Computer Security Symposium 2019
21 - 24 October 2019

# サイバー攻撃誘因基盤「STARDUST」の検証

水口　喬詔[1,a)]　小熊　永久[1]　大坪　雄平[1,2]

**概要**：本研究は，国立研究開発法人情報通信研究機構（NICT）が開発したサイバー攻撃誘引基盤「STARDUST」及びその中で構築した環境を検証するものである．攻撃者が攻撃動作を行った際の痕跡を STARDUST 上で確認するため，STARDUST において構築した一般的な企業のネットワークを模した環境に対し，脆弱性試験用ソフトウェアを使用して自らの手で一連の攻撃動作を実施した．それにより，STARDUST が自動的に取得する痕跡及び構築した環境内から得られる痕跡を元に攻撃動作の調査を行い，STARDUST の有用性，問題点及び改善点を検証する．

**キーワード**：STARDUST, 有用性, 改善案

# A survey of the large-scale infrastructure for luring and monitoring cyber adversaries, called “STARDUST”

TAKATSUGU MINAKUCHI[1,a)]　NAGAHISA KOGUMA[1]　YOHEI OTSUBO[1,2]

***Abstract:*** This research is to survey the large-scale infrastructure for luring and monitoring cyber of adversaries, called “STARDUST” and the environment built in it, developed by National Institute of Information and Communications Technology (NICT). We used penetration testing tools to execute a series of attack operations with our own hands on an environment that simulates a general company network built in “STARDUST”, and investigated the traces of attacks that remain on STARDUST. In this way, we investigated the attack behavior based on the traces automatically acquired by STARDUST and the traces obtained from the built environment, and evaluated the usefulness, problems and improvements of STARDUST.

***Keywords:*** STARDUST, Utility, Improvement plan

## 1. はじめに

近年，サイバー攻撃対策として，ファイアウォール等のネットワーク機器を使用した従来の境界防御だけではなく，Cyber Deception にも注目が集まっている。Cyber Deception とは，ネットワーク内におとりサーバやハニーポット等を設置し，攻撃者を誘導してその手口の情報を収集したり，攻撃活動を遅らせたりすることを意味している [1]．しかし，企業で実際に稼働しているネットワーク内に新たに Cyber Deception を構築するのは容易ではない．このような状況において，国立研究開発法人情報通信研究機構（NICT）は STARDUST を開発した．この STARDUST は，ワームホール機能を使用することで，企業に対する攻撃を STARDUST に誘引し，攻撃者の行動を検知・観測することができる．そのため，企業内に Cyber Deception を構築する際に大きな助けとなるだろう．

本研究は，STARDUST 環境をより良く活用するための手法の検討を目的としている．まず，STARDUST に構築した環境に対し，我々が攻撃者役として攻撃活動を模擬する．その後，STARDUST の機能及びクライアント環境に残存する攻撃の痕跡の調査を行うことで，STARDUST の有用性，問題点及び改善案を検討する．

1　警察庁
National Police Agency
2　情報セキュリティ大学院大学
Institute of information security
a)　minakuchi@npa.cyberpolice.go.jp

© 2019 Information Processing Society of Japan

## 2. STARDUST とは

### 2.1 STARDUST の概要

STARDUST とは，標的型攻撃等の攻撃者を誘引し，その攻撃活動を長期観測するために NICT が開発したサイバー攻撃誘引基盤である [2][3][4][5]．この STARDUST 内で各種サーバやクライアント環境を実稼働させることにより，実在の政府や企業等の組織を模擬したネットワークの構築が可能とされる．なお，STARDUST の初期状態におけるネットワーク環境では，ログの取得設定は各 OS の初期状態である．例えば，Windows OS を使用したサーバ及びクライアント環境に関しては，イベントログ等の取得設定は初期状態から変更されていない．これらに関しては，利用目的に応じて設定を変更する必要がある．

### 2.2 STARDUST のネットワーク技術

STARDUST の環境内で送受信された通信内容はすべて記録されており，利用者はそれらの情報をリアルタイムで確認することができる．また，過去に行われた通信も遡って確認することができる．さらに，ワームホールという機能を使うことで，STARDUST の出口の IP アドレスを組織が実際に使用している IP アドレスに設定することができる．これにより，攻撃者に偽のネットワークであると気づかせにくくすることも可能である．これらの機能を使用し，標的型メール等の侵入活動に用いられたマルウェア検体を STARDUST 内のクライアント環境上で実行し，攻撃者を誘引する．これにより，外部から接続を試みた攻撃者による調査行為や感染拡大行為，情報窃取等の挙動を観測し，リアルタイムの挙動観測・分析が可能となる．

