Computer Security Symposium 2014
22 - 24 October 2014

実環境におけるサイバー攻撃検知システムの有効性評価および検知範囲の拡大に向けた検討

大谷 尚通† 益子 博貴† 重田 真義†

†株式会社 NTT データ
135-8671 東京都江東区豊洲 3-3-9
{ootanihs,mashikoh,shigetam}@nttdata.co.jp

あらまし 我々が開発したサイバー攻撃検知システムは, ネットワーク機器のログに残った Drive-by-Download 攻撃の定性的な特徴を用いてマルウェアを検知する. そのため特徴の異なる Exploit Kit の出現にあわせて検知パターンを継続的に追加している. また実環境では, マルウェアは Drive-by-Download 攻撃以外の方法でも組織内の端末に感染する. そこで感染後のマルウェアを検知できるよう, C&C 通信のログを分析して新たな検知方式を検討した. 本稿では, 本システムの実環境における検知実績および MWS2014 データセットに対する検知率の評価結果を述べる. C&C 通信ログの分析結果および検知方式の検討結果も説明する.

Study for the expansion of the detection range and the assessment of the effectiveness of cyber attack detection system in a real system

Hisamichi Ohtani† Hiroki Mashiko† Masayoshi Shigeta

†NTT DATA Corporation
Toyosu 3-3-9, Koto-ku, Tokyo 135-8671, JAPAN
{ootanihs,mashikoh,shigetam}@nttdata.co.jp

Abstract Cyber attack detection system developed by us detects malware by using the qualitative features on the network device's log by the Drive-by-Download attacks. Therefore, each time we found the Exploit Kit with different features, we are adding the detection pattern constantly. In addition, malware can infect the windows terminal on the actual organization network by without of the Drive-by-Download attack. Therefore, in order to detect the malware infection, we examined the detection method using the feature by analyzing the C&C communications log. In this paper, we describe the evaluation results of the detection rate for MWS2014 dataset, and an example detected by the system on the actual organization network. We also explain the consideration results of the detection method and analysis of C&C communications log.

1 はじめに

我々が開発したサイバー攻撃検知システム [1] は, ネットワーク機器のログを用いて Drive-by download 攻撃（以下,「DBD 攻撃」とする）によるマルウェア感染を検知する [2]. 本システムの検知方式は, DBD 攻撃のメカニズムによって発生する定性的な特徴を利用する. たとえばマルネ

ット 4 層モデル [3] と呼ばれる方式の DBD 攻撃は,「おとり」「リレー」「Pre-Exploit」「Exploit」の 4 段階の状態を遷移してマルウェアに感染させる. この状態遷移のメカニズムによって Web ブラウザの内部の状態変化が起こり, その特徴的な状態が Proxy サーバの通信ログに記録される. 筆者らはこの 4 段階の状態遷移を感染フェーズ (図 1) と定義し, この状態遷移を利用して DBD 攻撃を検知する [1]. このような DBD 攻撃の基本メカニズムによって発生した定性的な特徴は, 攻撃者側が容易に変更できない. よって本システムの検知方式は, Exploit Kit の設定変更や亜種への変化などの軽微な差異や, Exploit Kit の種類による違いに影響されずに DBD 攻撃を検知できる. また感染フェーズで DBD 攻撃を検知するため, マルウェア本体をダウロードする前にマルウェア感染の危険性を検知でき, 検知後すぐに通信を遮断すればマルウェア感染を未然に防ぐことができる. 本稿では, まず本システムの実環境における検知実績と MWS2014 データセットにおける検知率の評価結果を述べる.

2 検知実績

本システムが 2013 年 6 月から 2014 年 8 月の間に検知したサイバー攻撃のうち, Exploit Kit を使用した DBD 攻撃によるものを図 2 に示す. 使用した Exploit Kit を推定できた場合はその Exploit Kit 別に色分けした. 検知件数が少ない Exploit Kit はその他へ, Exploit Kit が推定できなかった場合は不明へ分類した.

