資料９－２

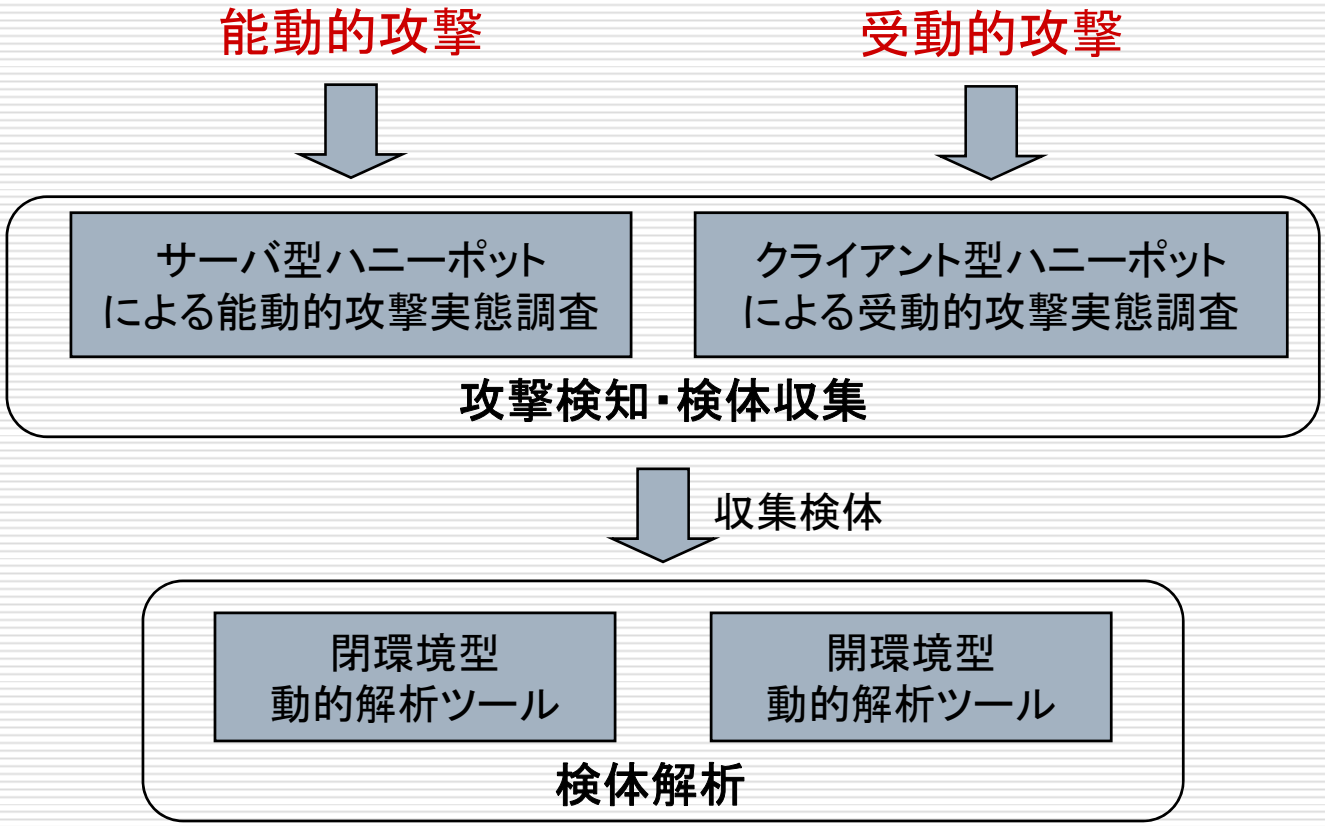
ボットネット実態調査

平成２０年６月１８日

NTT情報流通プラットフォーム研究所

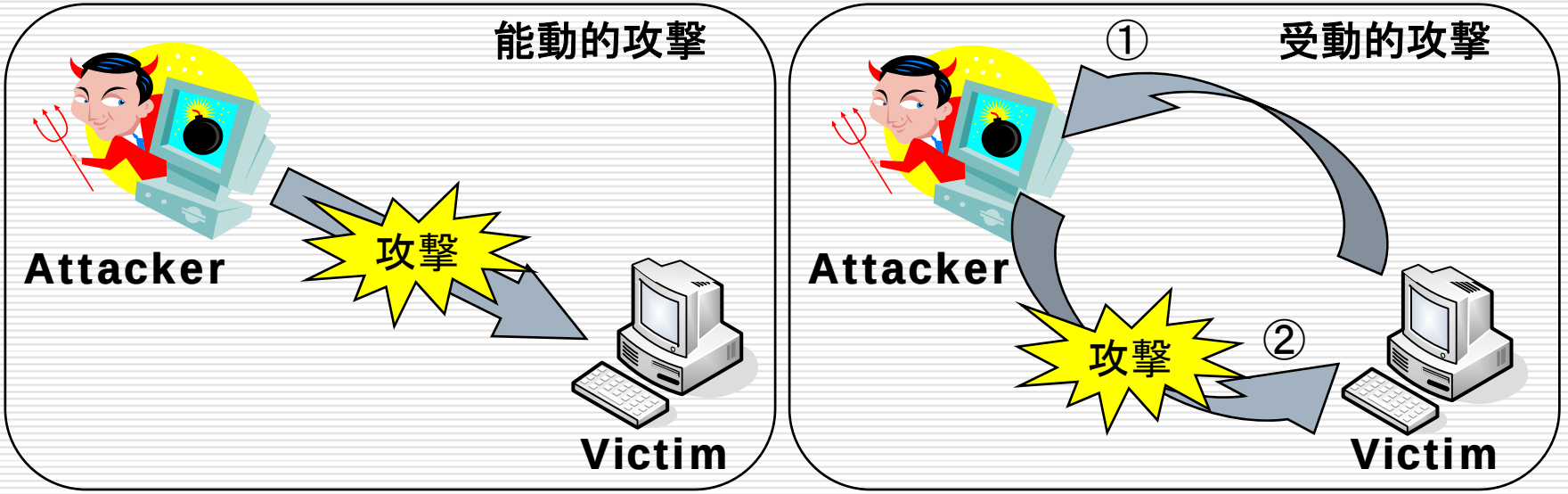
調査手法

- 2種類のハニーポットと、2種類の動的解析システムで、ボットネットの実態を「攻撃検知」・「検体収集」・「検体解析」の面から調査

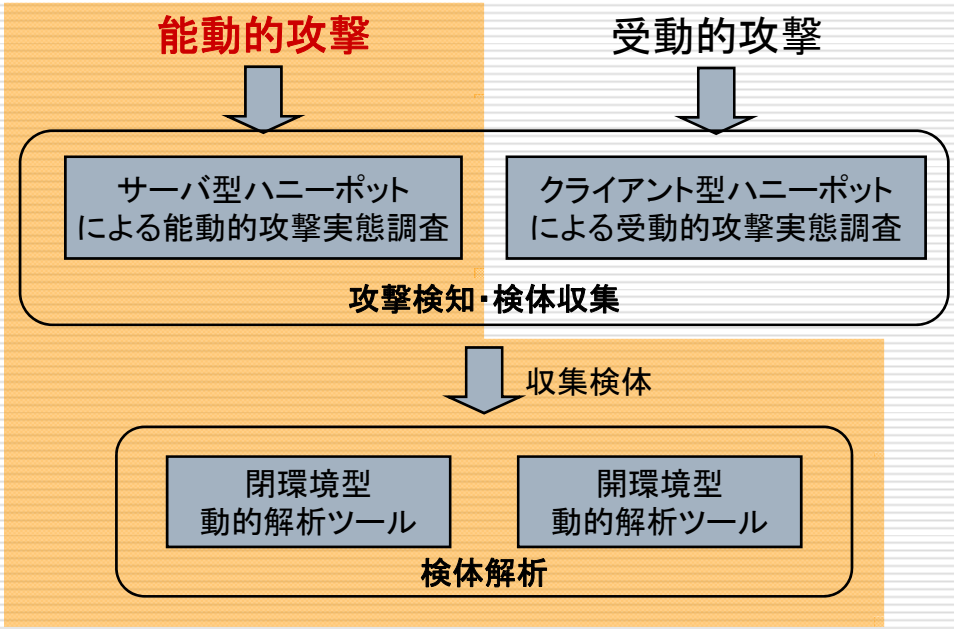


能動的攻撃と受動的攻撃

- 能動的攻撃
  - 利用者が特に操作を行わずとも、攻撃者が能動的に仕掛けてくる操作により実現される攻撃
