悪性サイトドメインの長期観測結果に基づくブラックリスト利用の有効性に関する一考察

須藤　年章†

†NTT コミュニケーションズ株式会社
105-7104　東京都港区東新橋 1-5-2 汐留シティセンター4F
t.sudou@ntt.com

あらまし 近年、サーバーやウェブアプリケーションのアカウント情報を窃取することを目的とした攻撃が大量に発生している。これらの攻撃へ対応方法の一つとして悪性サイトや攻撃元サイトのIPアドレスやドメイン名、URLを元にしたフィルタリングやブロッキングを実施することで攻撃や情報漏えいを防ぐ方法があるが悪性サイトは、機能や手法により長期間存在しているものもあれば数時間で役割を果たしてしまうものもあり、また長期間存在していたとしても実害はないものがある。本研究では MWS Datasetから得られる悪性サイト情報を含む様々な悪性サイト情報に関して生存時間と影響度に着目した解析を行い悪性サイト情報の有効性と精度の向上について考察する。

A study on the effectiveness of black list use based on long-term observations of malignant site domain

Toshiaki Sudoh†

†NTT Communications Corporation
Shiodome City Center 5-2 Higashi Shinbashi 1-Chome Minato-Ku,Tokyo 105-7104,Japan
t.sudou@ntt.com

Abstract Recently, attacks intended to steal the account information and web application server is generated in large quantities. There is a way to prevent information leakage and attacks by implementing the blocking and filtering that is based on domain name or IP address, the URL of the offending site and malignant site as one of how to respond to these attacks malignant site, some no harm even if existed a long period as it would play a role in a few hours if some of which are present a long period by a procedure or function also has. We consider improving the accuracy and effectiveness of the malignant site information and analyzes focused on impact with the survival time with respect to malignant sites variety of information, including malignant site information obtained from MWS Dataset in this study.

1　はじめに

マルウェア感染、コマンドコントロール、窃取した情報収集などに利用されるサーバーは、一般のウェブサーバーと同等の運用技術と品質で運用されていることが多く、そのサーバーへのアクセスコントロールの基本機能として DNS を利用した名前解決であることも一般サービスと同様である。また攻撃に利用されるドメインは長期利用されるもの、攻撃毎に変更されたり、短期で使い捨てられるもの、時間毎にランダムに変更同期していくものなどがあり、検出および対策を逃れるための機能がと運用手法が多く盛り込まれており、ブラックリストベースでのフィルタリング等で意図通りの効果が得られにくい状況が生まれている。本稿では攻撃に利用されたドメインの長期利用動向を解析し、攻撃サイト用ドメインの利用期間に着目した特性と、ブラックリスト等で利用する際の問題点について考察する。

2　攻撃用システムの構成

攻撃に利用されるシステムは古くは単純な構成であったが、最近の攻撃では、一般ユーザーのサイトを改ざんしたものを利用したり、複数のホスティングサービスを利用し、機能別に分散設置する構成が取られている場合が多い。攻撃システムを構成する要素を表 1 にま

表 1　攻撃システム構成要素

	種別	機能
1	リダイレクタ	攻撃サイトへ誘導するための初期アクセスサイト
2	攻撃サイト	各種脆弱性を実際につく攻撃を行うサイト
3	マルウェア配布サイト	マルウェアを保存しているサイト。ダウンロードサイト
4	情報収集サイト	窃取した情報を集める
5	C&C	ボットをコントロールするコントロールサイト

2.1　リダイレクタ

リダイレクタは、ここ数年流行のウェブ感染型攻撃の感染トリガーとなる初期アクセスに利用される仕組みであり、このサイトにアクセスすることにより攻撃サイトに転送される。攻撃サイト本体を隠蔽し守る仕組みである。通常は乗っ取りや改ざんされた一般ユーザーや商用サービスのサイトが利用される。被害者はスパムメール等に記載された URL を踏むことでアクセスする場合や、日常のウェブ閲覧をしているだけでもこれらの改ざんサイトにアクセスしてしまうこともある。基本的に解析を逃れるために同一の攻撃に利用される期間が非常に短いことが知られており、解析や対策の迅速性が求められる。

2.2　攻撃サイト

リダイレクタから転送される実際に攻撃を行うサイトである。OS や各種アプリケーションの脆弱性を突き、マルウェア感染を行う。直接アクセスさせず前段にリダイレクタを置く構成をとることで、サイトを守っているため、リダイレクタよりは比較的長い期間存在する。しかし攻撃サイトもある程度の期間をもってドメインの変更もしくは IP アドレス自体の変更を行うことが多い。

