A-1.
標的型メールによるサイバー攻撃

青山学院大学
根本　貴弘

このセッションの目的

- **標的型攻撃メールの中身とマルウェア感染の影響**
  - 「どこで」「どうやって」感染するのか？
  - 感染すると何が起きるのか？
- **サイバー攻撃のシナリオ**
  - 内部調査→感染拡大→目的達成

↓

マルウェアに感染したときの影響をいち早く想像できる

マルウェア概観

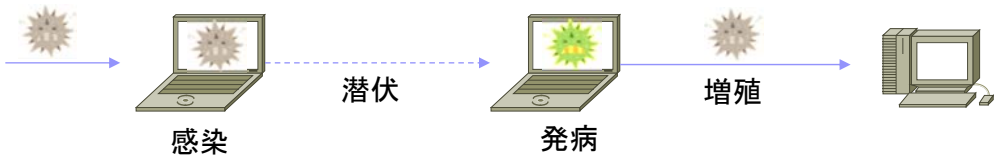
マルウェアとは？

- 不正な動作をすることで，コンピュータやプログラムに対して被害を加える悪意あるソフトウェアの総称
- malware = malicious(悪意ある) + software
- 様々な種類がある
  - 拡散方法による分類
    - ウイルス
    - ワーム
    - トロイの木馬
  - 機能による分類
    - 情報の持ち出し（スパイウェア）
    - 他のマルウェアへの感染（ダウンローダーやドロッパー）
    - 遠隔制御（ボットやRAT）
    - ファイルの暗号化（ランサムウェア）

…等々

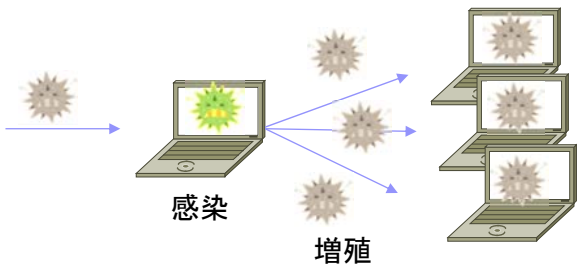
拡散方法による分類：ウイルス

- **自己増殖機能**を持ち，**他のプログラムに寄生**し，そのプログラムを実行することで，コンピュータやプログラムに対して被害を加えるように作成されたマルウェア
- 特徴
  - 自己増殖
    - 感染PCの機能を用いて（もしくはプログラムを書き換えて），**他のPCにウイルスをインストール**する
  - 潜伏
    - 感染PC内で**特定のプログラムが実行されるまで，不正な挙動を示さない**．一定時間や特定の時刻になるまで不正な挙動を示さない場合もある
  - 発病
    - 感染PC内の**情報の消去**，**改ざん**，**外部流出**等，利用者の意図しない挙動を行う



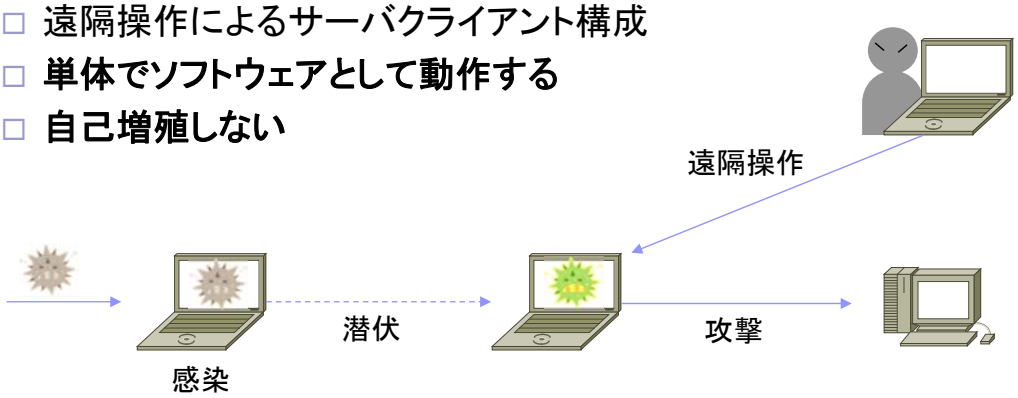
拡散方法による分類：ワーム

- **単独で**自己増殖可能で，他のプログラムの動作を妨げたり，利用者の意図しない挙動を示すマルウェア
- 特徴
  - 完全に**自己完結したプログラム**
    - ホストプログラムやユーザの操作を必要としない
  - **自己増殖**
  - データの**改ざん**や**削除**等を行うものが多い
  - ウイルスやトロイの木馬と比較して**感染速度が早い**



拡散方法による分類:トロイの木馬

- 利用者にとって**有用なソフトウェアを装い**感染PCに潜伏し，破壊活動や情報窃取を行うマルウェア
- 攻撃者による**遠隔操作**によって行動するものもある
  - RAT(Remote Access Tool)と呼ばれることがある
  - 攻撃者側クライアントを**C&C(Command & Control)サーバ**と呼ぶ
- 特徴
  - 遠隔操作によるサーバクライアント構成
  - **単体でソフトウェアとして動作する**
  - **自己増殖しない**