2013 年下半期は DBD 攻撃を数多く検知した. これは, 水飲み場型攻撃 (Watering Hole Attack) の一種である Web 待ち伏せ攻撃を多く検知できたためである. 水飲み場型攻撃は, 特定の人物や組織を狙い, その標的がアクセスする可能性の高い Web ページへ DBD 攻撃などの罠を仕掛けておき, 当該 Web ページをアクセスした標的の PC へマルウェアを感染させる攻撃である. Web 待ち伏せ攻撃は, 攻撃対象を限定せず, 有名な Web ページや有用な情報が掲載された Web ページなど不特定多数の Web 閲覧者がアクセスする Web ページへ, DBD 攻撃などの罠を仕掛ける攻撃である. われわれは, この水飲み場型攻撃と少し異なる攻撃方法を Web 待ち伏せ攻撃と呼ぶ [1].

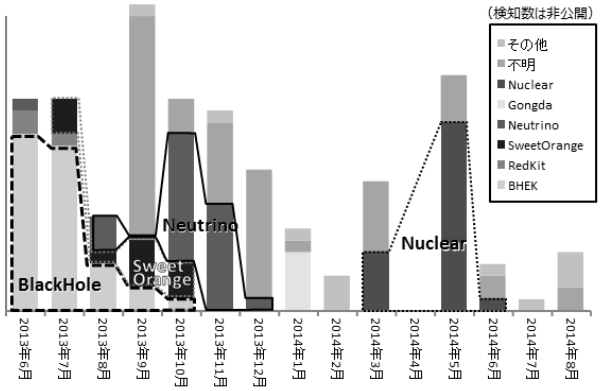

図 2: DBD 攻撃等の検知実績

本システムが検知した Web 待ち伏せ攻撃の実例を以下に示す.

- 無料ブログページ, 旅行代理店の Web ページ (広告表示) の Web 待ち伏せ攻撃
- VAWTRAK[1] 関連の Web 待ち伏せ攻撃
- 個人ブログやアフィリエイト広告表示経由

[1]2014 年 5 月 20 日から 5 月 28 日にかけて DBD によって感染が増加したネットバンキングの認証情報を詐取するマルウェア

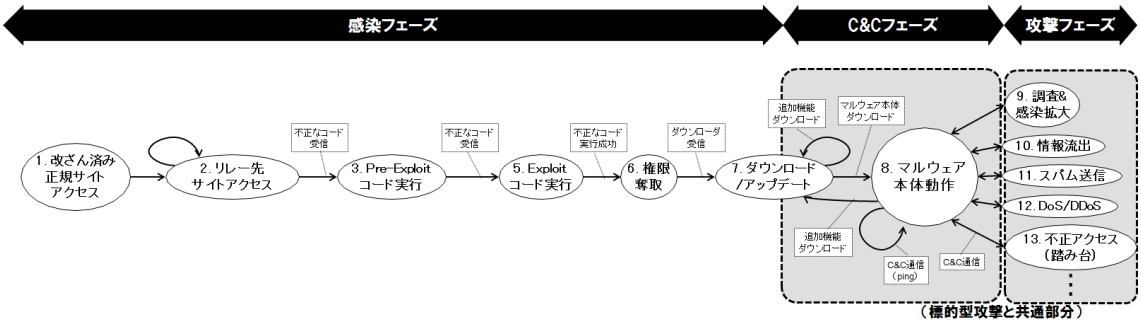

図 1: Web 待ち伏せ攻撃の状態遷移

の Web 待ち伏せ攻撃

Web 待ち伏せ攻撃に使われている Exploit Kit は, 2013 年 6 月から 10 月までは BlackHole Exploit Kit, 2013 年 7 月から 10 月までは SweetOrange Exploit Kit, 2013 年 10 月から 12 月までは Neutrino Exploit Kit, 2014 年 3 月から 2014 年 6 月までは Nuclear Exploit Kit といったように 3ヶ月〜5ヶ月程度で傾向が変化している (図 2). 攻撃者が, ウイルス対策ソフトによる検知を回避するために, 水飲み場型攻撃や Web 待ち伏せ攻撃に使用する Exploit Kit のライフサイクルを管理していることが予想される.

