Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

# インターネット接続型動的解析における IP アドレス使用法に関する考察

細渕嘉彦[†]　笠間貴弘[†]　吉岡克成[†]　松本 勉[†]

本稿では，マルウェアがアクセスする C&C サーバやダウンロードサーバ(以降，攻撃者サーバと呼ぶ)において，クライアント側の IP アドレスの使用頻度に基づくアクセス制御が行われていることを実際の攻撃者サーバへの接続実験により確認する．ハニーポットにより収集した 441 体のマルウェアが実際にアクセスする攻撃者サーバに対して接続実験を行った結果，使用頻度の高い IP アドレスを用いたクライアントからの接続要求に対して，一定期間アクセスをブロックするサーバの存在を確認した．このことから，インターネット接続型の動的解析では，毎回 IP アドレスを変更して解析を行うことが望ましいといえる．

# Consideration of IP Address Usage in Malware Sandbox Analysis with Internet Connection

Yoshihiko Hosobuchi[†]　Takahiro Kasama[†]
Katsunari Yoshioka[†]　and Tsutomu Matsumoto[†]

We carry out an experiment to investigate an access control capability of C&C servers and download servers with which malware communicate. In the experiment using 441 malware samples captured in the wild, we found two servers that indeed have a capability to block accesses from a client with a frequently used IP address. Consequently, we conclude that it is preferable to change an IP address of a sandbox when analyzing malware that communicate with such servers.

## 1. はじめに

ウイルス，ボット，スパイウェア等のマルウェアの挙動や特徴を解析し，有効な対策につなげるために，これまで多くの研究がなされている．特に，解析対象のマルウェア検体を解析環境内で実行し，その挙動を観測するマルウェア動的解析が注目されており[1-3,5-7,9,10,14-15,17,18,20,22]，インターネット上で実行ファイル等の検体を受け付け，自動的に動的解析を行い，解析レポートを検体投稿者に提供する公開型動的解析のサービス[14,15,18,20,22]も運用されている．

一方で，動的解析の解析環境として利用されることの多い仮想マシンやデバッガの存在を検知すると，動作停止や変更により解析を妨害するマルウェア[4]や，グーグル等の有名サイトに接続を試みることでインターネット接続の可否を調べ，隔離型の解析環境を検知する機能をもつマルウェア[7]の存在が報告されている．近年のマルウェアの中には，C&C サーバやダウンロードサーバなど攻撃者が制御する外部サーバ(本稿では，攻撃者サーバと呼ぶこととする)と連携して活動するものも多いため，解析環境をインターネット接続した上で動的解析を行う場合が多い．このようなインターネット接続型動的解析では，上述の解析環境検知に加えて，攻撃者サーバにおける解析環境検知についても注意する必要がある．

我々は文献[13]において公開型動的解析サービスに対する新たな解析環境検知の方法として IP アドレス特定攻撃の可能性を指摘した．IP アドレス特定攻撃では，攻撃者はまず自らが制御する攻撃者サーバへアクセスを行うダミー検体を用意し，これを公開型動的解析サービスに投稿することで，当該サービスの解析環境が用いている IP アドレスを特定する．公開型動的解析サービスが固定の IP アドレス帯を用いている場合は，攻撃者は特定された IP アドレスをもとに容易に解析環境を検知することができる．2009 年 7 月から 8 月にかけて我々が行った実験によると，現在運用中の 6 種類のインターネット接続型の公開型動的解析サービスは，実験当時，いずれも固定の IP アドレス帯を用いており，IP アドレス特定攻撃に対して脆弱であることがわかっている．

本稿では，文献[13]の結果を踏まえ，攻撃者サーバにおける解析環境検知の実態を調査する．具体的には，ハニーポットにより収集した実マルウェア検体 441 体を動的解析し，得られた 79 個の攻撃者サーバのドメインに対して継続的に接続要求を行い，セッション確立の成否を調べた．この結果，同一 IP アドレスを用いて一定回数接続を行うと，その後，一定期間 TCP セッションが確立できなくなる攻撃者サーバが存在することを確認した．このサーバでは，クライアントの IP アドレス毎のアクセス履歴に基づくアクセス制御をおこなっている可能性が高いと考えられる．したがって，インターネット接続型の動的解析においては，解析環境がインターネット接続に用いる IP アドレスを毎回変更して解析を行うことが望ましいといえる．

