Vol.2009-CSEC-46 No.18
2009/7/2

nicter によるネットワーク観測および分析レポート

– Conficker のの経過観測およびマクロとミクロの相関分析の一例 –

中里 純二[†1] 大高 一弘[†1]
島村 隼平[†2] 中尾 康二[†1]

本報告では，インシデント分析センター nicter における長期間のネットワーク観測およびマルウェアの自動解析で得られた，いくつかの特徴的な事象をレポートする．特に，2008 年 11 月以降，大規模感染を引き起こしている Conficker の経過観測と，その他新種のマルウェアの動向について，nicter のミクロ–マクロ相関分析の一例を交えながら報告する．

Network Observation and Analysis Report on nicter

– Continuous Observaion of Conficker and a Primary Example of Maco-Micro Correlation Analysis –

Junji Nakazato ,[†1] Kazuhiro Ohtaka ,[†1]
Jumpei Shimamura [†2] and Koji Nakao [†1]

In this report, we show a continuous observation report of Conficker, which is a pandemic malware since November 2008, based on the darknet monitoring in the nicter. We also show an activity of a certain new malware with a primary example of the macro-micro correlation analysis in the nicter.

†1 情報通信研究機構
National Institute of Information and Communications Technology
†2 フォースクーナ株式会社
ForSchooner Inc.

1. はじめに

2008 年 11 月頃から Win32/Conficker（別名 Downadup）と呼ばれるマルウェアによる大規模感染が社会的な問題となっている．このマルウェアは，Windows OS の脆弱性（MS08-067）を利用して感染拡大を行う事が知られている．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．そのため，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，このようなマルウェアの感染活動等がネットワークに及ぼす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 アドレス空間で，サービスを一切提供しないネットワーク（ダークネット）をモニタリングしている．既に，ダークネットの長期的な観測によって得られた観測結果より，パケット数・ホスト数の統計値を示し，攻撃のステルス化（1 ホスト辺りの攻撃パケット数の減少）が行われていることを報告した[1)]．また，いくつかの具体的な事例をもとに，攻撃ホストごとのスキャン方法（振舞）に着目した振舞タイプによる詳細分析を行い，新たな攻撃の増加や振舞タイプの変化から Win32/Conficker およびその亜種の出現が確認できたことを報告した．

本報告では，インシデント分析センター nicter[2),3)] によって観測されたネットワークトラフィックを分析し，長期的観測を行う事で得られる傾向の変化や，振舞の変化等を報告する．さらに，マルウェア検体の解析により得られた結果から，事象を起こしている原因として可能性のある振舞を分析し，ダークネットで観測される事象と，マルウェア解析によって得られる原因との結びつけを行う．

第 2 章では，nicter の概要を説明する．特にスキャンの傾向を捉えることが可能な振舞分析エンジンと，マルウェア検体の解析を行うミクロ解析システムについて説明する．第 3 章では，1) で報告した 2009 年 2 月末以降の観測結果として，2009 年 3 月と 4 月を加えた結果を紹介する．特に Win32/Conficker による影響の報告を行う．第 4 章では，ミクロ解析システムにより解析されたマルウェア検体の振舞タイプと，現在ダークネットで観測されている振舞タイプの比較から，事象と原因の結びつけを行う．最後に第 5 章でまとめる．

2. nicter プロジェクト

情報通信研究機構が研究・開発を行っている nicter プロジェクトでは，**図 1** に示すように 4 つのコンポーネントからなっている．まず，多地点によるネットワーク攻撃の情報を収集・解析する「マクロ解析システム」，ハニーポット等を用いて捕獲したマルウェア検体を

