情報処理学会論文誌 Vol.54 No.9 2167–2176 (Sep. 2013)

アカウント情報の能動的な漏洩による攻撃者の活動観測

秋山 満昭[1,a)] 八木 毅[1,b)] 青木 一史[1,c)] 針生 剛男[1,d)]

受付日 2012年11月30日, 採録日 2013年6月14日

概要：正規 Web サイトを悪用してユーザ端末をマルウェアに感染させる攻撃が脅威となっている．この攻撃では，正規 Web サイトが改竄され，当該サイトにアクセスしたユーザ端末が，マルウェアに感染させるために攻撃者が用意した悪性 Web サイトに誘導される．さらに，マルウェアに感染したユーザ端末から様々なアカウント情報が漏洩し，特に漏洩した FTP アカウント情報を悪用することで当該ユーザの Web サイトコンテンツが攻撃者に改竄される．この際の通信やコンテンツを分析すれば，新たな悪性 Web サイト情報などを攻撃に利用される前に発見して対策を講じることができる．そこで本論文では，おとりの FTP アカウント情報を漏洩させ，監視下にある Web サイト管理システムの改竄を誘発して改竄の特徴を分析するシステムを設計および実装し，観測した情報を分析した結果を報告する．

キーワード：ハニーポット，マルウェア，情報漏洩

Observation for Activity of Adversary by Active Credential-information Leakage

Mitsuaki Akiyama[1,a)] Takeshi Yagi[1,b)] Kazufumi Aoki[1,c)] Takeo Hariu[1,d)]

Received: November 30, 2012, Accepted: June 14, 2013

Abstract: Recently, with the widespread of the web, malware has been spreading via malicious websites. In many cases, the malicious websites are constructed by compromised websites. A user, who accesses the compromised website, is redirected to an attacker's website and is forced to download malware. Additionally, the attacker steals the user's credentials such as FTP account information stored on the victim computer infected by the malware. Furthermore, the attacker tries to compromise the user's website as a website administrator using the stolen FTP account information. To detect and prevent such an attack, it is necessary to reveal its characteristics, especially the method to compromise websites. In this research, we proposed an observation procedure to analyze the activity of account-stealer on our monitored website management system using decoy FTP account information.

Keywords: honeypot, malware, information leakage

1. はじめに

正規 Web サイトの改竄によって悪性 Web サイトへ転送されるインシデントが発生している．改竄された Web サイトは Web コンテンツの一部にリダイレクトコードが挿入される．改竄された Web サイトを閲覧したユーザのアクセスは，ユーザの意図とは無関係に，攻撃者が用意した悪性 Web サイトへ転送される．悪性 Web サイトには，Web ブラウザやプラグインの脆弱性を標的とする攻撃コードが設置されており，ユーザは閲覧するだけでマルウェアに感染する．この際に感染するマルウェアの一部は，感染した端末上の各種アカウント情報を収集して外部へ漏洩させる機能を保有している．このため，感染端末上に Web サイト管理用サーバのアカウント情報が保存されている場合は，その情報が攻撃者に漏洩してしまい，新たな Web サイト改竄を引き起こす（**図 1**）．このように，Web サイト改竄

[1] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, Musashino, Tokyo 180–8585, Japan
[a)] akiyama.mitsuaki@lab.ntt.co.jp
[b)] yagi.takeshi@lab.ntt.co.jp
[c)] aoki.kazufumi@lab.ntt.co.jp
[d)] hariu.takeo@lab.ntt.co.jp

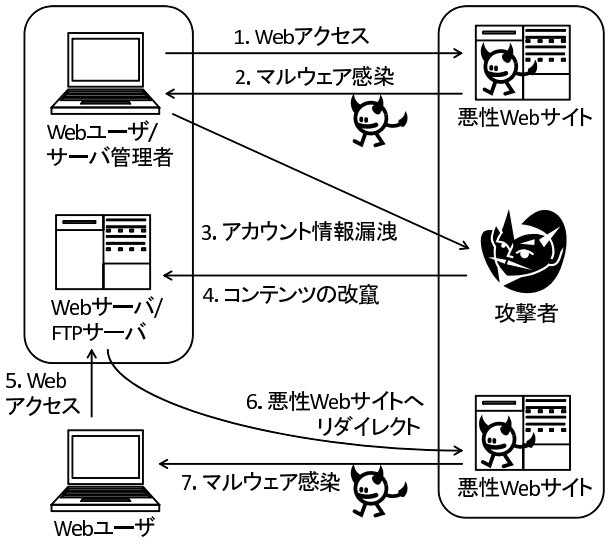

図 1 典型的な攻撃手順
Fig. 1 Typical attack model.

とアカウント情報漏洩を引き起こす一連の攻撃では，Web サイト改竄とマルウェア感染が繰り返されることで，被害が拡大する仕組みになっている．Web 空間に存在する悪性 Web サイトを発見する方法については近年さかんに研究されており [12], [17], [19]，Web クライアントとして Web サイトを検査することで悪性 Web サイトを発見する方法や，検査の際に Web 空間を効率的に探索する方法が提案されている [5]．しかしながら，広大な Web 空間から悪性 Web サイトを迅速に発見することは容易ではない．また，漏洩したアカウント情報が実際に攻撃者にどのように利用され，サーバ上でどのように Web ページが改竄されているかについては，クライアント側から観測することが困難である．そこで本論文では，アカウント情報を能動的に漏洩させることにより，サーバ上での攻撃者の挙動を観測するシステムを提案する．本論文による貢献は以下の 3 点である．

- 漏洩したアカウントの悪用を観測する手法を確立し，おとりサーバに対して攻撃者に改竄を行わせることに成功したこと
- おとりサーバ上で攻撃者の挙動を明らかにしたこと
- 攻撃者の IP アドレスや未知の悪性 Web サイトを迅速かつ効率的に発見できること

