Vol.2019-CSEC-85 No.3
Vol.2019-IOT-45 No.3
2019/5/23

大分大学のダークネットにおける SMB宛トラフィックのWannaCryによる影響調査

小川 健太[1]　池部 実[2]　吉崎 弘一[3]　吉田 和幸[3]

概要：2017 年にワーム型ランサムウェア WannaCry が問題となった．ランサムウェアは利用者の端末のファイルを暗号化し，復号するために金銭を要求するマルウェアである．WannaCry は，一つの端末に感染すると組織のネットワークを通じて他の端末に感染する感染活動を行う．さらに WannaCry はインターネット上のランダムな宛先に対しても感染拡大活動を行う特徴をもつ．本研究では WannaCry がランダムな宛先に対してポートスキャンすることから，組織内で未割当ての IP アドレス空間であるダークネットを用いて WannaCry に関連する通信を観測した．WannaCry は感染のために Windows のファイル共有プロトコル SMB で使用する TCP/445 を利用していることから，TCP/445 および SMB が利用している他のポート番号に着目し，ダークネットにおいて WannaCry による影響を分析した．

キーワード：ダークネット観測，WannaCry，ランサムウェア，ネットワークセキュリティ，SMB プロトコル

A survey of SMB trafffic affected by WannaCry in darknet of Oita University

Kenta Ogawa[1]　Minoru Ikebe[2]　Kouichi Yoshizaki[3]　Kazuyuki Yoshida[3]

Abstract: The worm-type ransomware WannaCry became a problem in 2017. Ransomware is a malware that requires money to encrypt and decrypt files on users' computers. If WannaCry infected a computer, it performs infection activity through the internal network. Furthermore, WannaCry has the spread to random destinations IP addresses. In this research, we foucus that the WannaCry scans ports for random destination IP addresses, We observed the packets related to WannaCry using our darknet. The darknet is an unassigned IP address space in organizations. WannaCry tar gets TCP/445 port as a Windows file sharing protocol SMB for infection. Therefore, we analyzed the affect of the WannaCry in our darknet. And we observed other ports using SMB protocols.

Keywords: Darknet Monitoring, WannaCry, Ransamware, Network Security, SMB protocol

1. はじめに

2017 年に登場した WannaCry や NotPetya 等のランサムウェアによる被害が深刻となった．ランサムウェアとは別名身代金要求型マルウェアと呼ばれるマルウェアの 1 種である．従来の AIDSTrojan や CryptoLocker 等のランサムウェアは感染経路に外部記憶媒体やドライブバイダウンロード攻撃を用いる．一方で 2017 年に猛威を振るった WannaCry は，これまでのランサムウェアにない自己増殖機能を有する点が従来と異なる点である．自己増殖機能とは，感染した端末自身がマルウェアをコピーし他の端末へ感染を拡大する機能である．これにより，一つの端末が感

[1] 大分大学大学院工学研究科工学専攻
Graduate School of Engineering, Oita University
[2] 大分大学理工学部共創理工学科
Department of Integrated Science and Technology, Faculty of Science and Technology, Oita University
[3] 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita Universityn

染し，組織内のネットワークに接続すると他の端末も感染しファイルも暗号化され，使用できなくなる可能性がある．WannaCry の自己増殖機能により多くのネットワークで感染拡大し，病院や鉄道などのシステムが停止されサービスに影響を及ぼした事例 [1] [2] も報告されている．WannaCry は，マカフィーが 2017 年 12 月に発表したレポート「2017 年 最も悪質な大規模感染「WannaCry」から学ぶ今後の教訓」[3] によると，2017 年の 5 月 12 日に発生し，発生後 24 時間で 150 ヶ国，30 万台以上のコンピュータに感染したことが報告されている．通常ランサムウェアは身代金を獲得することが目的であるが，WannaCry では振り込み人を特定する機能を持たず，身代金による被害は比較的少なかったとされている．一方で組織内のネットワークから感染が拡大し，システムの停止による損失は大きかった．WannaCry による騒動というのは登場から 1 年を経て目立った活動は見られなくなった．しかしながら，2009 年に大きな感染被害をもたらした Windows を標的とするワーム型マルウェアである Conficker [4] は現在でも多くの検出報告がされている．WannaCry の脅威は Conficker と同様に長い期間に及ぶ可能性がある [5] と述べられていることから，WannaCry についても長期的な観測・検知が必要となる．

WannaCry は感染の拡大に，ファイル共有プロトコル SMB(Server Message Block) の脆弱性を用いている．そこで本研究では，ファイル共有プロトコル SMB が使用するポート番号に対する WannaCry によるポートスキャンに着目し，WannaCry がダークネットに与える影響を分析した．ダークネットとはインターネット上で到達可能な未使用の IP アドレス空間である．ダークネットでは通常の通信によるパケットが到達しないことから，不正な活動に起因するパケットであるポートスキャンやマルウェアの活動によるパケットのみを観測可能である．今回は，WannaCry がランダムな宛先 IP アドレスに対してポートスキャンすることからダークネットトラフィックを調査した．

