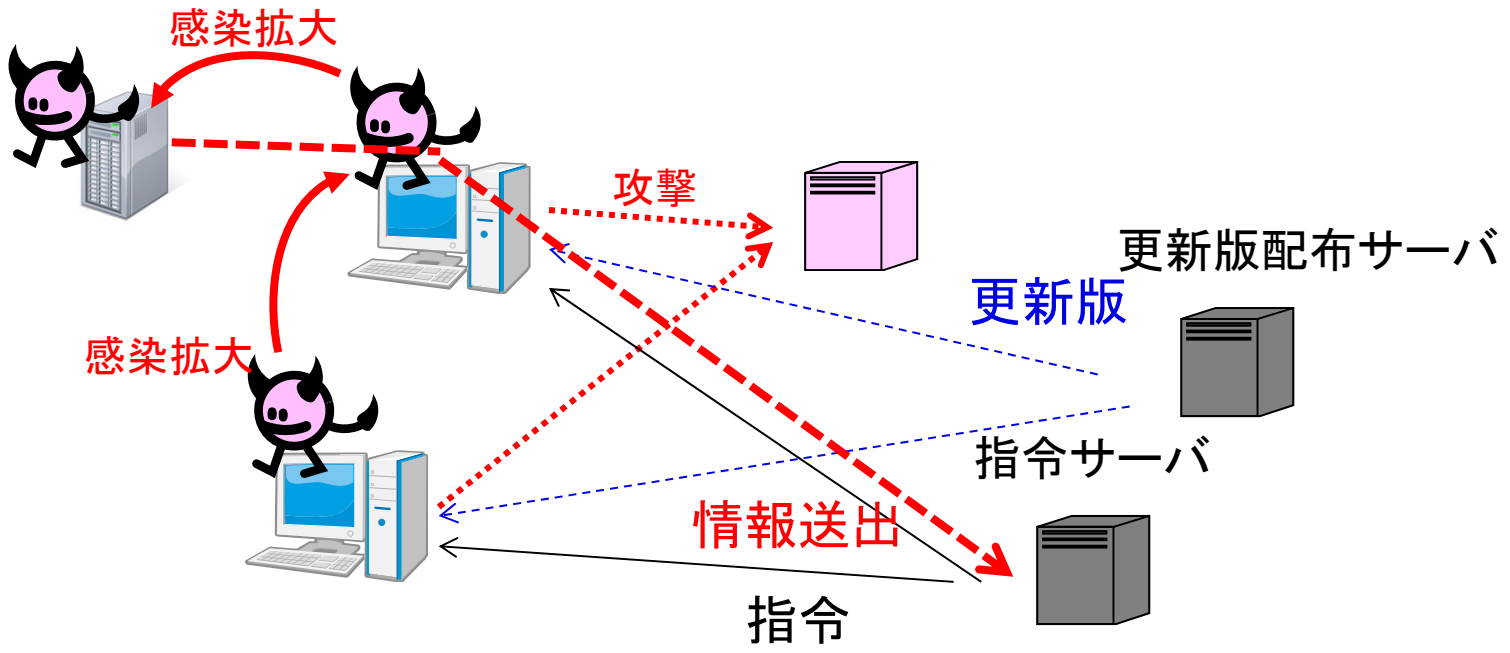
マルウェア設置じゃないバックドア

もともとあるバックドアをマルウェアが活用することもある

- 隠しログインIDをのあるファームウェア
  - IoT系のデバイスでしばしば見つかって問題になる
  - バグ(開発用の消し忘れ)であったり意図的な物っぽかったり…
- システム構築時に作成した一時アカウント
  - グローバルIPアドレスを割り当てていない構築中状態だということで、よくあるIDとパスワードを付与したのを公開時に消し忘れる
  - 自分で作らなくても、構築を依頼した業者が作って消し忘れたいたり…
- (今はほぼ無いが…)OSのデフォルト設定で起動するサービスの存在を知らなくてそのデフォルトアカウントが…
- (放置された脆弱性もバックドアと言えなくもない)

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統合版
- 指令を受け取って感染拡大、情報窃取、自身の更新/消去、(攻撃)などの動作を取る
  - 個人的には、高機能なRATを単純な外部攻撃に使う事例は少な目だと思う



代表的なRATの機能

- スクリーンショット、音声、Webカメラの画像の取得
- アクティブなポートの表示
- 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
- 自身の更新、再起動、終了

参考: RATを体験してみよう

- 体験用RATとして(会社上層部へのデモなど) 、マクニカネットワークスの凌さんがShinoBOTを作って公開している
  - 悪用されないよう、常にShinoBOT動作中のウィンドウがトップに出るし、C&Cは固定
- ShinoSec Suiteという、脆弱性を利用してマルウェアを送り込むドロッパ作成から体験できる物も
  - 脆弱性の監査やExploitテストでは、Metasploitも有名

https://shinobot.com/

兵器化されるランサムウェア

- どうも悪人はランサムウェアを効果的な金銭窃取道具と認識したようで、攻撃が高度化している
  - 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
  - ビットコイン払いに不慣れな人に対し遠隔サポートして払わせたり
- 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
  - 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
  - セキュリティアップデート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が多い

高度化したランサムウェア

- 暴露型ランサムウェア[1]
  - ファイル暗号化とともに、ファイル自体を外部に送出し、「暴露してほしくなければ…」と脅迫
  - 暴露されると困る情報を得るために、RATを使って深く浸潤して一斉に動作
  - 2020年以降に増えてきた感じ
- 被害者の挙動を見て脅迫するランサムウェア
  - ランサムウェアにRAT機能が追加され(逆かも)、被害者のPC操作の様子を見つつ効果的に脅迫
- RaaS(Ransomware as a Service)の出現
  - (RATと同様に、)送り込みキットからサーバまでのサービスパッケージを提供し、身代金の一部を受け取る