- 受動的攻撃
  - 利用者側が行う何らかの操作を契機とし、攻撃者が受動的に行う攻撃

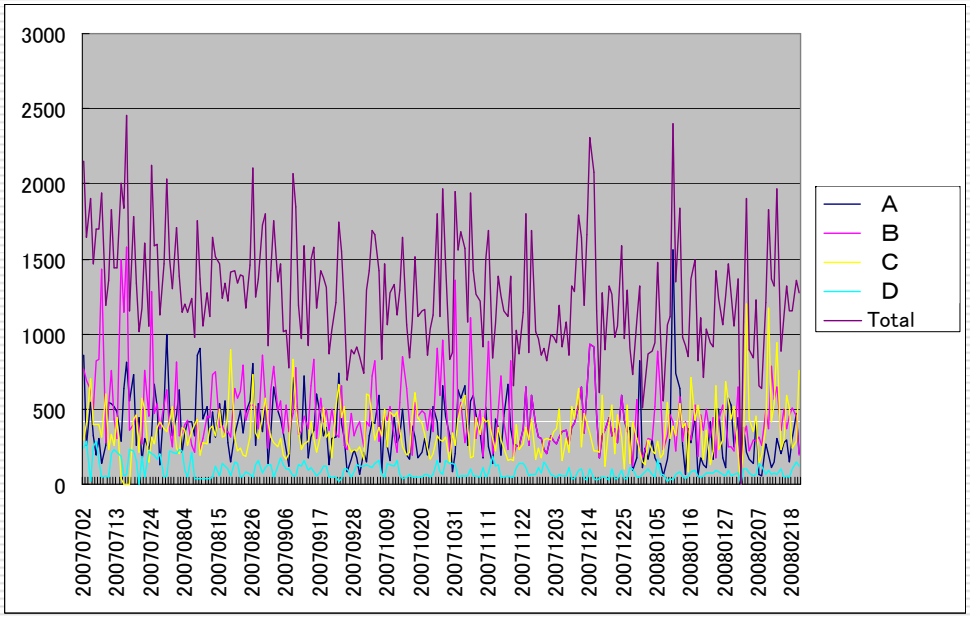


能動的攻撃調査結果

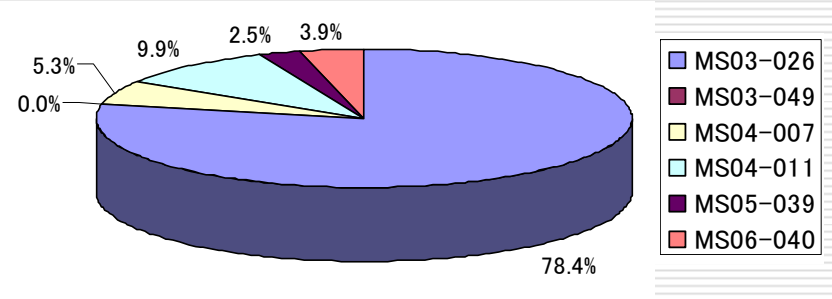


攻撃検知数推移

- ISP毎に攻撃検知数にばらつき
  - 少ないところでは一日平均92回、多いところでは476回の攻撃検知
- 攻撃対象脆弱性はMS03-026が約8割を占める
  - MS03-026は攻撃コードの完成度が高く、バージョン（XP/2000）や言語（JP/EN）に依存しない攻撃コードが流通している



