STARDUST（サイバー攻撃誘引基盤）

板谷 佳美
Yoshimi ITAYA

1　はじめに

近年，サイバー攻撃が悪質・巧妙になり，その被害が深刻となっている．従来のサイバー攻撃は，無差別型攻撃や脆弱性を突いた攻撃が主流であった．しかし，ここ数年は特定の企業を対象とした標的型攻撃が多くなっている．標的型攻撃は，解析や研究がされていないため，有効な対抗策がない．

そこで，NICT のサイバーセキュリティ研究室は，2011 年に STARDUST の研究開発をはじめ，2017 年 5 月に発表した．STARDUST は，標的型攻撃等の攻撃者を模擬環境に誘引し，その攻撃の挙動を観測・分析するシステムである．STARDUST を使用することで攻撃者の挙動を明らかにし，標的型攻撃への対抗策を打つことができる可能性がある [1)]．

2　STARDUST（サイバー攻撃誘引基盤）

2.1　標的型攻撃

STARDUST は，サイバー攻撃の中でも特に標的型攻撃に対して効果が期待されている．標的型攻撃とは，政府や企業などの特定組織を標的にしたサイバー攻撃である．攻撃者は電子メールに添付したマルウェアによって標的組織内の端末に侵入を図り，外部から情報窃取・破壊を行う．

標的型攻撃の手順を Fig. 1 に示す．

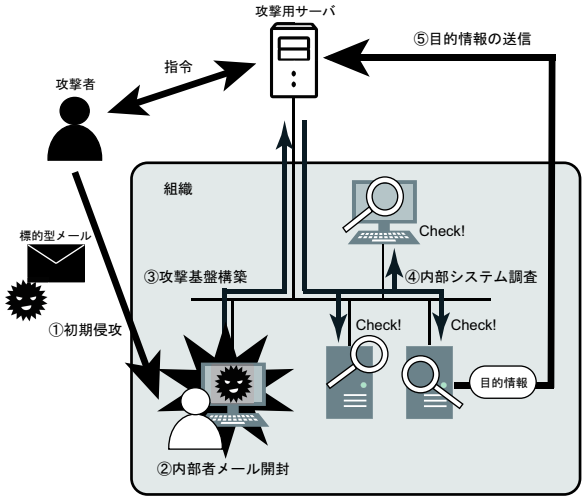

Fig.1　標的型攻撃の手順

まず，事前に入手した特定の組織のメールアドレスにマルウェアを添付したメールを送る．次に組織内部の人が届いたメールを開封し，添付ファイルをマルウェアに気付かず開く．それにより，マルウェアが組織内部の端末に感染し，攻撃者はその端末を乗っ取ることができる．そして，攻撃者は組織のネットワークに外部のサーバである攻撃用サーバを接続する．攻撃者は攻撃用サーバを通して，組織のネットワーク内から目的の情報を探索する．そして目的の情報を発見すると，その情報を攻撃用サーバへ送信する．

2.2　従来の標的型攻撃対策

ここ数年で標的型攻撃が急激に増加し，その被害もまた増えているため，その対策が必要である．従来は，不審なメールへの対処やマルウェアの解析など，Fig. 1 に示した攻撃の初期侵攻の研究と対策を行ってきた．しかし，攻撃者の組織内侵入以降の挙動は，全く分からなかった．理由として，データ収集が困難であることと検証環境が無かったことが挙げられる．

そこで NICT は標的型攻撃研究のために STARDUST を開発した．政府や企業などの組織を精巧に模した大規模インフラの模擬環境上に攻撃者を誘引し，その攻撃者の挙動を観測・分析できるシステムである．これにより，実ネットワークに影響を与えることなく，攻撃者の挙動をリアルタイムに観測し，研究者が分析ができるようになった．

2.3　システム構成と動作手順

STARDUST は，並行ネットワークと環境構築システム，ワームホール，挙動解析システム，解析用データストアで構成される．STARDUST の構成要素について，Table 1 に示す．

Table1　構成要素

要素	概要
並行ネットワーク	組織を精巧に模擬したネットワーク環境
環境構築システム	並行ネットワークの構築と管理
ワームホール	並行ネットワークを実ネットワークの IP アドレスに模擬する機器
挙動解析システム	攻撃者の挙動を解析
解析用データストア	ネットワーク上の挙動ログの保存場所

並行ネットワークは実組織の模擬環境であり，各種サーバーやパソコンを数十台から数百台を稼働できる．環境構築システムは，並行ネットワークの構築と管理運用を行い，数十の並行ネットワークを同時に稼働できる．ワームホールは，攻撃者を実ネットワークから並行ネットワークに誘引する役割を担っている．挙動解析システムは，並行ネットワーク内の攻撃の挙動をリアルタイムで観測し，分析する．解析用データストアは，挙動解析システムで観測・分析されたデータを保存する．

