マルウェア感染によるダークネットパケットへの影響について

樫木 惟人[1]　古本 啓祐[1]　森井 昌克[1]　池上 雅人[2]　長谷川 智久[2]　石川 堤一[2]　中尾 康二[3]

概要：先に，我々は複数の国家におけるダークネットに到達するパケットの解析を行った．それぞれの国に到達するダークネットパケットについて時系列分析を行い，攻撃側 IP の分類とその攻撃ツールの推定を行った．その結果，Morto 等のマルウェアによる攻撃およびスキャンが多数見られ，マルウェア感染による攻撃の拡大，自動化が対策への課題となることが示された．本稿では，まずマルウェアの発生状況について，その時系列分布を与える．このデータはセキュリティ対策ベンダの各国でのマルウェア検出センサの結果を利用している．さらに，複数国家でのダークネットパケットの到達状況およびそのデータから得られる，それら複数国家からのアウトバウンドパケット（複数国家で観測された特定国家からのパケット）の状況を与える．最後に，それらの国におけるマルウェアと，そのマルウェアが影響しているであろうダークネットパケットとの関係を与える．

キーワード：ダークネット, マルウェア, 相関解析

The Effect of the Malware Infection on the Darknet Packets

Korehito Kashiki[1]　Keisuke Furumoto[1]　Masakatu Morii[1]　Masato Ikegami[2]
Tomohisa Hasegawa[2]　Teiichi Ishikawa[2]　Koji Nakao[3]

Abstract: Previously, we analyzed the packet to reach the darknet in multiple national. By carrying out the time-series analysis to darknet packet, we went the classification of the attacking IP and an estimate of the attack tools. As a result, attacks and scan by malware such as Morto were observed in a large number, expansion and automation of attack by malware infection was shown to be a challenge to measure. In this paper, first, we show the time series distribution of malware of occurrence. This data is utilizing the result of the malware detection sensor in each country of the security vendor. Secondly, we give the status of the outbound packets from the data of the darknet packet with multiple national. Finally, we provide the relationship between malware in their countrythe and darknet packet in the malware has affected.

Keywords: Darknet, Malware, Correlational Analysis

1. はじめに

近年，インターネットが広く普及したことに伴い，世界中でサイバー攻撃が増加している．多くのコンピュータがインターネットに常時接続されており，セキュリティ対策が不十分な場合はクラッカーやマルウェアの脅威に晒されることになる．サイバー攻撃を受けた場合，過負荷によるサービスの停止や情報漏洩，Web 改ざんといった被害が発生する．さらに，DoS 攻撃の踏み台となる恐れもある．企業や国家機関においてもサイバー攻撃による情報漏洩の被害が報告されており，サイバー攻撃への対策は急務である．サイバー攻撃への対策には，不正トラフィックの検知やマルウェアの攻撃傾向の解析などが挙げられる．不正ト

[1] 神戸大学
Kobe University
[2] キヤノン IT ソリューションズ株式会社
Canon IT Solutions Inc.
[3] 情報通信研究機構
National Institute of Infomation and Communication Technology

ラフィックの検知手法の一つにダークネット観測が挙げられる．ダークネットの未使用の IP アドレス群を利用した観測を行うことにより，不正な通信を効率良く見つけることが可能である．PRACTICE[1] と呼ばれるプロジェクトでは，異なる地域に存在する複数のダークネットの観測データを利用した攻撃解析が行われている．PRACTICE におけるダークネットの膨大な量のトラフィックデータを効率的に解析し，攻撃傾向やスキャンツールを分類する手法 [2][3][4][5] が提案されている．マルウェアの攻撃傾向の解析では，ESET[7] においてマルウェアの脅威に関する国別の観測情報が公開されている．ESET の公開情報には日毎や月毎の時系列データや各マルウェアの観測日が含まれている．また，マルウェアのスキャンアルゴリズムに着目した攻撃元のプロファイリング及び分類手法 [6] が提案されている．