2. マルウェア感染手法

ネットワーク経由での攻撃（リモートエクスプロイト攻撃）は Windows のサーバプロセス（DCOM，LSASS，印刷スプーラなど）に存在する脆弱性を標的としたものであり，2000 年代初頭から CodeRed，Blaster など，また 2008 年ごろには Conficker などが悪用し，猛威をふるってきた．このような攻撃に対して，Windows OS の基本機能としてパーソナルファイアウォールが適用されたことや，NAT 環境下でのインターネット利用の普及，不必要な TCP/UDP ポートの遮断などにより，外部ネットワークから直接 Windows OS に対する脆弱性への攻撃が減少してきた．一方で，Web ブラウザやプラグインの脆弱性は 2007 年ごろから大量に発見され続けており，この脆弱性を攻撃してマルウェアに感染させる悪性な Web サイトが多数存在する．この悪性 Web サイトにアクセスした Web クライアントは脆弱性を攻撃された後，制御を奪われ，マルウェアを自動的にダウンロードおよび実行させられる（ドライブバイダウンロード攻撃）．さらに，このドライブバイダウンロード攻撃は，正規の Web 通信プロトコル（HTTP/HTTPS など）にのっとって感染が行われるため，ポートブロックやプロトコル異常による検知ができない．これらの理由によりドライブバイダウンロードがマルウェアの感染方法として主流となっている．

ドライブバイダウンロード攻撃を行う悪性 Web サイトは，スパムメールのリンク URL，SEO（悪性 Web サイト自体を検索エンジンの上位にする），改竄された Web サイトからのリダイレクトなどによって標的の Web クライアントを誘い込んで攻撃を試みる．本論文で対象とするマルウェア感染は，ドライブバイダウンロード攻撃と一般 Web サイト改竄による悪性サイトへの誘導を組み合わせたものである．脆弱な Web ブラウザやプラグインを使用しているユーザは，攻撃者が用意した改竄コンテンツを閲覧した際に，攻撃コードやマルウェアが配置された悪性 Web サイトに誘導され，マルウェアに感染する．このように連鎖的にマルウェア感染と悪性 Web サイトへの誘導が発生する．

3. 事前調査

情報漏洩を行うマルウェアが対象とするアプリケーションを特定するため，マルウェアを実際に動作させることによりファイルアクセスやレジストリアクセスを観測した．マルウェアは公開のブラックリスト（malwaredomainlist.com [11]）から収集したものである．その結果，十数種類の FTP クライアントアプリケーションに関連するレジストリや設定ファイルにアクセスするマルウェアが存在することを確認した．これらのレジストリや設定ファイルには FTP のアカウント情報（アカウント名，パスワード，サーバの IP アドレス，サーバのドメイン名）が平文もしくは暗号化されて保存されている．マルウェアは取得したアカウント情報を攻撃者に送信する．マルウェアの通信の中で，平文や Base64 によるエンコードもしくは暗号化されたペイロードが HTTP 送信され，このペイロードに FTP のアカウント情報が記述されていることを確認した．

4. 観測システムの設計

4.1 構成

漏洩したアカウントを攻撃者が悪用する動作を観測するために，アカウント情報漏洩マルウェアの収集，情報の漏

洩，サーバでの観測を行う必要がある．よって，マルウェアの収集を行う Web クライアントハニーポット，マルウェアの動的解析により情報を漏洩させるマルウェア動的解析器，Web サイト管理システムを模擬して FTP サーバへのアクセスとコンテンツの改竄を観測する FTP ハニーポット，からなる一連の解析システムを設計および実装する．これらの検知/解析/観測技術はそれぞれが連携して自動的に動作するよう設計する．

4.1.1 Web クライアントハニーポット

Web クライアントハニーポットは，ドライブバイダウンロード攻撃を試みる悪性 Web サイトを検知するためのおとりホストである．ハニーポットはエミュレータを用いる低対話型と，実際の OS やアプリケーションを用いる高対話型がある．ドライブバイダウンロード攻撃では，脆弱性を攻撃するコードが Web コンテンツの内部に埋め込まれており，様々なクライアントアプリケーション（Web ブラウザおよび Acrobat，Java，Flash などのプラグイン）が処理するフォーマット（html，js，pdf，jar，swf など）として存在する．また，攻撃コードを含む Web コンテンツは解析や検知を回避するために難読化されている場合が多く，Web コンテンツを処理する過程で難読化された攻撃コードが実行される．このため，低対話型での攻撃検知は，エミュレータがクライアントアプリケーションを忠実に模擬できるかどうかに依存している．現状の低対話型 Web クライアントハニーポットは，JavaScript，PDF，Java，Flash などの攻撃に利用される Web コンテンツを処理するためのエミュレーションが不完全なため，攻撃の見逃しが多く発生する．

一方，高対話型は脆弱性があるクライアントアプリケーションを用いることで攻撃を受けることができる．高対話型における攻撃の検知は，ファイルシステムやレジストリアクセスおよびプロセス生成のイベントがあらかじめ定義された正常動作かどうかを判別する方法がある [18]．また，特定の脆弱性箇所に対するデータフローを監視し，脆弱性が発症する条件を満たすデータが入力された場合（たとえば，バッファサイズを超過するデータが入力された場合にバッファオーバフローであると判断）に検知する方法がある．また，悪性 Web サイトの生存期間は正規 Web サイトと比較して短く，特にブラックリストに掲載されたものは 1 カ月以内に半数以上が消滅することが我々の事前研究で判明している [4]．このため，定期的に一定数のサイトを検査する必要があり，高速に検査できる手法が求められる．

検査の正確さと高速化を両立させるため，我々の事前研究である Marionette [3] を用いる．Marionette は，同一 OS 上で複数のブラウザプロセスを並列して動作させるマルチプロセス化と，単一のマネージャが複数の OS を分散して配置するマルチエージェント化によって，検査速度の向上とスケーラビリティを実現している．これにより，短

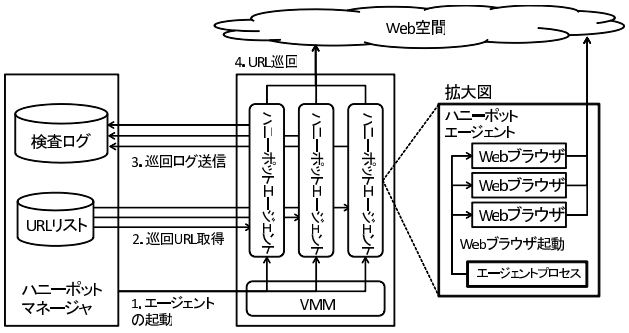

図 2 Web クライアントハニーポット
Fig. 2 Web client honeypot.

