情報処理学会論文誌 Vol. 50 No. 9 2147–2162 (Sep. 2009)

能動的攻撃と受動的攻撃に関する調査および考察

青木一史[†1] 川古谷裕平[†1] 秋山満昭[†1]
岩村誠[†1,†2] 針生剛男[†1] 伊藤光恭[†1]

近年，ボットをはじめとするマルウェアが猛威を振るっており，その感染手法はOSレベルでの堅牢性向上を背景に，従来行われてきた能動的攻撃に加え，利用者が行う何らかの操作を契機とする受動的攻撃も広がりをみせている．マルウェア対策を検討するための攻撃実態調査はこれまでも行われてきたが，効果的な対策を策定するにはさらなる調査が必要である．本稿では，標的となりやすい脆弱性，利用されるShellcodeのトレンド把握，攻撃Webサイトが有する性質把握，感染端末に見られる挙動把握を目的とし，能動的攻撃と受動的攻撃に関する情報収集が可能な2つの異なるハニーポットと，閉/開環境型動的解析システムにより調査を行った．調査の結果，能動的攻撃に関しては，攻撃対象脆弱性がMS03-026に偏っていることや，Anti-Virusを停止させたうえでマルウェアをダウンロードさせるShellcodeの存在が明らかとなった．また，受動的攻撃に関して，iframeタグを用いた攻撃の場合，Webサイト群は集約構造となる傾向が強いことを明らかにした．さらに，収集したマルウェアの動的解析からは，IRCボットが接続するC&Cサーバの待ち受けポートが，TCPポート8080番のような，一般的なサービスで利用されているものに変化していることや，C&Cサーバとの通信でHTTPを利用するボットが多数存在することが明らかとなった．本稿では，調査で明らかとなった事実をもとに，ハニーポットや解析技術の今後の課題を示すとともに，能動的攻撃/受動的攻撃からユーザを保護するための対策指針を提唱する．

Investigation and Understanding Active/Passive Attacks

Kazufumi Aoki,[†1] Yuhei Kawakoya,[†1]
Mitsuaki Akiyama,[†1] Makoto Iwamura,[†1,†2]
Takeo Hariu[†1] and Mitsutaka Itoh[†1]

In these days, Bot programs and other malwares are serious threats in the Internet and their infection techniques are not only Active Attacks but also Passive Attacks against OS security technology improvements. Though there are some investigations to adopt countermeasures against attacks, a further investigation is necessary to settle on effective measures. In this paper, we investigate the actual condition of Active Attacks and Passive Attacks by two types of HoneyPots and open/close types of dynamic analysis system. Our investigation shows that there are some biases on target vulnerabilities and new types of Shellcode which stop Anti-Virus software were detected on Active Attack survey. From Passive Attack survey, Attacking Web sites which contain iframe tags have intensive structures. And many IRC based C&C servers are listening on general service port numbers, e.g., TCP Port 8080. In addition, we observed many Bot programs using HTTP protocol for communication with C&C servers. we suggest further issues for HoneyPots and analysis systems and some countermeasures against Active/Passive attacks based on investigation results.

1. はじめに

近年，ボットをはじめとするマルウェアが猛威を振るっており，その感染活動では能動的攻撃に加え，受動的攻撃が用いられるようになった．能動的攻撃および受動的攻撃は次のようなものである．

能動的攻撃 利用者が特に操作を行わなくても，攻撃者が能動的に仕掛けてくる操作により実現される攻撃のこと．標的となった端末に対して，攻撃者が悪意のあるデータを送信し，任意のコードを実行させる攻撃である．具体例として，MS Blastのようなワームの感染活動があげられる．

受動的攻撃 利用者が行う何らかの操作を契機として行われる攻撃のこと．利用者がWebアクセスのような何らかの操作を行うことで，攻撃者から悪意のあるデータを送り込まれ，任意のコードを実行させる攻撃である．具体例として，脆弱性の存在するブラウザで悪意のあるWebページを閲覧させ，マルウェアに感染させる攻撃があげられる．

マルウェア対策を検討するための能動的攻撃の実態調査は，これまでにも実施されているが[1)]，適切かつ効果的な対策を策定するためには，さらなる調査が必要である．たとえば，プログラムの脆弱性を狙う攻撃の場合，狙われる脆弱性や攻撃コードの特徴を把握することで，優先して適用すべきセキュリティパッチの選定や，IDS/IPSでの効果的なシグネチャ

†1 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories, NTT Corporation
†2 早稲田大学
Waseda University

© 2009 Information Processing Society of Japan

を生成することが可能になる．

また，MPack[2] という Web ブラウザ攻撃ツールの出現を背景に，受動的攻撃の中でも，Web 閲覧を感染経路とするものが猛威を振るっている．Web 閲覧を感染経路とする受動的攻撃では，踏み台となる URL を複数経由させることで，実際に攻撃コードを送り込んでくるサイトが見え難くなっている[3]．そのため，URL フィルタリング等の対策を実施しようとした場合，攻撃 Web サイト間の構成を把握することは有益な情報となりうる．

さらに，ボットをはじめとするマルウェアには，感染後，特定のホストへ自動的に接続する等の特徴がある[1]．そのため，マルウェア実行時にみられる通信の特徴を把握することは，すでにマルウェアに感染してしまった一般ユーザを特定し，駆除を促すための手助けとなる．加えて，DDoS 攻撃やスパムメール配信等の感染後の活動への対策を検討するうえでも有用である．

本調査では，現在脅威となっている能動的攻撃および受動的攻撃の実態を明らかにし，さらに，これらの攻撃により拡散するマルウェアの挙動を分析することで，マルウェア対策技術の今後の課題を示すとともに，脅威を低減させるための対策指針を示すことを目的としている．

2. 調 査 項 目

本調査では，能動的攻撃や受動的攻撃から一般ユーザを守る，という観点から，次の項目に着目した．

- 優先して適用すべきセキュリティパッチ選定のための，脆弱性別にみられる攻撃傾向の把握．
- IDS/IPS，FW におけるシグネチャ生成のための，Shellcode[⋆1] にみられる傾向および特徴の把握．
- URL フィルタリング等によるアクセス制御のための，攻撃 Web サイトが有する特徴の把握．
- 感染端末にみられる通信の特徴に基づく感染者特定のための，マルウェアの挙動把握．
- 日々変化する攻撃実態に即した対策を策定するための，攻撃傾向の変化の調査．

そこで，本稿では，ハニーポットと動的解析システムにより，次の項目の調査を実施した．

(1)　ハニーポットによる攻撃情報およびマルウェアの収集
- 能動的攻撃に悪用される脆弱性の傾向分析
- 能動的攻撃における Shellcode の傾向分析
- 能動的攻撃の傾向変化（2006 年度調査との比較）
- 受動的攻撃に悪用される脆弱性の傾向分析
- 攻撃 Web サイトにおけるサイト間構造調査

(2)　収集したマルウェアの挙動解析
- 能動的攻撃で収集されたマルウェアの挙動分析
- 受動的攻撃で収集されたマルウェアの挙動分析

3. 調 査 手 法

ハニーポットによる攻撃情報およびマルウェアの収集と，収集したマルウェアの挙動解析には，我々が開発した下記の技術を用いた．

- 攻撃情報収集/マルウェア収集技術
  - DenDenHoney（能動的攻撃用ハニーポット）
  - Marionette（受動的攻撃用ハニーポット）
- マルウェア解析技術
  - Matrix Daemons（閉環境型動的解析）
  - Botnet Watcher（開環境型動的解析）

本研究の取り組みにおける調査項目と各技術の関係を**図 1** にまとめる．

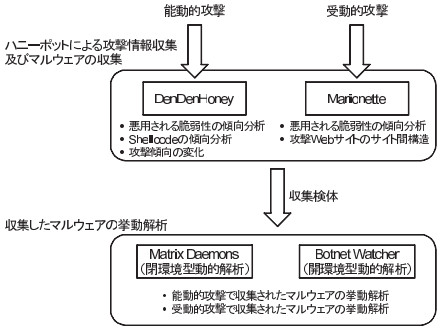

図 1　調査項目と各技術との関係
Fig. 1　Relationships between survey items and techniques.

⋆1 攻撃が行われる際に，攻撃者が意図する何らかの挙動をもたらすために挿入される比較的サイズの小さなコード

© 2009 Information Processing Society of Japan

表 1　DDH が対応している脆弱性一覧
Table 1　List of detectable vulnerabilities on DDH.

