IPS への実装を想定したマルウェアの通信検知方法の一検討

大西 祥生 †　　常松 直樹 ‡

株式会社 MC セキュリティ
690-0816 島根県松江市北陵町 51-2
† s.ohnishi@mcsecurity.co.jp　‡ n.tsunematsu@mcsecurity.co.jp

あらまし 悪意のあるソフトウェアをダウンロードする動作や、外部からコントロール可能となる機能に代表されるマルウェアの攻撃動作により、情報漏洩の被害報告は後を絶たない。それに伴いマルウェア対策の手法も多様化している。しかし、日々増加するマルウェアに対応するには、パターンマッチングのような静的防御手法では限界がある。本論文では、研究用データセット CCC DATA set 2012 の解析を行った結果から、マルウェアの発生する通信の挙動に注目し、IPSによる動的防御手法を検討する。

A study of malware communication detection method that postulate the imple mented to the IPS

Sachio Ohnishi †　　Naoki Tsunematsu ‡

MC Security Co., Ltd.
51-2 Hokuryou-cho, Matsue-city, Shimane 690-0816, JAPAN
† s.ohnishi@mcsecurity.co.jp　‡ n.tsunematsu@mcsecurity.co.jp

Abstract Because of the malware to perform software downloads and malicious attacks, such as remote control, damage report of unending information leakage. Also, anti-malware techniques have diversified accordingly. However, in order to take measures to malware that is increasing every day, there is a limit in the static defense techniques such as pattern matching. The results were analyzed CCC DATA set 2012 data set for research, we focus on the behavior of the communication that occurs of malware, in this paper, we propose a new method for dynamic defense IPS.

1　はじめに

近年のセキュリティ関連のニュースは増加の傾向をたどり、マルウェアなどによる感染の事例や、情報漏えいのニュースは毎日 Web 上や新聞紙面上に載るようになっている現在、大企業だけでなく中小企業にもセキュリティ対策の必要性は注目されており、ウイルス対策ソフトによる保護だけでなく、UTM などの導入[1]により内外からの侵入・情報漏えい対策を実施する事業所が増加している。

しかし、ファイアウォールなどのセキュリティ機器単体では防御することは難しい。

本論文では CCC DATA set 2012 の検体における通信を分析し、詳細な動作を解析することにより IPS および他のセキュリティの観点において防御手法を考察することを目的とする。

2　検体についての情報

2.1　検体解析の目的

IPS では、パケットのペイロード部分を検出することを主に行っており、パケットのヘッダ部分はファイアウォール、構文解析は WAF 等に分担されている現状である。

国内最大のハニーポットにて収集された CCC DATA set 2012（以降、CCC2012）の検体を解析することにより、本来の IPS の役割にとらわれず、防御すべき通信内容を特定し、IPS の立場として可能な防御手法を検討することを目的とする。

2.2　検体の分類

研究用データセット CCC2012 の基本情報を表 1 に示す。

マルウェア名称は主要ウイルス対策ソフト 5 製品による検出の結果である。

表 1　検体の基本情報

検体数	10538
個体識別方法	ハッシュ
マルウェア名称	あり
通信データ	なし

表 1 のマルウェア名称を基準とし、CCC2012 をマルウェアの種類別にて分類した結果を表 2 に示す。

表 2　マルウェアの分類

種類	個数
Worm Allaple	9817
Worm Downad	683
PE Virut	13

表 2 より、CCC2012 は Worm Allaple 群に属するマルウェアが大半を占める。

よって本研究も Worm Allaple 群に属する検体を中心に行うこととする。

2.3　検体の基本動作の調査

2.2 節の通り、Worm Allaple は主要ウイルス対策ソフトにおいて検出可能であるため、ベンダーにおけるマルウェアの動作を調査した。

Worm Allaple の動作[2]

- 既知の Windows 脆弱性を利用
- 特定のレジストリキーの作成
- System32 ディレクトリ配下にファイルを作成
- 外部サーバの特定ポート番号に対してアクセスを試行

2.4　検体の選定

2.2 節において、Worm Allaple 群を中心に調査することとしたが、このうちどの検体を対象として抽出するかを決定する。

表 3 Worm Allaple 亜種分類

Worm Allaple 群		9817	100%
	Allaple.IK	9601	97%
	Allaple.PF	214	2%
	他の亜種(2 種類)	2	0%
Allaple 類似のもの※		13	
	Virut.AV	11	
	Virut.AT	2	