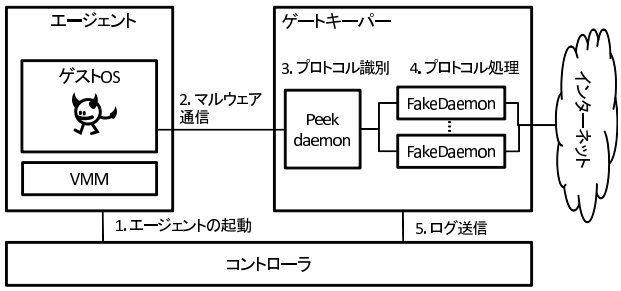

図 3 マルウェア動的解析器
Fig. 3 Malware dynamic analysis system.

時間で多数の URL を検査し，悪性 Web サイトの検知とマルウェアの収集を行う．Marionette の構成図と処理手順を図 2 に示す．

4.1.2 マルウェア動的解析器

マルウェアにアカウント情報を漏洩させるためには，インターネットに接続された環境でマルウェアを実行する必要がある．マルウェアを実行して解析する環境はマルウェア動的解析器と呼ばれる．マルウェアを解析する際，ホスト外部に対して感染行動やスパム送信などの攻撃を行うマルウェアが存在するため，安全性を考慮してインターネットとは隔離された環境で動作させる場合が多い．しかし，外部ホスト（攻撃者）と情報を送受信しながら動作するボットやダウンローダなどのマルウェアは，動作を解析するうえでインターネットの接続性が必須となる．本論文が対象としている情報漏洩を引き起こすマルウェアについても同様にインターネットの接続性が必須となる．よって，一般ホストへの攻撃を防いだうえで攻撃者と通信させる，安全性を考慮した半透過的な解析環境を用いる必要がある．そこで，安全性を担保したうえで外部への通信を許可するマルウェア動的解析器（BotnetWatcher [8]，図 3）を用いる．BotnetWacher は，マルウェアを OS 上で動作させるエージェント，マルウェアの通信を制御するゲートキーパからなる．ゲートキーパはマルウェアが行う通信のプロトコル判別を行う PeekDaemon，仮想ネットワーク上で動作する代理サーバプログラムである FakeDaemon を持つ．PeekDaemon は TCP/UDP およびプロトコルを判

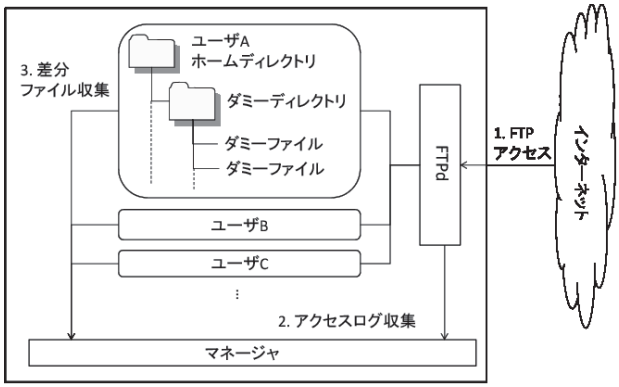

図 4 FTP ハニーポット
Fig. 4 FTP honeypot.

別し，TCP であれば 3way-handshake 確立まで処理し，プロトコルに対応する FakeDaemon に処理を委譲する．外部への通信が許可されたプロトコルの場合，FakeDaemon は該当の通信を外部に通し，許可されていないプロトコルの場合は FakeDaemon が擬似的な応答を行う．なお，本実験では HTTP/IRC/DNS の FakeDaemon については外部に通すように設定した．

事前調査においてアカウント情報漏洩マルウェアを解析した結果，複数の FTP クライアントから情報を盗むことが判明している．そのため，マルウェア解析環境上にあらかじめ FTP クライアントを複数種類インストールし，マルウェアの解析ごとにアカウント情報を生成し設定する．これにより，マルウェアの解析ごとにアカウント情報を生成するため，アカウント情報は解析対象のマルウェア固有のものとなり，後ほど FTP ハニーポットのログで対応付けることができる．

4.1.3 FTP ハニーポット

FTP ハニーポット（**図 4**）は，Web サイトのコンテンツサーバであると見せかけることで，攻撃者による Web コンテンツの改竄を誘い込むおとりサーバである．よって，FTP ハニーポットはダミーの Web コンテンツ（html, php, js ファイルなど）をファイルとして各 FTP アカウントのユーザディレクトリ配下に配置し，FTP アカウントごとにユーザディレクトリ配下を自由にアクセスさせる．FTP ログイン情報や FTP コマンド履歴およびファイルの変更などはログとして出力する．ファイルは変更された際にファイル自体のバックアップをとり，オリジナルのファイルとの差分を抽出して保存する．このように攻撃者が行うサーバ側での動作や実際の改竄コンテンツを観測し，これらのログをアカウントごとにまとめて管理する．FTP ハニーポットのホスト上では FTP サーバのみ起動しており，他のネットワークサービス（Web サーバなど）は停止させる．また，アカウント情報漏洩を行うマルウェアの多くが FTP サーバの IP アドレスと同時にドメイン名も漏洩させていたことから，FTP ハニーポットにはドメイン名を割り当てた．

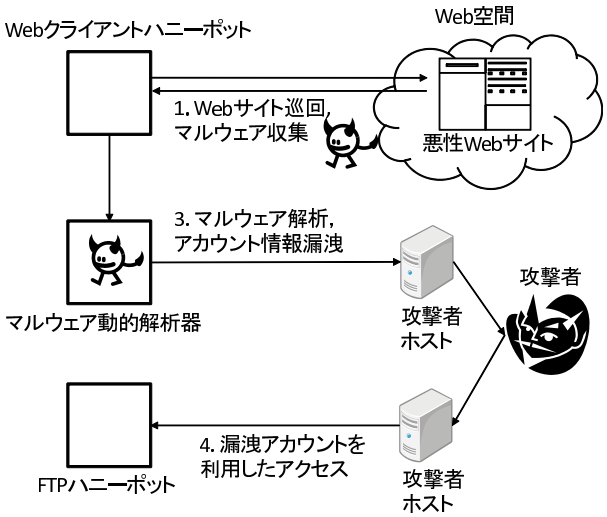

図 5 解析手順
Fig. 5 Analytical procedure.