脆弱性 ID	概要[5)]
MS03-026	RPC DCOM インターフェイスの脆弱性
MS03-049	Workstation サービスの脆弱性
MS04-007	ASN.1 の脆弱性
MS04-011	LSASS の脆弱性
MS05-039	UPnP の脆弱性
MS06-040	Server サービスの脆弱性

表 2　Marionette が対応している脆弱性一覧
Table 2　List of detectable vulnerabilities on Marionette.

脆弱性 ID	概要[5),8)]
MS06-001	WMF の脆弱性
MS06-014	MDAC の脆弱性
MS06-055	Vector Markup Language の脆弱性
MS06-057	WebViewFolderIcon の脆弱性
MS07-004	Vector Markup Language の脆弱性
MS07-017	GDI の脆弱性
CVE-2006-5198	WinZip の FileView ActiveX コントロールの脆弱性
CVE-2007-0015	Apple QuickTime の rtsp:// URI 処理の脆弱性

3.1　調査に利用した各技術について

3.1.1　DenDenHoney

DenDenHoney（以下，DDH とする）は，脆弱性箇所を監視するモジュール[4)] により，攻撃者（または感染者）が能動的に行う攻撃を検知し，マルウェアに感染することなく検体を収集するハニーポットである．DDH で検知可能な脆弱性を**表 1** に示す．なお，DDH は Windows に対する能動的攻撃を検知するために，Windows XP（SP なし）上で動作させた．

また，攻撃に用いられる Shellcode の傾向を分析するために，検知した Shellcode を次のような命名規則により分類した．

- Shellcode 名は「セッション部」＋「中間部」＋「実行部」のように構成される．
- 各部の名前は Shellcode が呼び出している API 名またはコマンド名をもとにする．ただし，セッション部について，Shellcode が多段構成となる場合[6)] には “Stager” を追記する．
- 「セッション部」は，セッションを確立し，マルウェアをダウンロードする方法を示す．Shellcode に直接コマンドが埋め込まれている場合には，セッション部が存在しないこともある．
- 「中間部」は，マルウェアのダウンロードから実行までの間に行われる挙動を示す．セッション部で API を呼び出さず，中間部でコマンドを実行してマルウェアのダウンロードを行う場合もある．また，実行部で API を呼び出さずに，中間部でマルウェアの実行を行う場合もある．
- 「実行部」は，ダウンロードしたマルウェアの実行方法を示す．ただし，cmd.exe から直接マルウェアが実行された場合，実行部が存在しない場合もある．

3.1.2　Marionette

Marionette[7)] は，Web ブラウザやサードパーティアプリケーションにおける脆弱性箇所を監視するモジュールにより，Web ブラウザを介して行われる受動的攻撃を検知し，マルウェアに感染することなく検体を収集するハニーポットである．MPack が流通している現状をふまえ，Marionette では，MPack が攻撃対象としている脆弱性への攻撃を監視している（**表 2**）．表 2 に記載の脆弱性に対する攻撃を検知するために，Internet Explorer 6.0 を使用し，プラグインとして QuickTime6.5.2 および WinZip10.0 をインストールした．

また，iframe タグを用いた攻撃サイト間の構造を調査するために，Marionette には Web ページに含まれる iframe タグを抽出するモジュールが組み込まれている．

3.1.3　Matrix Daemons

Matrix Daemons（以下，MD）は，実インターネットから隔離された環境に構築された擬似サーバ群からなる仮想インターネット上でマルウェアを実行し，短時間で検体の挙動を解析する技術である．MD による解析では，次のような結果を取得できる．

- マルウェア実行時の通信先
- マルウェア実行時の通信ペイロードおよびプロトコル

通信プロトコルはペイロードを確認することで判別している．ただし，IRC プロトコルは通信に FTP と重複する部分が存在するため，ペイロードから IRC プロトコルだと断定できない場合がある．その場合は，“IRC?” と判定する．なお，MD は実インターネットとは接続していないため，ボットが C&C サーバに接続した後の挙動（追加プログラム取得や DDoS 攻撃等）を観測することはできない．

© 2009 Information Processing Society of Japan

3.1.4 Botnet Watcher

Botnet Watcher[9]（以下，BW）は，攻撃者からの命令に起因するマルウェアの挙動や，シーケンシャルマルウェア[10]による追加プログラムのダウンロード等を把握するために，実インターネットとの接続が一定の制限下で許可された仮想インターネットを用いて，検体の挙動を解析する技術である．BW による解析では，次のような結果を取得できる．

- マルウェア実行時の通信先
- マルウェア実行時の通信ペイロードおよびプロトコル
- C&C サーバとボット間の命令のやりとり
- 追加プログラムの収集および実行監視

MD とは異なり，一部通信が実インターネットに通過するため，ボットネットの挙動（命令に起因したボットの活動）や，シーケンシャルマルウェアが実際にダウンロードするマルウェアの収集と挙動把握が可能である．

3.2 調査データの収集環境

3.2.1 能動的攻撃調査データの収集環境

4 カ所の ISP に 1 台ずつ DDH を設置し，能動的攻撃の調査データを収集した．設置した DDH の環境と調査データ収集環境をそれぞれ**表 3**，**表 4** に示す．ハニーポットの IP アドレスについて，DDH_{2006} では固定アドレスとし，DDH_{2007} では 1 日に 1 回リナンバするようにした．また，DDH_{2007} では表 1 に記載の 6 個の脆弱性への攻撃を検知するモジュールが組み込まれているが，DDH_{2006} では MS05-039 の攻撃検知モジュールが組み込まれていない．

$A_{2007,2006}$ では能動的攻撃を脆弱性別に検知し，マルウェアの収集を行った．また，A_{sc} の期間には，攻撃に用いられた Shellcode の分析を行った．

3.2.2 受動的攻撃調査データの収集環境

Marionette により悪性 URL リスト[⋆1]（全 31,234 URL）を巡回し，受動的攻撃の調査データを収集した．調査データ収集環境を**表 5** に示す．

$P_{1,2}$ では主に攻撃検知とマルウェア収集を目的に巡回し，P_{link} では P_1 で脆弱性に対する攻撃を検知した 3,408 URL を対象に，攻撃サイト間構造を調査した．ただし，P_1 と P_{link} では巡回した日時が異なるため，P_1 で検知した URL が，P_{link} の時点では消滅していることがある．また，攻撃サイト間構造を形成する方法は，iframe タグによるものや META タグを利用するもの，JavaScript の location.href を利用するもの等，種々存在しているが，本調査では，近年その脅威が増大しているといわれる iframe タグ挿入[11]による攻撃サイト間構造に着目した．

表 3　DDH の環境
Table 3　Environments of DDH.

	DDH_{2007}	DDH_{2006}
IP アドレス	1 日に 1 回リナンバ	固定
対応脆弱性数	6 個	5 個
設置 ISP 数	4 ISP	4 ISP
ISP ごとの設置台数	1 台	1 台

表 4　能動的攻撃検知データ収集環境
Table 4　Environments of active attack survey.

	データ収集期間	DDH の環境
A_{2007}	2007.7.2〜2008.2.20	DDH_{2007}
A_{2006}	2006.6.9〜2007.2.25	DDH_{2006}
A_{sc}	2008.1.21〜2008.2.20	DDH_{2007}

表 5　受動的攻撃検知データ収集環境
Table 5　Environments of passive attack survey.

	データ収集期間	調査対象 URL 数
P_1	2008.1.22〜1.27	URL リスト内の 31,234 URL
P_2	2008.2.15〜2.16	URL リスト内の 31,234 URL
P_{link}	2008.2.13〜2.18	P_1 で検知した 3,408 URL

3.2.3 検体挙動解析データの収集環境

能動的攻撃および受動的攻撃により得られた検体について，MD および BW により動的解析を行った．MD および BW による解析データ収集環境を，それぞれ**表 6**，**表 7** に示す．

MD での解析では，$A_{2007,2006}$ および P_1 で収集した検体のうち，SHA1 のハッシュ値がユニークなものを解析対象とした．また，検体種別の傾向を見るために，$MD_{a2007,p}$ の検体を ClamAV[12),⋆2]でスキャンした．

BW の解析では，実インターネットにおけるボットの挙動を長期間観測する．そのため，

⋆1 NTT コミュニケーションズ株式会社の協力の下，マイクロソフト株式会社より提供された URL リスト

⋆2 Engine: ver-0.94.1, Virus Databases: main.cvd ver-49, daily.cvd ver-8596（2008.11.10）

© 2009 Information Processing Society of Japan

表 6　MD による検体解析データ収集環境
Table 6　Environments of malware dynamic analysis by MD.