2. SMB と WannaCry

2.1 SMB

SMB とは Windows ネットワークにおけるファイル共有を実現するためのプロトコル [6] である．Windows ネットワークにおけるファイル共有サービス用のプロトコルには，「Common Internet File System(CIFS)」と呼ばれるプロトコルも存在する．CIFS は，SMB を仕様変更や機能拡張により Windows 以外の OS でも広く実装できるように改良されたプロトコルである．CIFS は SMB を拡張したプロトコルであり，インターネット上で SMB サービスと同様にファイルやプリンタの共有機能を実現する．初期の SMB では通信を実現するために NetBIOS で用いられる 137 から 139 番ポートで通信していた．しかし CIFS や Windows2000 以降の SMBv1 以降では 445 番ポートを用いて通信することが可能となった．必要なコネクションが 1 つですむため，効率がよく，ファイアウォール設定やルーティングを管理しやすくなる．実際にサーバと通信をする場合，NetBIOS インタフェースを使用する．同時に，TCP/445，UDP/445 番ポートも呼び出すように実装されている．SMB における各ポートの役割を表 1 に示す．

表 1 SMB における各ポートの種類と用途

ポート番号	種別	用途
137	TCP/UDP	NetBIOS 名前サービス
138	UDP	NerBIOS データグラム・サービス
139	TCP	NetBIOS セッション・サービス
445	TCP/UDP	ダイレクト・ホスティング SMB サービス

2.2 WannaCry

WannaCry は，自己増殖機能を持つランサムウェアである．また WannaCry の自己増殖機能は，組織ネットワーク内だけでなく，インターネット上のランダムな宛先に対して行われることから，世界中で感染を大きく拡げる一因となった．この自己増殖機能は厳密にはランサムウェアの機能ではなく，EternalBlue と呼ばれるエクスプロイトキットの機能である．EternalBlue とは，Microsoft 社製品である SMBv1 プロトコルの脆弱性 (CVE-2017-0144) [7] を利用しているバッファオーバフローを引き起こすツールである．EternalBlue が SMBv1 の TCP/445 をインターネット上に公開している端末に対してバックドアツール DoublePulsar を仕込むことで，バックドアの DoublePulsar から WannaCry を動作させる命令を実行する．DoublePulsar とは，メモリ内でカーネルモードで動作するバックドアである．WannaCry の詳しい挙動を図 1 に示す [8].

(手順 1)EternalBlue を用いて CVE-2017-0144 の脆弱性をつき，WannaCry のコピーを送り込む．再度 EternalBlue を用いて，DoublePulsar を動作させる．
(手順 2)DoublePulsar を介して WannaCry を動作させる．
(手順 3)攻撃者が事前にハードコーディングした URL[*1]への接続を確認する．通信に成功した場合 WannaCry の動作は終了する．失敗した場合以下の動作に進む．
(手順 4)被害者が身代金を支払い，復号鍵を攻撃者から入手するために必要な経路を Tor ブラウザを介して確立する．
(手順 5)端末内のローカルドライブ上に保存されているファイルおよび接続されているネットワークドライブ上のファイルを暗号化する．また，システムの復元に用いられるボリュームシャドウコピーを削除する．
(手順 6)同じサブネット内の IP アドレスを昇順に，EternalBlue を用いた感染活動を行う．また，ランダムな

[*1] Wanna Cry 登場時は存在しない URL.

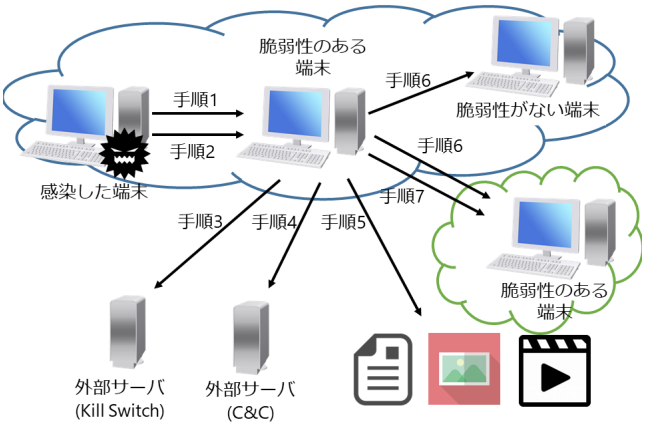

図 1　WannaCry の挙動

IP アドレスに対する感染活動も同時に行う．

(手順 7)手順 6 で侵入に成功すると，仕掛けられたバックドア DoublePulsar を介して新たな端末で WannaCry を実行する．

このように SMBv1 を実装している WindowsXP などにおいて，脆弱性を攻撃され任意のコマンドを実行される危険性が存在する．WannaCry の標的であった Windows7 では SMBv2.1 が実装されている．しかし，Windows ネットワークの互換性維持のために Windows7 においても SMBv1 も実装されている．2017 年当時のデスクトップ向け OS のシェアの約 5 割が Windows7 [9] であったことから WannaCry の標的とされ，大規模に感染が発生した．現在普及している Windows10 では 2017 年の 10 月に配信された Fall Creators Update を適用すると，SMBv1 は利用停止されるようになっている．

3. 調査概要

WannaCry によるダークネット上での影響を観測するために WannaCry が感染に用いている TCP/445 番ポート宛の通信を収集，解析した．本調査では TCP/445 の他にも表 1 に示した SMB で用いている TCP/137，UDP/137，UDP/138，TCP/139 を調査した．

今回の調査の収集方法として，大分大学宛のダークネットに到達したパケットを収集した．ダークネットとはインターネット上で到達可能な未使用の IP アドレス空間である．ダークネットでは通常の通信が行われないため，不正な通信に起因するパケットのみを観測できる．これによりインターネット上の不正な活動の傾向を把握することが可能である．