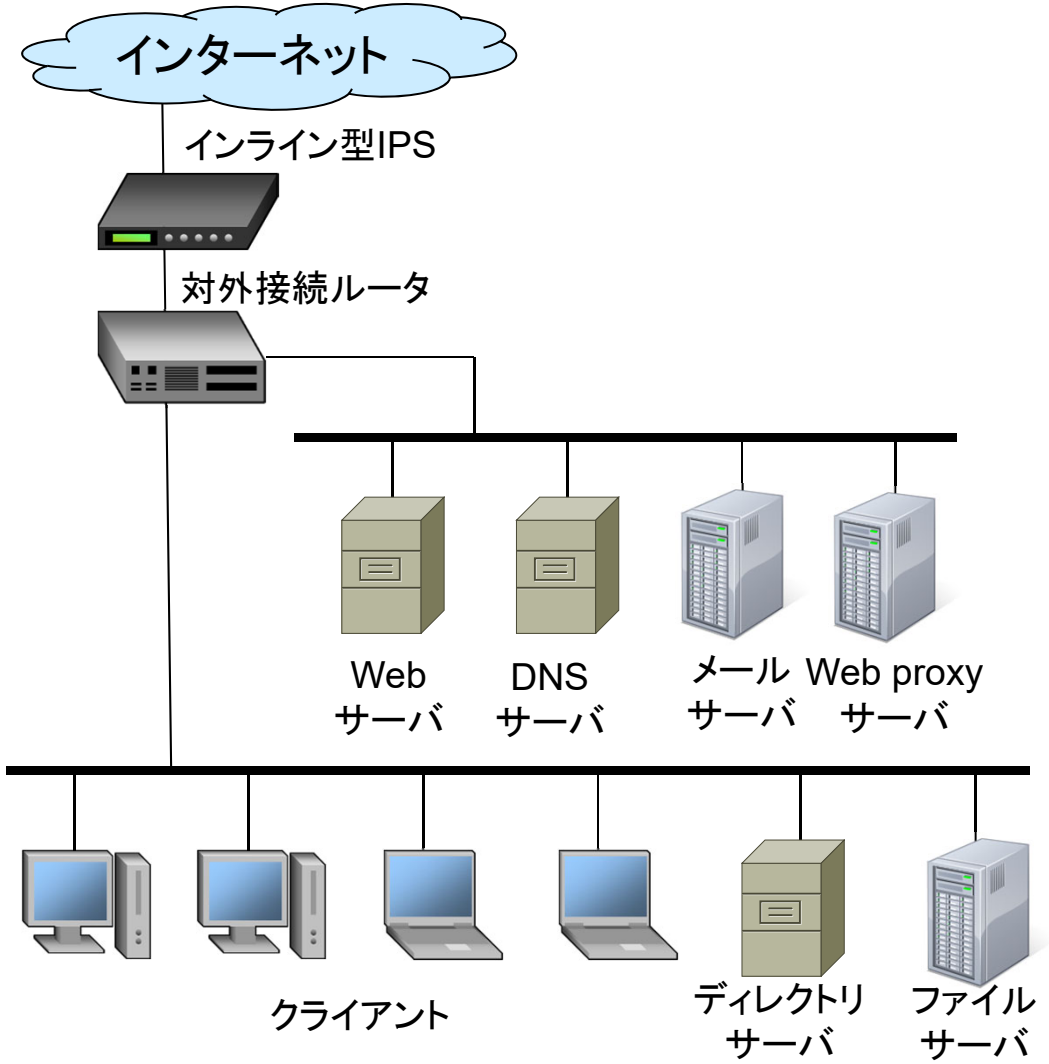
[1] https://www.macnica.net/pdf/sandj_ransomware.pdf

概要

- マルウェアの概要
  - マルウェアの種類
  - マルウェアの識別
- ネットワークを介したマルウェアの送り込みとその検知
  - メールベースの送り込み
  - Webベースの送り込み
- ネットワークを介したマルウェアの活動とその検知
- 標的型攻撃とマルウェア

セキュリティ話でよく想定される現在の一般的な組織のネットワーク構成

- 組織内の認証管理のためにディレクトリサーバが置かれている
- DMZの各種サーバ類は無い(クラウドに置く)所も多い
- Web proxyは特に無い組織が多い
  - 昔はWebページのキャッシュとかの意味もあったが



マルウェアの送り込みパターン(1/3)

- 昔ながらのメール
  - 最近では、メールボックス内メールに返信の形で出すEmotetが話題
  - 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
    - Microsoft Officeのマクロを実行させてダウンロードと実行
  - メールクライアントの任意コード実行[1]脆弱性を狙う事例も考えられる
- アプリストアに紛れ込ませる
  - 有名アプリと似た名前でマルウェアをパックした物とか
  - 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とか多かった(最近だとChatGPT)

[1] https://piyolog.hatenadiary.jp/entry/2020/04/23/123730

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 or Web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
    - 悪性JavaScriptを使ってダウンロードを促す物が多い
    - プラグインの脆弱性利用もまだまだある
  - 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
- 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(2/3)

- ソフトウェアの脆弱性(特に任意コード実行)を利用して実行させる
  - ブラウザ、ブラウザプラグイン、その他Webコンテンツを表示(インクルード)可能なアプリ
    - 裏でWebソケットベースで通信しているアプリはけっこう多い
- 各種URLのリンクを通じたダウンロード
  - 意外と普通の人はURLを意識していないことは多い
  - 最近だといろいろな所(メールクライアント、Webアプリ)でURLに対して自動的にリンクを張ってくれるので攻撃者にとって都合が良さそう

攻撃用メールアカウントはどう作られる?