## 3. 構築したネットワーク環境

本研究を実施するにあたって，我々が構築したネットワーク環境は図 **1** のとおりである．このネットワーク環境は，STARDUST の初期状態におけるネットワーク環境を利用して構築した．本研究では，我々は攻撃者役として攻撃を行い，実際に攻撃者を呼び込む必要はないため，ワームホール機能は使用しない．

なお，3 台のクライアント環境に関しては，脆弱性を突いた攻撃を成功させるために，Windows Update 等による更新は必要最低限としている．また，一部のユーザに関しては，他 PC へのリモートデスクトップ接続を許可するように設定している．さらに，クライアント環境内には Microsoft 製プロセスモニタリングソフトウェア Sysmon をインストールしている．Sysmon は，新たにプロセスが起動した場合，そのプロセスのファイルパス，親プロセス，実行時間及び実行時の引数等の情報を記録するソフトウェアである．

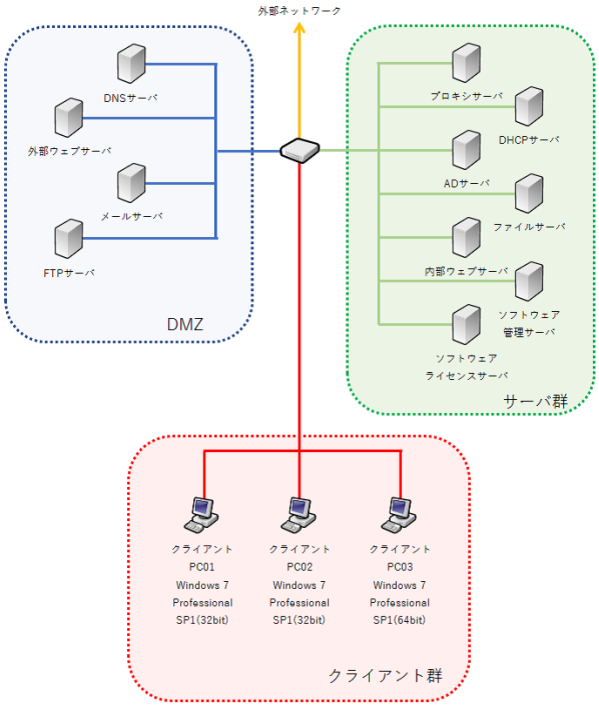


**図 1** ネットワーク図
**Fig. 1** Network diagram

## 4. 実施した攻撃動作の流れ

### 4.1 攻撃の流れの概要

検証作業を実施するにあたり，我々が攻撃者役として模擬した攻撃の流れの概要を図 **2** に示す．図 2 の各段階において模擬した攻撃内容について以下に述べる．

#### 4.1.1 感染

一連の攻撃のきっかけとして，攻撃者が作成した不正プログラムの検体をクライアント PC01 の一般ユーザが実行する．これにより，クライアント PC01 はインターネット上で稼働している C&C サーバとの通信を開始し，攻撃者による遠隔操作が開始される．攻撃者は，クライアント PC01 内のネットワーク情報やシステム情報の収集等を実施する．

#### 4.1.2 権限昇格

クライアント PC01 内で一般ユーザからの権限昇格を行い，攻撃者はクライアント PC01 の System 権限を取得する．クライアント PC01 内のファイルの窃取や不正プログラムの自動実行登録等を実施した後，他のクライアント環境からアクセス可能な共有フォルダを作成し，その中に感染拡大用の不正プログラムを蔵置する．

#### 4.1.3 クライアント PC02 への横展開

攻撃者は，リモートデスクトップ接続機能を使用して，一般ユーザとしてクライアント PC01 からクライアント PC02 へと接続し，感染の拡大を試みる．その後，攻撃者がアクセス可能な領域内に必要な情報が存在しなかったた

