大分大学のダークネットトラフィックにおける ゼロデイ攻撃の影響の分析

東條 貴明[1] 池部 実[2] 吉田 和幸[3]

概要：インターネット上の脅威の中でも，ソフトウェアの脆弱性が解消される前に攻撃が行われるゼロデイ攻撃が問題になっている．ゼロデイ攻撃は脆弱性に関する情報や対応策が提供される前に攻撃が行われるため，検知や予防などの対策が困難である．そこで，我々はゼロデイ攻撃の予兆となる活動を把握するために，インターネット上での不正な活動に起因する通信が多く観測されるダークネットに着目した．ダークネットとは，インターネットから到達可能かつ未使用の IP アドレス空間であり，脆弱な機器を探索するスキャン攻撃をはじめとした様々な不正な通信が観測されている．

本論文では，大分大学のダークネット宛トラフィックを収集し，過去に報告された 47 件の脆弱性について，脆弱性が報告されたソフトウェアが使用するポート番号宛のトラフィックに注目して調査をした．その結果，脆弱性情報の公表の前後に於けるトラフィックの顕著な増加を 4 件観測した．本発表では脆弱性に関連したトラフィック増加事例と，ゼロデイ攻撃がダークネットのトラフィックに与える影響について調査した結果を報告する．

Analysis for influence of zero-day attacks on darknet traffic of Oita University

TAKAAKI TOJO[1] MINORU IKEBE[2] KAZUYUKI YOSHIDA[3]

1. はじめに

インターネットの急速な普及に伴い，ネットワーク上で様々な情報のやり取りがされるようになった．電子メールなどのコミュニケーション手段にとどまらず，行政手続きやクレジットカード番号などを利用した電子決済サービスなど公共性の高いサービスが提供されている．そのため現在では，インターネットは重要な社会的基盤の 1 つとなっており，生活に不可欠な存在となっている．一方で，インターネットを利用した不正通信も存在し，ソフトウェアの脆弱性を悪用する，サーバへの不正アクセスなどの様々な脅威が存在する．インターネット上の脅威の中でも，ソフトウェアの脆弱性が解消される前に攻撃が行われるゼロデイ攻撃が問題になっている．2016 年 4 月に Symantec 社が発表した「2016 年インターネットセキュリティ脅威レポート」[1] によると，2015 年に発見されたゼロデイ脆弱性は 54 件で，2013 年の 23 件，2014 年の 24 件に対して増加傾向にあった．また，2017 年 4 月に Symantec 社が発表した「2017 年インターネットセキュリティ脅威レポート」[2] では，ソフトウェアのベンダが発見しなかったゼロデイ脆弱性の数が報告されており，その数字は 2014 年が 4,958 件，2015 年が 4,066 件，2016 年が 3,986 件と減少傾向にある．バグバウンティングプログラムの人気が高まったことや，製品開発プロセスの中でセキュリティがより重要視されるようになったことで，攻撃者が脆弱性を発見するのが難しくなったことが理由として挙げられている．ゼロデイ攻撃は脆弱性に関する情報や対応策が提供される前に攻撃が行われるため，ソフトウェアのエンドユーザのみならず，セキュリティ管理者や開発ベンダにとっても検知や予防などの対策が困難である．

そこで，我々はゼロデイ攻撃の予兆となる活動を把握するために，インターネット上での不正な活動に起因する通信が多く観測されるダークネットに着目する．ゼロデイ攻

1 大分大学大学院工学研究科工学専攻知能情報システム工学コース
2 大分大学理工学部共創理工学科知能情報システムコース
3 大分大学学術情報拠点情報基盤センター

撃の予兆となる活動を把握できれば，攻撃を早期に発見する上で有用となる．ダークネットとは，インターネットから到達可能かつ組織内で未割当な IP アドレス空間の事を指す．ダークネットは未使用の IP アドレスであるため，通常はダークネットに対してパケットが送信されることはない．しかしながら，ダークネット上で大量のパケットが観測されているのが現状である．ダークネットで観測されるパケットには以下に示すようなものが含まれていると報告されている [3].

