国立研究開発法人
情報通信研究機構

プレスリリース
2017年5月31日
国立研究開発法人情報通信研究機構

サイバー攻撃誘引基盤“STARDUST”（スターダスト）を開発

～標的型攻撃の攻撃者を模擬環境に誘い込み、長期挙動分析を可能に～

【ポイント】

- 標的型攻撃等の攻撃者を誘い込むための模擬環境“並行ネットワーク”を高速に自動構築
- 企業を精巧に模した“並行ネットワーク”内で、攻撃者の挙動をステルスに長期分析可能に
- 今後、攻撃誘引の結果はセキュリティ関連組織等と共有し、日本のセキュリティ向上に貢献

国立研究開発法人情報通信研究機構（NICT、理事長：徳田　英幸）サイバーセキュリティ研究室は、標的型攻撃等のサイバー攻撃対策として、政府や企業等の組織を精巧に模擬したネットワークに攻撃者を誘い込み、その攻撃活動を攻撃者には察知できないよう（ステルス）に長期観測することで、従来では収集が困難であった攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能にするサイバー攻撃誘引基盤「STARDUST」（スターダスト）を開発しました。

STARDUSTについては、2017年6月7日（水）～9日（金）に幕張メッセで開催される「Interop Tokyo 2017」で動態展示を行います。（https://www.interop.jp/）

【背景】

標的型攻撃に代表される政府や企業等の組織を狙ったサイバー攻撃では、組織への初期侵入に際し、メール等に添付されたマルウェア（不正プログラム）が使用されます。侵入後は感染したマルウェアが裏口（バックドア）として使われ、攻撃者による手動の攻撃活動が組織のネットワーク内部で進められます。そのため、標的型攻撃に用いられるマルウェアを解析するだけでは、組織への初期侵入という表層的な情報しか得られませんでした。

また、標的型攻撃の被害に遭った組織から、自組織の機微情報や不利益情報が含まれる可能性がある攻撃関連のデータが公表されることは非常に稀であるため、実データセットが不足しており、そのことが、標的型攻撃対策技術の研究開発を更に難しくしていました。標的型攻撃対策の実践的な研究開発を行うためには、マルウェア感染後の攻撃者の挙動を含む標的型攻撃の実データセットを自ら作り出せる研究基盤が必要となっていました。

