『Internet Week 2009 - *H1 インターネットセキュリティ2009* -』

脅威のトレンド2009
～ソフトウェア、プロトコル、ウェブサイトをめぐる動向～

一般社団法人

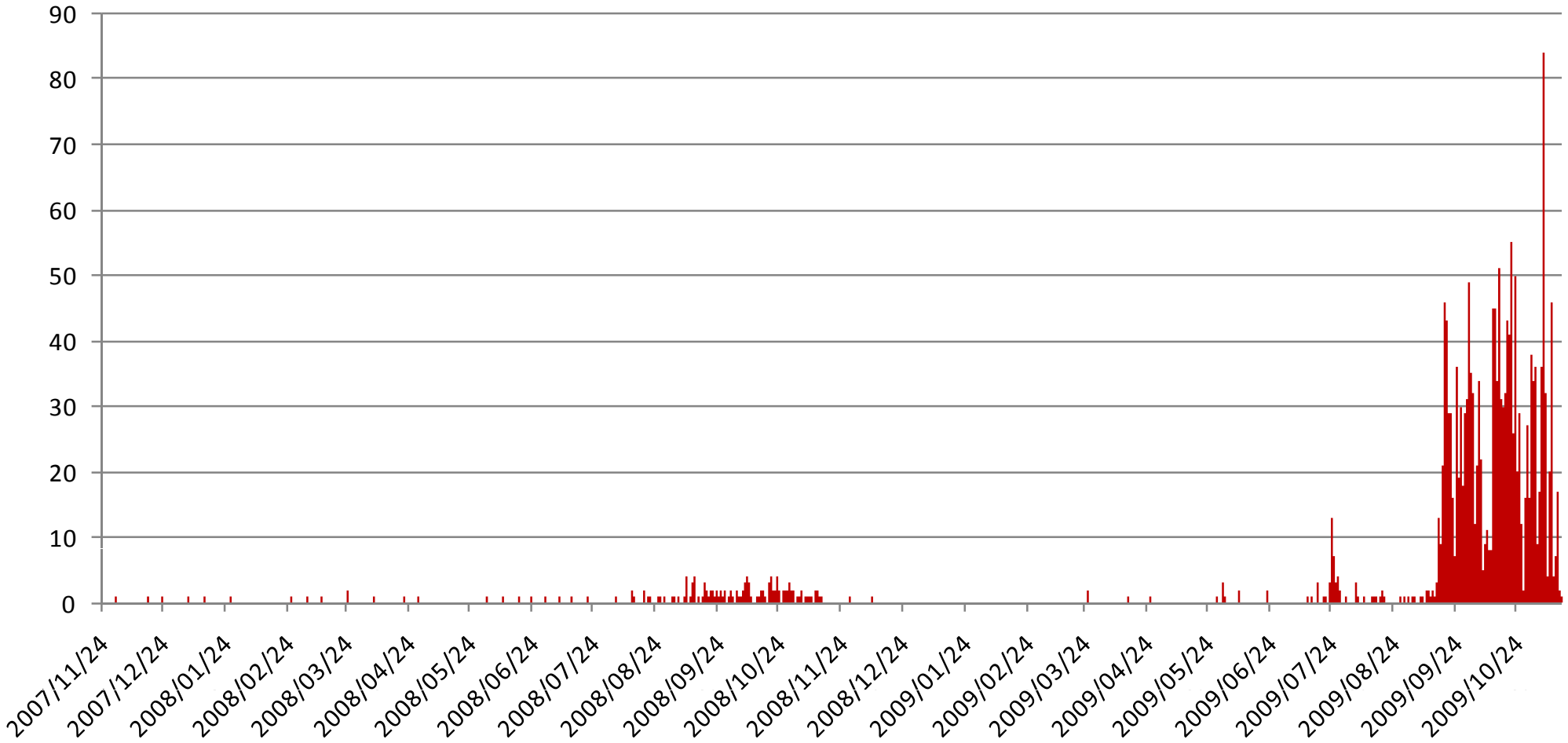
JPCERTコーディネーションセンター

2009年11月24日　　真鍋 敬士

