

『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

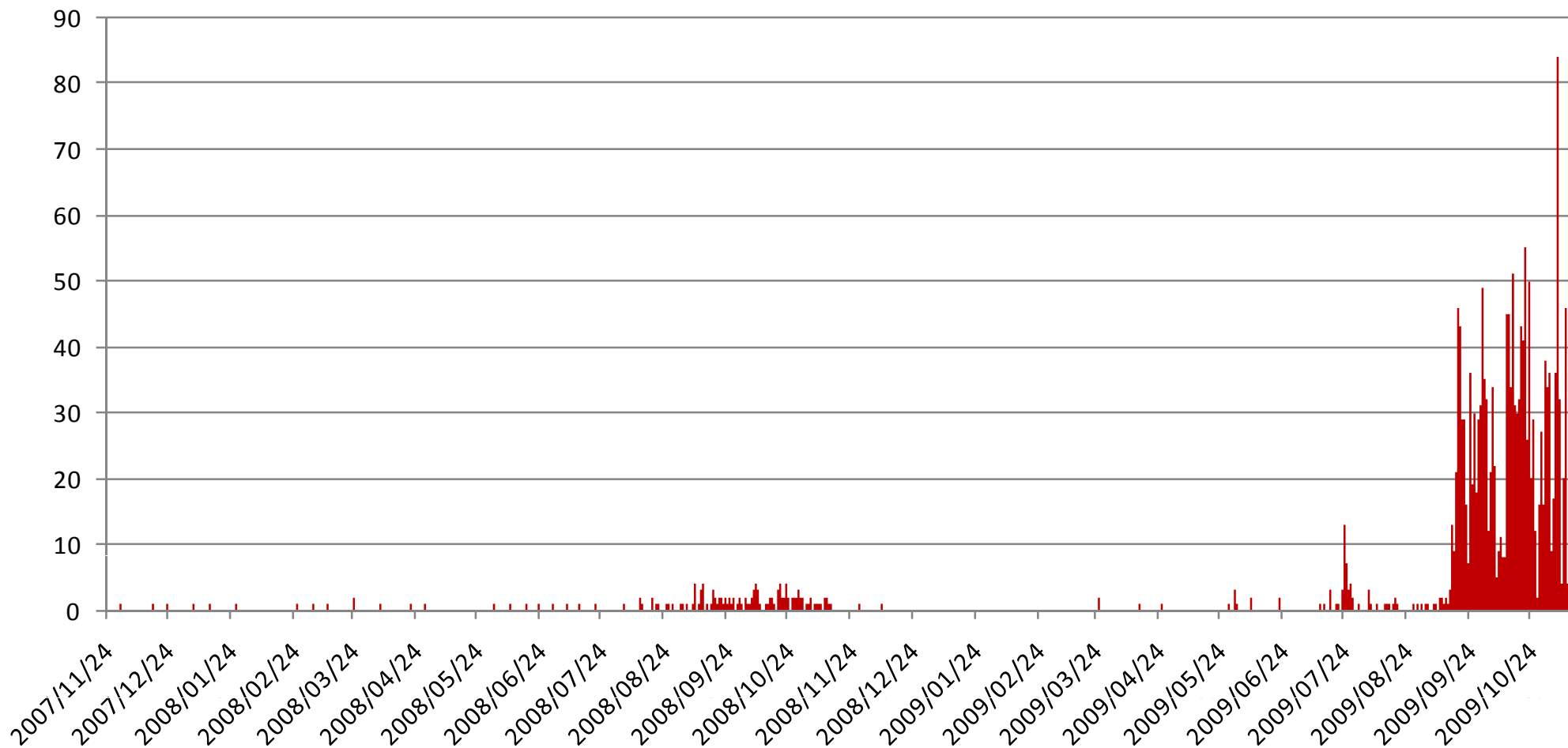
JPCERTコーディネーションセンター

2009年11月24日

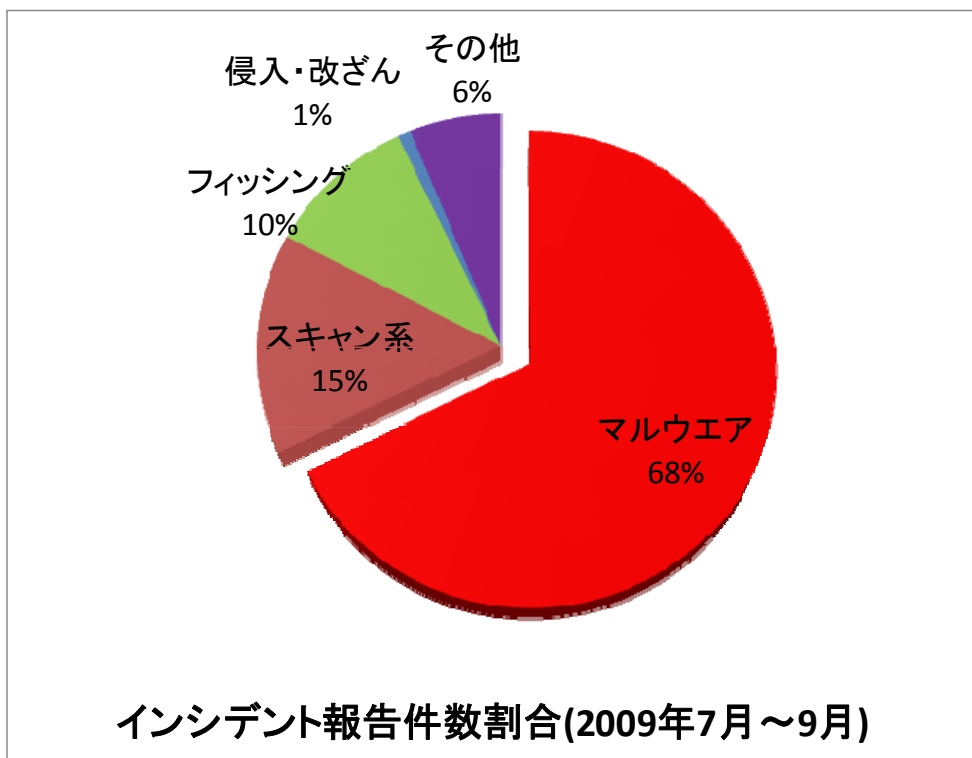
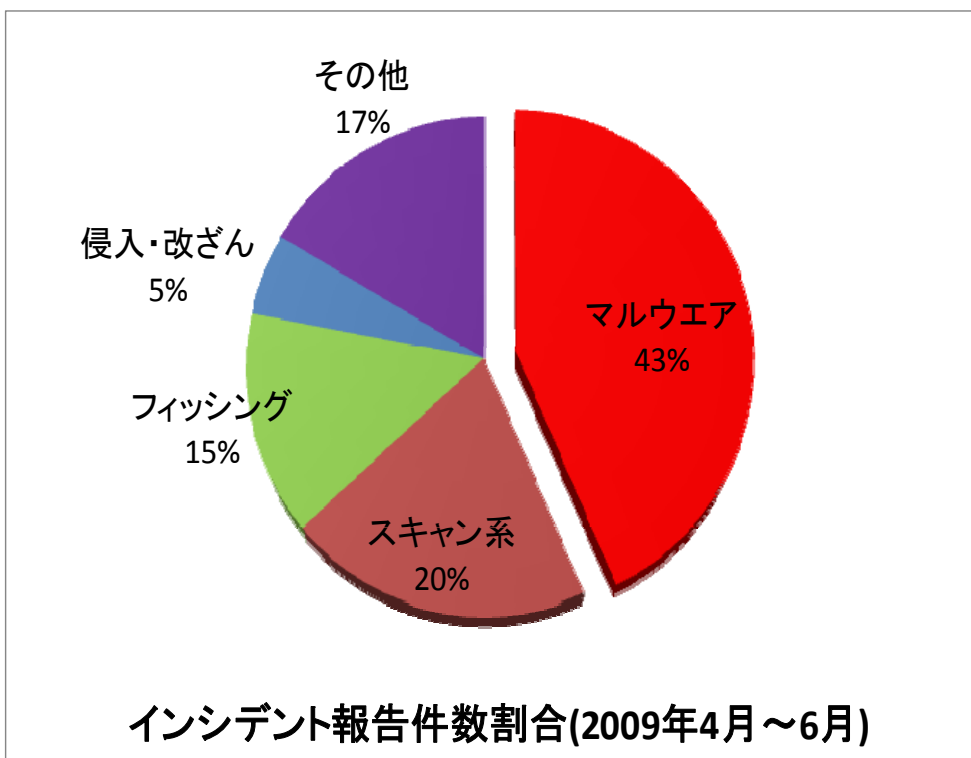
真鍋 敬士

# 最近、気になっていること

## 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



<http://www.jpccert.or.jp/ir/report.html>より

## ■ 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

# マルウェア添付メール

差出人: [redacted] 宛先: [redacted]  
件名: Thank you for setting the order No.475456 日時: Mon, 5 Oct 2009 11:23:50 -0500

Dear Customer!