【今回の成果】

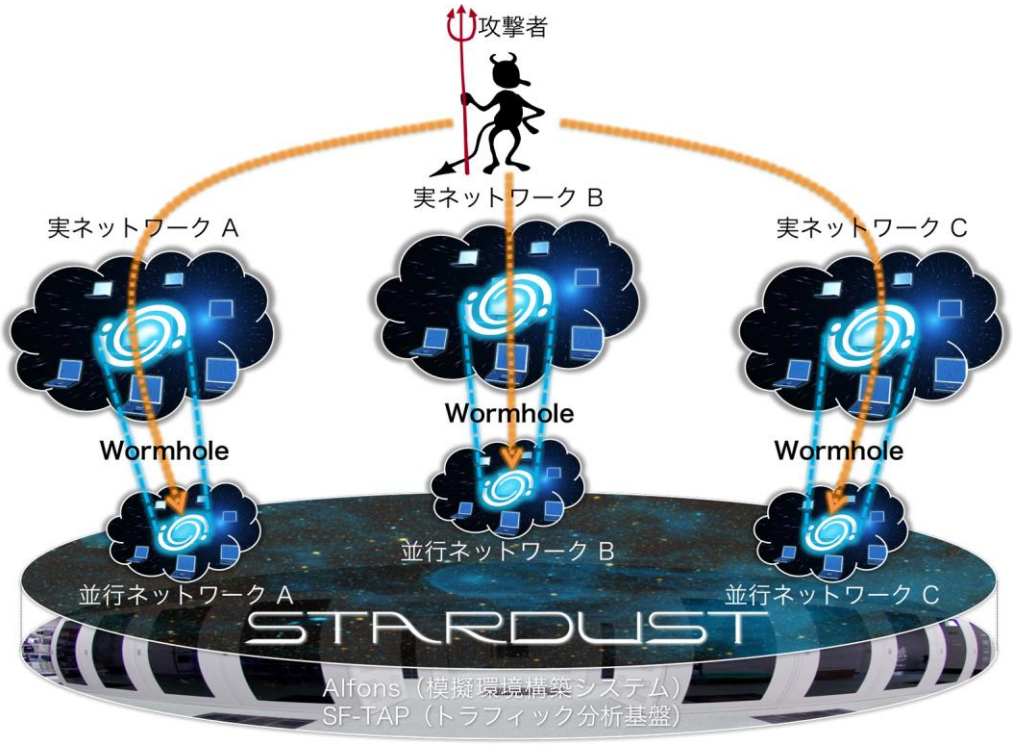

図1 STARDUST

NICT は、標的型攻撃等の攻撃者を誘い込み、その攻撃活動を長期観測することを可能にするサイバー攻撃誘引基盤「STARDUST」（スターダスト）を開発しました（図 1 参照）。STARDUST は、政府や企業等の組織を精巧に模擬したネットワークである「並行ネットワーク」を柔軟かつ高速に（数時間程度で）構築することが可能です。並行ネットワーク上では、各種サーバ（Web サーバ、メールサーバ、ファイルサーバ、DNS サーバ、認証サーバ、プロキシサーバ等）や数十台～数百台の PC が実稼働し、さらに、サーバや PC には組織の情報資産を模した模擬情報が配置され、あたかも実在の組織のように振る舞います（補足資料 図 2 参照）。

並行ネットワーク上の PC「模擬ノード」で標的型攻撃に用いられるマルウェア検体を実行すると、マルウェアが設けたバックドアを経由して攻撃者が外部から接続を試みます。並行ネットワークに侵入した攻撃者は、調査行為や感染拡大行為、情報窃取等を試みます。STARDUST は、このような攻撃者の挙動を攻撃者には察知できないステルス性の高い手法で観測し、リアルタイムの挙動観測・分析を可能にします（補足資料 図 3、図 4 参照）。

STARDUST を用いて攻撃誘引を行うことで、標的型攻撃の実データセットを作り出し、対策技術の研究開発を大きく進展させることが期待できます。

なお、STARDUST は NICT に加え、下記の組織の研究者、技術者、解析者の協力を得て、研究開発を進めています。

株式会社富士通研究所、株式会社サイバーディフェンス研究所、株式会社セキュアブレイン、株式会社ニッシン、株式会社日立製作所、株式会社日立システムズ、日本電信電話株式会社 NTT セキュアプラットフォーム研究所、エヌ・ティ・ティ・アドバンステクノロジ株式会社（順不同）

【今後の展望】

今後、STARDUST による攻撃誘引の結果を標的型攻撃対策技術の研究開発に活用するとともに、セキュリティ関連組織等と適宜共有し、日本のセキュリティ向上に貢献していきます。

また、STARDUST 上の並行ネットワークは複数同時並行で稼働させることが可能であり、セキュリティ関連組織の分析活動における STARDUST の活用を進めていきます。

STARDUST については、2017 年 6 月 7 日（水）～9 日（金）に幕張メッセで開催される「Interop Tokyo 2017」（https://www.interop.jp/）で動態展示を行います。

＜用語解説＞

*1 Alfons: 高速・精巧な模擬環境構築システム

S. Yasuda, R. Miura, S. Ohta, Y. Takano, and T. Miyachi, “Alfons: A Mimetic Network Environment Construction System,” 11th EAI International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TRIDENTCOM 2016), 2016.

*2 SF-TAP: 柔軟・スケーラブルな汎用 L7 トラフィック解析基盤

Y. Takano, R. Miura, and S. Yasuda, K. Akashi, T. Inoue, “SF-TAP: Scalable and Flexible Traffic Analysis Platform Running on Commodity Hardware,” USENIX LISA15, 2015.

＜ 本件に関する問い合わせ先 ＞
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
井上 大介、津田 侑
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