- リモートエクスプロイト型マルウェアが次の感染対象を探査するためのスキャン
- マルウェアが感染対象の脆弱性を攻撃するためのエクスプロイトコード
- 送信元 IP アドレスが詐称された DDoS 攻撃を被っているサーバからの応答であるバックスキャッタ

本論文では，ゼロデイ攻撃の早期発見に役立てることを目的に，ダークネット上のトラフィックの変動からゼロデイ攻撃の予兆を把握する方法について考察する．そのために，大分大学のダークネット宛トラフィックを収集し，ソフトウェアの脆弱性情報が公表された前後の期間において，その脆弱性に関連するポート番号宛のパケット数・送信元ホスト数の変動を調査した．宛先ポート番号ごとのトラフィックの変動に注目することで，特定のポート番号を用いるソフトウェアに対する攻撃の発見を期待できる．過去に報告された 47 件の脆弱性について，そのソフトウェアが使用するポート番号宛のトラフィックに注目して調査をした結果，脆弱性情報の公表の前後におけるパケット数の顕著な増加を 4 件観測した．

2. 関連研究

ダークネットに関する関連研究として，情報通信研究機構 (NICT) の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が研究開発を進めている，大規模ダークネット観測網 nicter[4] がある．nicter では大規模ダークネット観測網で収集した観測情報の一部を Web で公開している．サイバー攻撃の大局的な傾向を広く公開することにより情報セキュリティ関連組織や企業・大学の情報セキュリティ管理部門等との情報共有を促進している．また，NICT では nicter の観測結果にもとづくアラートシステムである DAEDALUS[5] を開発・運用している．DAEDALUS は観測対象の組織について，組織内のマルウェアによる感染活動や，組織内から組織外への感染活動，組織外から受けている DoS 攻撃の跳ね返り（バックスキャッタ）などをダークネットで観測すると，当該組織へアラートを送信して，迅速なインシデント対応を促している．

3. 大分大学のダークネット宛トラフィックの分析

大分大学のダークネット宛トラフィックをブラックホールセンサで収集する．ブラックホールセンサとは，パケットの送信元に対して全く応答を返さないセンサであり，複雑なシステム構成やマシンリソースを必要としないため，設置や運用が容易であり大規模なネットワーク観測に適している．一方で，パケットの送信元に対して応答しないため，TCP/UDP のスキャンや UDP パケットに含まれるペイロードやエクスプロイトコードは観測できるが，攻撃者の詳細な挙動や TCP コネクション確立後に送信されるペイロードまでは観測できない．

本論文で対象としたダークネットトラフィックの分析期間は 2015 年 4 月から 2017 年 3 月 (24 ヶ月分) である．期間中にダークネットで観測した総パケット数は 51,303,079,681 件で，1 日あたりの平均観測パケット数は約 70,182,052 件であった．一意な送信元 IP アドレス数は 117,589,232 個であった．本論文ではゼロデイ攻撃がダークネットトラフィックに与える影響を分析するために，ダークネットで収集したパケットを TCP/UDP の宛先ポート番号ごとに分類して集計し，過去に脆弱性が報告されたソフトウェアが使用するポート番号宛トラフィックの変動を調査する．宛先ポート番号ごとのトラフィックの急激な増加などの変動に注目することで，変動があったポート番号を用いるソフトウェアへの攻撃発見が期待できる．もし脆弱性情報の公表前に，脆弱性の影響を受けるソフトウェアが用いるポート番号宛のトラフィックが顕著に変動していたならば，ゼロデイ状態の脆弱性の影響がダークネット上にあらわれたと考えることができる．

脆弱性情報は CVE(Common Vulnerabilities and Exposures)[6] を参照した．CVE とは共通脆弱性識別子のことで，個別製品中の脆弱性を対象として米国政府の支援を受けた非営利団体の MITRE が採番している識別子である．2015 年 4 月から 2017 年 3 月に発表された CVE 14,718 件のうち，ネットワークを介して攻撃可能かつ攻撃対象となるポート番号が判明している脆弱性情報 47 件を分析対象とした．

4. ダークネットトラフィックにおけるゼロデイ攻撃の影響の調査結果

大分大学のダークネット宛トラフィックを分析した結果，ソフトウェアの脆弱性の公表の前後におけるトラフィックの顕著な変化を 4 件観測した．また，観測した送信元 IP アドレスを whois や逆引きにより，当該 IP アドレスのサービスや所属を調査した．以下に観測した事例の詳細について示す．

