NanoCoreHunter:
NanoCore C&C サーバの追跡と
180日間の RAT オペレータの行動監視

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティ研究室

松本 隆志

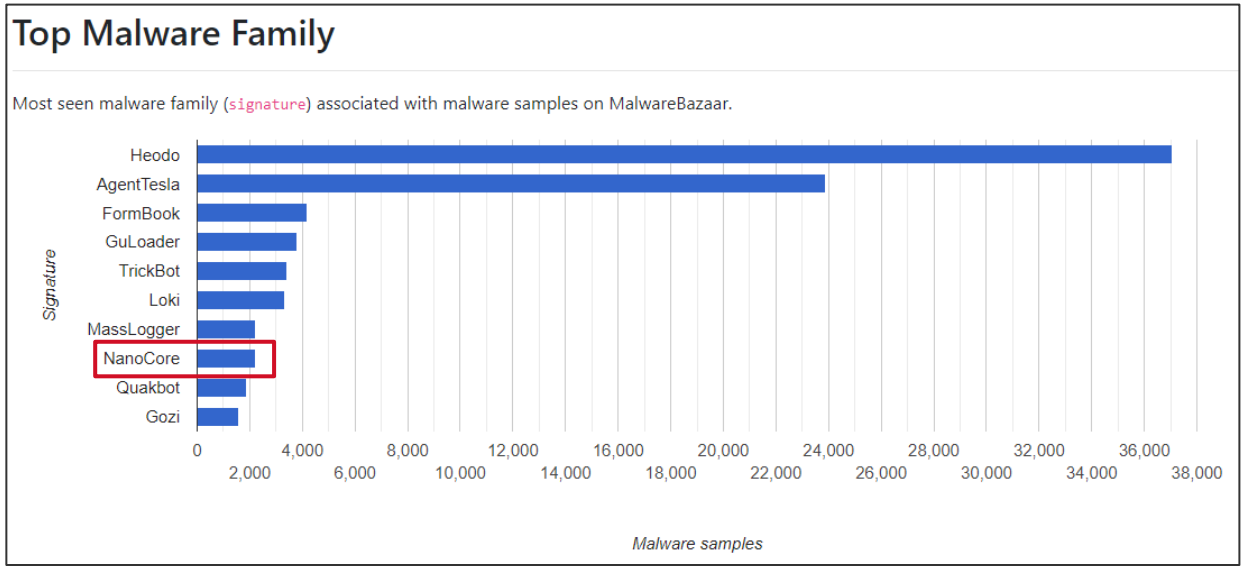
発表内容

- **NanoCore C2 サーバの検知手法**
  - 新たに発見した NanoCore C2 サーバの検知手法について紹介する
- **NanoCore C2 サーバの長期観測**
  - C2サーバの IP アドレスはアメリカとヨーロッパに偏っている
  - 観測から得られた C2 情報を各国の CERT に提供している
- **NanoCore オペレータの誘引実験**
  - 多くのオペレータは，メールアカウントやパスワードを窃取する
  - 一部，NanoCore 以外の複数の RAT に感染させるケースを確認した

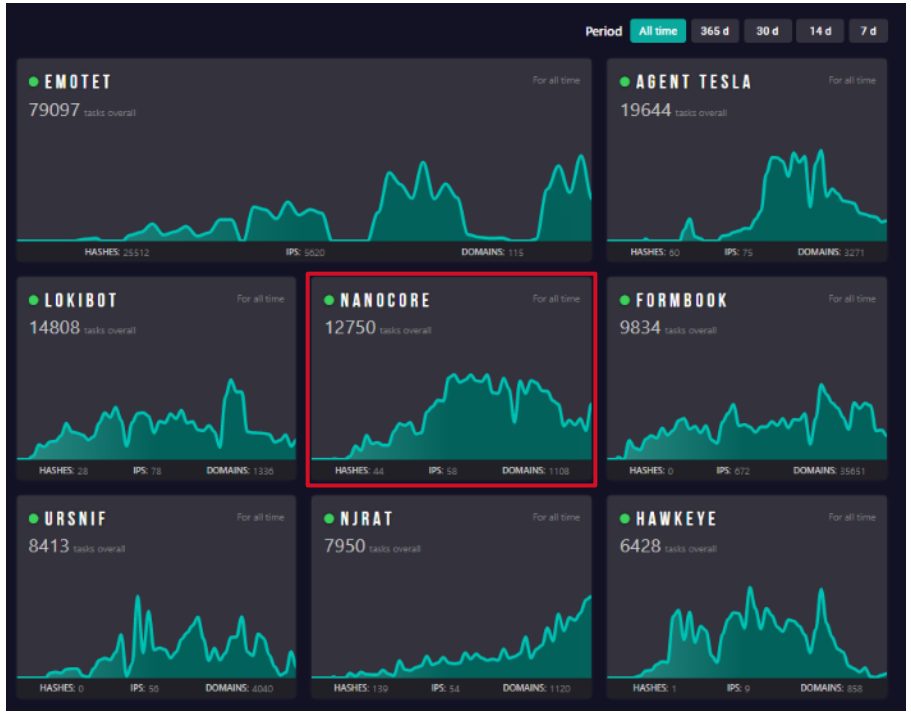
NanoCore RAT について

NanoCore の概要

- 2013年に初めて登場した Remote Access Trojan（RAT）である
- 2021年現在も利用されている
  - ANY.RUN や MalwareBazaar の統計でも常にトップ10に入っている
  - 我々の組織にも定期的に NanoCore が添付された SPAM メールが届いている



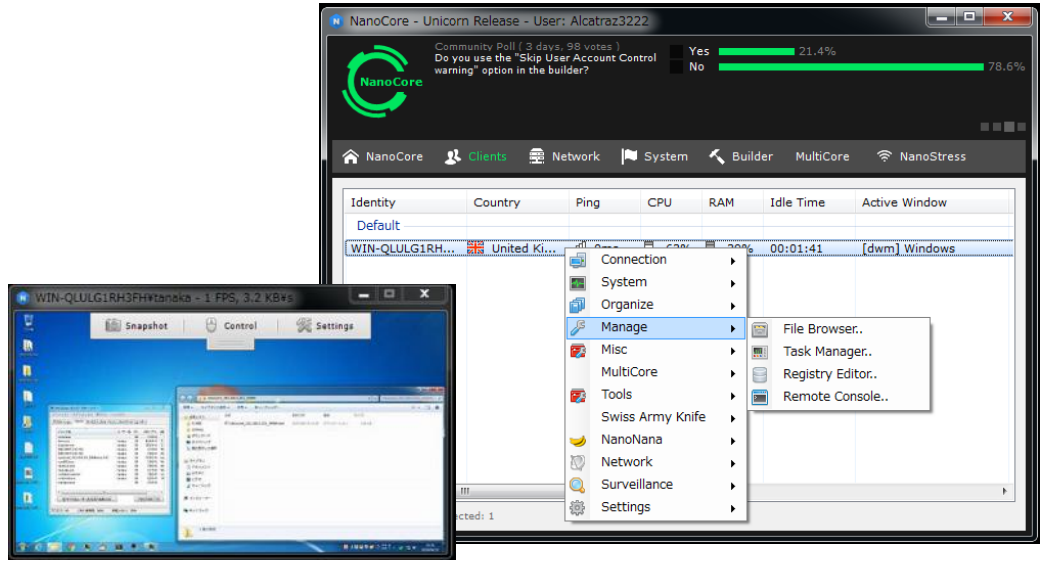
Top 10 Malware Family（MalwareBazaar by abuse.ch）



Malware Trends Tracker（ANY.RUN）

NanoCore の概要

- NanoCore の機能
  - 画面共有
  - データの窃取（ファイル，パスワードなど）
  - キーロガー
  - マイクや Webカメラへのアクセス など



リークされた NanoCore v1.2.2.0

- NanoCore v1.2.2.0
  - v1.2.2.0 が最新バージョンであり，
    このバージョンが広く利用されている
  - ダークウェブ等にリークされており，簡単に入手可能
  - 実際に入手して解析を行ったところ，設定に不備があることが判明した

非公開スライド

非公開スライド

非公開スライド

NanoCore C2 サーバの追跡

非公開スライド

NanoCore C2 サーバ検知用の NSE スクリプト

- 作成した NSE スクリプト
  - NanoCore C2 サーバのスキャン手順
    1. NanoCore クライアントの初回通信を模倣したペイロードを送信する
    2. 返ってきたデータをDESで復号する
    3. 同じキーで復号できた場合に NanoCore C2 サーバと判定する
  - **送信するペイロードの内容**（以下のデータをNanoCoreと同じ手順で暗号化する）
    - GUID（PCの識別に使用される，毎回ランダムな値にする必要がある）
    - Identity (ホスト名¥ユーザ名)
    - NanoCore グループ名（デフォルト値: Default）
    - NanoCore バージョン（デフォルト値: 1.2.2.0）

DESで暗号化する

```
00000000  38 00 00 00 17 f5 4b 2c  c3 65 ca 9f eb bc fd 67   8.....K, .e.....g
00000010  ad 6d 0e c4 33 7d b6 40  17 17 97 a1 d9 7c 3c b3   .m..3}.@ .....|<.
00000020  04 ea d0 16 ce 72 94 94  71 8e 87 45 32 0a 22 49   .....r.. q..E2."I
00000030  81 66 f3 8b c2 9b 2b 97  84 c8 c7 52               .f....+. ...R
```

```lua
function nanocore_payload(guid, identity, group, version)
    local des_key = "\x72\x20\x18\x78\x8c\x29\x48\x97"
    local des_iv = des_key

    local payload = "\x00\x00\x00\x00"
    .. "\x12" .. guid
    .. "\x0c" .. string.char(string.len(identity)) .. identity
    .. "\x0c" .. string.char(string.len(group)) .. group
    .. "\x0c" .. string.char(string.len(version)) .. version

    local enc_payload = des_encrypt(des_key, des_iv, payload)
    local payload_len = fromInt32(string.len(enc_payload))
    return payload_len .. enc_payload
end
```

nanocore.nse の一部

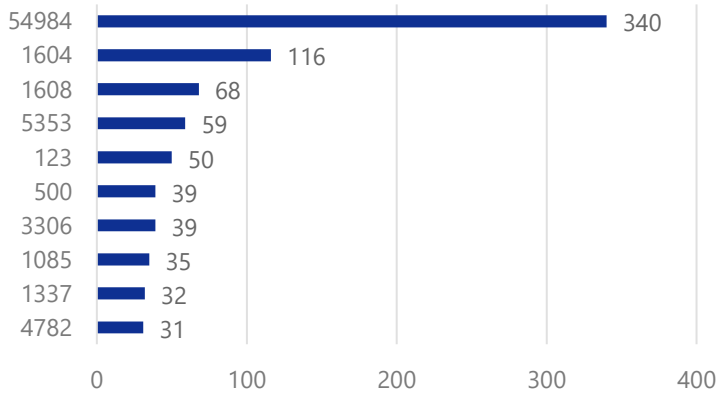
【一部非公開】

NanoCore C2 サーバの長期観測結果（1/5）

- 観測期間
  - 2020/05/14 ~ 2020/11/10

非公開

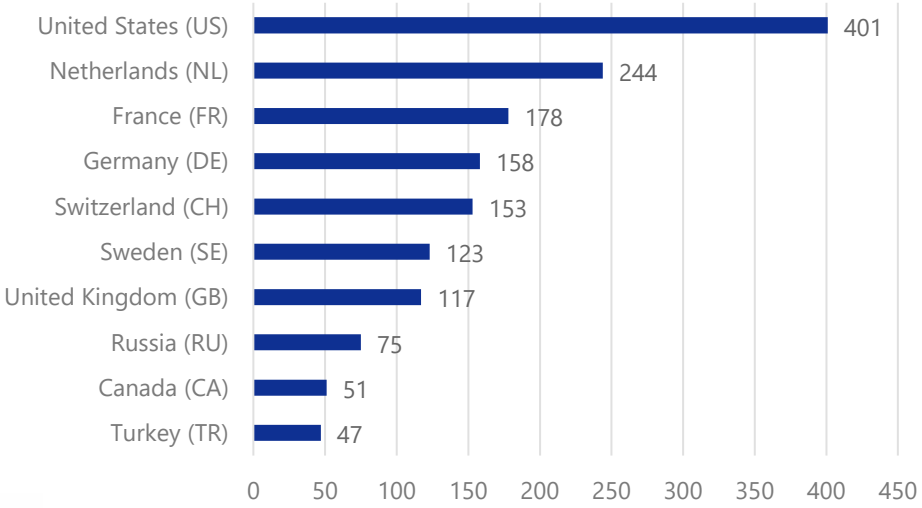
- 検知した NanoCore C2 サーバ数
  - ユニークなIPアドレス数: **2,075**
  - ポート別: **3,671**
- 使用されたポート番号
  - **54984/tcp**: NanoCoreのデフォルトポート
  - **1085/tcp**: リークされた NanoCore v1.2.2.0 が開けているポート
  - **1604/tcp**: DarkComet RAT のデフォルトポートと同様
    DarkComet RAT を使用していたオペレータが
    NanoCoreに移行した可能性がある？