本稿では，PRACTICE におけるダークネットのトラフィックデータと ESET の観測データを利用して，マルウェア感染がダークネットのトラフィックデータに与える影響について解析を行う．マルウェアによる感染拡大や攻撃が行われる際，使用されるポート番号には一定の規則があると考えられるが，その大部分は不明である．そこで，本稿ではマルウェア感染とポート番号との相関関係を明らかにすることを目的とする．PRACTICE におけるダークネットのトラフィックデータは，ポート毎に国別の時系列のデータとして利用する．ESET の公開情報は，各マルウェア毎に国別の時系列データとして利用する．各国における特定の期間の PRACTICE と ESET の時系列データを比較し，相関性を検証する．本稿で示したマルウェアの感染と各ポート番号におけるトラフィックデータの相関関係を把握することで，マルウェア感染に対して適切な対策を講じることが可能である．

2. マルウェアの時系列発生分布

セキュリティ対策ベンダによる各国での大規模なマルウェア検出センサで収集されたデータ [7] を利用することで，各国でどのようなマルウェアがどれだけ発生しているか把握することが可能である．マルウェアの検体が世界規模でどれだけ発生しているのかを表す検体発生数の推移を図 1 に示す．図 1 より，マルウェアの周期は 1 週間となっており，土曜日と日曜日には少なくなる傾向がある．また，世界規模の検体発生数はなだらかではあるが減少傾向にあることが見て取れる．世界規模での 1 年間の合計発生数が上位 10 個の検体名を表 1 に示す．表 1 より，上位 10 個の検体の発生数は非常に多く，発生数全体の約 20 パーセントを占めている．

3. ダークネットパケットの時系列分布

PRACTICE[1] では，異なる地域に設置された複数の

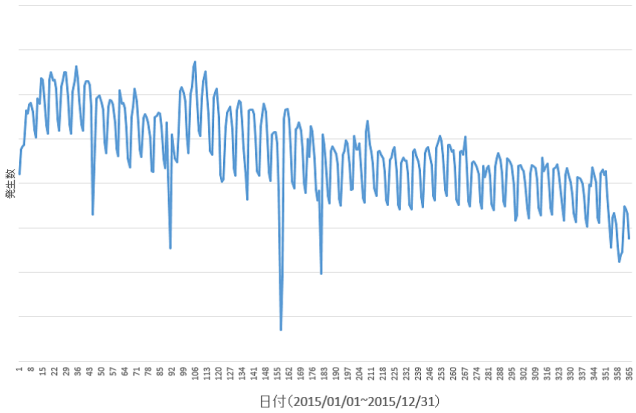

図 1 世界（147 カ国）合計の検体発生数推移

検体名	1 年間合計発生数
JS/Toolbar.Crossrider	21038086
Win32/ELEX	19371122
Win32/Toolbar.CrossRider	18020516
Win32/BrowseFox	17907938
Win32/Toolbar.SearchSuite	17351170
Win32/Bundpil	16627799
Win32/Toolbar.Conduit	16446703
Win32/InstallCore	15906271
Win32/AlteredSoftware	13163275
Win32/Systweak	11689672

表 1 世界 (147 カ国) 合計の検体発生数 TOP10

ダークネットの観測データを利用して攻撃解析が行われている．PRACTICE におけるダークネットのトラフィックデータを効率的に解析し，攻撃傾向やスキャンツールを分類する手法 [2][3][4][5] が提案されている．文献 [5] では，観測された攻撃元 IP アドレスに対して，スキャンに関係する特徴量を求めることで，スキャンツール等の分類を可能としている．本稿では，PRACTICE における観測データをポート毎の国別の時系列のデータとして扱う．解析結果では扱うデータの性質上，国名は伏せ字で表記している．また，ダークネットレンジの推定に繋がるため，具体的なパケット数も伏せて表記している．インバウンドの具体的な観測結果の例を図 2,3,4 に示す．図 2,3,4 では，各国において半年間に観測されたパケット数の時系列データを示している．また図 2,3,4 では同じグラフ上にアウトバウンドのパケットも載せている．アウトバウンドとは各国が送信元となっている PRACTICE 参加 6 カ国でのダークネット上で観測されたパケット数のことを示している．グラフでは扱うデータの性質上，国名は伏せ字で表記している．またダークネットレンジの推定に繋がるため，具体的なパケット数は標準化して表記している．