Thank you for ordering at our online store.  
Your order: Sony VAIO A1133651A, was sent at your address.  
The tracking number of your postal parcel is indicated in the document attached to this letter.  
Please, print out the postal label for receiving the parcel.

Internet Store.

install.zip

差出人: [redacted] 宛先: [redacted]  
件名: Microsoft Outlook Notification for the mailer-daemon@list.jpccert.or.jp 日時: Sat, 17 Oct 2009 10:18:41 -0600

You have (5) New Message from Outlook Microsoft

- Please re-configure your Microsoft Outlook Again.
- Download attached setup file and install.

install.zip

差出人: [redacted] 宛先: [redacted]  
件名: Contract of Settlements 日時: Mon, 26 Oct 2009 18:38:17 +0900

Greetings.

We have prepared a contract and added the paragraphs that you wanted to see in it.  
Our lawyers made alterations on the last page. If you agree all the provisions we are <  
ready to make the payment on Friday for the [redacted] Consignment.  
We are enclosing the file with prepared contract. Password: 345543

If necessary, we can send it by fax.  
Looking forward to your decision.

contract\_1.zip

差出人: [redacted] 宛先: [redacted]  
件名: Conflicker.B Infection Alert 日時: Mon, 19 Oct 2009 21:27:05 -0300

Dear Microsoft Customer,

Starting 18/10/2009 the Conflicker.B worm began infecting Microsoft customers unusually rapidly. <  
Microsoft has been advised by your Internet provider that your network is infected.

To counteract further spread we advise removing the infection using an antispyware program. We <  
are supplying all effected Windows Users with a free system scan in order to clean any files <  
infected by the virus.

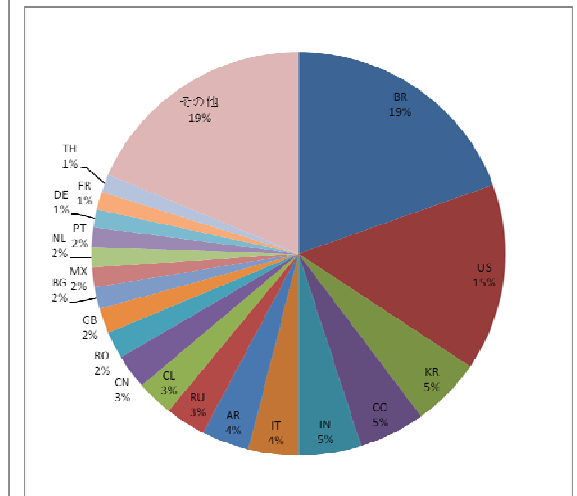
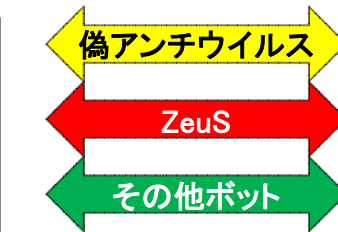
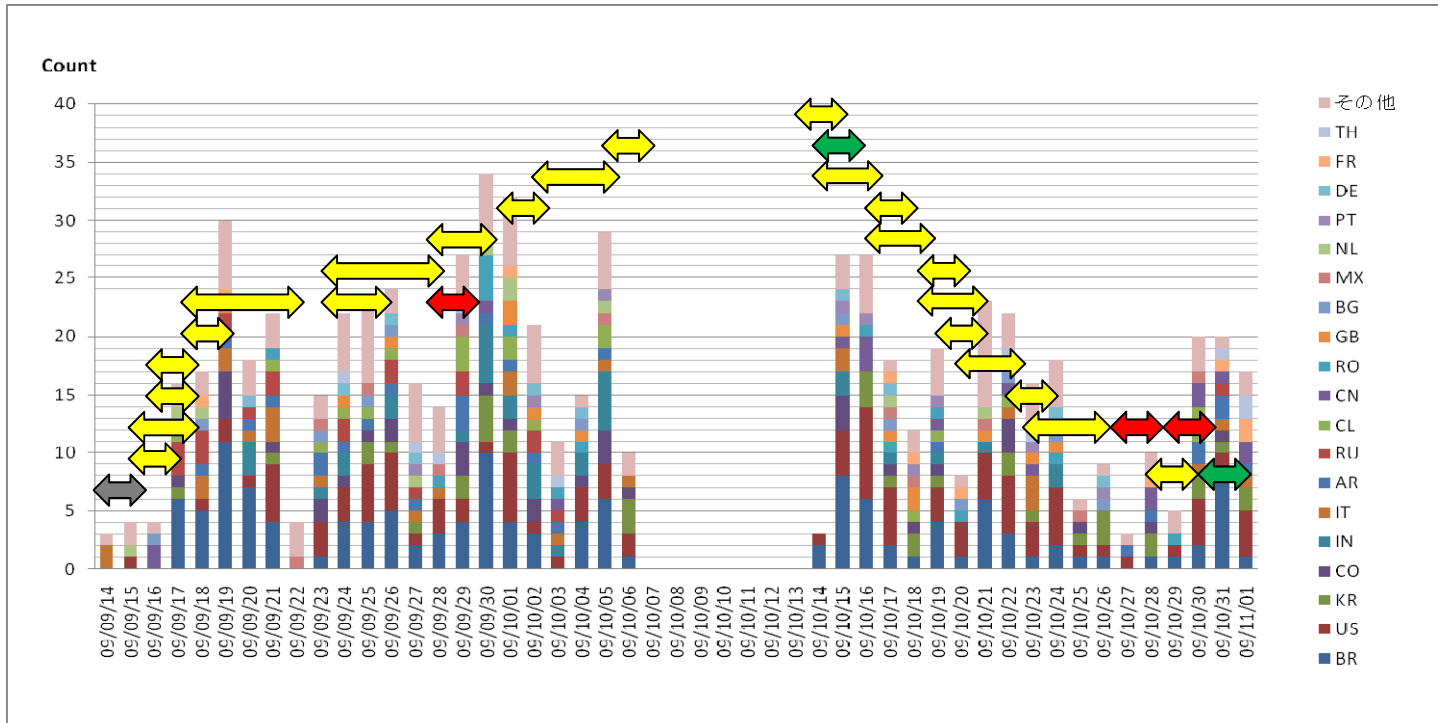
Please install attached file to start the scan. The process takes under a minute and will prevent <  
your files from being compromised. We appreciate your prompt cooperation.