	検体収集環境	解析検体種類数	解析時間
MD_{a2007}	A_{2007}	16,467 種類	30 秒
MD_{a2006}	A_{2006}	967 種類	30 秒
MD_p	P_1	136 種類	30 秒

表 7　BW による検体解析データ収集環境
Table 7　Environments of malware dynamic analysis by BW.

	検体収集環境	BW 解析期間	解析検体数
BW_a	A_{2007}	2008.2.8〜2.12	50 種類
BW_p	P_1	2008.2.12〜2.18	42 種類

DDH や Marionette で収集したすべての検体を BW で解析することは困難である．そこで，BW による解析では，MD による解析結果に基づき，次のような条件で解析対象を選別した．

- BW 解析期間の 5 カ月前までに収集した検体であること
- MD の解析結果で，IRC または HTTP による通信が確認されていること
- BW 解析対象検体で MD で抽出された接続先を網羅できること

4. ハニーポットによる攻撃調査結果

4.1 能動的攻撃調査結果

4.1.1 脆弱性別攻撃検知状況

A_{2007} の攻撃検知数および収集検体数を**表 8** に示す．また，脆弱性別の攻撃検知数・検体収集率を**表 9** に示す．

1 台あたりの平均攻撃検知数は 320.0 回/日であった（表 8）．この攻撃頻度は，2005 年の調査で報告されたもの[13] とほぼ同一である．

また，表 9 に示すように，攻撃に悪用された脆弱性の約 80%は MS Blast というワームが悪用した MS03-026 であった．脆弱性別に検体収集数をみると，90%以上の検体が MS03-026 で収集されたことが分かる．一方，MS03-049，MS04-007，MS04-011，MS05-039 で収集された検体数は，いずれも全収集検体数の 1%未満であった．検体収集率は，MS03-049，MS04-007，MS04-011，MS05-039 では 3%未満であった．

また，A_{2007} では複数脆弱性を 1 度に攻撃する連続攻撃が観測された．連続攻撃は 3 連続，4 連続，5 連続のケースが確認されており，それぞれ攻撃に使われる脆弱性と，攻撃順序は**表 10** のようになっていた．

表 8　DDH における攻撃検知数と収集検体数（A_{2007}）
Table 8　The number of attacks and malwares detected by DDH (A_{2007}).

	攻撃検知		検体収集	
	検知数	一日平均	検体数	一日平均
ISP-A	86,241	368.6	46,552	198.9
ISP-B	109,331	467.2	59,973	256.3
ISP-C	82,542	352.7	42,860	183.2
ISP-D	21,757	93.0	10,808	46.2
4 ISP 合計	299,871	1,281.5	160,193	684.6
1 台平均	74,968	320.0	40,048	171

表 9　攻撃された脆弱性と収集検体数（A_{2007}）
Table 9　The number of attacks and malwares detected by DDH with respected to each vulnerability (A_{2007}).

脆弱性 ID	攻撃検知数	取得検体数	検体収集率※1
MS03-026	235,122	154,074	65.5%
MS03-049	28	0	0.0%
MS04-007	16,040	68	0.4%
MS04-011	29,564	82	0.2%
MS05-039	7,382	170	2.3%
MS06-040	11,735	5,799	49.4%

※1（検体収集率）=（取得検体数）/（攻撃検知数）

表 10　連続攻撃で狙われる脆弱性とその順序
Table 10　Vulnerabilities and sequence used for sequential attack.

3 連続	MS03-026	⇒	MS04-011	⇒	MS04-007			
4 連続	MS05-039	⇒	MS03-026	⇒	MS04-011	⇒	MS04-007	
5 連続	MS06-040	⇒	MS05-039	⇒	MS03-026	⇒	MS04-011	⇒ MS04-007

4.1.2 Shellcode の傾向分析

A_{sc} での攻撃データについて，用いられた Shellcode の傾向を分析した．検知した Shellcode を分類すると**表 11** のようになった．

分類された Shellcode について，脆弱性別の検知割合を**図 2** に示す．なお，A_{sc} では MS03-049 への攻撃が検知されなかったため，図から当該脆弱性の項目は省いている．検知した Shellcode を脆弱性別に比較すると，次のような傾向があった．

© 2009 Information Processing Society of Japan

表 11　Shellcode の分類
Table 11　Classification of shellcodes.

ID	セッション部	中間部	実行部
SC-1	connect Stager	-	CP
SC-2	accept Stager	-	CP
SC-3	accept	cmd tftp	-
SC-4	accept	cmd ftp	-
SC-5	accept	-	WinExec
SC-6	accept	cmd net cscript	-
SC-7	accept	cmd net ftp	-
SC-8	accept	cmd cscript	-
SC-9	connect	cmd tftp	-
SC-10	-	tftp	CP
SC-11	URLDownload	-	WinExec
SC-12	-	cmd Ftp	-

CP: CreateProcess

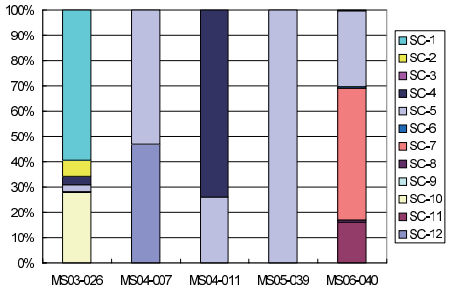

図 2　脆弱性ごとの Shellcode 検知割合
Fig. 2　The number of shellcodes with respected to vulnerabilities.

(1)　脆弱性ごとに使用される Shellcode に偏りが存在
(2)　MS06-040 で使用される Shellcode には，他の脆弱性では見られないもの（SC-6，7，8，11）が頻繁に出現

また，特徴的な Shellcode として，Anti-Virus ソフトを停止させた後にマルウェアをダウンロードさせる Shellcode を確認した（**図 3**）．図 3 のような Shellcode は，A_{sc} の間に 6 度観測した．

さらに，4.1.1 項で述べた連続攻撃では，異なる脆弱性を攻撃するものの，利用する Shellcode は同一であり，TCP ポート 9988 番で接続を待ち受けるタイプのものであった（表 11 中 SC-5 型に分類）．

```
20080217 17:02:13  CreateProcessW  ・C:¥WINDOWS¥system32¥net.exe
                                   ・net stop "Norton AntiVirus Auto Protect Service"
20080217 17:02:13  CreateProcessW  ・C:¥WINDOWS¥system32¥net.exe
                                   ・net stop Mcshield
20080217 17:02:13  CreateProcessW  ・C:¥WINDOWS¥system32¥net.exe
                                   ・net stop "Panda Antivirus"
20080217 17:02:13  CreateFileW     ・c:¥1.vbs
...                ...             ...
20080217 17:02:13  CreateProcessW  ・C:¥WINDOWS¥system32¥cscript.exe
                                   ・cscript /Nologo /B c:¥1.vbs
```

図 3　Anti-Virus ソフトを停止させる Shellcode での API シーケンス例
Fig. 3　Shellcode example which stop Anti-Virus software programs.

表 12　A_{2007} と A_{2006} の比較
Table 12　Compare with A_{2007} and A_{2006} attack detection results.

	A_{2007}	A_{2006}
総攻撃検知数	299,871 回	51,792 回
総取得検体数	160,193 検体	51,792 検体
総取得検体種類数	16,476 種類	967 種類

4.1.3　能動的攻撃の傾向変化

$A_{2007,2006}$ における攻撃検知結果の概要を**表 12** に示す．なお，検体種類は SHA1 のハッシュ値をもとに区別した．A_{2006} と A_{2007} では DDH の環境が異なるため，単純な比較はできないが，A_{2006} と比較し，A_{2007} では総攻撃検知数，収集検体数，検体種類数が増加していた．

4.2　受動的攻撃調査結果

4.2.1　攻撃 Web サイト検知結果

$P_{1,2}$ の攻撃検知結果を**表 13** に示す．なお，検体種類は SHA1 のハッシュ値をもとに区別した．P_1 と比較し，P_2 では攻撃検知率が 0.3%低下した．さらに，収集した検体数および種類数も低下した．

また，収集検体数と種類数について，$P_{1,2}$ のいずれも，検体数に対する種類数の割合が 2%以下であった．収集した検体の SHA1 ハッシュ値を確認したところ，$P_{1,2}$ ともに 34365285AC89E9654D5457A15DA240649166AF3F というハッシュ値を持つマルウェアが 6,000 個以上存在した．

また，今回攻撃を検知した URL では，80%以上で MS06-014 の脆弱性に対する攻撃が行われていた（**表 14**）．

© 2009 Information Processing Society of Japan

表 13　悪性 URL リスト巡回結果
Table 13　Results of crawling malicious URL list by Marionette.

