1-403-45
2017/3/2

一般利用者がコンピュータへのサイバー攻撃の脅威を実感するための通信可視化システムの構築

加藤里奈[†1]　森博志[†2]　吉岡克成[†3]　村山優子[†1]

概要：近年,コンピュータの通信は膨大なものとなっている.そのため,一般利用者は自分のコンピュータがどのような通信を行っているのか把握することは困難である.また,一般利用者があまり通信状況を把握できていないことから,自分のコンピュータが常に脅威に晒されていると実感していないと考えた.そこで,Google Maps と円グラフを用いて通信状況や通信プロセスの可視化を行い,一般利用者が専門知識を必要とせずにコンピュータにおけるサイバー攻撃の脅威を実感できるシステムを構築した.

A Construction of Communication Visualizing System for the General User to Realize the Threat of Cyber Attacks

RINA KATO[†1]　HIROSHI MORI[†2]
KATSUNARI YOSHIOKA[†3]　YUKO MURAYAMA[†1]

Abstract: Recently, a communication of computers has been increasing. Therefore, it is difficult for the general user to grasp the communication of their computers. Also, because the general user cannot grasp a communication status, we thought the general user hardly realized that their computers were exposed to the threat of cyber attacks. We visualized a communication status and communication processes using Google Maps and pie chart and constructed a visualizing system for the general user to realize threats of cyber attacks without specialized knowledge.

1. はじめに

現在インターネットは利用者の生活にとって身近な存在かつ便利なものとなっている.それにも関わらず自分のコンピュータがどのような通信を行っているか正確に把握している利用者は少ない.特にここ数年で SNS,インターネット広告そして動画配信サイトが急速に普及しているため,コンピュータの通信量は膨大なものとなっている.そのため,自分のコンピュータがどのような通信を行っているのか把握することは困難である.また,ネットワークに詳しくない一般利用者は自分のコンピュータが大量の通信を受信・送信している事を知らないという点に着目した.このままでは自分のコンピュータが常にサイバー攻撃の脅威に晒されている事を実感できない.

そこで,本研究の対象者がネットワークやセキュリティに詳しくない一般利用者という点を踏まえて,専門知識を必要とせずに,個人のコンピュータが常にサイバー攻撃の脅威に晒されていると実感できる事を目的とし, 個人のコンピュータがどのような通信を行ったか効率良く把握できる通信可視化システムを構築した.

†1 津田塾大学
Tsuda College
†2 横浜国立大学大学
Yokohama National University
†3 横浜国立大学大学院環境情報研究院/先端科学高等研究院
Graduate School of Environment and Information Sciences/Institute of Advanced Sciences, Yokohama National University

2. 関連研究

個々のコンピュータが行う通信の可視化に関する先行研究として文献[1]や文献[2]がある.文献[1]では長期間行われていた通信を可視化することでマルウェアの動的解析を支援するシステムが提案されている.文献[1]の提案手法にはグラフビューと世界地図ビューがある.グラフビューでは宛先ポート番号ごとに単位時間当たりの通信量を折れ線グラフで可視化しており,世界地図ビューではマルウェアの犠牲ホストとその通信先を世界地図上で線を結び可視化している.位置情報を元に個人のコンピュータにおける通信を世界地図上に可視化するという点で本研究と類似しているが,文献[1]ではマルウェアの通信のみを対象としているため,一般利用者の操作による通信は可視化対象としていない.さらに文献[1]で提案しているシステムの対象者がマルウェア解析者のため,ネットワークやセキュリティの専門知識が乏しい一般利用者にとって可視化内容を理解する事は簡単ではない.また,より一般利用者が通信内容を把握できるよう通信を行っていたプロセスの可視化も行った.文献[2]では一般利用者のセキュリティ意識向上を目的としたパケットヘッダの可視化が提案されている.文献[2]の提案手法にはクライアントとサーバ間における通信の流れをアニメーションでの表示,さらにポート番号に対応した通信量をグラフで表示する手法が取られている.一般利用

© 2017 Information Processing Society of Japan

者を対象者としコンピュータにおける通信内容を可視化している点では類似しているが,文献[2]では通信量の可視化に焦点を当てている.また,個々のコンピュータ通信を可視化しているわけではないが,通信の可視化を行っている先行研究としてシステム[3]をあげる.システム[3]は情報通信研究機構が開発した可視化システムで,ダークネットと呼ばれる未使用の IP アドレス空間で観測した通信を世界地図上に可視化している. 世界地図を用いて通信の可視化を行っている点で類似しているが,システム[3]はダークネットへ届く一方向の通信を可視化している点が異なる.