2.3　マルウェア配布サイト

感染に利用するマルウェアを保存しているサイトのことである。ウェブ経由の感染においては、攻撃サイトと同一の場合が多い。その他の古典的な bot 化やダウンローダー経由での感染についてはこれらのサイトのドメインや URL がダウンローダーそのものにプログラムされている。これらのサイトもある程度の期間でドメインや IP を変えて運用されるか、使い捨てられる。

2.4　情報収集サイト

マルウェア感染により感染端末から窃取された個人情報や、カード番号、各種ネットサービス

にログインするための ID やパスワードを収集するサイトである。比較的長期間変化がなく運用され続ける例が多いが、目的の情報収集が終わったら、ドメインや IP を変更し使い捨てられる。

3 攻撃用ドメインの利用期間

それぞれのサイト機能および攻撃手法の違いにより期間の長短はあるが、利用されるドメインには生存期間があり、変化のスピードに追随できないと有効な対策が打てない。そこでドメイン利用期間の特性を解析することでブラックリストやフィルタリング対応の効率を高める検討をする必要がある。攻撃に利用されるドメインの変化の特性および利用期間について解析する。

3.1 攻撃用ドメインの変化の影響

攻撃用のドメインの変化には二種類あり攻撃の種類によりどちらかの手法が用いられている。

- 登録されている A レコードが変化
- ドメイン自体が短期間で使い捨てられる

この手法の違いは対策方法への影響を与える。

3.1.1 登録されている A レコードの変化

攻撃用ドメインに登録されている A レコードが変化する場合は、ドメイン自体は変化せず利用され続けられるため、ドメインベースのフィルタリングを行うためのブラックリストへの適用は有効である。ただし IP アドレスベースのフィルタリングやブラックリストに適用する場合は、A レコードの変化に追随する必要がある。

3.1.2 ドメイン自体が短期間に使い捨てられる場合

最近の攻撃手法で広く利用されている手法であり、一日未満で使い捨てられるなど、短期間で変化していく場合があるためドメインベースのブラックリストを利用した対策を行う場合、発見、解析、ブラックリストへの登録に時間がかかってしまうと、すでに攻撃利用されなくなってしまっているという事態が想定される。そのため攻撃に利用されるドメインの利用状況、期間の特性について解析することで対策準備に利用できる期間や効果の有無について検討する。

4 攻撃用ドメインの利用期間解析

データセットから得られる攻撃サイトのドメイン情報の長期解析結果を利用し、攻撃サイトの変化、利用期間、再利用等の状況を分析する。

4.1 攻撃に利用された悪性サイトドメイン

攻撃に利用された悪性サイトドメインと長期観測データとの相関分析を行うために CCC Dataset 2008[1]、CCC Dataset 2009[1]、CCC Dataset 2010[1]、CCC Dataset 2011[1]から各種攻撃に利用されたドメイン情報を抽出した。各データセットから抽出した攻撃用ドメイン数を表 2 に示す。

表 2 各データセットからのドメイン抽出数

No	Dataset	ドメイン数
1	CCC Dataset 2008	32
2	CCC Dataset 2009	12
3	CCC Dataset 2010	10
4	CCC Dataset 2011	2

各データセットに共通のドメインもあり 2008 年から 2010 年の 3 つのデータで共通的に抽出されたドメインが 4 個、2008 年と 2009 年 2 つのデータで共通的に抽出されたドメインが 9 個あった。これらの重複を取り除いた結果ドメイン数は全体で 37 個となった。またそのドメインが利用されるサイトの機能は C&C およびマルウェア配布サイトのみであった。

4.2　ドメイン利用期間の解析

抽出されたドメインが 2007 年 7 月 1 日から 2013 年 7 月 31 日の間に利用可能であった日数について分析した結果を図 1 に示す。これはそのドメインにグローバル IP アドレスが A レコードとして登録されていた期間の集計であり、攻撃に加担していない日数も含んでいる。

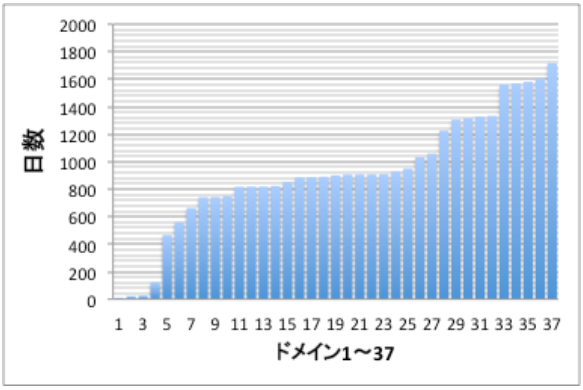


図 1　利用可能だった日数

最短で 19 時間であり、その状況を図 2 に示す。このドメインは 2009 年 12 月 7 日にこの時間だけ復活した Kraken のドメインである。それ以外の期間は 127.0.0.2 が登録されており、攻撃に利用できないように設定されている。この期間だけ復活した理由は不明である。