	攻撃検知		検体収集	
	検知数	検知割合	検体数	種類数
P_1	3,408	10.9%	9,533	136
P_2	3,324	10.6%	8,408	119

表 14　Marionette における脆弱性別攻撃検知数
Table 14　The number of attacks with respected to each vulnerabilities on Marionette.

脆弱性 ID	P_1	P_2
MS06-014	3,351	3,281
MS07-017	396	487
MS06-001	94	120
MS06-057	46	25
MS06-055	39	42
MS07-004	4	3
CVE-2006-5198	0	7
CVE-2007-0015	0	0

表 15　P_{link} における iframe タグの利用状況
Table 15　Use of iframe tag in P_{link}.

			URL 数
調査対象 URL			3,408
	アクセス可		2,642
		iframe あり	2,466
		iframe なし	176
	アクセス不可		766

4.2.2　攻撃 Web サイト間の接続構造分析

P_1 で攻撃を検知した 3,408 URL のうち，P_{link} でアクセスできた URL 数および iframe タグを利用していた URL 数を**表 15** に示す．P_{link} においてアクセスできた URL の 90%以上で iframe タグが利用されていた．

また，P_{link} において iframe タグを利用していた 2,466 URL について，iframe タグにより構築される攻撃サイト間構造を**図 4** に示す．図 4 では，ノードが URL（URL パラメータ部分は削除），エッジがリダイレクトの方向を表している．検知 URL は複数のクラスタを形成しており，約 88%の URL が，特定の URL に集約されるという構造が確認された．また，最大のクラスタでは，1,899 URL が最終的に同一の URL に集約されていた．

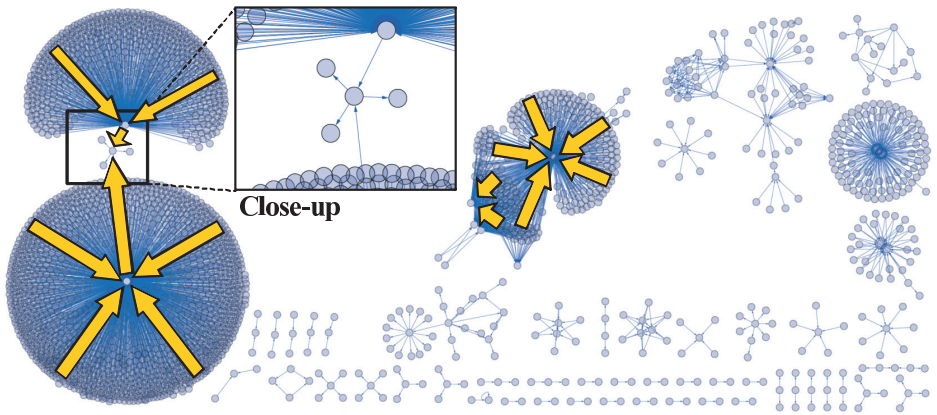

図 4　iframe タグにより構築されるサイト間リンク構造
Fig. 4　Structure of attacking web sites linked by iframe tags.

5.　収集したマルウェアの挙動解析結果

MD_{a2007} および MD_p の解析対象検体について，ClamAV によりスキャンした結果を**図 5** に示す．MD_{a2007} と MD_p の検体では，判定された結果には次のような特徴が確認された．

MD_{a2007} の検体　ワーム（Worm.Allaple）やボット（W32.Bobax，Trojan.SdBot，Trojan.IRCBot，Trojan.Vanbot，Trojan.Poebot，Trojan.Mybot）と判定されたものが複数存在．

MD_p の検体　シーケンシャルマルウェア（Trojan. Downloader，Trojan. Dropper，Trojan. Downloader.Small）と判定されたものが複数存在．

5.1　閉環境動的解析結果の分析

MD_{a2007} および MD_p での閉環境動的解析結果をそれぞれ**表 16**，**表 17** に示す．また，MD_{a2007} について，マルウェアが利用する TCP プロトコルの分布を**図 6** に示す．なお，MD でプロトコル判別ができなかった通信については，“PORT_[ポート番号]” と標記している．

MD_{a2007} では，ボット-C&C サーバ間のやりとりに用いられる IRC での通信[1)] が確認された．IRC での接続先ポート番号，すなわち，C&C サーバの待ち受けポート番号の分布

© 2009 Information Processing Society of Japan

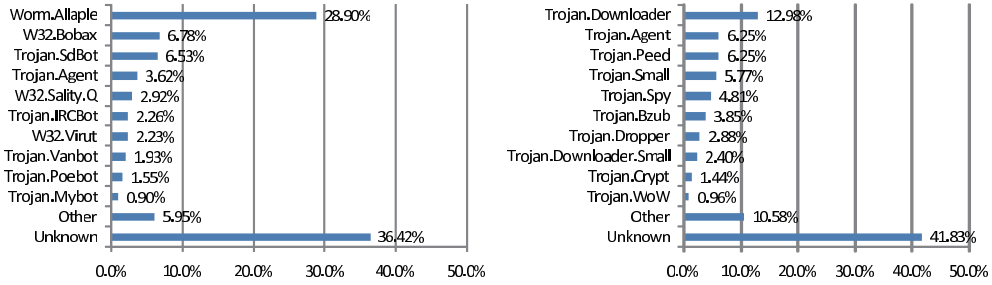

図 5　MD 解析検体の ClamAV スキャン結果（左：MD_{a2007}，右：MD_p）
Fig. 5　ClamAV scan results (left: MD_{a2007} malwares, right: MD_p malwares).

表 16　MD による解析結果（MD_{a2007}）
Table 16　Dynamic analysis result by MD (DDH malwares).

			検体数
実行可			7,030
	通信あり		6,163
		TCP	6,120
		UDP	2,629
	通信なし		867
実行不可			7,030

表 17　MD による解析結果（Marionette の検体）
Table 17　Dynamic analysis result by MD (Marionette malwares).

				検体数
実行可				124
	通信あり			73
		TCP		68
			HTTP	65
			PORT_80	1
			PORT_2703	2
			PORT_3461	1
		UDP		64
			DNS	64
			PORT_123	1
	通信なし			51
実行不可				12

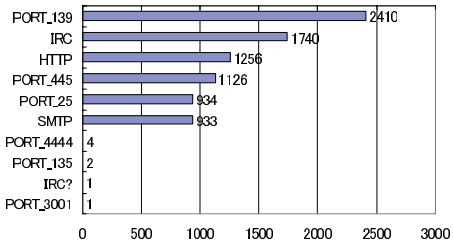

図 6　TCP プロトコルの分布（横軸は検体数）
Fig. 6　Distribution of TCP protocols (x-axis: malware counts).

を調査し，上位 10 ポートを集計すると，**図 7** のようになる．上位には，TCP ポート 8080 番（HTTP Alternate）や TCP ポート 5190 番（AOL Instant Messenger），TCP ポート 1863 番（MSN Messenger）といった一般的なサービスで利用されるポート番号が確認された．また，IRC で一般的に用いられるポート番号は TCP ポート 6667 番であるが，今回得られた解析結果では，TCP ポート 6667 番を利用する検体は全体の 7.7%程度であった．

ボットが HTTP で通信する用途として，C&C サーバとの指令のやりとりや，追加プログラムダウンロードがある．解析した検体の中に，HTTP を利用するボットがどの程度存在したかを確認するために，MD_{a2007} について，HTTP 利用検体の GET リクエスト URI を調査した．その結果，HTTP ボットが C&C サーバとの通信で利用するものと同形式[14]のものが 931 検体存在した．なお，UDP の通信については DNS アクセス以外は確認されなかった．

$MD_{a2007,a2006}$ の解析結果を比較したものを**表 18** に示す．MD_{a2006} と比較し，MD_{a2007}

© 2009 Information Processing Society of Japan

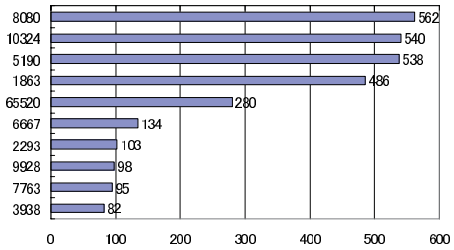

図 7　C&C サーバ（IRC）で利用されるポート番号トップ 10（横軸は検体数）
Fig. 7　Top 10 port number of IRC C&C servers (x-axis: malware count).