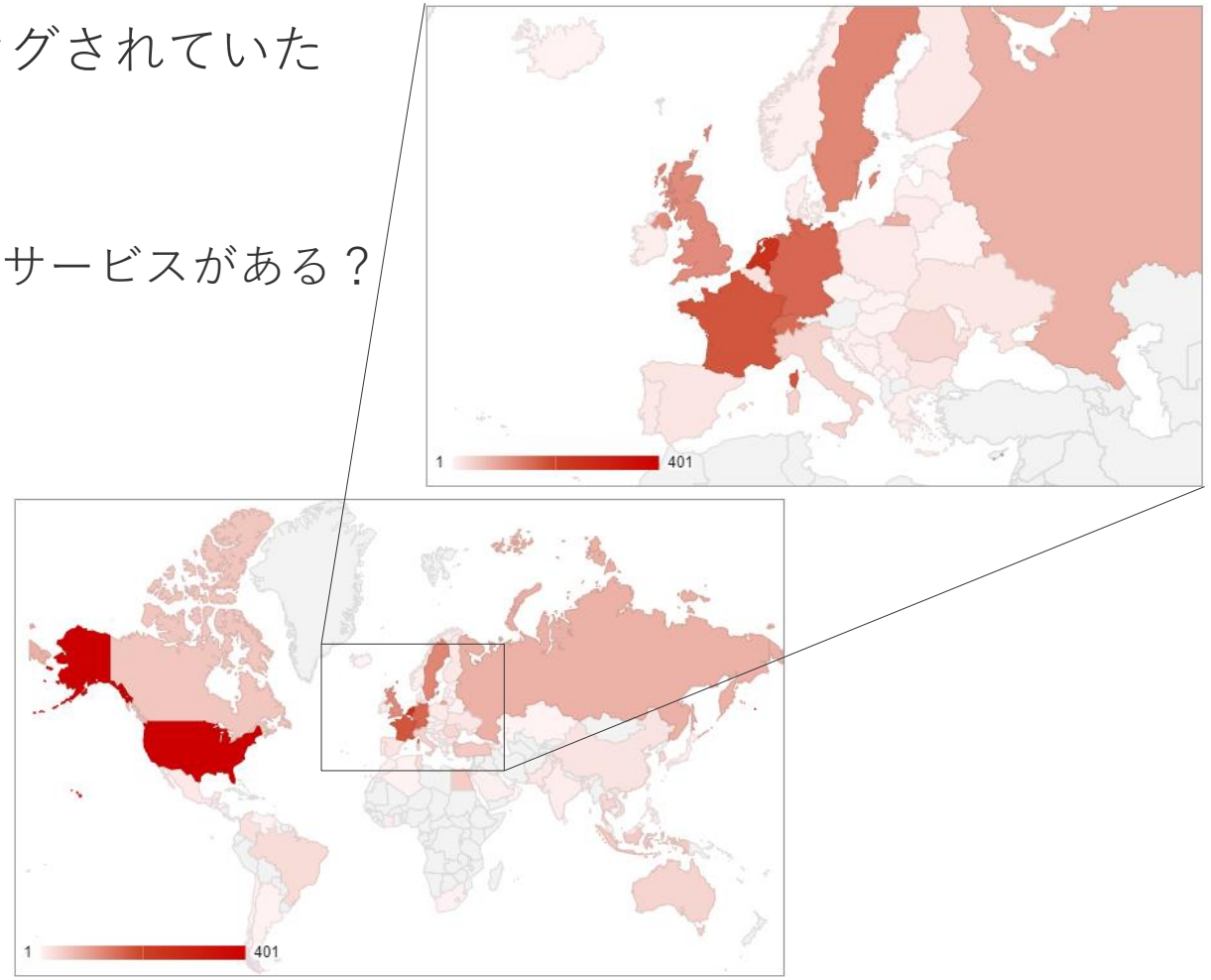
使用されてポート（上位10件）

NanoCore C2 サーバの長期観測結果（2/5）

- 国別
  - **85カ国**に NanoCore C2 サーバがホスティングされていた
  - 特に**アメリカ**と**ヨーロッパ**に偏っている
    - オペレータが活動している国？
    - オペレータに人気のある VPN やホスティングサービスがある？
    - これらの国が標的となっている？



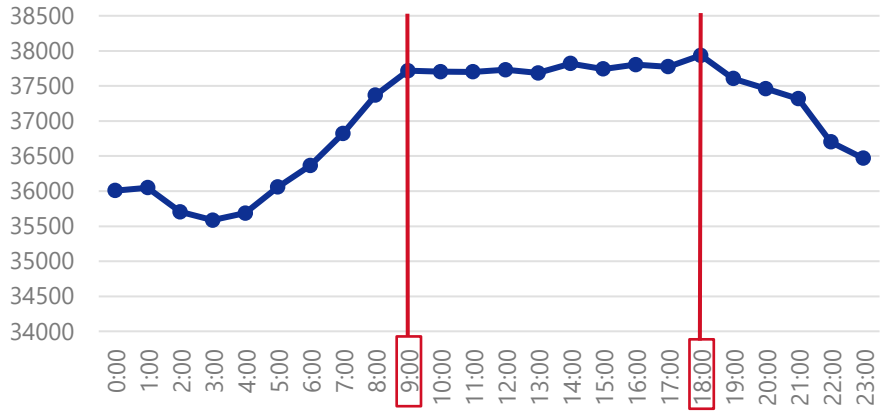
上位10カ国



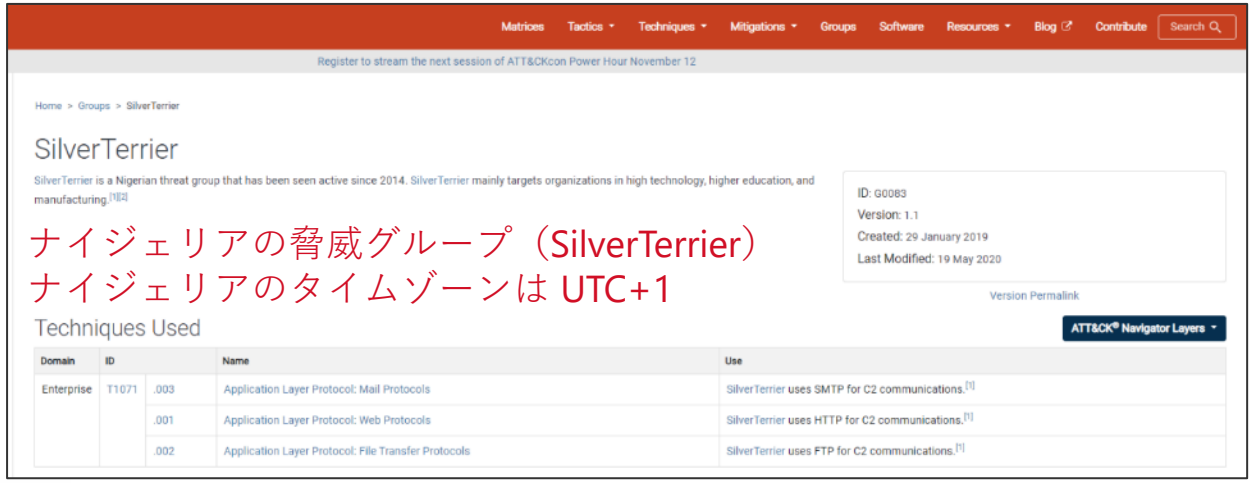
C2 サーバがホスティングされている国

NanoCore C2 サーバの長期観測結果（3/5）

- 時刻別
  - **9:00 ~ 18:00（UTC）**に稼働しているサーバが多い
    - 主要な RAT オペレータの活動時間？
      - この時間帯が日中である国が狙われている可能性が高い
    - ナイジェリアの脅威グループ（SilverTerrier）が関与している？
      - https://attack.mitre.org/groups/G0083/
      - https://unit42.paloaltonetworks.com/silverterrier-2019-update/



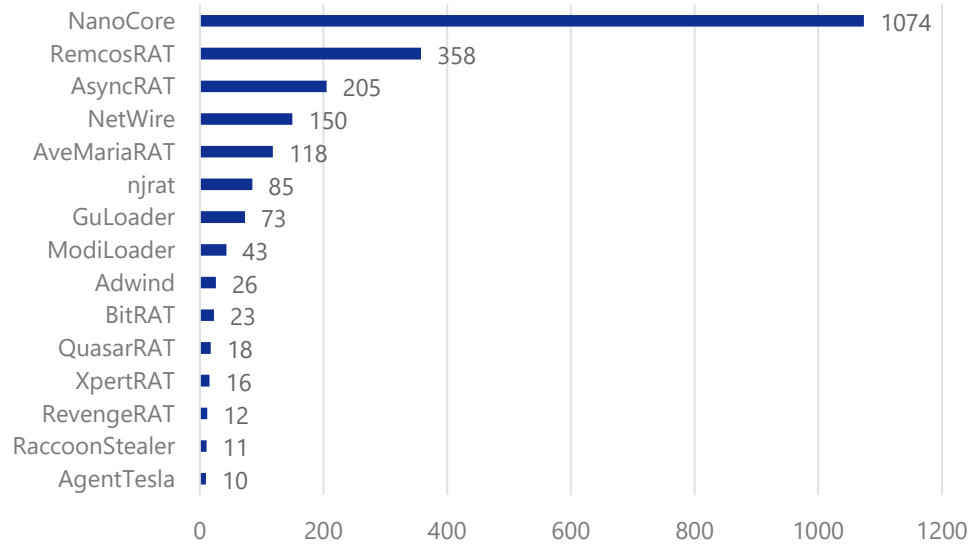
1時間毎のオープンポート数の合計



SilverTerrier, Group G0083 | MITRE ATT&CK

NanoCore C2 サーバの長期観測結果（4/5）

- VirusTotal に登録されていた C2 の IP アドレス
  - 未登録の IP アドレス数: 480
  - 登録済みの IP アドレス数: 1,812
  - IP アドレスに紐づくマルウェア
    - NanoCore 以外の RAT も使用されている
    - 複数の RAT を併用して使用している可能性がある
- CERT 連携
  - 毎月 JPCERT/CC に C2情報を提供している
  - JPCERT/CC 経由で各国の CERT に C2情報を提供している



