2-3 nicterレポート～長期ネットワーク観測に基づく攻撃の変遷に関する分析～

2-3 nicter Report —Transition Analysis of Cyber Attacks Based on Long-term Observation—

中里純二　大高一弘
NAKAZATO Junji and OHTAKA Kazuhiro

要旨

nicterプロジェクトにおいて蓄積した長期間のネットワーク観測データを基に、サイバー攻撃や、収集されたマルウェアの傾向の変化などについて報告する。特に、2008年11月以降、大規模感染を引き起こしたConfickerワームがネットワークに与えた影響について分析する。また、nicterで観測されたボットネットの規模の変化についても報告を行う。

In this report, we provide a statistical data concerning cyber attacks and malwares based on a long-term network monitoring on the nicter. Especially, we show a continuous observation report of Conficker, which is a pandemic malware since November 2008. In addition, we report a transition analysis of the scale of botnet activities.

[キーワード]
インシデント分析，ダークネット，ネットワークモニタリング，マルウェア解析
Incident analysis, Darknet, Network monitoring, Malware analysis

1　はじめに

我々は、マルウェアの感染活動などがネットワークに及ぼす大局的な影響を把握するため、インターネット上で到達可能かつ未使用のIPアドレス空間（ダークネット）の大規模モニタリングを行っている。本報告では、インシデント分析センタnicter[1][2]において6年以上に渡って観測・蓄積を行ってきたダークネットトラフィックを分析し、長期的な観測によって得られたサイバー攻撃の傾向変化や、攻撃元ホストの振舞の変化などを報告する。特に、2008年11月に大規模感染を引き起こしたConfickerワームに着目し、同マルウェアのインターネットに及ぼした影響や現在の活動状況について報告する。また、長期観測の間に見られたボットネットのスキャンを抽出し、ボットネットの規模の変化を報告する。

nicterでは、ブラックホールセンサをダークネットに設置し、大規模なダークネットトラフィックの収集・分析を行っている。ブラックホールセンサとは、到達するパケット全てを無応答で収集するセンサであり、マルウェアによるスキャンの傾向や、Backscatter（IPアドレスを詐称し送られたDDoS攻撃に対する応答）を観測することができる。本報告では図1に示す、それぞれ異なったネットワーク環境に設置した4つのブラックホールセンサにより観測したトラフィックを利用する。

- **センサⅠ**：クラスBのネットワーク内にライブネットとダークネットが混在する構成
- **センサⅡ**：クラスBのネットワーク全てがダークネットである構成
- **センサⅢ**：クラスBのネットワーク内の/24のサブネットがダークネットである構成*1
- **センサⅣ**：クラスBのネットワーク内にライブネットとダークネットが混在する構成

*1　観測している/24のネットワーク以外にもダークネットが存在し、それ以外はライブネットで構成されている。

これら4つのセンサにより得られたトラフィックは、nicterの様々な分析エンジン[3][4]により分析され、分析結果とともに長期保存されている。

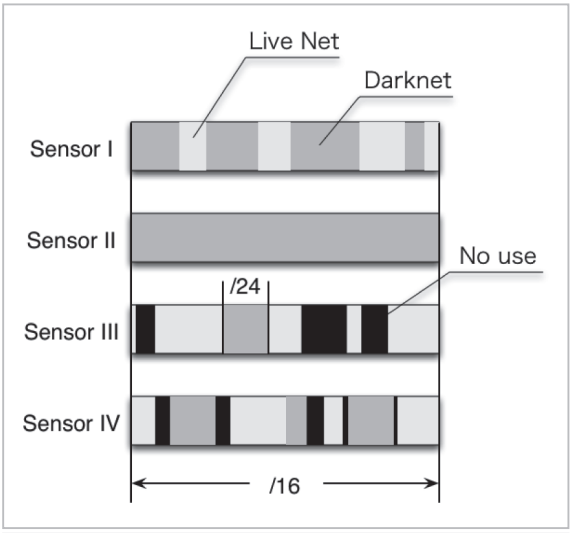


図1 観測ネットワーク概要

nicterではダークネットトラフィックの大規模観測を行う一方で、その原因となるマルウェアを特定するため、マルウェアの収集を行うハニーポットの設置・稼働も行っている。本報告で利用するハニーポットは、250個の連続したIPアドレスに設置しているハニーポットⅠ、1つのIPアドレスに設置しているハニーポットⅡ、ハニーポットⅢ、3つのIPアドレスに設置しているハニーポットⅣ、外部組織よりデータ提供を受けているハニーポットⅤの5種類を用いた。ハニーポットⅠ、Ⅱ、Ⅲは一般的な脆弱性をエミュレーションするソフトウェア（低対話型ハニーポット）により構成し、ハニーポットⅣは、バージョンの異なるWindows OSを実機上でローテーションさせ、未知の脆弱性にも対応できるよう構成している（高対話型ハニーポット）。