攻撃対象脆弱性の割合



設置期間	2007.7.2～2008.2.20 （234日間）
総検体数	160,193検体
総検体種類数※	16,476種類

※・・・種類はSHA1のハッシュ値により分類

特徴的なShellcode

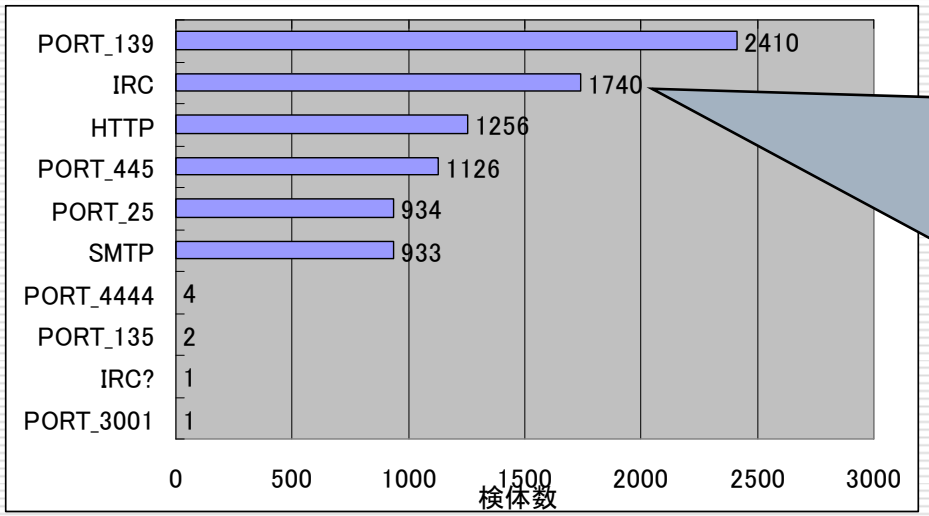
- Anti-Virusソフトを停止させるShellcodeを検知
  - Anti-Virusを導入しているが未パッチ、というユーザが感染してしまう
    - 一般にShellcode(メモリ上のデータ)はAnti-Virusソフトのスキャン対象外
  - Anti-Virusを導入していてもOSパッチを徹底すべき

```
20080217 17:02:13 [API]        CreateProcessW: C:¥WINDOWS¥system32¥net.exe:net stop "Norton
AntiVirus Auto Protect Service"
20080217 17:02:13 [API]        CreateProcessW:C:¥WINDOWS¥system32¥net.exe:net stop Mcshield
20080217 17:02:13 [API]        CreateProcessW: C:¥WINDOWS¥system32¥net.exe:net stop "Panda
Antivirus"
20080217 17:02:13 [API]        CreateFileW: c:¥1.vbs

    ...

20080217 17:02:13 [API]        CreateProcessW:C:¥WINDOWS¥system32¥cscript.exe:cscript
//Nologo /B c:¥1.vbs
```

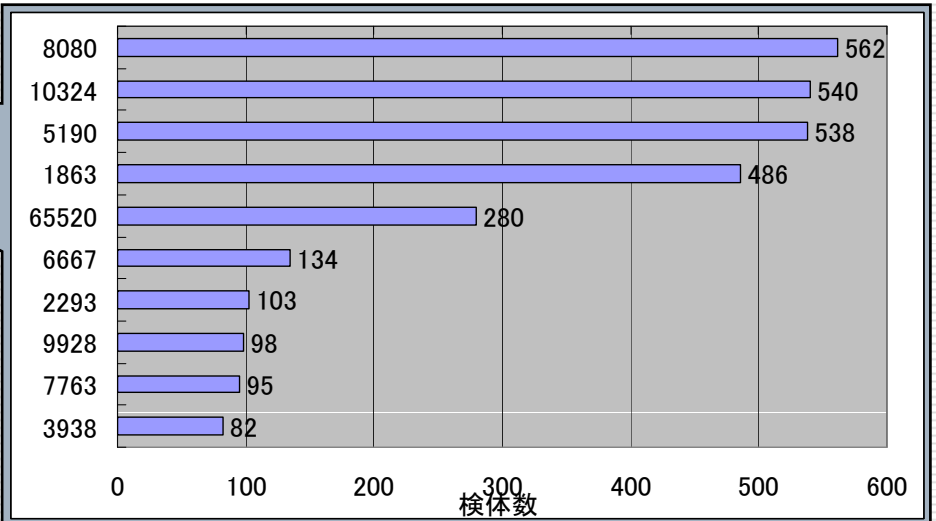
閉環境での動的解析

- ワーム（PORT139,445）とボット（IRC, HTTP）の活動が見られる
- IRCでの接続先ポート番号分布の上位に一般的なサービスで利用するポートがきている
  - ポート番号のみでのフィルタリングは困難