本調査において WannaCry が大流行した 5 月 12 日を含む 2017 年 1 月 1 日から 2017 年 9 月 30 日に収集したダークネットトラフィックを用いた．ダークネットトラフィックの収集方法を図 2 に示す．調査対象のダークネットトラフィックにおけるパケットの総数は 633,394,776(約 6 億) パケットであった．また調査期間中に観測した一意な送信元 IP アドレス数は 7,740,499 個であった．

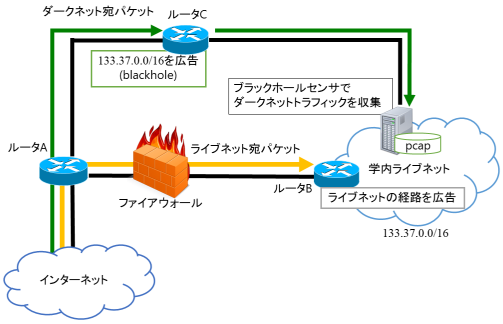

図 2　ダークネットトラフィックの収集方法

調査手順として，まず WannaCry の発生前後でトラフィックにどのような変化が起こったのかを観測するために大分大学のダークネットにおいて 2017 年 1 月から 9 月までの期間において，TCP/137，UDP/137，TCP/138，UDP/139，TCP/445 宛に送信された 633,394,776 個のパケットを調査した．これは 2017 年 5 月 12 日に WannaCry が発生したことから，発生以前と発生前後，発生以降として 3 ヶ月ごとに，調査した．そして，各ポート番号宛のパケット数とホスト数を 1 日単位で集計した．その後，ポート番号ごとに国や OS の分布を調査した．

4. 調査結果

WannaCry は TCP/445 に対してポートスキャンを送信する．TCP/445 では，WannaCry のほかにも Windows 標的としたマルウェアである Conficker が存在する．Conficker に感染したホストは，インターネットの複数のグローバル IP アドレスに対して，TCP/445 へのポートスキャンを行う．Conficker の影響により，WannaCry 以前から一定以上のパケット数が TCP/445 で観測されていた．Conficker の主な標的として，WindowsXP や Windows2000 であることから送信元ホストの OS を調査することにより Conficker と WannaCry を判別することが可能である．このことから本調査では，大分大学のダークネットにおいて WannaCry が攻撃に用いる TCP/445 のトラフィックの集計結果を示したのち，SMB が用いる他のポートである TCP/137，UDP/137，UDP/138，TCP/139 のトラフィックの集計結果について述べる．

4.1 TCP/445

調査期間となるダークネットトラフィックから TCP/445 宛の一日ごとのパケット数および送信元 IP アドレス数を集計したグラフを図 3 に示す．また送信パケットを国ごとに分類し，送信パケット数上位 20 位の国までを抽出した