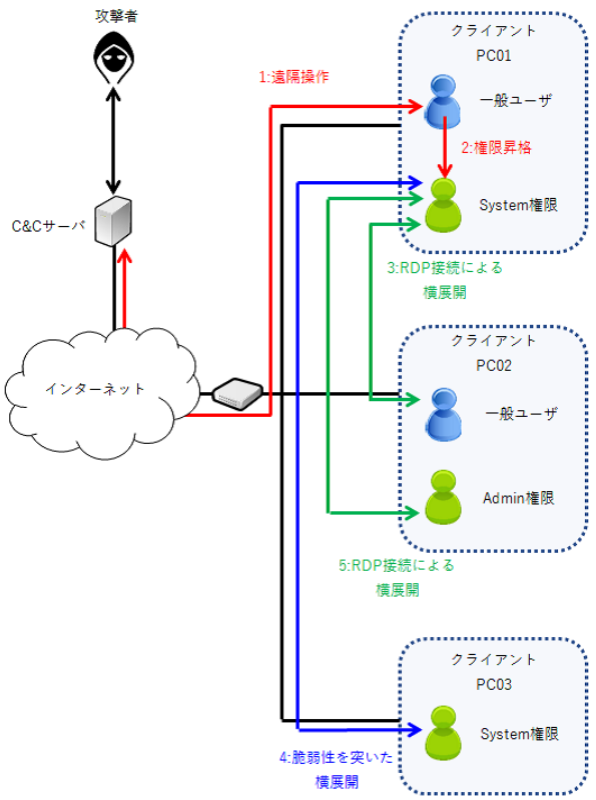


図 2　実施した攻撃の流れの概要
**Fig. 2**　Schematic diagram of the attack flow

め，クライアント PC02 へのリモートデスクトップ接続を解除する．

#### 4.1.4　クライアント PC03 への横展開

攻撃者は，クライアント PC01 からクライアント PC03 に対して，クライアント PC03 に存在する脆弱性を突くことにより，クライアント PC03 の System 権限を取得し，感染を拡大する．攻撃者は，クライアント PC03 内で情報収集やファイルの窃取，不正プログラムの自動実行登録等を実施する．

#### 4.1.5　クライアント PC02 の Admin 権限への横展開

クライアント PC03 内で入手した情報を元にして，攻撃者は再度リモートデスクトップ接続を使用して，Admin 権限ユーザとしてクライアント PC01 からクライアント PC02 へと接続し，感染を拡大する．その後，攻撃者はクライアント PC02 からクラウドストレージサービス上に前もってアップロードしていたツール類をダウンロードし，情報収集やファイルの窃取，不正プログラムの自動実行登録等を実施する．

以上の攻撃が終了した後，作成したフォルダ及びファイル等を削除し，最終的に攻撃者はシステムから退出する．

### 4.2　模擬した攻撃の詳細

我々が攻撃者役として模擬した攻撃内容の詳細を**表 1** に示す．なお，表内の項番に関しては，図 2 に示した各攻撃フェーズにおける攻撃動作の順番を示している．

今回の攻撃を実施するにあたって，攻撃用ツールとして数種類の脆弱性試験用ソフトウェアを適宜使い分けることとした．使用した脆弱性試験用ソフトウェアの一部は，C&C サーバとクライアント間の通信内容を難読化する機能を有している．項番 1-1 に示している，一連の攻撃の発端となっている検体の実行動作のみ，STARDUST 上のクライアント PC01 環境を直接操作して実施した．これ以外の動作は，全て攻撃者用として STARDUST 外に準備した端末から実施している．なお，今回実施した一連の攻撃においては，ネットワーク内のクライアント環境内で記録される Windows イベントログ等の痕跡を削除していない．

## 5.　残存する攻撃の痕跡

一連の攻撃を実施した後，各クライアント環境内に存在している痕跡及び STARDUST によって自動的に収集される痕跡を調査し，攻撃者による攻撃活動をどこまで特定できるか確認した．

なお，STARDUST 内の環境のメモリや仮想ディスクのダンプデータはユーザが容易に取得できないようになっている．これはマシンリソースが有限なため，ユーザが各々に自由にダンプデータを取得するとリソースの枯渇が懸念されているためである．そのため，このようなデータが必要となった際は，管理者である NICT がデータを取得しユーザに何らかの手段でデータを提供する運用となっている点に留意した．

クライアント環境上で確認できた痕跡を**表 2** に，STARDUST の機能によって確認できた痕跡を**表 3** に示す．表内の記号の意味については，以下のとおりである．