Regards,  
Microsoft Windows Agent #2 (Hollis)  
Microsoft Windows Computer Safety Division

install.zip

- 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

# マルウェ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



- 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

-マルウェア添付メール-

# 偽アンチウイルス(インストール後)



購入を勧める  
ポップアップ

検出の演出

File name	Malware name
HKEY_LOCAL_MACHINE/Software/Office11/EXCEL.EXE/ /e	Registry item
HKEY_LOCAL_MACHINE/Software/C04FB1625D/ /tbodyPart	Registry item
HKEY_LOCAL_MACHINE/Software/Script/QUERY, 1400	Registry item
C:/Documents and Settings/Data/dobyqovisi.sys	BackWebLite
C:/Documents and Settings/ion Data/imukibofo.bat	AceBot
C:/Documents and Settings/Data/ixytisaken.pif	Backdoor.IRCBot
C:/Documents and Settings/uments/alehimadaw.lib	Adware.IpWins
C:/Documents and Settings/ers/Documents/ogaxa.dll	Msiebho
C:/Documents and Settings/uments/ogirecyhi.reg	AceBot
C:/Documents and Settings/cation Data/pxec.scr	A-Trojan 2.0
C:/Documents and Settings/ion Data/nazaseti.lib	MPOWER
C:/Documents and Settings/ation Data/ehowai...cu	Adware