トロイの木馬の種類

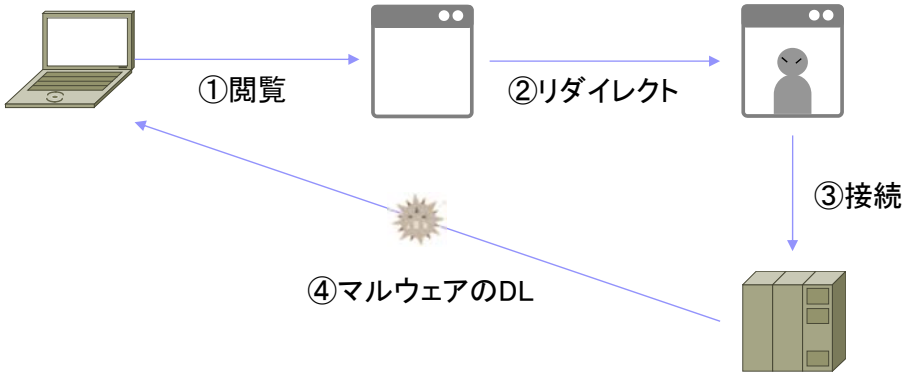
- **バックドア型(RAT)**
  - インターネット経由で標的PCを不正操作するためのソフトウェア
- **パスワード窃取型**
  - IDやPWなどの情報摂取を目的としたソフトウェア
- **ダウンローダー型**
  - バックドアとなる不正プログラムをダウンロードするソフトウェア
- **ドロッパー型**
  - バックドアとなる不正プログラムが内包されたファイルを感染PCにドロップする(ダウンロード型に比べてファイルサイズが大きい傾向にある)
- **プロキシ型**
  - 感染PCのルータやDNSの設定を改変し，PC上に踏み台用プロキシサーバを構築する．この種類の感染PCの集合体はボットネットとして機能することがある

マルウェアの感染経路

- **メール添付**
  - 添付ファイルにマルウェアが埋め込まれており，添付ファイルを開くと感染させられる
- **Web誘導**
  - メールに記載されたURLのWebページにアクセスするとマルウェアがダウンロードされる
- **Web閲覧**
  - 閲覧したWebページにマルウェアが埋め込まれており，Webページを閲覧した際にダウンロードされる
- **ネットワーク**
  - ネットワークスキャンを行うなどして，ソフトウェアの脆弱性やPCの設定不備をついて感染させる
- **外部記憶装置**
  - USBメモリ等の外部記憶装置経由で感染する
- **共有ディレクトリ**
  - 共有ディレクトリ経由で感染する

ドライブ・バイ・ダウンロード

- インターネット経由で，標的PCにマルウェア等をダウンロードさせるための攻撃手法

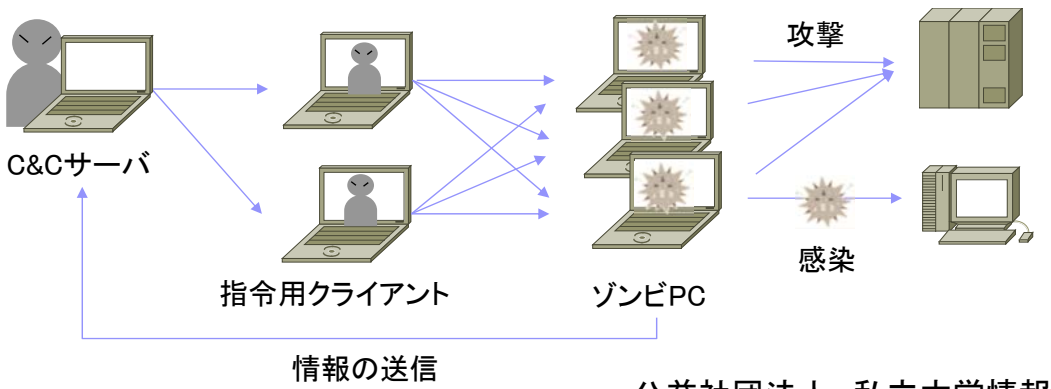


機能による分類：スパイウェア

- 利用者の情報を収集し，**収集した情報を攻撃者に送信するための不正プログラムの総称**
- 特徴
  - 利用者が気づかないように**バックグラウンドで情報収集**を行う
  - 正規のソフトウェアにも混入している場合がある
    - 利用者情報の収集のため
  - 収集する情報は，**ID/PWや**プライバー情報等
- 種類
  - システム・モニタ
  - トロイの木馬
  - アドウェア
  - トラッキングクッキー

機能による分類：ボットネット

- ボットと呼ばれるマルウェアに感染したPC等で構成されるネットワーク
  - トロイの木馬等で乗っ取られたゾンビPCで構成されたネットワークも含まれる場合がある
- 数百～数万台で規模で，攻撃者の指示で動作する
  - **DDoS攻撃**を用いたサイバー攻撃や**スパムメール**，**スパイウェア**等に悪用されることがある

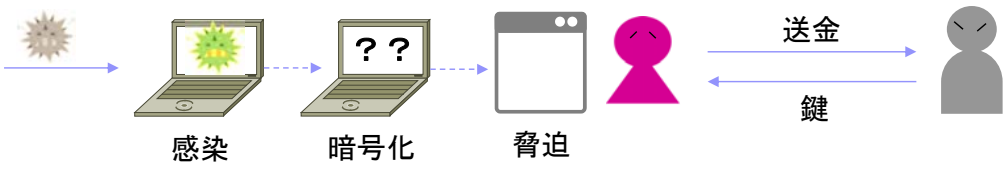


ボットとRATの違い

- ボット
  - **間接的**な遠隔操作
    - 感染PCが攻撃者からの指令を受け取りにいく
  - 操作対象となる感染PCは**不特定多数**
  - 機能は**限定的**
- RAT
  - **直接的**な遠隔操作
    - 攻撃者が直接感染PCを操作
  - 操作対象となる感染PCは**特定少数**
  - 機能は**無制限**
    - 代表的な機能は，感染PCの画面共有，ファイル閲覧，キー入力情報の取得，Webカメラの制御等

機能による分類：ランサムウェア

- 感染PCの利用に**制限**をかけることで，**身代金の要求**をすることを目的としたマルウェア
- Ransomware = Ransom(身代金) + Software
- 特徴
  - PC利用に制限をかける
    - ファイル暗号化型
    - 端末ロック型
  - 制限解除のためのメッセージが表示される