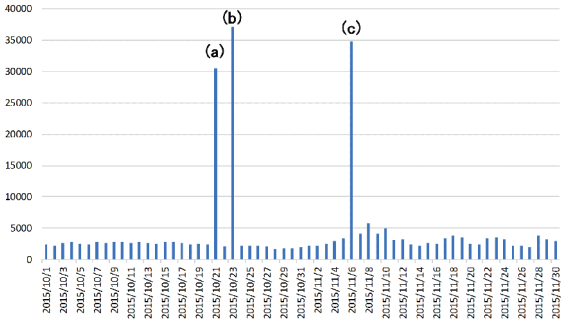

図 1　2015 年 10 月から 11 月における TCP6000 番ポート宛のパケット数の推移

4.1　MobaXterm にコマンドインジェクションの脆弱性

2015 年 11 月 2 日に，Mobatek 社製の X11 サーバソフトウェア MobaXterm において TCP6000 番ポート上でコマンドインジェクションを受ける可能性のある脆弱性 (CVE-2015-7244)[7] が報告された．脆弱性情報が公表された前後に，大分大学のダークネット上で TCP6000 番ポート宛パケット数の顕著な増加を計 3 回観測した (図 1(a)，(b)，(c))．パケット数の急増を観測したのは (a)10 月 21 日，(b)10 月 23 日，(c)11 月 6 日であった．それぞれの日における総送信元ホスト数は (a)36 件，(b)31 件，(c)65 件であり，3 日とも単一の送信元ホストが大量にパケットを送信したことにより，パケット数の急増が発生していた．(表 1，表 2，表 3)．

図 1 の (a)，(b)，(c) 以外において観測していた送信元ホスト数は平均 33 件であり，観測していたパケットのほとんどは Shodan[8] からのパケットであった．Shodan はインターネット上に接続されている機器に関する情報を収集及びデータベース化し，インターネットからの検索を可能にする Web サービスを提供している．1 日に Shodan から大分大学のダークネットに向けて送信されていた平均パケット数は 2,000 件前後であった．一方で図 1 中の (a)，(b)，(c) において大量にパケットを送信していた IP アドレスはブラックリストである AbuseIPDB[9] に登録されているホストであり，各ホストとも大分大学のダークネット全体を網羅するようにパケットを送信していた．そのことから，送信者の目的は脆弱性が解消されていない機器を探索する目的のスキャンであると推測できる．

Mobatek 社が当該脆弱性に対する修正プログラムをリリースしたのは 10 月 31 日であり，(a)10 月 21 日，(b)10 月 23 日は脆弱性に対する修正プログラムが存在しない状況でスキャンと考えられるパケットをダークネットで観測していた．

4.2　オムロン製 PLC および CX-Programmer に複数の脆弱性

2015 年 10 月 1 日に，オムロン社製の PLC(Programmable Logic Controller) 製品 CJ2 シリーズおよび，PLC や HMI(Human Machine Interface) の設定やプログラミングを行うためのソフトウェア CX-Programmer において，以下の 3 つの脆弱性が報告された．

- パスワードが平文で送信される脆弱性 (CVE-2015-0987) [10]
- CX-Programmer 用プロジェクトファイルからパスワードを取り出せる脆弱性 (CVE-2015-0988)[11]
- コンパクトフラッシュカードに保存されるオブジェクトファイルからパスワードを取り出せる脆弱性 (CVE-2015-1015)[12]

脆弱性報告の翌日に，当該システムが通信に用いる TCP9600 番ポート宛のパケット数 (図 2) と送信元ホスト数 (図 3) の顕著な増加を観測した．パケット数，送信元ホスト数ともに 10 月 2 日に急増している．平常時の送信元ホスト数は平均 22 件であるのに対し，10 月 2 日は平常時の約 3.5 倍の 74 件の送信元ホストからのパケットを観測した．表 4 に 10 月 2 日における送信元ホスト数の内訳を示す．表 4 に示す通り，複数の送信元ホストが 1,000 件前後のパケットを送信していた．また，送信元ホスト上位 10 件は whois で調査した結果すべて同じ ISP に属しており，上位 16 ビットが一致するホスト (112.94.*.*) を多数観測していた．そ

表 1　(a)2015 年 10 月 21 日における TCP6000 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
203.67.A.B	34,905	ISP(台湾)
71.6.C.D	322	Shodan
71.6.E.F	307	Shodan
71.6.G.H	298	Shodan
188.138.A.I	280	Shodan
合計	37,090	