以下、**2**で、6年に亘るダークネット観測により得られたサイバー攻撃の大局的な傾向変化を報告する。**3**に、2007年より運用を開始したハニーポットにより収集・解析を行ったマルウェアの統計情報を示す。**4**では、過去から現在に観測されたボットネットによるスキャンから、ボットネットの規模の変化を分析する。最後に、**5**でまとめる。

2 ダークネット観測における攻撃の変遷

2000年代前半には、MSBlasterなどに代表される大規模感染を引き起こすマルウェアが流行した。一方で、nicterによるダークネット観測を開始した2000年代後半のマルウェアは、高度化・巧妙化により利用者に検出される事を避け、静かに潜伏するようになった。大規模感染行動を行えば感染ホストの負荷やトラフィック量が増大し、利用者やネットワーク管理者が感染に気付き易くなるため感染行動は次第に小規模になっていった。また、ボットネットの登場により、複数の感染ホストが協調して動作し、1ホストあたりの感染行動は小規模化していった。その結果、2000年代後半には、ネットワークを介した大規模感染を引き起こすマルウェアはもう出現しないと思われていた[5]。実際に、nicterにおいても観測を開始した当初は、ホスト数に若干の減少傾向が見られていた。

2.1 ユニークホスト数・パケット数の変化

図2、図3にnicterのダークネットモニタリングにより観測されたトラフィックに含まれる、ユニークな送信元IPアドレス数（以下、ユニークホスト数）とパケット数の推移を示す。図では、各センサが観測した1日毎のユニークホスト数とパケット数の移動平均（ウィンドウサイズ：7日間）を示している。各センサの観測開始日は2006年9月5日（センサⅠ）、2004年12月14日（センサⅡ）、2007年10月22日（センサⅢ）、2009年7月10日（センサⅣ）となっている。なお、センサⅠ追加時（2006年9月5日）にセンサⅡのユニークホスト数・パケット数も増加しているが、これはセンサⅡのセンサ規模が/18のネットワークから/16のネットワークに増強されたためである。

図2より、ユニークホスト数は観測開始から2008年の後半にかけて若干の減少傾向にある事がわかる。しかし、2008年11月を境にユニークホスト数がセンサⅠ、センサⅡで約15倍、観測規模の小さいセンサⅢでも約10倍程度の爆発的増加が観測されている。このユニークホスト数の増加は、Conficker wormの大規模感染の影響である[6][7]。Conficker wormによる影響については**2.2**で述