※ 他のウイルス対策ソフトにおいて、Worm Allaple と同名のものを抽出した

表 3 にて分類された各亜種を最低 1 個抽出し動作させることとする。

2.5　検体の動作環境の検討

2.2 節におけるベンダーの情報を元に、CCC2012 の Worm Allaple に属する検体を下記環境にて実行し、Wireshark を用い通信データを取得した。

検体実行PCおよびデータ収集PCは仮想マシン上の動作とし、2.2節における既知の脆弱性の影響を確認するため、Windows XPにおいてService Pack未適用とした。

また、検証環境外へ影響を与えないよう、ファイアウォールにより外部IPアドレスへのアクセスをすべて遮断した。

また、L2SWにより上記PCとネットワーク機器のみの環境を構築した。

検体の実行にあたり、以下の項目に考慮した。

- 検体の実行中は該当 PC において別のタスクを実行しない
- 検体実行による時間変化を確認するため、8 時間以上動作させる

3　検体の動作および検証

3.1　検体の動作

項 2.3 の環境にて対象となる検体を実行した。

実行した検体はすべて Worm Allaple 群に属するため、基本的な動作は同一となった。主要な動作は下記の通りである。

1. 外部 IP アドレスに対して ICMP ping request を送る
2. 特定の 3 サイトについて、DNS query を送信し、IP アドレスを取得する
3. 2 にて受け取った IP アドレスの TCP 80,443 に対して SYN を送信する
4. 同一ネットワークの PC に対して SMB アクセスを試みる

また、時間による通信内容の変化を確認するため、パケットキャプチャの時間経過を図 1 に示す。

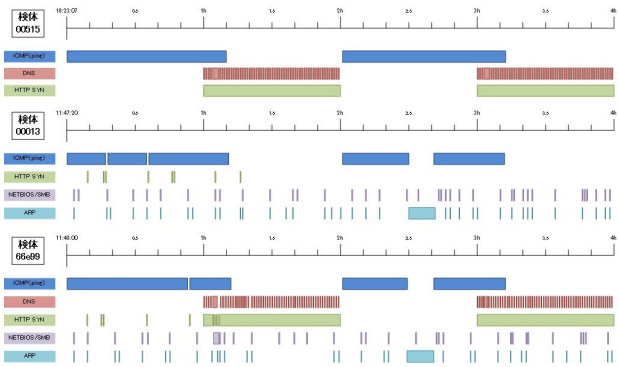

図 1　マルウェア動作シーケンス図（抜粋）

図 1 の解説を下記に示す。

1. 実行後、外部 IP アドレスに対して ping request を送る（60req/秒程度）
2. 実行から 1 時間経過後、www.if.ee および www.starman.ee の DNS query を DNS サーバに対して送信し、IP アドレスを取得する
3. 2 にて取得した IP アドレスに対して TCP 80,443 ポートに SYN を送る（3req/秒程度）
4. 実行開始から 1 時間 12 分経過後、1 の ping request が停止する
5. 実行から 2 時間経過後、2 の DNS および 3 の SYN が停止し、再度 ping request が再開する
6. 実行から 3 時間経過後再度 2 および 3 同様の DNS request および SYN 送信が始まる
7. 実行から 3 時間 12 分経過後、5 の ping request が停止する

4 時間経過後、6 の DNS request および SYN 送信が停止する

3.2　ICMP の動作

各検体において最初の動作である ping request について注目すべき下記の特徴が見受けられたため、動作を詳細に検証することとした。

- 各検体においてすべて最初が ping request から始まっている
- ping に先立ち DNS request などを行わないこと（IP アドレスが実行ファイルに内包されている）
- 約 60req/秒（3600req/分）である