表 2　(b)2015 年 10 月 23 日における TCP6000 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
203.67.A.J	28,339	ISP(台湾)
71.6.C.D	307	Shodan
71.6.G.H	266	Shodan
71.6.E.F	262	Shodan
198.20.K.L	234	Shodan
合計	30,552	

表 3　(c)2015 年 11 月 6 日における TCP6000 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
80.82.M.N	30,786	ISP(オランダ)
212.109.O.P	561	ホスティングサービス (ロシア)
71.6.C.D	366	Shodan
66.240.Q.R	357	Shodan
71.6.G.H	327	Shodan
合計	34,827	

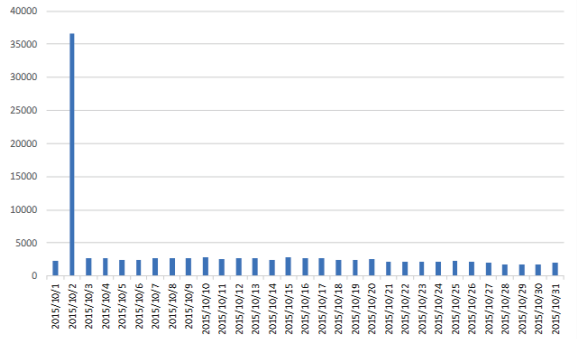

図 2 2015 年 10 月における TCP9600 番ポート宛のパケット数の推移

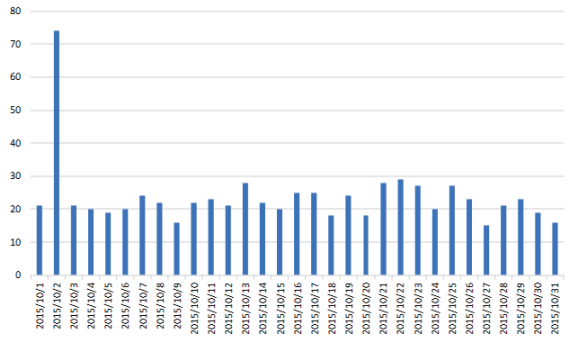

図 3 2015 年 10 月における TCP9600 番ポート宛の送信元ホスト数の推移

表 4 2015 年 10 月 2 日における TCP9600 番ポート宛パケットの送信元ホスト内訳 (上位 10 件)

送信元ホスト	パケット数	サービス名
58.248.A.B	1,104	ISP(中国)
112.94.C.D	977	ISP(中国)
112.94.E.F	971	ISP(中国)
112.94.G.H	969	ISP(中国)
112.94.I.J	960	ISP(中国)
120.85.K.L	945	ISP(中国)
112.94.I.M	943	ISP(中国)
112.94.N.O	934	ISP(中国)
112.94.P.Q	933	ISP(中国)
58.249.R.S	913	ISP(中国)
合計	36,625	

のことから，同一組織内の複数ホストからスキャンが行われていた可能性がある．

当該脆弱性に対する修正プログラムは脆弱性の報告と同日の 10 月 1 日にリリースされており，トラフィックの増加を観測したのが 10 月 2 日であるため，厳密にはゼロデイ状態で大量のトラフィックを観測したとは言えない．しかし，ソフトウェアの利用者は修正プログラムが公開されてから即時に適用できるとは限らないため，これも広義のゼロデイ攻撃と言える．

4.3 Cisco ASA (Adaptive Security Appliance) の IKEv1 と IKEv2 の処理にバッファオーバーフローの脆弱性

2016 年 2 月 10 日に，Cisco 社製のセキュリティ製品 Cisco ASA の IKE(Internet Key Exchange)v1，v2 において，バッファオーバーフロー攻撃を受ける可能性のある脆弱性 (CVE-2016-1287)[13] が報告された．

脆弱性の報告の前後に，IKE プロトコルが通信に用いる UDP500 番ポート宛のパケット数と送信元ホスト数の増加，また，IKE プロトコルが NAT トラバーサルをする際に用いる UDP4500 番ポート宛のパケット数の増加を観測した．2016 年 1 月から 3 月における UDP500 番ポート宛のパケット数の推移を図 4 に，2016 年 1 月から 3 月における UDP500 番ポート宛の送信元ホスト数の推移を図 5 に，UDP4500 番ポート宛のパケット数の推移を図 6 に示す．