本稿の構成は次のとおりである．まず，2 章で関連研究について説明する．次に 3 章でマルウェアと攻撃者サーバの連携による解析環境検知について説明し，4 章で実マルウェアを用いた検証実験について説明する．5 章では実験結果について考察し，6 章でまとめを行う．

[†] 横浜国立大学
Yokohama National University

Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

## 2. 関連技術

### 2.1 マルウェア動的解析

マルウェア動的解析の手法は，解析環境のインターネットへの接続可否の観点から隔離型動的解析とインターネット接続型動的解析に分類される．

前者の例として，Norman 社による Norman Sandbox[20]がある．Norman Sandbox は多くのネットワークサービス(HTTP，FTP，SMTP，DNS，IRC，P2P など)を模擬した隔離環境において解析を行う．先行研究[5,7,10]でも仮想ネットワークサービスを用いた隔離型の解析が行われている．これらの手法の問題は，マルウェアが行う多種多様な通信に対して，インターネット上のサービスを完全に模擬することが困難である点である．特に，マルウェア間の通信や，マルウェアと攻撃者サーバ間の通信では独自プロトコルが用いられる場合もあり[8]，ネットワークサービスの模擬がさらに困難になっている．

一方，インターネットへの接続を許可する，インターネット接続型動的解析の例として CWSandbox[9,15,22]，Anubis[14]，Joebox[18]がある．インターネット接続型動的解析では，実際の感染時と同様にインターネット接続された環境においてマルウェアの挙動の観測を行えるという利点があるが，解析中のマルウェアやマルウェアからの攻撃が解析環境外に流出する恐れがある点や，攻撃者サーバに解析中のマルウェアが接続するため，攻撃者に解析環境を検知され解析を妨害される可能性がある点が問題といえる．このような解析環境検知については 2.2 節および 3 節にて詳説する．

前述の Norman Sandbox，CWSandbox，Anubis, Joebox は，インターネット上でマルウェア解析サービスとして一般に公開されており，誰でも解析対象のマルウェアを投稿し，解析結果を得ることができる．本論文では，このような場合を公開型動的解析と呼び，解析者が外部に公開せずに解析を行う場合を非公開型動的解析と呼ぶ．

### 2.2 マルウェアによる解析環境検知

マルウェアによる解析環境の検知手法は，ホストベースとネットワークベースに大別される．ホストベースの検知では，デバイスやドライバなどのハードウェアに関する情報，メモリや OS などの実行環境に関する情報，アプリケーションのインストール状況や実行状況，処理時間などの挙動情報など様々な情報を用いて，解析環境を検知する[4]．典型的には，解析環境として用いられることが多い仮想環境やデバッガの存在を検出し，解析を回避する機能がよく知られている．

一方，ネットワークベースの検知として，マルウェアが実行されている環境がインターネットに接続できるかを検査することで隔離型の解析環境を検知する手法がある．例えば，グーグル等の有名サイトに接続を試みることでインターネット接続の可否を調べ，隔離型の解析環境を検知する機能をもつマルウェアが存在する[7]．また，ダウンローダのように本体を攻撃側サーバからダウンロードするマルウェアも実質的に隔離型動的解析を回避する機能をもつといえる．

上記のネットワークベースの解析環境検知に加えて，攻撃者サーバにおいて解析環境検知を行う可能性がある．我々は文献[13]において公開型動的解析に対する新たな解析環境検知の方法として IP アドレス特定攻撃による解析回避の問題を指摘すると共に，実運用中の 6 種類のインターネット接続型の公開型動的解析サービスは，いずれも IP アドレス特定攻撃に対して脆弱であることを示した．本稿では，実際のマルウェアがアクセスする攻撃者サーバにおける，IP アドレスに基づいた解析環境検知の実態を調査する．

## 3. 攻撃者サーバにおける解析環境検知

本章では，攻撃者サーバにおける解析環境検知について考察する．まず，3.1 節において，マルウェア，攻撃者サーバ，動的解析環境といったエンティティの関係をモデル化し，攻撃者サーバにおける解析環境検知に関する問題設定を行う．次に 3.2 節において，想定される解析環境検知の手法について述べる．