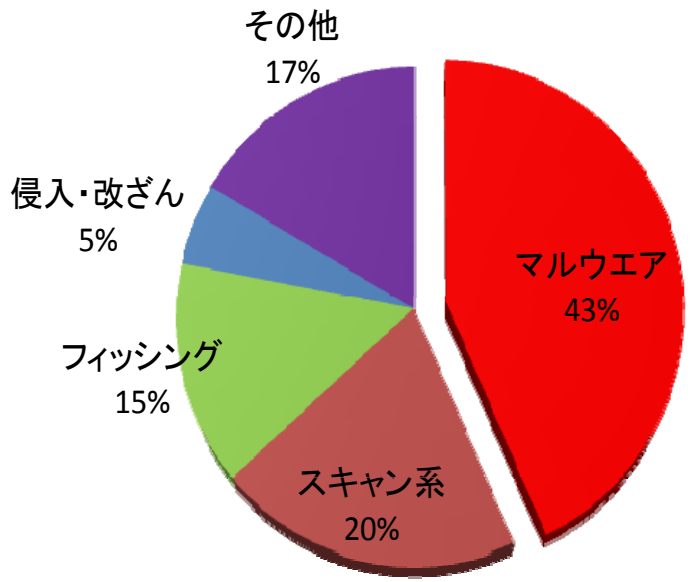
最近、気になっていること

JPCERT CC®

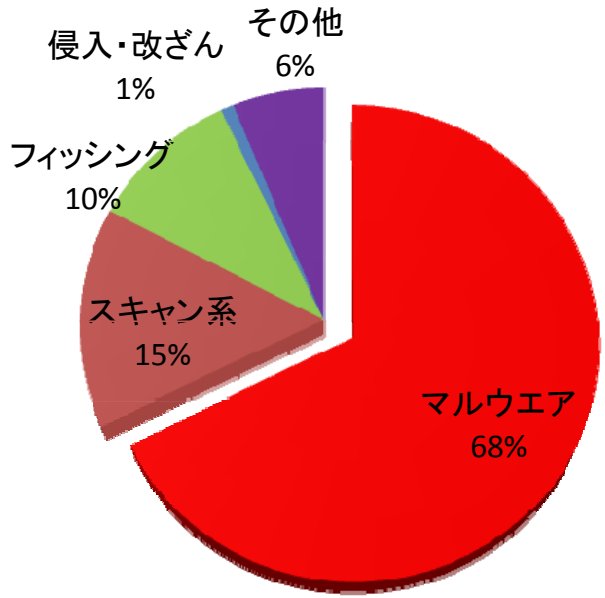
ある公開アドレスに届いたメールのうち実行ファイルが添付されていた数



JPCERT/CCに報告されたインシデントの傾向



インシデント報告件数割合(2009年4月～6月)