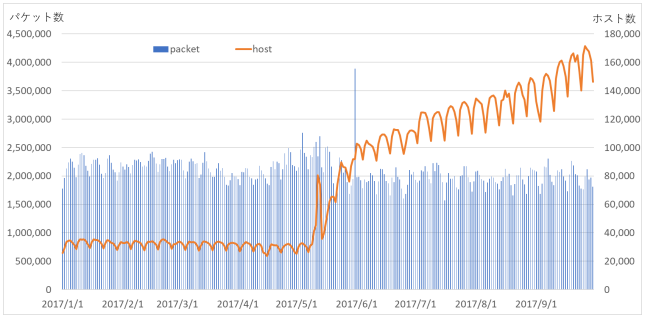

図 3 2017 年 1 月から 9 月における 1 日の TCP/445 宛の送信パケット数と送信ホスト数

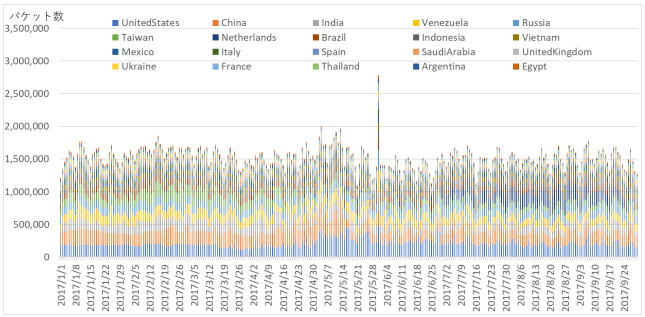

図 4 2017 年 1 月から 9 月における 1 日の TCP/445 宛の送信元国別上位 20 位の送信パケット数

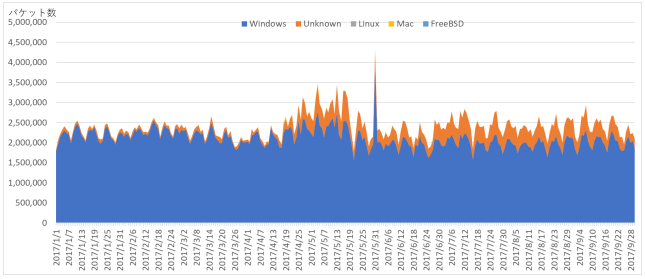

図 5 2017 年 1 月から 9 月における 1 日の TCP/445 宛の OS 別の送信パケット数

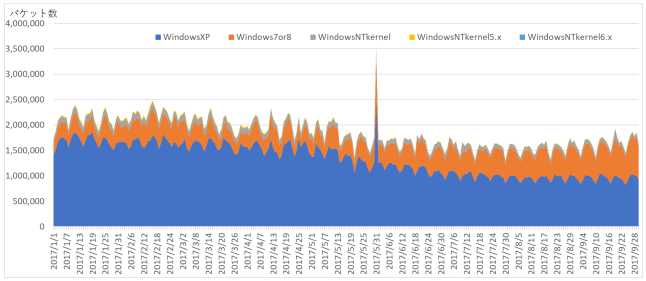

図 6 2017 年 1 月から 9 月における 1 日の TCP/445 宛の Windows と判定された送信パケット数

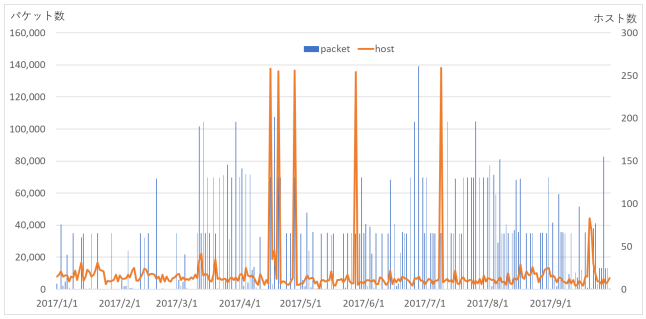

図 7 2017 年 1 月から 9 月における 1 日あたりの TCP/137 宛の送信パケット数と送信ホスト数

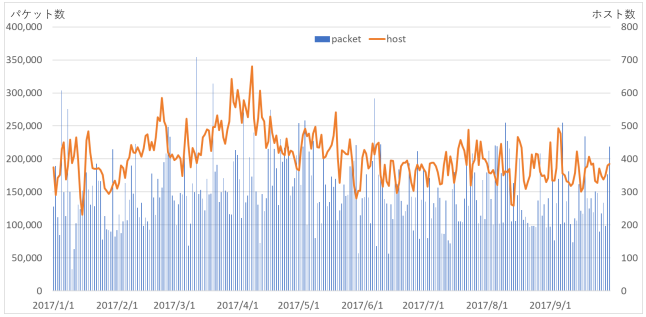

図 8 2017 年 1 月から 9 月における 1 日あたりの UDP/137 宛の送信パケット数と送信ホスト数

ものと送信パケットを OS ごとに集計した結果を図 4 と図 5 に示す．送信元 IP アドレスの国の分類には GeoLite2 Country2 [10] のデータベースを参照した．OS の判定には OS 判定ツールである p0f [11] を用いた．さらに Windows をバージョンごとに分類し，集計したものを図 6 に示す．図 5 の Unknown は p0f にて判定できなかった OS をあらわしている．

図 3 において WannaCry の被害が相次いで報告された 2017 年 5 月 12 日に送信ホストが急増していた．また，5 月 12 日以降送信ホストが増加し続けていた．5 月 12 日以降の送信ホスト数の増加に反して，パケット数に関しては 5 月 12 日以前と比較すると緩やかな減少傾向であることを確認した．次に図 4 を見ると，全体を通して世界中からパケットが送信されていることが観測できた．これは，世界中で感染が報告された Conficker や WannaCry の影響だと推測した．さらに図 5 を見ると，送信元の多くが Windows と判定されていることが分かる．図 6 を見ると，Windows XP と判定されたパケットが減少傾向であるのに対して Windows7or8 と判定されたパケットの割合が徐々に増加していた．WannaCry は Windows7 を標的としたマルウェアであることから，増加した時期と合わせて WannaCry の感染活動の影響と推測した．以上のことから WannaCry が攻撃に利用している TCP/445 番ポートにおいて，WannaCry 発生と同時期に大分大学のダークネットにおいて送信ホストが急増し，以降も上昇傾向であることを観測した．次に NetBIOS を利用する各ポートに関しては，特徴があった部分だけ述べる．しかし，各ポートに関して TCP/445 と関連がみられる挙動は発見できなかった．

