Vol.2014-CSEC-67 No.6
2014/12/5

プロキシサーバを用いた水飲み場型攻撃検出手法

金 東徳[†1]　星 徹[†2]　手塚 悟[†2]

近年，水飲み場型攻撃という攻撃手法が確認された．それは，攻撃者が標的とするユーザの頻繁にアクセスする Web サイトを調査し，その Web サイトを改ざんして，標的ユーザがアクセスしてきた場合のみ，攻撃者が用意したマルウェア配布サイトへリダイレクトするようにし，マルウェアをダウンロードさせ，実行させるという攻撃手法である．対策としてウイルス対策ソフトを導入するという方法があるが，必ずしもマルウェアを検出できるわけではなく，完全とは言えない．そこで，本稿では水飲み場型攻撃サイトは，標的ユーザがアクセスしたときのみマルウェア配布サイトにリダイレクトするという特徴に着目．この特徴を検出するプロキシサーバを用いた水飲み場型攻撃検出手法を提案する．ユーザが Web ページにアクセスすると同時に，異なる IP アドレスを持つ多数のプロキシサーバを用いて同じサイトにアクセスし，リダイレクトの有無を比較することにより水飲み場型攻撃を検出し対策する．

A Detection Method against Watering Hole Attack Using the Proxy Server

TOUTOKU KIN[†1]　TOHRU HOSHI[†2]
SATORU TEZUKA[†2]

Recently, cyber attack called the watering hole attack has been found.The attacker is looking for a Web site that target users frequently access, and consequently finds it and tamper with it. When the target user has accessed the Web site, his/her access is redirected to the malware distribution site, then the access is forced to download the malware.We pay attention to the characteristic that the redirection to the malware distribution site occurs at the time when the target user accesses the watering hole attack site. We propose a watering hole detection method using proxy servers to detect this feature. When a user accesses a Web page, to access the same site from a number of proxy servers having a different IP address at the same time, and to compare the presence of redirection.

1. はじめに

水飲み場型攻撃とは Web を介した特定の組織や個人を狙う標的型攻撃の手法の 1 つである．水飲み場型攻撃は 2012 年に EMC コーポレーションの RSA FirstWatch チームにより観測された攻撃手法を，ウォーターホール(Water Holing)と命名し発表されたことで一般に認知された攻撃手法である[1]．この事例では攻撃者が標的とするユーザのアクセスする可能性のある Web サイトを選んだ上で Web サイトを改ざんし，攻撃者の用意した Web サイトに誘導する仕掛けを施す．誘導後の Web サイトではアクセス元の PC 環境をチェックし，攻撃者の意図する PC 環境であれば脆弱性を利用しブラウザを乗っ取り，マルウェアをインストールおよび実行する．

前述の事例では攻撃者の意図する PC 環境であればアクセスしてきたユーザ全員にマルウェアを感染させる．そのため攻撃者の標的でないユーザからのアクセスでもマルウェア感染させてしまい攻撃を発見される可能性が高くなる．2013 年に日本でこのような問題を解決する水飲み場型攻撃が観測された[2]．前述の事例のような手法に加え，Web アクセス者の IP アドレスを識別することにより，標的とする IP アドレスからのアクセス時のみマルウェア感染させるという手法を用いていた．こうすることによりマルウェアをダウンロードされる機会を減らし発見される可能性を低くできる．また，この事例では知の脆弱性を用いた攻撃(以下 0 デイ攻撃)を用いて確実にマルウェア感染させるようにしていた．

関連する対策技術について述べる．既存の Web 感染型マルウェアの対策としてユーザ側ではマルウェア対策ソフトや，リダイレクトを防止するブラウザのプラグインを導入するなどの方法がある．しかし，水飲み場型攻撃は 0 デイ攻撃を用いる場合があるため完全に防げるわけではない．Web 管理者側では Web 改ざん防止サービスなどを導入することで改ざん防止することができるが，全ての Web サイトに導入することはコスト的に困難である．Web サイトを巡回しマルウェアを検出するものに Web クライアント型ハニーポッド[3]というものがある．これは実際の Web サイトを巡回することで Web サイトにマルウェアが感染していないかを検出するものである．しかし，水飲み場型攻撃はアクセス元の IP アドレスを識別し，マルウェア感染させるかを決定するため，標的でない Web クライアント型ハニーポッドからのアクセスでは検出できない．