標的型攻撃メール

「情報セキュリティ10大脅威2018」

■ 「組織」向け脅威

1. 標的型攻撃による被害
2. ランサムウェアによる被害
3. ビジネスメール詐欺による被害
4. 脆弱性対策情報の公開に伴う悪用増加
5. 脅威に対応するためのセキュリティ人材の不足
6. ウェブサービスからの個人情報の窃取
7. IoT機器の脆弱性の顕在化
8. 内部不正による情報漏えい
9. ービス妨害攻撃によるサービスの停止
10. 犯罪のビジネス化（アンダーグラウンドサービス）

出展：IPA（独立行政法人　情報処理推進機構）https://www.ipa.go.jp/security/vuln/10threats2018.html

「情報セキュリティ10大脅威2018」

第1位　標的型攻撃による情報流出

企業や民間団体や官公庁等，特定の組織を狙う，標的型攻撃が引き続き発生している**メールの添付ファイル**を開かせたり，**悪意あるウェブサイト**にアクセスさせて，PCをウイルスに感染させるその後，組織内の別のPC やサーバーに感染を拡大され，最終的に**業務上の重要情報**や**個人情報**が窃取されるさらに，金銭目的な場合は，**入手した情報を転売等されるおそれもある**

出展：IPA（独立行政法人　情報処理推進機構）https://www.ipa.go.jp/security/vuln/10threats2018.html

標的型攻撃とは

- **情報窃取を目的**とし，**特定の組織**を対象に継続的に行われる一連のサイバー攻撃
  - 攻撃対象
    - 政府，官公庁，企業など，重要情報を持つ組織
    - 上記に関連する他組織や個人が一時的な攻撃対象となる場合もある
    - 不正プログラムをばらまき，侵入に成功した組織

- **事前調査**の後，対象組織の端末に**不正プログラム(主にRAT ※1)を侵入**させ，**C&C通信※2による遠隔操作**で情報窃取のための**基盤構築**，**内部調査**を行い目的を遂行する

  ※1　Remote Access Tool．ユーザがコンピュータを遠隔操作するためのツール

  ※2　攻撃者サーバからの命令(Command)を受信し，不正プログラムを制御(Control)する通信

  - 不正プログラムを侵入させるために様々な手口が使われる
    - メール（ばらまき型，やりとり型等）
    - Web閲覧（水飲み場）
    - ソフトウェアアップデートの悪用
    - USB
    - ソーシャル・エンジニアリングを用いず直接システムの脆弱性をつく

標的型攻撃の流れ

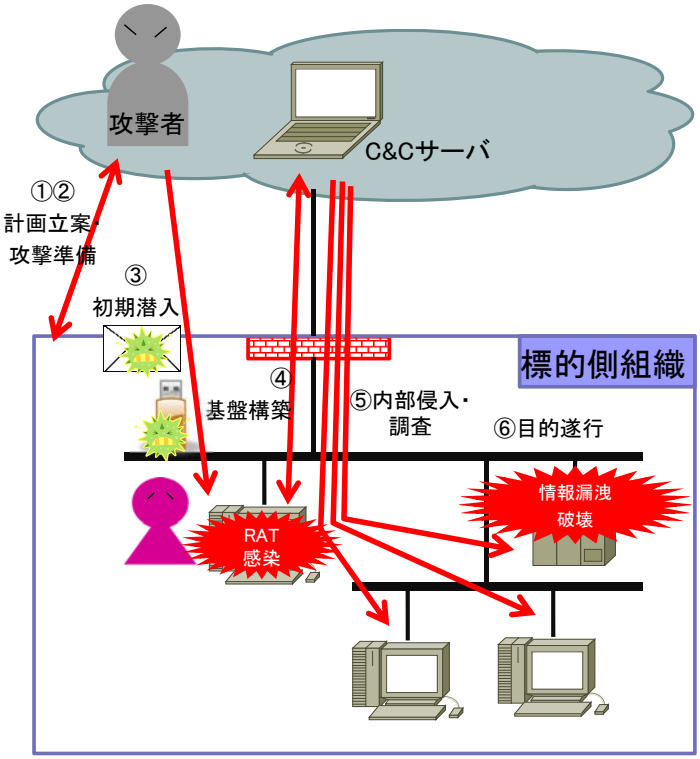
① 計画立案
② 攻撃準備
標的となる組織の情報を収集，準備を行う．

③ 初期潜入
標的型メール等でウィルス(主にRAT)を送信，感染．SNSやUSBメモリを使う場合も

④ 基盤構築
RAT経由で各種ハッキングツールを送信

⑤ 内部侵入・調査
④のツールを用いてさらに内部システムの侵入を行い調査を進める

⑥ 目的遂行
⑦ 再侵入
最終目的の達成



標的型攻撃メールとは

- **情報窃取を目的**として**特定の組織**に送られるウイルスメール [1]
  - 送信者名として，実在する信頼できそうな組織名や個人名を詐称
  - 受信者の業務に関係の深い話題や，詐称した送信者が扱っていそうな話題
  - ウイルス対策ソフトを使っていてもウイルスが検知されない場合が多い
  - メールが海外のIPアドレスから発信される場合が多い
  - 感染しても，パソコンが重たくなるとか変なメッセージが表示されることは余りない
  - 外部の指令サーバ(C&Cサーバ)と通信
  - 長期間にわたって標的となる組織に送り続けられる(内容は毎回異なる)

[引用1] IPA(独立行政法人 情報処理推進機構)：標的型攻撃／新しいタイプの攻撃の実態と対策(2011年11月)
https://www.ipa.go.jp/files/000024542.pdf

同じ文面やプログラムによるメール

[参考] 平成29年の傾向
- 標的型メール攻撃件数：6,027件(過去最多)
  - ばらまき型：5,846件　(平成28年は3,641件，平成27年は3,508件)
  - ばらまき型以外：181件(平成28年は405件，　平成27年は320件)
- 添付ファイルのファイル形式
  - 圧縮ファイル：58%　(平成28年は89%)
  - Word文書：28%　(平成28年は9%)