- 安直な物
  - 適当なメールサーバを立てる(クラウドサービスで復権中?)
    - 最近はGMailがspam判定厳しくしたので、さらに減るかも
  - セキュリティのゆるいフリーメールアドレスを利用する
    - 評判が悪くなるとフリーメールアドレスサービス丸ごとブラックリストに入れられたり
- 信頼性の高い物
  - Gmailなどメジャーなフリーメールアドレスの利用
  - メジャーな組織のメールアカウントを乗っ取って送信
    - さらに、知り合いからのメールと見せかけることができれば開封される可能性はさらに高い
      - Emotetは受信箱のメールに返信する形で信頼性を上げている
    - 攻撃対象組織の部署とやりとりに関係する所のメールアドレスを狙うこともありうる
      - 最近ではサプライチェーン攻撃なる名前も

メールアカウントの乗っ取り

- 「Webメールの認証変わったよ(移行してね)」なフィッシングメールはよく来る
  - 「メールボックスいっぱいだよ」なフィッシングもよく来る
- 他のサービスとユーザ名とパスワードを共有していて、他のサービスでパスワード漏洩が起こる
- 信頼性の低いネットワークでPOP3/IMAP4などのパスワードを含めた通信を暗号化しないプロトコルを使う所を狙う
  - 組織が昔から使っているメールサーバとかで、昔のプロトコルそのまま使っていることはありうる
- 信頼できないネットワークで偽の(Web)メールサーバに誘導される

送り込みメールの実例

- 2017/4に送られてきたもの
  - これが一番できが良かったし、微妙なのはSubjectとFrom関係ぐらい
- マルウェアをzip圧縮ファイルで添付

From: 日本人姓名 <xxxx@xxxx.xxx.go.jp>
Subject: ご注文ありがとうございます

各位

完成しております。

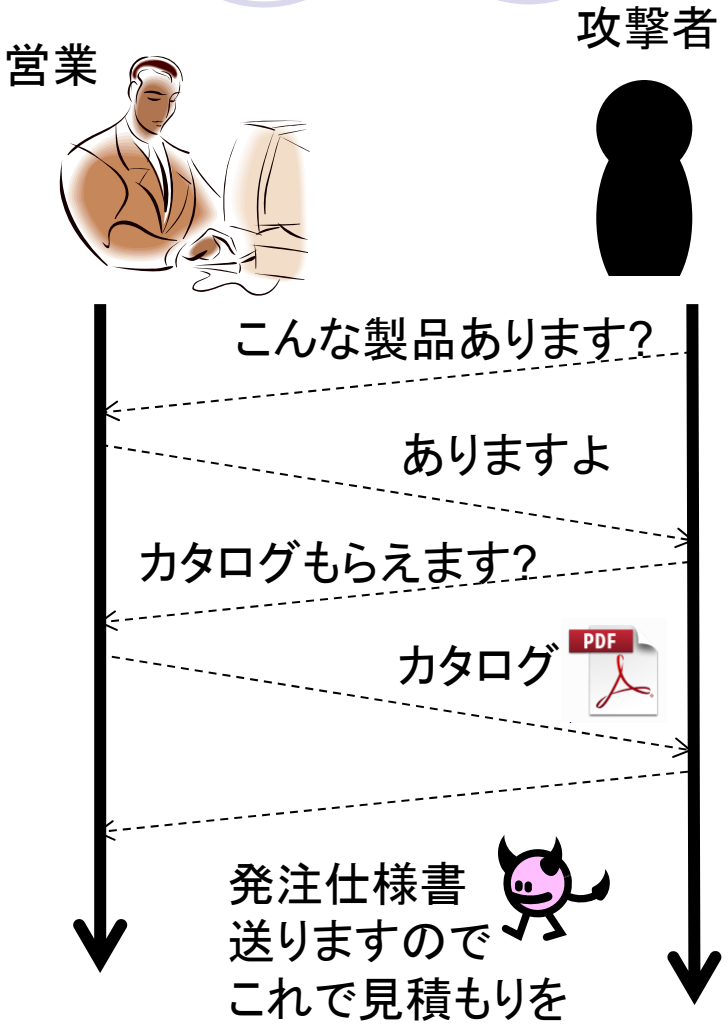
宜しくお願い致します。

実在しそうな日本人姓名と
政府系を装ったメールアドレス
をFrom欄で騙る

内容を長く書かないことで
ボロを出さないように
しているのか?

メールでのマルウェア送り込みのテクニック: やりとり型攻撃

- 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)経由の攻撃の脅威度が上昇中[1]



[1] 2018年「セキュリティ10大脅威」 http://www.security-next.com/102106

SNSの投稿やメッセージングサービスを利用した送り込み

- 主に悪性URLへの誘導
  - ファイル添付できるメッセージングサービスもあることにはあるが…
  - 最近だと、SNS上での製品に対する不満の表明に対して、公式サポートを装って悪性URLへ誘導する事例も[1]
- SNS上で悪性URLを相手に提示する方法
  - 新規アカウントを作ってフォローして相手の関心を引く
  - SNSのアカウント自体を盗んで送り込み
  - SNS関連アプリやSNS連携サービスを装ってメッセージング権限(API)の利用を認可させて送り込み
- 攻撃対象者をSNSのコミュニティや対象者の活動から絞りやすいという利点もある

[1] https://blog.kaspersky.co.jp/brand-scams-on-twitter/31236/

携帯電話のSMS(Short Message Service)を利用した送り込み

- 主に悪性URLへの誘導
- スマホの悪性アプリがSMS送信権限を得て大量に送る事例が最近増えている感じ
  - SMS送信権限を要求してくるアプリは怪しいと思った方が良さそう
- SMS送信サービスを悪意のある人が(ちゃんとお金を払って)利用して送る事例もある
- 受信側としては、送信元の情報は電話番号だけなので、判別しようがないのがめんどくさい
  - 宅配業者とか通販業者とか金融業者とか装うのが多い感じ
- 個人的には、SMSは携帯電話の初期頃からあるサービスのため、仕様を拡張してのセキュリティ対応が難しいと思う

