パスシーケンスに基づく Drive-by-Download 攻撃の分類

桑原 和也 †　安藤 槙悟 ††　藤原 将志 †††　菊池 浩明 †　寺田 真敏 †††
趙 晋輝 ††

† 東海大学大学院工学研究科情報理工学専攻 259-1292 神奈川県平塚市北金目 4-1-1
mulberry, kikn@cs.dm.u-tokai.ac.jp

†† 中央大学大学院理工学研究科情報工学専攻 112-8551 東京都文京区春日 1-13-27
sando@doi-lab.ise.chuo-u.ac.jp, jchao@ise.chuo-u.ac.jp

††† 日立製作所 (HIRT) 212-8567 神奈川県川崎市幸区鹿島田 890 日立システムプラザ新川崎
masato.terada.rd@hitachi.com

あらまし 本研究では，Drive-by-Download 攻撃の通信パケットから成る研究用データセット D3M 2010 を解析し，攻撃通信データについての通信データの遷移や特徴を抽出する．さらに，観測された全ての通信のふるまいに基づいて，Web 感染型マルウェアの攻撃で使われるパスによる攻撃の分類手法を提案する．

Classification of Drive-by-Download attacks based on a sequence of paths used in the attacks

Kazuya Kuwabara†　Shingo Andou††　Masashi Fujiwara†††
Hiroaki Kikuchi†　Masato Terada†††　Shinki Cyou††

†Course of Information Science and Engineering,
Graduate School of Engineering, Tokai University
4-1-1 Kitakaname, Hiratsuka, Kanagawa 259-1292, JAPAN
††Graduate School of Science and Engineering, Chuo Universityy
1-13-27 kasuga, bunkyou-ku, Tokyoto 112-8551 JAPAN
†††Hitachi Incident Response Team (HIRT), Hitachi, Ltd.
890 Kashimada, Kawasaki, Kanagawa, 212-8567, JAPAN

Abstract This paper analyzes the D3M 2010 Dataset, captured packets used in, Drive-by-Download attack, in order to investigate features on the communications and the trasmition of states. Based on the analysis of the observed behavior of all data, we propose a method for classification of attacks with sequence of path used by the attacks.

1　はじめに

近年，インターネット上の脅威の一つとして，Web ブラウザの脆弱性を利用して感染させる Drive-by-Download 攻撃 [1] によるマルウェアの感染被害が後を絶たない．中でも 2009 年 4 月に出現した Gumblar は，亜種の発生が非常に早く [2]，従来のパターンマッチングによるマルウェアの検知では対応が遅れてしまう．例えば，IP フィルタリングは，既知の IP からの攻撃を防ぐことは可能であるが，存続期間が短

い Drive-by-Download などの Web を利用した攻撃には有効でない．次々と新たなホスト名を用いた攻撃サイトが作られる [3].

そこで本研究では，マルウェア本体の挙動ではなく，マルウェアがダウンロードされるまでの通信と挙動の特徴に着目し，未知の攻撃に対しても有効な分類方法を提案する．サーバのアドレスが変わっても，引き起こされる一連の攻撃のパス列は変動しないことに着目し，攻撃検知や識別に利用することが出来るのではないかと考える．そこで，私たちは，Web 感染型マルウェアの通信を観測した MWS2010 研究用データセット D3M2010 攻撃通信データ [4] を用いて，本仮説を検証した．通常の通信から逸脱している通信の遷移を特定することにより，Drive-by-Download 攻撃固有のパスに注目し，次の 3 つの提案手法により攻撃の分類を試みる．

攻撃パターン特徴量 A**.** Drive-by-Download 攻撃に用いられる通信の発信元 IP などの特徴.

フルパスインデックス B**.** 一連の攻撃に用いられる URL のパス列.

脆弱性特徴量 C**.** 攻撃に用いられる脆弱性の種類と数.

2 D3M 2010 攻撃通信データの解析

D3M 2010 攻撃通信データは，Web クライアントハニーポット 10 台で特定の URL を巡回した時の通信をキャプチャした pcap 形式のデータである．特定の URL は，公開ブラックリストの提供サイト (malwaredomailist.com) に登録されている URL の中から，Drive-by-Download 攻撃を検知した URL である (以下，この URL を巡回対象 URL と呼ぶ).