攻撃対象に特化したメール(やりとり型等)

[参考] 警視庁：平成29年におけるサイバー空間をめぐる脅威の情勢について(2018年3月)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf

標的型攻撃メールの事例

- 業務連絡を装うメール．複数の組織を標的としたようなメールもある
  - 内部組織や外部組織，複合機からの連絡メールを偽装したもの

［参考］青山学院大学情報メディアセンター：
【注意喚起】添付ファイルの付いた不審なメールについて（2015年10月）http://www.aim.aoyama.ac.jp/c/4662/
【注意喚起】人事課を装った添付ファイル付きの不審なメールについて（2016年1月）http://www.aim.aoyama.ac.jp/info/aim/5052/
【注意喚起】文部科学省を装った添付ファイル付きの不審なメールについて（2016年5月）http://www.aim.aoyama.ac.jp/info/aim/5607/

［送信元アドレス］ RNP0026738E40D2**@aoyama.ac.jp**
［件名］ Message from “RNP0026738E40D2”
［内容］
このメールは『RNP0026738E40D2』（MP C5503 JPN）から送信されたものです

読み取り日時: 2015.10.08 7:20:34 (+0900)
問い合わせ先: xxxx**@aoyama.ac.jp**

西東京複合機より送信

添付されていたファイルは，
「Word文書」形式

- 「ばらまき型メール」の日本語化・巧妙化に伴い，標的型攻撃と同等のリスクの懸念
  - クロネコヤマト，日本郵便の配達通知メールを偽装したもの

［参考］ヤマト運輸：ヤマト運輸の名前を装った添付ファイル付きの不審メールにご注意くださいhttp://www.kuronekoyamato.co.jp/info/info_160629.html

- メールアカウントの不正利用による標的型攻撃メールのばらまき

［参考］青山学院大学情報メディアセンター：
【緊急】（大学・短大の教員の方へ）LDAPパスワード変更のお願い（2017年12月）https://www.aim.aoyama.ac.jp/c/7477/

標的型攻撃メール例（「やりとり」を伴う手口）

- はじめから攻撃（不正プログラムの送付）を行わず，偵察を通じ標的組織からの返信を待ち，返信のあった連絡先に対して攻撃を行う
- 事前調査で盗みとった業務メールの文面が利用される場合もある

表 2014年10月の「やり取り型」攻撃の事例（メールの流れ）［2］

No.	種別	内容
1	偵察	某所の研究員を名乗る者から，当該組織がウェブサイトで公開している記事への質問について，問い合わせ窓口の確認の無害なメールが届いた．宛先のメールアドレスは，当該組織のウェブサイトから知ったと書かれていた．
2	返信	質問を受け付ける旨，返信した．
3	攻撃	「質問内容を送付する」という内容で，**パスワード付きzipファイル**が添付されたメールが届いた．更に，**パスワードは別途送付する**旨が書かれていた（このzipファイルの中には，Word文書ファイルのアイコンに偽装した実行ファイル形式のウイルスが入っていた）．
4	偵察	約1分半後，zipファイルのパスワードを通知するメールが送られた．メールの文面には，「このメールは自動で配信されています．」などと書かれており，**メール暗号化システムが自動的にパスワードを作成・送付しているかのように見えるものに偽装**されていた．
5	返信	添付ファイルの内容が確認できなかったこと，そして，**メール本文に用件を記載して再送いただくよう**返信した．
6	偵察	約40分後，記事の内容に関する質問が**メール本文に書かれて**再送されてき

［引用2］IPA（独立行政法人 情報処理推進機構）：組織外部向け窓口部門の方へ：「やり取り型」攻撃に対する注意喚起 ～ 国内5組織で再び攻撃を確認 ～
https://www.ipa.go.jp/security/topics/alert20141121.html

初期潜入方法

- 代表的な潜入方法
  - メールからの潜入（ばらまき型，やりとり型）
    - 不審なファイルを添付したメールを送信
    - 不審なURLリンクが本文に記載されたメールを送信
  - USBメモリからの潜入
  - Webからの潜入（水飲み場型）

- 添付ファイルを実行，またはURLリンク先にアクセスさせた後にRAT（遠隔操作マルウェア）を使って次の段階（基盤構築）に進む

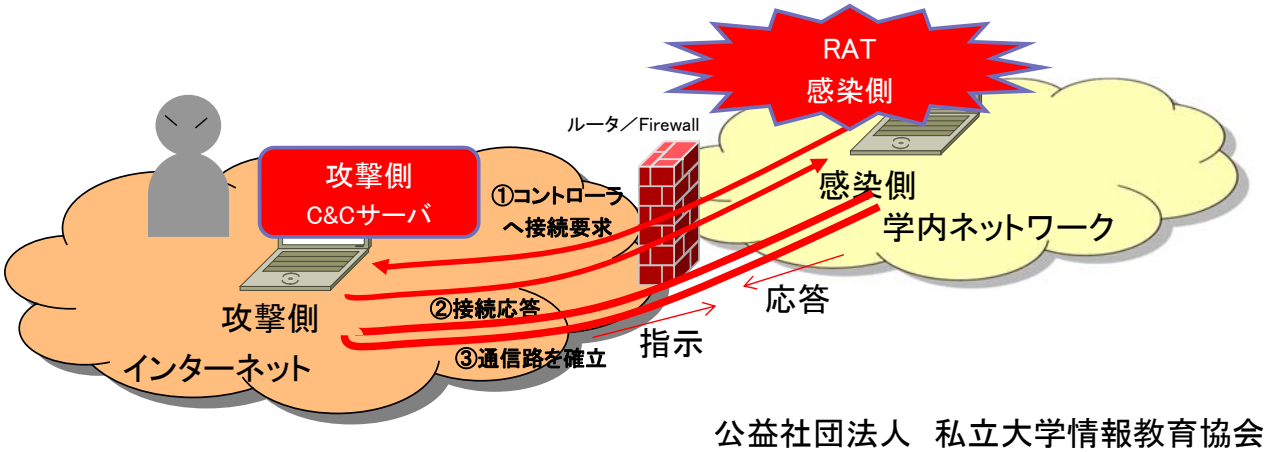
RATとは

- RAT = Remote Admin Tool (?)
  Remote Access Trojan(?)
- 「バックドア通信」を行うマルウェアの総称
  - インターネット上の攻撃側サーバ(C&Cサーバ)からの指示により，マルウェアの拡散や情報収集の足がかりに