動作開始から 1 時間 12 分までの ping request についてアクセス先ネットワークアドレスの抽出を行った。

また、各ネットワークについて 1 秒間にアクセスする回数について表 4 に示す。

表 4 検体 00515 アクセス先ネットワーク数

第 2 オクテットによる分類	4
第 3 オクテットによる分類	1032
Ping 送信回数総計	4196 回

時間経過による動作の変化を調べるため、第 2 オクテットによる分類にて集計した結果を図 2 に示す。

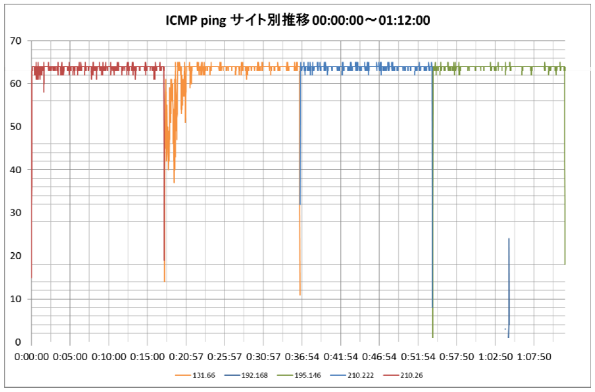

図 2　検体 00515 ICMP アクセス先
（IP アドレス第 2 オクテットによる分類）

図 2 に示したように、第 2 オクテットによる分類をすると、約 18 分毎にアクセスするネットワークが切り替わっている。

第 3 オクテットによる分類を行うと、同一のネットワークに対しては 1 秒間に 1～3 回送信し、1 秒間ウェイト、その後 1～3 回送信、と繰り返す。

3.3　DNS の動作

実行後 1 時間から開始する DNS request および TCP SYN アクセスについて注目すべき下記の特徴が見受けられたため、この動作も詳細に検証した。

- 実行より 1 時間経過後 DNS request および TCP SYN アクセスが開始し、1 時間で停止する。
- 1 時間 1 分からの 3 分間、DNS アクセス回数が非常に多くなる

DNS query は、前述のウイルス対策ベンダーによる調査結果同様、3 つのサイトに対してのアクセスしか発生しなかったが、リクエスト回数が非常に多かった。

特に多かった 1:01:00～の 1 分間では、3699 回の DNS query を送信していた。

3.4　動作についての考察

通常ネットワークの疎通確認に使用する場合の ping request は 1req/秒程度である。

第 3 オクテットによる分類によると、各 IP アドレスに対しては 1～3req/秒となっているため、IP アドレス単体で見ると通常の ping request に見える。

しかし、第 2 オクテットによる分類になると、60req/秒を超え、分あたり 3600 回を超えるリクエスト数となるため、異常な ping request と判断する。

DNS query は、通常であれば、要求ドメイン名と結果の IP アドレスがキャッシュされるため、今回のように 1 秒間に 60 回を超える DNS query および 1 分間に 3600 回を超えるアクセスは異常であると判断する。

4　IPS による防御検討

4.1　検体動作を踏まえた検討

2.6 節にて第 3 オクテットにて分類すると単体では正常であるが、第 2 オクテットにて分類すると異常値となることを説明した。

既知の手法であれば同一 IP アドレス宛のアクセスの制限は可能であると考えられるが、第 2 オクテットにより制限する手法を検討する必要がある。

また、一般的にスパム等が多く送信される国の IP アドレスに対してもアクセスの制限手法を検討する必要がある。

4.2　ping request の頻度

通常、ICMP ping は通信の疎通確認に使用するが、大量の ping request を送信することは通信路の輻輳および送信先への過度な負荷につながるため、今回のような平均 60req/秒の ping request は適正であるかを検証する必要がある。

通常、通信の疎通確認の目的としての ping 送信ケースである、クライアントによる ICMP echo request の送信頻度を調査した。

Windows における ping 送出頻度は 1req/秒である。[3]

Mac OS X における ping 送出頻度は 1req/秒である。[4]

Linux(Ubuntu)における ping 送出頻度は 1req/秒である。[5]

この ping request の防御を検討するにあたり、各検体の ping request の送信間隔を調査した結果を表 5 に示す。

表 5 ping request の送信間隔

検体ハッシュ	最大送信間隔
7daac	53ms
00515	33ms
a6b66	55ms
00013	68ms
66e99	93ms
82c67	93ms
38787	70ms
99836	50ms
a5df5	90ms