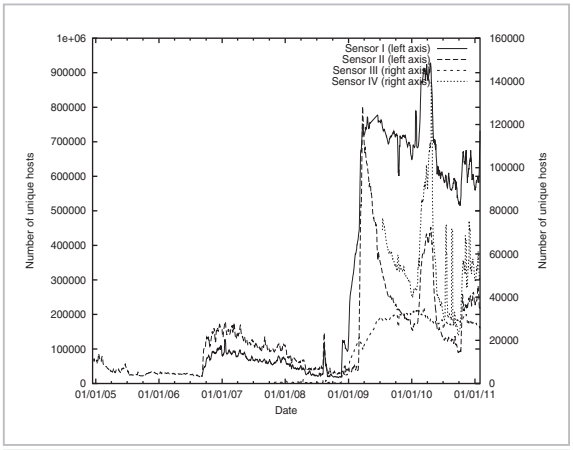


図2 ユニークホスト数推移（7日間の移動平均）

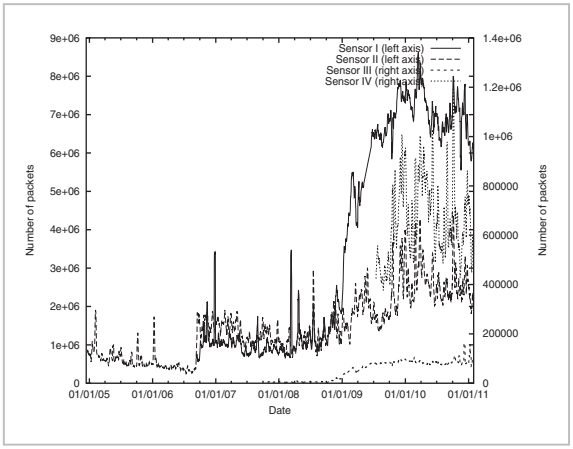


図3 パケット数推移（7日間の移動平均）

べる。

図3より、パケット数もユニークホスト数の推移と同様に、2008年後半を境に急激な増加を観測している。2008年11月以前のパケット数は、乱高下はあるものの平均的にほぼ横ばいである事が分かる。ユニークホスト数は減少している一方でパケット数は横ばいになっている事から、1ホストあたりの平均的なパケット送信数は若干増加傾向にある事が図より読み取る事ができる。一方で、2008年11月以降では、最も多くのパケットを観測しているセンサⅠでパケット数が約7倍程度と、ユニークホスト数の増加率（約15倍）と比べパケット数の増加率は半分程度になっている。つまり、1ホストあたりの平均的なパケット送信数は2008年11月以前と比べ、ほぼ半分になっている。

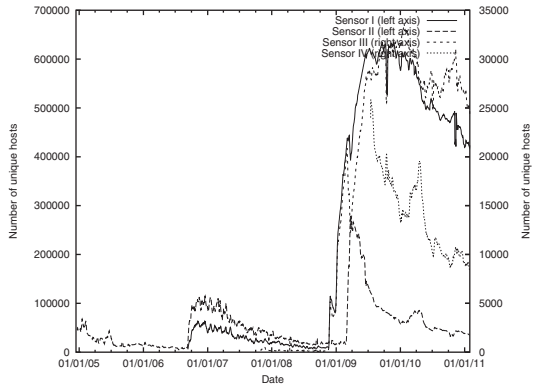
以上をまとめると、2000年代後半から2008年11月以前までは、感染ホスト数は若干の減少傾向が観測されていた。一方で、送信パケット数は、ほぼ横ばいで推移している事から1ホストあたりの平均的な送信パケット数は、若干増加傾向にあった。そして、Conficker ワームが発生した2008年11月以降、感染ホスト数は爆発的に増加するとともに、1ホストあたりの平均的なパケット送信数は約1/2になっている事が観測された。

2.2 Conficker ワームのネットワークに及ぼす影響

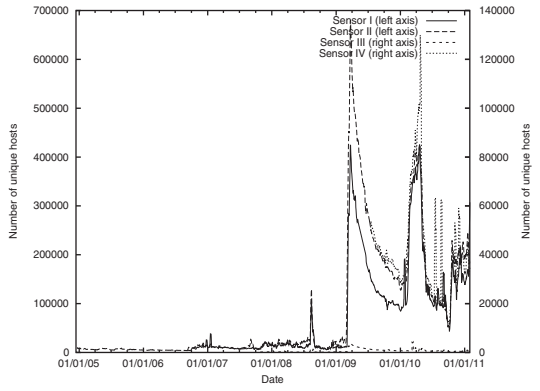
2008年11月頃からWin32/Conficker（別名Downadup）と呼ばれるワームによる大規模感染が社会的な問題となっている。このワームは、感染拡大の一手段としてWindows Serverサービスの脆弱性（MS08-067）を利用する事が知られている。この脆弱性は、ネットワークを経由して攻撃を行う事が可能であるため、Conficker に感染したコンピュータ（ホスト）は次の感染先を探すため、ネットワークに対して広範囲にスキャンを行う。我々は、文献[6]および文献[7]においてConficker.A（2008年11月21日に発生）、Conficker.B（同年12月29日に発生）、Conficker.C（2009年2月20日に発生）、そして、Conficker.D（2009年3月4日に発生）による影響の分析を報告した。Conficker は、2009年4月8日に発生が確認されたConficker.Eを最後に、Microsoft からの亜種の報告は行われていない[8]。