  （例） **Bozok，H-Worm**
  - 感染してしまうと攻撃者は感染端末に対して以下のようなことを行えるようになる
    - 各種コマンドの実行
    - キー入力情報の取得
    - 画面閲覧，操作
    - ファイル転送

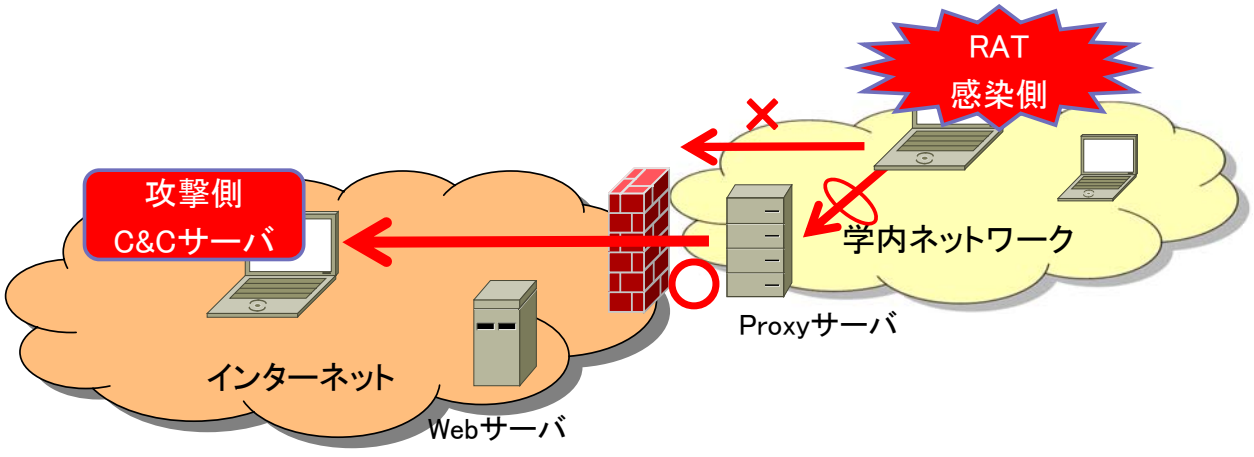
RATの特徴 （1）

- 攻撃側への着呼型
  - もともと内部ネット→外部ネットへ通信可能なサービスを模して，感染PC～攻撃PC間の通信路を確立
  - 通常の通信とRAT通信の見分けが困難
    - ポート番号： 80/tcp(http)， 443/tcp(https)等



RATの特徴 （2）

- 出口対策が困難
  - Proxyサーバに対応しているRATもある
    - 感染PCからインターネットへブラウザでアクセス可能ならば，攻撃側PCから感染PCのコントロールが可能



RAT感染後：基盤構築

- 初期潜入に成功すると，攻撃者は次に潜入先の内部情報を窃取するための「**基盤構築**」を行う
- 基盤構築の段階では，内部情報を窃取するためのツールを送り込み，インストールされる
- 現在の標的型サイバー攻撃は「**潜伏型**」と「**速攻型**」の2種類に大別できる
  - 「潜伏型」：重要情報窃取を果たすまで活動する
    - 潜入してから実際に攻撃を開始，終了までの期間が長いもの（平均5か月）
    - 潜入後，攻撃（情報窃取）のための基盤を拡大する
    - 攻撃終了の際には痕跡も消していく
  - 「速攻型」：重要情報窃取に向けた，最低限の情報を入手する
    - 潜入してから攻撃が終了するまでの期間が数時間～1日程度
    - 潜入後の基盤拡大，痕跡消去は行わない

RAT感染後：内部侵入・調査，感染拡大，目的達成

- 内部ネットワークの調査
  - 標的組織の内部ネットワークシステムを把握
  - 基盤構築時にインストールした攻撃ツール等を利用
- 端末間での侵害拡大
  - 他端末のアクセス権限を入手，他端末へ侵害
  - パスワードの窃取（IE PassViewなど）
  - pwdump7, Gsecdump （ハッシュ値入手）
  - Pshtoolkit, Metasploit PSEXEC module（偽装アクセス）
- サーバへの侵入，機密情報の摂取
  - ユーザ端末からサーバへのリモート操作
  - PsToolsなど

内部侵入・調査活動

内部侵入・調査概観

- 標的組織の内部ネットワークシステムを把握
- 内部侵入・調査の流れ
  - **初期調査**
    - 感染端末に関する情報収集
  - **探索活動**
    - ネットワーク内の端末やリモート端末に保存されている情報を調査
  - **感染拡大**
    - 他のマルウェアを感染させたり，他の端末への接続
  - **痕跡削除**
    - 攻撃者の使用したファイルやログの削除
- 攻撃者が使用するツール
  - 攻撃ツール以外に，**Windowsコマンド**や**正規のツール**も使用
    - これらのコマンドやツールはウイルス対策ソフトでは検知されないため発見が困難