4.2 TCP/137，UDP/137

次にダークネットトラフィックより TCP/137, UDP/137 宛の一日ごとのパケット数および送信元 IP アドレス数を

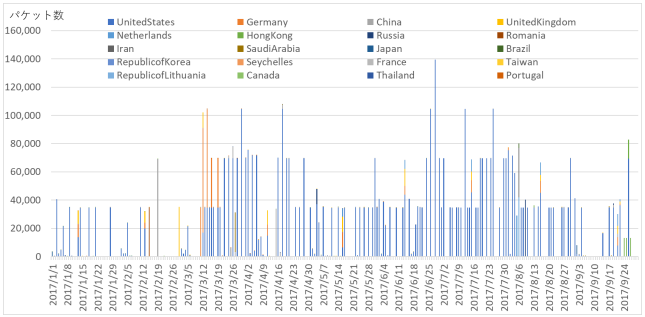

図 9 2017 年 1 月から 9 月における 1 日あたりの TCP/137 宛の送信元国別上位 20 位の送信パケット数

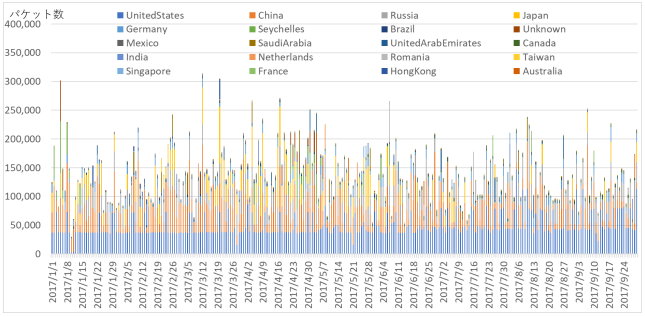

図 10 2017 年 1 月から 9 月における 1 日あたりの UDP/137 宛の送信元国別上位 20 位の送信パケット数

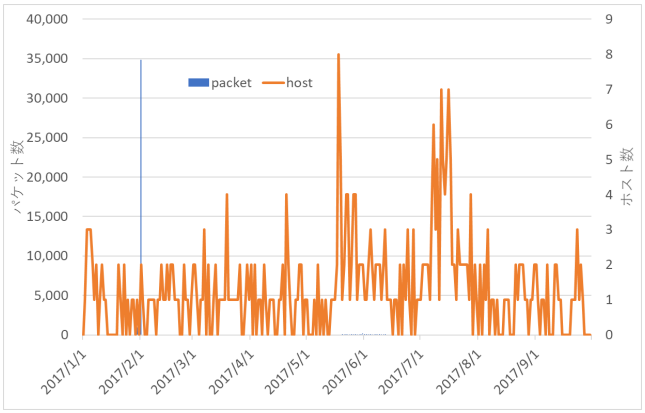

図 11 2017 年 1 月から 9 月における 1 日あたりの UDP/138 宛の送信パケット数と送信ホスト数

集計したグラフを図 7 と図 8 に示す．また TCP/445 と同様に送信パケットを国ごとに分類し，送信パケット数が上位 20 位の国を抽出したものを TCP と UDP それぞれで集計した結果を図 9 と図 10 に示す．

図 7 と図 8 をみると，どちらも 5 月 12 日周辺で急激な変化は観測できなかった．図 9 を見てみると，TCP/137 で観測したパケットのその多くがアメリカからであることを確認した．一方で図 10 を見ると，UDP/137 では TCP/137 の場合と同様にアメリカからの送信パケットを多数観測するとともに，中国やロシア，日本からも多くパケットが送信されていることを観測した．しかし，5 月 12 日前後では TCP/137，UDP/137 ともに国の分布にあまり顕著な変化は見られなかった．

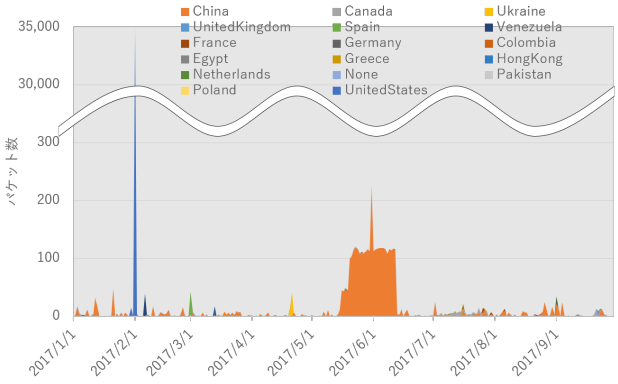

図 12 2017 年 1 月から 9 月における 1 日あたりの UDP/138 宛の送信元国別上位 20 位の送信パケット数

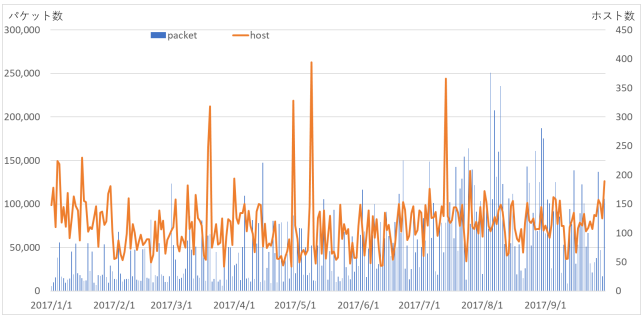

図 13 2017 年 1 月から 9 月における 1 日あたりの TCP/139 宛の送信パケット数と送信ホスト数

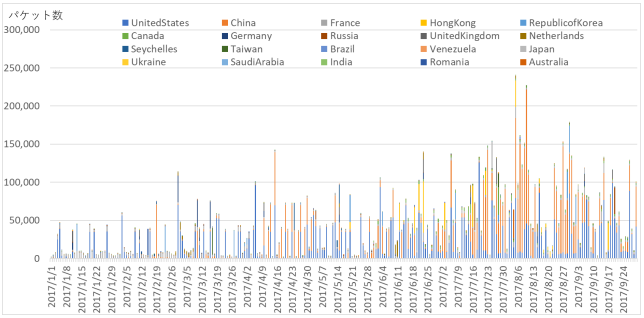

図 14 2017 年 1 月から 9 月における 1 日あたりの TCP/139 宛の送信元国別上位 20 位の送信パケット数

4.3 UDP/138

UDP/138 宛の一日ごとのパケット数および送信元 IP アドレス数を集計したグラフを図 11 に示す．また送信パケットを国ごとに分類し，送信パケット数を集計した結果を図 12 に示す．図 12 の縦軸では，300 から 30000 までの数値を省略して表記している．

図 11 を見ると，5 月 12 日周辺において急激な変化を観測できなかった．しかし，図 12 をみると，5 月中旬において中国からまとまったパケットが送信されていることを観測した．そこで送信元ホストを調査してみたところ，中国のインターネットプロバイダからのパケットであった．