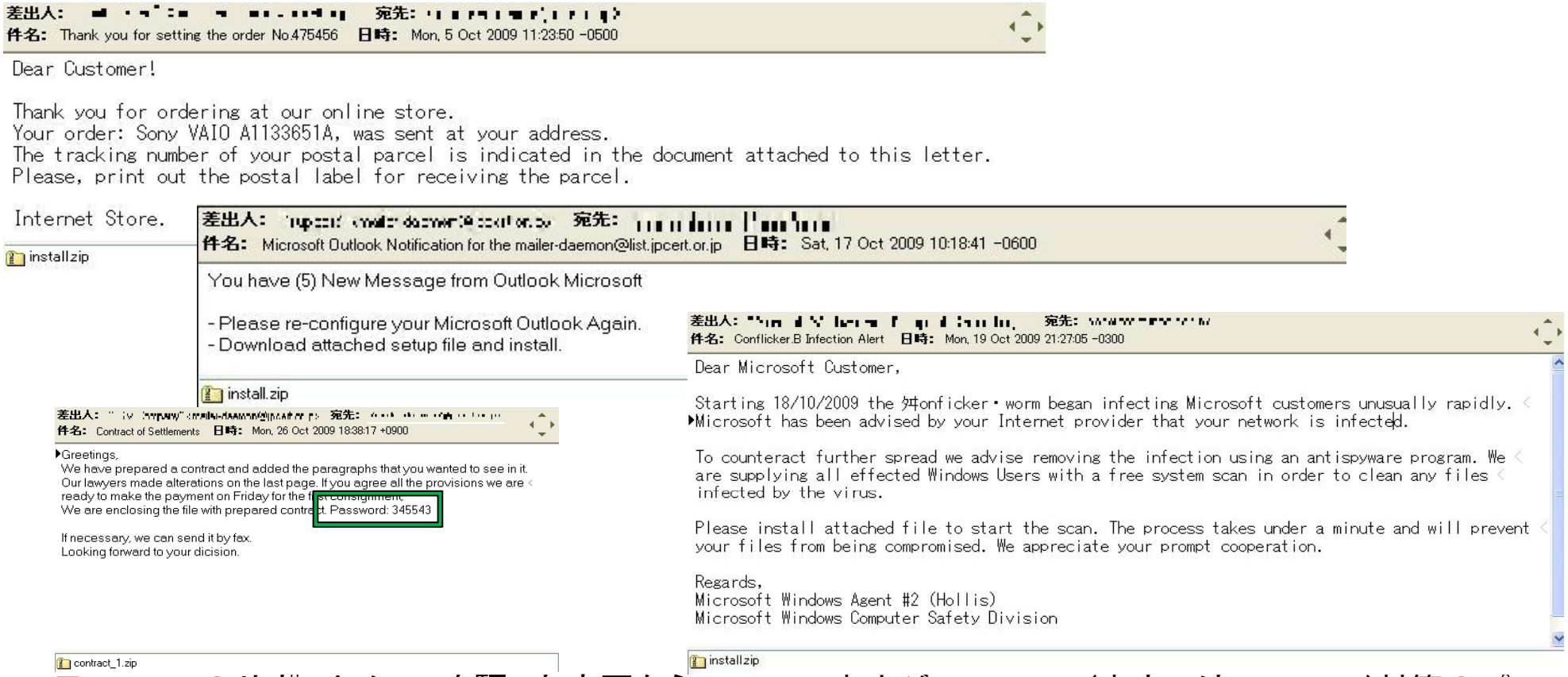
インシデント報告件数割合(2009年7月～9月)

http://www.jpcert.or.jp/ir/report.htmlより

攻撃の特徴

- 脆弱性の悪用
  - Adobe Reader/Acrobat
    - util.printf
    - Collab.collectEmailInfo
    - Collab.getIcon
    - JBIG2
  - Flash
    - 影響はFlashPlayerのみならず
      - Adobe Reader/Acrobat
      - Excelなど
  - Internet Explorer
    - MS09-032(ActiveX)
- JavaScriptが大活躍
  - PDF
    - JavaScript上の脆弱性
    - スプレイ用に
  - Web
    - ホスティングサイトへの誘導
    - 悪性コードの埋め込み