3. 提案手法

本研究では一般利用者を対象としているため専門知識を必要としないシンプルな可視化システムを目指す.提案手法には以下の特徴がある.

- 通信先サーバと通信している様子を世界地図に矢印で描く(世界地図可視化ページ)
- 通信先サーバ上に立っているマーカーにポート番号情報を付随(世界地図可視化ページ)
- ポート番号説明表(世界地図可視化ページ)
- 通信プロセスを個数ごとに円グラフで表示(円グラフ可視化ページ)

3.1 世界地図可視化ページ

世界地図可視化ページでは以下に記載する 2 種類の通信をそれぞれ可視化している.

- コンピュータからサーバへ送られる通信
- サーバからコンピュータへ送られる通信

上記の通信をパケットキャプチャツールで取得し,MaxMind 社[4]が提供する取得データと IP アドレスに対応している位置情報データベースである GeoLite2 City を元にコンピュータの通信先を Google Maps 上に矢印で描く.シンプルなシステムという点を踏まえてパケット単位ではなくフロー単位で通信の可視化を行っている.一例として世界地図可視化結果を図 1, 図 2 に示す.図 1 では正規の web サイトである楽天市場(www.rakuten.co.jp)を閲覧していた時の通信状況で,図 2 は morto というマルウェアに感染した時の通信状況である. morto はワーム型のマルウェアであり,感染してしまうとさらに感染を広めるため無作為に多数の通信先を選びアクセスを試みる.提案手法により,この様子が直感的に表現されている。

図 1 世界地図可視化ページ表示例(正規)
Figure 1 The example of visualization on map(Proper)

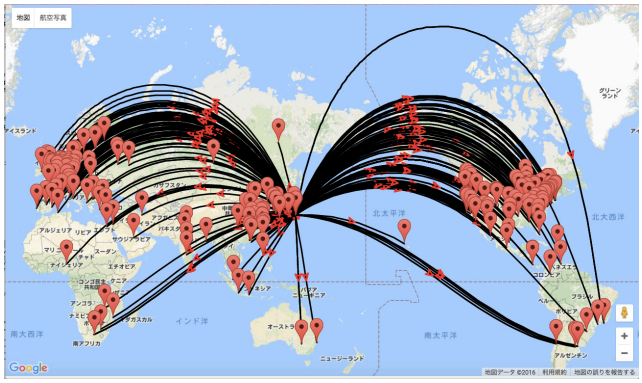

図 2 世界地図可視化ページ表示例(マルウェア)
Figure 2 The example of visualization on map(Malware)

また,ズームインすることで通信先サーバの所在地の詳細も把握することができるようにした.

さらに,通信先サーバの所在地上に立っているマーカーをクリックするとポート番号が表示される.しかし,ネットワークにあまり詳しくない一般利用者はポート番号のみを表示されても理解できない.そこで,世界地図の下にポート番号の説明表を表示する(表 1).

Port番号	説明
23	遠隔操作[telnet]
25	メール転送[smtp]
80	webサイト閲覧[HTTP]
443	webサイト閲覧(セキュア)[HTTPS]

表 1 世界地図可視化ページ ポート番号説明表
Table1 The instruction of the number of ports

3.2 円グラフ可視化ページ

円グラフ可視化ページでは,コンピュータ上で TCP 通信を行っていたプロセスの個数を元に円グラフで表示する.凡例部分にプロセス名と個数を記載した.一例として図 3

© 2017 Information Processing Society of Japan

に円グラフ可視化結果の一例を示す.