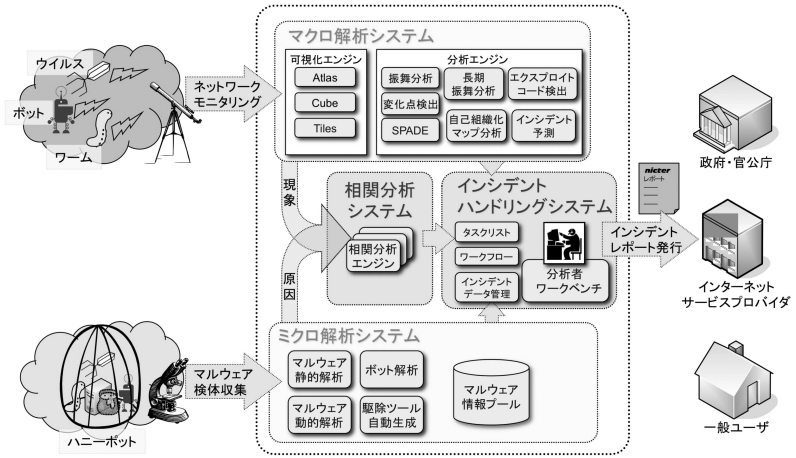


図 1 nicter 構成図

解析する「ミクロ解析システム」，ネットワーク上で起きている「事象」（マクロ解析システムにより解析）とその「原因」（ミクロ解析システムにより解析）を結びつける「相関分析システム」，さらにオペレータとのインターフェイスである「インシデントハンドリングシステム」がある．この 3 つのコンポーネントにより，インターネット上で発生している事象がどのようなマルウェアに起因しているかを実時間で推定することができる．

マクロ解析では，ブラックホールセンサをダークネットに設置し，広域なネットワークイベントの収集・解析を行っている．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 TCP SYN に対する ACK）を観測することができる．本報告では下記に示す異なった特徴を持つ 3 つのブラックホールセンサにより観測したイベントを利用する．

- 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 I）
- 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 II）
- 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 III）

3 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により分析され，結果とともに長期的に保存される．

ミクロ解析では，ハニーポット等で捕獲したマルウェア検体の解析を行う．検体の解析方法には，「静的解析」と「動的解析」の 2 種類がありそれぞれの結果は，データベースに蓄積・保存される．

本報告では，事象の分析にマクロ解析システムの「振舞分析エンジン[5)]」によって得られた結果を，原因の分析にミクロ解析システムの「動的解析エンジン」によって得られた結果を利用する．

2.1 振舞分析エンジン

振舞分析エンジン[5)] は，攻撃元ホストの挙動に注目した解析を行う．具体的には，攻撃元ホスト毎に “送信元ポート数”，“送信パケット数”，“宛先ポート数”，“宛先 IP アドレス数”，そして “宛先 IP アドレスの遷移”（宛先の IP アドレスがシーケンシャルになっているか，ランダムになっているかの 2 値）の 5 つのパラメータを基にスキャンの形状を分類する．さらに，“宛先ポート番号”，“パケットのプロトコル[⋆2]” とともに MD5 値を計算する．本報告では，この MD5 値のことを “振舞タイプ” と呼ぶ．振舞分析の特徴は，スキャン方法が同じホストを同じ振舞タイプとして自動分析することが可能であるところにある．また，ダークネットトラフィックを振舞タイプごとに分け，その統計量の変化を観測することが可能になる．

図 2 に，振舞分析エンジンの可視化例を示す．この図は，送信元ホストごとに描かれるもので，上述した振舞タイプの計算に用いるパラメータ群が視覚的に配置されている．中央から左半面が送信元情報を，右半面が宛先情報を示しており，左半面の横軸には時刻（最大 30 秒間），縦軸には送信元ポート番号，右半面の横軸には宛先 IP アドレス，縦軸には宛先ポート番号がマッピングされる．図 2 の場合，送信元ホストは送信元ポート番号を徐々に増やしつつ，一定間隔で，宛先 IP アドレスを増やしながら同じ宛先ポート番号にスキャンを行っていることが分かる．つまり，ネットワークスキャンを行っていることが視覚的に理解できる．

⋆1 観測している/24 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．
⋆2 TCP，UDP，ICMP で分類する．TCP の場合はさらに，TCP フラグの情報を付け加える．