### 3.1 モデル

今，ある攻撃者サーバrと，感染するとrに接続しrからの指示に従い不正活動を行うマルウェアxを考える．このとき，rに接続を試みるホスト群として，被害者ホスト群V，動的解析ホスト群D，監視用ホスト群M，その他のホスト群Eを考える．ここで被害者ホスト群Vは，システムの脆弱性やユーザの不適切な操作により意図せずにマルウェアxに感染した実際のマルウェア被害者のマシン群とする．一方，Dは解析を目的としてマルウェアxに意図的に感染した動的解析用マシン群とする．監視用ホスト群Mは動的解析とは異なる方法で攻撃者サーバrへの接続を行うホスト群である．監視用ホストの例としては，攻撃者サーバへのファイル要求をwget[16]等のソフトウェアによって模擬する方法[13]や，動的解析によって観測されたマルウェアの通信を模擬する擬似クライアントを用いる方法[12]がある[a]．その他のホスト群EはV，D，Mのいずれにも属さないマシン群であるが，具体例として，ランダムに生成された送信先にスキャンを行うワーム等に感染したホストが考えられる．

このとき，攻撃者は r に接続を試みるホスト群の中から，V を識別し V に対して不正活動を行うための指示を返信し，V 以外のホスト群に対しては指示を送らないことで，D および M による解析や監視の妨害を試みるものとする．上記の設定を図示した

a 実際，論文[13]で行った実験では，マルウェアが攻撃者サーバに対して送信する要求を wget[16]等のプログラムによって模擬し，継続的に攻撃者サーバを監視する機能をもつ解析システムの存在が確認されている．

Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

ものを図 1 に示す.

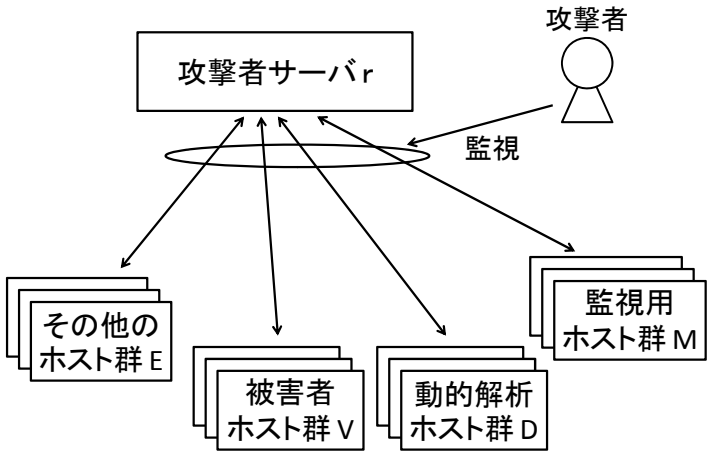


図 1　攻撃者サーバによる解析環境検知のモデル

### 3.2　解析環境の検知手法

3.1 節で説明したモデルにおいて，想定される解析環境検知の方法を説明する.

(1) **IP アドレスによる検知**　動的解析ホスト群 D および監視用ホスト群 M の検知を行う方法として, 各ホストが接続に用いる IP アドレスの使用頻度に基づく検知方法が考えられる．特に，D や M が固定の IP アドレスを用いて大量のマルウェア検体を解析する場合，攻撃者は D や M を統計的に識別できる可能性がある．また，文献[13]で指摘されたとおり，公開型動的解析に対しては，動的解析ホストおよび監視用ホストが用いる IP アドレスを特定する攻撃が存在しており，特定された IP アドレスに基づく検知が想定される.

(2) **通信機能の実装や性能の差異による検知**　被害者ホスト群Vと, 動的解析ホスト群Dおよび監視用ホスト群Mの通信機能の実装や性能に差異がある場合，攻撃者はこれらを識別できる可能性がある．例えば，TCP/IPスタックの実装の差異を判別するフィンガープリンティング技術[21,23]を用いて，Vと異なる実装を行ったMを検知する方法が考えられる．また，Dは仮想マシンによって実現される場合も多いが，攻撃者は仮想マシンに特徴的な通信挙動を検知することで，Dを検知する可能性がある[4][b].

(3) **通信の内容による検知**　攻撃者は，監視用ホスト群 M の通信と，実際のマルウェア x が行う通信の内容の差異から識別を行うことが考えられる．たとえば，マルウェア x が送信するデータを単純にリプレイするような監視用ホストに対しては，チャレンジレスポンスによるエンティティ認証を行うことで検知を行うことができる.