図4にプロトコル別ユニークホスト数（TCP、UDP）および、Conficker ワームが感染に利用する445/TCPに対するユニークホスト数の推移を示す。図4（a）、（c）より、Conficker の発生が確認された11月以降にセンサⅠ、センサⅢで観測したTCPパケットを送信するホストの大多数は445番ポートに送信している事が確認できる。一方で、センサⅡ、センサⅣは445/TCPの影響は特に観測されず、図4（a）、（b）より、4ヶ月後の2009年3月頃よりTCP、UDPに対するユニークホストの増加を観測している。2009年3月4日に発見されたConficker.DはP2Pランデブー機能を有し、ハイポート（一般的に1024番ポート以上のポート番号）へのTCP、UDPスキャンを広範囲に送信することが報告されている[7]。そのため、スキャンにより影響を受けるネットワークが変化し、センサⅡ、センサⅣの傾向が変化したものと考えられる。

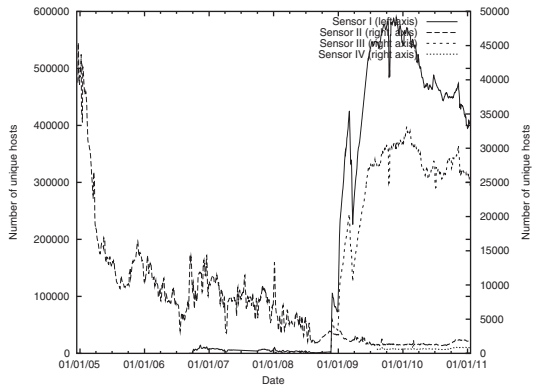
445/TCPの影響を受けていないセンサⅡ、センサⅣは、3月18日をピークにTCP、UDPともにユニークホスト数は減少している。TCP、UDPのユニークホスト数はほぼ同様の減少傾向を示している。UDPユニークホスト数に関してはセンサⅠも同様に減少していることから、P2Pランデブー機能を有したConficker.Dが減少し、ハイポートのスキャンが減っている事が考えられる。しかし、445/TCPに対するスキャンはセンサⅠ、センサⅢで2010年2月頃のピークより2割程度減少しているが、2011年1月現在でも大量に観測されている。したがって、Conficker.D以外の亜種は現在でも多くの感染ホストが存在しているものと推測される。



(a) TCPユニークホスト数



(b) UDPユニークホスト数



(c) 445/TCPユニークホスト数

図4 ネットワークに及ぼすConfickerワームの影響（7日間の移動平均）

3 マルウェアの推移

nicterでは、マルウェアによるスキャンの原因追求やその対策のため、2007年よりハニーポットを稼働させ、マルウェアの動作解析を行っている。様々なタイプのマルウェアに対応するため、低対話型ハニーポット、高対話型ハニーポット、webクローラなどの性質や環境（OS）が異なる複数のハニーポットが稼働している。2011年1月現在までに、160万以上の検体を取得し解析を行っている。図5に、性質の異なる5つのハニーポットによって取得したマルウェア種類*2の累計を示す。5つのハニーポットの運用開始時期は異なっているが、現在までに合計で約9,000種類のマルウェアを取得している。