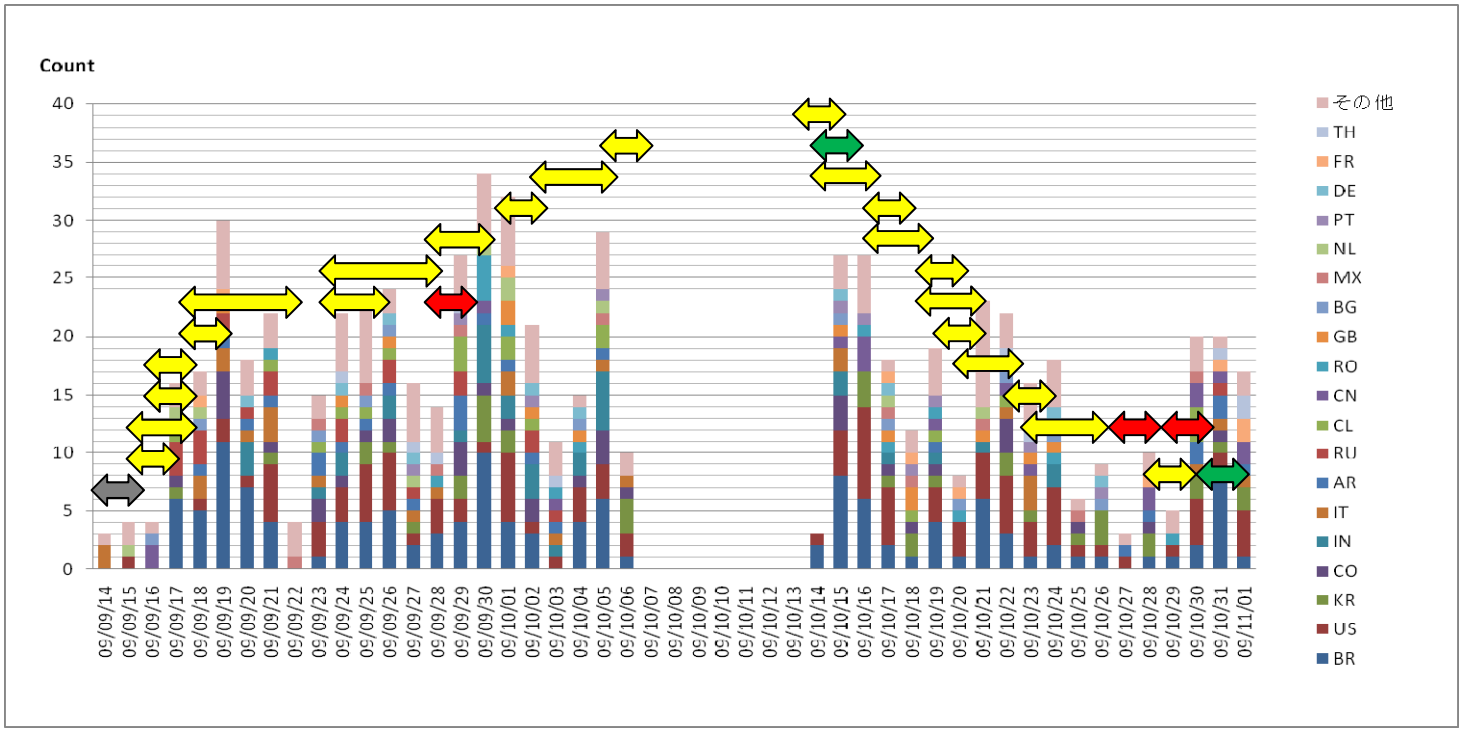
マルウエア添付メール

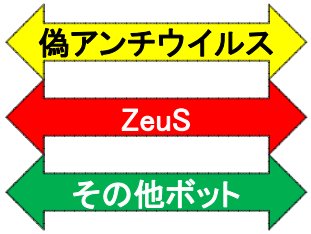


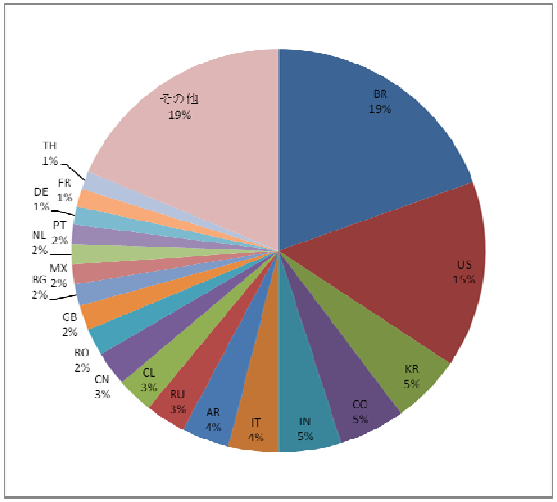
- VAIO のサポートメールを騙った文面から Outlook および conflicker (本文ではConficker)対策のパッチ適用を促す内容に変化
- ecard、DHLなどメールの内容が変化し継続的に受信を観測
- パスワードが記載されているものもあり、実際に Zip にパスワードがかかっていたケースも