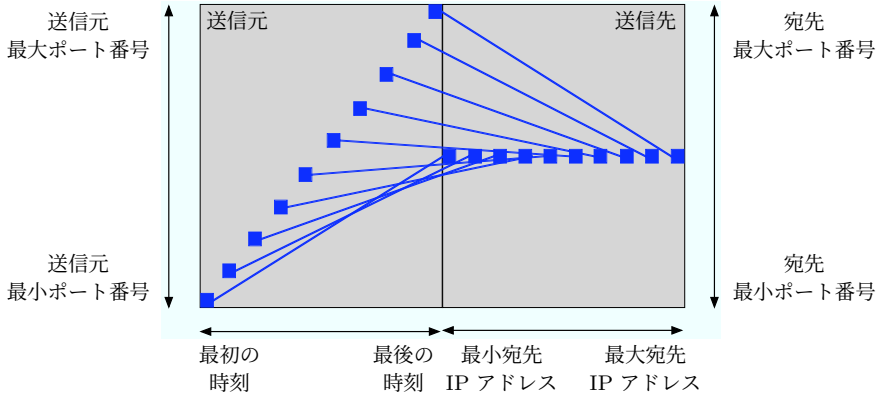


図 2 振舞分析エンジンの可視化例

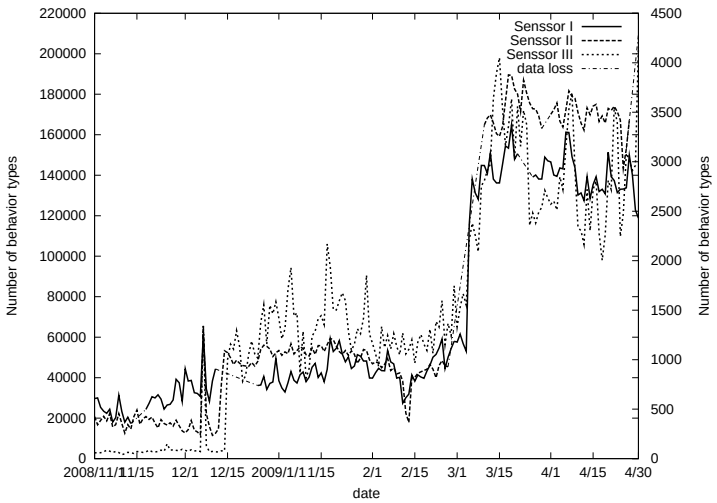
2.2 ミクロ解析システム

ミクロ解析システム[4] では，ハニーポット等によって収集されたマルウェア検体の解析を自動で行うことが可能である．マルウェア検体は，コードレベルでの解析である「静的解析」と，インターネットを模擬した環境（箱庭環境）の中での実動に基づく解析である「動的解析」が行われる．本報告では，ミクロ解析システムの動的解析エンジンを用いた解析結果を用いる．

動的解析エンジンでは，犠牲ホスト（実際にマルウェアを感染させるホスト）を箱庭環境内に完全隔離し，その対向に DNS や IRC 等の多数のダミーサーバーからなる擬似インターネットを設置することで，安全な動的解析を実現している．犠牲ホストは OS 自動復元機構と API フック機能を有する実マシンによって構成されている．動的解析エンジンによって，犠牲ホスト内でのマルウェアの動作や，マルウェアのネットワークに対する行為（サーバアクセスやスキャン等）を自動的に抽出することができる．本報告の後半（第 4 章）では，ある新規マルウェアを動的解析した結果，得られたスキャンについて，その振舞タイプを分析し，現在ダークネットで観測されているスキャンとの比較・検討を行う．

3. 長期観測報告

ここでは，2008 年 11 月 1 日 ～ 2009 年 4 月 30 日までの 6ヶ月間に及ぶ観測結果を報告する．**図 3** に観測パケット数 (a)，ユニークホスト数 (b)，445/TCP に限定したユニークホスト数 (c) の推移を示す．ここで，ユニークホスト数とは，1 日に観測されたホストのユニーク数（IP アドレスの重複を取り除いた数）を表す．