TCP8080･･･HTTP Alternate
TCP5190･･･AOL Instant Messenger
TCP1863･･･MSN Messenger



TCPプロトコル

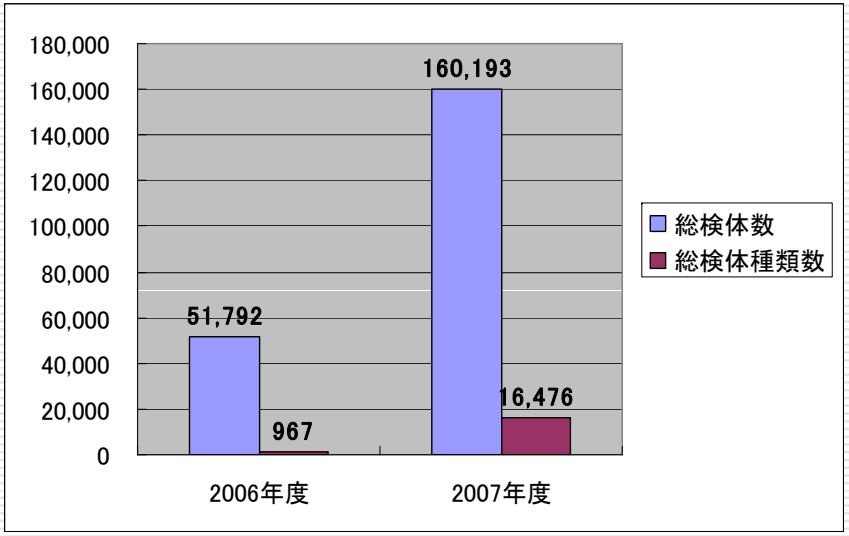


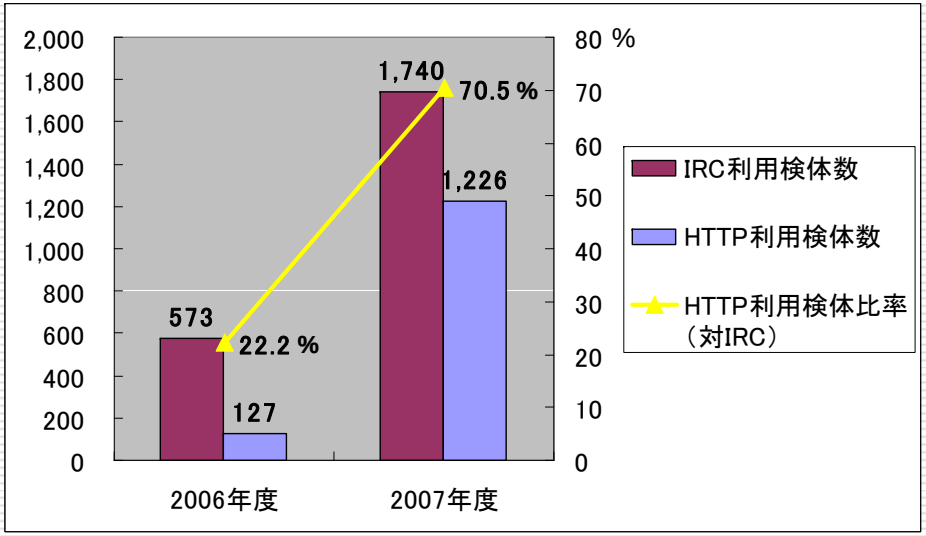
IRCでの利用ポート トップ10

前年度からのマルウェアの傾向変化

- 取得検体数増加
  - 監視対象となるIPアドレスが増加したことが影響
- 検体種類数増加
  - ポリモーフィックワーム※の流行が原因
- HTTP利用検体比率増加
  - ボットの使うプロトコルがIRCからHTTPへ移行している

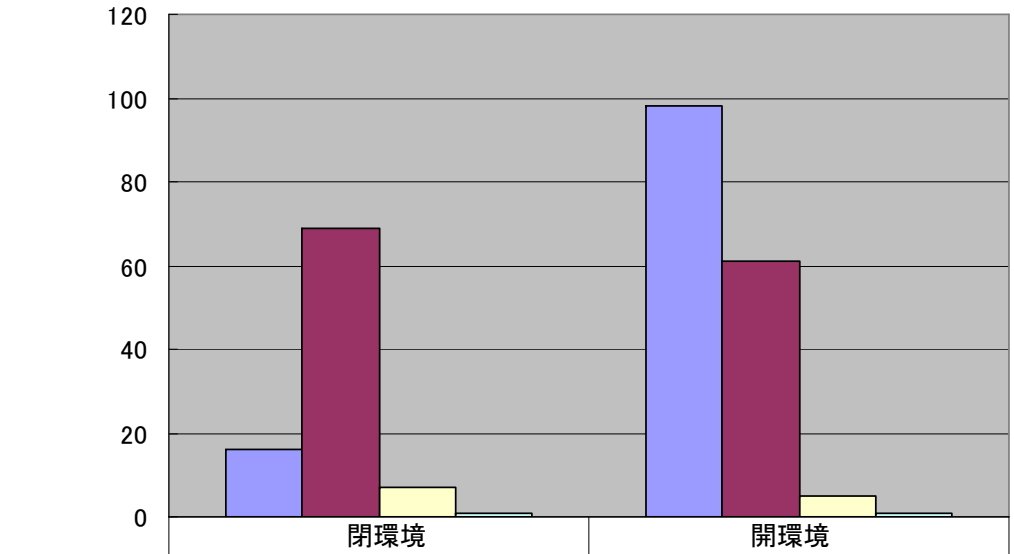
※：他PCへ感染時に、自分自身を改変するもの．改変後はハッシュ値が異なるため、ハッシュ値ベースのマルウェアの分類では別種類に分類される。





開環境での動的解析

- 開・閉環境での解析における取得接続先数の比較（同一50種類の検体での解析結果を比較）

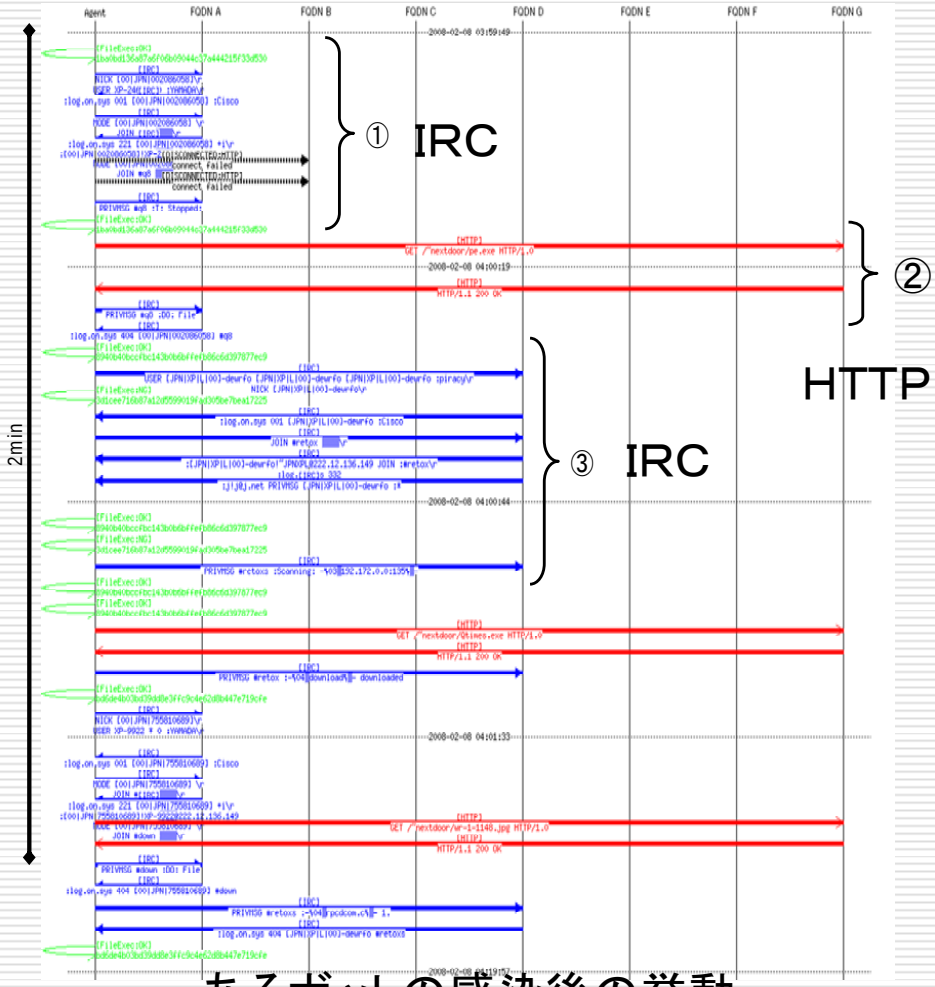


	閉環境	開環境
HTTP	16	98
IRC	69	61
SMTP	7	5
UNKNOWN	1	1

- IRC・・・閉環境の方が多い
  - ボットにハードコーディングされたバックアップ用C&Cサーバのアドレスを抽出したため
- HTTP・・・開環境の方が多い
  - 攻撃者からの命令に起因したHTTPの接続先（追加バイナリ取得等）を収集したため

ボットの活動シーケンス

- 開環境型動的解析により、ボット感染後の挙動追跡が可能
  - 活動シーケンスにはボット特有のものが確認される
    - IRCによる命令受信
    - HTTPによる追加バイナリダウンロード
  - 活動シーケンスに基づく対策が有効と思われる.