表 18　$MD_{a2007,a2006}$ の解析結果比較
Table 18　Compare with MD_{a2007} and MD_{a2006} result.

	MD_{a2007}	MD_{a2006}
IRC 利用検体種類数	1,740 種類	528 種類
HTTP 利用検体種類数	1,226 種類	127 種類
HTTP 利用比率※1	70.5%	24.1%

※1 HTTP 利用比率 = HTTP 利用検体種類数 ÷ IRC 利用検体種類数

は IRC 利用検体数に対する HTTP 利用検体数の割合が増加していた．

また，MD_p と，MD_{a2007} とでは利用する TCP プロトコルの種類に差がある．MD_p の結果には，IRC による通信を行う検体は存在せず，多くは HTTP による通信を行うものであった．

5.2　開環境動的解析結果の分析

5.2.1　実インターネットにおけるボットの挙動

図 8 は，BW_a のあるボット（SHA1=1BA0BD136A87A6F06B09044C37A444215F33D530）を解析した際にみられた挙動である．この検体は，まず特定の C&C サーバ（IRC サーバ ①）に接続を試みた．接続が成功すると，C&C サーバを介して追加プログラム取得命令を受け取り（図 8 ①），HTTP サーバ ① から追加プログラムをダウンロードした（図 8 ②）．この追加プログラムを実行することにより，当初は接続していなかったホスト（IRC サーバ ②）への IRC 接続を行うようになった（図 8 ③）．追加プログラムをダウンロードし実行する行為は，この例では合計 3 回確認されており，マルウェア実行から 3 回のダウンロードを終えるまでは約 2 分であった．

表 19 は $BW_{a,p}$ で確認された追加プログラムの種類数を示している．$BW_{a,p}$ ともに，複

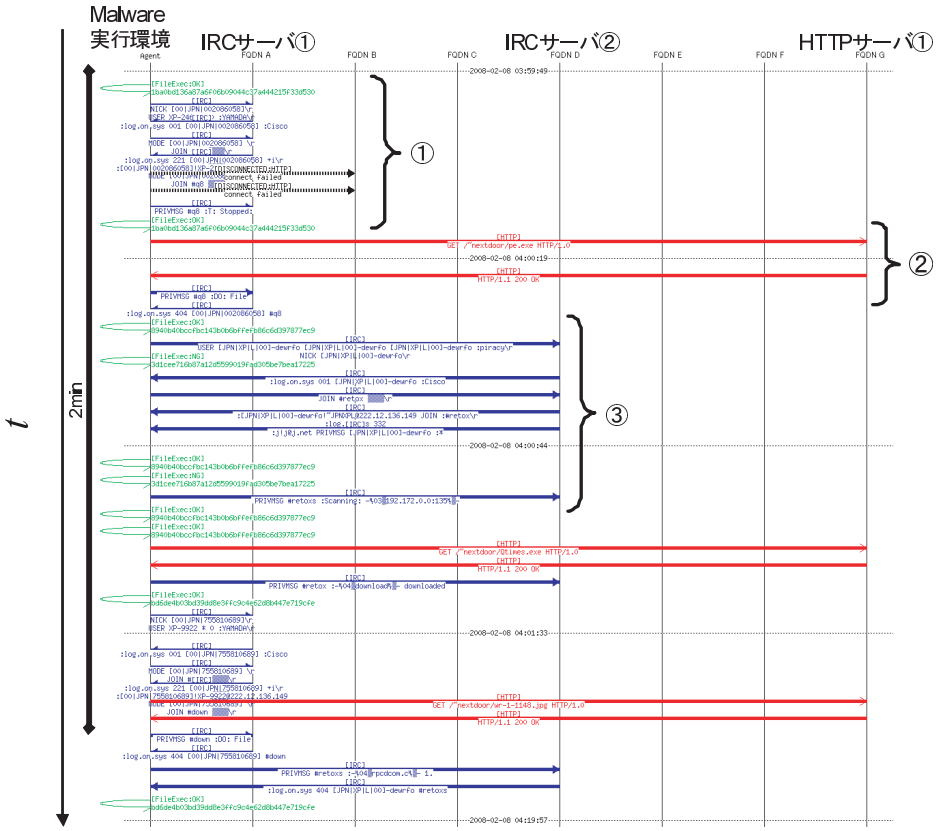

図 8　実インターネットにおけるボットの活動例（緑：ファイル実行，青：IRC 通信，赤：HTTP，黒：接続エラー）
Fig. 8　Sequential Activity of some malware on Internet.

数のプログラムを外部からダウンロードし実行しているが，BW_p の方が多くのプログラムを実行しているという結果が得られた．

また，BW_a での解析中，IRC によるボット-C&C サーバ間通信で**図 9** に示すような暗号化されたコマンド列が観測された．これは従来観測されていた比較的コマンドの意味を類推しやすいもの[1] とは異なっている．

© 2009 Information Processing Society of Japan

表 19　$BW_{a,b}$ で得られた追加実行プログラム数
Table 19　Additional executed programs observed under BW analysis.

	EXE	DLL
BW_a	10 種類	3 種類
BW_p	38 種類	12 種類

例1　=35PIIY8WfC4qo7yWM4B8RFzmJV42WSsUSpfVm72IG
SymNxLuGTaTJiZ5JvLIUXBGMQh

例2　=t6i5XGF1Bi9a/BbZN3xp2j9cfR/Ecc6xwbIc9XAMU7Vfs
AKIIYtdGu9xnaFk36trNQa6++1/jlzI2uTG4FNcTK4v1HU1
oysNaH81mCk1uFZ8wEyPeR3KXNfxvuvUAltMwQh

図 9　BW で観測されたボットへの暗号化された命令の例
Fig. 9　Examples of crypted instruction on IRC Botnet.

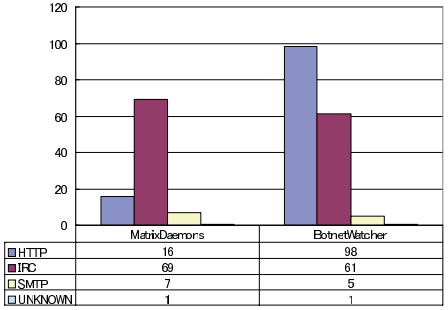

図 10　BW_a 解析検体の MD および BW での TCP プロトコル別接続先数の比較
Fig. 10　TCP destination hosts distribution compared BW result with MD (BW_a malwares).

5.2.2　開環境/閉環境での取得接続先数の変化

動的解析環境の違いがもたらす影響を調べるために，BW で解析した検体について，MD で解析したときにみられるプロトコル別接続先数（TCP）を調査した．MD_{a2007} と BW_a との比較結果を**図 10** に示す．また，MD_p と BW_p との比較結果を**図 11** に示す．なお，図 11 では，ランダムに生成された FQDN のホストに対する外部接続確認を結果から除外した．

いずれの比較についても，BW で解析した結果の方が HTTP での接続先を多数取得した．また，MD_{a2007} と BW_a との比較においては MD_{a2007} での解析結果の方が IRC での接続先を多数取得した．

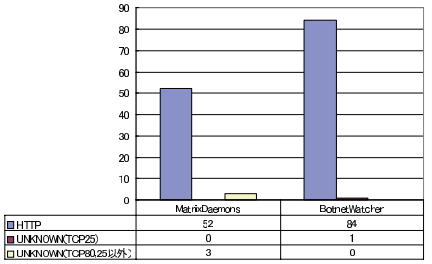

図 11　BW_p 解析検体の MD および BW での TCP プロトコル別接続先数の比較
Fig. 11　TCP destination hosts distribution compared BW result with MD (BW_p malwares).