本研究では 2013 年に日本で観測された Web アクセス者の PC 環境および，IP アドレスを識別するタイプの水飲み

†1 東京工科大学大学院　バイオ・情報メディア研究科
Tokyo University of Technology
†2 東京工科大学　コンピュータサイエンス学部
Tokyo University of Technology

場攻撃を研究の対象とする．また，水飲み場型攻撃の特徴に着目し，この水飲み場型攻撃を検出し対策する手法を提案する．

本稿の構成は以下の通りである．まず 2 章で水飲み場型攻撃について説明する．3 章で既存技術を用いて水飲み場型攻撃を検出する際の問題点を述べる．4 章で提案システムについて述べる．

2. 水飲み場型攻撃

2.1 概要

水飲み場型攻撃とは，特定の組織や個人を狙う標的型攻撃の手法の 1 つである．サバンナなどで肉食獣が池の周囲などで待ち伏せし，水を飲みに現れた草食動物を狙い撃ちにする様子になぞらえて命名された．英語では「Watering hole attack または water holing」と表記され，日本語では「水飲み場型攻撃」または「たまり場型攻撃」と訳される[4]．また，Web サイトで待ち伏せするということで「Web 待ち伏せ攻撃」と呼ばれることもある[5]．

水飲み場型攻撃の流れについて説明する．攻撃者の標的がアクセスする可能性のある Web サイトを標的の企業や業種，SNS などを用いて推測または，実際に Web サーバに侵入し標的がアクセスしているかを観測することで調べる．その後，攻撃者が調べた標的がよくアクセスする Web サイトを改ざんし，アクセスした利用者にマルウェアを感染させる仕掛けを施す．改ざんサイトにアクセスしたユーザはマルウェア配布サイトへ誘導される．マルウェア配布サイトではアクセス元のブラウザや環境を調べ，脆弱性を突く攻撃ができる環境の場合のみ攻撃コードの実行し，マルウェアを感染させる．

近年ではこの手法に加え，さらに標的のみにマルウェア感染させるため，標的以外の IP アドレスからのアクセスでは通常の Web レスポンスを返すが，標的の IP アドレスからのアクセスのみマルウェアを感染させるという手法が登場した[2]．感染させる対象を絞ることでセキュリティベンダーなどからの発見を遅らせることができる．

2.2 本研究が対象とする水飲み場型攻撃

本研究で対象とする 2.1 章で述べた攻撃者の標的とする企業や個人がアクセスする可能性のある Web サイトを改ざんし，標的とする PC 環境や IP アドレスからのアクセスのみ攻撃を仕掛ける水飲み場型攻撃の詳しい流れを説明する．攻撃フローを図 1 に示す．

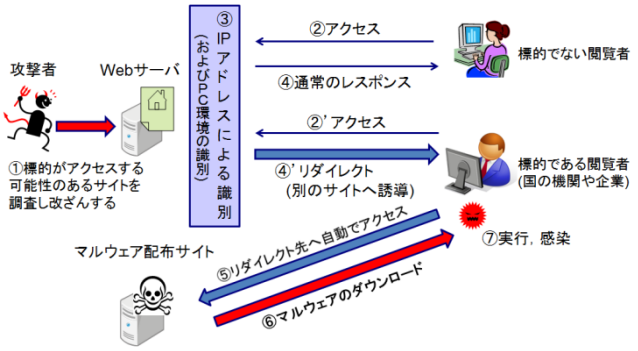

図 1　水飲み場攻撃のフロー

Figure 1　Flow of Watering Hole Attack.

まず，(①)攻撃者は標的が今後アクセスする可能性のある Web サイトがどれかを調べる．調べる方法は標的とする企業や個人，SNS の情報からアクセスしそうな Web サイトを推測したり，実際に Web サイトに侵入し，アクセス者を観測したりといった方法で調べていると考えられている[2]．そして調べた Web サイトを改ざんする．改ざん内容は，標的とする IP アドレス，OS，ブラウザ，プラグインからのアクセス時のみ脆弱性を突く攻撃および，マルウェア配布サイトにアクセスさせ，マルウェア感染させる仕掛けを施す．

標的でない閲覧者がアクセス(②)しても IP アドレスによる識別(および PC 環境の調査)をされ(③)，通常のレスポンスが返される(④)．

しかし，標的である閲覧者がアクセスしてきた場合(②’)，Web サイトは標的からのアクセスであると認識し(③)，別のサイトへリダイレクト(別のサイトへ誘導する)命令(④’)を返す．リダイレクト命令を受け取ったブラウザは⑤でリダイレクト先のマルウェア配布サイトへ自動的にアクセスする．そして⑥でマルウェアのダウンロードが開始され⑦で実行，感染する．