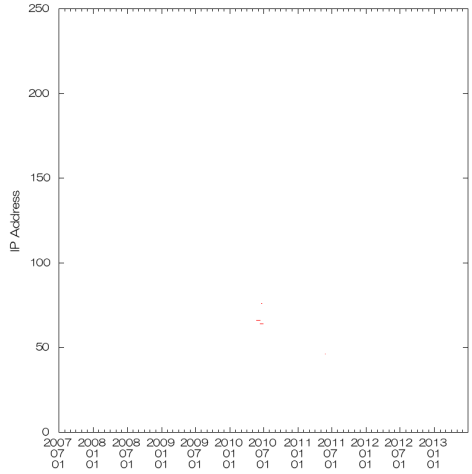


図 2 最短ドメイン

最長は 1717 日で全観測期間で稼働し続けている ftp サーバーである。全期間は 2222 日であるが、データ取得に失敗している期間があるため、実施には全観測期間存在している。その状況を図 3 に示す。

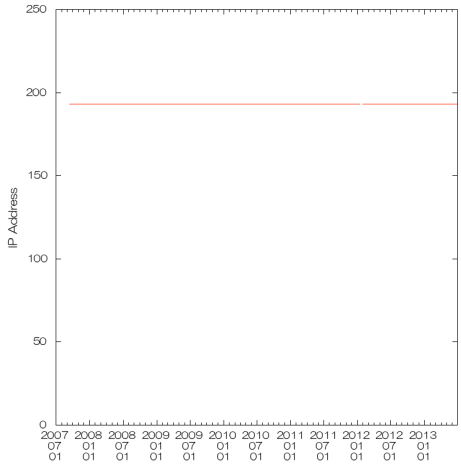


図 3　最長ドメイン

平均すると 917 日となり、想定よりも長い期間となった。数個のドメインについてはドメイン事業者に買い取られて、単に A レコードが登録されているだけで攻撃に全く関連していない期間が長いものもあるが、その要素を除外した場合でも平均で 700 日程度となり全観測期間 2222 日の 31.5%の期間でサーバーとして稼働可能な状況にあったことになる。また、攻撃利用されているもの、サイトは存在するが攻撃利用されていないもの含めて 2013/7/31 の時点でドメインおよびサイトが存在するものは 37.8%の 14 個である。また完全に利用されなくなるまでの期間は平均で 3.84 年であった。

4.3　特徴的なドメインの解析

次に特徴的なドメインの例を解析する。

4.3.1　domain1

domain1 の A レコード登録状況を図 4 に示す。domain1 は、当初は rbot の C&C サーバーとして利用されていたものである。2008 年 12 月に C&C は閉鎖され、このドメインはドメイン管理業者に買い取られて管理されていた後 NXDOMAIN となったが、3 年後の 2011 年 12

月に別の新しいbotnetのC&Cと復活したが約1ヶ月でまたNXDOMAINとなり現状も復活していない。

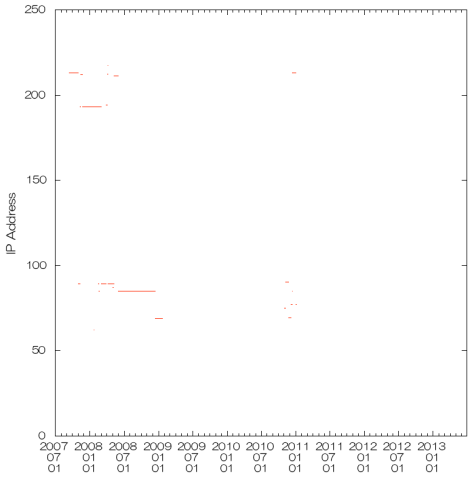


図 4 domain1

4.3.2 domain2

domain2 の A レコード登録状況を図 5 に示す。domain2はVirutのC&Cとして利用されたドメインであり、2 年程度で対策され一時期ドメイン管理業者の管理になっていたがその後復活している。2012年に入ってからも短期間ではあるが Virut の C&C として利用されるなどの想定不能な挙動を示しているが、これは攻撃者によるものなのかセキュリティ対策関連組織により sinkhole やその他の情報収集用に利用されているものなのか不明である。