3 D3M の検知率

D3M (Drive-by Download Data by Marionette) を用いて本システムの検知率を評価した. D3M には, 以下の 2 種類のデータが含まれている [5].

- Web クライアント型ハニーポット (Marionette) が悪性 URL を巡回して得た DBD 攻撃の通信データ
- 上記の Web クライアント型ハニーポットが取得したマルウェアをマルウェアサンドボックス (Botnet Watcher) 上で実行して得た C&C 通信データ

本システムは, 主に DBD 攻撃を検知するため, 前者の DBD 攻撃の通信データを使用して検知率を測定した. DBD 攻撃の通信データは pcap 形式のため, 通信データから HTTP 通信のみを抽出し, 本システムが処理可能な Proxy ログ形式へ変換した. また, DBD 攻撃の通信データには, 直接マルウェアを取得している場合など,「リレー」「Pre-Exploit」「Exploit」の状態遷移の通信データがない場合が含まれている. これらの通信データを除いて検知率を測定した.

3.1 検知率の評価結果

本評価では, Proxy ログ形式の D3M の通信データ 276 個に対して本システムに実装されている DBD 攻撃の検知パターン 12 個を実行した.

表 1: 通信データ取得年別の検知率

取得年	通信データ数	検知数	検知率
2011	116	64	55.2%
2012	110	94	85.5%
2013	42	40	95.2%
2014	8	0	0.0%
合計	276	198	71.7%

通信データの取得年別に検知率を求めると, 2011 年の検知率は 55.2%と低いが, 2012 年と 2013 年は検知率 80%以上を達成し, 2013 年の検知率 95.2%が最も高い. 2014 年の通信データからは DBD 攻撃を検知できなかった. Web で使用される Exploit のうち, 90%以上は Java の脆弱性を悪用していると言われている [4]. そのため本システムの DBD 攻撃の検知パターンは,Java の脆弱性を悪用した Exploit を検知するパターンが多い. D3M 2014 を分析したところ, 2014 年の通信データには Java の Exploit の特徴が含まれていないことがわかった. そのため本システムは, D3M 2014 の通信データ 8 個を検知できなかった.

表 2： 検知パターンと検知数の関係

パターン / 年月日	A	B	B,C 重複	C	C,D 重複	D	E
2011年	0	21	31	15	0	0	1
2012年	7	0	0	63	4	0	0
2013年	40	0	0	1	0	0	0
2014年	0	0	0	0	0	0	0
小計	47	21	31	79	4	0	1

パターン	A	B	C	D	E
合計	47	52	114	4	1

本システムの DBD 攻撃の検知パターン 12 個のうち, A〜E の 5 個の検知パターンで重複を除き 198 個の DBD 攻撃を検知した. 本システムは, 定性的な特徴を用いて DBD 攻撃を検知するため, 複数の定性的な特徴を持つ DBD 攻撃は, 複数の検知パターンが重複して検知する.

表 2 から, DBD 攻撃を検知したパターンは通信データ取得年別に偏っていることがわかる. 2011 年は検知パターン B と C, 2012 年は検知パターン C, 2013 年は検知パターン A が多く検知されている. D3M の DBD 攻撃の通信データ

からも, DBD 攻撃の感染手法の傾向が変化していることがわかった.

誤検知率は, D3M の通信データでは評価できない. そこで実際の組織の Proxy ログを用いて誤検知率 (False Positive) を測定した. Proxy ログから, Google や Microsoft などの Web ページの改ざんが起きにくくアクセス数が多い Web ページへのアクセスログを取り除き, 残った約 1200 万行, 約 8 万 9000 ドメインに対して誤検知 (False Positive) を調査したところ, 0.011〜0.0033%であった [2].

3.2 DBD 攻撃検知方式の課題

D3M を用いた検知率の評価結果や実環境での運用経験から, 以下の本システムの検知方式の課題が得られた.

