3Z-5

マルチ環境解析を利用した悪性Webサイトアクセス時のリスク分析支援

義則 隆之† 神薗 雅紀‡,†† 廣友 雅徳‡‡ 毛利 公美††† 白石 善明‡‡‡

†名古屋工業大学 ‡情報通信研究機構 ††(株)セキュアブレイン ‡‡佐賀大学 †††岐阜大学 ‡‡‡神戸大学

1. はじめに

マルウェアによるセキュリティ被害が社会問題化している．組織内の端末がマルウェアに感染すると，組織の情報資産が外部に漏えいするなどの被害を受ける．マルウェアの感染方法は，以前はOSの脆弱性が利用される傾向にあったが，OSが強固になったことでアプリケーションの脆弱性が利用される傾向となっている．中でも，悪性なWebサイトへのアクセスを契機として，Webブラウザやプラグインの脆弱性を悪用し，強制的にマルウェアをダウンロードさせるDrive-by Download攻撃が主流となっており，Drive-by Download攻撃への対策及び攻撃の解析技術の研究開発が盛んに行われている．クライアントによる悪性Webサイトへのアクセスを防ぐために，クライアント側で悪性URLのブラックリストへのアクセスを制御する技術[1][2]がある．Webブラウザが悪性Webサイトを表示させる前に検知することで，リアルタイムでの防御が可能である．しかし，多くの場合，攻撃の起点となるWebサイトは攻撃者によって改ざんされた正規サイトであること，悪性WebサイトのURLは短期間で別のURLに遷移すること[3]，未知の脆弱性が悪用されるケースが存在することから，未然の防御には限界がある．そこで，悪性Webサイトによりある組織内で発生したインシデントに対して，組織の保有するPC環境で当該Webサイトにアクセスするとどのに対してリダイレクトされるか，そのリダイレクト先でどのような攻撃ファイルが実行されるかといった，リスクを分析することが重要となる．

Webサイトを自動的に動的解析した結果を利用者に提供するサービス[4][5][6]がインターネット上で提供されている．しかし，悪性Webサイトは端末等の環境を識別して挙動を変えるため，これらのWebサイト解析サービスではリスク分析に必要な情報が十分に得られない．そこで，端末の環境を変更して，悪性Webサイトを解析する手法がLuら[7]，Wangら[8]により提案されており，我々も同様の提案をしている[9]．しかし，その解析結果を悪性Webサイトによる被害を受けた組織のリスクヘッジにどのように結び付けてどのように利用できるかを示しているものは著者らの知る限り存在しない．

本稿では，端末等の環境を識別し挙動を変化させる悪性Webサイトの情報を分析するマルチ環境解析と，その結果を利用したリスクの分析支援について述べる．マルチ環境解析を実装し，実際に悪性Webサイトをマルチ環境で解析した結果を利用してリスク分析を行い，組織のリスクヘッジにどのように利用できるかを考察する．

2. 悪性Webサイトの特徴

悪性Webサイトは主にExploitKitと呼ばれるソフトウェアで作成され，攻撃者はWebサーバにExploitKitをインストールすることで，悪性Webサイトの作成が可能となる．ExploitKitによって作成された悪性Webサイトによる攻撃の全体像の一例を図1に示す．悪性Webサイトは Webブラウザ（Internet Explorer，Firefoxなど）やプラグイン（Flash Player，PDFやJavaなど）の脆弱性に対する攻撃を行い，攻撃が成功すると端末にマルウェアをダウンロードさせ，実行させる[10]．ExploitKitで作成された悪性Webサイトは攻撃の成功率を高めるために，複数のアプリケーションのバージョンの脆弱性に対する攻撃を用意しており，端末のWebブラウザやプラグインの種類やバージョンを識別してその脆弱性に応じた攻撃を実行する．また，解析者による検知を回避するために，端末等の環境に標的とするバージョンのアプリケーションが存在しない場合は，害のないWebサイトにリダイレクトさせる，アクセスした端末のIPアドレスを記録し，同一IPアドレス