  →SMSを情報サービスに連携させるのは悪手

Webサイトからのマルウェア送り込みのテクニック

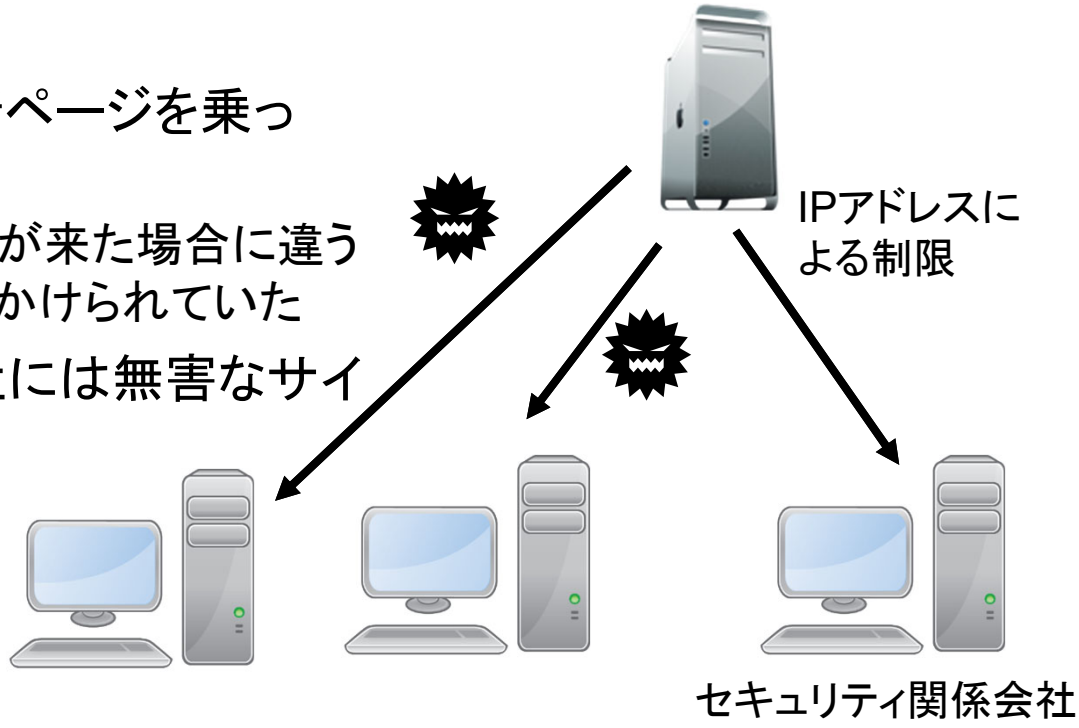
- マルヴァタイジング(Malvertizing)
  - セキュリティ警告の偽装
- 水飲み場型攻撃
- Drive by Downloadによる欺瞞/隠蔽

マルヴァタイジング(Malvertizing)

- MALware + adVERTIZING
- インターネット広告を使ってマルウェアを送り込む
  - 昔は脆弱性なプラグイン(Java, Adobe Flash)がよく狙われていた
  - 最近は悪性JavaScriptでリダイレクトとかクリックハイジャッキングとかが多そうな印象
- 最近だと、「広告業者がマルウェア配布広告を排除できないならば、AdBlockされるのはしかたがない」と言われることも
  - でも、比較的まともそうな所が利用している広告業者でも稀にマルウェア配布広告がまぎれこむことも…
- 偽セキュリティ警告を出して「アンチウイルスソフトウェア」と称してマルウェアをインストールさせることも
  - 最近だと、裏に人がいてリアルタイムでサポートするサポート詐欺も(マルウェアを入れられた上にサポート料を窃取されたり)