図6に、マルウェア名トップ10を示す。ここでは、Symantec社のAntiVirusソフトウェアを用

*2 ハニーポットごとに取得したハッシュ値（MD5値）が異なるマルウェア数

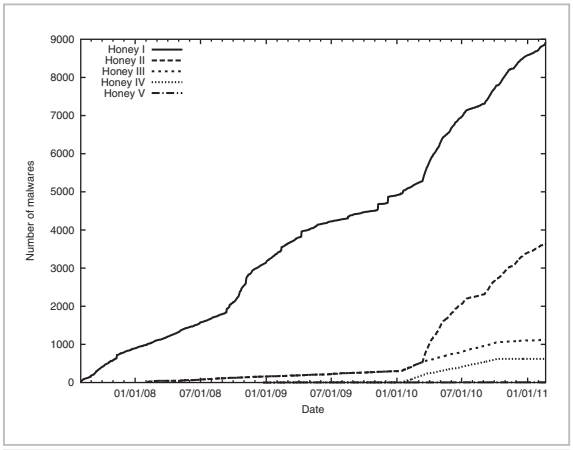


図5 取得マルウェア（積み上げ・累計）

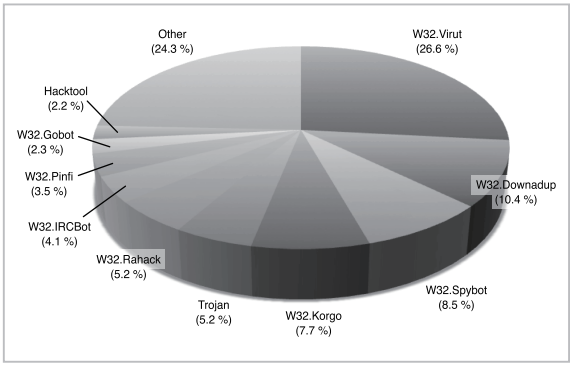


図6 取得マルウェアファミリ

いて検体名の取得を行っており、亜種による違いは考慮していない。例えば、W32.Virut は W32.Virut.A や W32.Virut.B など様々な亜種の存在が確認されているが、いずれも W32.Virut として集計を行っている。全体は約 350 種類に分類され、そのうち約 1/4 を W32.Virut が占めていた。上位を占めている W32.Virut、W32.Spybot、W32.Korgo などは 2007 年以前から存在する比較的古いマルウェアであるにもかかわらず、全体の半数近くを占める結果となった。また、W32.Downadup（別名 Conficker）は、発見から 2 年程で第 2 位に位置し、感染規模の大きさがうかがえる結果となった。1 ヶ月間（2010 年 12 月）の取得件数を見ても、61 検体中 33 検体が W32.Downadup という結果であり、現在でも大きな脅威になっていることが分かる。

4　ボットネットの規模の変化

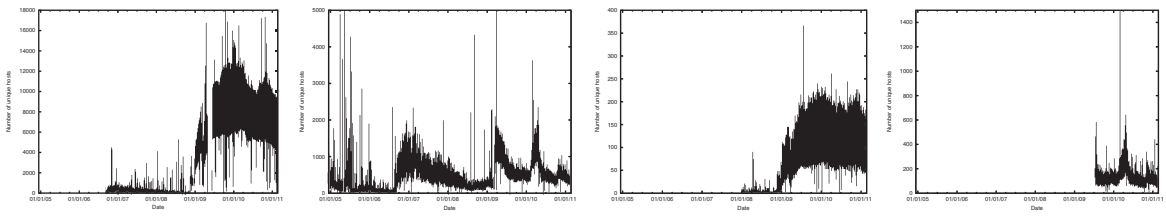
ダークネットでは、ボットなどによる脆弱なホストの探索のための広範囲で大規模スキャンが観測できる。ボットは、IRC などを用いた C&C サーバからの指令を受け取り協調動作を行う。そのため、同じ IRC チャネルに接続しているボットは、同じタイミングで指定された動作を行うことになる。したがって、単位時間あたりのユニークホスト数の急激な増加に着目する事で、ボットによるスキャンの可能性があるトラフィックを検出できる。ここでは、以下の事象をボットネットからのスキャンと定義する。

1）複数のホストが同時期に協調的に動作を行う
2）感染拡大のために広域スキャンを行う
3）特定の脆弱性を探索する

ダークネットでは、特定の脆弱性を狙うためのファーストコンタクト（通信を開始するためのパケット）が観測されるため、TCP、UDP パケットを送信するユニークホスト数の推移により、ボットネットの規模の推測を行うことができる。そこで、5 分間のユニークホスト数の推移から一定以上のユニークホスト数の増加を検出し、ボットネットによるスキャンを抽出する。図 7、図 8 に TCP、UDP パケットを送信した 5 分ごとのユニークホスト数の推移を示す。各図より複数の部分で急激なホスト数の増加（スパイク）を観測している事が分かる。