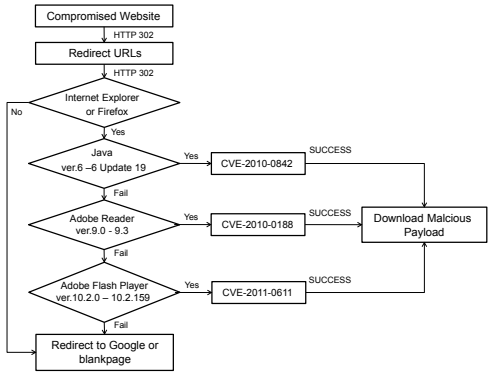

図1 悪性Webサイトによる攻撃の全体像の例

からのアクセスを制御するといった機能を持つ[11][12]．このような特徴を有する悪性Webサイトを組織の保有しているPCやネットワークの実態に即して解析できれば，悪性Webサイトにより組織にもたらされるリスクを分析できると期待される．

3. マルチ環境解析を利用したリスク分析支援

3.1 マルチ環境解析

端末等の環境を識別し挙動を変化させる悪性 Web サイトにアクセスするリスクを分析するために，端末の環境を変更して悪性Webサイトを分析するマルチ環境解析を行う．本稿で行うマルチ環境解析は，処理内容としてはWebクライアント型ハニーポットである．Webクライアント型ハニーポットとは，Webサイトに能動的にアクセスし悪性Webサイトの情報を収集する技術である．それには，脆弱性に対する攻撃を実行できる仕組みで当該 Web サイトを巡回しなければならないため，実際のアプリケーションを利用する高対話型ハニーポットを利用する．マルチ環境解析の構成は，仮想端末上に種類やバージョンの異なるブラウザやプラグインを導入した環境を構築したものである．また，IPアドレスによる制御を回避するため，悪性Webサイトにアクセスする度に異なるIPアドレスを設定する．マルチ環境解析により，既存のサービスと比較し，各環境でアクセスした際のリダイレクト先 Web サイトや当該 Web サイトで実行される攻撃などの情報が得られる．

3.2 マルチ環境解析を利用したリスク分析手法

単にマルチ環境で URL 情報やダウンロードされるコンテンツを収集しただけでは，それが本当に攻撃に利用されたものなのか，組織にどのようなリスクがもたらされているのかを判断することができない．そのために組織にもたらされるリスクは，URL情報やコンテンツ情報から分析することになる．リスクの分析方法の例を以下に示す．

URL 情報の分析

マルチ環境解析によって得られたリダイレクト URL を，組織内の端末のログや組織のファイアウォールのログと突合することで，被害がどの程度進行してしまったのか分析する．また，組織が認識していなかった悪性 Web サイトにアクセスした可能性なども分析する．

悪性 Web サイトのコンテンツファイルの解析

難読化された JavaScript を解析する技術[13][14]やサービス[15][16]等を利用し，攻撃に利用された JavaScript からリダイレクト先 URL や悪用する脆弱性に関する情報を取得する．

最終的にダウンロードされるマルウェアの解析

マルウェアをサンドボックス内で動的に解析し，アクセスするファイルやレジストリの情報を取得する．また，通信挙動を捕捉することで，マルウェアの通信や情報漏洩先を特定する．

4. マルチ環境解析の実装と分析事例

3.1 で述べたマルチ環境解析を表 1 に示したソフトウェア及び

Supporting Risk Assessment of Accessing Malicious Web Sites with Multi-Environment Analysis

† Takayuki YOSHINORI・Nagoya Institute of Technology

‡,†† Masaki KAMIZONO・NICT，Secure Brain Corp.

‡‡ Masanori HIROTOMO・Saga University

††† Masami MOHRI・Gifu University

‡‡‡ Yoshiaki SHIRAISHI・Kobe University

解析環境で実装した．マルチ環境解析で悪性 Web サイトを分析するにあたり，攻撃の成功率を高めるために OS，各種 Web ブラウザやプラグインにはセキュリティパッチを一切適用しないものとした．

続いて，マルチ環境解析でブラックリスト Malware Domain List[17]に掲載されている悪性 Web サイトに実際にアクセスし，その結果を 3.2 で述べたように分析する．分析手順は，まず解析環境 1-3 でそれぞれ悪性 Web サイトにアクセスし，その通信内容を Wireshark[18]を使って保存する．そして，保存した通信データから当該 Web サイトが組織にもたらすリスクを分析する．