＜ 広報 ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

補足資料

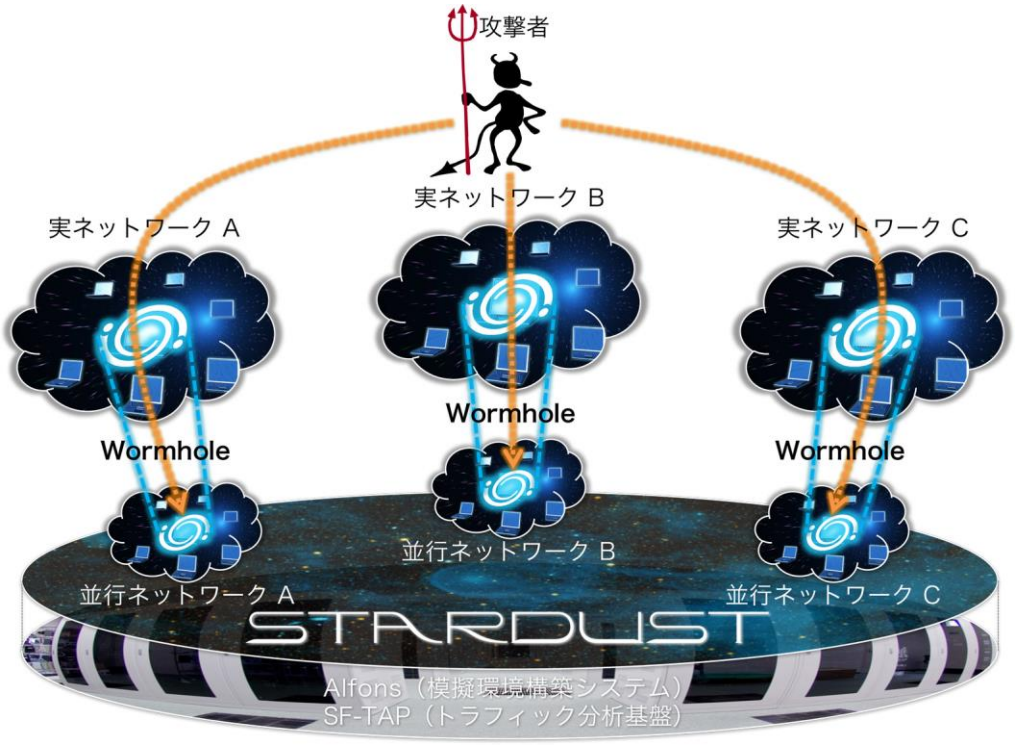

図 1 STARDUST（再掲）

標的型攻撃の攻撃者を模擬環境である並行ネットワークに誘引し、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・分析可能なサイバー攻撃誘引基盤。実ネットワークと並行ネットワークを、Wormhole（ワームホール）と呼ばれる VPN（仮想プライベートネットワーク）と多段 NAT（ネットワークアドレス変換）を組み合わせたネットワーク機器で接続することで、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ことができ、更に高度な模倣も可能である。

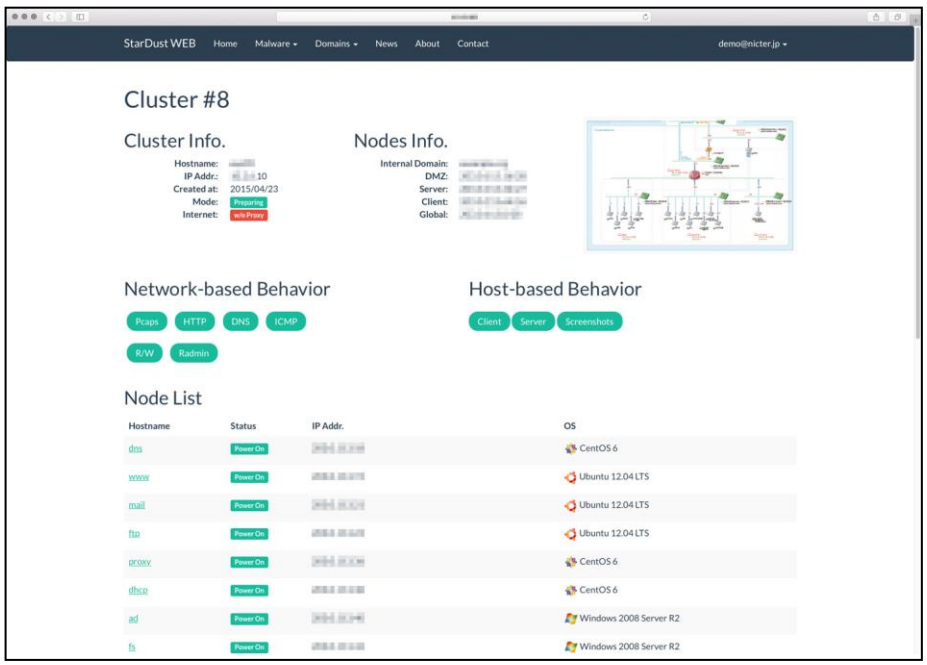

図 2 並行ネットワーク

模擬環境構築システム「Alfons」[*1] によって、各種サーバや数十台～数百台の PC を含む並行ネットワークが数時間程度で自動構築可能である。STARDUST では複数の並行ネットワークを同時稼働できる。