上述の検知方法の中で，(2)と(3)は動的解析ホストおよび監視用ホスト自体の実装の不備をついた検知方法であるため，動的解析ホストおよび監視用ホストを注意深く実装することで検知を回避できると思われる．一方，IP アドレスによる検知は解析環境の実装が完全であっても適用可能であるため，特に注意すべきである．そこで本稿では，特に IP アドレスの使用頻度に基づく検知に注目し，その実態を調査する.

## 4.　実験

本章では，攻撃者サーバにおける解析環境検知の実態を調査するための実験について説明する．本実験では，特に攻撃者サーバに接続する際にクライアント側が用いる IP アドレスの使用頻度に基づく検知に注目し，同一 IP アドレスを用いて連続的にアクセスを行った場合と，毎回異なる IP アドレスを用いた場合について，攻撃者サーバとの TCP セッション確立の成否を比較した.

### 4.1　事前準備

本実験では，ハニーポット Nepenthes を用いて 2008 年 6 月から 7 月の期間に収集した実マルウェア 441 検体を動的解析し，得られた通信ログ(検体が動的解析環境内で行った通信のパケットキャプチャデータ)から攻撃者サーバに関する情報を抽出し，調査を行った．具体的には，論文[11]において行ったマルチパス動的解析手法の評価実験により得られた通信ログを利用した．この通信ログから，攻撃者サーバ情報として，ドメイン名(または IP アドレス)，待ち受けポート，プロトコル(TCP/UDP)，送信したアプリケーションデータ(HTTP の GET 要求や IRC プロトコルによる C&C 通信など)を抽出した．その結果，79 種類のドメイン名(または IP アドレス)に対応する攻撃者サ

b 但し，文献[4]で示されている仮想マシン検知手法では，攻撃者は対象ホストに SYN パケットを数百程度送信し，TCP ヘッダオプションの time stamp 値の推移を観測する必要があるため，このような検知が実際に行われているならば，その事実を解析側が把握することは比較的容易と思われる．また，仮想化技術の近年の発展と普及は著しく，今後は被害者ホスト群 V として仮想マシンが利用されることが予想されるため，仮想マシンの検知による解析環境群の検知は攻撃者にとって，より困難になると思われる.

Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

ーバ情報が得られた．なお，プロトコルは全て TCP だった．

次に，これらの攻撃者サーバへの通信を再現するため，実験用クライアントを用意した．実験用クライアントは，攻撃者サーバ情報を入力とし，入力されたドメイン名の名前解決を行い，対応する待ち受けポートに対して接続要求を行う．接続が確立された場合は，対応するアプリケーションデータを送信し，指定期間tだけセッションを保持した後に切断する．また接続が確立されない場合は，指定時間tだけ接続要求を繰り返すようにした．上記の接続試行を指定回数iだけ繰り返し，その間の実験用クライアントの全通信をキャプチャした通信データを接続実験結果として出力する. さらに，接続試行毎に実験用クライアントが用いるIPアドレスを変更する機能を実現し，固定IPアドレスによる接続実験と変動IPアドレスによる接続実験に対応可能とした[c]．図 2 に実験の概要を示す.