以下では，www.******.com.br/wp-enter.php?xIKVC3UCMRU05WH6C をマルチ環境解析し，その結果を分析した事例を示す．その分析結果を図 2 に示す．図 2 を見ても分かる通り，アクセスした Web ブラウザによって捕捉できた悪性 Web サイトの挙動が異なることが分かる．Internet Explorer，Firefox と Google Chrome でアクセスした場合とでリダイレクトされる Web サイトが異なり，Google Chrome は無害な Web サイト（me******.com）にリダイレクトされた．Internet Explorer と Firefox は同一の Web サイト（(A)http:// 78.**.**.**/closest/i9jfuhioejskveohnuojfir.php）にリダイレクトされた後，Firefox は http://78.**.**.**/closest//Main にリダイレクトされ，当該 Web ページは 404 Not Found であった．Internet Explorer では(B)http://78.**.**.**/closest/i9jfuhioejskveohnuojfir.php?1aa10bb101bb00=b11.....，(C) http://78.**.**.**/closest/i9jfuhioejskveohnuojfir.php?bbbbb00abab0bab1a1a=73.....へのリダイレクトを経て，(D) http://db******.com/，http://ca******.com/などの多数の URL 群にリダイレクトしていることが分かった．

次に(B)-(D)を解析する．(B)では http ヘッダの content-type から Java アーカイブファイルをダウンロードしていることが分かった．当該 Java ファイルを通信データから再構築し，VirusTotal[19]で分析したところ，複数のウイルス対策ソフトで悪性のものと判定され，その検知結果に CVE 番号（CVE-2013-0422）が明記されていた．CVE 番号を JVNDB（脆弱性対策情報データベース）と照合したところ，Java の脆弱性であることが判明した．続いて(C)との通信内容（ペイロード）から，実行可能な EXE ファイルをダウンロードしていることが分かった．当該 EXE ファイルを通信データから再構築し，ThreatExpert[20]で分析したところ，当該 EXE ファイルが多数の URL にアクセスするものであると分かった．得られた URL は(D)と合致しており，当該 EXE ファイルが(D)にアクセスを試みていることが判明した．この結果から，CVE-2013-0422 が存在する Java アプリケーションを搭載した InternetExplorer で www.******.com.br/wp-enter.php?xIKVC3UCMRU05WH6C にアクセスすると，Java の脆弱性が悪用されマルウェアに感染し，当該マルウェアが多数の URL にアクセスを試みることが分かった．

これらの結果から，組織にもたらされるリスクについて次のように考察した．CVE-2013-0422 に対する攻撃が成功したことから，組織内の端末にソフトウェアのアップデートを適切に実施できていないものがある，もしくは組織による端末管理に不備があると推測される．また，組織のプロキシサーバや端末内に保存された通信ログと(B)-(D)の URL を照合することで，今まで把握していなかった端末が実は攻撃を受けていたりマルウェアに感染していたといった被害状況を特定することが可能となる．(D)は不特定多数のドメインで構成され，ダウンロードされたマルウェアは(D)に通信を試みており，通信内容が判読不能な文字列であることから，動的に生成したドメインに，端末から窃取した情報を暗号化して持ち出しているのではないかと推測される．このことから，当該マルウェアの挙動をより正確に分析することで窃取された情報を特定できると考えられる．今回はブラウザのみを変更した実験を行ったが，組織内の端末環境に応じてプラグインやそのバージョンを変更したマルチ環境解析を行えば，組織にもたらされるリスクをより精緻に分析することができると期待される．

5. まとめ

本稿では端末等の環境により挙動を変える悪性 Web サイトのマルチ環境解析により，当該 Web サイトが組織にもたらすリスクの分析支援を提案した．マルチ環境解析を実装し，実在する悪性 Web サイトを解析した結果を利用して，当該 Web サイトが組織にもたらすリスクを分析する方法を示した．

表 1　実装に利用したソフトウェア及び評価用解析環境

仮想マシン	VirtualBox 4.3.6 r91406
ゲストOS	Windows XP SP2
ホストOS	Debian 6.0.8
Webブラウザ	解析環境1：Internet Explorer 6 解析環境2：Firefox 0.8 解析環境3：Google Chrome 1.0.154
プラグイン	Java 5.0 Update 22 Adobe Reader 4.0 Adobe Flash Player 6 QuickTime 5.0 Shockwave Player 7.0.3