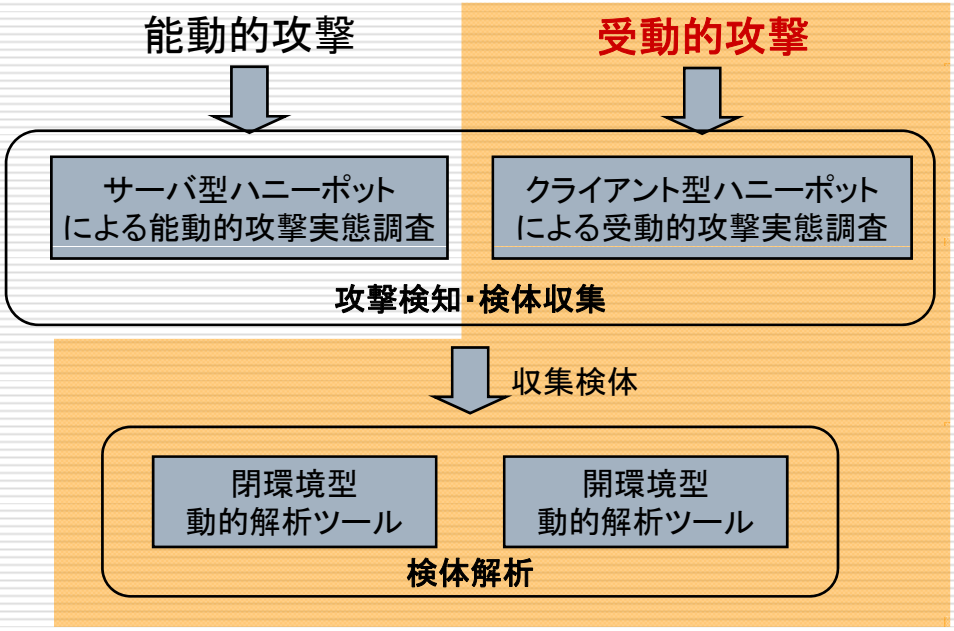
あるボットの感染後の挙動

考察

- 依然能動的攻撃が猛威を振るっている
  - Anti-Virusを止める特徴的なShellcodeが出現
    - 「Anti-Virus有り・パッチ適用無し」では不十分
    - Shellcodeを実行させないためにも、パッチの適用を推進する必要がある
- ボットは一般的なアプリケーションのポート番号を利用して通信を行う
  - ポート番号のみでのフィルタリングは困難
  - ペイロードまで見てフィルタリングする必要がある
- ポリモーフィックワーム※が蔓延
  - 優先的に対処すべきマルウェアを見逃さないためにも、マルウェアの分類が必要と考えられる
- 開環境型動的解析により実インターネットでのボットの活動を把握
  - 感染した場合に接続するアドレス（C&Cサーバ・追加バイナリダウンロードサイト）を収集
    - 感染時に見られる接続先に基づく対策に利用可能
  - ボットの活動シーケンスを収集
    - ボット特有の活動シーケンスに着目したフィルタリング等の対策が有効

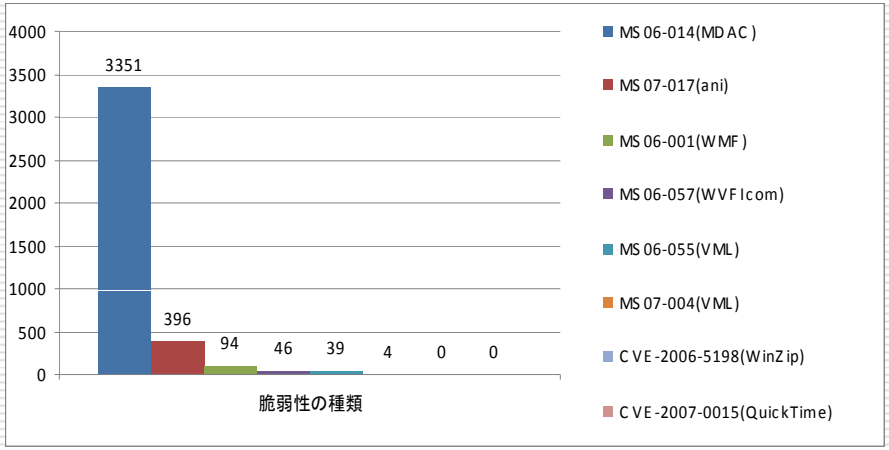
※：他PCへ感染時に、自分自身を改変するもの．改変後はハッシュ値が異なるため、ハッシュ値ベースのマルウェアの分類では別種類に分類される。

受動的攻撃調査結果

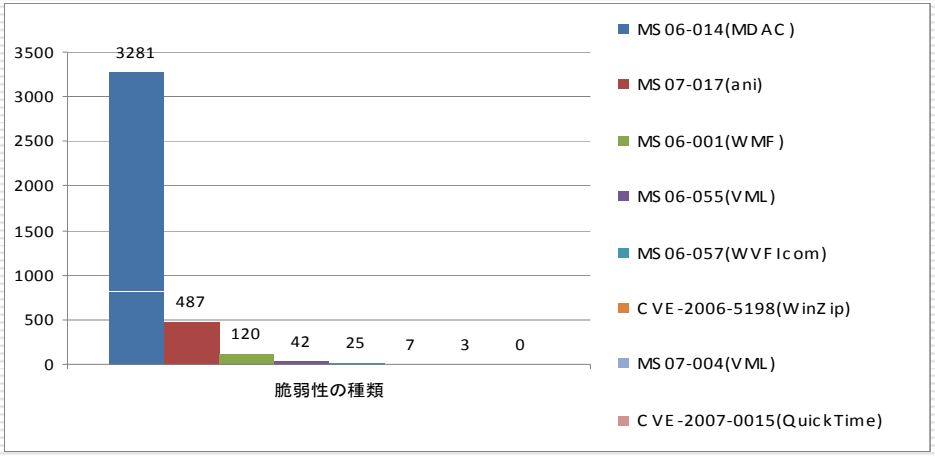


悪性URLリスト巡回結果

- ある悪性URLリストをクライアント型ハニーポットで巡回
  - 悪性リストに含まれるURL数・・・31,234URL
  - 検知数
    - 一回目（2008.1.22～27）：3,408URL（10.9%）
    - 二回目（2008.2.15～16）：3,324URL（10.6%）
- 攻撃に利用される脆弱性に偏り