UDP500 番ポート宛のパケット数については，脆弱性が報告される約 1 ヶ月前から (a)1 月 16 日，(b)1 月 19 日にスキャンを観測している．脆弱性が報告された 2 月 10 日近辺でも大規模なパケットの増加を観測し，その後も散発的にスキャンを観測した．観測した UDP 番ポート宛のパケットはペイロード部が IKE のフォーマットに従ったパケットや UDP ヘッダのみのパケットなど様々なパケットを観測した．しかし，実際にバッファオーバーフローを引き起こすエクスプロイトコードは観測していない．顕著なパケット数増加を観測した日の送信元ホスト数は，(a)27 件，(b)31 件，(c)24 件，(d)29 件，(e)24 件，(f)20 件，(g)26 件，(h)54 件，(i)31 件，(j)64 件であった．(a) から (j) に示した日以外に観測していた送信元ホスト数は平均 36 件であり，観測していたパケットは他の事例と同様に Shodan からのパケットがほとんどであった．

また，(a)1 月 16 日 (表 5) と (c)2 月 10 日 (表 7)，(d)2 月 12 日 (表 8)，(e)2 月 13 日 (表 9) におけるパケットの増加について，158.130.A.B を調査したところペンシルバニア大学が保有する，脆弱性の影響を調査するスキャンを行っていたホストであった [14]．しかし (b)1 月 19 日 (表 6)，(f)2 月 15 日 (表 10)，(g)2 月 19 日 (表 11)，(h)2 月 26 日 (表 12)，(i)3 月 10 日 (表 13)，(j)3 月 22 日 (表 14)，のパケット増加は，すべて AbuseIPDB のブラックリストに登録されているホストからのスキャンであった．

UDP500 番ポート宛の送信元ホスト数 (図 5) については，1 月 1 日から 2 月 23 日までは平均 26 件だったのに対し，2 月 24 日に増加してからは平均 52 件と 2 倍近い値で推移していた．

UDP4500 番ポート宛のパケット数については，(a)1 月 20 日にスキャンを観測した後に，(b)2 月 12 日にもスキャンを観測していた．UDP4500 番ポート宛のパケットでは，UDP ヘッダのみのパケットを大量に観測した．(a)1 月 20 日 (表 15)，(b)2 月 12 日 (表 16) のパケット増加は，とも

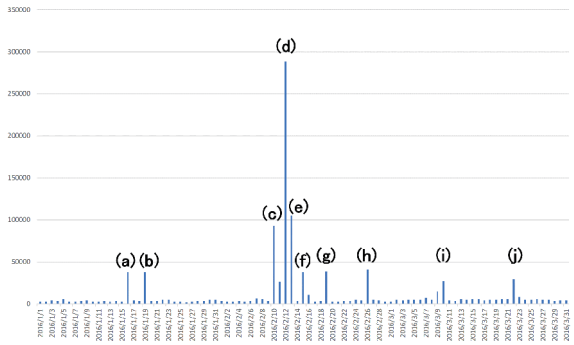

図 4　2016 年 1 月から 3 月における UDP500 番ポート宛のパケット数の推移

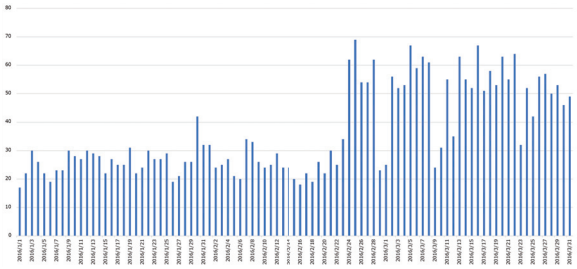

図 5　2016 年 1 月から 3 月における UDP500 番ポート宛の送信元ホスト数の推移

表 5　(a)2016 年 1 月 16 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
158.130.A.B	35,472	ペンシルバニア大学
66.240.C.D	298	Shodan
66.240.E.F	278	Shodan
71.6.G.H	266	Shodan
71.6.I,J	261	Shodan
合計	37,839	

表 6　(b)2016 年 1 月 19 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
89.248.I.K	34,987	IPS(オランダ)
1.202.L.M	336	ISP(中国)
71.6.I.J	306	Shodan
66.240.E.F	300	Shodan
71.6.G.H	290	Shodan
合計	37,797	

表 7　(c)2016 年 2 月 10 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
158.130.A.B	90,274	ペンシルバニア大学
71.6.G.H	261	Shodan
66.240.C.D	237	Shodan
66.240.E.F	232	Shodan
71.6.I.J	227	Shodan
合計	92,722	