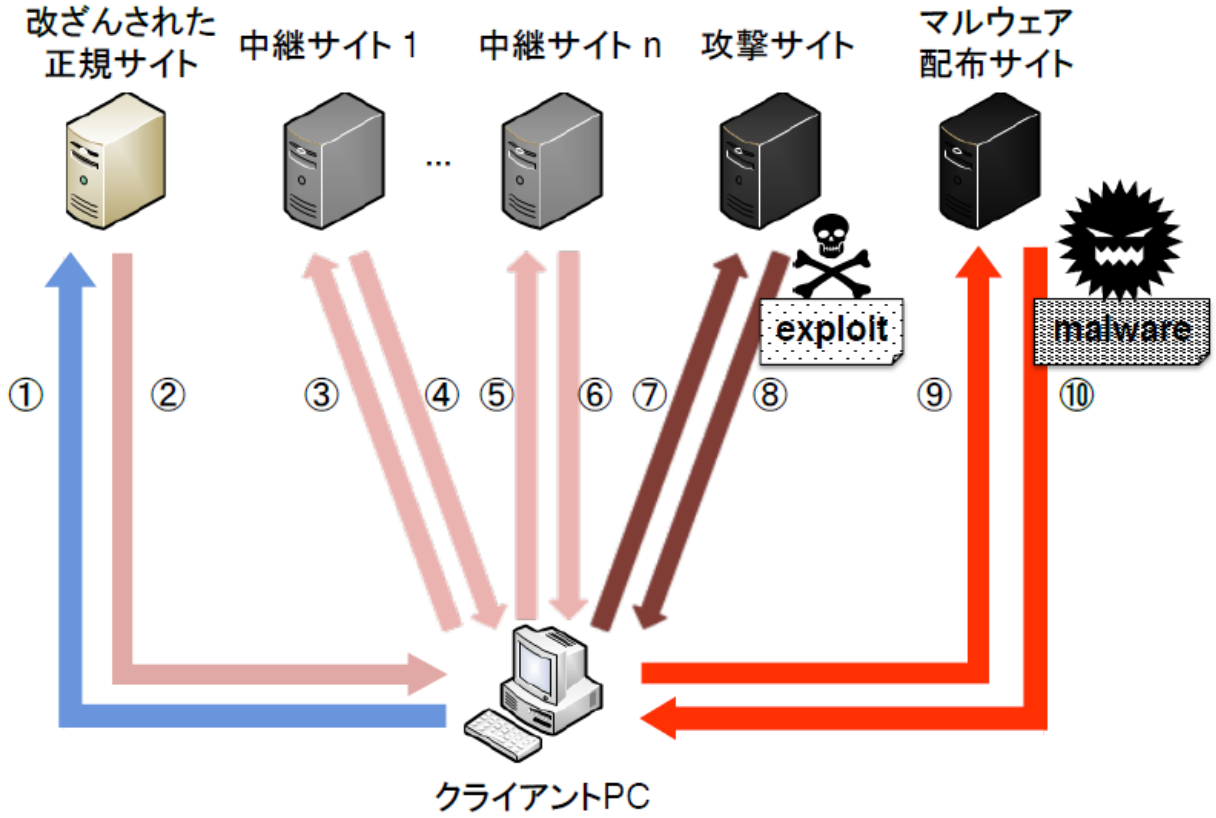
マルウェア送り込みのテクニック: 水飲み場型攻撃

- 「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



Drive by Downloadによる欺瞞/隠蔽

- 複数のサイトを経由することでマルウェア配布を欺瞞/隠蔽
  - Web側のリダイレクタやドロッパ型マルウェアの利用
  - 特定のサイトとの通信シーケンスをもととした検知を逃れたり



マルウェア送り込み時の隠蔽テクニック

- 実行ファイルをパッカーでパッキングして検知回避
- OSやブラウザのバージョンによってドロッパの挙動を変える
  - 本命以外がアクセスしてもマルウェアが送り込まれない
  - インシデント対応する人やアンチウイルスベンダの対応が遅れる
- サンドボックス検知回避
  - サンドボックスを備えたセキュリティ機器を回避
  - アンチウイルスソフトウェアベンダにおける解析回避も兼ねる
- 本命マルウェア以外のおとりマルウェアも送り込む
  - アンチウィルスでスキャンした時におとりマルウェアが検出/駆除されると人間は安心する

ネットワーク上でどうマルウェア送り込みを検知する? (1/3)

- IDS(Intrusion Detection System)
  - 基本は悪性通信の検知だが、マルウェア対策にも使える
    - 「マルウェア配布先」とblacklistに乗っているURLやIPアドレスを検知
    - サンドボックスを備えてダウンロードした実行ファイルを動作確認できるIDSも多い
    - ただし、マルウェア対応の追加ライセンスが必要だったりする
  - 自動でブロックまでやるIPS(Intrusion Prevention System)も
  - 最近だと、いろいろやるのでUTM(Unified Threat Management)システムを名乗っていることも
  - ただし、最近はTLSで暗号化された通信で送り込まれることが多いため、Man-in-the-Middleをしないとurlやファイルの検知ができない
    - クライアントにUTMのTLS証明書を入れないとMITMできない
    - 正規のTLSを使った通信も一旦暗号化を解くのはプライバシーの問題が発生する点がやっかい(業務規則で縛れる会社はやりやすいが…)

ネットワーク上でどうマルウェア送り込みを検知する? (2/3)

- URL blacklist対応Web proxy
  - やることはIDS/IPS側と変わらない
  - ファイアウォールでproxyを迂回したWebアクセスの禁止も忘れずに
- DNS (DNS blacklisting)
  - 悪性ドメインの名前解決が来たら返事を返さない
  - 外部のDNSを参照されたりすることで迂回されないように注意
    - DNS over HTTPSとかやられたら対策無理そう
- メールサーバ側でのアンチウイルスソフトウェア実行
  - クライアント側に入る前にブロックできるならばその方が良い
    - 警告を無視して実行する人が世の中にはいっぱいいる
  - 特定の形式の添付ファイルは全て落とすという対策もあり
  - 添付ファイルは全てプレビュー機能付きファイルサーバに送り込んでファイルサーバへのリンクを貼るという対策もある

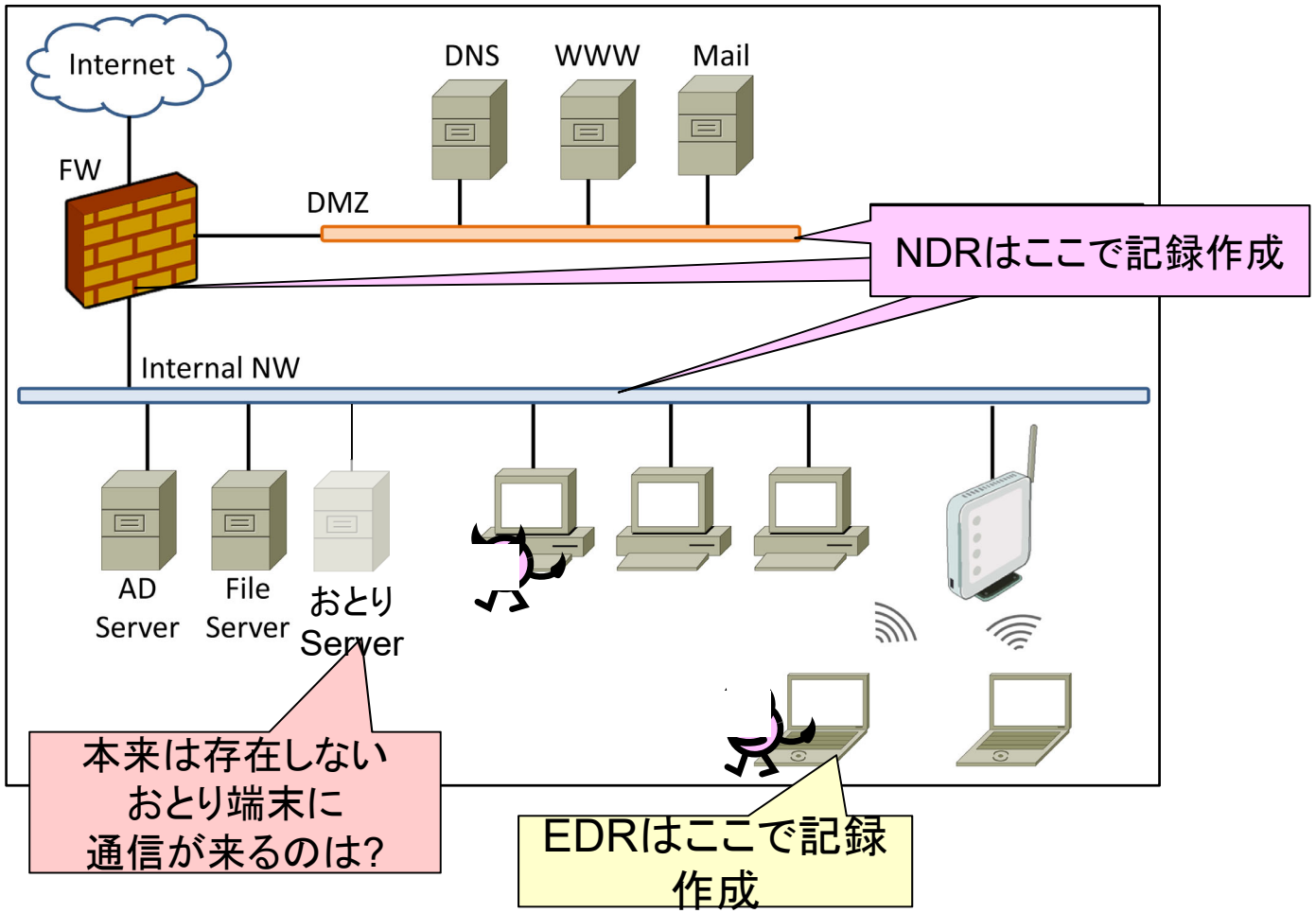
ネットワーク上でどうマルウェア送り込みを検知する? (3/3)