- ○　その攻撃活動が実行されたことを特定できる情報が記録されている
- ×　その攻撃活動に関する情報が記録されていない，又は内容を判別することができない
- △　その攻撃活動に関する情報が記録されているが，不完全
- -　その攻撃活動に関する情報が仕様上記録されることがない

また，一部の項番に関して，詳細な結果を**表 4** から**表 8** に示す．

表 2 及び表 3 に示したとおり，クライアント環境上で確認できる痕跡に関しては，Windows 標準の機能だけでは多くの情報を得ることができていない．メモリから得られる情報に関しても，今回の結果では攻撃者が実行した攻撃指令をほとんど取得できていないことからわかるとおり，不確実である．また，STARDUST の機能によって確認できた痕跡に関しては，ある IP アドレスとの間で通信が発生していることが確認可能である．STARDUST の機能によって通信内容に関しても確認可能であるが，今回使用した脆

表 1　攻撃の流れ
**Table 1**　Flow of attacks

| 項番 | 概要 |
|---|---|
| 1-1 | PC01 において，<br>ユーザが不正プログラムの検体を実行 |
| 1-2 | PC01 において，<br>ログインしているユーザの情報，PC01 の設定情報，<br>STARDUST 環境内のネットワーク情報を収集 |
| 1-3 | 侵入した環境が仮想環境かどうかのチェックを実施 |
| 1-4 | PC01 の同一ネットワーク内に対して，<br>ポートスキャンを実施 |
| 2-1 | PC01 に存在している脆弱性を突き，権限を昇格 |
| 2-2 | C&C サーバを経由して，<br>攻撃に使用するツールを PC01 内に蔵置 |
| 2-3 | PC01 内にフォルダを作成し，そのフォルダ内に<br>PC01 内から収集したファイルをコピーして保存 |
| 2-4 | PC01 内で収集したファイルをパスワードをかけて圧縮 |
| 2-5 | 生成した圧縮ファイルを C&C サーバにアップロード |
| 2-6 | PC01 起動時に検体を自動実行するため，<br>PC01 のサービスとして検体を登録 |
| 2-7 | PC01 のファイアウォールを無効化 |
| 2-8 | PC01 内に共有フォルダを作成し，<br>他の PC からアクセス可能に設定 |
| 2-9 | 作成した共有フォルダ内に検体を蔵置 |
| 2-10 | PC01 のパスワード情報やパスワードハッシュを収集 |
| 3-1 | PC01 を経由して，入手した情報 (一般ユーザ) を元に<br>PC02 に対してリモートデスクトップ接続 |
| 3-2 | PC02 内で，<br>PC01 の共有フォルダ内に蔵置している検体を実行 |
| 3-3 | PC01 から PC02 に対する<br>リモートデスクトップ接続を終了 |
| 4-1 | PC01 を経由して，脆弱性を突くことで PC03 に侵入 |
| 4-2 | PC03 内で，<br>PC01 の共有フォルダ内に蔵置している検体を実行 |
| 4-3 | PC03 起動時に検体を自動実行するため，<br>PC03 のレジストリ内に検体を登録 |
| 4-4 | C&C サーバを経由して，<br>攻撃に使用するツールを PC03 内に蔵置 |
| 4-5 | PC03 内にフォルダを作成し，そのフォルダ内に<br>PC03 内から収集したファイルをコピーして保存 |
| 4-6 | PC03 内で収集したファイルを<br>パスワードをかけて圧縮 |
| 4-7 | 生成した圧縮ファイルを C&C サーバにアップロード |
| 4-8 | PC03 のパスワード情報やパスワードハッシュを収集 |
| 5-1 | PC01 を経由して，入手した情報 (管理者権限) を元に<br>PC02 に対してリモートデスクトップ接続 |
| 5-2 | PC02 内で，<br>PC01 の共有フォルダ内に蔵置している検体を実行 |
| 5-3 | PC01 内の共有フォルダへのアクセス権<br>及び共有フォルダを削除 |
| 5-4 | PC02 起動時に検体を自動実行するため，<br>PC02 内のスタートアップフォルダ内に検体を登録 |
| 5-5 | クラウドストレージを経由して，<br>攻撃に使用するツールを PC02 内に蔵置 |
| 5-6 | PC02 内にフォルダを作成し，そのフォルダ内に<br>PC02 内から収集したファイルをコピーして保存 |
| 5-7 | PC02 内で収集したファイルをパスワードをかけて圧縮 |
| 5-8 | 生成した圧縮ファイルを C&C サーバにアップロード |
| 5-9 | PC01 から PC03 までの全てにおいて，<br>作成したフォルダ，作成した圧縮ファイル，<br>使用したツールを削除する |