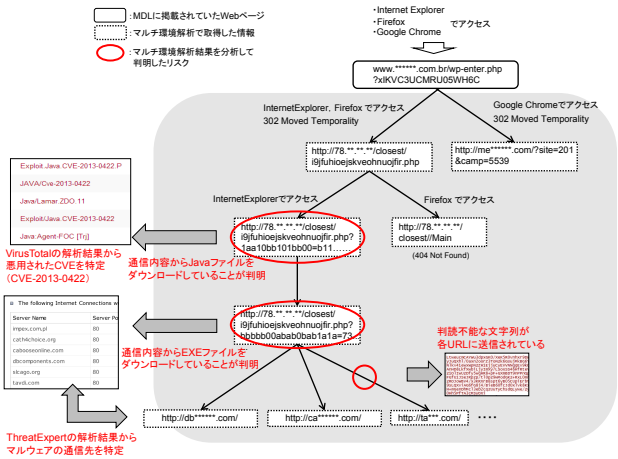

図 2　www.******.com.br の分析結果

参考文献

[1] Google: Google Safe Browsing API, available from< https://developers.google.com/safe-browsing/?hl=ja> (accessed 2014-01-11).
[2] Microsoft: SmartScreen Filter, available from< http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/smartscreen-filter> (accessed 2014-01-11).
[3] Provos, N., Mavrommatis, P., Rajab, M. A. and Monrose, F.: All Your iFRAMEs Point to Us, Proc. 17th USENIX Security Symposium, pp.1-15 (2008).
[4] Aguse: available from< www.aguse.jp/> (accessed 2014-01-11).
[5] Anubis: available from< http://anubis.iseclab.org/ > (accessed 2014-01-11).
[6] gred: available from< check.gred.jp/> (accessed 2014-01-11).
[7] Lu, L., Yegneswaran,V., Porras, P., Lee, W.: BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, Proc. the 17th ACM Conference(ACM CCS'2010), pp.1-11(2010).
[8] Wang, Y.M., Beck, D., Jiang, X., Roussev, R., Verbowski, C., Chen, S. and King, S.: Automated Web Patrol with Strider Honeymonkeys, Proc. Network and Distributed Systems Security Symposium, pp.35-49(2006).
[9] 義則隆之，神薗雅紀，廣友雅徳，毛利公美，白石善明：挙動を変える悪性 Web サイトのマルチ環境解析，コンピュータセキュリティシンポジウム 2013（CSS2013），2B2-2（2013）．
[10] Grier, C., Ballard, L., Caballero, J., Chachra, N., Dietrich, C., Levchenko, K., Mavrommatis, P., McCoy, D., Nappa, A., Pitsillidis, A., Provos, N., Rafique, M.Z., Rajab, M.A., Rossow, C., Thomas, K., Paxson, V., Savage, S. and Voelker, G.: Manufacturing Compromise: The Emergence of Exploit-as-a-Service, Proc. the 19th ACM Conference on Computer and Communications Security, pp.821-832(2012).
[11] Dell SonicWALL: Blackhole Exploit Kit: Rise & Evolution, available from< http://software.sonicwall.com/gav/Blackhole%20Exploit%20Kit%20-%20Rise%20&%20Evolution.pdf>(accessed 2014-01-11).
[12] 松木隆宏，新井悠，寺田真敏，土居範久：マッシュアップによる Web マルウェアの実態調査，情報処理学会論文誌，Vol.52，No.9，pp.2748-2760（2011）．
[13] 神薗雅紀，西田雅太，小島恵美，星澤裕二：抽象構文解析木による不正な JavaScript の特徴点抽出手法の提案，情報処理学会論文誌，Vol.54，No.1，pp.349-356（2013）．
[14] 佐藤両，義則隆之，松井拓也，廣友雅徳，毛利公美，神薗雅紀，白石善明：Windows API フックの通信監視による攻撃コードを含む PDF ファイルの検知，全国大会講演論文集 2013，No.1，pp.551-553（2013）．
[15] The University of California: Wepawet, available from< http://wepawet.iseclab.org/> (accessed 2014-01-11).
[16] Google Project Hosting: Jsunpack, available from< http://jsunpack.jeek.org/> (accessed 2014-01-11).
[17] Malware Domain List: available from< http://www.malwaredomainlist.com/>(accessed 2014-01-11).
[18] Riverbed Technology: Wireshark, available from<http://www.wireshark.org/>(accessed 2014-01-11).
[19] VirusTotal: VirusTotal, available from< https://www.virustotal.com>(accessed 2014-01-11).
[20] ThreatExpert: ThreatExpert, available from< http://www.threatexpert.com/>(accessed 2014-01-11).