- クライアント側でのアンチウイルスソフトウェア実行
  - 最近はblacklist入りしているURL等への接続の段階でブロックしたりしてくれる
  - 最近はWindows Defenderが良くなっているので、変なアンチウイルスソフトウェアを入れるよりはWindows Defenderを使った方が良い
    - 逆に、アンチウイルスソフトウェア会社の方がインストール(=金を取る)させるためにアレなことをやっている事例も
  - 最近では、ログなどをがしがし採取した上で外部での状況解析も得意なEndpoint Detection and Response型の製品も多い
    - クライアント上でのプロセスの実行、ファイル操作、ネットワークアクティビティ、ログイン状況、シェル上での実行内容、などを採取
    - 採取されたログはネットワークで上流にあるUTM製品などとの連携や組織のSOCなどで検知に利用される

多くのセキュリティソリューションも端末上やネットワーク上の挙動から検知に

- 最近はセキュリティソリューションがEDR/NDR/(+おとり端末)を押しているのをよく見かける
  - EDR(Endpoint Detection and Response): 端末にEDRソフトウェアを入れてイベント(API呼び出し、ファイル操作)を記録し事後対応へ
  - NDR(Network Detection and Response): 組織内ネットワークのネットワークスイッチ等から通信サマリを収集して事後対応へ
  - おとり端末: 組織内ネットワークにおとり端末を設置し、アクセス元を怪しい認定
- どれも、「マルウェア等に感染して、怪しい行動を取っているけど、マルウェアの初期侵入は防げていない」状態を想定
  - 記録から怪しい端末を探して詳細解析へ
    - 「これ感染しています!」までは断定できないレベルから検知
  - 記録から被害範囲を同定して、いち早く通常業務に復帰

EDRとNDR(+おとり端末)の記録する所



概要

- マルウェアの概要
  - マルウェアの種類
  - マルウェアの識別
- ネットワークを介したマルウェアの送り込みとその検知
  - メールベースの送り込み
  - Webベースの送り込み
- ネットワークを介したマルウェアの活動とその検知
- 標的型攻撃とマルウェア

ネットワークから見るマルウェア検知

- 検知は主にネットワーク型侵入検知システム(NIDS)で実施
  - IPSやUTMのようにブロックまで行うものも
  - 最近ではEDR(Endpoint Detection and Response)のようにクライアント端末と連携も
- 「感染後に何が行われたか」を追跡して確認できるよう記録を残す側面も大きい
  - 現状、マルウェア感染は誰かがやらかすと想定すべき
  - 組織への標的型攻撃も想定すると、特に追跡は大事

  →ネットワークフォレンジック
- とは言え、いろいろとブロックできたら嬉しい通信も多数
  - ドロッパ系マルウェアによるより高機能なマルウェアの送り込み
  - マルウェアの遠隔操作を行うC&C通信
  - スパイウェア系マルウェアによる情報送出

ドロッパ系マルウェアの通信

- Webサイトなどからより高機能なマルウェアをダウンロード
- ただし、あの手この手で検知を避ける努力をされている
  - 例: 複数のファイルに分割した上に暗号化されているものを再構築
  - 例: 他の形式のファイルやパケットの空き領域に分割し…
- ネットワーク上での検知
  - 脅威情報に基づく悪性URLや悪性IPアドレスへのアクセスを検知
    - 可能ならば、脅威情報はセキュリティ関連会社で分単位でアップデートされるレベルの物を利用(もちろん、お高い)
  - (怪しいファイルの送り込みを検知)
    - HTTPSとか使われると検知できない (企業とかでは暗号化をほどくUTMやproxy併用したり)
- 利用者にURLを誤クリックさせる系の送り込みも同様に検知

マルウェアの遠隔操作に使われる通信 (Command and Control通信) (1/2)

Command and Control (C&C, C2)通信と呼ばれる

- はるか昔は独自プロトコルや普通はあまり使わないプロトコルなどが使われた
  - 独自プロトコルだと、独自のポート番号を設定するので分かりやすい
  - IRC(Internet Relay Chat)のプロトコルもよく使われた
    - その関係で、いくつかの組織でIRCプロトコル自体の禁止のルールが残っていたりする
- 今はWebサーバを立てて、HTTPSを当たり前のように使う
  - よく使われる通信にまぎれ込ませて検知を難しくさせる
  - よく利用されるWebアプリケーションをC&Cに使うことも
    - Twitter, GitHub, Gmail(のメールボックス), Slack, など