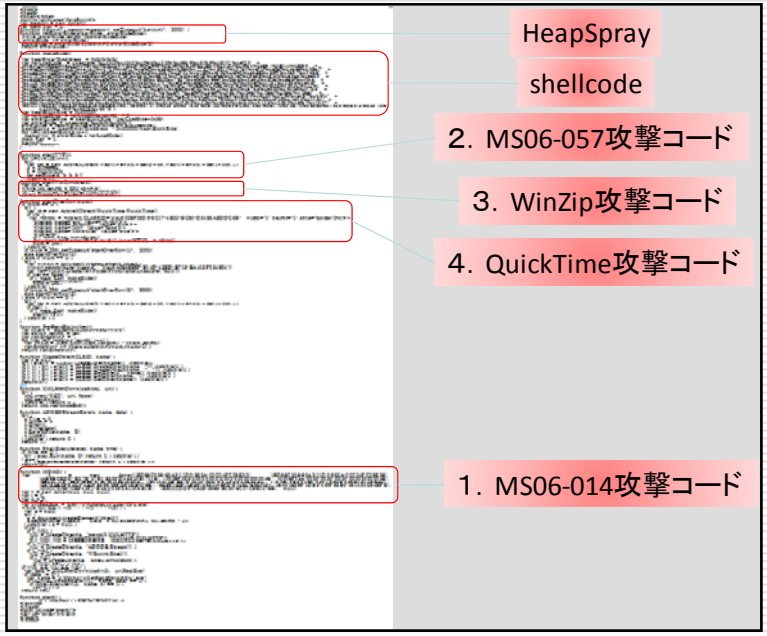
巡回1回目



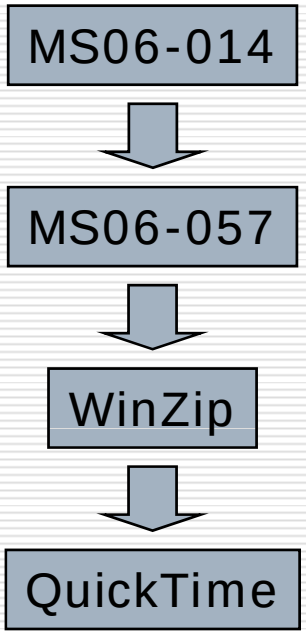
巡回2回目

攻撃対象脆弱性の偏りの原因

- MPackでは複数の脆弱性を連続的に攻撃
  - MS06-014（MDACの脆弱性）に対する攻撃は連続攻撃で一番最初に使われている
  - いずれかの攻撃成功すると、その後の攻撃は行われない



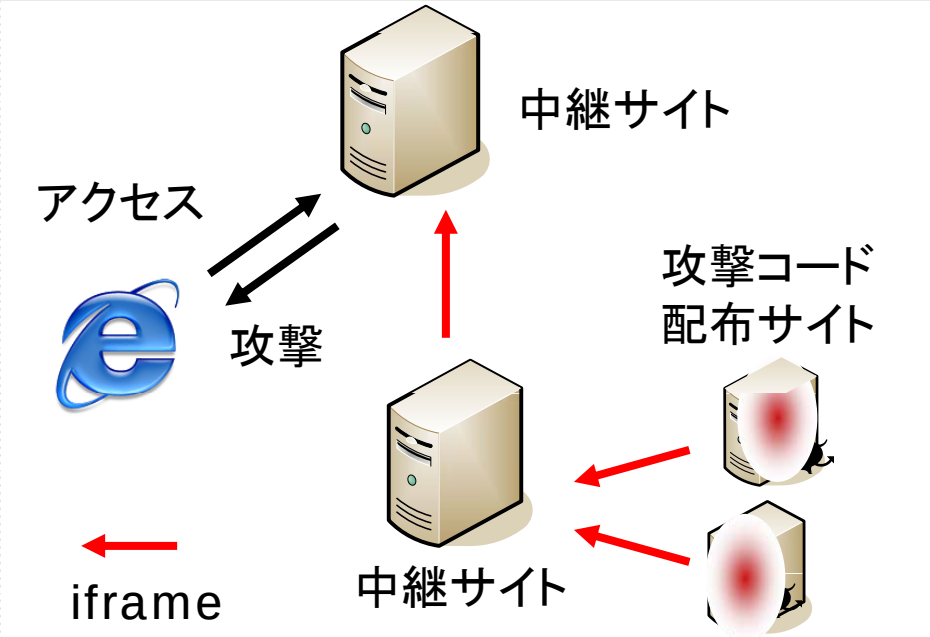
MPackにおける攻撃コード



攻撃サイト群のiframe構造

- iframe※によって構成される攻撃サイト群の構造を調査
  - 攻撃サイトは複数のWebサイトから構成されることが多かった
  - 検知したURLのうち、93.3%にはiframeが含まれていた