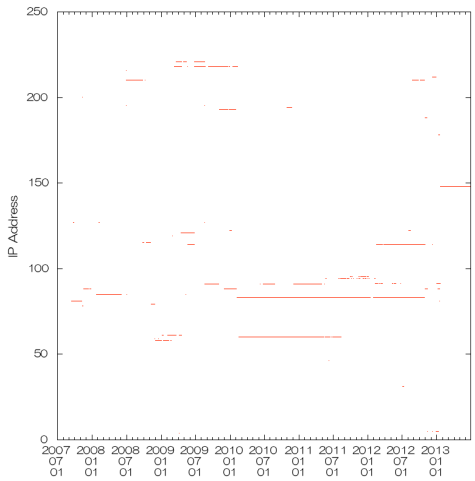
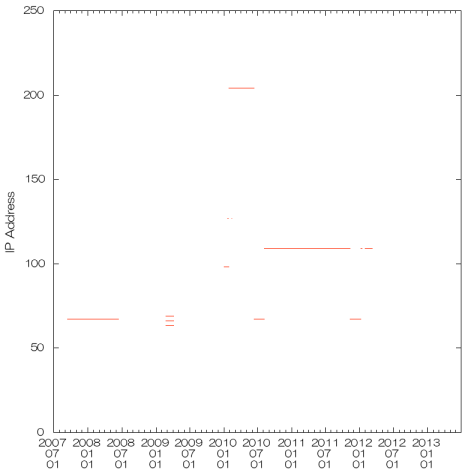


図 5 domain2

4.3.3 domain3

domain3 は CCC Dataset 2008[1],CCC Dataset 2009[1]、CCC Dataset 2010[1]でもっとも目立つドメインであり、関連するドメインが全部で 9 個抽出される。Domain3 の A レコードの登録状況を図 6 に示す。このドメインは 2007 年から 1 年間 C&C として利用されたドメインであるが、2008 年から 2009 年末までの間は NXDOMAIN になったり、短期間ドメイン管理業者に管理される状態が続いていたが 2010 年から 2012 年の間 Mariposa の C&C サーバーとして復活し利用されていたが、その後は NX Domain となったままである。



.

図 6 domain3

4.4 長期間利用されているドメイン

ほとんどのドメインが、断続的な利用であるなか、全観測期間利用され続けているドメインは 1 つあった。前述の ftp サーバーであり、マルウェア配布用サイトとして利用されつづけている。

4.5 超短期間利用ドメイン

最近の攻撃の流行ではよく見られる特性であるが、今回の解析対象のドメインでは 24 時間未満しか利用されなかったドメインは 2 つしかなかった。

4.6 再利用されないドメイン

過去に一度攻撃に利用されていたが攻撃期間終了後完全に使い捨てられ一般利用としても再度利用されないドメインは19 個であった。

4.7 再利用されるドメイン

残りの中で 10 個のドメインについては数ヶ月から数年の期間を開けて何らかの形で攻撃に再利用されたことを確認できた。ただし、セキュリティ調査団体による解析、検証の可能性もあるため明確に攻撃利用と判断できるものは少ない。

4.8 一般サイトへの転用の有無

所有者は転々としているものも含め、一般ユーザーが取得可能な状態になっているものもあるが、一般サイトに再利用されたものはなかった。

5 結果

解析の対象のドメインがマルウェア配布サイト、C&C用のドメインであったことが原因だと思われるが、想定よりも長期間にわたり利用されていたことがわかった。使い捨てられたドメインは3つだけであり、数ヶ月から数年の間隔をあけて断続的に利用され続ける期間は平均で3.84年であるため、ブラックリストには4年程度は登録したままにすることで、期間をおいての被害を未然に防ぐことができる。また利用期間が24時間未満だった例が2つあったが、このような超短期利用のドメインについては、発見から対策の時間をいかに短縮するかが重要となる。

6 今後について

単純にそのドメインが利用されているかいないかの判断は簡単であるが、攻撃に利用されているかいないかの判断については自動化を含め検討の余地がある。また今回の解析対象となっていない、スパム誘導で利用されるドメインやリダイレクタや攻撃サイトに利用されるドメインは、1日未満の期間で使い捨てられるものが多いことが知られているため、これらのドメインについての特性について同様の解析を行っていく。

参考文献

[1] 神薗 雅紀, 他:マルウェア対策のための研究用データセット ～MWS Datasets 2013～, MWS2013（2013 年 10 月）