表 5 の結果より、ping 最大送信間隔は 93ms であることが判明した。

つまり、1 秒間に少なくとも 10.75req/秒以上の ping request を送信している。これを元に 10req/秒を以上のしきい値とする。

具体的な動作は、毎秒監視を行い、この条件に一致するものがあれば一定時間アクセス制限を行う。

また、今回の検体のアクセス先 IP アドレスを国別に分類し、国や地域に偏りがあるか調査した。

スパムメールなどにおいては、国別 TLD により分類され、特定の国から送信されることが多いことが知られている。

今回の ping request 先にも同様の関連性があるか確認した。

アクセス先 IP アドレスの国別に分類した結果を図 3 に示す。

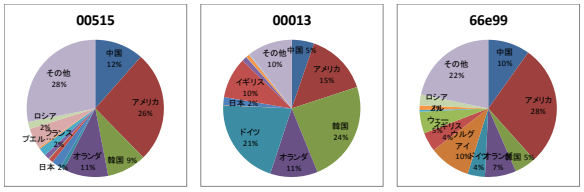

図 3 ICMP アクセス先国別分類

この図によると、スパムメール送信国として著名である東アジア地域、旧ソ連地域、中東地域のアクセスはある程度多いが、検体によりばらつきがあるため、国別ではフィルタリングできないことが判明した。

図 3 での 00515,66e99 検体で中国やアメリカへのアクセスに偏っていたものの、00013 検体では別の国のネットワークにアクセスするという動作を確認した。

今回の調査対象の検体ではスパムメール拒否および一般的なサーバへの攻撃を防御する手法として存在する「国別によるフィルタリング」による効果がうすいと考えられる。

4.3 DNS request の頻度

DNS は、通常、ドメイン名と IP アドレスの紐付けに利用される。

まず優先 DNS サーバに向けて DNS request を送信し、応答がない場合 1 秒後にリトライする。

また、結果が帰ってきた場合はその IP アドレスとドメイン名の紐付けをリゾルバキャッシュに TTL の秒数保存し、その間はキャッシュを利用し DNS アクセスをしない。

上記のように通常であれば DNS アクセスが頻繁に発生することはないが、一定の時間や単位時間あたりのアクセス回数などによる制限を行うと、サーバ移行時等 TTL を短くしている場合に影響が出る可能性があるため、一定のしきい値による防御は難しいと考えられる。

4.4 防御手法についての課題

IPS による防御を行う場合、製品ベンダー等が提供するシグネチャと呼ばれる定義ファイルを元に異常通信を判定するが、一般にペイロード部分のデータ異常や改ざん、プロトコル異常を判定し、防御する動作が主とされている。

また、フォールスポジティブ（偽陽性）が発生した場合、本来通過すべき通信を遮断してしまうことになるため、レスポンス低下やアクセス不能に陥る可能性があるため、しきい値のレートはクライアント数等に応じて変動させる必要があるか、検討する必要がある。

4.2 節にて ping request 対策の検討を行っ

たが、ping request の遮断を行う時間はさらなる検討の余地があると考えられる。

4.3 節にて DNS request 対策の検討を行ったが、DNS は TTL の影響などがあるためしきい値を設定することが難しい。

今後は時間と回数以外の別の観点から DNS を利用した負荷や攻撃の防御を検討を行う必要がある。

また、本検体では ping および DNS の動作が特徴的であったが、他のプロトコルを使用した場合も検証と防御の検討をする必要がある。

5　おわりに

今回は、検体のうち特に 00515,00013,66e99 について取り上げた。

図 1 の動作シーケンス図の通り、2 時間毎のサイクル動作をしている点、また ICMP, DNS, TCP についても 1 時間周期による動作をしている点はさらなる検証が必要である。

また、3.2 節のように、第 3 オクテットにて分類すると、1req/秒となっている点など、既存の防御手法を回避する目的と思われる動作は大変興味深いものであった。

今後もマルウェア解析を通じてクラッカー側の攻撃手法の考え方をアップデートし、今後の防御手法の検討に反映させていきたいと考える。

参考文献

[1] Web ゲートウェイ・セキュリティ製品シェア：標的型攻撃の増加で注目度が向上、老舗が 1 位を維持
http://www.sbbit.jp/article/cont1/25335/
[2] 日本 F-Secure 株式会社：ウィルス情報 Allaple.A
http://www2.f-secure.co.jp/v-descs/v-descs3/allaple-a.htm
WORM_ALLAPLE.IK | トレンドマイクロ：セキュリティデータベース
http://about-threats.trendmicro.com/malware.aspx?language=jp&name=WORM_ALLAPLE.IK
[3] ping - @IT
http://www.atmarkit.co.jp/fwin2k/win2ktips/640pinginf/pinginf.html
[4] man ping – Mac OS X Mountain Lion
[5] man ping – Ubuntu 12.04 LTS