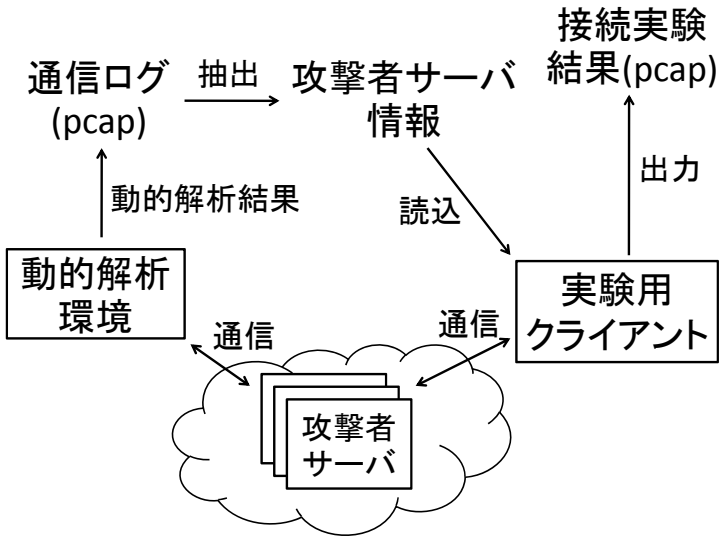


図 2 実験の概要

c 接続実験には，商用 ISP の変動 IP アドレスサービスを使用した．当該回線の PPPoE セッションを再接続すると，プロバイダから新しい IP アドレスが割り当てられることを利用し，IP アドレスの変更を行った．また，実験中に同一のアドレスが複数回割り当てられる場合があるため，実験に使用済みのアドレスを記録し，アドレス変更した際には，常に実験期間中で未使用の新しいアドレスを利用できるようにした．

### 4.2 攻撃者サーバへの接続実験

**実験方法** 4.1 節の事前準備において抽出された 79 種類の攻撃者サーバのドメインに対して，クライアントの IP アドレスとして固定 IP アドレスを用いる方法と，接続試行毎に IP アドレスを変更する方法で接続実験を行った. なお, 指定期間 t は 1 分とし，指定回数 i は 300 回とした.

**実験結果** 全 79 ドメインのうち，45 ドメインについては，送信元IPアドレスの固定・変動に関わらず，常にTCPセッションを確立することができた．また，33 ドメインについては，送信元IPアドレスの固定・変動に関わらず常にサーバからのSYN+ACKパケットが届かず，TCPセッションを確立することができなかった．唯一 1 つのドメイン(xx.xaxek.com)[d]については, 送信元IPアドレスを変動させた場合は毎回TCPセッションが確立できたのに対して，固定のIPアドレスを用いた場合には，TCPセッションが確立できる場合とできない場合が発生する現象が確認できた．なお，当該ドメイン名を名前解決すると，2 つの攻撃者サーバのIPアドレスが得られるが，そのいずれにおいても同様の現象が確認できた．また，これらの 2 つのサーバはいずれもIRCサーバであり，その通信内容からC&Cサーバであることがわかった.

### 4.3 詳細調査

**実験方法** 4.2 節の接続実験でクライアントの IP アドレスの固定・変動に応じてセッション確立の成否に変化が見られた攻撃者サーバ(xx.xaxek.com)に関して詳細調査を行った．具体的には，2 つの攻撃者サーバ(それぞれ攻撃者サーバ A，攻撃者サーバ B と呼ぶ)に対してそれぞれ，固定の送信元 IP アドレスを用いて指定期間 t を 10 秒として接続実験を行った．また，当該サーバに送信するアプリケーションデータとして，動的解析時に実際にマルウェア検体が送信したデータを送信する場合，固定のダミーデータ(文字列”hello”)を送信する場合, 何も送信しない場合の 3 通りで実験を行った.

**実験結果** 当該サーバに対してアプリケーションデータを送信しない場合，同一の送信元 IP アドレスを用いても毎回セッションが確立できた．しかしながら，実験用クライアントにより TCP セッションが切断されるまで, 当該サーバからクライアント側に対してアプリケーションデータが送られることはなく，TCP セッションを切断するために FIN パケットを送ると当該サーバから接続エラーメッセージがアプリケーションデータとして送信された.

次にマルウェア検体が動的解析時に送信したデータを送信した場合は，セッション確立の成否が変化した. 接続実験開始時からの時間経過と単位時間(100 秒)当りの TCP

d ドメイン名の一部を x でマスクしている

Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

セッション確立成功回数を図 3 (攻撃者サーバ A)), 図 4(攻撃者サーバ B)に示す. 図 3, 図 4 の通り，複数回連続してセッション確立が成功した後，一定時間セッションが確立できない期間があり，この期間を経過すると再び連続してセッション確立が成功するようになった．連続してセッション確立が成功する回数にはばらつきがあり，攻撃者サーバ A では平均 2.8 回，攻撃者サーバ B では平均 3.8 回であった．また，セッション確立が失敗し続ける期間(アクセスブロック期間と呼ぶこととする)の分布を図 5 に示す．なお，アクセスブロック期間の平均値は，攻撃者サーバ A が 716 秒，攻撃者サーバ B が 713 秒であった．なお，TCP セッション確立時にダミーデータを送った場合も同様の傾向が観測できたが，ここでは詳細は割愛する．