表 2　クライアント環境上で確認できた各攻撃の痕跡
**Table 2**　Traces of each attack confirmed on the client

| 項番 | メモリ | NTFS 管理ファイル | プリフェッチ | イベントログ (Sysmon 以外) | レジストリ | Sysmon |
|---|---|---|---|---|---|---|
| 1-1 | ○ | △ | × | - | × | ○ |
| 1-2 | × | - | × | - | - | ○ |
| 1-3 | × | - | × | × | - | ○ |
| 1-4 | × | - | - | ○ | - | × |
| 2-1 | × | - | - | × | - | ○ |
| 2-2 | × | △ | - | - | - | - |
| 2-3 | × | × | - | - | - | ○ |
| 2-4 | × | × | × | - | × | ○ |
| 2-5 | × | - | - | - | - | - |
| 2-6 | △ | - | - | ○ | - | ○ |
| 2-7 | × | - | - | ○ | ○ | ○ |
| 2-8 | × | △ | - | - | - | ○ |
| 2-9 | × | △ | - | - | - | - |
| 2-10 | × | - | - | - | - | × |
| 3-1 | × | - | × | ○ | - | ○ |
| 3-2 | ○ | × | × | - | × | ○ |
| 3-3 | × | - | - | × | - | ○ |
| 4-1 | × | - | - | × | - | ○ |
| 4-2 | ○ | △ | × | - | - | ○ |
| 4-3 | × | - | - | - | △ | ○ |
| 4-4 | × | × | - | - | - | - |
| 4-5 | × | × | - | - | - | ○ |
| 4-6 | × | × | △ | - | - | ○ |
| 4-7 | × | - | - | - | - | - |
| 5-1 | × | - | - | × | - | ○ |
| 4-8 | × | - | - | - | - | × |
| 5-2 | ○ | △ | △ | - | × | ○ |
| 5-3 | × | - | - | - | - | × |
| 5-4 | × | × | - | - | - | ○ |
| 5-5 | × | × | - | - | - | - |
| 5-6 | × | × | - | - | - | ○ |
| 5-7 | × | × | △ | - | × | ○ |
| 5-8 | × | - | - | - | - | - |
| 5-9 | × | - | △ | - | × | ○ |

弱性試験用ソフトウェアの機能により通信内容が難読化されているため，C&C サーバからクライアントに対して送られている指令の内容を確認することはできなかった．

## 6.　STARDUST の有用性，問題点及び改善案

### 6.1　STARDUST の有用性

#### 6.1.1　不正プログラムの実行環境

不正プログラムが活動すると，それ単体で動作するものだけでなく，最初のファイルを起因として外部から必要なスクリプト等を取得して実行する検体も多数存在する．その際，自組織のインターネット環境に接続した状態で不正プログラムを実行し，C&C サーバに接続することにより，自組織の内部 IP アドレス等のシステム構成を攻撃者に把握されると支障が出る場合もあると考えられる．そのような場合，STARDUST の環境を利用することによって，自組織のシステム構成等の情報を攻撃者に知られることなく，自組織に似せた環境を使用して，検体実行後の動作を調査・観測することが可能となる．

自組織において，インターネットに接続した状態で検体を実行し，動作の全容を観測する環境が整っていない場合でも，STARDUST によるパケットキャプチャにより，効率的に不正プログラム動作を確かめることができる．