初期調査で実行されるコマンド

頻度	コマンド	機能
1	tasklist	実行中のタスクを表示
2	ver	OSの種類やバージョン，ビルド番号を表示
3	ipconfig	IPネットワーク設定の表示
4	net time	時刻同期
5	systeminfo	システム情報の表示
6	netstat	ネットワーク接続状態の表示
7	whoami	ログインアしているカウントの情報を表示
8	nbtstat	NetBIOS情報の表示
9	net start	サービスの表示，開始
10	set	環境変数の設定，表示，削除
11	qprocess	実行中のプロセスを表示
12	nslookup	DNSサーバ情報の表示

出展：攻撃者の行動を追跡せよ – JPCERT コーディネーションセンター
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

初期調査における傾向

- どのような端末が感染したのかを調査
  - tasklistやver，ipconfig，systeminfo等のコマンドを使用し，ネットワーク情報やプロセス情報，OS情報等を収集
- 侵入した端末がマルウエア解析のためのおとり環境でないかなどを確認
  - 解析環境だった場合，攻撃者はすぐにログアウトする

探索活動で実行されるコマンド

頻度	コマンド	機能
1	dir	ファイルの一覧表示
2	ping	IPパケットの到達性確認
3	net view	接続可能なネットワーク上の端末を一覧表示
4	type	ファイルの内容を表示
5	net use	リソースへのアクセス
6	echo	標準出力を画面に表示
7	net user	ローカル及びドメインのアカウント管理
8	net group	特定のドメイン名のグループに所属するユーザー一覧取得
9	net localgroup	ローカルのグループに所属するユーザー一覧取得
10	dsquery	ADに含まれるアカウントの検索
11	net config	Server等のサービスの構成情報を表示
12	csvde	ADに含まれるアカウント情報取得

出展：攻撃者の行動を追跡せよ – JPCERT コーディネーションセンター
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

探索活動における傾向

- 感染端末に保存されている情報の調査
  - ファイルを探索するためにdir及びtypeを使用
    - dirコマンドに適切な引数を指定することで，感染端末内のすべてのドキュメントファイルの一覧を収集可能
  - ネットワークの探索にはnetコマンドを使用
  - Active Directoryを使用している環境の場合，dsqueryやcsvdeを使用
    - これらのコマンドは，Windows Serverに搭載されているコマンドで，本来はクライアントOSには存在しないが，攻撃者はこれらのコマンドを外部からダウンロードしインストールした上で実行する

感染拡大で実行されるコマンド

頻度	コマンド	機能
1	at	指定日時にプログラムを実行
2	move	ファイルを移動
3	schtasks	タスクスケジューラにタスクを登録
4	copy	ファイルをコピー
5	ren	ファイル名の変更
6	reg	レジストリの操作
7	wmic	システムのインベントリ情報の取得
8	powershell	PowerShellの実行
9	md	ディレクトリの作成
10	runas	別のユーザ権限でプログラムを実行
11	sc	サービス状態の表示，制御
12	netsh	ネットワークインターフェースの設定

出展：攻撃者の行動を追跡せよ – JPCERT コーディネーションセンター
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

感染拡大における傾向

- リモート端末上でマルウエアを実行
  - atやschtasks，wmicを利用
  - atやschtasksコマンドでは，以下のように接続可能な端末に対してファイルを実行するタスクを登録し，リモート端末上でコマンドを実行可能

```
> at ¥¥[リモートホスト名 or IPアドレス] 12:00 cmd /c "C:¥windows¥temp¥mal.exe"
```

```
> schtasks /create /tn [Task Name] /tr C:¥1.bat /sc onstart /ru System /s [IP Address]
```

  - wmicコマンドでは，以下のように引数を指定することで，リモート端末上のコマンドを実行可能

```
> wmic /node:[IPアドレス] /user:"[ユーザ名]" /password:"[パスワード]" process call create
"cmd /c c:¥Windows¥System32¥net.exe user"
```

出展：攻撃者の行動を追跡せよ – JPCERT コーディネーションセンター
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