4.2 解析手順

アカウント情報漏洩マルウェアの解析手順を説明する（**図 5**）．

(1) マルウェアの収集
Web クライアントハニーポットを用いて，公開ブラックリストに登録されている最新の悪性 Web サイトを巡回し，マルウェアを収集する．収集したマルウェアはマルウェア動的解析器に送信される．

(2) アカウント情報の漏洩
収集したマルウェアをマルウェア動的解析器で解析する．解析は収集後 24 時間以内に実行する．解析ごとにアカウント情報を生成して設定しておき，マルウェアごとに漏洩させるアカウント情報を変化させる．

(3) アカウントの不正アクセス観測
漏洩させたアカウント情報に対応するユーザディレクトリおよびダミーの Web コンテンツを作成し，攻撃者からのアクセスを観測する．アカウントごとにアクセス履歴や FTP コマンド履歴および変更があったファイルの内容などをログとして保存する．

5. 実験

本システムの目標は，攻撃者のサーバ上での挙動を把握し，またその結果としてドライブバイダウンロード攻撃を行う悪性 Web サイトを効率的に発見することである．特に，不正アクセスを行う攻撃者の IP アドレスや悪性 Web サイトが実際に悪用される前に発見することで，フィルタリングなどの対策に活用することができる．

本システムによる観測は 2012 年 3 月から同年 11 月末までの 8 カ月間行った．

5.1 マルウェアの収集

Web 経由のマルウェア感染はドライブバイダウンロー

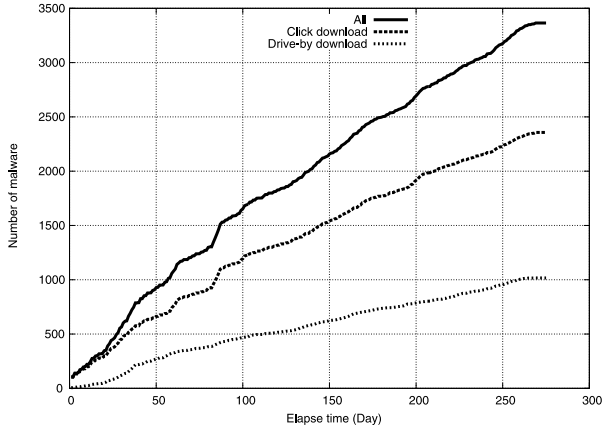

図 6 Web 巡回で収集した検体の累積（ハッシュ値ユニーク，2012 年 3 月からの累計）

Fig. 6 Cumulative number of collected malware (unique hashes, collected from Mar. 2012).

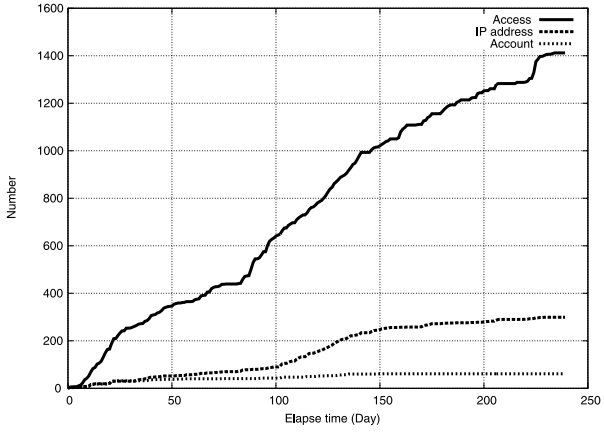

図 7 漏洩アカウントに不正ログインを行う IP アドレス（2012 年 3 月からの累計）

Fig. 7 Cumulative number of IP addresses attempting fraudulent access with stolen credentials (collected from Mar. 2012).

ドだけでなく，クリックダウンロードがある．クリックダウンロードとは，実行ファイルへの直接リンク URL にアクセスしてダウンロードダイアログをユーザがクリックすることによるマルウェア感染である．クリックダウンロードの実行ファイルが必ずしもマルウェアであるとはいえないが，本システムではマルウェアかどうかにかかわらず収集し，以降は便宜上クリックダウンロードのマルウェアと呼ぶ．

マルウェアを収集する際の巡回対象 URL として公開ブラックリスト（malwaredomainlist.com）約 8 万 URL および検索エンジンから取得した一般サイト約 15 万のトップページ，合計約 23 万 URL を使用した．なお，公開ブラックリストは巡回ごとに最新の URL を取得した．この巡回対象を数日間隔で巡回し，ドライブバイダウンロードやクリックダウンロードによりマルウェアを収集した（**図 6**）．期間中に，ドライブバイダウンロードで得られた検体を約 1,000 種類，クリックダウンロードで得られた検体を約 2,400 種類収集した．

時間経過とともにユニークな検体数が増加しているのは，ブラックリスト自体がつねに更新されていることによって新規悪性 Web サイトから新種検体が取得できていることや，既知の悪性 Web サイトであっても配布されるマルウェアが変化していることが要因である．なお，同一のマルウェアであっても別巡回で取得した場合はそのつどマルウェア動的解析器に送信し解析される．

5.2 攻撃者が利用する IP アドレス

FTP アクセスを行うアクセス元 IP アドレスを観測することにより，アカウント情報漏洩マルウェアを制御する攻撃者の IP アドレスを特定できる．FTP サーバに対するアクセスにおいて，ブルートフォースのアクセスと区別するために，アカウント名とパスワードを間違えることなくログインしてきた IP アドレスのみを対象とし，それ以外のブルートフォースを試みるアクセスを対象外とする．

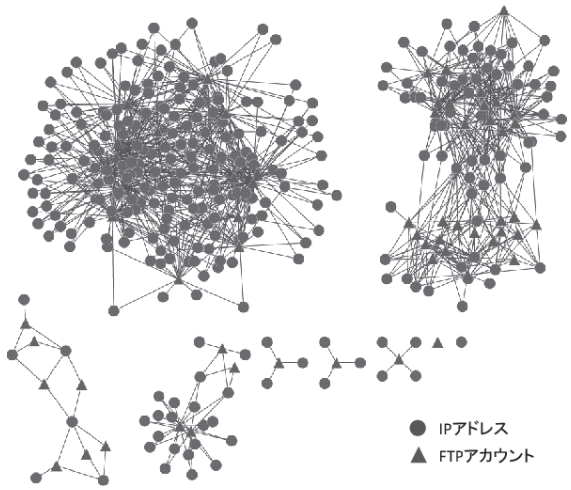

図 8 攻撃者グループのクラスタ（FTP アカウントと IP アドレスのグラフ構造）

Fig. 8 Cluster of adversary groups (graph structure of FTP account and IP address).