2.1 攻撃通信データの分割

基本となる攻撃の単位を次の様に定義する．

表 1: 各観測日の巡回対象 URL へのアクセスのデータ

観測日	2010/3/8	3/9	3/11
抽出不能 URL	205	180	172
該当スロットなし URL 数	25	6	5
一意な URL 数	163	158	158
不確定 URL 数	17	16	9
計	180	174	164

表 2: 巡回対象 URL へのアクセスが確認できなかった URL に対しての調査

観測日	2010/3/8	3/9	3/11
抽出不能 URL	25	6	5
DNS 応答なし	4	0	0
DNS（応答ある）解決不能	2	2	0
DNS 応答あり 3-way 未確立	19	4	5

定義 1 (スロット) *1* つの巡回対象 *URL* へのアクセスにより生じる一連の通信，すなわち，*HTTP* 通信が行われ，リダイレクト，外部サイトのスクリプトや画像の読み込みなどの派生先 *URL* へのアクセスを含む複数の通信路を**スロット**と呼ぶ.（スロットは“ 観測日-識別番号 ”の形式の *ID* で識別する）.

スロットへの分割は次のように行う；(1)Referer ヘッダ (参照元 URL) を含まない GET リクエストを抽出，(2) 巡回 URL リストの URL を照会し，巡回対象 URL へのアクセスを行っている GET リクエストを抽出，(3)GET リクエストが複数出力された場合は，目視で調査し巡回対象 URL へのアクセスを特定する.

各観測日の巡回対象 URL へのアクセスデータは表 1 の通りである．1 件も候補が存在しない URL に対しては，DNS による名前未解決，サーバーエラーなどの原因が考えられる．失敗の原因を表 2 に示す．巡回対象 URL のリストに幾つか重複した URL が存在していたが，抽出した GET リクエストのパケットログを調査した結果，URL が重複していてもアクセスは 1 度きりであると判明したため，重複 URL はユニークとした.

以上の処理により，D3M 攻撃通信データ 3 日間を 518 スロット分割にした.

表 4: パスのゆらぎ (攻撃パターン $B-1$)

308-2	308-45	308-149	309-4	309-82	309-155	311-53	311-59	311-74
15	15	15	15	15	15	15	15	15
15	15	15	15	15	15	1	180	1
57	57	57	57	57	57	180	169	
1	1	1	1	1	1	169	170	
180	180	180	180	180	180	170	171	
169	169	169	169	169	169	171	176	
170	170	170	170	170	170	176	173	
171	171	171	171	171	171	173	174	
176	176	176	176	176	176	174	175	
173	173	173	173	173	173	175	181	
174	174	174	174	174	174	181	50	
175	175	175	175	175	175	50	183	
181	181	181	181	181	181	183	184	
50	50	50	50	50	50	184	179	
183	183	183	183	183	183	178	175	
184	184	184	184	184	184	172	168	
180	177	180	180	180	180	172	177	
174	172	173	177	177	174	182	178	
182	175	182	178	179	178	183	168	
178	180	176	173	178	175	173	173	
172	174	177	179	173	179	176	174	
185	182	172	175	176	173	168	176	
177	170	175	174	175	177	171	168	
172	179	178	176	170	176	181	172	
175	172	172	167	167	170	183	170	
179	176	185	167	167	171	179	170	
181	178	167	172	172	183	174	172	
	181	179	172	172	167	177		
	185	181	172	167	172	173		
	168	174	167	172	182	174		
	168	167	181	181	168	170		
	167	172	167	167	172	172		
	167	168	182	182	168	172		
	172	167	185	185	167	170		
	168	167	168	168	172	177		
	167	168	168	168	185	170		
	170	168	168	168	181	171		
	175	170	176	173	168	185		
	173	175	170	174	174	168		
	176	176	174	170	176	170		
		174	175	175	173	169		
					175	183		
						172		
						175		

3 提案方式

3.1 既知攻撃の特徴

D3M2010 の攻撃通信データには，Gamblar の亜種であり，8080 ポートを使うことで有名な ru:8080[6] が 13 回，3129-3126 ポートを使うインジェクション攻撃 [7] が 13 回観測された．ru:8080 で引き起こされる一連の URL の関係を図 1 に示す．