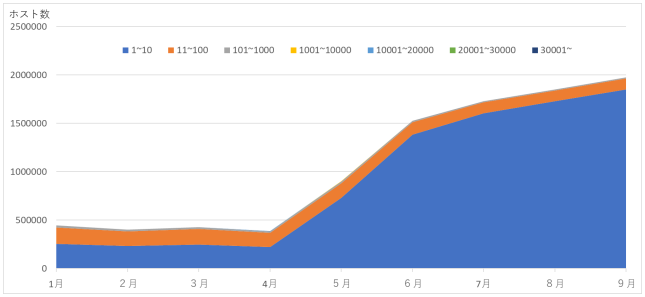

図 15 2017 年 1 月から 9 月における送信パケット数ごとに分類した送信ホスト数

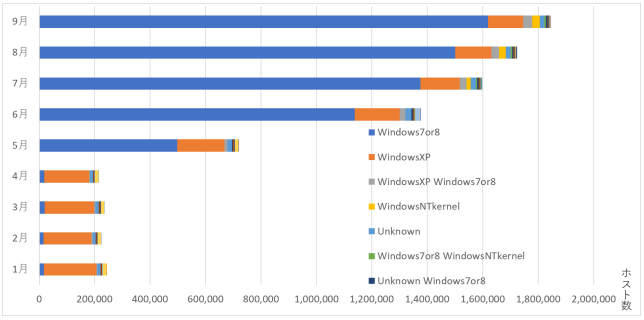

図 16 2017 年 1 月から 9 月まで平均パケット数が 1 から 10 までの OS 別のホスト数

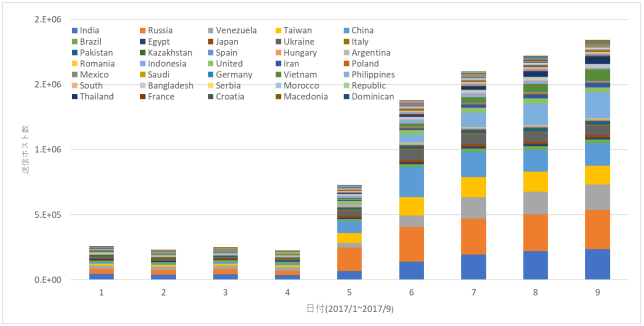

図 17 2017 年 1 月から 9 月まで平均パケット数が 1 から 10 までの国別のホスト数

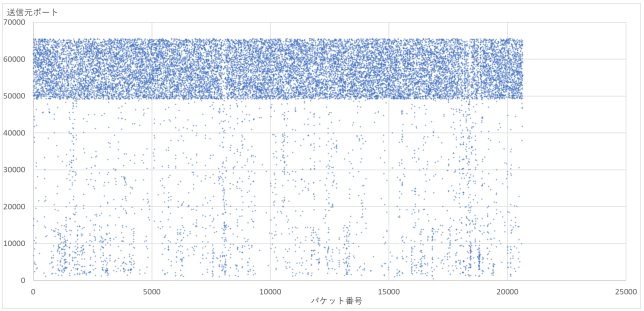

図 18 2017 年 5 月 13 日の送信元ポート番号の分布

4.4 TCP/139

TCP/139 宛の一日ごとのパケット数および送信元 IP アドレス数を集計したグラフを図 13 に示す．また送信パケットを国ごとに分類し，送信パケット数が上位 20 位の国までを抽出したものを集計した結果を図 14 に示す．図 13 において 2017 年 1 月から 9 月の期間において，送信ホスト数の急増を 4 回観測した．どの送信ホストも大部分がアメリカからのものであり，一つは WannaCry とほぼ同時期に急増しているが送信ホストを調査したところネットワークホスティング企業からのものであった．一方で図 14 を見ると，送信ホストが急増した時期にアメリカからのパケット数の増加は観測できなかった．さらにこの企業から NetBIOS の他のポートに対しても通信していることが観測できたが，TCP/445 に関しては通信は観測できなかった．このことから，送信ホストの増加に関しては調査目的であり，WannaCry による影響とは無関係であると推測する．

4.5 TCP/445 宛の送信パケット数による分類と OS

大きく変化が見られた送信ホストに関して，送信パケット数から大まかに送信ホストの挙動を区別するために一日の 1 送信ホスト当たりの平均送信パケット数を 10 のべき乗ごとに分類した．1 日の 1 送信ホスト当たりの平均パケット数を 10 のべき乗ごとにランク分けしたグラフを図 15 に示す．図 15 より平均パケット数が 1 から 10 の送信ホストの増加を確認した．これは，ワーム型のマルウェアは感染拡大のために少量のパケットを送信する特徴があり，ワーム型である WannaCry の活動の影響と推測する．

さらに，平均パケット数が 1 から 10 の送信ホストにおいて，p0f を用いて OS を判別した結果を図 16 に示す．図 16 を見ると WannaCry 発生以前の 1 月から 4 月にかけて，WindowsXP のホストが約 5 割を占めていることが観測できた．しかしそれ以外の OS に関する比率に関しては大きな変化を確認できなかった．WannaCry が発生した 5 月には 4 月までトップであった WindowXP を上回り，Windows7or8 と判定された送信ホストが急増していた．さらに 5 月以降は，Windows7or8 と判定された送信ホストが月ごとに増加していた．WannaCry は SMBv1 を標的としたランサムウェアであることや 2017 年当時のデスクトップ向け OS のシェア率は Windows7 が約 5 割を占めていたこと，そして Windows7 では互換性のために SMBv1 が動作していたことから WannaCry に感染した Windows7OS の送信ホスト数が急増したと推測した．

また，平均パケットが 1 から 10 の送信ホストにおいて，国を判別した結果を図 17 に示す．図 17 を見ると，2017 年 5 月以降ロシアからのホスト数が増加していることを観測した．これは 2017 年に警察庁が報告された WannaCry に感染した端末からの感染活動が見られた送信元の国 [12] と一致する部分がみられることから，WannaCry の影響により送信元ホスト数が増加した可能性が推測される．

