サイバーセキュリティの可視化技術*

井上 大介**

Visualization Technologies on Cybersecurity

Daisuke INOUE

1. はじめに

インターネットの進歩・発展の陰で、インターネットを経由したサイバー攻撃も日々大規模化と高度化を続けており、重大な社会問題となっている。本稿では、サイバー攻撃対策を目的としたサイバーセキュリティ分野の可視化技術について、著者らの研究グループが取り組んでいる「インシデント分析センタ NICTER」とそのスピンオフ技術を中心に紹介する。

2. インシデント分析センタ NICTER

NICTER¹⁾²⁾ (ニクター) はインターネットの広範に影響を及ぼすワーム型 (自己増殖型) マルウェアの大局

的な活動傾向を観測・分析するための複合的なシステムである。

NICTER は、ダークネットと呼ばれる未使用の IP アドレス空間の大規模観測 (本稿執筆時点で約 30 万アドレス) を行っている。未使用の IP アドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においては稀であるが、実際にダークネットを観測してみると、相当数のパケットが到着することが分かる。これらのパケットの多くは、ワーム型マルウェアが感染拡大する際に、攻撃対象を自動探索するためのスキャンと呼ばれる通信である。そのため、ダークネットに到着するパケットを大規模に観測・分析することで、マルウェアの大局的な活動傾向の把握が可能になる。

Fig. 1 Atlas.

* 原稿受付 2016 年 1 月 26 日

** 非会員 国立研究開発法人 情報通信研究機構
(〒184-8795 東京都小金井市貫井北町 4-2-1,
E-mail: dai@nict.go.jp)

この膨大なダークネットトラフィックの大局的な傾向や変化を捉えるため、データマイニングや機械学習を応用した様々な自動分析エンジンを開発するとともに、人間の分析者の迅速な「気付き」を促すリアルタイム可視化エンジンを開発している。サイバーセキュリティは大量の通信や、各種セキュリティ機器やセキュリティ対策ソフトウェアが生成するログやアラートなど、ビッグデータとの戦いであり、可視化技術はその効率化をサポートするとともに、非専門家のセキュリティウェアネス向上にも役立つものである。

以降では、NICTER およびそのスピンオフ技術のリアルタイム可視化エンジンについて概説する。

2.1 Atlas

Atlas (Fig. 1) は、ダークネットトラフィックを世界地図上でリアルタイムにアニメーション表示する可視化エンジンである。ダークネットに到着したパケットの1つ1つについて、送信元 IP アドレスから送信元の緯度・経度を割り出し、その送信地点から宛先 IP アドレスが属する国の首都にパケットが飛来する様子をアニメーション表示することで、世界的なマルウェアの活動傾向を直感的に把握することができる。各パケットの色はパケットの種別を表し、パケットの軌道の高さはポート番号の大きさに比例（対数軸）している。また、マウス操作による視点の変更や拡大縮小、パケットオブジェクトのクリックによる詳細情報の表示など、分析者のインタラクティブな操作を可能にしている。

2.2 Cube

Cube (Fig. 2) は、ダークネットに到達したパケットを、その送信元と宛先の各種情報に基づいて、三次元空間に浮かぶ立方体中にアニメーション表示する可視化エンジンである。立方体の縦軸に送信元/宛先 IP アドレスを、横軸に送信元/宛先ポート番号を取り、送信元 (Fig. 2 の左平面) から宛先 (Fig. 2 の右平面) に向けてパケットを通過させることで、スキャンなどの形状が可視化される。Cube は Atlas と同様、マウス操作による視点の変更や拡大・縮小、パケットの詳細情報の表示などが行え、送信元ホストからの攻撃の様子をリアルタイムに把握することが可能であり、分析者が詳細な分析を開始するためのトリガとして非常に有用である。

Fig. 2 Cube.

2.3 Tiles

Tiles (Fig. 3) はダークネットトラフィックを送信元ホストごとにスライスし、各ホストの短期間 (30 秒間) の挙動を分析・可視化するエンジンである。Fig. 3 の小さなタイルの1つ1つが送信元ホスト毎の挙動を表しており、最新の分析結果に随時更新されていく。タイルの裏側は送信元ホストが属する国の国旗が示されている。1つのタイルは、ある送信元ホストが30秒間に送出したパケットの時刻、送信元/宛先ポート番号、宛先 IP アドレスを用いて Fig. 4 の様に可視化される。ここで、1つのパケットは送信元 (左半面) と宛先 (右半面) を結ぶ1本の線で表現されている。Fig. 4 は送信元ポート番号を増加させながら、複数の宛先 IP アドレスの単一宛先ポートに TCP SYN パケットを送信するネットワークスキャンの典型的なパターンである。

Fig. 3 Tiles.

Fig. 4 Details of a tile.

3. 対サイバー攻撃アラートシステム DAEDALUS

DAEDALUS³⁾ (ダイダロス) は、NICTER の大規模ダークネット観測網を応用したアラートシステムである。その動作原理は非常にシンプルであり、特定の組織内でサーバやホストが使用している IP アドレス空間 (以下、ライブネット) から、NICTER の観測網にパケットが送信されると、当該組織に向けてアラートを発行する。Fig. 5 は DAEDALUS のアラート発行状況を俯瞰的に把握するための可視化エンジン DAEDALUS-VIZ である。

Fig. 5 DAEDALUS-VIZ.