これらの攻撃にはそれぞれの特徴的なポートを使う事に加え，表 3 に示す一連の通信で用いられるディレクトリ構造 (以下，パス) の特徴が見られた．このように初めの誘導サイトと中継サイトのホスト名はまちまちであったが，そこで用いられるシーケンスは全て同じであった．これは，ru:8080 に限らず他の攻撃にも観測される特徴であり，例えば表 4 に示される 9 スロットは最初の 4 つを除いてほぼ一定のパスシーケンスを持つ．これらは，後述する攻撃パターン $B1$ に分類されるパスシーケンスである．

3.2 攻撃パターン特徴量 A

表 5 に，518 スロットから抽出した代表的な攻撃パターンの一覧 $A1, \ldots, A12$ を示す．各パターンは，URL のパスの特徴的な文字列によって識別されている．ここで DNS 数，IP 数は，各攻撃パターンの特徴を満たすのものの数である．表 5 の 1〜7 の攻撃パターンは全て，1 つのパスに対して，複数の IP が存在する．攻撃パターン 13 は 1 つの IP からの攻撃であるが，同じパスのシーケンスにもかかわらず，マルウェアの配布を成功した場合とそうでない場合が存在する．このことから，ある決まった条件の時のみ，マルウェアをダウンロードするように考えられる．

最も頻度が高かった攻撃は，pdf.php を含む攻撃パターン $A3$ である．

3.3 フルパスインデックス特徴量 B

3.1 節の解析により，同一のマルウェアによる攻撃は，脆弱性コードを埋め込む Web サーバは変わっていても，そこから遷移するパスは共通であることが多い事が分かった．そこで，このパスのシーケンスを，攻撃を識別するための特徴量として用いることを提案する．URL から DNS 名を取り除いたものをフルパスと呼び，一意な識別番号で参照する．パスシーケンスの中の特徴的な部分パスを用いて，表 6 の 21 パターンの特徴量 $B1, \ldots, B21$ を定めた．これをフルパスインデックスと呼ぶ．

3.4 脆弱性特徴量 C

同一のマルウェアならば，用いる脆弱性コード CVE の組みにも共通の特徴が見られるはずである．そこで，Blake Hartstein によって開発されたマルウェアアンパックツール jsunpack-n[5] を用いて，各攻撃で用いられる脆弱性を抽出し，その組を特徴量とすることを考える．

jsunpack-n とは、通信に含まれる脆弱性を突いた攻撃の検出を行うツールで、通信の要約、受信データの解読、難読化の解除を行うことができる．D3M では，CVE2005-2127 から 2010-0249 までの 14 種類の脆弱性が用いられた．攻撃パターン 3 の脆弱性を表 7 に整理した．(図 2 は，誘導される URL 数の分布を示している．平均 7.29 である．)

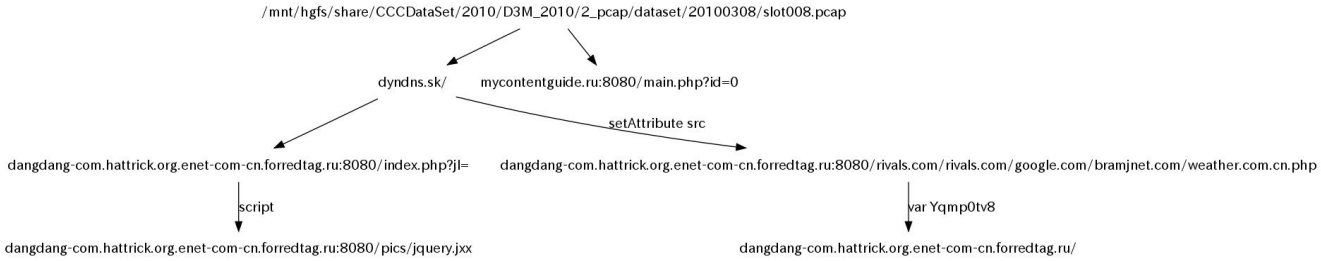

図 1: ru:8080 攻撃により誘起される URL の関係 (スロット ID，308-8)

表 3: ru:8080，3126-3129 攻撃のパスのシーケンス

No.	ru:8080 Gumblar	3126-3129 インジェクション攻撃
1	/index.htm またはなし	.html またはなし
2	.com.php または.com.cn.php	/in.php
3	/index.php?jl=	/js
4	/pics/jquery.jxx	/download/index.php
5	/mycontentguide.ru:8080 /main.php?id=0	/download/jabber.php
6	/pics/ChangeLog.pdf	/download/banner.php?spl=mdac
7	/pics/java.html	
8	/pics/JavaJopa.jar	
9	/pics/JavaJopa.jar	
10	/pics/JavaJopa.jar	
11	/pics/JavaJopa.jar	
12	/welcome.php?id=9&hey240	