に AbuseIPDB のブラックリストに登録されているホストからのスキャンであった．

表 8　(d)2016 年 2 月 12 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
158.130.A.B	250,703	ペンシルバニア大学
87.190.N.O	35,146	ISP(ドイツ)
71.6.P.Q	287	Shodan
71.6.G.H	286	Shodan
66.240.C.D	278	Shodan
合計	288,670	

表 9　(e)2016 年 2 月 13 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
158.130.A.B	101,545	ペンシルバニア大学
222.163.R.S	455	ISP(中国)
71.6.G.H	262	Shodan
66.240.C.D	250	Shodan
71.6.P.Q	239	Shodan
合計	104,434	

表 10　(f)2016 年 2 月 15 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
179.43.T.U	35,052	ホスティングサービス (スイス)
71.6.I.J	253	Shodan
71.6.G.H	250	Shodan
71.6.P.Q	240	Shodan
66.240.E.F	223	Shodan
合計	37,812	

表 11　(g)2016 年 2 月 19 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
179.43.T.U	35,052	ホスティングサービス (スイス)
222.161.V.W	302	ISP(中国)
116.225.X.Y	288	ISP(中国)
71.6.I.J	278	Shodan
71.6.Q.H	270	Shodan
合計	38,102	

表 12　(h)2016 年 2 月 26 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
179.43.T.Z	35,052	VPN サービス
78.115.a.b	1620	ホスティングサービス (フランス)
71.6.G.H	289	Shodan
93.80.A.c	273	ホスティングサービス (ロシア)
66.240.C.D	269	Shodan
合計	38,102	

4.4　「提督業も忙しい！」がオープンプロキシとして動作する問題

2015 年 5 月 26 日に，オンラインゲーム用ユーティリティツール「提督業も忙しい！」において，オープンプロキシとして動作する脆弱性 (CVE-2015-2947)[15] が報告された．脆弱性の報告の前後に，当該ツールが初期設定で用いる TCP37564 番ポート宛のパケット数の増加を観測した．2015 年 5 月における TCP37564 番ポート宛のパケッ

表 13　(i)2016 年 3 月 10 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
94.102.d.e	23,058	VPN サービス
71.6.G.H	280	Shodan
66.240.E.F	280	Shodan
71.6.P.Q	274	Shodan
71.6.I.J	253	Shodan
合計	26,866	

表 14　(j)2016 年 3 月 22 日における UDP500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
72.14.f.g	24,849	ホスティングサービス (アメリカ)
71.6.G.H	284	Shodan
71.6.I.J	269	Shodan
198.20.h.i	248	Shodan
188.0.j.k	236	ホスティングサービス (カザフスタン)
合計	29,140	

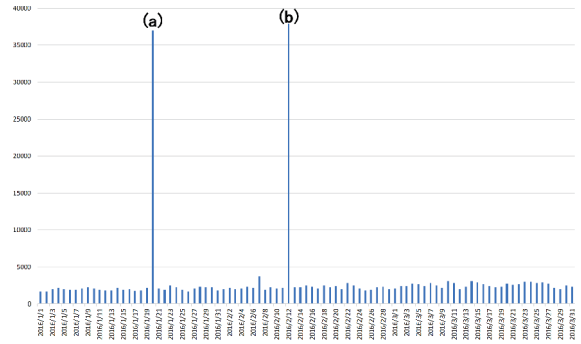

図 6　2016 年 1 月から 3 月における UDP4500 番ポート宛のパケット数の推移

表 15　(a)2016 年 1 月 20 日における UDP4500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
89.248.I.K	34,839	ISP(オランダ)
71.6.G.H	295	Shodan
66.240.C.D	268	Shodan
66.240.E.F	267	Shodan
71.6.I.J	259	Shodan
合計	37,026	

表 16　(b)2016 年 2 月 12 日における UDP4500 番ポート宛パケットの送信元ホスト内訳 (上位 5 件)

送信元ホスト	パケット数	サービス名
87.190.N.O	35,297	ISP(ドイツ)
66.240.C.D	254	Shodan
66.240.E.F	237	Shodan
71.6.P.Q	233	Shodan
198.20.h.i	230	Shodan
合計	37,874	