定期的に感染し  
ていることを警告



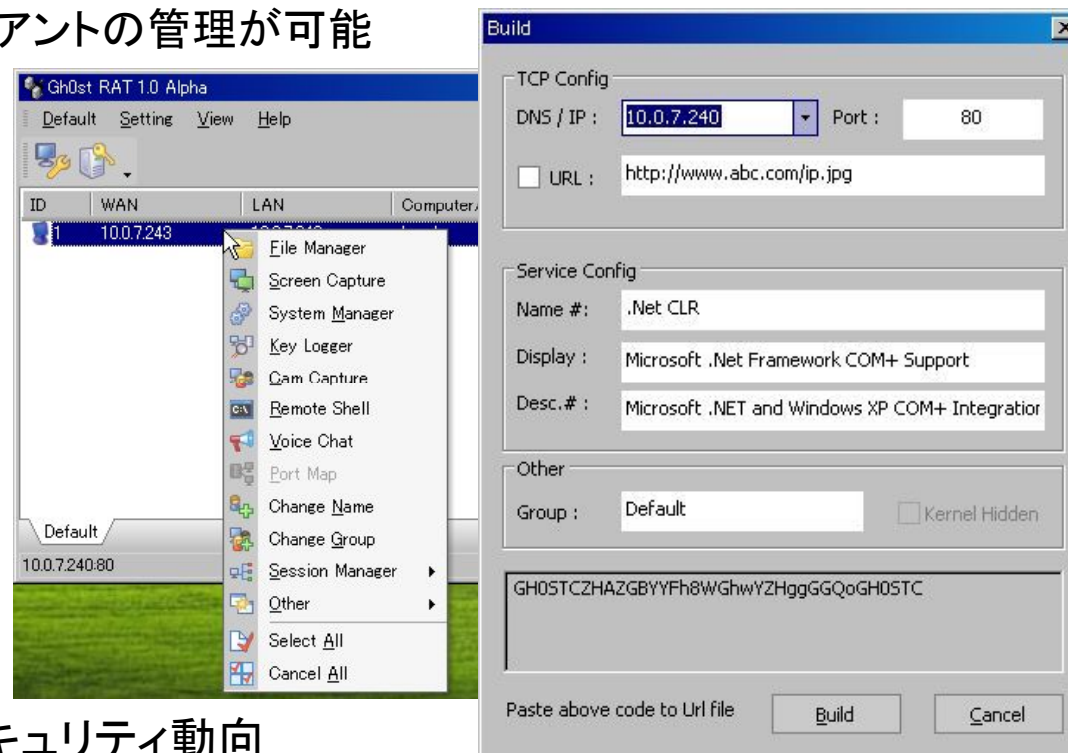
- PCの遠隔操作を可能にするツール
  - GUIによりマルウェアの作成やクライアントの管理が可能

## ■ 主な機能

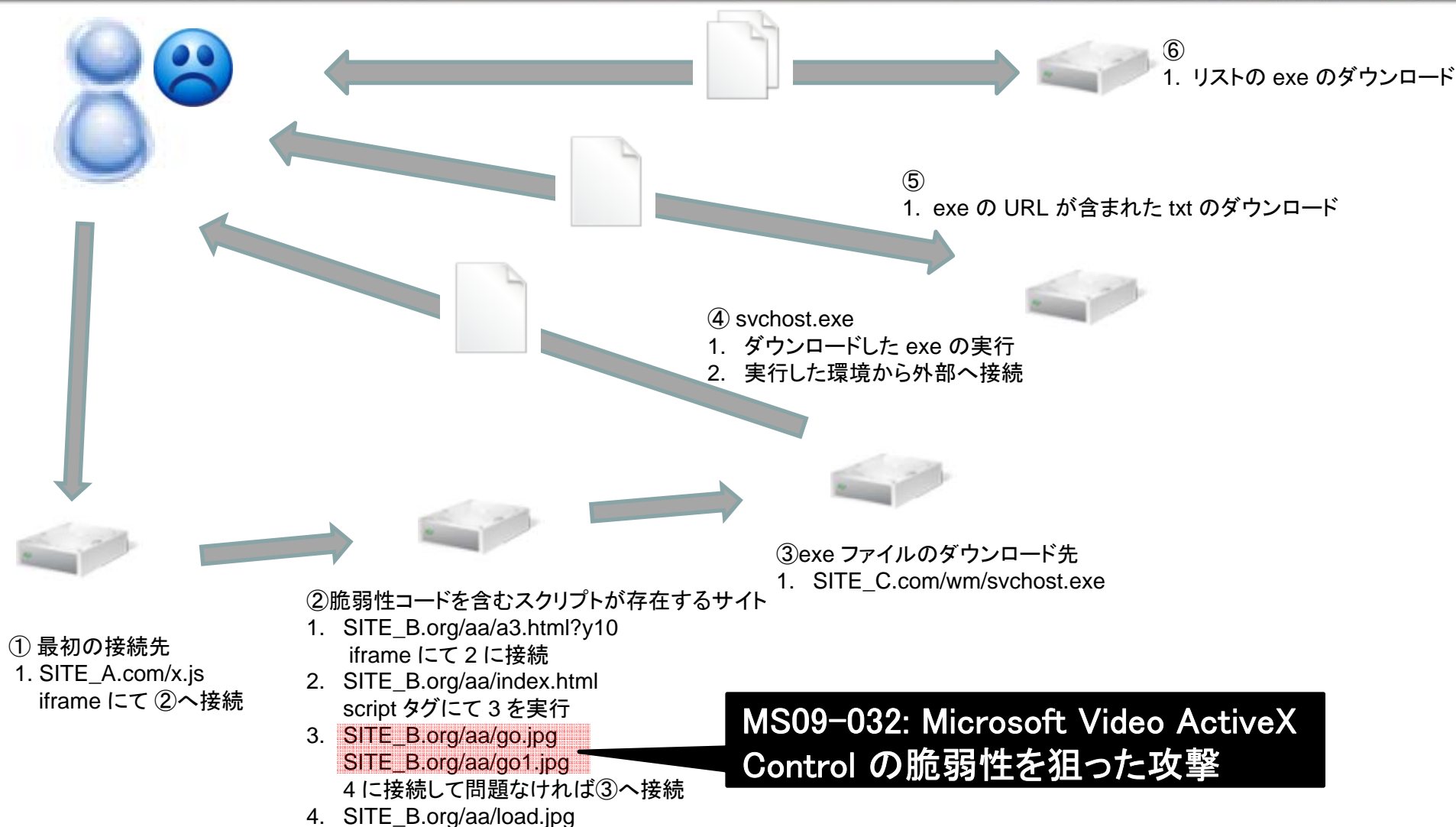
- プロセス情報の取得
- 特定プロセスの停止
- 特定のウイルス対策ソフトのバイパス
- マシンのシャットダウン、リモート
- リモートからのデスクトップ操作
- 任意のプログラムの実行
- スクリーンショットの取得
- Webカメラの操作
- 音声の録音
- キーロガー