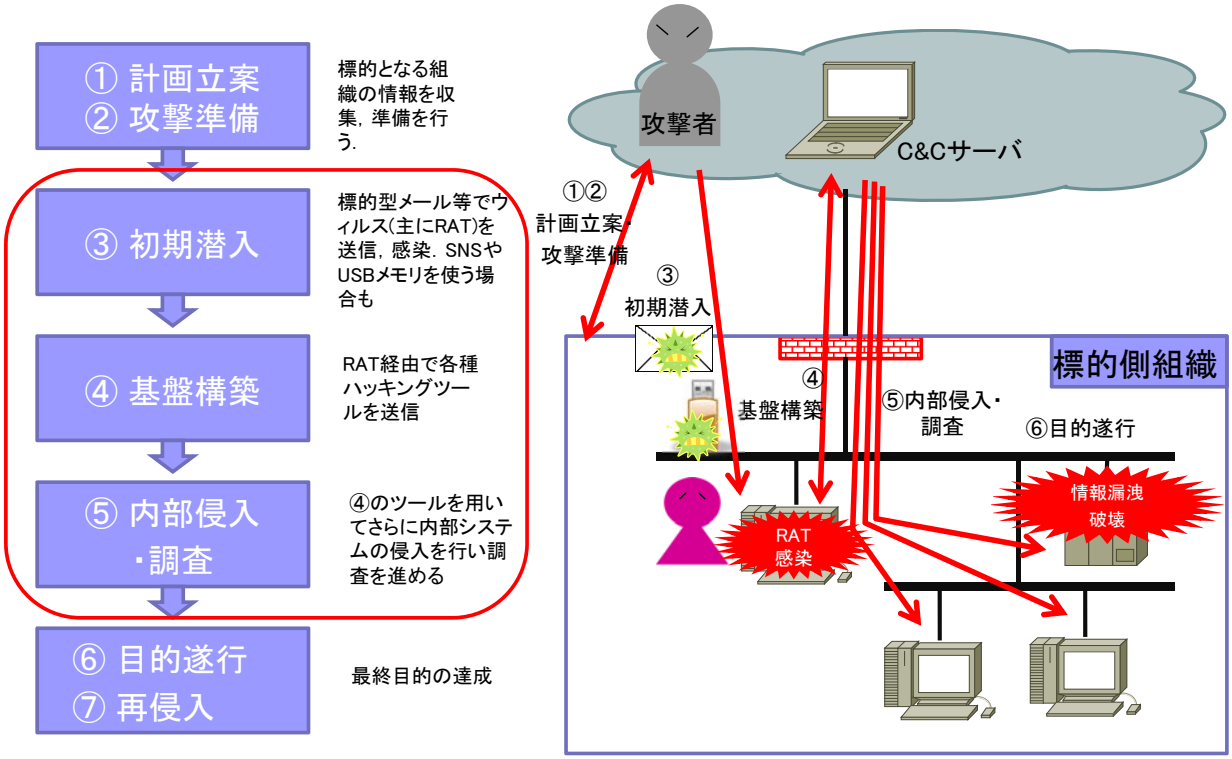
痕跡削除で実行されるコマンド

頻度	コマンド	機能
1	del	ファイルの削除
2	taskkill	タスクやプロセスの終了
3	klist	Kerberosチケットの表示，削除
4	wevtutil	イベントログの削除
5	rd	ディレクトリの削除

出展：攻撃者の行動を追跡せよ – JPCERT コーディネーションセンター
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

実習概要

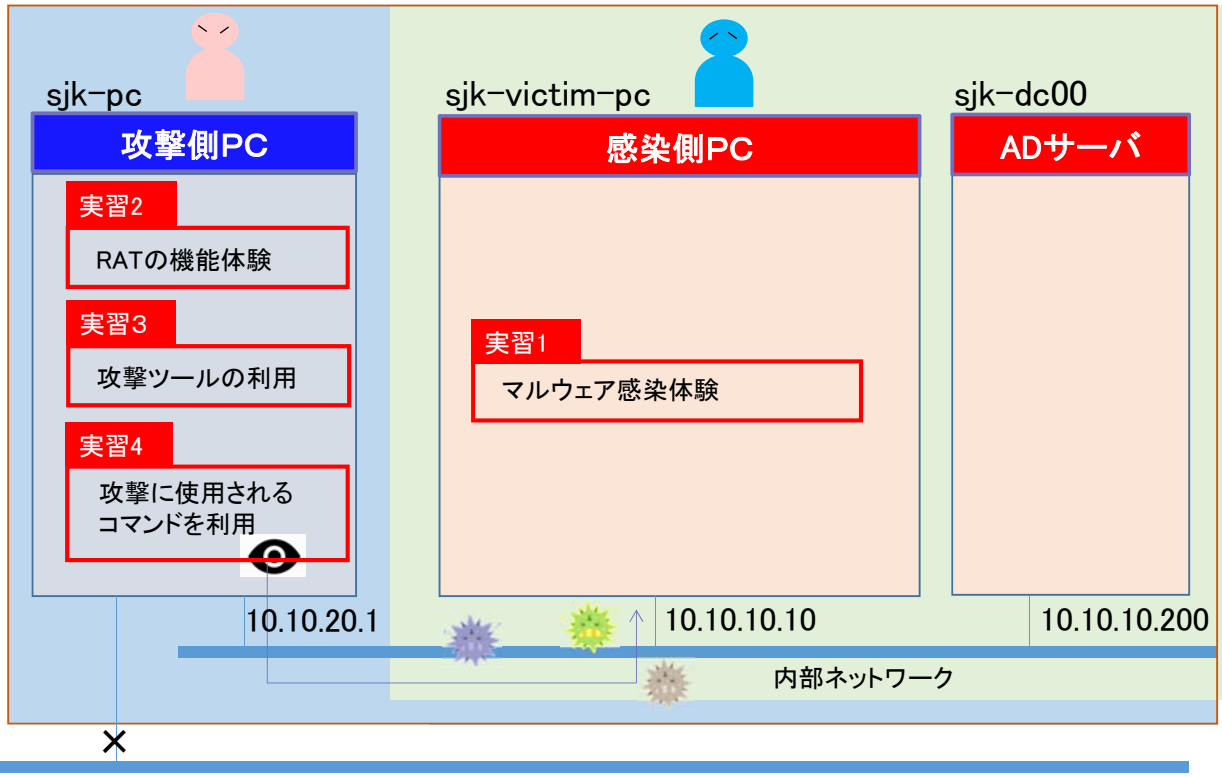
実習範囲



実習概要

- 標的型攻撃メールに添付されたファイルを実行してみる
  - マルウェア感染体験（実習1）
- RATに感染すると何が起こるのか攻撃者の立場になって体験し，どのような情報が窃取されるかを確認する
  - RATの機能体験（実習2）
  - 攻撃ツールの利用（実習3）
  - 攻撃に使用されるコマンドを利用（実習4）