ト数の推移を図 7 に示す．

5 月 11 日にパケット数が急増して以降，5 月下旬に至るまで 1 日あたり 2,000,000 パケット前後の高い水準でパケットを観測した．5 月中の送信元ホスト数は平均 10 件

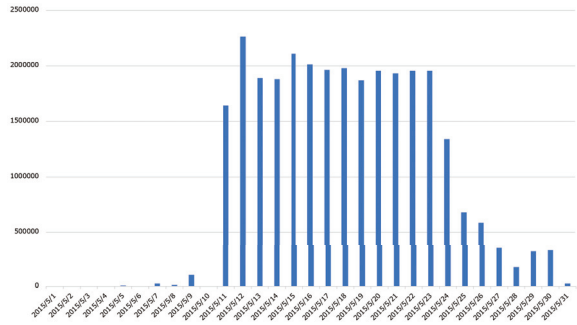

図 7　2015 年 5 月における TCP37564 番ポート宛のパケット数の推移

表 17　2015 年 5 月中における TCP37564 番ポート宛パケットの送信元ホスト内訳 (上位 10 件)

送信元ホスト	パケット数	サービス名
61.183.A.B	22,656,622	ホスティングサービス (中国)
178.19.C.D	3,930,194	ホスティングサービス (ポーランド)
116.211.E.F	2,528,228	ISP(中国)
178.19.C.G	113,487	ホスティングサービス (ポーランド)
222.186.H.I	69,895	ISP(中国)
222.186.J.K	69,718	ISP(中国)
80.82.L.M	472	ISP(オランダ)
64.237.N.O	9	ホスティングサービス (アメリカ)
188.165.P.L	9	ISP(フランス)
69.89.Q.R	8	ホスティングサービス (アメリカ)
合計	29,368,945	

```
[Tue May 12 00:00:00 2015] [60] [TCP] srcIP[61.183.A.B] srcport[55151] dstIP[133.37.*.*] dstport[37564]
[Tue May 12 00:00:00 2015] [60] [TCP] srcIP[61.183.A.B] srcport[55151] dstIP[133.37. *.*] dstport[37564]
[Tue May 12 00:00:00 2015] [60] [TCP] srcIP[61.183.A.B] srcport[55151] dstIP[133.37. *.*] dstport[37564]
[Tue May 12 00:00:00 2015] [60] [TCP] srcIP[61.183.A.B] srcport[55151] dstIP[133.37. *.*] dstport[37564]
[Tue May 12 00:00:00 2015] [60] [TCP] srcIP[61.183.A.B] srcport[55151] dstIP[133.37. *.*] dstport[37564]
```

図 8　2015 年 5 月における TCP37564 番ポート宛のスキャンの例

で，1 ヵ月を通して目立った増減は見られなかった．5 月中に TCP37564 番ポート宛に通信を行った送信元ホストを調査したところ，特定少数の送信元ホストが大量にパケットを送信した結果パケット数の急増が発生していた．表 17 に 2015 年 5 月中における TCP37564 番ポート宛パケットの送信元ホスト内訳を示す．送信元ホスト上位 6 件は，すべて大分大学のダークネット全体を網羅するようにスキャン活動を行っていた．6 ホストとも 5 月中に複数回スキャンを観測しており，1 回のスキャンでは送信元ポート番号を固定した通信を確認した (図 8)．また送信元ホスト上位 6 件すべてが脆弱性に対するスキャン活動を行っているホストとして，IBM が公表しているサイバー上の脅威のデータベースである X-Force Exchange[16] に登録されていた．また，80.82.L.M はセキュリティ関連企業の，インターネット上のオープンプロキシサーバを調査する目的のホストであった．大規模なスキャン活動が開始されたのが 5 月 11 日であるのに対し，問題の脆弱性に対する修正プログラムがリリースされたのが 5 月 26 日なためゼロデイ状態で大量のスキャンが発生していたことになる．

4.5 観測事例についてのまとめ

大分大学のダークネット宛通信を分析した結果，ソフトウェアの脆弱性が公表された日時の近辺に，そのソフトウェアが利用するポート番号宛のパケット数や送信元ホスト数が顕著に増加していた．正規の通信は観測されないダークネット上でこのようなパケット増加を観測しており，さらに，送信元ホストの挙動は観測対象の IP アドレスを網羅するようにパケットを送信しているものがほとんどであった．そのため，設定ミスやマルウェアがランダムにパケットを送信した結果によりトラフィックが増加したのではなく，脆弱性のある機器を探査する目的のスキャンによりトラフィックが増加したものとみられる．スキャンは攻撃の前段階として行われることが多いため，ダークネット上にゼロデイ攻撃の予兆となる活動があらわれていた．