3. 既存の Web 感染型マルウェア対策技術を水飲み場型攻撃に適用する際の問題点

水飲み場型攻撃でない Web を介したマルウェア感染への対策技術である第 3 者機関による Web サイト巡回によるマルウェアの検査技術とユーザ側の対策について述べ，水飲み場型攻撃の対策として適用させる際の問題点を挙げる．また，Web 感染型マルウェアの発見が遅れた際の問題点を述べる．

3.1 第 3 者機関による Web サイト巡回による検査

(1)　Web クライアント型ハニーポッド

Web サイトを検査しマルウェアに感染していないかを検査するものに Web クライアント型ハニーポッドがある．Web クライアント型ハニーポッドとは実際に多数の Web ページにアクセスし，ファイルの解析を行うことでマルウェアを配布するサイトであるかを判断する[3]．Web クライアント型ハニーポッドは大きく 2 種類に分けられる．OS や

アプリケーションをエミュレートして構成される低対話型と，実際の OS やブラウザによって構成される高対話型の 2 種類に分けられる．低対話型より高対話型の方がより多くの情報を得られるとされている．

水飲み場型攻撃を Web クライアント型ハニーポッドで検出する際の問題点として，水飲み場型攻撃が仕掛けられている Web サイトにアクセスしても標的とする IP アドレスからのアクセスではないため通常のレスポンスが帰ってくるため検出することができない．

(2) Web クライアント型ハニーポッドの派生

文献[6]では，特定の PC 環境からのアクセスのみマルウェアをダウンロードさせるものがある．そのような Web サイトは単一の環境からのアクセスではマルウェアを感染させてこない場合がある．そこで多数のブラウザやプラグイン環境を用意し，アクセスすることで解析するという手法が提案されている．

問題点として環境によって攻撃するかしないかを決定するタイプの攻撃を検出することはできるが，標的の IP アドレスを識別する水飲み場型攻撃を検出することはできない．

3.2 ユーザ側の対策

(1) マルウェア対策ソフト

マルウェア対策として導入される．パターンマッチングやプログラムの振る舞いなどからマルウェアを検出する．問題点として新型のマルウェアや未知の脆弱性を用いる攻撃などは検出できない場合がある．水飲み場型攻撃は確実にマルウェア感染させるために 0 デイ攻撃を用いる可能性が高いと考えられるため完璧な対策とはいえない．

(2) ブラウザでの対策

ブラウザプのラグインを用いてリダイレクトを防止することにより，リダイレクトさせた後にマルウェア配布サイトへアクセスさせるタイプの Web 感染型マルウェアの感染を防止することができる．

しかし，1 章で述べた事例[2]ではブラウザが行う通常の URL リダイレクトではなく，ブラウザの脆弱性を突き，任意のコードを実行することによりマルウェア配布サイトへアクセスさせていた[7]．そのためリダイレクトを防止するためのプラグインを導入していたとしても防げない場合がある．

3.3 Web 感染型マルウェアの発見が遅れた際の問題

Web 改ざんによるマルウェア改ざんは発見が遅れると Web 閲覧によるマルウェア感染が拡大していく可能性がある．よって水飲み場型攻撃についても早期発見し感染拡大による被害を抑える必要がある．IP アドレスで対象を識別するタイプの水飲み場型攻撃は対象を絞っているため実際に被害に合うユーザは少ないと考えられる．しかし，複数の標的を指定している場合は，早期に発見することで被害者を少なくすることができる．また，改ざんサイトを用いてさらなる攻撃のために使われたりする可能性があるので早期発見する必要がある．

3.4 水飲み場攻撃を検出する際の問題点のまとめ

3.1 章に挙げるように IP アドレスで標的を識別するタイプの水飲み場型攻撃を検出ことは難しい．3.2 章に挙げるように 0 デイ攻撃を検出し，対応するのは難しい．3.3 章に挙げるように水飲み場型攻撃は早期発見する必要がある．以上に挙げた問題点を 3 つの課題として以下にまとめる．

課題(1) アクセス元の IP アドレスを識別することにより，標的からのアクセスのみマルウェア感染させる

課題(2) 0 デイ攻撃を用いられると検出が困難である

課題(3) 水飲み場型攻撃による被害者を最小限にするためには早期発見する必要がある

本研究ではこの 3 つの課題を解決し，水飲み場型攻撃を検出する手法を提案する．

4. 提案内容

4.1 提案

3.4 章で挙げた 3 つの課題に対する解決策をそれぞれに対して提案する．

課題(1)に対しては，標的ユーザからのアクセスのみ挙動が変わるということを利用すれば水飲み場型攻撃を検出できると考えた．具体的には，標的の IP アドレスからのアクセス時のみリダイレクトし，標的以外の IP アドレスではリダイレクトしない．Web アクセス時にこの挙動を観測することができれば水飲み場型攻撃が仕掛けられているとすることができる．