攻撃者が利用した IP アドレスおよびログインが成功したアカウント数について時系列累積グラフを**図 7** に示す．観測期間中にアクセスされたアカウントは 61 種類であり，これらのアカウントに対する FTP アクセスを 1,412 回，攻撃者の IP アドレスを 299 種類収集できた．漏洩させた FTP アカウント数と比較して，IP アドレス数は約 5 倍程度収集できている．これは，攻撃者が同一の FTP アカウント情報を用いて複数の IP アドレスから FTP ハニーポットへアクセスしていることを示している．

図 8 は FTP ハニーポットへのアクセスに利用された FTP アカウントとアクセス元の IP アドレスのグラフ構造を示している．これらの各グラフがそれぞれ攻撃者グループを形成していると考えられる．これらの攻撃者グループ

表 2 情報漏洩を行ったマルウェアの検体数とファミリ名
Table 2 Number and family name of information-leaking malware.

ESET-NOD32	Forefront	Kaspersky
36, Win32/Kryptik	16, PWS:Win32/Fareit	7, Trojan-FakeAV
6, Win32/Spy/Zbot	11, TrojanDownloader/Waledac	7, Trojan.Win32.Jorik
4, Win32/Injector	9, Backdoor:win32/Kelihos	7, Trojan-PSW:Win32:Tepfer
3, Win32/PSW.Agent	6, PWS:Win32/Zbot	5, Trojan-Ransom.Win32.Birele
	6, TrojanDownloader:Win32/Dofoil	4, Trojan-Ransom.Win32.Gimemo
	1, Trojan:Win32/Orsam	4, Trojan-Spy/Win32.Zbot
		5, その他の検知検体
		10, 未検知検体

表 1 攻撃者グループ
Table 1 Adversary groups.

攻撃者グループ	マルウェア検体	漏洩アカウント	攻撃者の IP アドレス
A	15	15	189
B	20	31	69
C	4	4	21
D	7	7	6
E	1	1	3
F	1	1	3
G	1	1	4
H	1	1	1

に属する情報を**表 1** に示す．同一のアカウントに対してアクセス元の IP アドレスが複数存在することから，攻撃者はボットを用いている可能性が高い．さらに，1 つの IP アドレスから複数のアカウントへのアクセスや，複数の IP アドレスが単一のアカウントへアクセスする状況がグラフ構造から把握できる．このクラスタが攻撃者グループを示していると考えられ，大小あわせて 8 種類の攻撃者グループを観測できた．なお，各グループの特徴として同種の改竄などを行うことを観測している．

攻撃者の IP アドレスが判明することで，対策として Web サーバや FTP サーバへのアクセスを監視することで攻撃者が改竄コンテンツをアップロードするアクセスを検知できる可能性がある．

5.3 情報漏洩を行ったマルウェア

不正にログインされたアカウントから，マルウェア動的解析器のログを参照し，どのマルウェア解析時に漏洩したアカウントかを特定し，それによって漏洩を行ったマルウェアを特定した．その結果，漏洩を行った 49 種類のマルウェアを特定した．これらのマルウェアのうち，クリックダウンロードによる収集は 15 検体，ドライブバイダウンロードによる収集は 34 検体であった．3 種類のアンチウィルスソフト（ESET-NOD32，Forefront，Kaspersky）でスキャンした結果を**表 2** に示す．FakeAV はアンチウィルスソフトを装って主にクレジットカードなどの認証情報を搾取するマルウェアの一般名称として知られている．Zbot はバンキングなどの様々なアカウント情報を盗むことで知られている．その他，アカウント情報を盗むことがすでに知られているマルウェアファミリが多く存在している．今回解析したこれらの検体は FTP のアカウント情報を漏洩させる機能を保有するマルウェアであり，また FTP 以外のアカウント情報も漏洩させる機能があることが推測される．

5.4 改竄コンテンツ

Web サーバや FTP サーバにアップロードされるコンテンツに対して FTP ハニーポットで収集した改竄コンテンツとの一致性を確認することで，攻撃者による Web サイトの改竄を検知できる可能性がある．

FTP ハニーポットでは，オリジナルの内容と変更が加わった内容について自動的に差分を抽出している．この差分の多くはリダイレクトコードである．このリダイレクトコードは攻撃者があらかじめ準備した悪性 Web サイトへのリダイレクトを行う．なお挿入されたコードは難読化されており，Web ブラウザで実行して初めてリダイレクトコードが出現する．Web クライアントハニーポットで実際に Web コンテンツを処理させることにより，リダイレクト先の悪性 Web サイトの URL を抽出できる．

改竄が行われた 61 アカウントについて，トップページ相当の Web コンテンツを分析したところ，外部の URL に対するリダイレクトが発生するものが 50 アカウント存在した．リダイレクト先の多くは Exploit kit [*1] で作成された悪性 Web サイトやそのサイトへリダイレクトを行う踏み台の URL であった．つまり，改竄による主な目的は，新たなドライブバイダウンロード攻撃を仕掛けるための入り口として一般サイトを改竄したといえる．

ここでは特にノード数の多い上位 2 種類のグループである A と B について，それぞれの改竄コンテンツを分析した．その結果，同一グループに所属するアカウントは Web

[*1] ドライブバイダウンロード攻撃を行う Web サイトを構築するためのツールキット．アンダーグラウンド市場で様々な種類のツールキットの売買がされている．

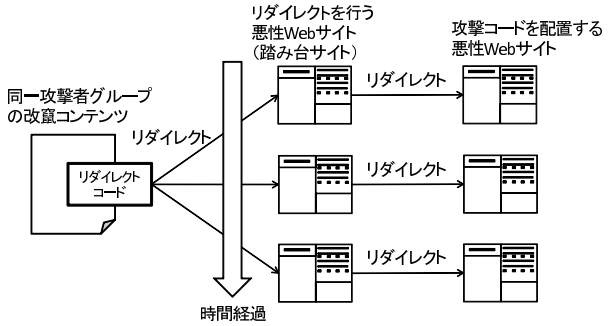

図 9 本システムで観測したマルウェア配布ネットワーク
Fig. 9 Observed malware distribution network.