5. おわりに

5.1 まとめ

本論文では，ゼロデイ攻撃の予兆となる活動を調査するため，不正な活動に起因する通信が多く観測されるダークネットに着目した．大分大学大学のダークネット宛トラフィックを収集し，過去に報告された 47 件の脆弱性について，そのソフトウェアが使用するポート番号宛のトラフィックに注目して調査をした結果，脆弱性情報の公表の前後におけるトラフィックの顕著な増加を 4 件観測した．今回観測したトラフィック増加の要因は，脆弱な状態の機器を探査する目的のスキャンであると推測できる．スキャンは攻撃の前段階として行われることが多いため，ゼロデイ攻撃の予兆となる活動がダークネットで観測されるトラフィックにあらわれていた．ダークネットにおける宛先ポートごとのトラフィックの変動に注目することで，特定のポートを用いるソフトウェアに対する攻撃の予兆の発見を期待できる．

5.2 今後の課題

本調査では脆弱性の情報を参照することで，その脆弱性に関連したポート番号宛トラフィックの変動を発見した．しかし通常，ゼロデイ攻撃の発生時点では参照する脆弱性情報は存在しないため，未知の脆弱性に関連するトラフィックの変動を発見するためにはすべてのポート番号宛のトラフィックを監視する必要がある．よって今後は各ポート番号毎のトラフィック異常を自動で検出し，警告を発するシステムの構築を目指す．

参考文献

[1] Symantec: 2016 年インターネットセキュリティ脅威レポート，入手先 ⟨https://www.symantec.com/content/ja/jp/enterprise/infographics/ig-zero-day-jp-2.pdf⟩ （参照 2017-04-17）.

[2] Symantec: 2017 年インターネットセキュリティ脅威レポート，入手先 ⟨https://www.symantec.com/ja/jp/security-center/threat-report⟩ （参照 2017-05-01）.

[3] 井上大介: 情報セキュリティ技術動向調査 (2008 年下期) 7 ダークネット観測の技術動向と観測事例，入手先 ⟨https://www.ipa.go.jp/security/fy20/reports/tech1-tg/2_07.html⟩ （参照 2017-04-17）.

[4] 中里 純二， 島村 隼平， 衛藤 将史， 井上 大介， 中尾 康二: nicter によるネットワーク観測および分析レポート組み込みシステムに感染するマルウエア (セキュリティ，一般)，電子情報通信学会技術研究報告 ISEC 情報セキュリティ（参照 2017-04-17）

[5] 鈴木 未央， 井上 大介， 衛藤 将史， 宇多 仁， 中尾 康二: 大規模ダークネット観測に基づくアラートシステムの実装と運用，電子情報通信学会技術研究報告. ICSS, 情報通信システムセキュリティ（参照 2017-04-17）

[6] MITRE:CVE - Common Vulnerabilities and Exposures，入手先 ⟨https://cve.mitre.org/⟩ （参照 2017-04-17）

[7] MITRE:CVE-2015-7244，入手先 ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7244⟩ （参照 2017-04-17）

[8] Shodan，入手先 ⟨https://www.shodan.io/⟩ （参照 2017-04-17）

[9] AbuseIPDB，入手先 ⟨https://www.abuseipdb.com/⟩（参照 2017-04-17）

[10] MITRE:CVE-2015-0987，入手先 ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0987⟩ （参照 2017-04-17）

[11] MITRE:CVE-2015-0988，入手先 ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0988⟩ （参照 2017-04-17）

[12] MITRE:CVE-2015-1015，入手先 ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1015⟩ （参照 2017-04-17）

[13] MITRE:CVE-2016-1287，入手先 ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1287⟩ （参照 2017-04-17）

[14] University of Pennsylvania:Network Security Research Scans at The University of Pennsylvania，入手先 ⟨http://research-scan.cis.upenn.edu/⟩（参照 2017-04-17）

[15] MITRE:CVE-2015-2947，入手先 ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2947⟩ （参照 2017-04-17）

[16] IBM:X-Force Exchange，入手先 ⟨https://exchange.xforce.ibmcloud.com/⟩ （参照 2017-04-25）