1. Java 以外の脆弱性, 特に IE や Flash, Silverlight の脆弱性を悪用した DBD 攻撃の検知
2. 通信データに定性的な特徴が現れにくい基本メカニズムを使用した DBD 攻撃は, 検知精度の高い検知パターンの作成が困難
3. DBD 攻撃の基本メカニズムが大きく変化した場合, 既存の検知パターンでは対応できない
4. DBD 攻撃以外の方法で組織内の端末がマルウェアに感染した場合は, 検知できない

たとえば, 本システムが検知できなかった 2014 年の DBD 攻撃の通信データを分析すると, Proxy ログ形式へ変換後の通信データは既存の検知パターンと一致しないだけでなく, 定性的な特徴が乏しく有効な検知パターンの作成も困難なことがわかった.

通信データに定性的な特徴が現れにくい基本メカニズムを使用した DBD 攻撃や DBD 攻撃の基本メカニズムが大きく変化した攻撃が出現した場合も, 本システムは検知できない.

また標的型攻撃メールにマルウェアが添付されていたりメール本文の URL リンクや SEO 攻撃などにより, ユーザが操作してマルウェアをダウンロードしてインストールする場合も, 本システムの DBD 攻撃検知方式ではマルウェアを検知できない.

4 C&C 通信の検知方式の検討

DBD 攻撃検知方式の課題を解決するためには, まず特徴の異なる Exploit Kit の出現にあわせて検知パターンの継続的な追加が必要である. しかし通信データに定性的な特徴が現れにくい Exploit 通信の場合や DBD 攻撃以外の方法でマルウェアに感染する場合は, 検知パターンの追加では対応できない. そこで感染後のマルウェアを検知できるよう, 図 1 の C&C フェーズ以降の通信のログを分析して新たな検知方式を検討した.

4.1 D3M の C&C 通信の分析

D3M のうち, マルウェアサンドボックス (Botnet Watcher) が収集した通信データを分析した. マルウェアサンドボックスは, Web クライアント型ハニーポットが取得したダウンローダやマルウェアをサンドボックス上で実行して, マルウェア本体のダウンロード通信や C&C 通信を pcap 形式で取得している. 前記の検知率評価の場合と同様に, pcap 形式の C&C 通信データをトランスポート層, アプリケーション層レベルのデータへ再構成して, 処理しやすいログ形式へ変換したのちに分析した.

4.1.1 C&C 通信 (Protocol) の分析結果

D3M の C&C 通信データ 48 個について,TCP 通信と UDP 通信の比率を分析した結果を図 3 に示す. D3M の C&C 通信データは, 平均して約 25%が TCP 通信, 約 75%が UDP 通信であった. 個別の C&C 通信データを比べても,UDP 通信の占める割合が高い場合が多い. したがって多くのマルウェアは, 図 1 の C&C フェーズ以降において,UDP 通信を多用すると予想される. ただし D3M 2014 の C&C 通信データは, TCP 通信の占める割合が高い (図 3) .