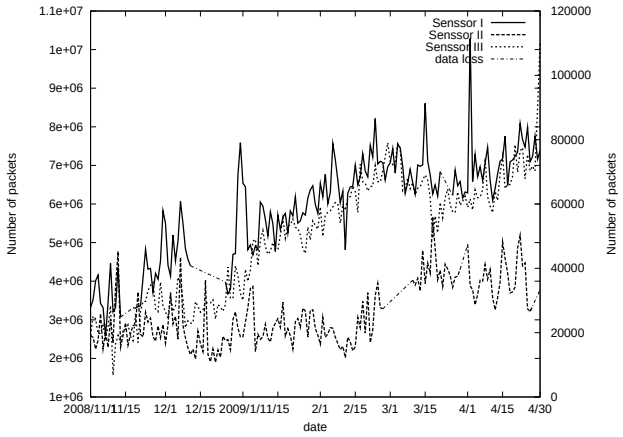
センサ III は第 2 軸を利用

図 4 各センサで観測された振舞タイプの種類数

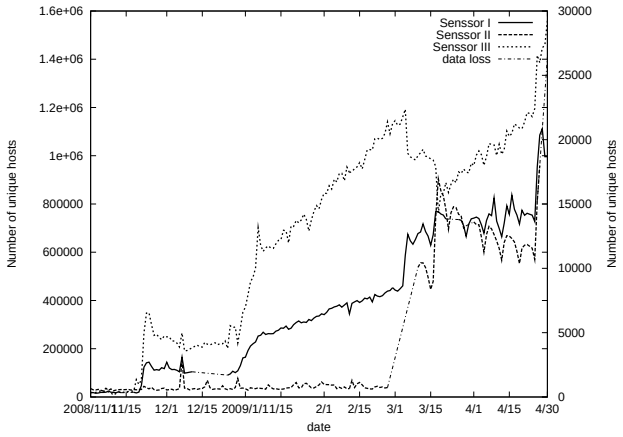
3.1 長期的な傾向

図 3 (a) より，パケット数は若干増加傾向にあるが，増加幅は 2 倍から 3 倍程度とほぼ横ばいになっていることが分かる．図 3 (b) より，1) で報告した 2009 年 2 月 28 日以降でもユニークホスト数は依然として増加傾向にあり，多くのホストが新たに何らかのマルウェアに感染をしていることが確認できる．観測されたパケット数がほぼ変わらず，ユニークホスト数が増加を続けていることから，1 ホスト辺りの送信パケット数はさらに減少し，ますます攻撃のステルス化が進んでいることが分かる．また，1) の報告で Conficker による影響をほとんど受けていなかったセンサ II でも 3 月頃よりユニークホスト数の増加が確認できる（2009 年 2 月 27 日 ～ 2009 年 3 月 9 日まではデータが欠損している）．しかし，図 3 (c) より，445/TCP に対するユニークホスト数はセンサ II では変化が見られないことから，1) で報告された Conficker.A，Conficker.B による影響ではないことが分かる．

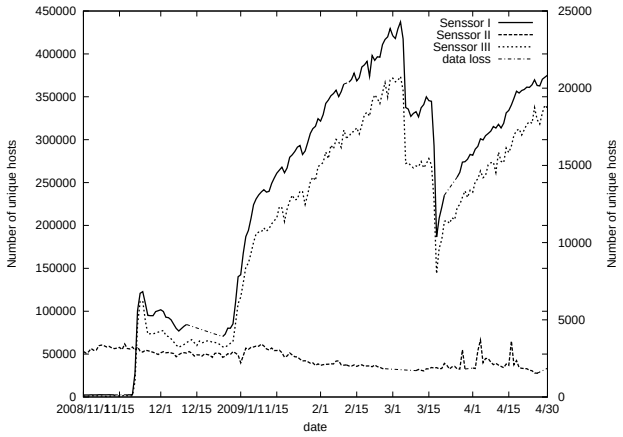
ここで，各センサにおいて観測された振舞タイプの種類数の推移を**図 4** に示す． 図 4 より，2008 年 12 月 10 日前後と 3 月を境に振舞タイプの種類の急激な増加が観測されている．



センサ III は第 2 軸を利用
(a) 観測パケット数推移



センサ III は第 2 軸を利用
(b) 観測ユニークホスト数推移



センサ II，センサ III は第 2 軸を利用
(c) 445/TCP に限定した観測ユニークホスト数推移

図 3 2008 年 11 月 1 日 ～ 2009 年 4 月 30 日の観測統計データ

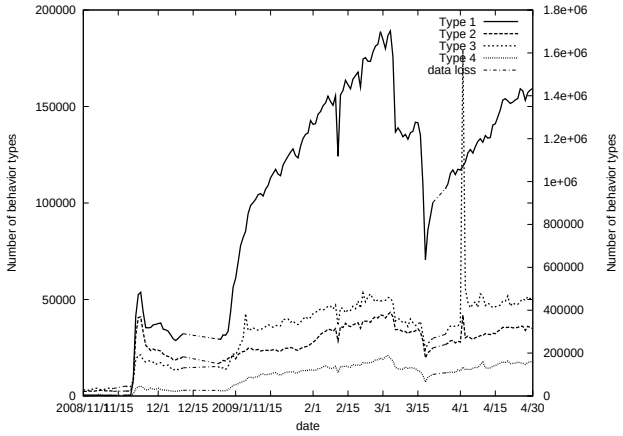
特に，ユニークホスト数の急激な増加が観測されている 3 月頃には振舞タイプの種類が 2 倍から 3 倍程度増えていることが分かる．

以上のことより，3 月上旬にマルウェアの動きに大きな変化が起こった可能性が考えられる．特に，センサ I やセンサ II のように規模の大きなダークネットを観測しているセンサでユニークホスト数が増えていることから，Conficker.A や Conficker.B で見られた近くのネットワークへのスキャン（感染ホストの IP アドレスの第三オクテッドを変更し，スキャンを行う[6]）から，ネットワーク全体に対するランダムなスキャンへと変わっていることが予想される．