4.6 Windows7 ホストの分析

今回の調査で得られたデータをもとにダークネットで収集したパケットヘッダから WannaCry を判別することは

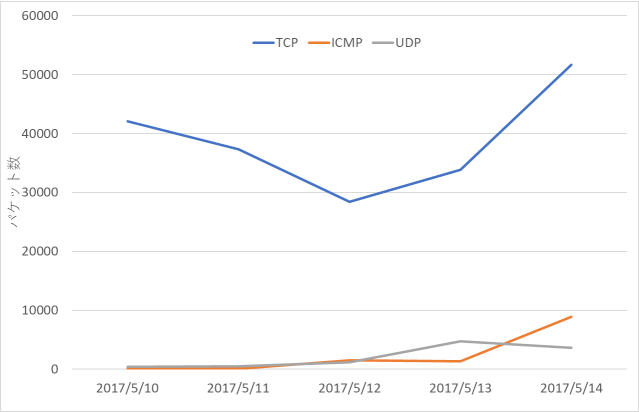

図 19 2017 年 5 月 10 日から 14 日までの各プロトコル毎の送信パケット数

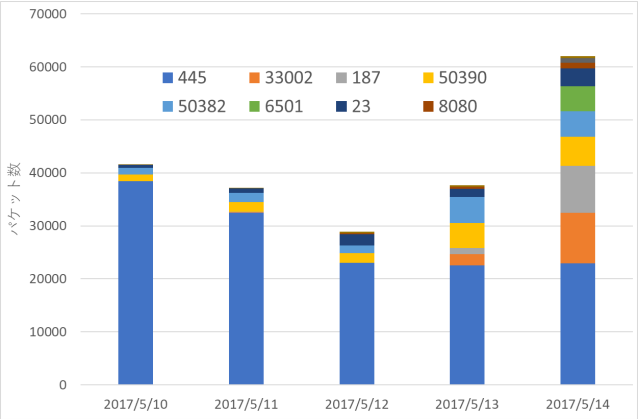

図 20 2017 年 5 月 10 日から 14 日まで宛先ポートごとの上位 10 位のパケット数

できないかと考え，4.5 節で Windows7or8 と判定された送信ホストの TCP/445 に対する通信のパケットヘッダを調査した．調査対象には，2017 年 5 月 13 日に Windows7 と判定された送信ホストである 40,855 ホストのうち無作為に 10,000 ホスト分の TCP/445 への通信に対するパケットヘッダを抽出した．

Mirai [13] では送信元 IP アドレスと初期シーケンス番号が一致する特徴がある．Mirai とは 2016 年に登場したワーム型マルウェアである．このマルウェアは，ボットネットを形成するために自己増殖するが，この時独自に生成する探索用パケットのパケットヘッダの送信元 IP アドレスと初期シーケンス番号が一致する特徴がある．Mirai はスキャン活動において OS の持つ TCP スタック機能を使わずに自身でパケットを生成して，送信している．このようなことから SMB，TCP/445 宛のパケットヘッダについても詳しく調査した．そのために p0f を用いるだけでなく，実際にパケットヘッダを抽出し，各数値のパラメータの分布を分析した．. 送信元ポートに関する調査結果を図 18 に示す．図 18 は 2017 年 5 月 13 日の送信元ポート番号の分布である．縦軸は送信ポート番号，横軸は送信されたパケットの IP アドレスを昇順に並べており，一つの点がパケットを表している．図 18 を見ると，ダイナミックポートの 49152 番から 65535 番に分布が集中していることを観測した．これらのポートは通信をする際に OS により自動的に割り振られるポート番号であることから OS の TCP スタック機能によりパケットが送信されたと判断した．さらに WannaCry 発生前後の TCP/445 宛にダークネットに送信した送信パケット数が 1 から 10 のホストでかつ，Windows7 と判定されたホストに関して 2017 年 5 月 10 日から 14 日までの各日から無作為に 10,000 ホスト分のパケットを抽出し，同様の調査を行った．しかし，各 TCP ヘッダのパラメータに関して，急激な変化は発見できなかった．

そこで，今回抽出した送信ホストに関して，他のポートへの通信を観測することにより WannaCry の判別ができないかを調査した．今回の調査で 5 月 12 日以前と以降に大きな変化が見られた各プロトコルと宛先ポートについて報告する．図 19 は 2017 年 5 月 10 日から 14 日までの各プロトコル毎のパケット数の変化を表したものである．図 20 は 2017 年 5 月 10 日から 14 日までの宛先ポート毎のパケット数が大きいもの上位 10 個のパケット数の変化を表したものである．

図 19 を見ると，5 月 12 日以降 ICMP のパケットが増加していることが観測できた．これに関して，それぞれの宛先を調査したところ，特定のアドレスに対して 5 月 12 日以前と比較して大量のパケットが送信されていた．しかし送信ホストに関しては増加がみられたのが 5 月 14 日のみであることから，WannaCry の影響とは判断できなかった．次に図 20 を見ると，12 日以前では TCP/445 へのパケットがほとんどであった．12 日以降では，12 日以前にも見られた 50390 や 50382 に対するパケットも増加しており，23 や 187，33002 などに対する通信が活発となった．しかし，送信ホスト数に関してはどのポートも大きな変化は見られなかった．