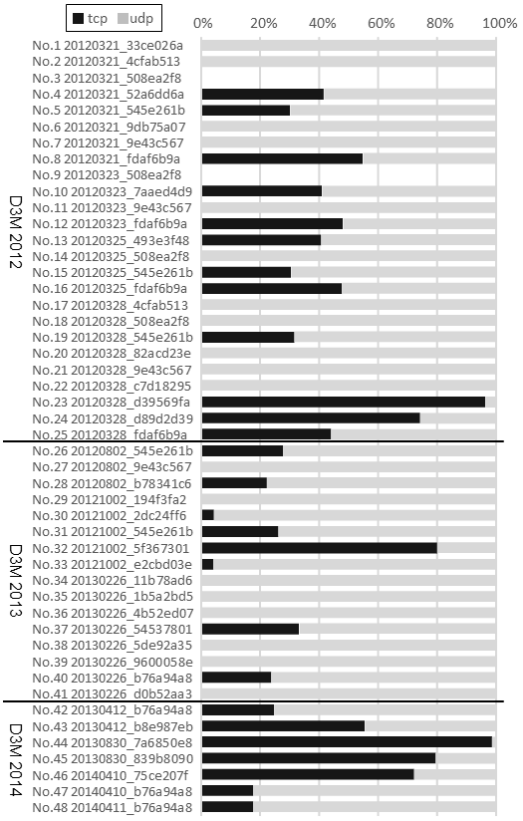

図 3: D3M の C&C 通信 (Protocol) の構成

表 3： D3M 2014 の C&C 通信 (Port) の構成

D3M Botnet Watcher			arp	igmp	tcp							udp			
	No	通信データ			25	428	443	80	8080	8082	その他	53	137	138	その他
D3M 2012	1	20120321_33ce026a	4	2										3	
	2	20120321_4cfab513	6	1								2	18	4	1
	3	20120321_508ea2f8	5	2											
	4	20120321_52a6dd6a	6	2							9	4		6	4
	5	20120321_545e261b	6	2							16	17		3	17
	6	20120321_9db75a07	6	2										3	
	7	20120321_9e43c567	6	2								5	162	3	5
	8	20120321_fdaf6b9a	5	2							11	4		1	4
	9	20120323_508ea2f8	4	2											
	10	20120323_7aaed4d9	8	1					156			224		3	221
	11	20120323_9e43c567	6	1								5	162	3	5
	12	20120323_fdaf6b9a	6	1							13	5		4	5
	13	20120325_493e3f48	6	1					152			222		3	217
	14	20120325_508ea2f8	6	1										2	
	15	20120325_545e261b	6	2							18	19		3	19
	16	20120325_fdaf6b9a	6	1							11	4		4	4
	17	20120328_4cfab513	8	1								2	36	4	1
	18	20120328_508ea2f8	6	2										3	
	19	20120328_545e261b	5	2							18	18		3	18
	20	20120328_82acd23e	5	1										5	
	21	20120328_9e43c567	6	2								5	162	3	5
	22	20120328_c7d18295	5	2										3	
	23	20120328_d39569fa	7	2					11	22	4093	67		6	84
	24	20120328_d89d2d39	5	2				14			113	15			29
	25	20120328_fdaf6b9a	7	2							11	4		6	4
D3M 2013	26	20120802_545e261b	9	2							18	22		6	19
	27	20120802_9e43c567	14	1								5	54	3	5
	28	20120802_b78341c6	14	2				2				2		3	2
	29	20121002_194f3fa2	4	2							2	10		3	585
	30	20121002_2dc24ff6	5	2			2					33		6	6
	31	20121002_545e261b	5	2							17	24		6	18
	32	20121002_5f367301	8	2					12					6	
	33	20121002_e2cbd03e	6	2			2					34		6	7
	34	20130226_11b78ad6	7	2							2	10		6	613
	35	20130226_1b5a2bd5	9	2							2	10		6	632
	36	20130226_4b52ed07	8	2							2	10		6	627
	37	20130226_54537801	10	2			4					1		6	1
	38	20130226_5de92a35	7	1							2	10		6	592
	39	20130226_9600058e	9	2							2	10		6	611
	40	20130226_b76a94a8	16	2				4			109	9		9	345
	41	20130226_d0b52aa3	8	2										6	
D3M 2014	42	20130412_b76a94a8						2			111	9			334
	43	20130412_b8e987eb						78			41	78			78
	44	20130830_7a6850e8						162			3618	28			28
	45	20130830_839b8090			1259	517	411	1267			5328	1245			1026
	46	20140410_75ce207f						4			79	9			23
	47	20140410_b76a94a8						2			87	9			407
	48	20140411_b76a94a8						2			87	9			407

4.1.2 C&C 通信 (Port) の分析結果

D3M の C&C 通信データにおいて使用された TCP 通信と UDP 通信のポート番号を分析した結果を表 3 に示す. TCP と UDP の多数の High ポートに対する通信は, すべてを表に掲載することが難しいため「その他」にまとめた. D3M の C&C 通信データのうち, マルウェアによるものと思われる well-known ポートの通信は以下のとおりである.

UDP 53 (DNS) 同一通信先へのアドレス解決が一般的な通信時よりも頻繁に実行

UDP 137,138 (NetBIOS) NetBIOS Name Service の名前解決の通信が頻繁に発生

TCP 25 (SMTP) 短時間に多数の異なるメールサーバへメールを送信

TCP 443 (HTTPS)

TCP 80,8080,8082 (HTTP) POST 通信のみを繰り返し実行

D3M の C&C 通信データの分析結果から判明したその他の特徴, およびマルウェアとの関係の推測結果は以下のとおりである.