マルウェアの遠隔操作に使われる通信 (Command and Control通信) (2/2)

- DNS通信に紛れ込ませるものも存在[1]
- ネットワーク上での検知
  - 脅威情報に基づく悪性URLや悪性IPアドレスへのアクセスを検知
    - 可能ならば、脅威情報はセキュリティ関連会社で分単位でアップデートされるレベルの物を利用(もちろん、期間ライセンスがお高い)
  - (普段使われていないプロトコルや通信先との通信の検知)
    - こいつも暗号化が…(悪い人も暗号化を活用してくる)

[1] https://www.lac.co.jp/lacwatch/alert/20160201_000310.html

外部に情報を送出する通信の検知

- スパイウェアやRATは窃取した情報をネットワークを介して外部に送出する
- 検知
  - (脅威情報に基づく悪性URLや悪性IPアドレスへの…)
  - 通常の(業務)活動から見られない活動の検知(アノマリ検知)
    - 特定の外部IPアドレスやサービスとの継続的な通信
    - 特定の内部IPアドレスからの総通信量の統計の取得すると異常に多い
    - 規格上、微妙な通信がある
      - 他の通信のペイロードにまぎれこませる
      - 分割して送信している

組織内で感染拡大する通信の検知

- 組織内の(プライベート)IPアドレスをスキャン
  - ついでに、空いているポートの種類を調べる
  - ただし、低レートでスキャンしたりされると見つけにくい
- 空いているポートに対してサーバのバージョン等の情報取得の試み
- サーバ等の空いているポートや社内Webシステムへの認証突破の試み
- 空いているポートへの脆弱性を利用した感染拡大の試み
- 検知
  - 組織内通信に対するIDSの適用(…は高くつきそう)
  - 組織内通信のフローデータからの検知
  - 各端末側でのアンチウイルスソフトなどによるスキャン等

その他のマルウェアのネットワーク上での検知

- ランサムウェア系
  - そもそもネットワークで動きが見つかった時には手遅れ
  - クライアント端末が感染してファイルサーバを暗号化する動きは組織内トラフィックから検知できそう
    - ファイルサーバ側での異様なI/O量とかで検知した方が良さそう
- マイニングマルウェア系
  - マイニングネットワークへの接続で検知
- アドウェア/フリースウェア系
  - 普通に広告ネットワークや決済業者につないでいるだけなので検知は難しそう
    - アドウェアは、広告の量が多すぎる点で検知できる可能性はありそう

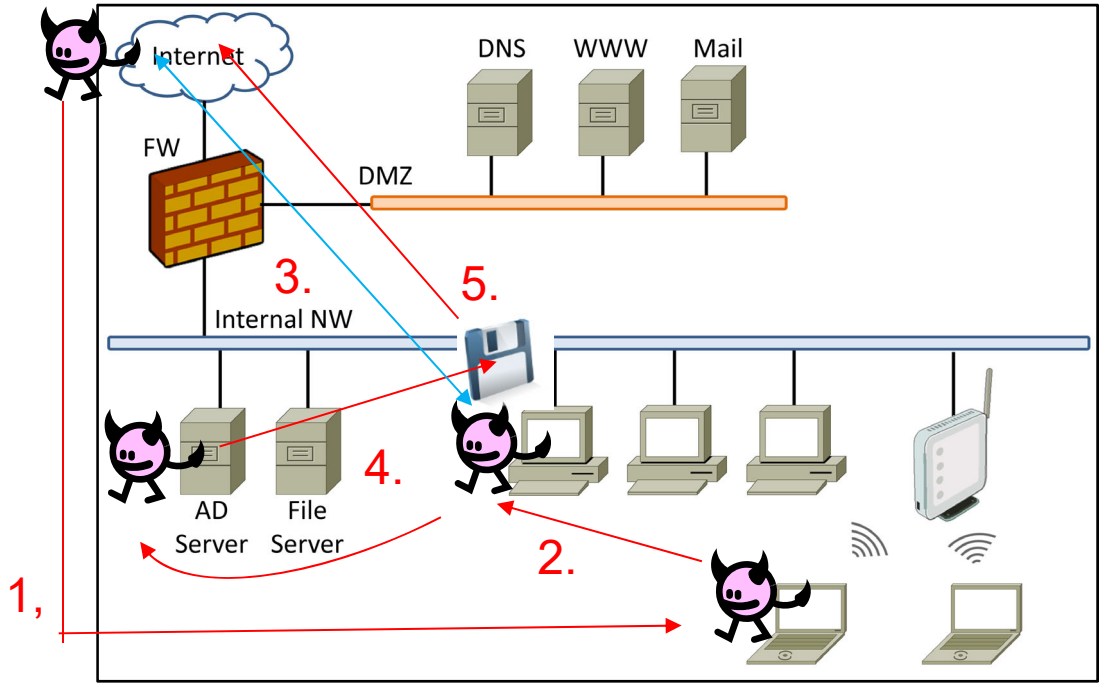
概要

- マルウェアの概要
  - マルウェアの種類
  - マルウェアの識別
- ネットワークを介したマルウェアの送り込みとその検知
  - メールベースの送り込み
  - Webベースの送り込み
- ネットワークを介したマルウェアの活動とその検知
- 標的型攻撃とマルウェア