表 3　STARDUST の機能によって確認できた各攻撃の痕跡
**Table 3**　Traces of each attack confirmed by the STARDUST function

| 項番 | パケット情報 | プロセス情報 |
|---|---|---|
| 1-1 | ○ | ○ |
| 1-2 | × | × |
| 1-3 | × | × |
| 1-4 | ○ | × |
| 2-1 | × | × |
| 2-2 | × | - |
| 2-3 | × | × |
| 2-4 | × | × |
| 2-5 | × | - |
| 2-6 | × | × |
| 2-7 | × | × |
| 2-8 | × | × |
| 2-9 | × | - |
| 2-1 | × | × |
| 3-1 | ○ | × |
| 3-2 | × | × |
| 3-3 | ○ | × |
| 4-1 | ○ | ○ |
| 4-2 | ○ | ○ |
| 4-3 | × | × |
| 4-4 | × | - |
| 4-5 | × | × |
| 4-6 | × | × |
| 4-7 | × | - |
| 4-8 | × | × |
| 5-1 | ○ | × |
| 5-2 | ○ | ○ |
| 5-3 | × | × |
| 5-4 | × | × |
| 5-5 | △ | - |
| 5-6 | × | × |
| 5-7 | × | × |
| 5-8 | × | - |
| 5-9 | × | × |

### 6.1.2　STARDUST によるパケットキャプチャ

今回実施した一連の攻撃において，攻撃者は C&C サーバからクライアント環境に対して，難読化した通信で指令を送信している．そのため，難読化アルゴリズムが特定できない限り，パケットキャプチャ結果だけからは，「ある時間に，ある IP アドレスから，あるクライアント環境に対して何らかの通信が行われた」以上のことを把握することはできなかった．しかし，**表 6** に示したとおり，攻撃者がネットワーク内で横展開を実施する際に発生した通信は平文で行われていたため，どの端末からどの端末に対してどの脆弱性を突いた攻撃を行っていたのかを特定することができた．

このパケットキャプチャ機能は，クライアント環境上でパケットキャプチャソフトウェアが動作しているというわけではないため，攻撃者がクライアント環境内で稼働しているプロセスを確認したとしても，通信が記録されている

表 4　項番 1-2 の詳細
**Table 4**　Details of No. 1-2

| 項目 | 詳細 |
|---|---|
| メモリ | 指令内容を取得できる可能性があるが，今回は取得不可能 |
| NTFS 管理ファイル | この項目には，関連する情報は記録されない |
| プリフェッチ | 関連する情報は記録されていない |
| イベントログ (Sysmon 以外) | この項目には，関連する情報は記録されない |
| レジストリ | この項目には，関連する情報は記録されない |
| Sysmon | 実行されたファイルのファイルパス，親プロセス，実行時間，実行時の引数等の情報が取得可能 |
| パケット情報 (STARDUST) | 通信自体は検知可能だが，指令内容は判別不能 |
| プロセス情報 (STARDUST) | 関連する情報は記録されていない |

表 5　項番 2-3 及び 2-4 の詳細
**Table 5**　Details of Nos. 2-3 and 2-4

| 項目 | 詳細 |
|---|---|
| メモリ | 生成に関する指令内容を取得できる可能性があるが，今回は取得不可能 |
| NTFS 管理ファイル | 関連する情報は記録されていない |
| プリフェッチ | 関連する情報は記録されていない |
| イベントログ (Sysmon 以外) | この項目には，関連する情報は記録されない |
| レジストリ | 関連する情報は記録されていない |
| Sysmon | 実行されたファイルのファイルパス，親プロセス，実行時間，実行時の引数等の情報が取得可能 |
| パケット情報 (STARDUST) | 通信自体は検知可能だが，指令内容は判別不能 |
| プロセス情報 (STARDUST) | 関連する情報は記録されていない |

表 6　項番 4-1 の詳細
**Table 6**　Details of No. 4-1

| 項目 | 詳細 |
|---|---|
| メモリ | 関連する情報は記録されていない |
| NTFS 管理ファイル | この項目には，関連する情報は記録されない |
| プリフェッチ | この項目には，関連する情報は記録されない |
| イベントログ (Sysmon 以外) | 関連する情報は記録されていない |
| レジストリ | この項目には，関連する情報は記録されない |
| Sysmon | PC01 及び PC03 に関して，実行されたツール及び脆弱性を突くことで起動したプロセスのファイルパス，親プロセス，実行時間，実行時の引数等の情報が取得可能 |
| パケット情報 (STARDUST) | 脆弱性を突いた攻撃に関するパケットが記録されている |
| プロセス情報 (STARDUST) | PC03 においては関連する情報は記録されていないが，PC01 においては使用したツールに関する情報が記録されている |