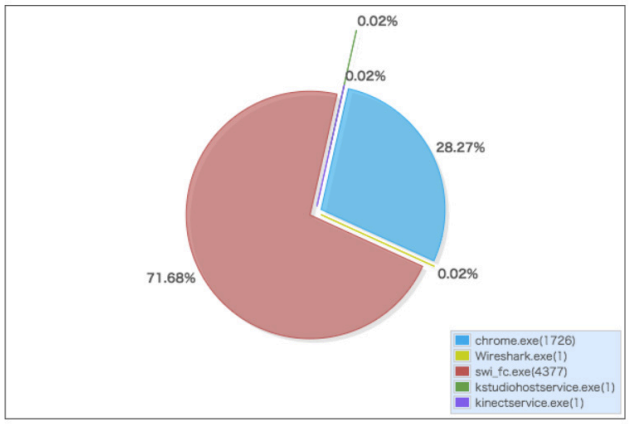

図 3　起動プロセスの可視化例

Figure3　The example of showing running process

4. 通信可視化システムの実装

提案手法を元に Web アプリケーションとして通信可視化システムを実装した.本システムのシステム構成を図 4 で示す.

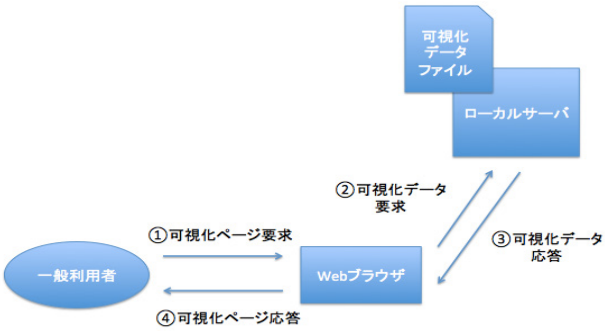

図 4　システム構成図

Figure4　System configuration

4.1 通信データ取得

4.1.1 世界地図可視化ページ

可視化するデータを Wireshark で PCAP ファイルとして取得する.

4.1.2 円グラフ可視化ページ

可視化するデータを Process Monitor を用いて CSV ファイルとして取得する.

4.2 通信データ処理

4.2.1　世界地図可視化ページ

tcpflow を用いて,取得した PCAP ファイルからポート番号と IP アドレスを抽出し,さらに MaxMind 社が提供している GeoIP2 Python API を使用して IP アドレスから位置情報へ変換する.

4.2.2 円グラフ可視化ページ

4.1.2 で取得したデータから TCP 通信を行っていたプロセスのみを抽出する.

4.3 可視化画面

世界地図可視化ページでは Google Maps JavaScript API[5] を用いて世界地図,アニメーションの矢印,マーカーを実装する.円グラフ可視化ページでは JavaScript のライブラリである Frotr2 を用いて実装する.

5. まとめと今後の課題

本提案システムによって通信プロセス名や個人のコンピュータがどこの国のサーバと通信を行っているのかを一瞬で把握することができた.また,正規の通信とマルウェアの通信を見比べると,どちらがマルウェア通信を可視化しているものか専門知識を必要とせずとも容易に理解できたと考えている.しかし通信先の国だけを把握できても,どんなサーバと通信をしていたのか理解することができない.そのため,通信先だけでなくドメイン名も一緒に表示することが必要である.また今回は線と矢印のアイコンで通信状況を表したが,線の色をポート番号ごとに変えたり,どのような通信かアイコンをつけて示したりと直感的に分かりやすく通信状況を把握できる方法に関してはまだ検討の余地があると考えている.今後,さらに一般利用者がコンピュータの通信を把握できるよう,このような機能を追加することを今後の課題とする.

参考文献

[1] 森博志, 吉岡克成, 松本勉:長期間のマルウェア動的解析を支援する通信可視化手法とユーザインタフェースの提案, 情報処理学会研究報告会, vol.2012-CSEC-58 No.38, vol.2012-SPT-4 No.38, pp.253-260
[2] 王亮, 白井春彦, 黒岩丈介, 小高知宏, 小倉久和:エンドユーザのセキュリティ意識向上を目指したパケットヘッダ可視化システム, 福井大学大学院工学研究科研究報告第 57 巻, pp.47-52, 2009
[3] NICTER, http://www.nicter.jp/
[4] MaxMind, https://www.maxmind.com/ja/home
[5] Google Maps API, https://developers.google.com/maps/?hl=ja

© 2017 Information Processing Society of Japan