標的型攻撃とその進行

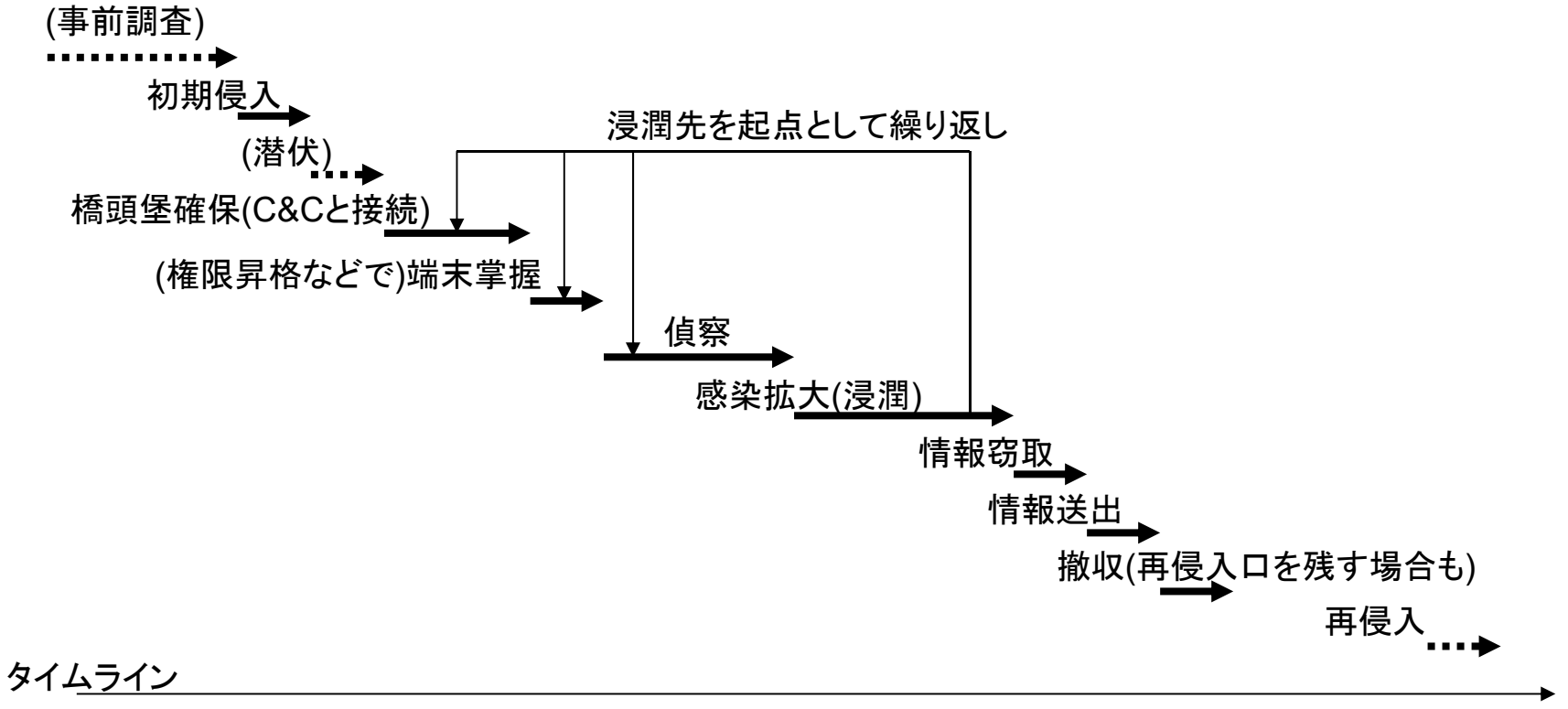
- 英語ではAdvanced Persistent Threat(高度な執拗な脅威)
  - 失敗しても何度も攻撃を試みる
- 代表的な標的型攻撃の進行
  - 侵入前に組織の内部構成を調査することもある
  - 長いものだと攻撃に数ヶ月かけることもある

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



標的型攻撃のタイムライン

- 事前調査や潜伏や再侵入は存在しないこともある
  - 個人的には、「うまく初期侵入できたから」という理由から始まる標的型攻撃もあると思う



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(1/2)

- 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

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(2/2)

- 海外拠点とBYOD端末の2経路から侵入されたNTTコミュニケーションズの事例[1, 2]
  - 海外拠点からの侵入は、3カ国の営業所を経由した多ホップの侵入
    - 撤去を控えたサーバを踏み台にされた
  - 2系統から最終的に社内ファイルサーバにたどり着かれた

個人的には、企業も標的型攻撃対策に活用できるレベルの報告書を出してきてくれて嬉しい

- 個人的には、このレベルで報告書を出せる企業の方が信用できると思う

[1] https://piyolog.hatenadiary.jp/entry/2020/07/03/180308
[2] https://www.ntt.com/about-us/press-releases/news/article/2020/0702.html

よく行われる標的型攻撃対策(1/2)

- ネットワーク分離や権限の分離
  - ただし、攻撃者側の執拗な攻撃に対しては、攻撃の進行を遅くする程度にしか役にたたない
- シナリオベースの標的型攻撃対応演習
  - CSIRT(Computer Security Incident Response Team)のチームとしての動きの練習としてよく行われる
  - レスポンスチームだけでなく、組織上層部の最終判断層も巻き込んで実施する
  - 攻撃者側もチームを組んで実施することも(レッドチーム)
    - 対応する防御側はブルーチームと呼ばれる
    - レッド/ブルーのチーム間で演習の効率を上げるために、状況を見つつ一部の情報(ヒント)を相手側与えるパープルチームという存在も

よく行われる標的型攻撃対策(2/2)

- ペネトレーションテストの実施と見つかった穴への対応
  - 現場レベルには事前連絡せずに、上層にのみ了承を取ってペネトレーションテストを実施することも
- 「怪しい挙動」を放置しない体制
  - 個人的には、「怪しい挙動」を調べて攻撃の発見に至る事例が多いように感じる
- クライアント端末上でも遠隔でインシデント対応できるセキュリティ体制の構築
  - EDR(Endpoint Detection and Response)製品群
  - クライアント端末上でのイベントをきっちりロギングした上で問題挙動をCSIRT等にレポート
  - CSIRT側はレポートをもとにインシデント対応方針を決め、クライアント端末側にアクションを指示