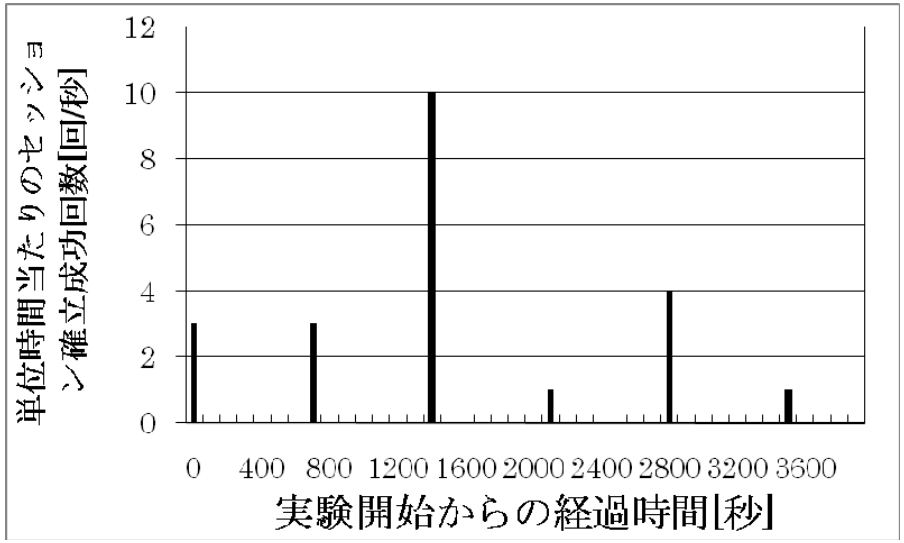


図 3　実験開始からの経過時間と単位時間当りのセッション確立成功回数
(攻撃者サーバ A)

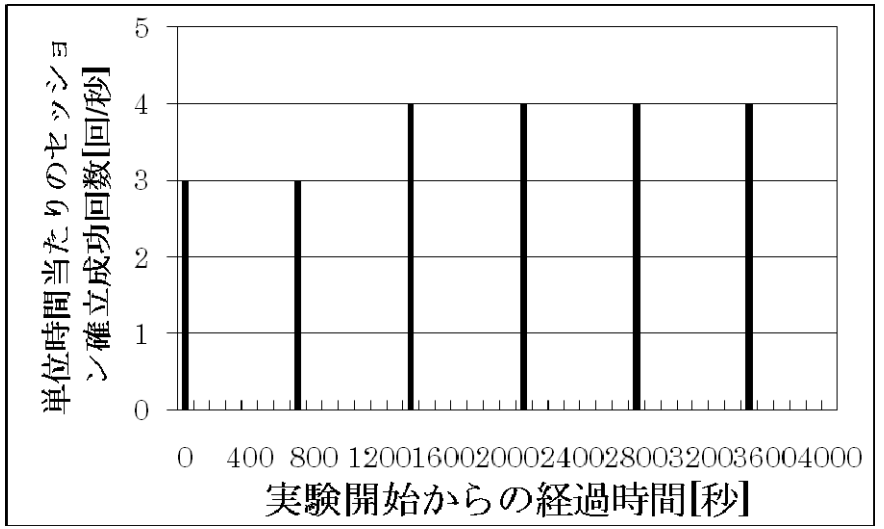


図 4　実験開始からの経過時間と単位時間当りのセッション確立成功回数
(攻撃者サーバ B)