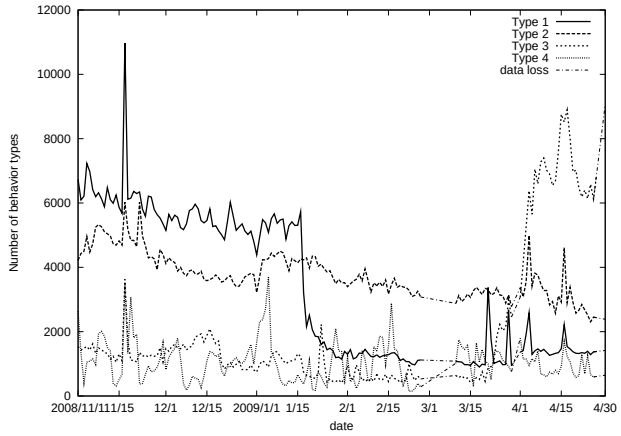
3.2 Win32/Conficker の傾向変化報告

1) では，Conficker.A（2008 年 11 月 21 日），Conficker.B（同 12 月 29 日）そして，Conficker.C（2009 年 2 月 20 日）が Microsoft により発見された時の，ユニークホスト数の推移，振舞タイプの変化を報告した．本報告ではその後の傾向として Conficker.D（2009 年 3 月 4 日）の発見による影響の分析を行う．**図 5** に 1) で報告された 4 つの振舞タイプの観測数推移を示す．また，**図 6** には 4 つの振舞タイプの可視化結果を示す．可視化を行うことで振舞タイプ 1 は 2 つのパケットを，振舞タイプ 2 では 3 つのパケットを，振舞タイプ 3 では 1 つのパケットを，振舞タイプ 4 では 4 つのパケットをそれぞれ同一のポート（445/TCP）に送信していることが分かり，それぞれの振舞が異なっていることが視覚的にも容易に認識できる． 図 5 より，Conficker.D が発見された 3 月 4 日前後から全てのセンサにおいて振舞タイプ 1 が急激に減少していることが分かる．また，図 3 (b) に示す通り，同時期にユニークホスト数の増加も観測している．特に，センサ II では増加前（センサ停止前）の 2 月 26 日の時点からピーク時（3 月 18 日）に約 30 倍程度の数のユニークホストを観測した．一方で，445/TCP に対するホストに限定した場合（図 3 (c)），ユニークホスト数の減少が観測されていることから Conficker.D の振舞に変化があったことが予測される．

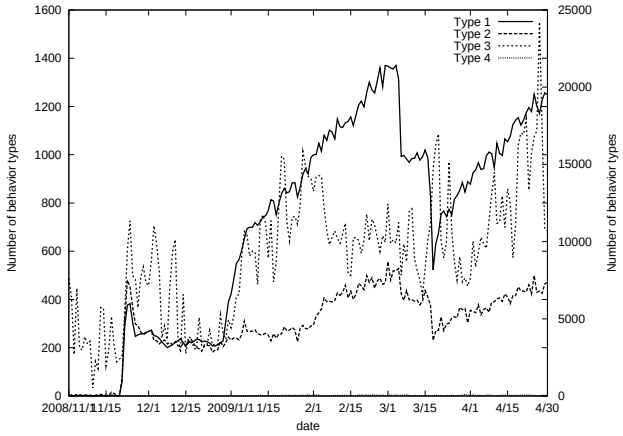
同時期に，振舞タイプの種類数の増加も観測している（図 4）．このとき，振舞タイプの多くが，良く知られたポート番号以外の非常に大きなポート番号に対して TCP パケットを 2 回または，UDP パケットを 1 回送信するという特徴があることが分かった．この振舞タイプの可視化結果を**図 7** に示す．実際には数多くの異なった振舞タイプが観測されているが，可視化を行うとほとんどが図 7 に示した結果となっていた． Microsoft の解析によると，Conficker.D に感染すると，P2P 接続を待ち受けるために TCP と UDP のポートをそれぞれオープンすることが分かっている[7]．待ち受け用のポート番号の決定には，感染ホストの IP アドレスが利用されることから，宛先 IP アドレスが分かれば P2P に接続することが可能である．しかし，感染ホストの IP アドレス情報は無いため，他の感染ホストに P2P