1. TCP,UDP の High ポートをスキャンしている. マルウェアが攻撃フェーズに遷移しポートスキャンを行っている
2. TCP,UDP の特定の High ポートを使用した通信が発生している. マルウェアが C&C サーバと C&C 通信, もしくは詐取した情報を送信している
3. HTTP,HTTPS を用いて同一通信先へ同じほぼ内容の通信を繰り返し発生している. マルウェアによる C&C 通信である. C&C サーバが変化する場合がある
4. 数種類のポートを使用した通信が繰り返し発生している. DNS,HTTPS,SMTP がセットになった通信は, マルウェアが攻撃フェーズに遷移しスパムメールの送信を行っている.SMTP の接続先も変更している
5. HTTP のうち, TCP 通信のコネクションは

確立したがその後の通信が失敗している場合がある. マルウェアの配布サーバや C&C サーバが反応せず C&C 通信が失敗している

6. NetBIOS の名前解決の通信が大量に発生している. マルウェアが NetBIOS の名前解決のブロードキャスト通信を行い, 同一ネットワークセグメント内のコンピュータを探索している

4.2 C&C 通信用検知パターンの開発方針

4.1.1 や 4.1.2 では, D3M の C&C 通信データからマルウェアの通信と思われるいくつかの特徴的な通信を抽出できた. これらの特徴的な通信は, 以下のポイントにまとめることができる. ただし, 本システムのように実際のネットワーク上のコンピュータに感染したマルウェアを検知する場合は, セキュリティ対策の状況によってマルウェア通信の挙動が変化する場合を考慮する.

- 4.1.2 の箇条書 1,2,4 から, C&C フェーズよりも, 攻撃フェーズの通信のほうが検知しやすい特徴を持っている
- 4.1.2 の箇条書き 4 から, 複数のプロトコルの通信が相関している
- インターネット境界において Firewall などで不要な Outbound 通信を遮断している場合は, 4.1.2 の箇条書 2 のような C&C 通信は行えない. ただし遮断された通信が再試行される場合がある
- HTTP,HTTPS の Outbound 通信は許可されているため,HTTP,HTTPS を用いた同一通信先へ類似内容を繰り返し送信する C&C 通信が発生する. ユーザ認証のある Proxy サーバが設置されている場合は, 認証を通過できる場合のみ C&C 通信が発生する. ただし類似した正常な通信とマルウェアによる C&C 通信との区別は難しく, 誤検知対策が必要
- インターネット境界において Firewall などで不要な Outbound 通信を遮断している場合は, 4.1.2 の箇条書 3 のような数種類のポートを使用した通信は継続的に行えない. ただし遮断された通信が再試行される場合がある
- 同一の通信先にも関わらず頻繁にアドレス解決の通信が発生するなど, 一般的な通信とはことなる異常な通信が発生する場合がある

以上から, 次の検知パターンの開発方針を決定した. C&C フェーズでは, 異常検知方式を中心に C&C 通信の検知パターンを開発する. NetBIOS や DNS,HTTP,HTTPS の通信など, 正常な通信とマルウェアによる通信との区別が難しい. そのため, マルウェアの種類による通信ポートの違いや通信データの特徴を利用した誤検知対策も検討する. 個々のマルウェアの特徴を利用するため, 定性的な特徴を利用した検知パターンではない. そのため Exploit Kit の設定変更や亜種への変化などの軽微な差異に影響されるおそれがある. 攻撃フェーズは, ポートスキャンや詐取情報の送信, スパムメール送信, DDoS 攻撃など検知しやすい特徴的な通信の検知パターンから開発する.

まず上記の方針に沿って, C&C フェーズと攻撃フェーズのマルウェアによる通信を検知するパターンを作成する. その検知パターンを実環境に適用し, 検知と誤検知のノウハウの蓄積, および検知パターンの改良を経て, 最終的には定性的な特徴を用いた汎用的な検知パターンの作成を目指す.