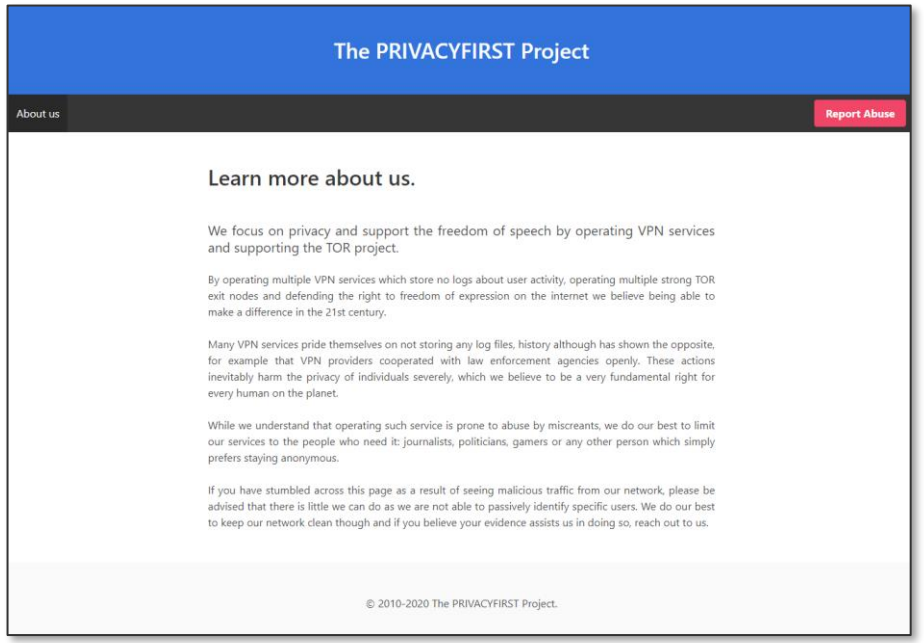
IPアドレスに紐づくマルウェア
（VirusTotal と MalwareBazaar）

- United States
- Netherlands
- Switzerland
- France
- Germany
- Sweden
- United Kingdom
- Russia
- Turkey
- Indonesia
- Canada
- Egypt
- Italy
- Romania
- South Korea
- Thailand
- Colombia

NanoCore C2 サーバの長期観測結果（5/5）

- CERT 連携の障害
  - non-logging VPN の利用
    - 約20%は，The PRIVACYFIRST Project に関連していた
    - オーナーに連絡したが役に立たなかったと報告を受けた（GovCERT.ch より）

- MISP を使った情報提供
  - 検知した NanoCore C2 サーバの IP アドレスとポートを毎日追加していく予定
  - CIRCL MISP Community 内で共有する



The PRIVACYFIRST Project（privacyfirst.sh）

```
organisation:   ORG-TPP6-RIPE
org-name:       The PRIVACYFIRST Project
descr:          www.privacyfirst.sh
```

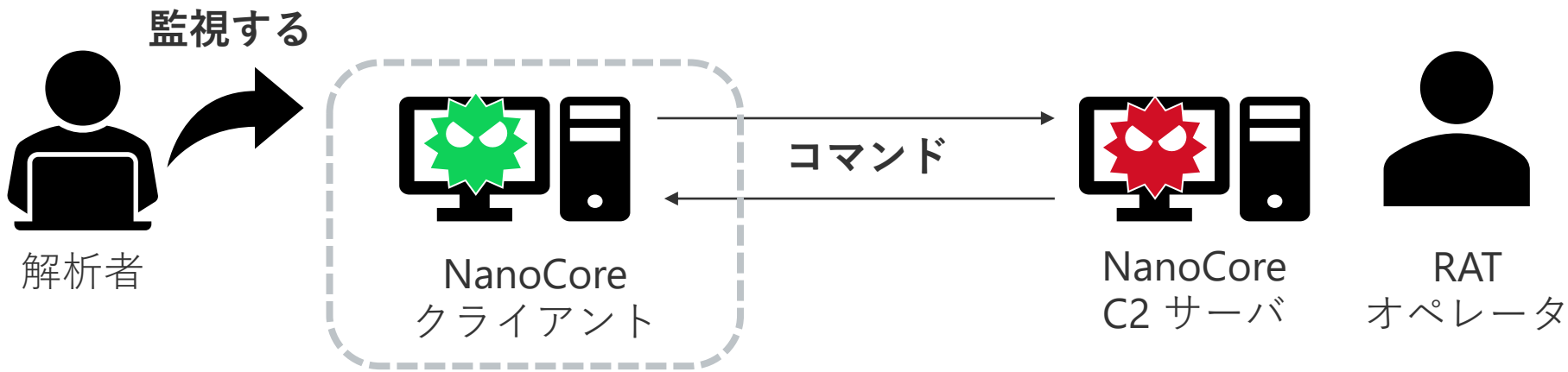
whois 結果の一部

NanoCore オペレータの誘引実験

NanoCore の利用目的を探る

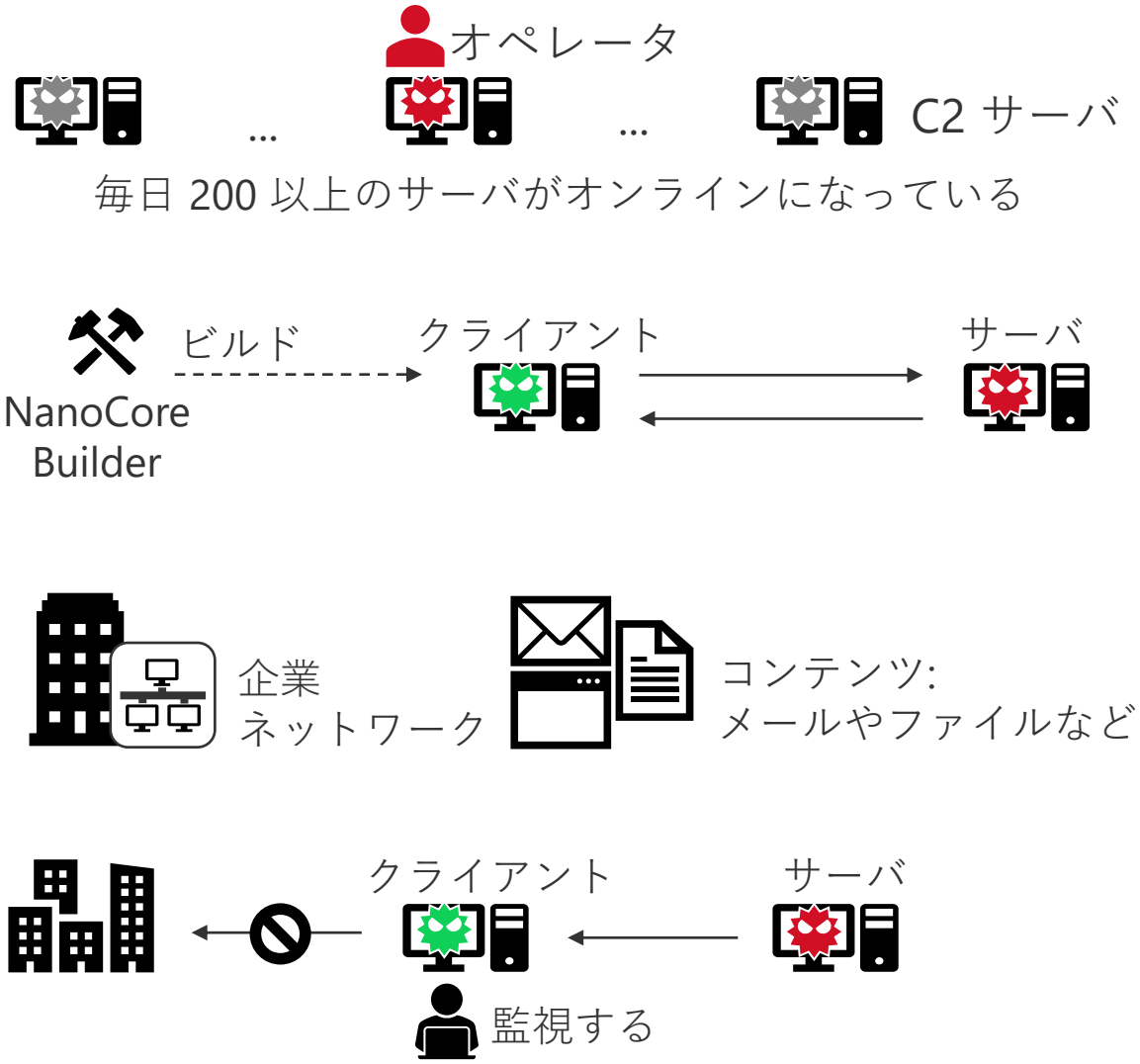
- NanoCore の利用目的は何なのか
  → 解析環境に RAT オペレータを誘引し，行動を観測することでその目的を明らかにする

- RAT オペレータの誘引実験
  - 検知した IP アドレスとポート番号を用いて，NanoCore C2 サーバに接続する
  - RAT オペレータの行動をリアルタイムで監視する

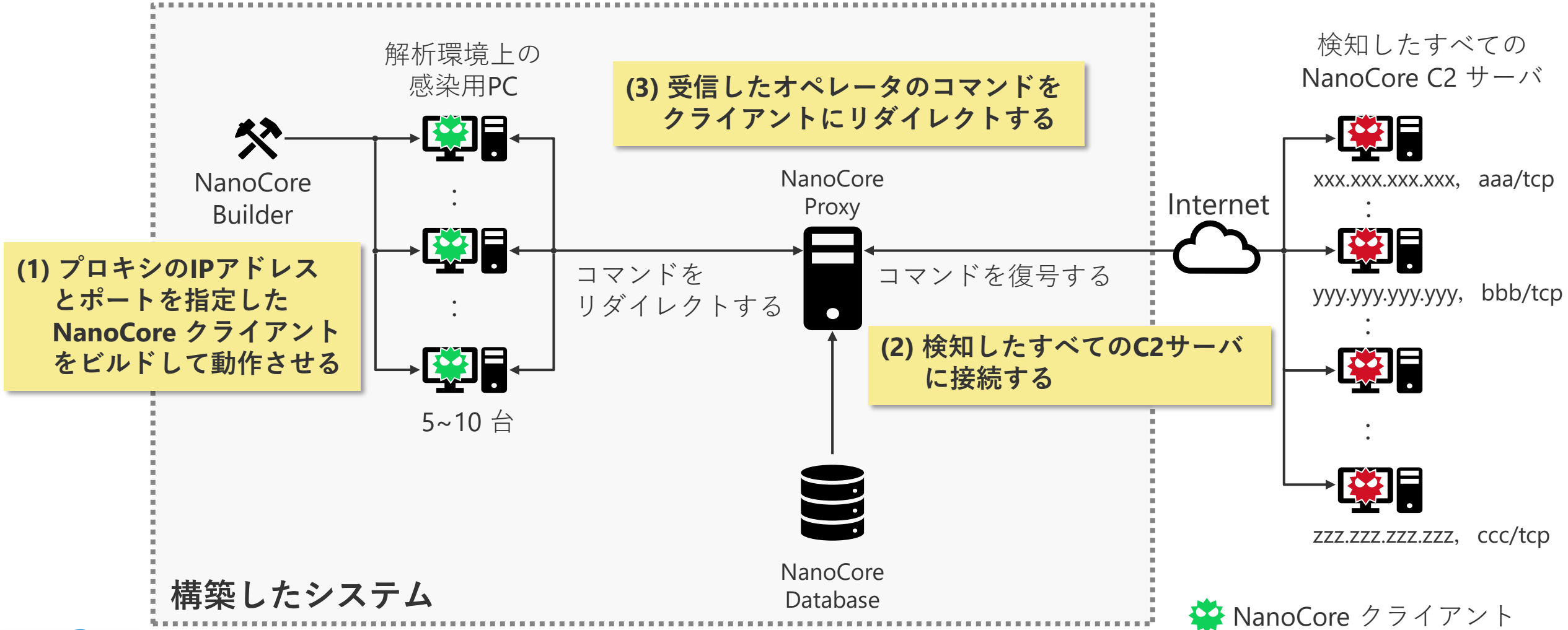


誘引実験を行う上で考慮すべきこと

- C2 サーバが稼働していたとしても，そこにオペレータがいるとは限らない
- C2 サーバ接続用のクライアントを用意する必要がある
- オペレータが興味を引くような環境を用意する
- 他組織への攻撃の踏み台になってはならない