タイプ 1 は第 2 軸を利用している
(a) センサ I における各振舞タイプの観測数推移



(b) センサ II における各振舞タイプの観測数推移



タイプ 1 は第 2 軸を利用している
(c) センサ III における各振舞タイプの観測数推移

図 5 Conficker の影響による振舞の推移

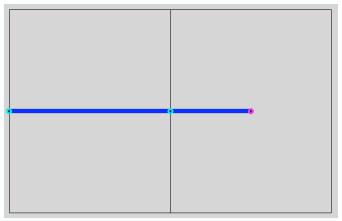
接続を行う場合，ランダムな宛先 IP アドレスから同様に宛先ポート番号を決定し，スキャンを行うとされる．従って，スキャンの方法が感染を広げる場合と違い，ランダムな IP アドレスに対して接続を試みるため，広範囲でスキャンパケットが観測可能である．

振舞タイプの種類数が増加したことは，宛先 IP アドレスごとに送信ポート番号が異なり，同じ挙動をしていても振舞タイプが変わったためだと考えられる．一方で，振舞タイプの種類数は センサ I，センサ II で 15 万前後に，センサ III で 3 千程度に収束していることから，同一 IP アドレスには同一ポート番号へ接続するため，振舞タイプの種類は一定以上増えない物と考えられる．また，ランダムな IP アドレスに対してスキャンを行うことで，Conficker.A や Conficker.B では影響が見られなかったセンサ II でも，数多くの振舞タイプを観測していると考えられる．

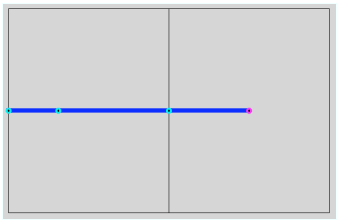
ここで，ある特定のホストに着目して振舞タイプの変化を観測した．その結果，センサ I では 2008 年 11 月 21 日に初めて攻撃を確認した（振舞タイプ 1）．その後，4 日間同振舞タイプを観測し，一端収束したかのように見えたが，再び 2009 年 3 月 7 日より攻撃を観測した．このとき，振舞タイプは前述の Conficker.D による P2P 接続のためと思われる TCP と UDP パケットによるスキャンに変わっていた．また，当該ホストはセンサ III でも同様に 2008 年 11 月 21 日に初めて攻撃（振舞タイプ 1）を観測したが，センサ II では，2009 年 3 月 10 日の Conficker.D と思われる攻撃まで観測が得られなかった．同様に，11 月頃よりセンサ I，センサ III では 445/TCP に対する振舞タイプを観測し，その後 3 月 10 日前後に非常に大きなポート番号に対する振舞タイプ（TCP，UDP）に変化し，センサ II でも同ホストからの非常に大きなポート番号に対する振舞を観測する様になる事例が多数存在していた．逆に，全てのセンサで 445/TCP に対する振舞タイプは観測していなかったが，新たに 3 月 10 日前後に Conficker.D の振舞タイプと考えることが可能な観測も多くあり，ユニークホスト数の増加に繋がっていると考えられる．

4. マクロ – ミクロ分析

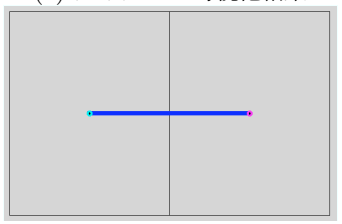
nicter では，ハニーポットやセキュリティベンダ等から最新のマルウェア情報の提供を受けている．ここでは，観測期間である 2009 年 3 月，4 月に取得したマルウェア検体の解析結果と，その検体がダークネットに及ぼす影響を調査した．本報告では，3 月に取得した検体 A の解析を行う．検体 A の詳細を**表 1** に示す． ここで，マルウェア検体名は市販のアンチウィルスソフトウェアによって付けられた名前を示す．複数の製品を用いて検証を行っているため，名前も複数になる．