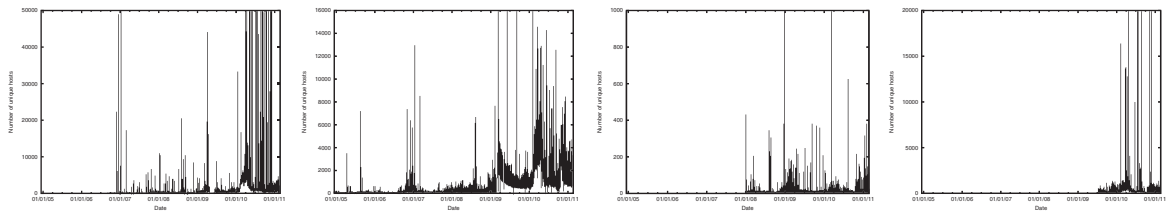
4.1　ボット活動時期の抽出方法

図 7、図 8 より、各センサ、各プロトコルでユニークホスト数の急激な増加（スパイク）を観測している。**4** に示した仮定より、同時期に特定プロトコルを利用したユニークホスト数の増加を観測した場合、それをボットによるスキャンであると



a）センサⅠ　b）センサⅡ　c）センサⅢ　d）センサⅣ

図7 5分間のユニークホスト数の推移（TCP）



a) センサⅠ　b) センサⅡ　c) センサⅢ　d) センサⅣ

図8 5分間の観測ユニークホスト数の推移（UDP）

見なす。以下にボットによるスキャンを抽出する方法を示す。まず、5分ごとに観測したユニークホスト数 h_i の移動平均

$$a_t = \frac{\sum_{k=t-m}^{t} h_k}{m} \tag{1}$$

を求める。ここで、m は移動平均を計算するために用いるデータの数（期間）を示す。次に、移動平均 a_t とユニークホスト数 h_t との分散

$$s_t = \sqrt{\frac{\sum_{k=t-m}^{t} (a_k - h_k)^2}{m}} \tag{2}$$

を求める。最後に、ユニークホスト数 h_t と平均値 a_t との差と、直前の分散値との比

$$r_t = \frac{(h_t - a_t)}{s_{t-1}} \times h_t^{\frac{1}{4}} \tag{3}$$

を求める。分散値は平均的な揺れ幅（平均値との差）を示すため、直前の分散値 s_{t-1} と平均値との差 $(h_t - a_t)$ の比を求める事でユニークホスト数の急激な増加を検出する事が可能となる。しかし、分散値はユニークホスト数の増加（移動平均の増加）により大きくなる傾向がある事から比率が小さくなってしまうため、$h_t^{\frac{1}{4}}$ により重み付けを行っている。最終的に r_t が閾値以上の値となる所にボットのスキャンが含まれている事になる。

4.2 ボットによるスキャン抽出

ここでは、**4.1** に示した方法により、図7、図8からボットによるスキャン（スパイク発生部）の抽出を行う。観測センサ、プロトコルにより観測規模が異なるため、それぞれにおいて閾値を設定し、ボットのスキャンを抽出した。表1にボットによるスキャンの抽出を行った結果を示す。ここで、移動平均の計算に用いた期間は $m = 288$（24時間）とした。

本報告では、ユニークホスト数の増加が比較的大きな部分を抽出するため閾値を高く設定した。その結果、631件の事象がボットのスキャンであると判定された。平均すると年間100回程度ボットの活動が観測されたことになる。

4.3 ボットネット規模の推定

図9に、各月ごとに観測されたボットのスキャン回数と、そのとき構成していた平均ボットネットサイズ（観測されたボットネットを構成するボットの数の平均）を示す。このとき、24時間の移動平均を定常時のユニークホスト数（ボット以外のマルウェアによるスキャン）と見なし、ボットネッ

表1 抽出したボットネットのスキャン

センサ	プロトコル	閾値	検出数
センサⅠ	TCP	30	99
	UDP	70	142
センサⅡ	TCP	30	90
	UDP	80	77
センサⅢ	TCP	10	66
	UDP	25	108
センサⅣ	TCP	20	28
	UDP	70	39