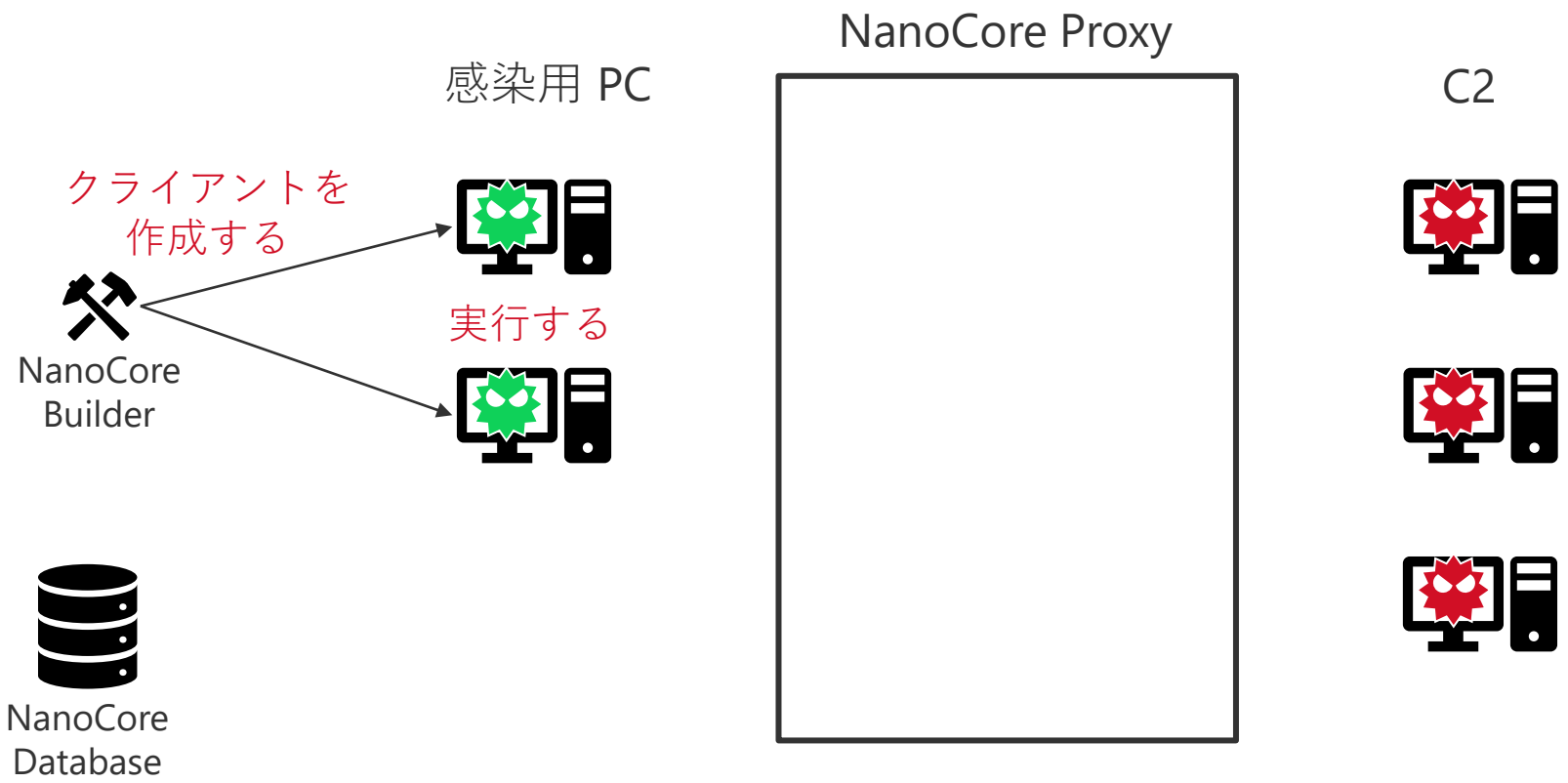


効率よくオペレータを誘引するための仕組み



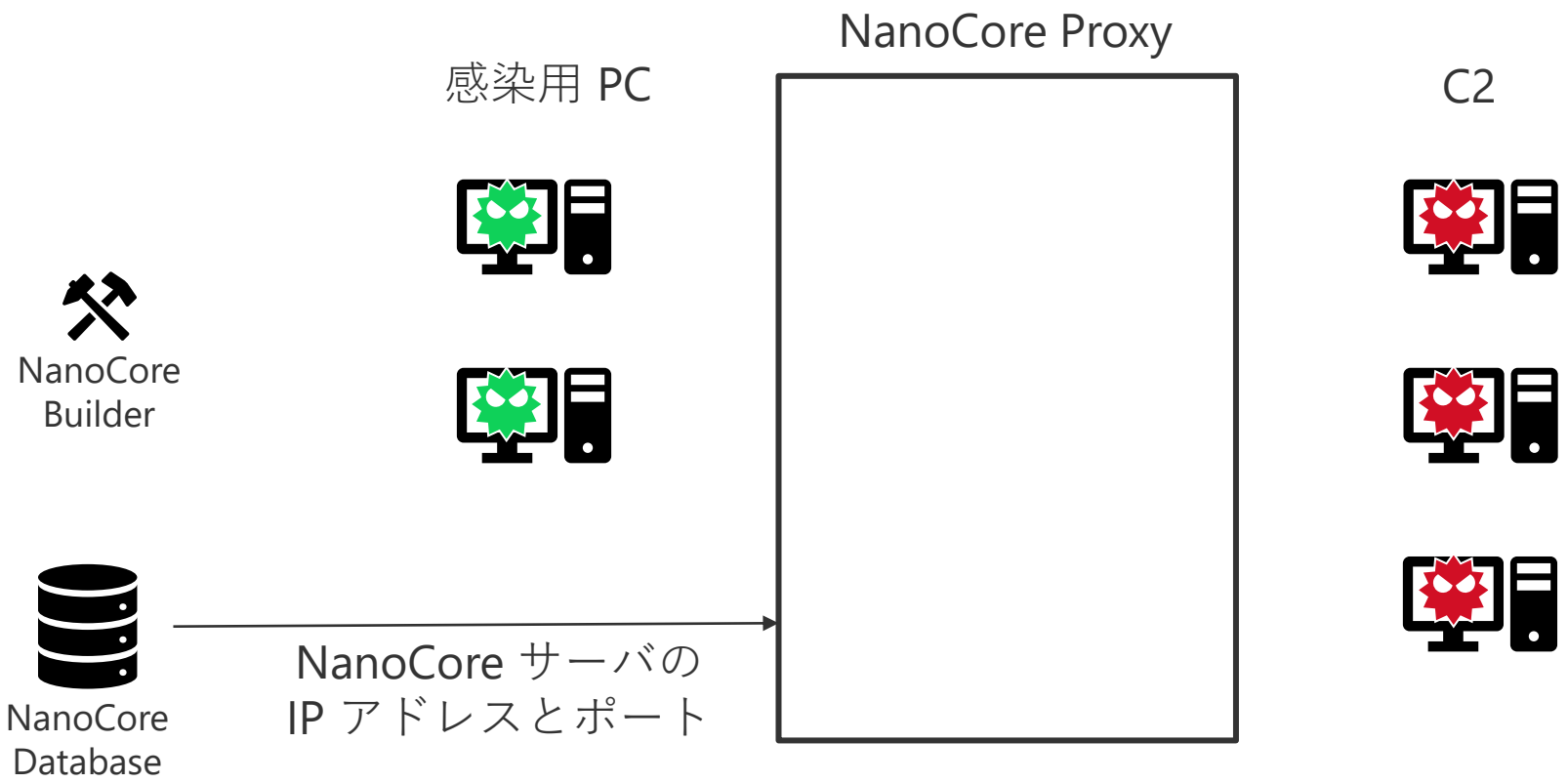
NanoCore Proxy の実行手順（1/8）

- プロキシに接続するように設定したクライアントを作成する
- 作成したクライアントを感染用 PC 上で動作させておく



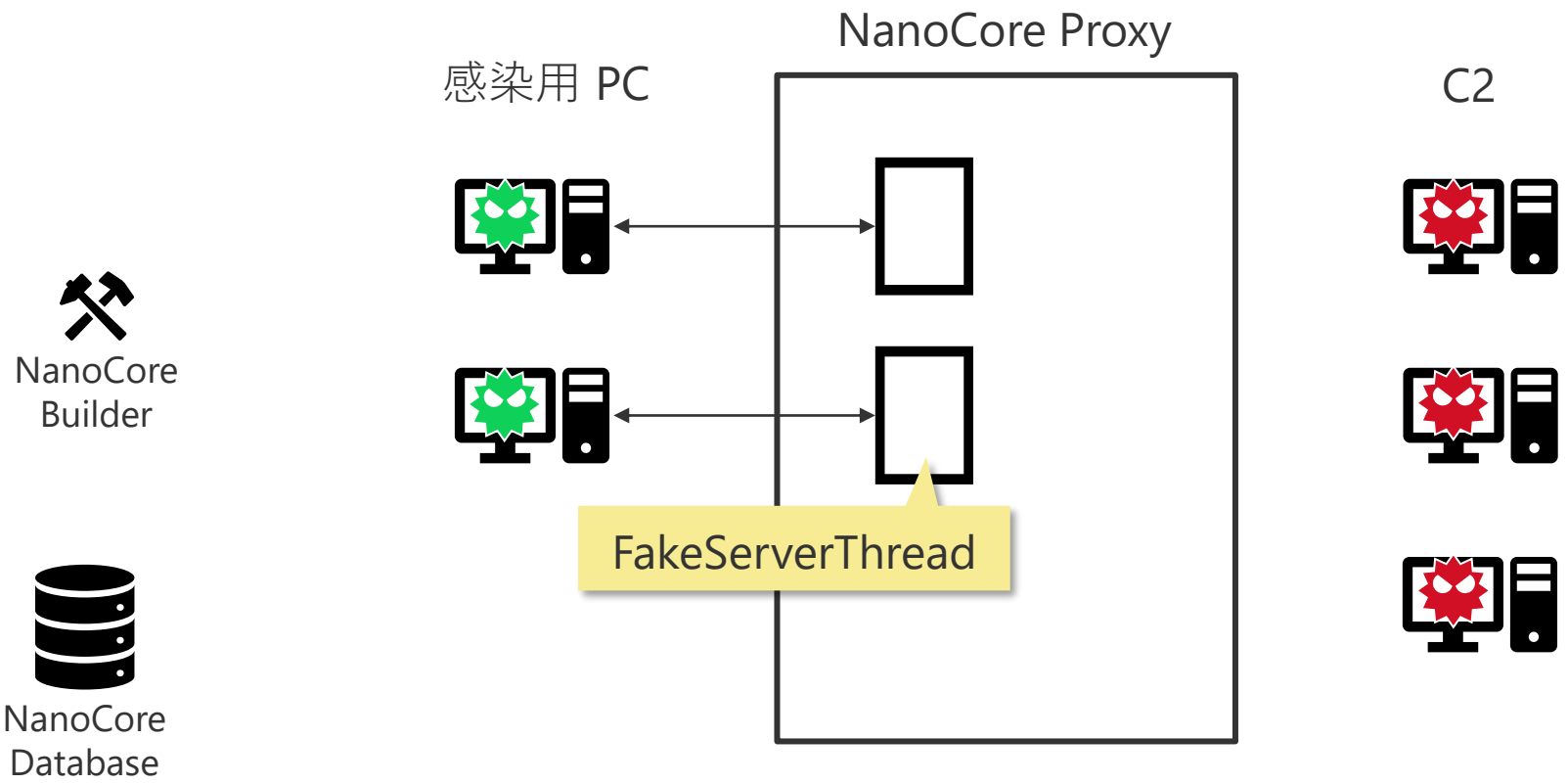
NanoCore Proxy の実行手順（2/8）

- 検知した NanoCore サーバリストを指定して，
  NanoCore Proxy を起動する



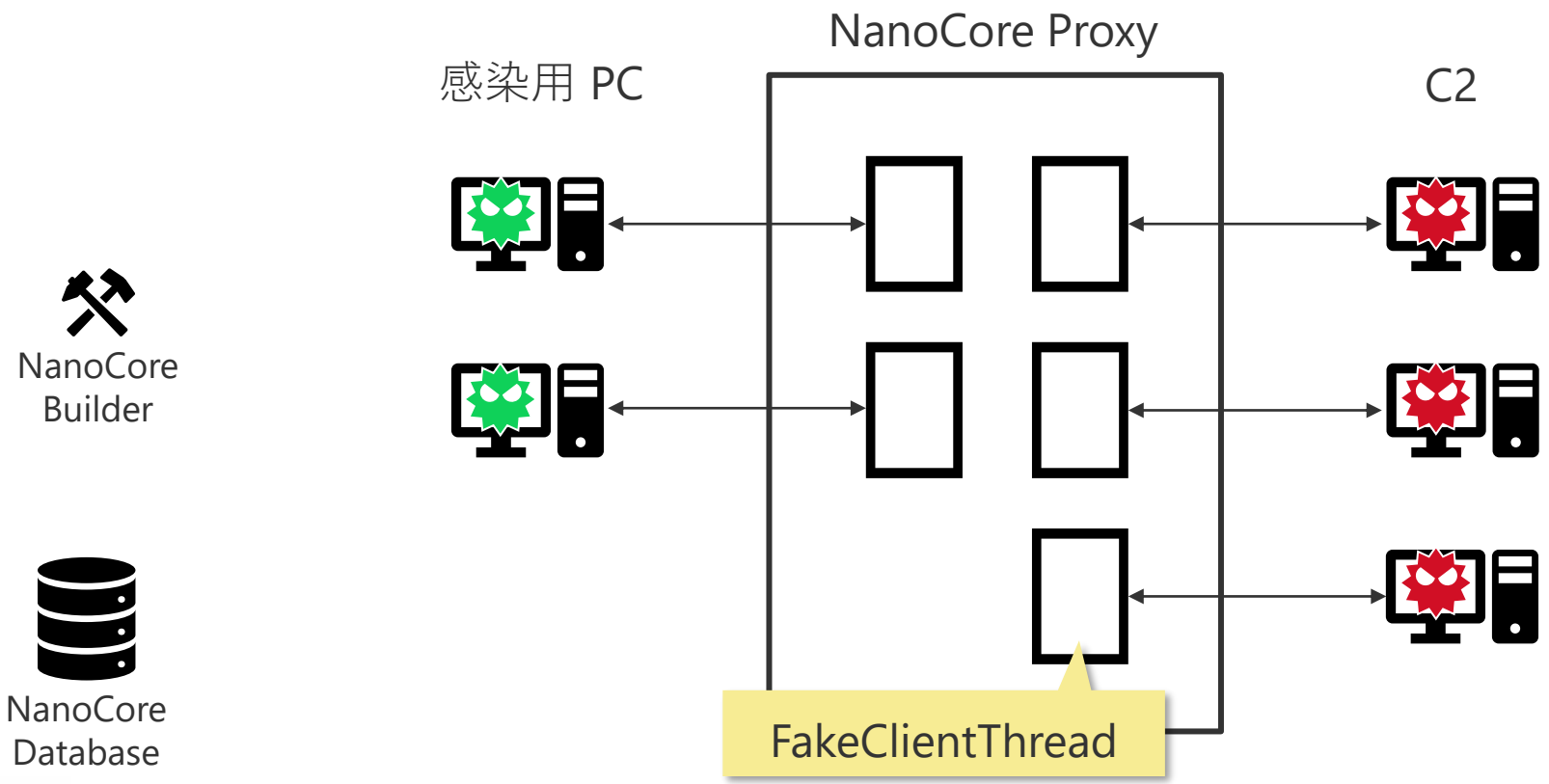
NanoCore Proxy の実行手順（3/8）

- FakeServerThread を起動し，
  NanoCore クライアント間の通信を確立させる



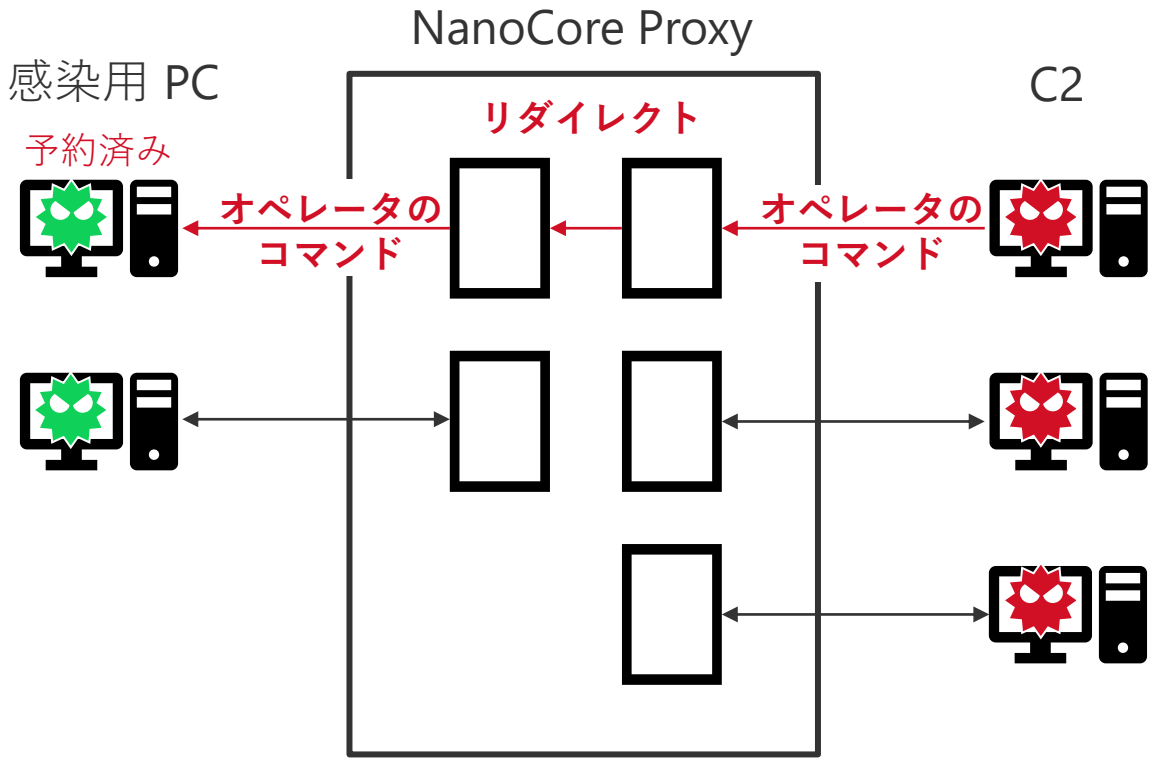
NanoCore Proxy の実行手順（4/8）

- FakeClientThread を起動し，C2 サーバ間の通信を確立させる
- C2 サーバとプロキシ間の通信は常に復号される



NanoCore Proxy の実行手順（5/8）

- コマンドを受信したら，感染用PCにリダイレクトされる