-マルウエア添付メール-

マルウエア添付メールの傾向







地域	BR	US	KR	CO	IN	IT	AR	RU	CL	CN	RO	GB	BG	MX	NL	PT	DE	FR	TH	その他
件数	135	104	38	36	34	27	26	22	20	19	15	14	12	11	11	11	10	10	10	129

※件数 が 10件以上の地域のみ

- メールの Received ヘッダーの一番最初の IP アドレスから判定
- BR と US が約 3分の1 の割合を占めている

偽アンチウイルス

- 実行した場合、感染しているというメッセージを表示
- 外部へ接続し偽アンチウイルスの本体となる実行ファイルをダウンロードして実行(※接続先についてはベーシック認証がかかっていたため確認ができていない)

※ 感染している旨のメッセージと install.exe のアイコン

※ Antivirus Pro 2010 のインストール画面とダウンロードした実行ファイルのアイコン

偽アンチウイルス(インストール後)

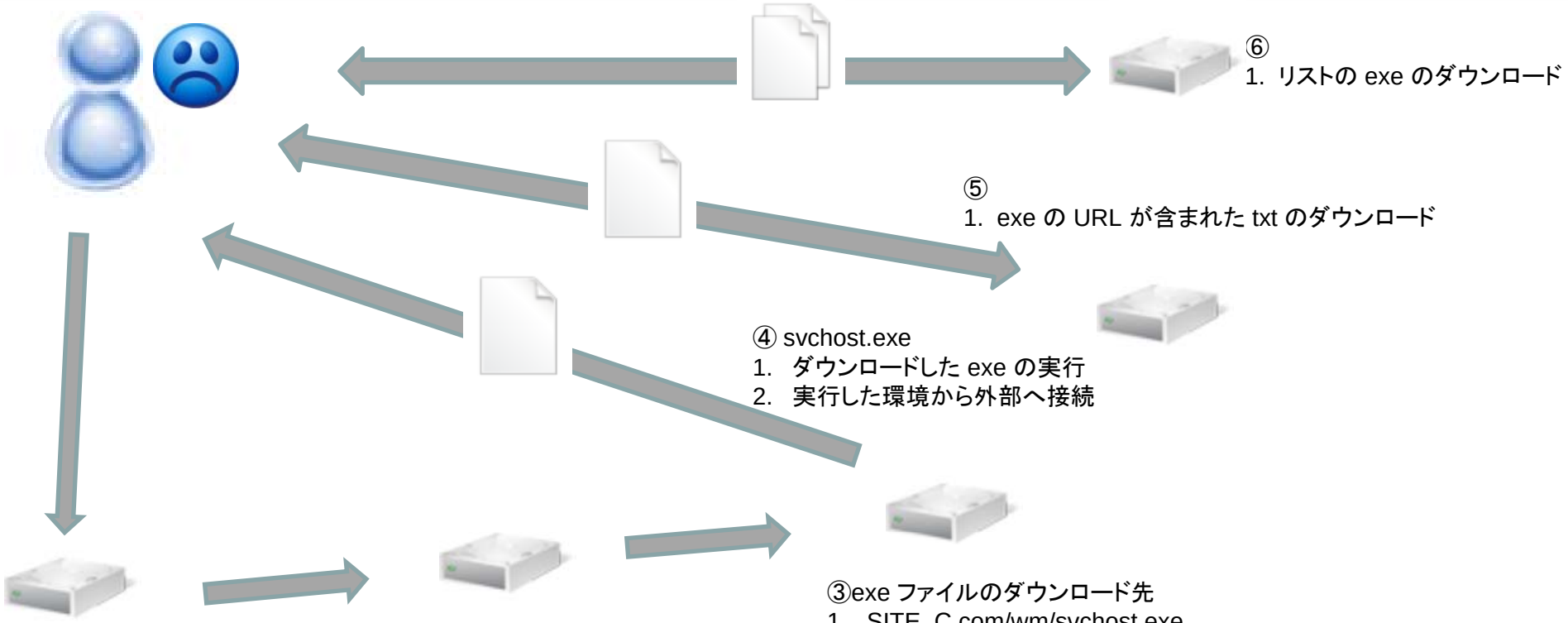
-マルウエア添付メール-

RAT(Remote Access Trojan/Administration Tool)