6.　ハニーポットによる攻撃検知に関する考察

6.1　能動的攻撃検知結果について

6.1.1　脆弱性別攻撃検知状況

A_{2007} では，表 9 に示す結果のとおり，MS03-026 に対する攻撃が最も多く，全体の 80%程度であった．また，MS03-026 に対する攻撃で収集した検体が，全収集検体の 90%以上となっている．MS03-026 については，OS のバージョン（XP，2000 等）や言語（日本語版，英語版等）に依存しない，完成度の高い攻撃コードが流通しており，攻撃者が利用しやすい脆弱性となってしまい，広く悪用されているものと推定される．

また，検体収集率については，MS03-049，MS04-007，MS04-011，MS05-039 の 4 つの脆弱性に対する攻撃では 5%未満と，MS03-026 や MS06-040 に比べると非常に小さい．この原因として次のことが考えられる．

(1)　連続攻撃による検体ダウンロード成功率の低下
(2)　検体ダウンロード成功率が低い Shellcode の利用

(1) について，4.1.2 項で述べたように，連続攻撃では異なる脆弱性を攻撃するものの，利用する Shellcode は同一のもので，いずれも TCP ポート 9988 番で接続を待ち受けるタイプのものであった．そのため，連続攻撃で最初に攻撃が成功した脆弱性で TCP ポート 9988 番での待ち受けを開始すると，続く脆弱性への攻撃では待ち受けるポート番号の重複が発生するため接続を待機することができず，検体収集に失敗する．つまり，連続攻撃で最初に狙われる脆弱性ほど検体収集率が上昇し，2 番目以降になるほど収集率が低下するものと思われる．

© 2009 Information Processing Society of Japan

また (2) について，図 2 によると，MS04-007 と MS04-011 で利用されている Shellcode は，連続攻撃で利用されている SC-5 型を除くと FTP コマンドを利用したタイプが大部分であることが分かる．FTP コマンドを利用してマルウェアをダウンロードさせる Shellcode では，2 本のセッションを確実に張る必要がある．そのため，どちらか 1 本でもセッションが確立できなければマルウェアのダウンロードが失敗してしまうので，当該 Shellcode を用いる場合には収集率が低下すると考えられる．

6.1.2　Shellcode の分析結果

A_{sc} で観測された Shellcode では，Anti-Virus ソフトを停止させた後にマルウェアを配布するものが存在した（図 3）．図 3 のような Shellcode は，A_{sc} の間に 6 度しか観測していないため，現時点では Shellcode として主流のものとはいい難い．しかしながら，このような Shellcode を用いられると，Anti-Virus ソフトをインストールしているユーザでも，適切にセキュリティパッチをあてていないと感染してしまう可能性が高くなる．つまり，Anti-Virus ソフトをインストールしておくだけでは攻撃から端末を保護することが困難であることを意味しており，Anti-Virus ソフトをインストールすることに加え，セキュリティパッチを適用することが重要であるといえる．

6.1.3　能動的攻撃の傾向変化

攻撃検知状況について，表 12 から，2006 年度と比較し，2007 年度には次のような傾向が見られる．

- 総攻撃検知数，総取得検体数が増加
- 総検体種類数が増加

攻撃検知数・取得検体数の増加については，ハニーポットを設置している環境が DDH_{2007} と DDH_{2006} とで，次のように変化していることが原因と考えられる．

(1)　攻撃検知可能な脆弱性が 1 つ増加（MS05-039）
(2)　設置 IP アドレスを固定から 1 日 1 回リナンバするように変更

(1) に関して，DDH_{2007} では MS05-039 への攻撃を検知するモジュールを追加したため，前年度よりも多くの攻撃を検知できるようになった．これにより，2006 年度よりも攻撃検知数が増加したと考えられる．

(2) について，DDH_{2006} ではハニーポットの IP アドレスを固定アドレスにしていたのに対し，DDH_{2007} では，1 日に 1 回リナンバするように変更した．2006 年と 2007 年とで，DDH の環境として異なるのは，対応している脆弱性の数と，IP アドレスの設定方法の 2 点である．DDH_{2007} で追加された MS05-039 での攻撃検知数をみると，全体の 2%程度であった．そのため，攻撃検知数増加の主たる要因は，IP アドレスのリナンバである可能性が高い．ただし，今回の調査では IP アドレスが固定されている場合と，リナンバするようにした場合とで，観測期間が異なっている．したがって，リナンバの影響を調べるためには，固定アドレスの環境と，IP アドレスをリナンバする環境とで，同時期に観測を行う必要がある．

また，検体種類数増加について，A_{2006} と比較し，A_{2007} では取得した検体の種類数が約 17.5 倍となっていた．この原因の 1 つとして，Allaple ワーム[15] のようなポリモーフィック型ワームの存在が考えられる．現在の Allaple ワームは，自身の機能・挙動に影響が出ない箇所を一部改変し，感染活動を行う機能を有している．そのため，ハッシュ値に基づく分類を行うと，機能・挙動がまったく同一の検体であっても，同一の検体としてカウントすることができず，種類数が膨大な数となってしまう．したがって，Anti-Virus シグネチャの作成や，マルウェアの詳細な脅威分析を行おうとした場合に，その優先度を見極めるためにもハッシュ値だけに頼らないマルウェア分類方法を確立する必要があると考えられる．

6.1.4　調査環境が及ぼす影響

今回の調査では，4 カ所の ISP に 1 台ずつ DDH を設置し，能動的攻撃の調査を行った．その結果，DDH を設置した ISP によって攻撃検知数に差がみられた（表 8）．これは，ボットが感染活動を行う際に，感染端末の近接アドレスを攻撃対象とする傾向があるためだと考えられる．したがって，ハニーポットを設置したアドレス付近の感染端末台数の違いから，検知数に差がみられたものと思われる．また，Allaple ワームのように，特定のアドレスリストから攻撃対象を選定するマルウェアが存在するため，ハニーポットを設置したアドレスが原因で，検知数にばらつきが生じうると考えられる．

6.2　受動的攻撃検知結果について

6.2.1　攻撃 Web サイト検知状況

$P_{1,2}$ で検知した攻撃 Web サイトでは，表 14 のように，MS06-014 の脆弱性に対する攻撃が，他の脆弱性に対するものと比較して非常に多い．この理由として，Web ブラウザ攻撃ツールである MPack や IcePack の流通があげられる．これらのツールには，様々な脆弱性に対して連続して攻撃を試行するルーチンが組み込まれており，最初に MS06-014 に対する攻撃が行われ，成功しなかった場合には異なる脆弱性への攻撃を開始する．また，MS06-014 に対する攻撃が成功した場合には，他の脆弱性に対する攻撃は行わない．そのため，最初に狙われる MS06-014 への攻撃が頻繁に確認されたものと考えられる．

また，$P_{1,2}$ ともに Apple Quick Time の脆弱性に対する攻撃をいっさい検知していない．

© 2009 Information Processing Society of Japan

Quick Time の脆弱性に対する攻撃を成立させるには，ダイアログボックス等によるユーザインタラクションが必要だが，本調査に用いた Marionette ではその処理を行っていない．そのため Quick Time のアプリケーションが起動するに至らず，攻撃を検知しなかったものと思われる．このように，脆弱性によっては，一般ユーザが Web サイトを閲覧した後，何らかの操作を行うことで攻撃が行われる場合がある．そのため，Web 閲覧を契機とする受動的攻撃を検知するハニーポットを設計する場合には，脆弱性ごとに適切なユーザインタラクション処理を行うようにする必要があるといえる．

また，表 13 では，同一の悪性リストを巡回したにもかかわらず，攻撃検知数，収集検体数，収集検体種類数のすべてにおいて数値が低下した．この理由として，次の 2 つが考えられる．

(1)　何らかの理由によりページもしくはサイトが消滅

(2)　攻撃側でアクセスしてきたユーザの IP アドレスを記憶

(1) について，ISP やサイト運用者が，攻撃者に Web ページやサイトを悪用されていることに気付き，対策を実施したことで，無害なサイトとなったことが考えられる．また，攻撃者自身が立ち上げている Web ページだった場合には，ハニーポット等に検知されるのを回避するために，一時的にサイトを閉じた可能性もある．

(2) は，アクセスしてきた IP アドレスに対して攻撃が成功すると，その IP アドレスを記憶しておき，次からは攻撃を仕掛けないようにする，という仕組みである．たとえば，MPack にはこの機能が存在している．2 回目の巡回時に攻撃を検知できなくなったいくつかの URL に対して，IP アドレスを変更して再度アクセスしたところ攻撃を検知した．したがって，攻撃サイトにおける IP アドレス記憶機能の存在が，攻撃検知数の低下を招いた 1 つの原因であると考えられる．