4.7 調査結果の考察

今回の調査では，2017 年 5 月 12 日に SMB が用いているポート番号のうち TCP/445 番ポートにて送信元ホスト数が急増していることを確認した．また，5 月以降送信元ホスト数の上昇が継続していることも観測できた．しかし，SMB が利用している他のポートでは TCP/445 と関連のある変化を観測できなかった．そして通信パターンや送信パケットの OS，送信ホストの国の情報から，Windows7 を標的とした WannaCry に感染したホストから通信が行われたのではないかと推察できる．さらに今回送信されたパケットのうち 2017 年 5 月 10 日から 14 日に Windows7or8 と判定されたホストのパケットヘッダを解析したが，パケットヘッダのそれぞれのパラメータにおいて大きな変

化は見られなかった．このことから p0f 以上の情報をパケットヘッダから得ることは困難であると推察した．また Windows7 と判断されたホストの TCP/445 以外の通信に関しても調査した結果，各プロトコルと宛先ポートに関してパケット数に変化を観測できた．しかし，パケット数が増加する一方で送信ホストがあまり増加していないことから，WannaCry が発生したことによる調査によってパケットが増加したのではないかと推察した．

このようにダークネットの情報のみで WannaCry を判別することは困難であることから仮想環境で実装可能な低インタラクション型のハニーポットの一つである Dioaea [14] に注目した．Dionaea は FTP や HTTP といった様々な種類のネットワークサービスを模倣可能であり，WannaCry が感染に用いている SMB も模倣可能である．また，WannaCry の挙動から DoublePulsar を用いて WannaCry を送りこんでいることから，DoublePulsar の挙動を模倣することにより WannaCry の通信を模倣することが可能である．

5. おわりに

5.1 まとめ

本研究では，2017 年 1 月から 2017 年 9 月までに観測した 633,394776 件の大分大学のダークネット宛の通信を対象に，SMB が用いる全ポートを調査した．その結果，WannaCry が発生して以降ダークネットにおいて WannaCry が標的としている SMBv1 を実装した Windows7 あるいは Windows8 と思しき送信ホストが増加していることが観測できた．このことから，ダークネットを観測することにより OS や通信パターン，送信ホストの国の情報から，WannaCry の影響と推察できる結果を得ることができた．しかし，SMB 宛のダークネットトラフィックのパケットヘッダを詳細に解析したところ初期シーケンス番号などの TCP ヘッダのパラメータから特徴のようなものは見られず，TCP ヘッダから攻撃を判定することは困難であると判断した．さらに TCP/445 以外の通信関しても調査を行ったが，WannaCry の挙動を観測できるような手掛かりを発見することはできなかった．

5.2 今後の課題

本調査では前述の通り大分大学宛の通信において WannaCry と推測できる送信ホストからの通信を確認した．今回観測に用いたダークネットではブラックホールセンサを用いている．ブラックボールセンサとは，相手の通信に対して応答しないので TCP の場合 3 ウェイハンドシェイクの最初の SYN パケットしか観測できない．そのため，ダークネットでは今回の調査結果で示した送信ホストの国や OS までが調査の限界である．このことから WannaCry の通信の詳細を調査するためにペイロードを取得する必要がある．SMB が用いるポートに対してハニーポットを設置することで WannaCry の詳細な通信の調査を目指す．

参考文献

[1] 日立製作所. ランサムウェアによる被害および復旧状況について. http://www.hitachi.co.jp/New/cnews/month/2017/05/0517a.html(アクセス日 2019/3/19).
[2] NHS Digital. Statement on reported nhs cyber attack. https://digital.nhs.uk/news-and-events/news-archive/2017-news-archive/statement-on-reported-nhs-cyber-attack/(アクセス日 2019/3/19).
[3] mcafee. 2017 年最も悪質な大規模感染「wannacry から学ぶ今後の教訓」, 2017 年 12 月. https://blogs.mcafee.jp/wannacry2017-future-lessons(アクセス日 2019/1/22).
[4] US-CERT. Conficker worm target micorosoft windows system, 2017 年 7 月. https://www.us-cert.gov/ncas/alerts/TA09-088A(アクセス日 2019/1/22).
[5] 金岡晃. 私たちは泣きたくない! -ランサムウェア「wannacry」の騒動. 情報処理 vol.58, No.7, 情報処理学会, 2017 年 6 月.
[6] Sever message block protocol, ms-smb. https://msdn.microsoft.com/en-us/library/cc246231.aspx(アクセス日 2019/1/22).
[7] CVE-2017-0144. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144(アクセス日 2019/1/22).
[8] macnica networks. Wannacry. https://www.macnica.net/file/news_what_wannacry.pdf(アクセス日 2019/4/16).
[9] 後藤大地. 2017 年デスクトップ os シェア動向まとめ. https://news.mynavi.jp/article/20180416-617098/(アクセス日 2019/3/19).
[10] MAXMIND. Geolite2 free dowloadable databases. https://dev.maxmind.com/geoip/geoip2/geolite2//(アクセス日 2019/3/22).
[11] p0f. http://lcamtuf.coredump.cx/p0f3/(アクセス日 2019/1/28).
[12] 警察庁. ランサムウェア「wannacry」の亜種に感染した pc からの感染活動とみられる 445/tcp ポート宛てアクセスの観測について. https://www.npa.go.jp/cyberpolice/detect/pdf/20170622.pdf(アクセス日 2019/4/11).
[13] US-CERT. Heightened ddos threat posed by mirai and other botnets, 2017 年 10 月. https://www.us-cert.gov/ncas/alerts/TA16-288A(アクセス日 2019/2/1).
[14] carnivore. Dionaea. https://dionaea.readthedocs.io/en/latest/index.html(アクセス日 2019/3/22).