- 一度リダイレクトされた感染用PCは，予約済みにする



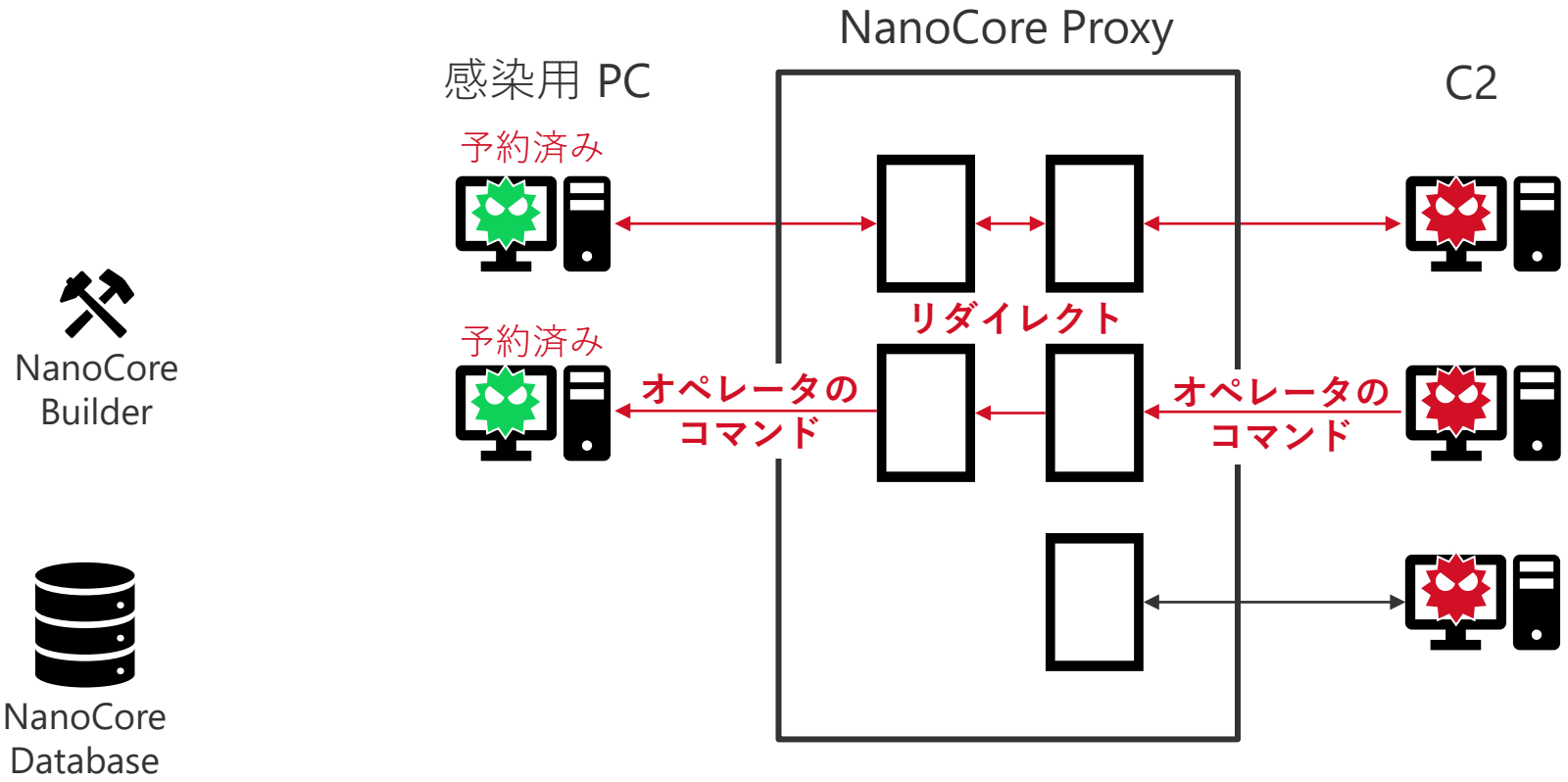
NanoCore
Builder

NanoCore
Database

備考: NanoCoreの初回通信と定常通信以外のデータをオペレータによるコマンドとして処理する

NanoCore Proxy の実行手順（6/8）

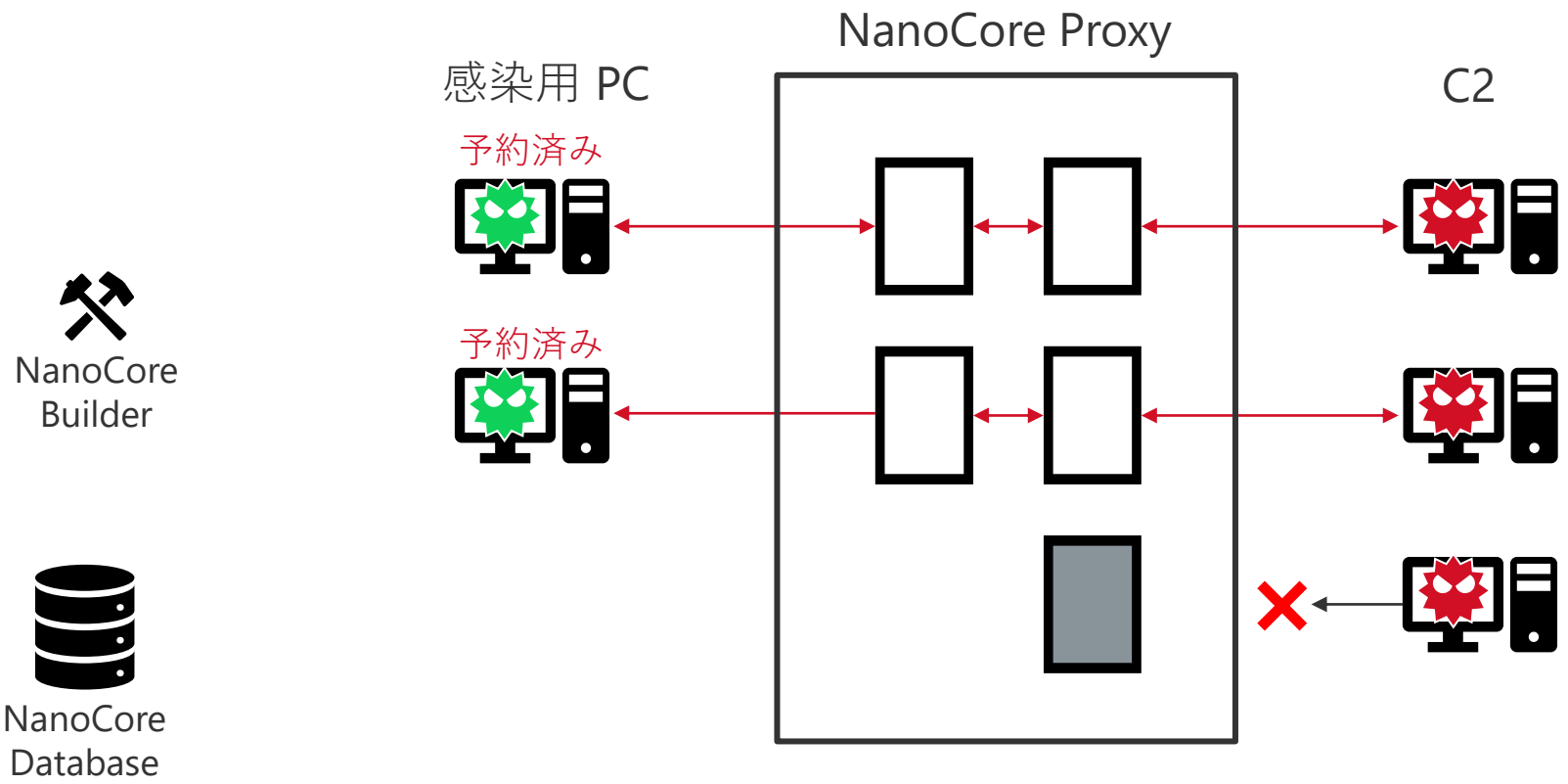
- コマンドを受信したら，感染用PCにリダイレクトされる
- 一度リダイレクトされた感染用PCは，予約済みにする



備考: NanoCoreの初回通信と定常通信以外のデータをオペレータによるコマンドとして処理する

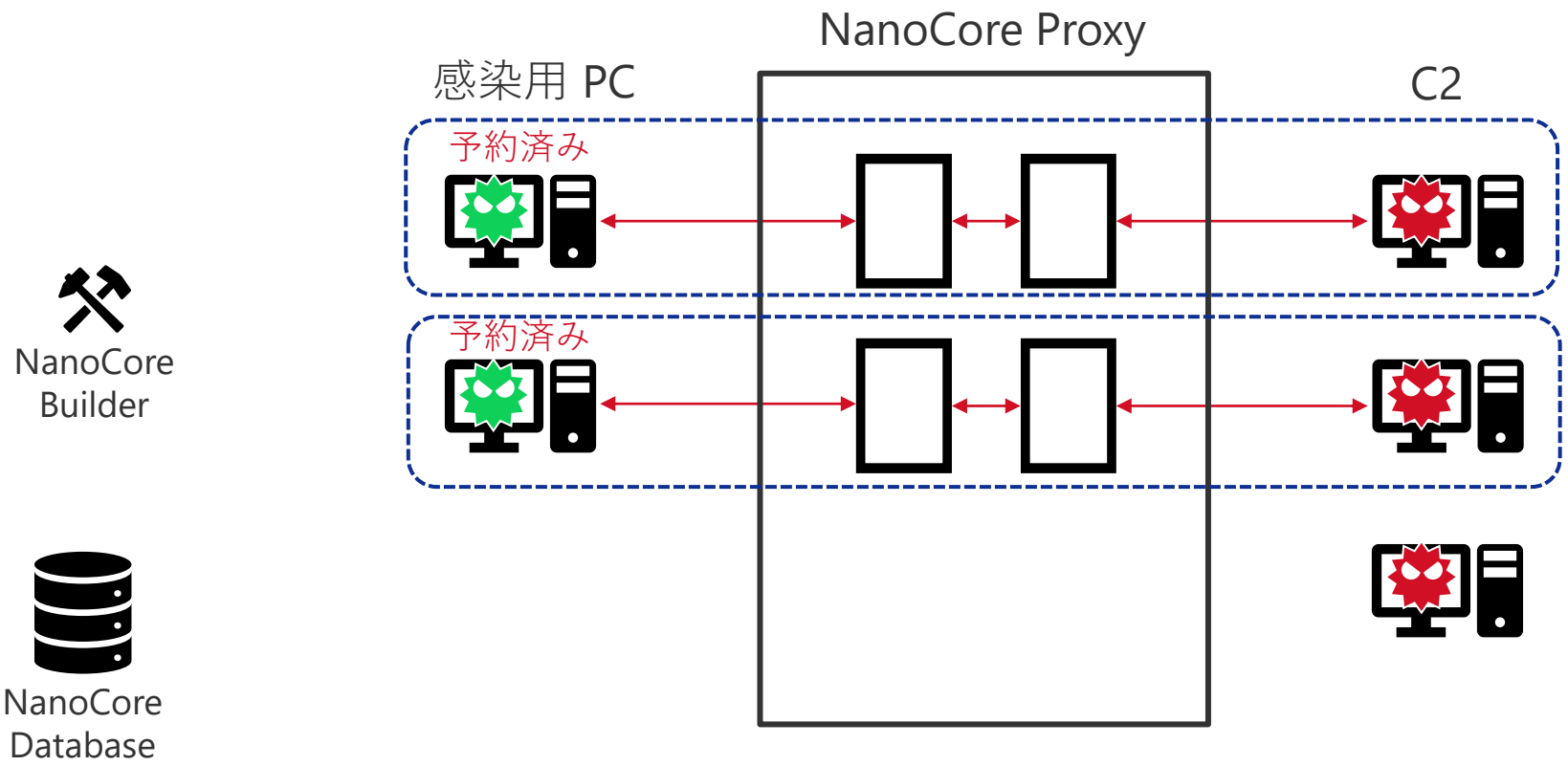
NanoCore Proxy の実行手順（7/8）

- すべての感染用PCが予約済みに遷移したら，
  新規コマンド受付を終了する



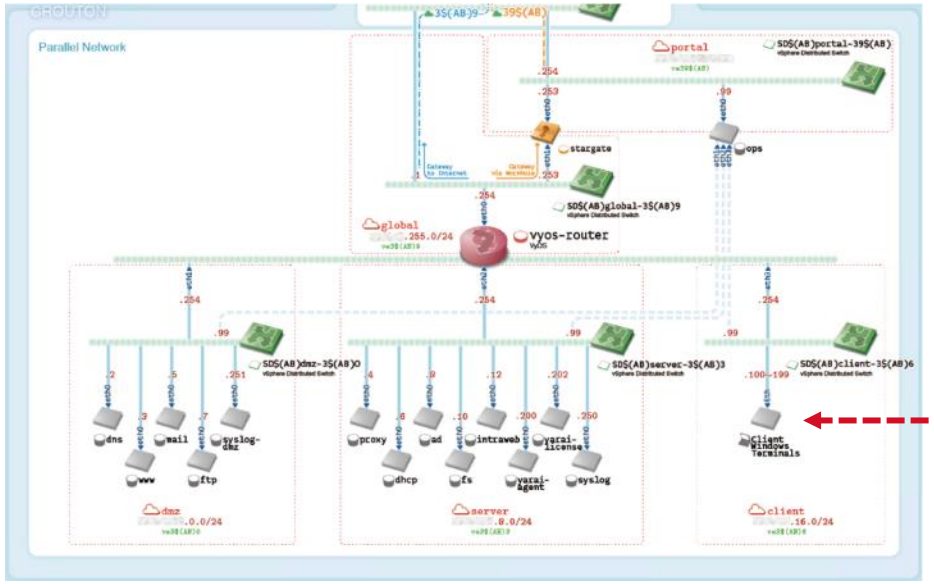
NanoCore Proxy の実行手順（8/8）

- 予約済みのクライアントは，対応するC2サーバとの接続を維持し，オペレータによるコマンドを待ち続ける

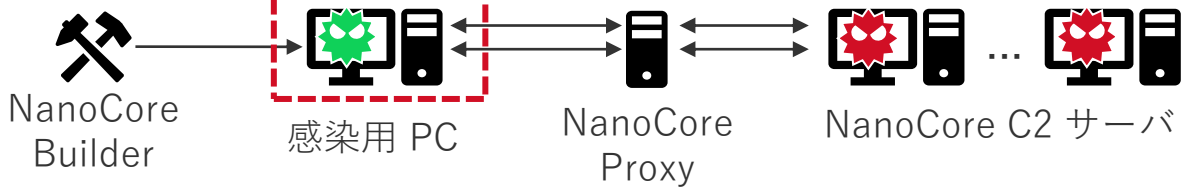


解析に使用する環境

- サイバー攻撃誘引基盤 STARDUST を利用する
  - 利用可能なログ
    - pcap，スクリーンショット，エンドポイントログ，フォレンジックログ など
  - 感染用 PCの構成
    - OS:
      - Windows7 x64
      - 言語: 日本語
    - インストールしたアプリ:
      - Chrome，MS Office 2013，Adobe Reader など
      - Filter Driver（解析用のツール）
    - コンテンツ:
      - ビーコンファイル（doc，xlsx，pptx，pdf）メール，ブラウザの閲覧履歴など



企業ネットワークに模倣した環境（STARDUST）



オペレータの誘引実験の結果（概要）

実験の結果 **88 件のオペレータによる侵入**を確認した

- **53 件** のオペレータは，1つ以上の目的を達成していた
  - ほとんどは，画面共有し，メールアカウント情報やパスワードを窃取していた
  - ブラウザやメーラーで有用なユーザかどうかを確認していた
  - 2次感染用に他のマルウェアが実行された

- **35 件** のオペレータは，ほとんど何もせずに去ってしまった
  - 画面共有のみ: **17 件**
  - 画面共有し，ブラウザを確認した: **8 件**
  - シャットダウンのみ: **3 件**
  - クライアントのアンインストールや画面のロックなど: **7件**