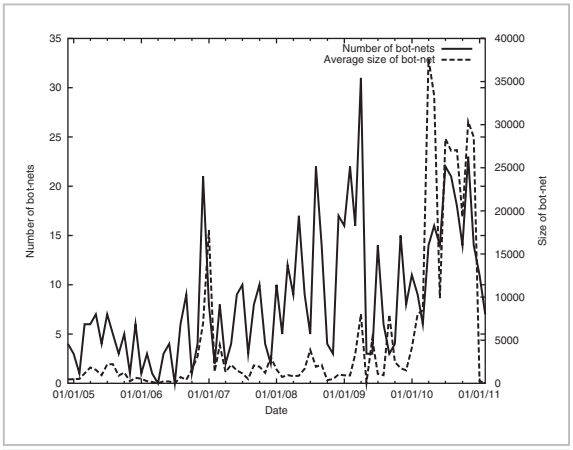


図9 ボットネットの規模の変化

トのサイズは定常時に観測されるユニークホスト数からの増加分 $(h_j - a_j)$ とした。

ボットネットによるスキャンの観測回数は、2010年前後は一時的に減少しているが、それ以外は年々増加している事がわかる。一方で、観測されたボットネットのサイズ（構成するボットの数）は、2010年以降に急増している事が分かった。このことより、近年では1つあたりのボットネットは大規模化し、スキャンの効率化、攻撃（DDoSなど）やスパム送信の大規模化が進んでいる事が考えられる。実際に、ボットネットを利用したスパムメール送信は多く行われており、ボットネット管理者は金銭目的でボットネットの貸し出し等を行っていると言われている。そのため、大規模なボットネットほど、高額で取引されている事が知られている[9]。

5 おわりに

nicterプロジェクトで蓄積された長期ネットワーク観測の結果と、その分析を行った。2008年前半までは、ダークネットに対してスキャンを行うホスト数は年々減少し、ネットワークを用いた大規模感染はもう起こり得ないとまで言われていた。しかし、Conficker の発生により状況は一変した。Conficker のネットワークに及ぼす影響は、現在でも継続しており、観測されるダークネットトラフィックの半数以上を占めている。

nicterプロジェクトで稼働させているハニーポットのマルウェア収集結果からも、W32.Virut、W32.Spybot、W32.Korgo など、過去に猛威を振るったマルウェアが現在でも検出されている事が明らかとなった。したがって、Conficker のような大規模感染を引き起こしたマルウェアは今後も消滅する事無く存在することが予想され、継続して経過観測を行う必要があると考えられる。

ボットによるスキャンの発生件数は、2010年前後でやや減少傾向が見られるが、全体的には増加傾向にあることが分かった。一方で、ボットネットの規模は2010年以降急増し、大規模化が進んでいる事が確認できた。今後も、ボットネット管理者が金銭搾取を目的としてボットネットの拡大を図る事が考えられるため、継続的な観測と分析が必要である。

参考文献

1 Koji Nakao, Katsunari Yoshioka, Daisuke Inoue, and Masashi Eto, “A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities,” The 2nd Joint Workshop on Information Security (JWIS07), pp. 267–279, 2007.

2 Daisuke Inoue, Masashi Eto, Katsunari Yoshioka, Syunsuke Baba, Kazuya Suzuki, Junji Nakazato, Kazuhiro Ohtaka, and Koji Nakao, “nicter: 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 鈴木和也，橋本良徳，馬場俊輔，“長期的傾向変化に着目したトラフィック解析システム,” Symposium on Cryptography and Information Security (SCIS 2007), 1F2-3, 2007.

4 Daisuke Inoue, Katsunari Yoshioka, Masashi Eto, Yuji Hoshizawa, and Koji Nakao, “Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities,” IEICE Trans. Information and Systems, Vol. E92-D, No. 5, May 2009.

5 井上大介，中尾康二，“マルウェアって？，” 情報処理，Vol. 51, No. 3, pp. 237–243, 2010.
6 中里純二，大高一弘，島村隼平，中尾康二，“nicter によるネットワーク観測及び分析レポート，” 信学技法，Vol. 109, No. 33, pp. 15–20, 2009.
7 中里純二，大高一弘，島村隼平，中尾康二，“nicter によるネットワーク観測及び分析レポート — Conficker の経過観測およびマクロとミクロの相関分析の一例 —，” 情処研報，Vol. 2009-CSEC-46, No. 18, 2009.
8 Microsoft セキュリティ TechCenter，“Windows を Conficker ワームから守る，”
http://technet.microsoft.com/ja-jp/security/dd452420
9 CNET News，“Botnet services for hire: $8.94 an hour,”
http://news.cnet.com/8301-1009_3-20005844-83.html

（平成 23 年 6 月 15 日 採録）

中里純二（なかざとじゅんじ）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室専攻研究員　博士（工学）
ネットワークセキュリティ、マルウェア解析、暗号理論、プライバシ保護

大高一弘（おおたかかずひろ）
ネットワークセキュリティ研究所
サイバーセキュリティ研究室主任研究員
ネットワークセキュリティ、宇宙天気