Fig. 5 の中央の球体がインターネット，その周りを周回している各リングが，NICTER のセンサを設置している組織のネットワークを表している．球体とリングの間を飛び交う流星状のオブジェクトはダークネットトラフィックを表している．リングの水色部分がライブネット，濃紺部分がダークネットであり，リングの外周の「警」のマークは組織内でアラートの原因となった送信元ホストを指し示している．

新規アラートの発生時には，注意喚起のため Fig. 6 のように警告アイコンが画面上に拡大表示される．

Fig. 6 New alert.

Fig. 7 は，ある組織でマルウェア感染が発生した際の，組織内感染活動の実例である．組織内のライブネットの 1 点（感染ホスト）から大量のスキャンがダークネット部分に到着している様子が確認できる．

Fig. 7 Internal scan by a malware infected host.

この DAEDALUS-VIZ 上でのアラート表示と同時に，該当組織にはメールベースのアラートが自動送信され，実際のセキュリティオペレーションのトリガとして活用されている．

4. サイバー攻撃統合分析プラットフォーム NIRVANA 改

NICTER は大規模ダークネット観測網を用いて，マルウェアによる無差別型のサイバー攻撃に関連した通信を観測・分析するための中央集中型のシステムである．一方，2011 年に国内の防衛企業への侵入と情報窃取を契機に明るみになった「標的型攻撃」は，特定の組織をターゲットに絞って攻撃を行うため，NICTER のような大規模観測網では捉えられないサイバー攻撃であり，現在も重大な脅威となっている．

Fig. 8 NIRVANA-KAI.

NIRVANA 改（ニルヴァーナ・カイ）は、このような標的型攻撃に対抗するため、組織内部にセンサを設置し、ライブネットを流れるトラフィックをリアルタイムに観測・分析・可視化するとともに、各種のセキュリティ機器からのアラートを集約・可視化する統合分析プラットフォームである。

Fig. 8 は NIRVANA 改のネットワークビューであり、IPv4 のインターネット空間全体（/0 ネットワーク）を 256 個のアドレスブロックに分割して平面状に配置している（すなわち、1 ブロックが 1 つのクラス A アドレスに対応している）。

Fig. 9 Drill down into an infected host.

アドレスブロック上を流れる三角錐は、観測対象の組織が組織外のアドレスブロックと送受しているパケットをリアルタイムに可視化したものである。アドレスブロックの直上に位置する六角形は、各種のセキュリティ機器から集約されたアラートを表しており、そのアドレスブロックの内部に異常が検知されたホストが存在していることを意味している。

Fig. 9 はインターネット空間全体のビューから、クラス A アドレス（/8 ネットワーク）、クラス B アドレス（/16 ネットワーク）、クラス C アドレス（/24 ネットワーク）と、アラートの発生源に向かって順次ドリルダウンしていき、最終的に 1 つのホストの内部（ホストビュー）まで到達する過程を示している。

Fig.10 はホストビューの詳細を示している。ホストビュー中央に位置するモニタの表面には、このホストの OS 情報やユーザ情報、MAC アドレスやプロセス数などの一般情報が表示されている。モニタの周囲を回るクリスタル型のオブジェクトは、現在実行中のプロセスを表している。最外縁のハイライトされたクリスタルは、マルウェアとして検出されたプロセスであり、そのプロセスが実行されるまでのプロセスの親子関係であるコールツリーを表している。マルウェア感染プロセスから外部に向けて TCP セッションが確立している様子も可視化されており、これは外部の攻撃者が組織内のマルウェア感染ホストに攻撃指令を出すための C&C（Command & Control）サーバとの通信である。

Fig.10 Host view.

Fig.11 は NIRVANA 改の自動防御機能を使って、マルウェアの大量感染が確認されたクラス C ネットワークを、組織内ネットワークから隔離した様子を可視化している。このクラス C ネットワーク内のホストから送信されたパケットが六角形のバリア状のオブジェクト（この例では自動設定されたファイアウォールルール）によって遮断されている様子を表している。

5. おわりに

無差別型攻撃から標的型攻撃まで、サイバー攻撃の手法は多岐に渡り、かつその進化は早く、全ての攻撃を未然に防ぐ単一の防御策の存在は最早幻想となっている。そのため、現在では様々な防御策を組み合わせ、総合的に組織のセキュリティを高めることが肝要であり、インシデント発生時には迅速な検知や対策を行えるシステム

設計が求められている。その際、複数のセキュリティ機器やセキュリティ対策ソフトウェアから出される大量のログやアラートを集約し、如何に効率的に処理するかが、有効なセキュリティオペレーションの鍵を握っている。人間の視覚情報処理能力を活かすための可視化技術によって、オペレーションの効率化と簡易化を図り、次世代の実践的なセキュリティオペレーションを確立することが喫緊の課題である。

参考文献

- 1) Nakao, K., Inoue, D., Eto, M., Yoshioka, K.: Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks based on Darknet Monitoring, IEICE Trans. Information and Systems, Vol.E92-D, No.5, pp. 787-798, 2009.
- 2) Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K., Nakao, K.: nict: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis, WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 58-66, 2008.
- 3) Inoue, D., Suzuki, K., Suzuki, M., Eto, M., Nakao, K.: DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System, 9th International Symposium on Visualization for Cyber Security (VizSec 2012), pp. 72-79, 2012.

Fig.11 Containment of a /24 network.