表 7: 脆弱性

脆弱性	観測回数	
$C1$	CVE-2005-2127	15
$C2$	CVE-2006-0003	35
$C3$	CVE-2006-3730	10
$C4$	CVE-2006-5820	1
$C5$	CVE-2007-0024	15
$C6$	CVE-2007-5659	159
$C7$	CVE-2008-0015	2
$C8$	CVE-2008-2463	28
$C9$	CVE-2008-2992	94
$C10$	CVE-2009-0927	107
$C11$	CVE-2009-1136	34
$C12$	CVE-2009-1492	36
$C13$	CVE-2009-4324	23
$C14$	CVE-2010-0249	36
計	595	

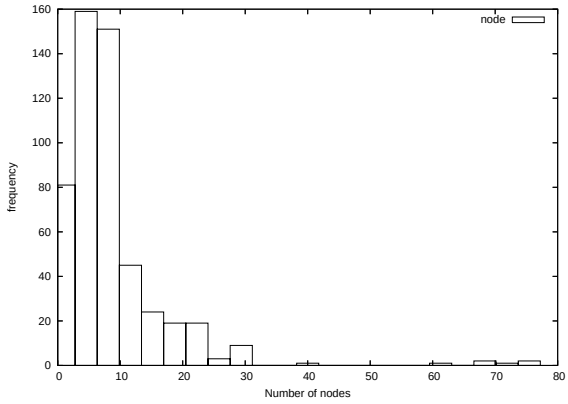

図 2: ノード数の分布

4 攻撃分割の精度

4.1 既知の攻撃に対する精度

提案した分割方法の有効性を考える．既知の攻撃 G(ru:8080，インジェクション-3129 攻撃等) に対して，攻撃パターン A，フルパスインデックス B，脆弱性 C の 3 つの方式での識別結果を表 8，9，10 に各々示す．それぞれの表で 0 は各パターン以外のその他に分類した．$A1$，$A5$，$A7$ によって既知攻撃 ru:8080 を識別する時の再現率，適合率は，

$$R_{A8080} = \frac{4}{13} = 0.31,$$
$$P_{A8080} = \frac{4}{49} = 0.08$$

であり，同様に 3126 に対しては，$R_{A3126} = 2/13 = 0.15$，$P_{A3126} = 2/5 = 0.4$ である以上により，

表 5: 攻撃パターン特徴量分割 A

攻撃パターン	パスに含まれる特徴的な文字列/発信元 IP	スロット数
$A1$	“index.php?spl=2”	27
$A2$	“cache/PDF.php?st=Internet\%20Explorer\%206.0”	34
$A3$	“pdf.php[pdf]”	55
$A4$	“load.php?a=a\&e=6$”	15
$A5$	“/load.php?spl=mdac$”	8
$A6$	“/load.php?id=0$”	7
$A7$	“/load.php”	24
$A8$	“85.17.90.206	17
$A9$	“91.213.174.22	8
$A10$	“213.163.89.54	21
$A11$	“$/newload.php?ids=MDAC$”	7
$A12$	115.100.250.73 ”	8
	計	231

表 6: パスによるスロットの攻撃分割 B

	フルパスシーケンス	第 1 フルパス（シーケンスの初めのパス）	スロット数
$B1$	180, 169, 170, 171, 176, 173,	/res/1/1/images/page_progressbar.gif	9
	174, 175, 181, 50, 183, 184		3
$B2$	60, 2	/java	19
$B3$	3, 4, 62	/cache/CSS.css	11
$B4$	199	/zcv.gif	20
$B5$	64, 66、67	/new/da.js	11
$B6$	71, 8	/pca3.crl	12
$B7$	56	/index.php	17
$B8$	53 or 63	/in.cgi?3	11
$B9$	4	/cache/PDF.php?st=Internet\%20Explorer%206.0	10
$B11$	(198)	/x/?html=1&id=992&hash=6339a5f067adeab2eb7cd0e942c81583	6
$B12$	197, 10, 9	/wp.js	6
$B13$	(7), 6	/cry217/xd.php	3
$B14$	(190), 193, 195	/webalizer/050709wareza/crack=17=keygen=serial.html	5
$B15$	58	/intl/ja/images/jawh_prodicons1.png	3
$B16$	(188), 52	/script/in.cgi?2	30
$B17$	72	/pdf.php	3
$B18$	12	/ga.js	7
$B19$	52	/in.cgi?2	3
$B20$	(54)	/in.cgi?4	6
$B21$	(187)	/s/	2