- PCの遠隔操作を可能にするツール
  - GUIによりマルウエアの作成やクライアントの管理が可能
- 主な機能
  - プロセス情報の取得
  - 特定プロセスの停止
  - 特定のウイルス対策ソフトのバイパス
  - マシンのシャットダウン、リモート
  - リモートからのデスクトップ操作
  - 任意のプログラムの実行
  - スクリーンショットの取得
  - Webカメラの操作
  - 音声の録音
  - キーロガー

- 関連記事
  - フォーティネットが総括：上半期のセキュリティ動向
    http://www.itmedia.co.jp/enterprise/articles/0907/30/news073.html
  - Tracking GhostNet: Investigating a Cyber Espionage Network
    http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
  - 「15万台が感染、国内でも被害多数」、ウイルスツール「Zeus」の脅威
    http://itpro.nikkeibp.co.jp/article/NEWS/20090827/336060/

改ざんされたWebからの誘導



⑥
1. リストの exe のダウンロード

⑤
1. exe の URL が含まれた txt のダウンロード

④ svchost.exe
1. ダウンロードした exe の実行
2. 実行した環境から外部へ接続

③exe ファイルのダウンロード先
1. SITE_C.com/wm/svchost.exe

② 脆弱性コードを含むスクリプトが存在するサイト
1. SITE_B.org/aa/a3.html?y10
   iframe にて 2 に接続
2. SITE_B.org/aa/index.html
   script タグにて 3 を実行
3. SITE_B.org/aa/go.jpg
   SITE_B.org/aa/go1.jpg
   4 に接続して問題なければ③へ接続
4. SITE_B.org/aa/load.jpg

① 最初の接続先
1. SITE_A.com/x.js
   iframe にて ②へ接続

MS09-032: Microsoft Video ActiveX Control の脆弱性を狙った攻撃

JSRedir-R(aka Gumblar)

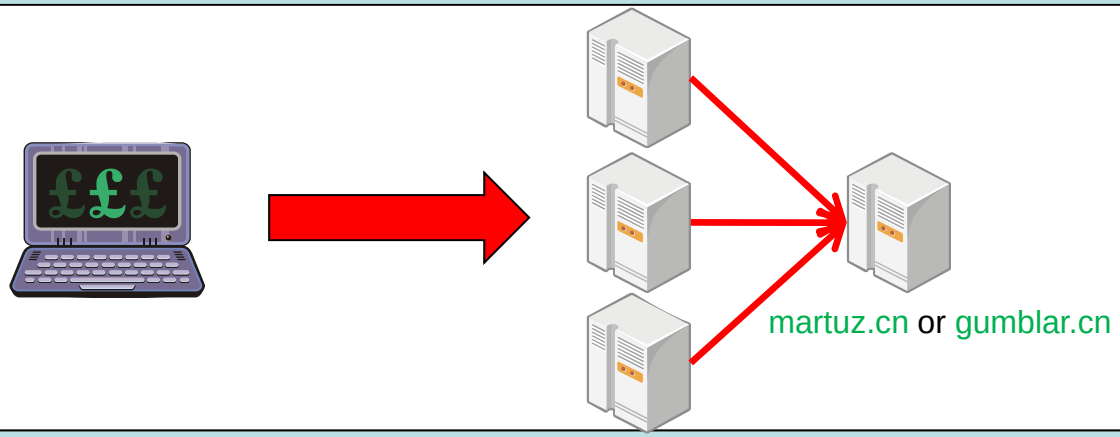
JPCERT CC®

- 共通的な挙動
  - ① Web改ざん
    - マルウエアホスティングサイトへ誘導するJavaScriptの埋め込み
  - ② ダウンローダ実行
    - 脆弱性を悪用して動作し、別のマルウエアをダウンロード
  - ③ マルウエア感染
    - アカウント情報盗聴等を行う