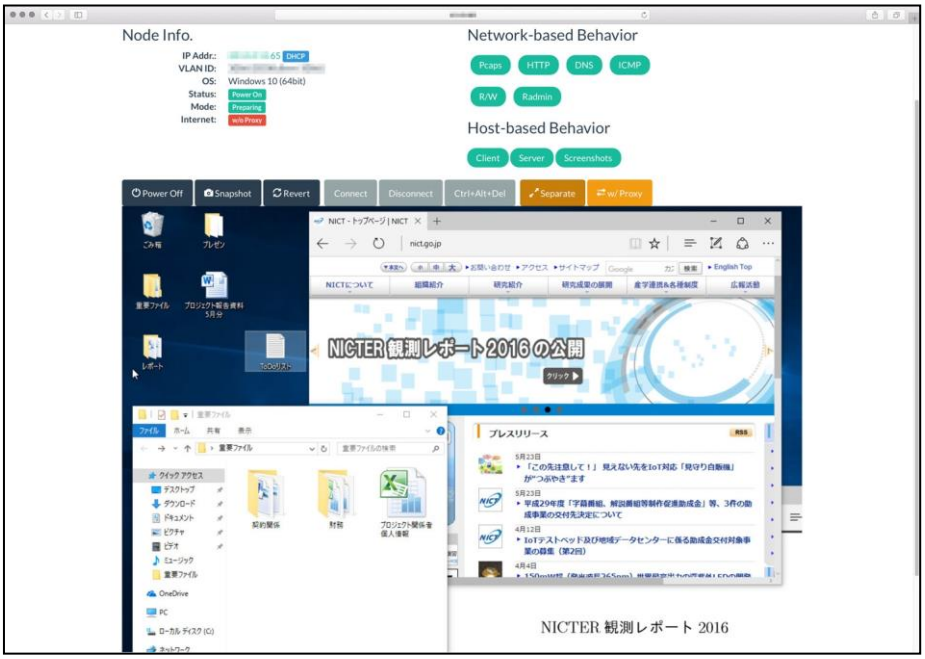

図 3 模擬ノード

並行ネットワーク内の模擬ノード上で標的型攻撃に用いられるマルウェア検体を実行し、攻撃者を外部から誘引する。模擬ノードは STARDUST の Web インターフェースである「STARDUST Web」によって集中制御が可能である。

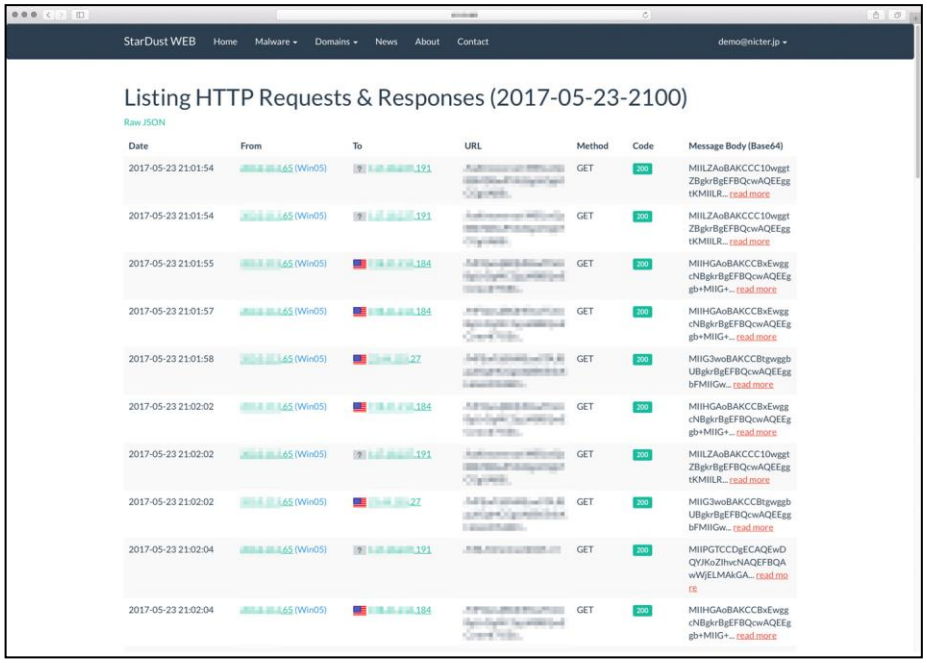

図 4 ステルス観測・分析

トラフィック解析基盤「SF-TAP」[*2] によって、攻撃者が察知できない並行ネットワークの外側から、攻撃者が送受信したパケットを観測し、通信内容を高速に再構成・分析可能である。