## ■ 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



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

## ■ 共通的な挙動

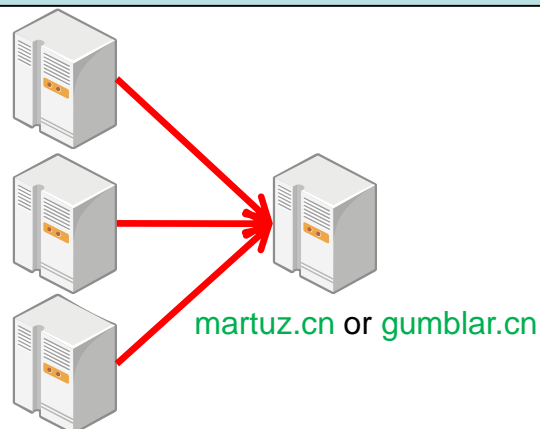
- ① Web改ざん
  - マルウェアホスティングサイトへ誘導するJavaScriptの埋め込み
- ② ダウンローダ実行
  - 脆弱性を悪用して動作し、別のマルウェアをダウンロード
- ③ マルウェア感染
  - アカウント情報盗聴等を行う

## ■ 問題を大きくする要因

- 技術的な難しさ
  - JavaScriptの難読化
  - マルウェアの多様性
    - パターンだけでは検知困難
  - 無数のマルウェ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

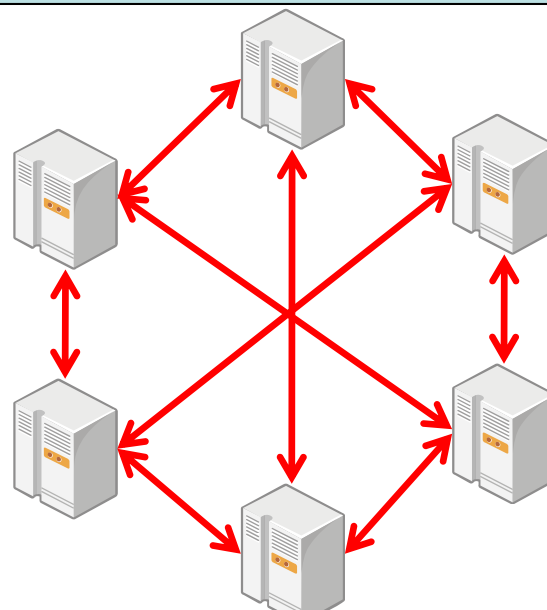
-改ざんされたWebからの誘導-  
5カ月で形態が変化

### 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

- 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



- 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以外のマルウェアにも注目
  - － 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 **CC**®

## JPCERTコーディネーションセンター

- Email: [office@jpcert.or.jp](mailto: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](mailto:info@jpcert.or.jp)
- Web: <http://www.jpcert.or.jp/form/>