表 7　項番 5-5 の詳細
**Table 7**　Details of No. 5-5

| 項目 | 詳細 |
|---|---|
| メモリ | 関連する情報は記録されていない |
| NTFS 管理ファイル | 関連する情報は記録されていない |
| プリフェッチ | この項目には，関連する情報は記録されない |
| イベントログ (Sysmon 以外) | この項目には，関連する情報は記録されない |
| レジストリ | この項目には，関連する情報は記録されない |
| Sysmon | この項目には，関連する情報は記録されない |
| パケット情報 (STARDUST) | クラウドストレージへの通信自体は 検知可能だが，具体的な通信内容は判別不能 |
| プロセス情報 (STARDUST) | この項目には，関連する情報は記録されない |

表 8　項番 5-9 の詳細
**Table 8**　Details of No. 5-9

| 項目 | 詳細 |
|---|---|
| メモリ | 削除に関する指令内容を取得できる可能性があるが，今回は取得不可能 |
| NTFS 管理ファイル | この項目には，関連する情報は記録されない |
| プリフェッチ | 削除ツールが実行された痕跡が記録されている |
| イベントログ (Sysmon 以外) | この項目には，関連する情報は記録されない |
| レジストリ | 関連する情報は記録されていない |
| Sysmon | 実行されたファイルのファイルパス，親プロセス，実行時間，実行時の引数等の情報が取得可能 |
| パケット情報 (STARDUST) | 通信自体は検知可能だが，指令内容は判別不能 |
| プロセス情報 (STARDUST) | 関連する情報は記録されていない |

ということに気付くことは難しいと考えられる．攻撃者に気付かれずに，攻撃者によって発生した通信の内容をリアルタイム又は事後に追うことができる．

## 6.2　STARDUST の問題点及び改善案

### 6.2.1　SSL/TLS 通信の記録

表 1，表 2 及び表 3 内の項番 5-5 に示したとおり，今回の一連の攻撃の中で，攻撃者はクラウドストレージの中に保存していたツール類をダウンロードして使用している．Dropbox をはじめ Google Drive や OneDrive 等のクラウドストレージサービスは多数存在している．これらのサービスの大半は，SSL/TLS 通信によるファイルの送受信を行っており，外部からその通信内容を把握することはできない．

**表 7** に示したとおり，STARDUST が記録するパケット情報だけでは，www.dropbox.com や drive.google.com といった通信先のドメイン名を確認可能だが，通信先ファイル名や通信内容までは把握できない．そのため，今回のように攻撃者がクラウドストレージから攻撃ツールをダウンロードする場合やクラウドストレージにファイルをアップロードする場合，記録したパケット情報からはその攻撃の詳細を観測することができない．なお，攻撃者が被害者端末上のウェブブラウザを直接操作してクラウドストレージに接続する場合は，STARDUST の機能により動作を目視確認することができる．しかしながら，攻撃ツールによっては非表示設定にしたコマンドライン経由でクラウドストレージに接続することが可能であるため，その場合は目視確認は不可能である．

以上のことから，現状の STARDUST の初期設定の機能だけでは攻撃者の通信内容を把握することができず，不十分である．そのため，利用者側が実施できる手法として，STARDUST 環境内に Man-In-The-Middle を行うプロキシを設定することが挙げられる．STARDUST 環境内に PolarProxy[*1]や Burp Suite[*2]といったプロキシツールを導入することにより，より詳細な通信内容の観測が可能となる．

また，SSL/TLS 通信を記録する仕組みのひとつとして NICT では GINTATE[6] の研究開発を進めている．GINTATE が STARDUST に統合されることにより，今後 SSL/TLS 通信の記録についての課題が解決されることが望まれる．

### 6.2.2　仮想環境の確認

表 1 項番 1-3 で示したとおり，今回実施した一連の攻撃動作の中で，攻撃者は侵入した環境が仮想環境かどうかを確認している．この時使用したツールは，一般に公開されている誰でも入手可能なものである．このツールを使用することによって，攻撃者は侵入した環境が仮想環境であると把握することが可能であった．今回の攻撃動作においては，その後も攻撃者による攻撃を続行しているが，侵入したクライアント環境が仮想環境であると気づいた場合，攻撃者はあまり積極的な攻撃活動を行わなくなるか，その環境以外に攻撃対象を変更する可能性が考えられる．

攻撃者に仮想環境であると特定されることは，解析環境であると気づかれることに繋がり長期の観測が困難になる可能性がある．NICT では仮想環境を物理環境と欺瞞する技術の調査およびシステム開発を行っており [7][8]，STARDUST への早期導入が望まれる．