※iframeとはページの中に、別のページをフレームとして埋め込むことができる仕組み



今回の検知したURL※でのiframe利用状況

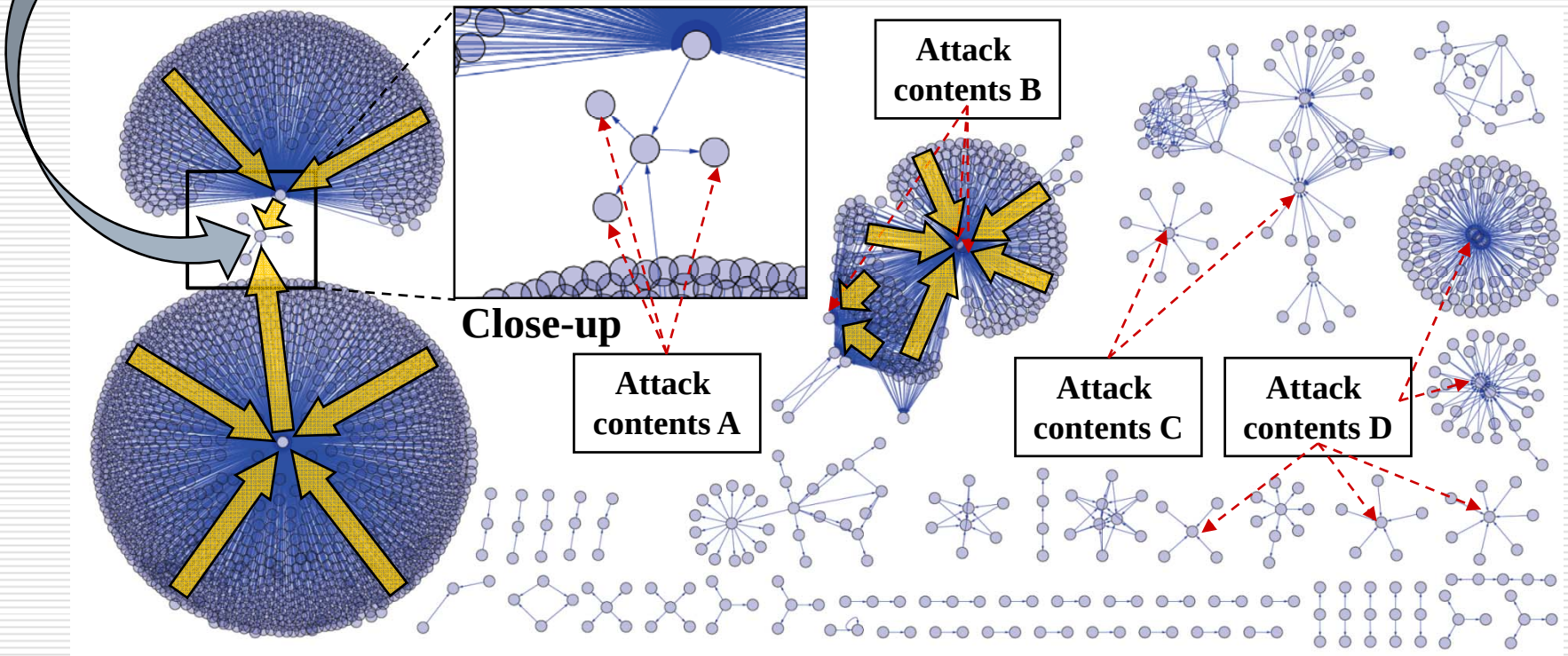
iframeが含まれるURL	2,466 URL（93.3%）
iframeが含まれないURL	176 URL（6.7%）