5 まとめ

本稿では, まず本システムの実環境における検知実績および MWS2014 データセットに対する検知率の評価結果を示した. MWS データセットの D3M に対する検知率の評価では, 平均 71.7% の検知率であった. 2011 年の検知率は 55.2%と低いが, 本システムは 2012 年から開発を開始しており, それ以前のマルウェアの検知パターンの開発は優先度が低いため, これを許容する. 本システムは, 実際に報道された DBD 攻撃が挿入された Web 改ざんインシデントをリアルタイムで検知でき, 定性的な特徴を用いた DBD 攻撃検知方式の有効性が実証された. ただし, 適切に

セキュリティパッチが適用されて脆弱性が対策されているコンピュータ環境では, DBD 攻撃が挿入された Web ページを閲覧しても DBD 攻撃が途中で失敗してしまい, 本システムでは検知することができなかった. DBD 攻撃が途中で失敗した場合はマルウェアに感染しておらず, リスクが低いため, 検知漏れを許容してもよいと判断する.

つぎに検知範囲の拡大に向けて, C&C フェーズと攻撃フェーズにおけるマルウェア通信の検知方式を検討した. 定性的な特徴が現れにくい DBD 攻撃や基本メカニズムが大きく変化した DBD 攻撃, ユーザが操作してマルウェアをダウンロードしてインストールする場合は, 本システムの DBD 攻撃検知方式ではマルウェアを検知できない. そこでコンピュータがマルウェアに感染したあとの C&C フェーズと攻撃フェーズのマルウェア通信を検知できる検知パターンを検討した. D3M の C&C 通信データを分析し, その結果にもとづいて C&C フェーズと攻撃フェーズのマルウェア通信の検知パターンの開発方針を決定した. 今後は, 上記の開発方針に沿って検知パターンを作成して実環境に適用し, 検知パターンの改良を進める. これにより本システムの検知率を確保しつつ, 検知範囲の拡大をめざす.

5.1 今後の課題

D3M の 2014 年の DBD 攻撃の通信データ 8 個を検知できなかった問題には, 今後,IE や Flash, Silverlight の脆弱性を悪用した DBD 攻撃の検知パターンを追加開発して解決したい.

また本システムを実環境で運用したことにより, 広告配信ネットワークを用いた Web 待ち伏せ攻撃を検知することができた. 広告配信ネットワークを用いた Web 待ち伏せ攻撃であっても DBD 攻撃を用いるため, 本システムで検知可能であった.

ただし, DBD 攻撃が仕込まれた広告の配信は動的な URL を用いており, 目視による追跡に手間がかかる. さらに広告は確率的に配信される場合もあるため, DBD 攻撃が仕込まれた Web ページを再度表示させることが難しく,DBD 攻撃が仕込まれた Web ページを特定して分析できない場合が多い. 攻撃時刻から追跡完了までに時間かかる場合も, おとりサイトやリレーサイトが消滅するよりも早く配信が終了するため, 攻撃の追跡や再現が困難になる. 本システムにおける攻撃受信から検知までのタイムラグの縮小と広告配信ネットワークを用いた Web 待ち伏せ攻撃の効率的な解析方法の開発は, 今後の課題である.

参考文献

[1] 大谷 尚通, 北野 美紗, 重田 真義, 企業内ネットワークの通信ログを用いたサイバー攻撃検知システム,MWS 2013

[2] 北野 美紗, 大谷 尚通, 宮本 久仁男,Drive-by-Download 攻撃における通信の定性的特徴とその遷移を捉えた検知方式,MWS 2013

[3] Chris Larsen, マルネットのトラッキングと可視化, ガートナー セキュリティ＆リスク・マネジメント サミット 2012

[4] Cisco,Cisco 2014 Midyear Security Report, http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf

[5] 秋山満昭, 神薗雅紀, 松木隆宏, 畑田充弘, ”マルウェア対策のための研究用データセット〜MWS Datasets 2014〜”, 情報処理学会 研究報告コンピュータセキュリティ（CSEC） Vol. 2014-CSEC-66, No. 19, pp. 1 - 7, 2014.