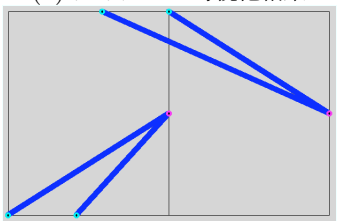
(a) タイプ 1 の可視化結果



(b) タイプ 2 の可視化結果

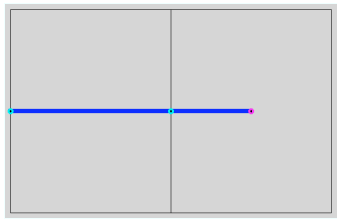


(c) タイプ 3 の可視化結果

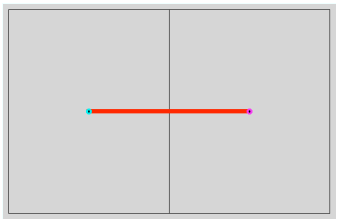


(d) タイプ 4 の可視化結果

図 6 Conficker が持つ 4 つの振舞タイプ



(a) TCP を送信する振舞タイプ



(b) UDP を送信する振舞タイプ

図 7 Conficker.D により増加した振舞タイプの可視化例

4.1 ミクロ解析による振舞分析

本報告では，マルウェアの振舞タイプに着目した分析を行う．そこで，検体 A がもつ振舞タイプを特定する必要がある．**図 8** に検体 A が解析環境で行ったスキャンの一部を示す．スキャンパターンを見ると，/24 のネットワークに対して 445/TCP のスキャンを行っていることが分かる．

動的解析エンジンにより取得したスキャンパターンを振舞分析エンジンにより分析した結果，振舞タイプ 4-A が観測された．**図 9** にこの振舞タイプの可視化結果を示す 視覚的にもシーケンシャルなスキャンを 445/TCP に対して行っていることがわかる．

表 1 ミクロ解析システムにより解析を行った検体 A

検体ハッシュ値	検体名
a2eaf57c47a118e91a5edf694685eee7	W32.SillyFDC.BAW
	W32/Spybot.worm.gen
	BKDR_AGENT.ANCQ

```
IP 192.168.20.21.1061 > 192.0.0.14.445: S
IP 192.168.20.21.1062 > 192.0.0.15.445: S
IP 192.168.20.21.1063 > 192.0.0.16.445: S
IP 192.168.20.21.1064 > 192.0.0.17.445: S
IP 192.168.20.21.1065 > 192.0.0.18.445: S
IP 192.168.20.21.1066 > 192.0.0.19.445: S
IP 192.168.20.21.1067 > 192.0.0.20.445: S
IP 192.168.20.21.1068 > 192.0.0.21.445: S
IP 192.168.20.21.1069 > 192.0.0.22.445: S
IP 192.168.20.21.1070 > 192.0.0.23.445: S
IP 192.168.20.21.1071 > 192.0.0.24.445: S
IP 192.168.20.21.1072 > 192.0.0.25.445: S
IP 192.168.20.21.1073 > 192.0.0.26.445: S
IP 192.168.20.21.1074 > 192.0.0.27.445: S
IP 192.168.20.21.1075 > 192.0.0.28.445: S
IP 192.168.20.21.1076 > 192.0.0.29.445: S
IP 192.168.20.21.1077 > 192.0.0.30.445: S
IP 192.168.20.21.1078 > 192.0.0.31.445: S
```

図 8 動的解析により得られたスキャンパターン

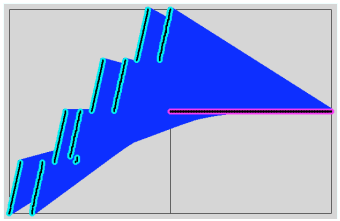


図 9 ミクロ解析によって得た検体 A の可視化例

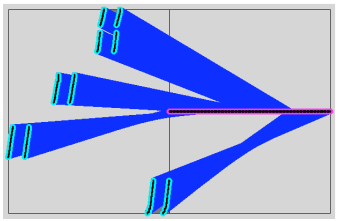


図 10 マクロで解析の振舞タイプ 4-A の可視化例

4.2 マクロ – ミクロによる連携

検体 A はネットワークに対してスキャンを行っていることから，nicter のマクロ解析システムにおいて振舞タイプ 4-A が観測されている可能性が高い．**図 11** に同振舞タイプがダークネットで観測された推移を示す． 図 11 より，振舞タイプ 4-A の観測数は 3 月以降に若干増加が認められる．また，観測数の増減も 3 月以降に激しく起こっていることから，検