コンテンツにリダイレクトコードが挿入されており，類似の URL へダイレクトされることが分かった（**図 9**）．なお，挿入されたリダイレクトコードは難読化されていたため，Marionette によってコンテンツを実際に動作させて解析を行い，その際に発生する HTTP リクエストからリダイレクト先の URL を特定した．これらのリダイレクト先 URL 情報は一定時間（数日程度）経過後に新しいものに変更されるため，長期的に改竄されたコンテンツを解析することで，攻撃者の悪性 Web サイトを特定できる．グループ A によって改竄されるコンテンツは踏み台サイトに対してリダイレクトを行い，さらにそのサイトから HTTP-302 リダイレクトにより異なる悪性 Web サイトへリダイレクトされる．この悪性 Web サイトは Exploit kit の `Blackhole` で構築されていた．グループ B はグループ A と同様に，踏み台サイトへリダイレクトを行い，さらにそのサイトから HTTP-302 リダイレクトにより `Redkit` で構築された悪性 Web サイトへリダイレクトされる．`Blackhole` および `Redkit` は近年最も流通している Exploit kit であり，多くの悪性 Web サイトで利用されていることが知られている [1], [2]．グループ A では異なるアカウントに対しても同種のリダイレクト先 URL が改竄コンテンツに含まれることを確認しており，時間が経過するとリダイレクト先のドメインも変化していく．なお，グループ B でも同様の傾向を確認している．

本実験によりこれらのリダイレクト先を Web クライアントハニーポットで定期的にアクセスすると，時間経過とともに変化する悪性 Web サイトのドメイン名や IP アドレスを効率的に収集できることが判明した．また，リダイレクトを行う中継サイトだけでなく，攻撃コードを配置している悪性 Web サイトも時間経過とともに変化することが判明した．なお，観測期間中に収集した悪性サイト情報は**表 3** のとおりである．時間経過によって新しい FQDN や IP アドレスが取得できた．特にグループ B の中継サイトは Fast-flux [*2] で構成されており，アクセスするごとに IP アドレスが変化し，合計で 1,276 種類の IP アドレスを取得できた．

[*2] DNS ラウンドロビンによって短期間に IP アドレスを切り替えることで悪性サイトの所在を突き止めにくくする方法．ボットネットによって行われる．

表 3 取得した悪性 Web サイト情報
Table 3 Obtained malicious website information.

攻撃者グループ	リダイレクトを行う悪性 Web サイト	攻撃コードを配置する悪性 Web サイト
A	190 FQDN 31 IP アドレス	110 FQDN 11 IP アドレス
B	36 FQDN 1,276 IP アドレス	36 FQDN 76 IP アドレス

表 4 公開ブラックリストとの比較
Table 4 Comparison with public blacklist.

	取得情報数	ブラックリスト含有数
攻撃者の IP アドレス	299	3
悪性 Web サイトの FQDN	411	0
悪性 Web サイトの IP アドレス	1,404	0

5.5 公開ブラックリストとの比較

本システムで取得した情報が最新の公開ブラックリストでどの程度発見できているかについて調査する．公開ブラックリストは収集にも利用した malwaredomainlist.com の 11 月末時点での最新のリストを用いる．このリストには 44,455 FQDN，19,672 IP アドレスが掲載されている．なお，これら FQDN や IP アドレスはすでに攻撃者に利用されていないものを多く含む．

本システムで収集した情報（IP アドレスおよび FQDN）をブラックリストと比較した結果を**表 4** に示す．悪性 Web サイトの情報は攻撃者グループ A および B から取得したものを利用する．なお，攻撃者グループ A と B で悪性 Web サイトの IP アドレスが 1 件のみ重複した．攻撃者の IP アドレスがブラックリストに 3 件のみ掲載されており，悪性 Web サイトはまったく掲載されていなかった．この結果は，既存のブラックリストを作成する技術とは異なる空間を観測できたことを示している．

6. 考察

6.1 安全性

攻撃を観測するにあたって解析システムを安全に運用することは，解析の継続性を担保するとともにセキュリティ研究者/技術者としての倫理的側面からも重要である．安全な運用とは，解析システム自体が乗っ取られること，その結果として外部ネットワークや外部ホストに対する攻撃の踏み台になることを防止することである．ここでは収集，解析，観測を行う各システムについて，安全性および安全性を担保するための仕組みについて説明する．

6.1.1 収集

マルウェアの収集はクリックダウンロードとドライブバイダウンロードに分けられる．前者は，ユーザがマルウェアのバイナリファイルへの直接リンク URL にアクセスし，ダウンロードダイアログを自らクリックすることでダウンロードしインストールする感染である．Marionette ではこのユーザのクリック動作を模擬し（ダウンロードダイアログのボタンを押下する），ダウンロードのみを行い，インストールはせず安全にマルウェアを収集する．後者は攻撃を受けてブラウザプロセスの制御が奪われた後にマルウェアのダウンロードとインストールを行うため，通常の高対話型ハニーポットの場合はマルウェアに感染してしまい，外部に対して攻撃などを仕掛ける可能性がある．このため，Marionette では，マルウェアのダウンロードまでを許可し，その後のマルウェア実行を抑制することでマルウェアに感染することを防止している．