これを利用し，特定の組織に対する水飲み場攻撃を検出する方法を述べる．標的とされているかを調べたい IP アドレスと比較のための異なる IP アドレスを用意する．標的とされているかを調べたい IP アドレスから Web アクセスする場合に，異なる IP アドレスからもアクセスする．アクセス後のリダイレクトの有無を比較し，標的とされているかを調べたい IP アドレスからのアクセス時のみリダイレクトした場合に，水飲み場型攻撃が仕掛けられているとする．

また，PC 環境により Web サイトの挙動が変わる可能性があるので，同じ環境で同時にアクセスし，IP アドレスの違いだけでリダイレクトの有無を比較できるようにする．

課題(2)対しては，0 デイ攻撃を用いられた場合，マルウェア対策ソフトでも検出できない場合がある．そこで課題(1)の提案方法で水飲み場型攻撃を検出した場合，通信を遮断しウイルスの感染を防ぐ．

課題(3)に対しては，攻撃者が水飲み場型攻撃を仕掛ける Web サイトは標的がアクセスする可能性のあるサイトに仕掛けるという点に着目して解決策を講じる．攻撃者が水飲み場型攻撃を仕掛ける Web サイトはランダムの可能性もある．しかし，攻撃者が改ざんする Web サイトを決定する方法の 1 つに実際に Web サーバに侵入し閲覧者を観測して

いる可能性が挙げられている．この場合，攻撃者が水飲み場型攻撃を仕掛ける Web サイトはユーザが一度でもアクセスした Web サイトである可能性がある．そのため，ユーザが一度でもアクセスした Web サイトを調べることで水飲み場型攻撃を早期検出することができるのではないかと考えた．具体的にはユーザの Web サイトのアクセス履歴を収集し，その履歴を課題(1)で提案した手法を用いて Web サイト巡回することで早期検出を目指す．

4.2 提案の実現方法

課題(1)，(2)，(3)の提案に対する具体的な実現方法を述べる．なおプロキシサーバとはインターネットへのアクセスを代行するサーバのことである．

課題(1)に対する提案の実現方法は，自分の組織からのアクセスと同時に，組織外部に設置したプロキシサーバからアクセスする．次に，自分の組織と，組織外部に設置したプロキシサーバの Web ページアクセス時のリダイレクトの有無をリアルタイムに比較する．リダイレクトは通信を観測することにより検出する．ある Web サイトにアクセスした時に続けて別の Web サイトへのアクセスがあった場合リダイレクトとみなす．また，自分の組織からのアクセス時のみリダイレクトした場合，アクセスした Web ページに水飲み場型攻撃が仕掛けられているとする．

課題(2) に対する提案の実現方法は，組織内にプロキシサーバを設置し水飲み場型攻撃検出した場合に Web 通信を遮断する．

課題(3)に対する提案の実現方法は，組織内部にプロキシサーバを設置し，ユーザが Web アクセスする際の履歴を収集するようにし，その履歴から Web サイト巡回することで実現する．巡回するタイミングはユーザが Web サイトにアクセスしていないとき(夜間など)とする．

課題(1)，(2)，(3)に対する提案の実現方法をまとめたシステム図を示す．ユーザが Web アクセスしている時としていない時で動きが異なるので，ユーザアクセス時とサーバ巡回時に分けてシステムを示す．

● ユーザアクセス時

ユーザが Web ページを閲覧している時のシステムの挙動を図 2 に示す．

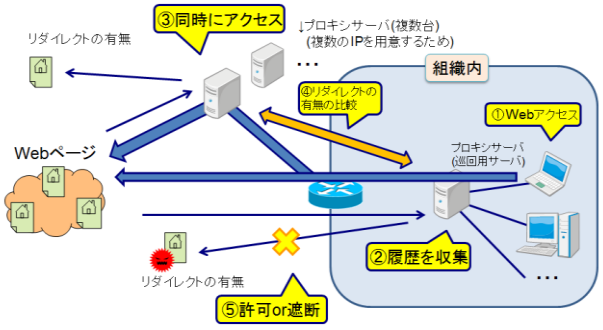

図 2 ユーザアクセス時のフロー

Figure 2 Flow at the time of user access.