6.2.2　攻撃 Web サイト間の接続構造

図 4 にみられるように，今回の攻撃 Web サイト間の接続構造調査では，iframe を利用した Web サイトに集約構造が存在した．攻撃 Web サイトが集約構造を形成していると，最初にアクセスする URL が異なっていても，最終的には同一の URL へアクセスし攻撃を受ける．つまり，URL フィルタリングで一般ユーザを保護する場合には，集約点 URL に対してフィルタリングを適用することで，効率的に対策を行うことが可能になると考えられる．加えて，SQL インジェクション等により，踏み台となるサイトが拡大された場合にも，集約点 URL に対してフィルタリングを行うことで，攻撃の脅威から一般ユーザを保護することが可能になると考えられる．

また，表 13 において，収集した検体数に対し，その種類数が著しく少なくなっているが，これは攻撃 Web サイトが集約構造を形成しているためであり，最終的にたどり着く攻撃サイトが同一のものとなっていることが原因である．

6.2.3　調査環境が及ぼす影響

本稿における受動的攻撃の調査では，MPack 等の攻撃ツール流通を背景に，Web ブラウザおよび関連プラグインの脆弱性に対する攻撃に着目した．そのため，攻撃を検知可能な脆弱性は，MPack で攻撃対象とするものに限られている．しかしながら，Adobe Acrobat の脆弱性を悪用するケースが報告されている等[16]，MPack が攻撃対象としている脆弱性以外に対しても受動的攻撃が行われている．受動的攻撃の全容を把握しようとした場合には，MPack 以外の脆弱性についても調査する必要がある．

また，調査対象の URL について，今回の調査には特定の悪性 URL リストのみを利用している．しかしながら，攻撃 Web サイトへの誘導方法には，掲示板やブログ，スパムメールを悪用する方法等が考えられる．そのため，調査対象 URL の収集方法についても今後検討が必要である．

攻撃 Web サイト間の構造調査では，iframe タグを利用したサイト間構造に着目した．しかし，攻撃 Web サイト間を自動的にリダイレクトする方法は，iframe タグ以外にも JavaScript や META タグを用いる方法等が考えられる．そのため，サイト間構造の全容を明らかにするには，iframe 以外のリダイレクト手法を用いる場合についても調査しなければならない．

7.　マルウェアの挙動解析に関する考察

7.1　閉環境における動的解析

MD による閉環境動的解析の結果，A_{2007} で収集した検体には，IRC のデフォルトポート（TCP ポート 6667 番）以外で IRC 通信を行う検体が多数存在していた（図 7）．上位を占めたポート番号には，一般的なサービスで利用されるものがあり，これはポート番号による単純なフィルタリングが困難であることを意味している．つまり，ボット-C&C サーバ間の通信を精度良く検知/遮断するには，ポート番号以外に，ペイロードの確認を行わなければならない．

また，表 18 に示すように，MD_{a2006} と比較し，MD_{a2007} では IRC 利用検体に対する HTTP 利用検体の割合が増加している．マルウェアの HTTP 利用用途としては，ボット-C&C サーバ間通信や追加プログラムのダウンロード等が考えられる．MD_{a2007} における HTTP 利用検体の GET リクエスト URI を調査した結果で，HTTP ボットが利用するもの

© 2009 Information Processing Society of Japan

と同形式の GET リクエストを送信する検体が 931 種類存在していたことから，MD_{a2007} で HTTP を利用するとの結果が得られたマルウェアのほとんどが HTTP ボットであると考えられる．つまり，攻撃者がボットを制御するプロトコルとして，従来の IRC に加えて HTTP を広く用いるようになったといえる．さらに，MD_p ではほとんどの検体が HTTP を利用しており，IRC の通信は確認されなかった．

HTTP は，多くの一般ユーザが用いるプロトコルであり，ポート番号に基づくフィルタリングを実施しているユーザでも，TCP ポート 80 番に対する通信は許可している可能性が高い．また，Web 閲覧を感染経路とする受動的攻撃の場合，攻撃が成功することは HTTP による通信経路が確保されていることを意味している．このように，HTTP は攻撃者からみると接続性・隠匿化という観点で使いやすいプロトコルとなるため，C&C サーバとの通信や，Web 閲覧を感染経路とするマルウェアで利用されていると考えられる．

7.2　開環境における動的解析

BW による観測では，暗号化された命令文字列を確認した．暗号化された文字列は，つねに一定の文字列ではなく，攻撃者の指令によって毎回変化する．このことから，単純なシグネチャベースの IDS/IPS でボットの命令を検知・遮断するといった対策は困難であると考えられる．そのため，今後はボットの挙動に基づく柔軟なフィルタリングを行う技術について検討を進める必要がある．

また，追加プログラム数（表 19）について，BW_a と比較し，BW_p の方が多数取得していた．これは，Marionette で収集した検体には，シーケンシャルマルウェアが複数存在したことが影響していると考えられる．図 5 によると，MD_{a2007} の検体ではボットやワームと判定されるものが多く，一方，MD_p の検体ではシーケンシャルマルウェアと判定されるものが多い．Anti-Virus ソフトによるウィルス名の判定は必ずしも正しくはないが，BW による解析で BW_p の方が多数の追加プログラムをダウンロードしていることから，MD_p の検体にはシーケンシャルマルウェアが多数含まれているのではないかと推察される．

シーケンシャルマルウェアの場合，それ自体には別のプログラムをダウンロードする機能しか具備されていない．そのため，シーケンシャルマルウェアに感染した場合，最終的にどのようなマルウェアをダウンロードして実行するかは，シーケンシャルマルウェアのみの解析では分からない．したがって，最終的にどのようなマルウェアに感染したかを把握するには，開環境での動的解析が有効な手段となると考えられる．

7.3　閉/開環境での動的解析の比較

図 10 に示す結果のとおり，IRC の接続先は MD の方が多数取得し，HTTP での接続先は BW の方が多数取得した．

MD の方が多くの IRC 接続先を取得した理由としては，ボットが接続を試みた C&C サーバからの応答有無が考えられる．ボットが実行直後に接続を試みる C&C サーバのアドレスは，ボットプログラム自身にハードコーディングされている．検体によっては，複数の C&C サーバアドレスを有しており，一方のアドレスでの接続に失敗した場合には，他方のアドレスでの接続を試みる．MD では仮想インターネット内に擬似 IRC サーバを用意しているが，ボットとの間でコネクションが確立した後，レスポンスを返していない．そのため，ボットは接続失敗と判断し，自身が有する別の C&C サーバアドレスでの接続を試みる．したがって，MD では，ボットプログラム内にハードコーディングされた C&C サーバのアドレスを，バックアップアドレスも含めて抽出したと考えられる．

一方，BW の場合，ボットが接続を試みた C&C サーバが実インターネット上で稼動していた場合には，当該サーバからの応答をボットに送る．そのため，すべての C&C サーバアドレスを抽出していない可能性がある．ただし，BW で得られる IRC サーバの接続先には，C&C サーバへの接続が成功した際に行われる追加プログラムのインストールに起因するものが含まれる．

また，BW の方が HTTP の接続先を多数取得した理由として，次の 3 つが考えられる．

- ボットの追加プログラムダウンロード試行
- 追加プログラム実行にともなう HTTP 通信
- マルウェアによる接続先ランダム生成

ボットには，C&C サーバに接続した後，HTTP で追加プログラムのダウンロードを行うものが存在するため，実インターネットに接続する BW では，ダウンロードのための接続先を収集していると考えられる．また，ダウンロードした追加プログラムが HTTP での接続を行うものだった場合には，追加プログラム実行時の接続先を収集する．さらに，マルウェアによっては，HTTP の接続先を毎回ランダムに生成するものが存在している．BW は MD よりも 1 検体あたりの解析時間が長いため，ランダムに生成された接続先を多数取得することになる．

以上のように，閉環境動的解析と開環境動的解析とでは得られる情報が変化するため，目的に応じて解析環境を選択する必要がある．たとえば，1 つの検体からすべての C&C サーバアドレスを抽出する場合には MD が適しており，二次検体の取得や二次検体の接続先取得を目的と場合には BW が適していると考えられる．

© 2009 Information Processing Society of Japan

7.4　調査環境が及ぼす影響

本調査で解析を行った検体は，3.2.3 項で述べたものに限られている．さらに，能動的/受動的攻撃で拡散するマルウェアの流行は日々変化するものであるため，今回の調査でみられた傾向は永続的なものではない．また，BW での解析対象となる検体は，一定の規則に基づいて選別しているため，同一の C&C サーバに対し異なる命令系統で通信する検体が存在する場合，その状況を把握することはできていない．したがって，ユーザを攻撃から守るための技術を検討していくうえでは，継続的にマルウェアを収集し，網羅的な分析を進めなければならない．