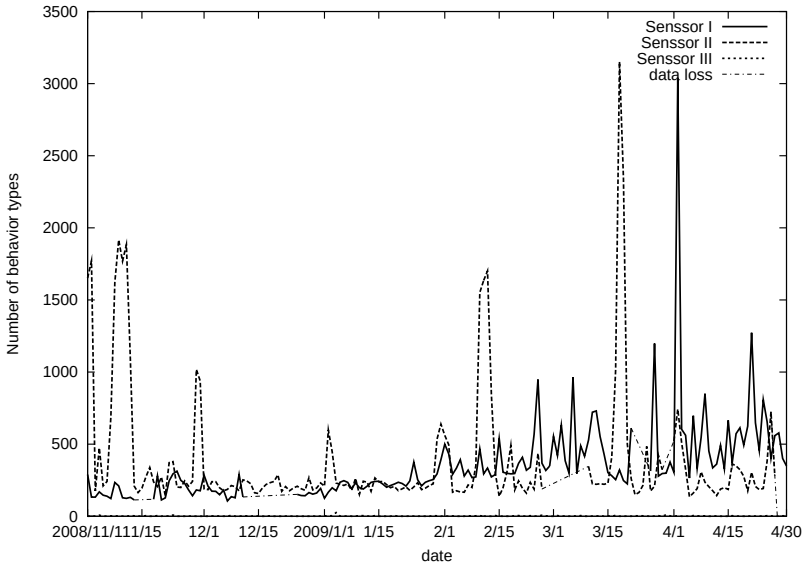


図 11 ダークネットで観測されている振舞タイプ 4-A

体 A が 3 月以降に動作し，ダークネットに影響が出た可能性が高い．Symantec の情報でも，検体 A は 2009 年 3 月 2 日に発見された[9] としているため，観測結果の整合性が確認された．**図 10** にマクロ解析システムで観測した振舞タイプ 4-A の可視化結果を示す．図 9 と図 10 より，ミクロ解析システムにより得られた振舞タイプ 4-A と，マクロ解析システムにより得られた同振舞タイプ 4-A は，ほぼ同一のパターンであることが視覚的にも確認できた．

従って，振舞タイプ 4-A が 3 月に増加している原因として，検体 A が関連していることが予想され，同じ振舞タイプを持っているホストは検体 A に感染している可能性があると言える．このように，ミクロ解析システム，マクロ解析システムの結果を付合わせることで，マクロ解析システムで捉えた現象の原因をミクロ解析システムで得ることが可能になる．

現在，445/TCP に関するトラフィックとして，ほとんどが Conficker によるものであることが図 3 と図 5 より確認できる．一方で，振舞タイプ 4-A の観測数には急激な増加が確認できないことから，Conficker のような大規模感染には至っていないことが考えられる．このように，ミクロ解析システムにより解析を行い，その結果を分析し振舞タイプを特定することで，大規模感染等で見えなくなるような小さな感染活動等も検知することが可能である．

5. おわりに

本報告では，長期観測から得られた統計データを用いた Conficker.D の傾向を報告した．また，ネットワークのスキャンを観測，分析しているマクロ解析に加えて，マルウェアそのものの解析を行うミクロ解析を紹介し，ミクロで観測した事象をマクロで確認した．

今後は，ハイインタラクションハニーポットを用いたマルウェアの収集・解析を行うことで，さらに精度の高い相関分析を行うことが可能になると考えられる．まず，感染拡大に必要不可欠なスキャンの振舞をマクロ解析により捉え，さらに，実際に感染を行うためのエクスプロイトコードをハイインタラクションハニーポットで取得し，感染に至るまでのプロセスをミクロ解析によりプロファイリングを行う．これらの情報を蓄積することで振舞タイプやエクスプロイトコードの種類により現在起こっている事象の原因の絞り込みを行うことが可能になる．

参 考 文 献

1) 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および分析レポート”, 信学技法, Vol. 109, No. 33, pp. 15 – 20, 2009.
2) 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.
3) Daisuke Inoue, Masashi Eto, Katsunari Yoshioka, Syunsuke Baba, Kazuya Suzuki, Junji Nakazato, Kazuhiro Ohtaka, 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.
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) 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.

6) STN Peer-to-Peer Discussion Forums, Symantec,
https://forums.symantec.com/t5/blogs/blogarticlepage
/blog-id/malicious_code/article-id/233 （2009 年 5 月現在）.
7) Microsoft Malware Protection Center,
http://www.microsoft.com/security/portal/Entry.aspx?
Name=Worm:Win32/Conficker.D （2009 年 5 月現在）
8) シマンテック セキュリティレスポンス,
http://www.symantec.com/ja/jp
/security_response/writeup.jsp?docid=2008-122211-3108-99
（2009 年 5 月現在）
9) シマンテック セキュリティレスポンス,
http://www.symantec.com/ja/jp
/security_response/writeup.jsp?docid=2009-030208-3009-99
（2009 年 5 月現在）