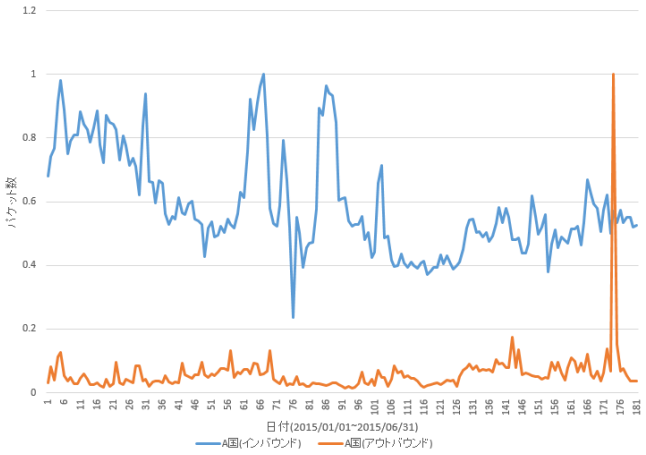

図 2　A 国パケット数推移

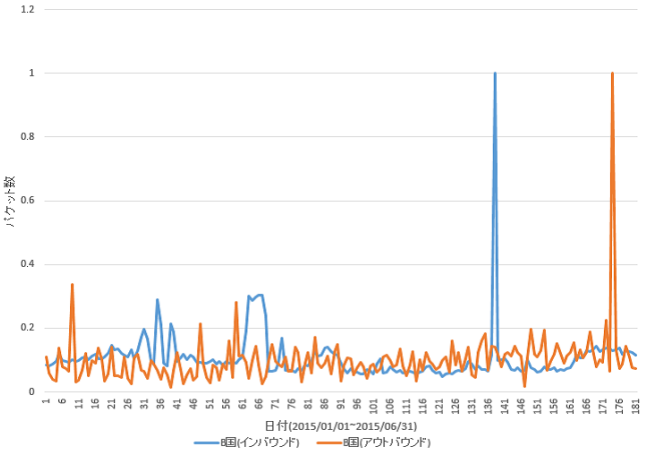

図 3　B 国パケット数推移

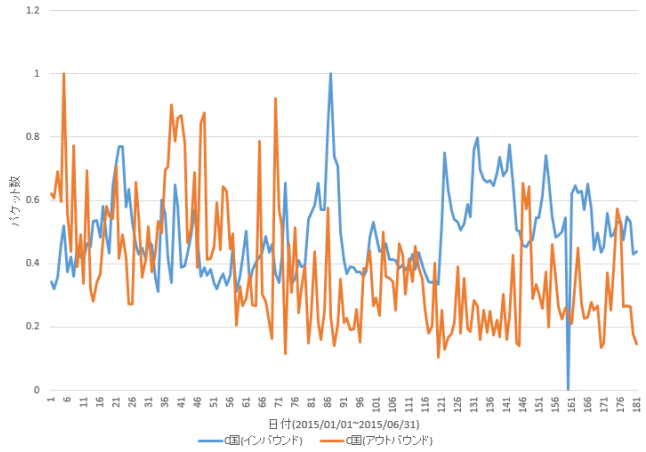

図 4　C 国パケット数推移

4. マルウェアとダークネットパケットとの時系列相関について

2 章で述べた ESET の観測データと 3 章で述べた PRACTICE におけるダークネットのトラフィックデータを利用して，マルウェア感染がダークネットのトラフィックデータに与える影響について解析を行う．ESET の公開情報は，各マルウェア毎に国別の時系列データとして扱う．PRACTICE におけるダークネットのトラフィックデータは，ポート毎に国別の時系列のデータとして扱う．各国における半年間の PRACTICE と ESET の時系列データを比較し，相関性を検証する．例として，PRACTICE において”A 国”に設置されたダークネットの”23 番ポート”で観測されたトラフィックデータを「A 国 - 23 番 tcp[udp]（インバウンド)」と表記する．また，A 国内の攻撃元から他の PRACTICE 参加国に対する攻撃に関するトラフィックデータを「A 国 - 23 番 tcp[udp]（アウトバウンド)」と表記する．ESET の公開情報において，”A 国”で観測された”Win32/Bundpil”の時系列データを「A 国 - Win32/Bundpil」と表記する．ここでは各国のマルウェアの発生数とポート毎のトラフィックデータから相関が見られる事例について紹介する．図 5 は A 国のアウトバウンドである 3389 番ポート（tcp）のパケット数のグラフと Win32/TrojanDownloader.Elenoocka の発生数のグラフである．