図 2 の動作の流れを以下に示す．

① 組織内のユーザによる Web アクセス
② 組織内プロキシサーバが履歴を収集
③ 組織内ユーザの Web アクセスと同時に外部のプロキシサーバから同時にアクセス
④ アクセスしたサイトの組織内部と外部のリダイレクトの有無を比較
⑤ 自分の組織内のアクセスのみリダイレクトした場合，リダイレクト通信を遮断

● サーバ巡回時

ユーザが Web ページを閲覧していない時は，組織内部のサーバで履歴を元にアクセス頻度の高いサイトを重点的に Web ページ巡回することで水飲み場型攻撃がないか調査し，早期発見する．システムの挙動を図 3 に示す．

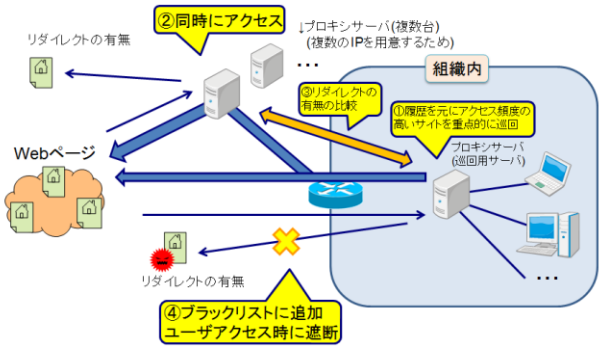

図 3 サーバ巡回時のフロー

Figure 3 Flow at the time of server cyclic.

図 3 の動作の流れを以下に示す．

① 組織内プロキシサーバが履歴を元にアクセス頻度の高いサイトを重点的に巡回
② 組織内プロキシサーバの Web アクセスと同時に外部のプロキシサーバから同時にアクセス
③ アクセスしたサイトの組織内部と外部のリダイレクトの有無を比較
④ 自分の組織内のアクセスのみリダイレクトした場合，プロキシサーバのブラックリストに追加し，ユーザアクセス時に遮断

4.3 提案のまとめ

提案システムにより水飲み場型攻撃を行う Web サイトを検出し，マルウェア感染を防止することができると考えられる．また，履歴を巡回することによりマルウェア感染拡大を抑えることができると考えられる．

課題としては導入した組織に対する水飲み場型攻撃しか検出できないこと，リダイレクトの有無のみで水飲み場型攻撃かどうかを判断しているため誤検出が生じる可能性があること，組織によっては Web アクセス履歴が膨大になり巡回しきれない可能性が考えられる．

5. おわりに

近年観測された攻撃者の標的とするユーザがアクセスする可能性のある Web サイトに，IP アドレスや PC 環境を識別することにより，標的ユーザのみをマルウェア感染させる水飲み場型攻撃を検出し対策する手法を提案した．異なる IP アドレスで同時にアクセスしリダイレクトを比較することにより検出し，通信を遮断することによりマルウェア感染を防ぐ．さらに履歴を巡回することにより早期発見を目指す．

今後は実際に水飲み場型攻撃のサイトを模したサイトを作成し，提案システムで検出できるか検証する．

参考文献

1) RSA FirstWatch Team (2013 年 2 月 20 日). “周到に準備された大規模攻撃 VOHO の詳細分析”
2) “防御困難な「水飲み場型攻撃」登場”．ITpro by 日経コンピュータ．http://itpro.nikkeibp.co.jp/article/COLUMN/20140317/544189/, (2014/11/10 参照)
3) 千葉 大紀, 森 達哉, 後藤 滋樹, "悪性 Web サイト探索のための優先巡回順序の選定法,"コンピュータセキュリティシンポジウム 2012 (CSS2012) 論文集, vol.2012, no.3, pp.805--812, Oct. 2012.
4) ITpro,.“水飲み場型攻撃”．Network キーワード．http://itpro.nikkeibp.co.jp/article/Keyword/20130301/460194/, (2014/11/10 参照)
5) “「水飲み場型攻撃」という直訳問題など考えながら 2013 年を振り返る”．INTERNET Watch．http://internet.watch.impress.co.jp/docs/column/security/20140110_630264.html(2014/11/10 参照)
6) 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
7) “新手の標的型攻撃「水飲み場型攻撃」、被害を最小化する 2 つのアプローチとは”．http://itpro.nikkeibp.co.jp/article/ESI/20140108/528729/?P=2, (2014/11/10 参照)