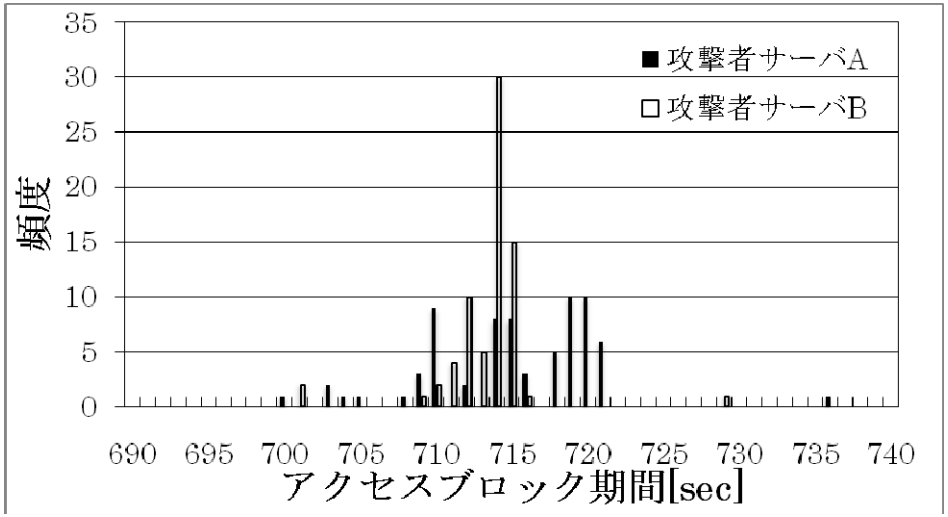


図 5　アクセスブロック期間の頻度分布

Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

## 5. 考察

### 5.1 IPアドレスの使用頻度によるアクセス制御が解析に与える影響

4 章の実験から，使用頻度が高い IP アドレスを用いたクライアントに対して一時的に応答を行わなくなる攻撃者サーバの存在が明らかになった．そこで，我々がこれまで解析済みの 3000 以上のマルウェア検体の中で当該ドメイン(xx.xaxek.com)へ接続するマルウェア検体を調べたところ，120 検体が該当することがわかった．これらの検体の MD5 値から Virustotal[24]により, Symantec と McAfee による検体名を調べた結果を表 1 に示す．表 1 から Virut, IRCBot, Sdbot の亜種を含む様々なマルウェアが当該サーバに接続する可能性があることが分かる. 固定 IP アドレスを用いてこれらの検体を動的解析する場合には，今回明らかとなったアクセス制御が動的解析の結果に影響する可能性がある. 特に同一送信元 IP アドレスを用いて複数の解析環境で並列解析を行う場合や多数の検体の連続解析を行う場合は，短時間に何回も当該サーバに通信しアクセス制御の影響を受ける可能性が高くなる．そのため，可能な限り頻繁に IP アドレスを変更し，動的解析を行うことが望ましいといえる．

表 1　IP アドレス使用頻度に基づくアクセス制御を行う攻撃者サーバと通信する検体名

| McAfee での検体名 | 検出数 | Symantec での検体名 | 検出数 |
|---|---|---|---|
| BackDoor-AWQ | 1 | Backdoor.IRC.Bot | 2 |
| Downloader-BZB | 3 | Backdoor.Sdbot | 1 |
| Exploit-DcomRpc.gen | 2 | W32.Bobax!dr | 7 |
| Generic BackDoor | 7 | W32.IRCBot | 12 |
| Generic Malware.dq | 5 | W32.IRCBot.Gen | 4 |
| Generic.dx | 3 | W32.IRCbot | 6 |
| New Malware.aj | 1 | W32.Linkbot.M | 1 |
| New Malware.dq | 1 | W32.Spybot.Worm | 19 |
| New Malware.n | 1 | W32.Trats!inf | 2 |
| W32/Bobax.worm.gen | 20 | W32.Virut!gen | 1 |
| W32/Nirbot.worm | 1 | W32.Virut.A | 1 |
| W32/Sdbot.worm | 2 | W32.Virut.B | 9 |
| W32/Sdbot.worm.gen.z | 4 | W32.Virut.R | 2 |
| W32/Trats | 2 | W32.Virut.U | 7 |
| W32/Virut.a | 1 | | |
| W32/Virut.gen | 26 | | |
| W32/Virut.gen.a | 26 | | |

### 5.2 アクセス制御のメカニズム

詳細調査では，当該サーバにアプリケーションデータを送った場合のみアクセスがブロックされたことから，アクセスブロックを行うか否かの判断は当該攻撃者サーバのアプリケーション層で行っていると思われる．一般にアプリケーション層では，ネットワーク層に比べて複雑なアクセス制御の判断基準を適用可能という利点がある．一方，アクセスブロック時には当該サーバから SYN+ACK の返信すら行われないことから，アクセス制御自体はネットワーク層で行っているものと予想される．ネットワーク層でのアクセス制御はアプリケーション層に比べて低負荷で行えるという利点がある．また，アクセスのブロックを解除するタイミングについては，図 5 よりアクセスブロック期間が 715 秒付近に集中的に分布していることから，アクセス制御を始めてから一定時間で解除するように設定されていると予想される．