悪性URLリストから得られた攻撃サイト群のiframe構造

- 検知URL※のうち約88％が何らかのURLに集約
  - 集約点に対するアクセス制御で大半の攻撃を無効化できる

例）ここへの接続を遮断することで1,899URL（検知URL※の71.9％）の脅威を無効化

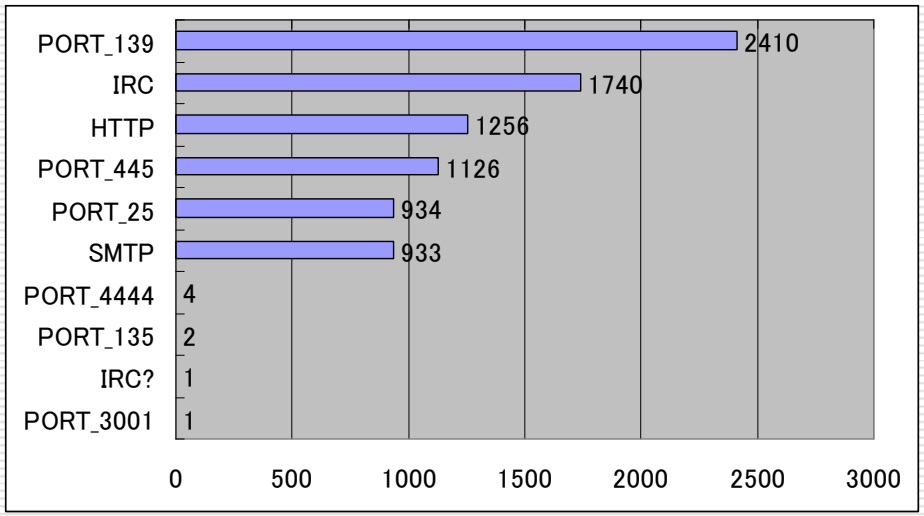
※・・・調査時に攻撃コンテンツが存在していた2,642URLが対象



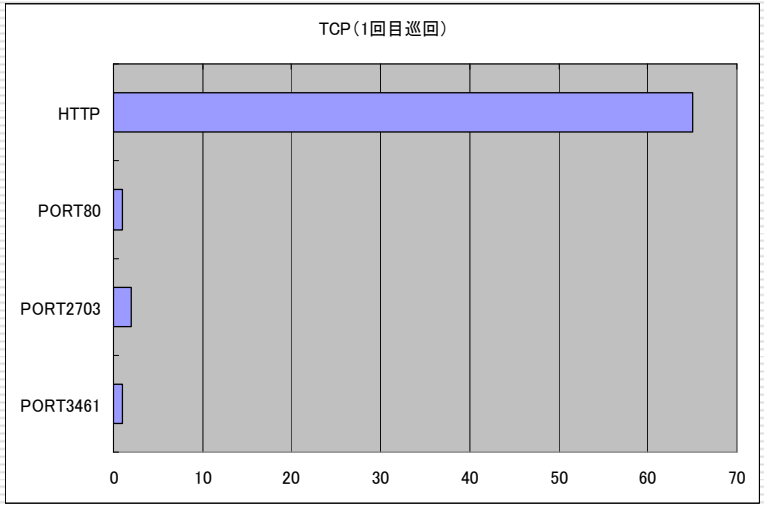
閉環境での動的解析

- HTTPによる通信を利用するものが主
  - 能動的攻撃で見られたIRCやTCP139，445への通信は見られない

TCPプロトコルの分布



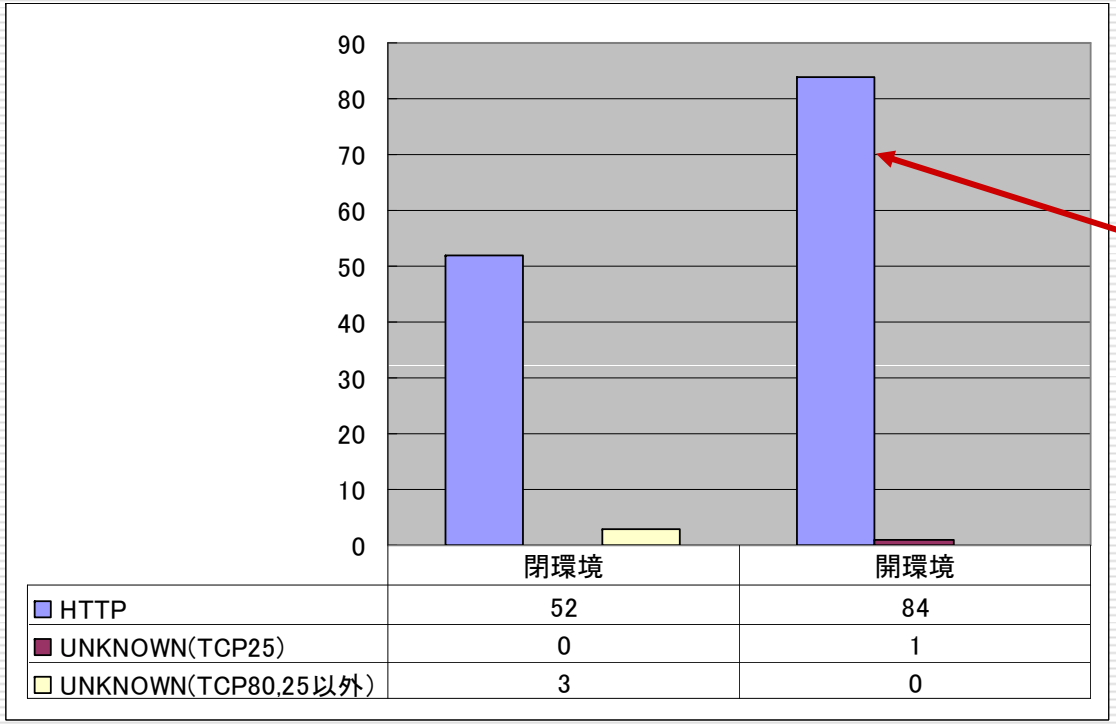
能動的攻撃での検体



受動的攻撃の検体

開環境での動的解析

- 閉・開環境での取得接続先数の比較（同一のマルウェア42種類での解析結果を比較）
  - 開環境により、追加バイナリ取得先のホスト名を取得



	閉環境	開環境
HTTP	52	84
UNKNOWN(TCP25)	0	1
UNKNOWN(TCP80,25以外)	3	0

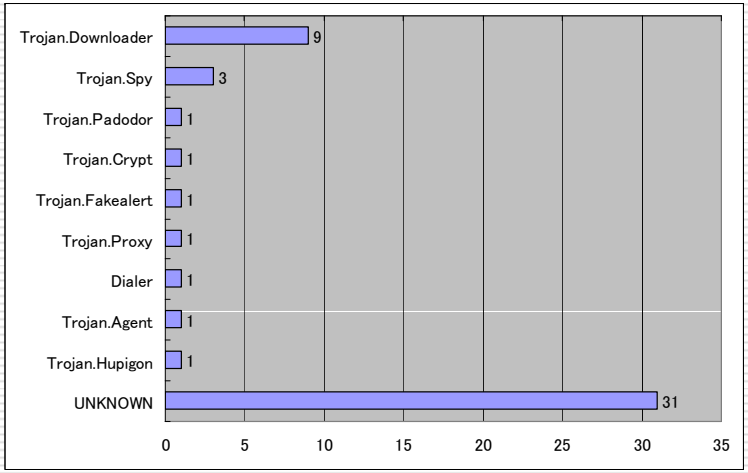
追加バイナリのダウンロードなどによる接続先を取得

※接続確認のためにランダムに生成されたホストへのアクセスは除いた

追加バイナリ取得状況

- 受動的攻撃での検体の方が、追加バイナリ数が多い
  - 受動的攻撃ではダウンローダと判定されるものが最も多い
  - 観測の中で、ダウンローダの多段構成が確認された

	解析検体数	解析期間	取得追加バイナリ数
能動的攻撃の検体	50種類	4日間	13種類
受動的攻撃の検体	42種類	6日間	50種類



Anti-Virusソフト※による受動的攻撃検体の追加バイナリ検査結果

※･･･ClamAVを利用

考察

- 攻撃サイト群のiframe構造を可視化
  - 検知URLの約88％は何らかのURLに集約
  - 集約点のURLに対するフィルタリング等を実施することで効率よく対策が可能
- 検知URLの約93％はiframeによる転送を利用
  - ブラウザでiframeを無効にすることは可能だが、利便性を考慮すると実現性は困難.
  - 加えて、攻撃者がiframe以外の手法で、利用者を攻撃コード配布サイトへ誘導することは容易.
- 受動的攻撃で取得した検体について、開環境での解析が特に効果的
  - 閉環境での解析より多くの接続先を収集
  - 1次検体がダウンローダであることが多いため、開環境型解析による本体収集が本当の脅威を知る上で必須

まとめ

- 攻撃検知・検体収集
  - 能動的攻撃・・・依然継続中
    - 新たなShellcodeの存在もあり、パッチ適用をより一層推進する必要がある
  - 受動的攻撃・・・脅威増大
    - 攻撃サイト群のiframe構造における集約点に対するアクセス制御は効果が大きい
  - 各々の攻撃手法に対応したハニーポットで調査・対策を進めていく必要がある
- 検体解析
  - ポリモーフィックワームに惑わされず効率的な解析を狙いとして、マルウェアの分類技術（自動化、可視化など）は必要不可欠
  - 解析技術者間での情報共有や感染者への注意喚起の迅速性、正確性を狙いとして、マルウェアのネーミングを統一することも必要.
  - 1次情報をすばやく情報を得るためには閉環境での解析が有効
  - 追加バイナリ・ダウンローダによる真の脅威把握、ボット感染時の接続先に基づく対策実施をより効果的にするには、開環境での解析が必要
    - 開環境型動的解析は、実インターネットにおけるボットの挙動、活動中のボットネットの挙動を把握できるため、対策に向けての効果が大きい
- マルウェア侵入経路の多様化・機能の高度化
  - 継続して、通信事業者・セキュリティベンダ等で連携して対策を進めていく必要がある