- 問題を大きくする要因
  - 技術的な難しさ
    - JavaScriptの難読化
    - マルウエアの多様性
      → パターンだけでは検知困難
    - 無数のマルウエアホスティングサイト
    - アクセス制限
      → 複数グループ
  - 事業者側での対応の限界
    - 不正なFTPアクセスの制限
    - 『改ざん』の判断
    - 繰り返される改ざん
      → 本質的な対策がなされていない

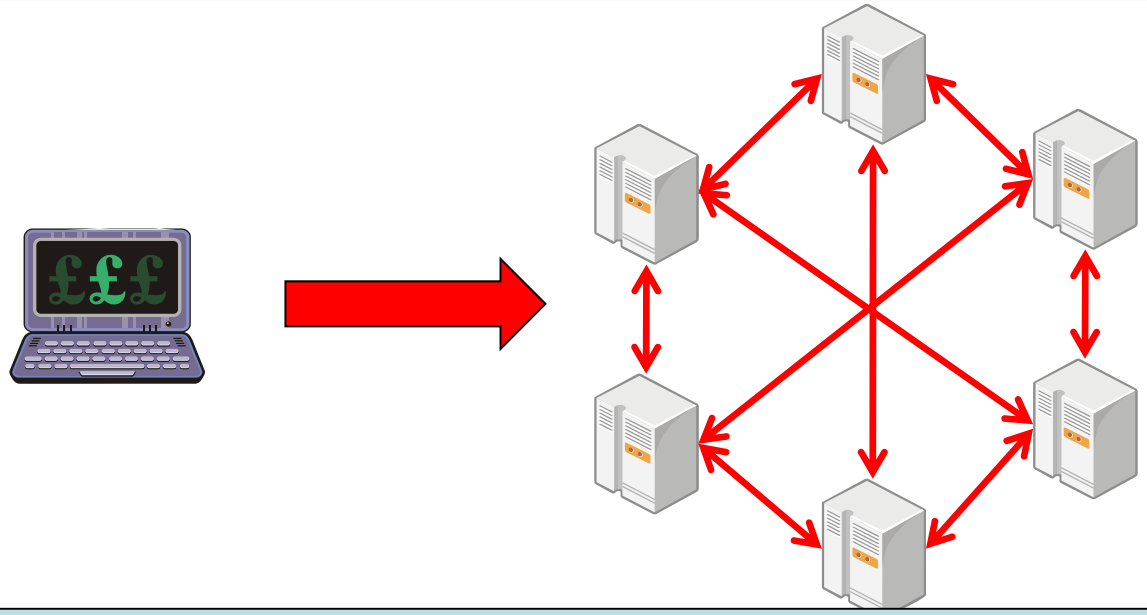
5カ月で形態が変化

旧 Gumblar



- 特に各ドメイン間の連携は確認できていない
- ドメイン停止により脅威が軽減

新 Gumblar



- 改ざんが確認されているサイトはリダイレクト元にも先にもなりうる
- 脆弱なシステムの輪が存在

対策はあまりにも基本的

- 一般ユーザ
  - OSやアプリケーションのアップデート
  - アンチウイルス製品の導入・運用
  - 最終ログイン日時等のアカウント情報への関心
- サイト管理者
  - Webコンテンツの定期・不定期の確認
  - 定期的なログの確認
  - パスワードの適切な運用
- 関連組織・事業者
  - 一般ユーザやサイト管理者への注意喚起
  - 組織間での情報共有

これから…

- Webからの誘導は引き続き攻撃の主流に
  - サーバ側でのセキュリティ対策が問われる
    - Webアプリケーションの脆弱性をどのように減らすか
    - FTPアカウント等、運用上の改善
    - Windows以外のマルウエアにも注目
  - 堅牢な攻撃システムの構築
    - 可用性の向上
    - 追跡を困難にする仕組み
- デスクトップの脆弱性対策
  - ベンダの対応如何が被害規模に直結
    - Windows 7の登場により古い環境が減る☺
    - サードパーティ製品でも自動更新が広まる

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- Web: http://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web:　http://www.jpcert.or.jp/form/