STARDUST のシステム概要図を Fig. 2 に示す．

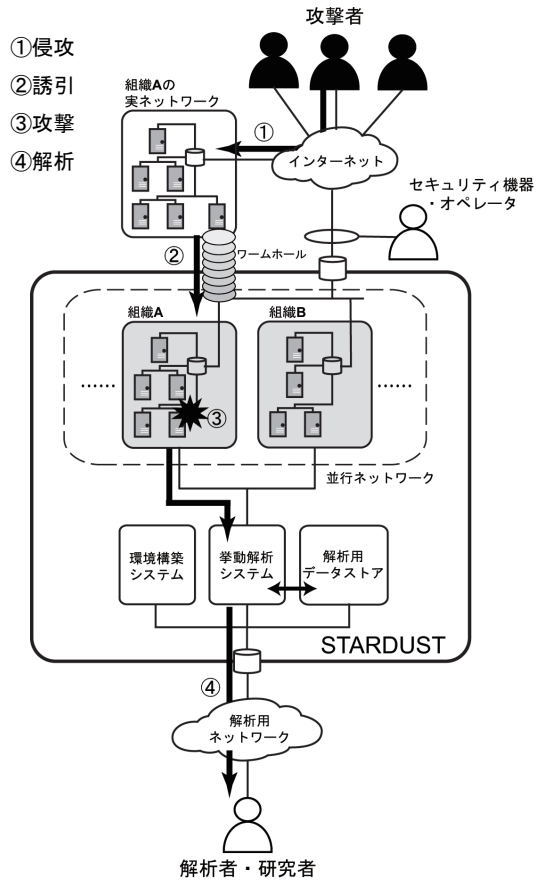

Fig.2　STARDUST のシステム概要

STARDUST によるサイバー攻撃の解析方法は次の通りである．インターネットを通じて組織 A に攻撃者が侵入する．攻撃者を検知すると，ワームホールは攻撃者を並行ネットワーク内の組織 A の模擬環境に移動する．その後，攻撃者はインターネットを通じて，実ネットワークではなく並行ネットワークを攻撃する．これにより，実ネットワークへの影響を無くすことができる．インターネットと並行ネットワーク間の通信は NICT のセキュリティ機器やオペレータが監視する．並行ネットワーク内で生じた攻撃は，挙動解析システムでリアルタイムに観測される．解析者は，挙動解析システムが観測した内容を，解析用ネットワークを通じて研究を行う．

3　STARDUST 運用実験

3.1　実験概要

NICT は，STARDUST の運用実験として，実際に攻撃グループに攻撃させ，解析した．対象となった実在する攻撃グループは，日本を標的にし絶えず攻撃を仕掛けている，Blue Termite と DragonOK の 2 グループである．その解析手順は次の通りである．まず，すでに出回っているマルウェアを入手し解析することで，攻撃者の情報を得る．そして，攻撃用サーバに接続できるか調べる．これは，実際に使用されているサーバであるのか確かめるためである．接続可能であれば，並行ネットワーク上に設置した端末でマルウェアを実行し，攻撃者に並行ネットワークを攻撃をさせる．そして，攻撃者との接続が途切れるまで観測・分析を行う．2015 年から 2016 年にかけて，Blue Termite の攻撃を 1 回，DragonOK の攻撃を 3 回，計 4 回の攻撃について解析を行った [2]．

3.2　実験結果

実験の結果，攻撃者による入力コマンドのログ解析から，次の 4 つのことがわかった．1 つ目は，攻撃者がネットワークや端末の状態を頻繁に調査していたことである．2 つ目はタイプミスを行っていたことである．3 つ目は*や?などの正規表現を用いたコマンド入力を行っていたことである．4 つ目は決まったコマンドで順番に攻撃していたことである．

従来，標的型攻撃は国家が関与した高度な攻撃であると考えられていた．また攻撃者は不用意なネットワークスキャンはせず，侵入先の職員の挙動を把握し慎重に行動するとされていた．しかし，STARDUST 運用実験より，マニュアルに沿った手動攻撃であることがわかった．また，事前にネットワークの状態を把握し攻撃してくるのではないこと，職員が使用しないコマンドを多数使用することが推察された．

これらの結果から，ある一定のログパターン動作監視やネットワークスキャンの調査，プロセスの監視をすることで，標的型攻撃を検知できる可能性が明らかになった．

4　今後の展望

サイバーセキュリティに関して，現在国家プロジェクトとしての推進体制が敷かれている．そのプロジェクトにおいて，STARDUST は IoT セキュリティ総合対策の研究開発推進における，基礎的，基盤的な研究開発の一環である．

NICT で行われた STARDUST 運用実験では，実ネットワークを模擬した並行ネットワークの作成とワームホールによる並行ネットワークへ誘引のプロセスが行われなかった．したがって，まず Fig. 2 に示したシステムで STARDUST の運用実験を行い，その後，実環境で稼働する必要がある．そのためには，各構成要素の機能を向上させることが必要だと考える．そしてさらに，標的型攻撃の新たなる手法や別の攻撃についても解析できるような研究基盤に発展していくと考える．

参考文献

1) サイバー攻撃誘引基盤“STARDUST”（スターダスト）を開発—NICT，
https://www.nict.go.jp/press/2017/05/31-1.html，参照 Apr.11, 2018
2) STARDUST による攻撃活動観測と 次世代のセキュリティ技術—NICT，
http://www2.nict.go.jp/csri/plan/H30-symposium/pdf/tsuda.pdf，参照 Apr.11, 2018