表 8: A と G の関係

G ＼ A	1	2	5	7	9	0	計
8080	2	0	1	1	0	9	13
3126-3129	0	1	0	0	1	11	13
その他	25	0	0	20	5	251	301

表 9: B と G の関係

G ＼ B	4	10	14	18	0	計
8080	2	0	0	0	11	13
3126-3129	0	1	6	1	5	13
その他	10	10	0	2	291	313

A の総合的な精度をこれらの平均再現率で,

$$R_A = \frac{0.31 + 0.08}{2} = 0.20$$

と定める.

再現率が低い理由は，A を定める際に，既知の攻撃を除外したためである．$G \times B$，$G \times C$ についても同様に $B4$ と $C1$，$C2$ を ru:8080 の識別条件として，再現率を求めると，$R_{B8080} = 2/13 = 0.15$, $R_{B3126} = 8/13 = 0.61$, $R_{C8080} = 4/13 = 0.31$, $R_{C3126} = 10/13 = 0.91$ であった. 再現率の平均値は,

$$R_B = 0.38, R_C = 0.54$$

，従って，既知攻撃に対しては，C が最も精度が高い.

表 10: G と C の関係

G ＼ C	1	2	3	4	5	6	7	8	9	10	11	12	13	0	計
8080	2	2	1	0	0	0	0	0	1	0	0	0	0	0	6
3126	0	1	3	1	2	1	0	0	1	1	0	0	0	1	11
その他	34	156	90	9	105	22	15	34	33	35	15	1	2	27	

表 11: A と C の関係

A ＼ C	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	36	63	28	7	24	5	15	11	5	22	2	1	1	4
1	0	24	6	0	24	0	0	0	0	0	0	0	0	1
2	0	19	7	0	7	0	0	8	0	0	0	0	0	8
3	0	41	41	0	41	18	0	13	0	14	13	0	1	13
4	0	1	1	0	1	0	0	2	0	0	0	0	0	2
5	0	2	2	0	2	0	0	0	2	0	0	0	0	0
6	0	7	7	0	0	0	0	0	7	0	0	0	0	0
7	0	0	0	3	0	0	0	0	21	0	0	0	0	0
8	0	2	2	0	8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0

4.2 分類方式間の相関

特徴量 A と脆弱性特徴量 C との相関をクロス集計で表 11 に示す．単一の攻撃パターンが数多くの脆弱性を使っている事が表されている．A と C は独立と言える．

5 結論

本論文では，D3M2010 攻撃通信データにおける，パスを用いた通信の振る舞いについて報告した．この攻撃パターンにはそれぞれ特徴があり，例えば，パスに pdf.php（$A3$）を含む攻撃では，多くの脆弱性が使われていた．従って，脆弱性の関連性から攻撃パターンを正しく識別することは困難である．

参考文献

[1] Alexander Moshchuk, Tanya Bragin, Steven D. Gribble, and Henry M. Levy: “A Crawler-based Study of Spyware on the Web”

[2] 水谷 正慶，武田 圭史，村井 純: “Web 感染型悪性プログラムの分析と検知手法の提案”，電子情報通信学会論文誌. B, 通信 J92-B(10), 1631-1642, 2009-10-01

[3] 阪井 哲晴，寺田 真敏，土居 範久: “Web サイトに埋め込まれたインジェクション攻撃の追跡検知システムの提案”，情報処理学会研究報告，Vol.2010-CSEC-48 No.9, 2010-03-04

[4] 畑田 充弘，中津留 勇，秋山 満昭，三輪 信介: “マルウェア対策のための研究用データセット ～ MWS 2010 Datasets ～”，マルウェア対策研究人材育成ワークショップ 2010（MWS2010），2010.

[5] jsunpack-n: https://code.google.com/p/jsunpack-n/

[6] Andrew Brandta: “When admins attack: 30 hours in the life of a Gumblar victim”

[7] インジェクション - 3129: http://jvnrss.ise.chuo-u.ac.jp/csn/