6.1.2 解析

インターネットと接続されている環境においてマルウェアを解析する場合は，外部ホストに対する攻撃を防止する必要がある．リモートエクスプロイト攻撃によるマルウェア感染に利用される TCP139/445，ホストの存在をスキャンするために利用される ICMP などは，マルウェア動的解析器内部で終端されるため，外部ホストに対して影響を及ぼすことはない．BotnetWacher は，これらの攻撃通信を遮断し，攻撃者との通信のみを通過させることで安全性を担保している．

6.1.3 観測

FTP ハニーポットで観測する場合，改竄された Web コンテンツを Web サーバとして公開した場合，一般のユーザが誤ってアクセスすることでマルウェアの感染に加担してしまう可能性がある．よって FTP ハニーポットでは Web サーバを立ち上げておらず，外部から Web サイトとしてアクセスすることはできない．

6.2 偽装性

ハニーポットやマルウェアの解析システムにおける問題点として偽装性があげられる．偽装性とは被害ホストを装って動作することで，攻撃者やマルウェアによる解析妨害を回避するために重要になる．攻撃者は実際の標的ホストと解析システムの挙動の差異により，解析しているかどうかを判別することが多い．

Web クライアントハニーポットでは，実際の OS やアプリケーションを用いて被害ホストを装っており，エミュレータ特有の不自然な動作は発生しない．また，悪性 Web サイトにアクセスする際は，送信元の IP アドレスを毎回変更しており，同一 IP アドレスからの重複したアクセスを行わないネットワーク環境を用意している．

マルウェア解析器においても同様に，実際の OS 上で動作させ，インターネットへの通信のうち攻撃者との通信は通過させ，攻撃と思われる通信は仮想インターネットで処理しており，どちらにせよホスト上のマルウェアからは正常にインターネットへの通信ができているかのように見える．

ただし本システムでは，マルウェアの収集をしたホスト（Web クライアントハニーポット）の IP アドレスと，アカウント情報を漏洩させたホスト（マルウェア動的解析器）の IP アドレスが異なる．攻撃者からみるとマルウェアを感染させたホストと感染後に情報を送信してきたホストが異なることから解析システムであることが感知される可能性がある．しかし，近年では “マルウェア感染の誘導”，“マルウェア配布”，“マルウェアの運用” の分業化（Pay-Per-Install [9]）が進んでいるため，単一の攻撃者が標的の IP アドレスの一貫性について必ずしも厳密に管理しているわけではない．実際に我々の実験においても複数の攻撃者グループから多数の改竄を受けていることからも，漏洩したアカウント情報の観測を行ううえでは影響は少ないことを示している．

6.3 アカウントの漏洩方法

今回のシステムでは，解析環境にあらかじめ FTP クライアントをインストールしておき，解析前にアカウント情報を設定したうえでマルウェアを実行する．マルウェアが情報を自動的に収集して外部に送信する場合は漏洩が成功するが，なんらかのイベントを契機とする場合は漏洩が成功しない場合がある．たとえば，Web ブラウザのヘルパオブジェクトとして動作するマルウェアの場合は，マルウェア解析時に Web ブラウザを起動させる必要がある．また，FTP クライアントが FTP サーバにアクセスする際の通信をのぞき見ることでアカウント情報を漏洩させるマルウェアの場合は，マルウェア解析時に FTP クライアントを起動して FTP サーバにアクセスさせる必要がある．また，キーロガーによる漏洩を行うマルウェアの場合は，解析時に実際にキー入力を行う必要がある．本システムでは，上記のような特定の起動条件もしくはなんらかのユーザイベントによって動作する情報漏洩マルウェアは対象外である．

7. 関連研究

7.1 マルウェア動的解析

マルウェア動的解析器として Cuckoo [14] やオンライン解析サービスである Anubis [7] などがある．Anubis はインターネットに接続された環境での動作結果を取得できるため，外部ホストとの通信に基づいて動作するマルウェアを解析できるが，安全性については特に考慮されていない．マルウェアの動的解析における安全性については文献 [21] で検討されており，通信の可否をポリシに基づいて行う方法が提案されている．また，通信先のドメインが悪性かど

うかを検索エンジンの結果から評価し，悪性の場合は攻撃者との通信を行うものとして外部と通信させる方法 [8] が提案されている．

7.2 ハニーポット

マルウェアは様々なレイヤの感染経路により感染拡大の活動を行うため，それぞれの感染経路に対応するハニーポットを設計する必要がある．Windows OS ハニーポット（Dionaea [15]），Web クライアントハニーポット（PhoneyC [13]，Capture-HPC [18]，BLADE [10]），Web アプリケーションハニーポット（Glastopf [16], WebPhantom [20]）などの種類が提案されている．これらのハニーポットはマルウェア感染時の情報を収集するものであり，前述のマルウェア動的解析器と組み合わせることによってマルウェア感染およびマルウェア感染後の動作を解析できる．

7.3 認証情報を用いた攻撃の観測

攻撃からマルウェア感染およびマルウェアによる二次的な攻撃などの一連の攻撃手順を観測する手法が提案されている [6]．この手法では，ドライブバイダウンロード攻撃に起因するマルウェアを収集し，そのマルウェアを動的解析することで，ボットネットの C&C 通信やスパム送信を行うためのメールアドレス送信，また認証情報の外部送信などの動作を明らかにしている．BotSwindler [22] は，マルウェアの動的解析時に様々なユーザインタラクションのイベントを発生させることで認証情報の漏洩を促し，またマルウェアによって漏洩した認証情報を用いた不正ログインを実在するサービス上で観測している．本論文の提案手法では，文献 [6], [22] が対象としているマルウェアの動的解析や漏洩した認証情報を用いた不正ログインの観測だけでなく，攻撃者グループの挙動や改竄されたコンテンツの分析により，マルウェア感染対策に有効な悪性サイト情報が収集可能であることを示した．

8. まとめ

本論文では，ドライブバイダウンロード攻撃と Web 改竄を組み合わせたマルウェア感染への対策として，漏洩アカウントの悪用方法を観測することが重要であると考えた．おとりの FTP アカウント情報を能動的に漏洩させることにより，攻撃者が行う Web サイトへの改竄を誘発し，サーバ上での攻撃者の動作や改竄コンテンツの特徴を分析するシステムを設計，実装した．提案システムを利用し 8 カ月間にわたり実験を行った結果，攻撃者による改竄を安定的かつ長期的に観測することに成功した．観測した攻撃者の情報の多くは公開ブラックリストには含まれておらず，本システムが従来の観測技術とは異なる空間を観測できることを示した．

参考文献

[1] Grier, C., Ballard, L., Caballero, J., Chachra, N., Dietrich, C.J., Levchenko, K., Mavrommati, 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.M.: Manufacturing Compromise: The Emergence of Exploit-as-a-Service, *Proc. 19th ACM Conference on Computer and Communication Security* (*CCS2012*) (2012).