オペレータの行動の分類

Category	Counts
SCREEN SHAREING	76
PASSWORDS	37
FILES	24
BROWSER	18
MALWARE	12
MAIL	7
UNINSTALL	6
TOOLS	5
SHUTDOWN	5
MISC	16

NanoCore オペレータの行動一覧

分類	行動
メール	Outlook を開く
	受信トレイを確認する
	送信済みアイテムを確認する
	下書きを確認する
	ユーザのアカウント情報を確認する
	特定のメールを検索する
	メールの送信を試みる
ブラウザ	Chrome や Internet Explorer を開く
	Google アカウントへのログイン状況を確認する
	言語設定を英語に変更する
	ブックマークを確認する
	ブックマークされたページを開く
	特定のページを開く（PayPal，Alibaba，xvideos など）
	閲覧履歴を確認する
	特定のツールをダウンロードする
	よくアクセスするページや最近閉じたタブを確認する
権限昇格	管理者権限を要求する

分類	行動
ファイルアクセス	デスクトップ上のファイルやフォルダを開く
	最近表示した場所を開く
	ファイルを圧縮する
	ネットワークドライブを確認する
	ファイルを C2 サーバにアップロードする
	他のマルウェアを実行する
	NanoCore クライアントを更新する
	NanoCore クライアントをアンインストールする
	スタートメニューからアプリやファイルを検索する
アカウント情報	ブラウザに登録されたパスワードを窃取する
	メーラーに登録されたアカウント情報を窃取する
ネットワーク接続	タスクバーのネットワークアイコンから通信状況を確認する
	コントロールパネルのネットワークと共有センターを確認する
コマンド	ipconfig，net view コマンドを実行する
	systeminfo コマンドを実行する
その他	NjRAT チャット機能で話しかけてくる
	操作できないようにするために画面をロックする

2次感染用に使用されたマルウェア一覧

分類	名前	備考
分類できたマルウェア	AsyncRAT	https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp
	LimeRAT	https://github.com/NYAN-x-CAT/Lime-RAT
	Lokibot	-
	Morphine	-
	NetWire	-
	NjRAT	-
	Orcus	-
	Remcos	-
	VenomRAT	https://github.com/mirkoBastianini/Quasar-RAT の亜種？
未分類	不明（ワーム）	autorun.inf を使って拡散する 正規の実行ファイルを改ざんし，ワーム経由で起動するようにする
	不明	「taskkill /f /im svchost.exe」を実行するだけ？

使用されたツールやテクニック

分類	名前	備考
ツール	Disable-Windows-Defender	https://github.com/NYAN-x-CAT/Disable-Windows-Defender
	Chrome-Password-Recovery	https://github.com/0xfd3/Chrome-Password-Recovery
	LastActivityView	https://www.nirsoft.net/utils/computer_activity_view.html
	Mail PassView（NanoCoreの機能）	https://www.nirsoft.net/utils/mailpv.html
	WebBrowserPassView（NanoCoreの機能）	https://www.nirsoft.net/utils/web_browser_password.html
	AnyDesk	https://anydesk.com/
	TeamViewer	https://www.teamviewer.com/
テクニック	Microsoft AMSI（Antimalware Scan Interface）Bypass	amsi.dll の AmsiScanBuffer にスキャンをバイパスするようにパッチを当てる類似コード https://github.com/rasta-mouse/AmsiScanBufferBypass/blob/master/ASBBypass/Program.cs
	HideProc	taskmgr.exe にインジェクションし，asz$ から始まるプロセス名を隠ぺいする

NanoCore オペレータの行動

- **Case1:**
  画面共有してパスワードを窃取したオペレータ（最も多く確認した行動）

- **Case2:**
  ブラウザとメーラーを慎重にチェックしていたオペレータ

- **Case3:**
  複数のRATへの感染を試みたオペレータ

NanoCore オペレータの行動 – Case 1

Case 1: 画面共有してパスワードを窃取したオペレータ（最も多く確認した行動）

- 期間
  - 2020/06/15 16:32:00 ~ 16:34:00（UTC+9）
- 行動
  - 画面共有をする
  - Recover Passwords （NanoCore Surveillance Plugin）
    - Outlook 2013 のメールアドレスとパスワードを窃取する
    - ブラウザに登録されたパスワードを窃取しようとする
  - NanoCore クライアントをアンインストールする

NanoCore オペレータの行動 – Case 1

- 画面共有していたが，マウスやキーボードの操作は行われなかった

- Recover Passwords（NanoCore Surveillance Plugin）
  - Outlook 2013 のメールアドレスとパスワードを窃取する
    - Nirsoft の Mail PassView を使用した https://www.nirsoft.net/utils/mailpv.html

```
UUID('2441ccc7-e521-6225-4a86-bbbd0ea9b98f'),
[{'type': <NanoCoreType.BYTE: 1>, 'value': b'\x00'},
 {'type': <NanoCoreType.BYTE: 1>, 'value': b'\x01'},
 {'type': <NanoCoreType.STRING: 12>, 'value': 'Outlook 2013'},
 {'type': <NanoCoreType.STRING: 12>, 'value': '[redacted]',
 {'type': <NanoCoreType.STRING: 12>, 'value': '[redacted]'
```

Mail address

Password

  - ブラウザに登録されたパスワードを窃取しようとする
    - Nirsoft の WebBrowserPassView を使用した https://www.nirsoft.net/utils/web_browser_password.html
    - ブラウザにパスワードを保存していなかったので，盗まれることはなかった

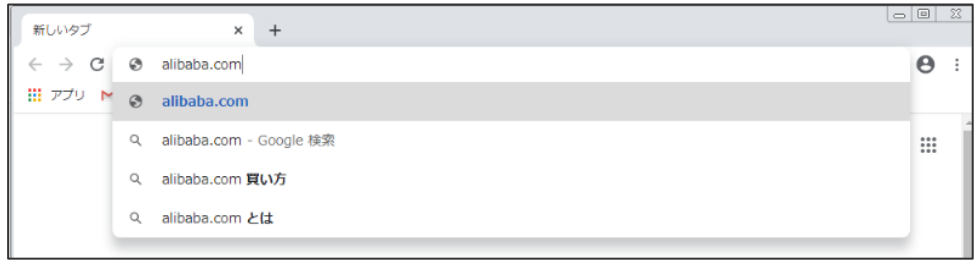
NanoCore オペレータの行動 – Case 2

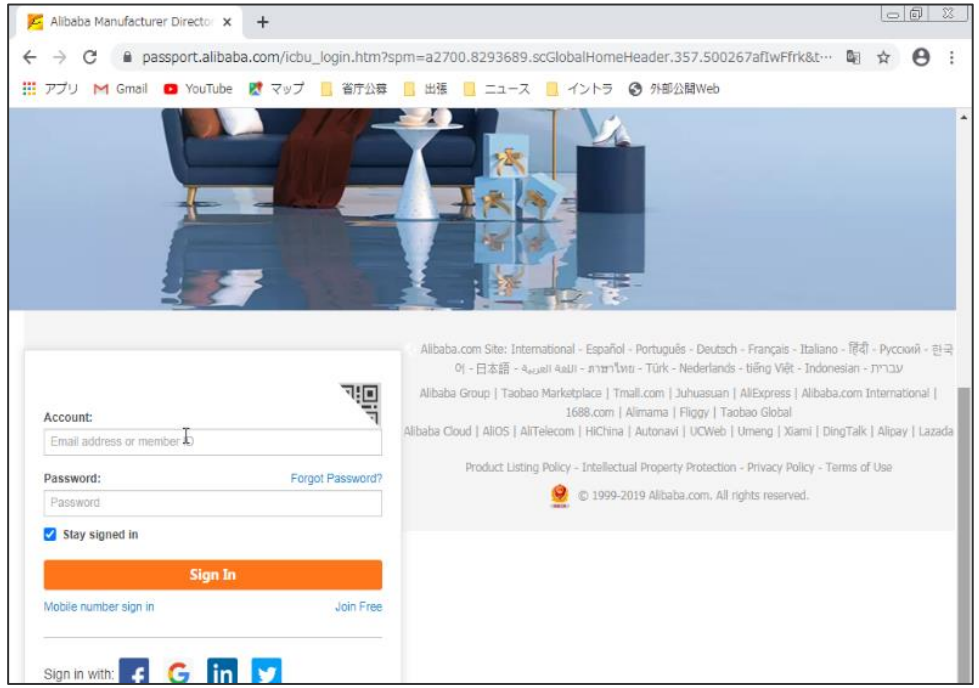
Case 2: ブラウザとメーラーを慎重にチェックしていたオペレータ

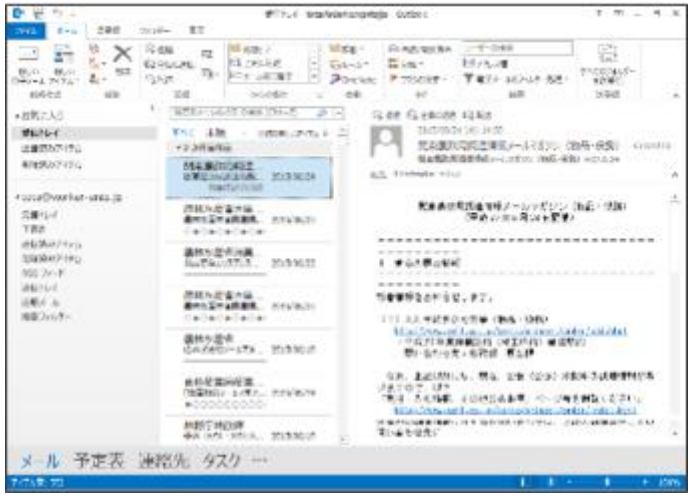
- 期間
  - 2020/07/08 16:07:10 ~ 16:56:47（UTC+9）
- 行動
  - 画面共有をする
    - デスクトップ上のフォルダを開く
    - ネットワーク接続を確認する
    - Outlook を何度も開く
      - メール一覧を注意深く確認する
      - 送信元のメールアドレスを確認する
      - Outlookのアカウント情報を確認する
      - ALI や alibaba というキーワードで メールを検索する
      - メールの表示を拡大する
    - タスクバーを確認する
    - Chrome を何度も開く
      - アドレスバーに alibaba.com と入力する
      - Alibaba の Sign In ページを開く
      - Chrome ログイン状況を確認する
      - ブックマークに登録していた yelp.com のページを開く
      - Chrome アプリを確認する
      - 言語設定を英語に変更する
    - スタートメニューを開く
      - al や english というキーワードで検索する
      - シャットダウンする

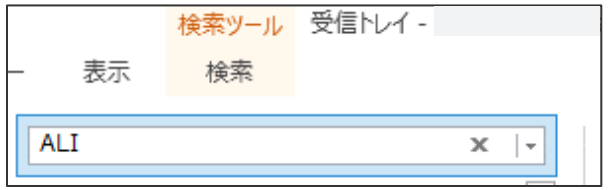
NanoCore オペレータの行動 – Case 2

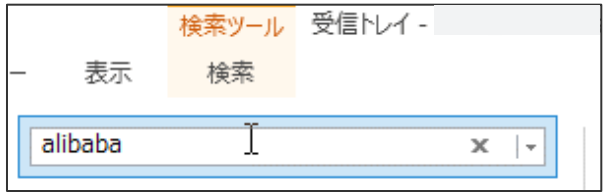
- Chrome と Outlook を交互に開きながら作業をしていた
  1. Chrome を開く
  2. alibaba.com を開く
  3. Sign In ページに移動する
  4. Outlook 2013 を開く
  5. メールの受信トレイを注意深く確認する
  6. ALI や alibaba というキーワードでメールを検索する
- 盗んだメールアドレスでアカウントを作成しようとした？