## 6. まとめと今後の課題

本稿では，マルウェアが通信を行う攻撃者サーバにおける，IP アドレスに基づく解析環境検知の実態を調査した．その結果，クライアントの使用頻度に基づくアクセス制御を行っている攻撃者サーバが存在することがわかった．このことから，インターネット接続型の動的解析においては, 解析環境がインターネット接続に用いる IP アドレスを毎回変更して解析を行うことが望ましいといえる．今後の課題は，使用する IP アドレスを変動させた場合と固定した場合での動的解析結果の比較である．

## 参考文献

1) M. Bailey, J. Oberheide, J. Andersen, Z. M. Mao, F. Jahanian, and J. Nazario, “Automated Classification and Analysis of Internet Malware,” Proc. of Recent Advances in Intrusion Detection, RAID07, LNCS Vol. 4637, pp. 178-197, 2007.
2) U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel, "A View on Current Malware Behaviors," Proc. 2nd Usenix Workshop on Large-Scale Exploits and Emergent Threats, LEET'09, 2009.
3) U. Bayer, C. Kruegel, and E. Kirda, "TTAnalyze: A Tool for Analyzing Malware," 15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR), 2006.
4) X. Chen, J. Andersen, Z. M. Mao, M. Bailey, J. Nazario, “Towards an Understanding of Anti-virtualization and Anti-debugging Behavior in Modern Malware,” Proc. International Conference on Dependable Systems and Networks, pp 177 – 186, 2008.
5) D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, K. Nakao, "Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware's Network Activity," IEEE International Conference on Communications (ICC 2008), pp. 1715-1721, 2008.
6) E. Kirda, C. Kruegel, G. Banks, G. Vigna, and R. Kemmerer. "Behavior-based Spyware Detection." Proc. Usenix Sec, 2006.

Vol.2010-DPS-142 No.38
Vol.2010-CSEC-48 No.38
2010/3/5

7) S. Miwa, T. Miyachi, M. Eto, M. Yoshizumi, and Y. Shinoda, "Design and Implementation of an Isolated Sandbox with Mimetic Internet Used to Analyze Malwares," Proc. DETER Community Workshop on Cyber Security Experimentation and Test, 2007.
8) P. Porras, H. Saidi, and V. Yegneswaran. “A Foray into Conficker’s Logic and Rendezvous Points.” Proc. USENIX Workshop on Large-Scale Exploits and Emergent Threats, 2009.
9) C. Willems, T. Holz, and F. Freiling, "Toward Automated Dynamic Malware Analysis Using CWSandbox," Security & Privacy Magazine, IEEE, Volume 5, Issue 2, pp. 32 - 39, 2007.
10) K. Yoshioka, D. Inoue, M. Eto, Y. Hoshizawa, H. Nogawa, and K. Nakao, "Malware Sandbox Analysis for Secure Observation of Vulnerability Exploitation," IEICE Trans. Vol. E92D, No.5, 2009.
11) K. Yoshioka and T. Matsumoto, "Multi-Pass Malware Sandbox Analysis with Controlled Internet Connection," IEICE Trans. Vol.E93-A No.1, pp.210-218, 2010.
12) 笠間貴弘,吉岡克成,松本勉,山形昌也,衛藤将史,中尾康二,“疑似クライアントを用いたサーバ応答蓄積型マルウェア動的解析システム,”マルウェア対策研究人材育成ワークショップ 2009(MWS2009), 2009.
13) 吉岡克成,細渕嘉彦,織井達憲,松本勉,“マルウェア動的解析オンラインサービスの脆弱性,”コンピュータセキュリティシンポジウム 2009(CSS2009), 2009.
14) Anubis, http://analysis.seclab.tuwien.ac.at/.
15) CWSandbox, http://www.cwsandbox.org/
16) GNU WGET, http://www.gnu.org/software/wget/
17) gred, https://www.gred.jp/
18) Joebox, http://www.joebox.org/.
19) Nmap, http://nmap.org/
20) Norman Sandbox,http://www.norman.com/technology/norman_sandbox/
21) Remote OS Detection, http://nmap.org/book/osdetect.html
22) Sunbelt CWSandbox, Malware Research Labs,http://www.sunbeltsecurity.com/
23) the new p0f, http://lcamtuf.coredump.cx/p0f.shtml
24) Virustotal, http://www.virustotal.com/