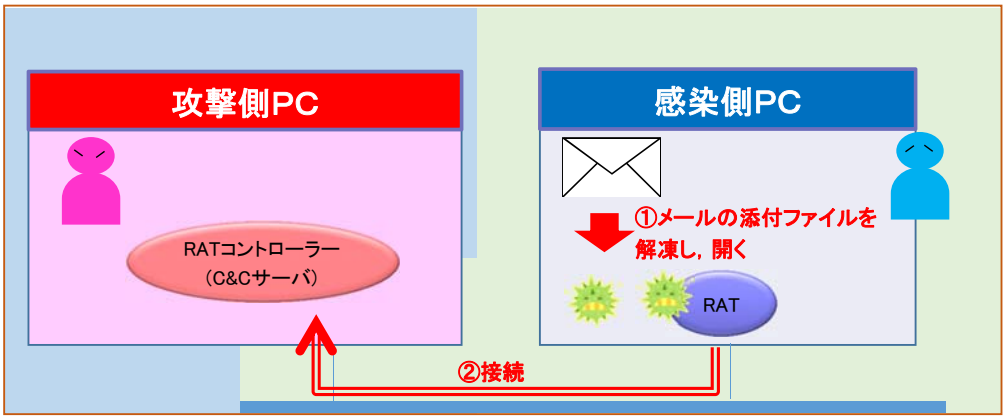
実習概要



実習1
マルウェア感染体験

マルウェア感染

- 感染側PCで，添付ファイル（受領書.pdf）を開く
- その結果，PCはマルウェアに感染
- 感染側PCから，攻撃側PCのC&Cサーバに接続



メールからの潜入

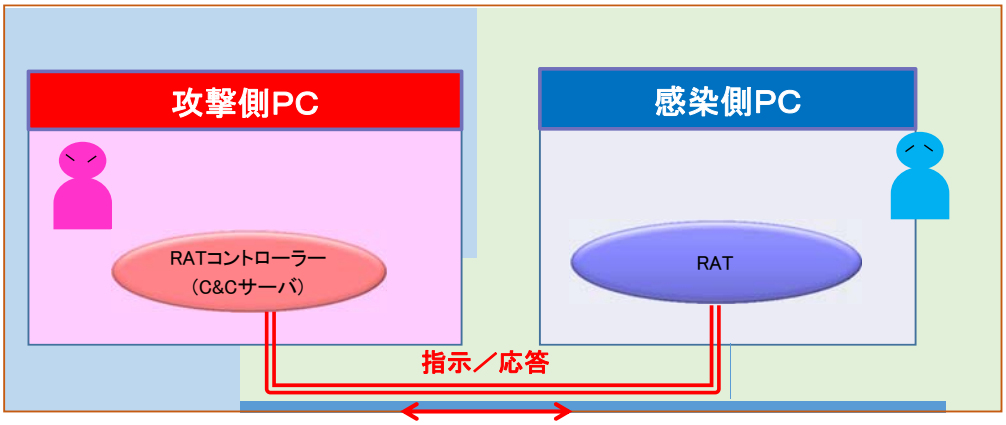
- 例：以下のメールを受信した

送信元	私立大学情報教育協会 〈contact@juce.org〉
宛先	私情協大学　教員A
表題	受領書の送付
本文	私情協大学　ご担当者様 お世話になっております． 郵送にてお送り頂きました調査報告書を受領致しました． つきましては，受領書の電子データをお送りします． 原本は郵送にてお送りさせて頂きます． どうぞよろしくお願い致します． -- 私立大学情報教育協会 私立　太郎
添付ファイル	受領書.pdf

実習2
RATの機能体験

攻撃側PCからの操作

- 感染側PCから攻撃側PCのC&Cサーバに接続されると，遠隔での以下のような操作が可能となる
  - 各種コマンドの実行
  - キー入力情報の取得
  - 画面閲覧，操作



実習3
攻撃ツールの利用

攻撃側PCから攻撃ツールの実行

- 今回は以下のツールを前もって準備し感染側PCにインストールを行っている
  - ネットワーク調査ツール(nmap)
    - 標的組織の内部ネットワークシステムを把握
    - 指定したホストやネットワークに対してポートスキャンをするためのツール
    - コマンド（nmap）と様々なオプションを組み合わせることで，内部ネットワークに接続されているコンピューターの情報を調査することが可能
    - OSを推定することも可能
    - オプション例
      - -A：OSとサーバーアプリケーションのバージョンを調査
      - -O：OSのバージョンを調査
      - -P0：pingスキャンを行わない
      - -F：限定したポートのみ調べる

実習4
攻撃に使用されるコマンドを利用

攻撃側PCから各種コマンドの実行

- 内部侵入・調査の流れに従い各種コマンドを実行し，どのようなことが行えるか確認をする
  - **初期調査**
    - 感染端末に関する情報収集
  - **探索活動**
    - ネットワーク内の端末やリモート端末に保存されている情報を調査
  - **感染拡大**
    - 他のマルウェアを感染させたり，他の端末への接続
  - **痕跡削除**
    - 攻撃者の使用したファイルやログの削除

対策とまとめ

対策：電子メールの信憑性確認

- 受信したメールについて以下の点について確認する
  - 知っている人からのメールか？
  - いつもと同じメールアドレスか？
    - gmailなどのフリーメールを利用していることが多い
    - Fromを偽装している可能性もあるため，怪しいと感じたらメールヘッダのSenderも確認してみる
  - 送信者と署名（シグネチャ）は同じか？
  - 文章が不自然ではないか？
  - 日本では一般的に使用しない漢字やフォントではないか？
  - URLは正しいものか？
    - あえて正式名称を一部に含むURLもあるため，怪しいと感じたらそのドメインについて検索してみる

対策：攻撃ツール等の実行痕跡の記録

- PCの監視を強化し，サイバー攻撃を受けた時の痕跡調査に備えることが必要
  - 初期設定状態では調査に必要な情報が揃わない
- 追加のログ設定が必要となる

まとめ

- メールの信憑性調査（すべてのメールに対して）
  - 通報メール自体が標的型サイバー攻撃の場合がある
  - メール本文，ヘッダー情報から信頼できるものかを判断する
  - 添付ファイルがある場合は更に慎重に調査する
- 標的型サイバー攻撃の手法
  - 初期潜入
    - メールの添付ファイルやURLリンクを使ってRATを送信，感染させる
  - 基盤構築
    - RAT経由で内部情報を窃取するためのツールを送り込む
  - 内部侵入・調査
    - 内部ネットワークシステムの調査・把握
    - 調査には攻撃ツールだけでなくWindowsコマンド等の正規のツールも利用される
  - 感染拡大・情報摂取