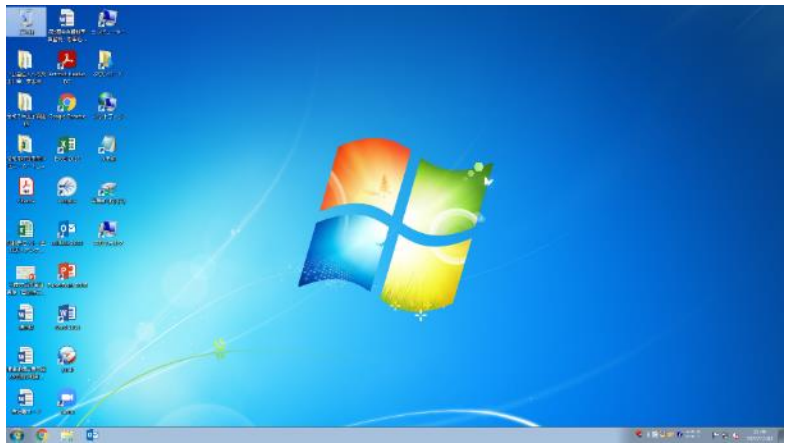
NanoCore オペレータの行動 – Case 3

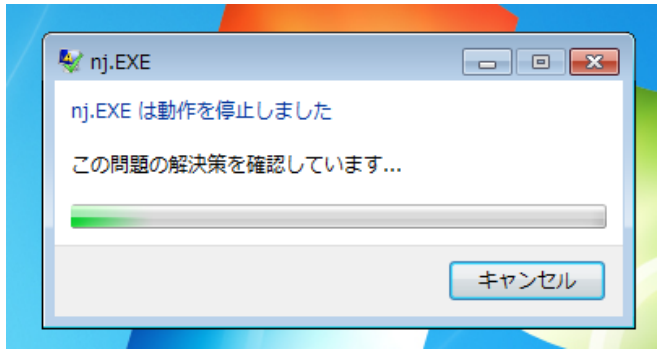
Case 3: 複数のRATへの感染を試みたオペレータ

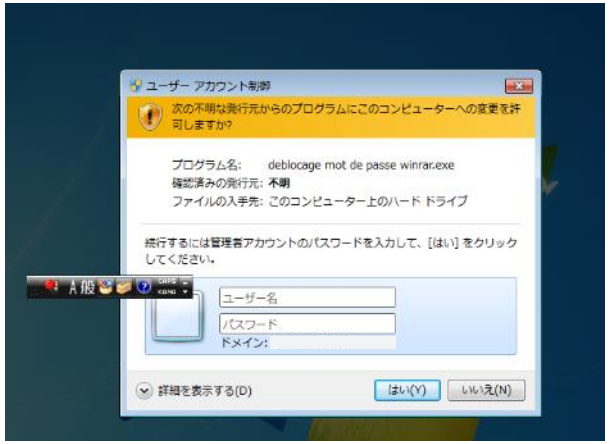
- 期間
  - 2020/10/08 15:38:44 ~ 15:44:27（UTC+9）
  - 2020/10/13 14:52:27 ~ 15:03:54（UTC+9）
- 行動
  - 画面共有をする
  - 他のマルウェアに感染させる
    - NjRAT，AsyncRAT，Remcos
  - Windows Defender を停止させる
    - Disable-Windows-Defender: https://github.com/NYAN-x-CAT/Disable-Windows-Defender
  - Microsoft AMSI（Antimalware Scan Interface）Bypass

NanoCore オペレータの行動 – Case 3

- **1日目:** 2020/10/08 15:38:44 ~ 15:44:27（UTC+9）
  - 画面共有していたが，マウスやキーボードの操作は行われなかった







  - NjRAT と Disable-Windows-Defender を実行する

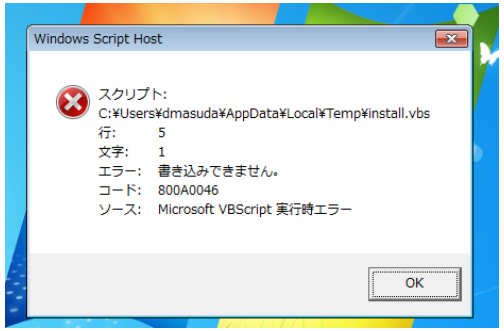
- dnshost.exe PID:2064
  - nj.EXE PID:2552
  - deblocage mot de passe winrar.exe PID:504
  - deblocage mot de passe winrar.exe PID:1964
    - powershell.exe PID:1868

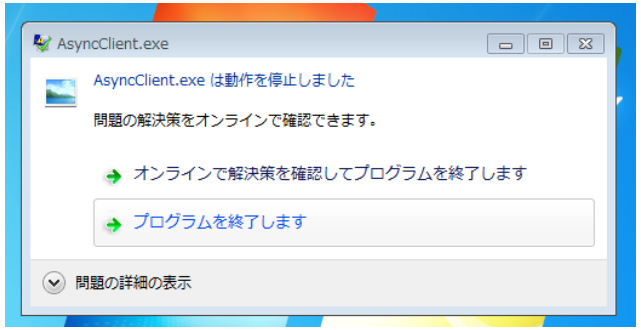
NjRAT
- Microsoft AMSI Bypass
- Win7 には AMSI バイパスに使用される amsi.dll が存在しないため，プロセスが異常終了していた

Disable-Windows-Defender
- https://github.com/NYAN-x-CAT/Disable-Windows-Defender
- 実行前に管理者権限を要求する

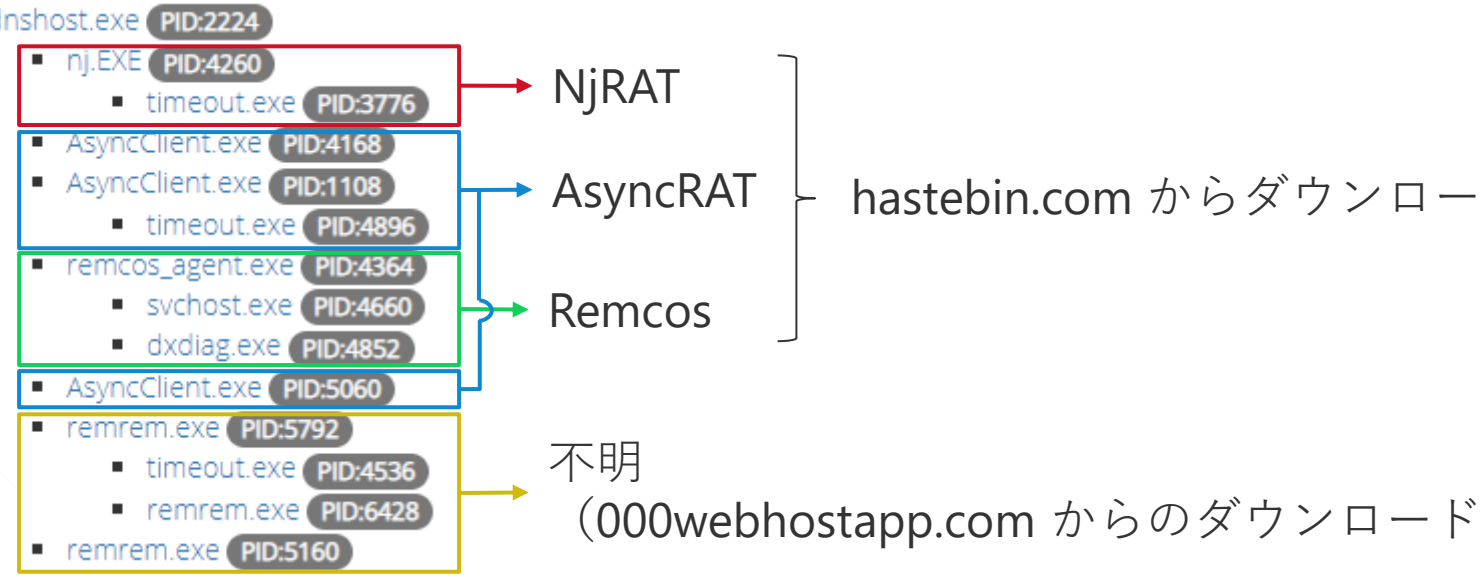
NanoCore オペレータの行動 – Case 3

- **5日後:** 2020/10/13 14:52:27 ~ 15:03:54（UTC+9）
  - 画面共有していたが，マウスやキーボードの操作は行われなかった





  - NjRAT， AsyncRAT， Remcos が実行された



NanoCore オペレータの行動 – まとめ

オペレータの主な行動

- **ユーザの偵察**
  - 21 人のオペレータは，**閲覧履歴やブックマーク，メールの受信トレイを注意深く確認していた**
  - 24 人のオペレータは，**デスクトップ，ドキュメント，共有フォルダを確認していた**

- **メールアカウント/パスワード，ファイルの窃取**
  - 37 人のオペレータは，**メールアカウントやパスワードを窃取していた**
  - 8 人のオペレータは，**ファイルを窃取していました**．最大で 221 のファイルが窃取された

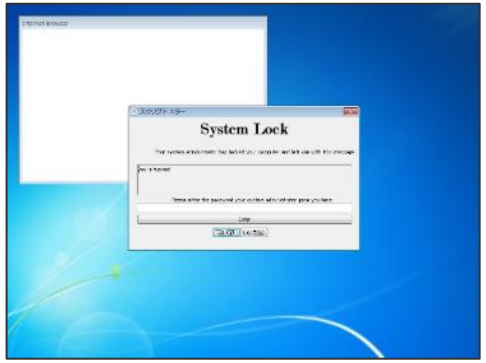
- **バックドアの設置**
  - 12 人のオペレータは，**NanoCore 以外のマルウェアに感染させていた**
  - 11 種類のマルウェアが使用されていました

NanoCore オペレータの行動 – 考察

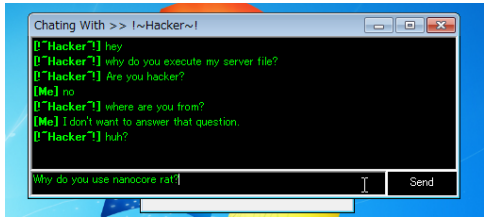
- オペレータがすぐに去ってしまった原因
  - **有用なユーザでないと判断された（解析環境だと気づいた）可能性がある**
    - **メールの受信トレイ，送信済みアイテム，下書きが空だった**
    - **ブラウザの閲覧履歴がない**
    - systeminfo コマンドを使用して動作環境を確認する
    - VM 検知
    - **Windows10 でしか動作しないマルウェアが実行された**
  - **そもそもターゲットが日本ではない？**
    - **平日の 9:00~18:00（UTC+9）に実験を行った**
    - **OS の言語設定やファイルなどすべて日本語であった**
    - 日本語に戸惑っているオペレータを何人か確認した

解析環境と気づいた後の行動:

シャットダウン



画面をロックする



チャットで話しかけてくる

File Creation(File System Tunneling)		scanresult.db-journal
File Creation		PING.EXE-371F41E2.pf
File Deletion		WrXE6.exe
File Creation		CMD.EXE-AC113AA8.pf
File Creation(File System Tunneling)		scanresult.db-journal

NanoCore をアンインストールする

おわりに

- **今回の発表**
  - **NanoCore C2 サーバの長期観測**
    - 主に アメリカとヨーロッパに C2 サーバがホスティングされている
    - 多くのサーバは 9:00~18:00（UTC）に稼働している
    - C2情報は，JPCERT/CC を通して各国の CERT に提供されている（MISP でも発信していく予定）
  - **NanoCore オペレータの誘引実験**
    - 多くのオペレータは，メールアカウントやパスワードを窃取する
    - 一部，NanoCore 以外の RAT に感染させるケースを確認した
- **今後について**
  - オペレータにより長い時間活動してもらえるような環境を調整する必要がある
  - 長期観測からオペレータがよく使用する VPN やアドレス帯が一部見えてきた
    それらをスキャンすれば，NanoCore だけでなく，他の攻撃ツールを検出できる可能性がある