### 6.2.3　Sysmon によるプロセス情報の取得

STARDUST が記録するプロセス情報は，環境内にインストールされているソフトウェアが定期的に稼働中のプロセスを取得し，その中から STARDUST 側で不正ではないと判断されたプロセスを除外した上で表示されている．この仕様により，ipconfig.exe や systeminfo.exe といった情

[*1] PolarProxy Released, NETRESEC, `https://www.netresec.com/?page=Blog\&month=2019-06\&post=PolarProxy-Released`

[*2] Web Application Security, Testing, & Scanning - PortSwi0gger,PortSwigger Web Security, `https://portswigger.net/burp`

報収集を行う実行ファイルは，プロセス起動後に各種情報を表示し，表示後すぐにプロセスを終了してしまうため，偶然プロセス情報取得のタイミングと一致していない限り，STARDUST の機能で稼働していたことを特定することができない．しかし，表 4，**表 5**，表 6 及び表 8 に示したとおり，Sysmon をインストールしていると，攻撃者がどのような攻撃を実行していたのかを高い精度で確認することができる．

特に，今回の一連の攻撃の中で，攻撃者は「収集した情報をパスワードをかけた状態で圧縮し，外部送信後にそれらのファイル類を削除する」という動作を行っている．「Sysmon」が稼働していると，攻撃者がどのようなファイルを狙っていたのか，どのようなパスワードを設定していたのかという情報を取得することができる．このような攻撃者の特徴ともいえる情報をより観測できるようにするためにも，クライアント環境内に Sysmon をインストールしておくことを推奨する．

## 7. おわりに

STARDUST を使用することにより，攻撃者の攻撃活動を観測することが可能であることが確認できた．攻撃者による攻撃の痕跡調査に関しては，STARDUST に標準で備わっている観測機能だけでは確認しきれないものがあるものの，STARDUST 環境内にプロキシソフトウェアを追加したり，クライアント環境内に Sysmon 等のモニタリングソフトウェアを追加したりすることにより，攻撃者の攻撃活動をより詳細に観測することが可能となる．これらの設定を行うことによって，STARDUST 環境をより良く活用することが可能となるだろう．

## 謝辞

本研究を実施するにあたり，国立研究開発法人情報通信研究機構 (NICT) からサイバー攻撃誘因基盤 STARDUST 環境の貸し出しを受けた．ここに感謝する．

### 参考文献

[1] E. Heckman, K., J. Stech, F., K. Thomas, R., Schmoker, B. and W. Tsow, A.: *Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense*, pp. 1–4, Springer International Publishing (2015).

[2] 国立研究開発法人情報通信研究機構：プレスリリース — サイバー攻撃誘引基盤“STARDUST”（スターダスト）を開発 — NICT-情報通信研究機構，https://www.nict.go.jp/press/2017/05/31-1.html.

[3] 寺田真敏：BOS/STARDUST を用いた攻撃者の活動観測 BOS: Behavior Observable System，https://www2.nict.go.jp/csri/plan/H31-symposium/pdf/terada.pdf.

[4] 井上大介：サイバー攻撃誘引基盤 STARDUST 事後対応からリアルタイム対応，https://digitalforensic.jp/wp-content/uploads/2018/03/community2017-05-3inoue.pdf.

[5] 津田　侑：STARDUST による攻撃活動観測と次世代のセキュリティ技術，http://www2.nict.go.jp/csri/plan/H30-symposium/pdf/tsuda.pdf.

[6] Miura, R., Takano, Y., Miwa, S. and Inoue, T.: GINTATE: Scalable and Extensible Deep Packet Inspection System for Encrypted Network Traffic, In Proceedings of the Eighth International Symposium on Information and Communication Technology, *SoICT 2017*, pp. 234–241 (2017).

[7] 岩本一樹，高田一樹，津田　侑，遠峰隆史，井上大介：マルウェアに実装されている仮想マシン検知機能の調査分析，コンピュータセキュリティシンポジウム 2017 (2017).

[8] 高田一樹，岩本一樹，津田　侑，遠峰隆史，井上大介：仮想マシン検知回避機能を持つ動的解析ツールの開発，コンピュータセキュリティシンポジウム 2017 (2017).