Win32/TrojanDownloader.Elenoocka はインターネットから他のマルウェアをダウンロードしようとするトロイの木馬である．2 つのグラフからほぼ同時期に観測数が大きく増えていることがわかり，ここからこのマルウェアが 3389 番で使用されるリモートデスクトップを感染活動の一環で使用している可能性が推測される．続いて，図 6 は B 国のアウトバウンドである 23 番ポート (tcp) のパケット数のグラフと VBA/TrojanDownloader.Agent の発生数のグラフである．VBA/TrojanDownloader.Agent はインターネットから他のマルウェアをダウンロードしようとするトロイの木馬である．2 つのグラフからほぼ同時期に観測数が変動していることがわかり，ここからこのマルウェアが 23 番で使用される telnet を感染活動の一環で使用している可能性が推測される．最後に，図 7 は C 国のアウトバウンドである 445 番ポート (tcp) のパケット数のグラフと Win32/RiskWare.PEMaform の発生数のグラフである．Win32/RiskWare.PEMaform は望ましくない可能性があるアプリケーション (PUA) に分類され，PUA はツールバーやプラグインにまぎれてインストールされることが多い．2 つのグラフを見比べるとほぼ同時期に観測数が増えていることから，感染活動の一環としてポート 445 番が使用されている可能性が推測される．

5. おわりに

本稿では，近年増加するサイバー攻撃への対策として，マルウェア感染がダークネットのトラフィックデータに与える影響について解析を行った．マルウェア感染に関するデータとして，ESET において公開されている観測情報を利用して，マルウェア発生の時系列データを示した．ダークネットのトラフィックデータとして，PRACTICE における各国のトラフィックデータを利用して，ポート毎の時系列データを示した．以上の二つの時系列データを検証す