また，BW による開環境動的解析では，解析を安全に実施するために，特定の通信のみを実インターネットに透過させている．しかし，ボットが行う独自プロトコルによる通信[17]は実インターネットに透過させていない．このように，開環境動的解析の安全性と精度のトレードオフにはまだ課題があるため，より精度良くかつ安全に開環境で動的解析を行うためにはさらなる検討が必要である．

8. 調査結果に基づく攻撃防御指針

ここで，本調査の結果に基づいた攻撃防御の指針を示す．

8.1　セキュリティパッチについて

本調査の結果では，能動的/受動的攻撃ともに，攻撃対象となる脆弱性に偏りがみられた．しかしながら，種々の脆弱性が攻撃対象となっていることから，セキュリティパッチを漏れなく適用することが最重要であると考える．

さらに，Anti-Virus を停止させる Shellcode が存在していることから，Anti-Virus をインストールしているだけでは不十分であり，セキュリティパッチを適用することが攻撃を回避するうえでは重要であるといえる．

8.2　URL フィルタリングについて

受動的攻撃について，攻撃 Web サイト間に集約構造がみられたことから，集約点となる URL に対する URL フィルタリングが，効果的な対策になると考えられる．今回の調査では，約 88%が何らかの URL に集約していたことから，少ない URL フィルタリングルールで，多数の攻撃 Web サイトへのアクセスを遮断できると考えられる．また，SQL インジェクション等で改ざんされ，踏み台となったサイトへのアクセスを遮断した場合，一般ユーザの利便性を損なう可能性があるが，集約点に対してフィルタリングを実施すれば，利便性を損ねることなく，攻撃の影響を低下させることができる．

8.3　マルウェアの挙動に基づく対策について

マルウェアの挙動解析の結果，ボットが利用するポート番号には，HTTP やメッセンジャ等で利用される，一般的なものが多く存在することが明らかとなった．したがって，感染してしまった一般ユーザを特定したり，通信を遮断したりする際に，ポート番号のみに依存した手法では困難であると考えられる．また，攻撃者からボットに対して送られる命令については，命令ごとに異なる文字列に暗号化されることがあり，単純なシグネチャを利用する IDS/IPS のみで対策を打つのも困難であると考えられる．

開環境での動的解析では，ボットに感染すると種々のホストに接続を試みるという特徴がみられている．そのため，ボットにみられるこのような特徴を利用することで，効果的なボット感染者特定や通信遮断を実現できる可能性がある．

以上のことから，感染してしまった一般ユーザを特定し，通信を遮断しようとする場合には，ポート番号や通信先，ペイロード，感染後に見られる挙動の変化を複合的に分析し，追跡することが必要であると考えられる．

9. ま と め

本調査では，DDH と Marionette という異なるタイプのハニーポットにより，能動的攻撃と受動的攻撃の現状を調査した．また，両ハニーポットで得られた検体については，MD/BW という閉/開環境動的解析システムにより，マルウェアの挙動分析を行った．

DDH による能動的攻撃調査では，狙われる脆弱性の偏りや，Shellcode のトレンドを明らかにした．また，動作中の Anti-Virus ソフトを停止させる Shellcode の存在が確認された．

Marionette による受動的攻撃調査において，iframe タグを用いる攻撃サイトは，サイト間に集約構造が存在する傾向が強いことを明らかにした．

MD と BW を用いた閉/開環境での動的解析では，マルウェアが利用する通信プロトコル，ポート番号が変化しているという事実を確認し，従来行われているポート番号ベースの単純なフィルタリングでは，感染後の被害を止めることが難しくなっているという現状を明らかにした．

以上の調査結果から，攻撃から一般ユーザを守るためには，

- セキュリティパッチの確実な適用
- 集約点となる攻撃 Web サイトに対して URL フィルタリングを実施
- ボットの通信先やペイロードに加え，ボットの挙動に基づくフィルタリングの実施

といったことが重要であると考えられる．

© 2009 Information Processing Society of Japan

今後は，各ハニーポットにより観測する領域を拡大し，より広範な能動的/受動的攻撃についての調査を行うとともに，動的解析の精度を向上させ，効率的な攻撃対策を実施するための検討を進める．

謝辞　本研究は，総務省の「スパムメールやフィッシング等サイバー攻撃の停止に向けた試行」の一環で行った調査・研究結果をまとめたものである．また，本研究を進めるにあたり協力いただきましたNTTコミュニケーションズ株式会社，Telecom ISAC Japanの関係者各位に深く感謝いたします．

参　考　文　献

1) 高橋正和，村上純一，須藤年章，平原伸昭，佐々木良一：フィールド調査によるボットネットの挙動解析，情報処理学会論文誌，Vol.47, No.8, pp.2512–2523 (2006).
2) Martines, V.: PandaLabs Report: MPack uncoverd (2007). http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf
3) Matsuki, T.: Revealing the Web-based Malware with the Client Honeypots, *Joint Workshop on Security 2008*, Tokyo (2008).
4) 川古谷裕平，柳原忠明，岩村　誠，伊藤光恭：HoneyPatch: Honeypotにおける攻撃検知手法の提案，電子情報通信学会2006総合大会，Vol.2006, No.2, p.211 (2006).
5) Microsoft: Microsoftセキュリティ情報検索．http://www.microsoft.com/japan/technet/security/current.aspx
6) skape: Understanding Windows Shellcode. http://www.nologin.org/Downloads/Papers/win32-shellcode.pdf
7) 秋山満昭，川古谷裕平，岩村　誠，伊藤光恭：クライアントハニーポットを用いたWeb感染型マルウェアの実態調査，*CSS2008*, Vol.2008, No.8, p.319 (2008).
8) Miter: Common Vulnerabilities and Exposures. http://cve.mitre.org/index.html
9) 青木一史，岩村　誠，伊藤光恭：半透性仮想ネットワークを用いたボットの動的解析手法の提案，電子情報通信学会2008総合大会，Vol.2008, No.2, p.93 (2008).
10) 独立行政法人情報処理推進機構セキュリティセンター：近年の標的型攻撃に関する調査研究 (2008). http://www.ipa.go.jp/security/fy19/reports/sequential/
11) Bambenek, J.: SQL Injection Worm on the Loose. http://isc.sans.org/diary.html?storyid=4393
12) Kojm, T.: Clam AntiVirus. http://www.clamav.net/
13) 小山　覚：ボットネット実態調査結果，*Black Hat Japan 2005 Briefings*, Telecom-ISAC Japan (2005).
14) ThreatExpert: ThreatExpert Report. http://www.threatexpert.com/report.aspx?md5=983c1f2eb2f939cd41e746c637b9fc52
15) 日本F-Secure株式会社：Allaple.A. http://www.f-secure.co.jp/v-descs/v-descs3/allaple-a.htm
16) 青木一史，伊藤光恭：CSS2008のCFPを騙ったウィルスメール検体解析結果 (2008). http://www.sdl.hitachi.co.jp/csec/css2008-cfp-malware/index.html
17) 水谷正慶，武田圭史，村井　純：通信の状態遷移に着目したボット活動の調査，マルウェア対策研究人材育成ワークショップ2008，Vol.2008, No.8, p.25 (2008).

(平成20年11月28日受付)
(平成21年 6 月 4 日採録)

青木　一史（正会員）
1981年生．2006年東北大学大学院情報科学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT情報流通プラットフォーム研究所勤務．

川古谷裕平
1980年生．2005年早稲田大学大学院理工学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT情報流通プラットフォーム研究所勤務．

秋山　満昭
1981年生．2007年奈良先端科学技術大学院大学情報科学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT情報流通プラットフォーム研究所勤務．

© 2009 Information Processing Society of Japan

岩村　　誠（正会員）

1978 年生．2002 年早稲田大学大学院理工学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所勤務．早稲田大学大学院基幹理工学研究科博士課程在学中．

針生　剛男

1967 年生．1991 年電気通信大学大学院電気通信学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所勤務．

伊藤　光恭

1959 年生．1984 年早稲田大学大学院理工学研究科修士課程修了．同年日本電信電話公社入社．現在，NTT 情報流通プラットフォーム研究所勤務．

© 2009 Information Processing Society of Japan