[2] Mcafee: Red kit an Emerging Exploit Pack, available from ⟨http://blogs.mcafee.com/mcafee-labs/red-kit-an-emerging-exploit-pack⟩.

[3] Akiyama, M., Aoki, K., Kawakoya, Y., Iwamura, M. and Itoh, M.: Design and implementation of high interaction client honeypot for drive-by-download attacks, *IEICE Trans. Commun.*, Vol.E93-B, pp.1131–1139 (2010).

[4] Akiyama, M., Kawakoya, Y. and Hariu, T.: Scalable and performance-efficient client honeypot on high interaction system, *Proc. 12th IEEE/IPSJ International Symposium on Application and the Internet* (*SAINT2012*) (2012).

[5] Akiyama, M., Yagi, T. and Itoh, M.: Searching structural neighborhood of malicious urls to improve blacklisting, *Proc. 11th IEEE/IPSJ International Symposium on Application and the Internet* (*SAINT2011*) (2011).

[6] Polychronakis, M., Mavrommatis, P. and Provos, N.: Ghost turns zombie: Exploring the life cycle of web-based malware, *Proc. 2nd Usenix Workshop on Large-Scale Exploits and Emergent Threats* (*LEET2008*) (2008).

[7] Anubis, available from ⟨http://analysis.seclab.tuwien.ac.at/⟩.

[8] Aoki, K., Yagi, T., Iwamura, M. and Itoh, M.: Controlling malware http communication in dynamic analysis system using search engine, *Proc. 3rd International Workshop on Cyberspace Safety and Security* (*CSS*) (2011).

[9] Caballero, J., Grier, C., Kreibich, C. and Paxson, V.: Measuring pay-per-install: The commoditization of malware distribution, *Proc. 20th USENIX Security Symposium* (2011).

[10] Lu, L., Yegneswaran, V., Porras, P. and Lee, W.: Blade: An attack-agnostic approach for preventing drive-by malware infection, *17th ACM Conference on Computer and Communications Security* (2010).

[11] Malware domain List, available from ⟨http://malwaredomainlist.com⟩.

[12] Moshchuk, A., Bragin, T., Gribble, S.D. and Levy, H.M.: A crawler-based study of spyware on the web, *13th Annual Network and Distributed System Security Symposium* (*NDSS*) (2006).

[13] Nazario, J.: PhoneyC: A virtual client honeypot, *LEET'09: Proc. 3rd Usenix Workshop on Large-Scale Exploits and Emergent Threats* (2009).

[14] The Honeynet Project: Cuckoo – Automated malware analysis, available from ⟨http://honeynet.org/project/Cuckoo⟩.

[15] The Honeynet Project: Dionaea, available from ⟨http://honeynet.org/project/Dionaea⟩.

[16] The Honeynet Project: Glastopf, available from ⟨http://honeynet.org/project/Glastopf⟩.

[17] Provos, N., Mavrommatis, P., Rajab, M.A. and Monrose, F.: All your iframes point to us, *SS'08: Proc. 17th Conference on Security Symposium*, Berkeley, CA, USA, USENIX Association, pp.1–15 (2008).

[18] Seifert, C. and Ramon, S.: Capture – Honeypot Client (Capture-HPC), available from ⟨https://projects.honeynet.org/capture-hpc⟩ (accessed 2008-09-22).
[19] Stokes, J.W., Andersen, R., Seifert, C. and Chellapilla, K.: Webcop: Locating neighborhoods of malware on the web, *LEET'10: Proc. 3rd Usenix Workshop on Large-Scale Exploits and Emergent Threats* (2010).
[20] Yagi, T., Tanimoto, N. and Hariu, T.: Intelligent high-interaction web honeypot based on URL conversion scheme, *IEICE Trans. Commun.*, Vol.E94-B, No.5, pp.1339–1347 (2011).
[21] Yoshioka, K., Kasama, T. and Matsumoto, T.: Sandbox analysis with controlled internet connection for observing temporal changes of malware behavior, *2009 Joint Workshop on Information Security* (2009).
[22] Bowen, B.M., Prabhu, P., Kemerlis, V.P., Sidiroglou, S., Keromytis, A.D. and Stolfo, S.J.: BotSwindler: Tamper resistant injection of believable decoys in VM-based hosts for crimeware detection, *Proc. 13th International Conference on Research In Attacks, Intrusions, and Defenses* (*RAID 2010*) (2010).

秋山 満昭

2005 年立命館大学理工学部卒業．2007 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．2013 年同大同研究科博士課程修了．2007 年日本電信電話株式会社入社．現在，NTT セキュアプラットフォーム研究所勤務．ネットワークセキュリティ技術，特にマルウェア対策とハニーポットに関する研究に従事．

八木 毅

2002 年千葉大学大学院自然科学研究科修士課程修了．2013 年大阪大学大学院情報科学研究科博士課程修了．2002 年日本電信電話株式会社入社．現在，NTT セキュアプラットフォーム研究所勤務．ネットワークセキュリティ技術，Web セキュリティ技術に関する研究に従事．

青木 一史 （正会員）

2006 年東北大学大学院情報科学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT セキュアプラットフォーム研究所勤務．ネットワークセキュリティ技術，特にマルウェア解析技術に関する研究に従事．

針生 剛男

1991 年電気通信大学大学院電気通信学研究科修士課程修了．同年日本電信電話株式会社入社．現在，NTT セキュアプラットフォーム研究所勤務．ネットワークセキュリティ技術，マルウェア対策技術の研究に従事．