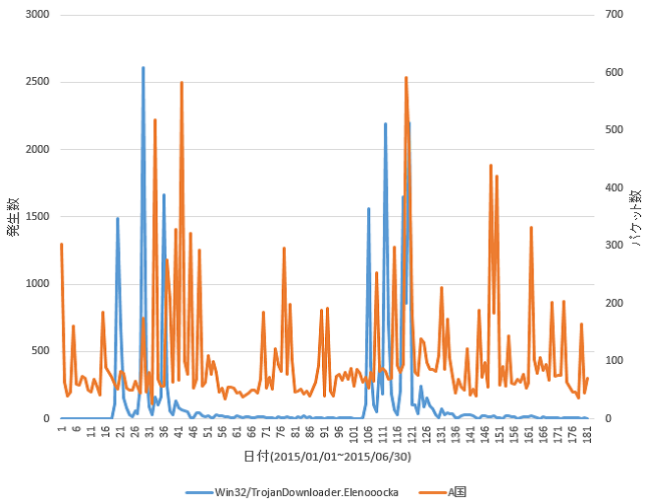

図 5 A 国 - 3389 番 tcp（アウトバウンド）と Win32/TrojanDownloader.Elenoocka 推移

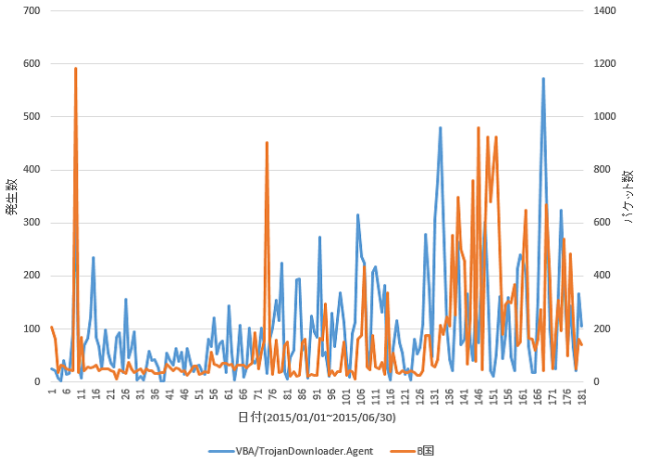

図 6 B 国 - 23 番 tcp（アウトバウンド）と Win32/TrojanDownloader.Elenoocka の発生数推移

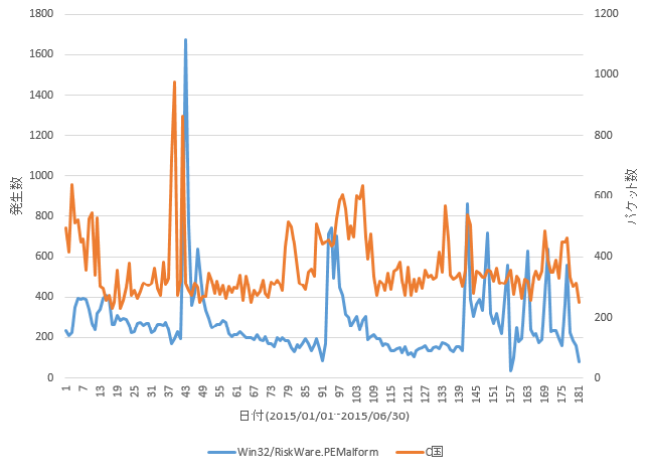

図 7 C 国 - 445 番 tcp（アウトバウンド）と Win32/RiskWare.PEMalform 推移

ることで，特定の国のある期間においてマルウェア発生の時系列データとポート別のトラフィックデータに相関があることを示した．マルウェア感染の際に使用されるポート番号には一定の規則があると考えられるが，その大部分はこれまで不明であった．本稿では相関のあるマルウェア発生の時系列データとポート別のトラフィックデータに着目することで，マルウェア感染の際に使用されていると推測されるポート番号を複数示した．本稿の解析結果を利用することで，マルウェア感染を早期発見し適切な対策を講じることが可能である．さらに期間を拡張した解析やポート番号以外の観測データに着目した解析は今後の課題とする．

参考文献

[1] 総務省｜国際連携によるサイバー攻撃予知・即応プロジェクト『PRACTICE』, http://www.soumu.go.jp/menu news/s-news/01ryutsu03 02000039.html

[2] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克“複数のダークネットに対するトラフィックデータ解析とその応用,”信学技報, ICSS, Vol.115, No.81, ICSS2015-7, pp.33-38, 2015 年 6 月.

[3] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克“複数のダークネットに対するトラフィックデータの解析結果とそこからの情報漏洩について,”第 14 回情報科学技術フォーラム (FIT2015), L-004, 第 4 分冊, pp.165-170, 2015 年 9 月.

[4] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克“ダークネットトラフィックへの時系列解析と攻撃手法の特徴分析,”2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 2016 年 1 月.

[5] 村井健祥, 古本啓佑, 村上洸介, 中尾康二, 森井昌克, ”PRACTICE ダークネットトラヒックへの時系列解析とスキャン特徴量によるスキャンツール等の分類,” 電子情報通信学会総合大会, 2016 年 3 月.

[6] 衛藤将史, 高木彌一郎, 宋中錫, 井上大介, 中尾康二,“スキャンの特徴抽出による攻撃元プロファイリング手法の提案,”信学技報, IA, Vol.111, No.81, IA2011-4, pp.19-24, 2011 年 6 月.

[7] Home — ESET Virusradar http://www.virusradar.com