Fake Malware and Virus Scanners

High Tech Bridge SA - http://www.htbridge.ch - Brian Mariani

Agenda

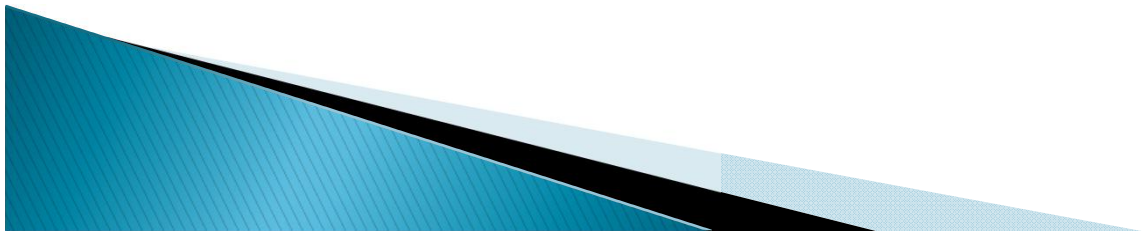
- Fake malware and virus scanners
- What are their goals?
- Malware statistics
- How they look like?
- Tricks by scammers to spread rogue malware
- A case study
- How to prevent them?

.

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

Fake Malware and Virus scanners

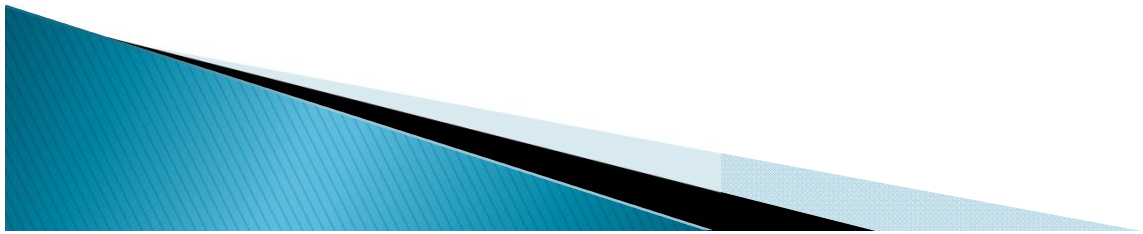
- A fake anti-antivirus or anti-malware scanner will mislead web visitors on fake scan results
- They will scare computer users by displaying files infection alerts
- It does not offer any protection to computer
- It uses false positives and fake alerts in order to trick user into obtaining a program
- The problem is widespread



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

What are their goals?

- Abuse the name of genuine malware scanner programs
- Force the user into buying for a fake anti-malware program
- Steal financial and personal information
- Compromise the target computer
- Stay resident



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

Malware Statistics

- The following statistics were compiled this year using data from computers running Kaspersky Lab products:

Monthly Malware Statistics, March 2011

March in figures

The following statistics were compiled in March using data from computers running Kaspersky Lab products:

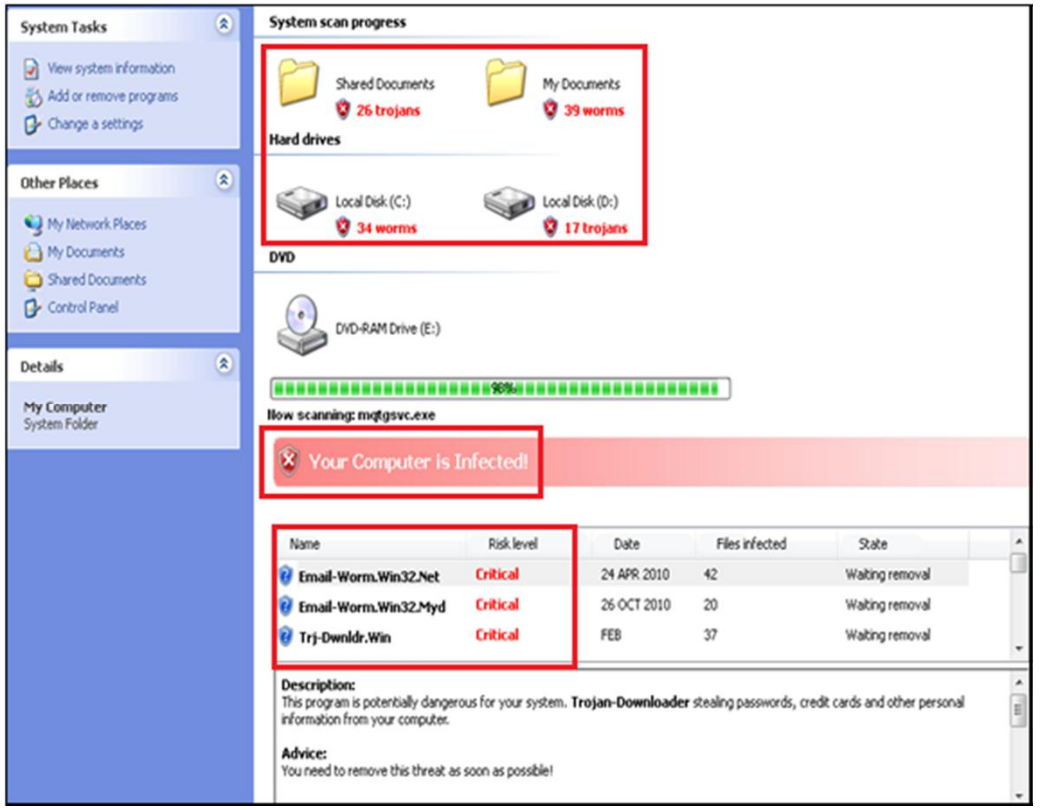
- 241,151,171 network attacks blocked;
- 85,853,567 attempted web-borne infections prevented;
- 219,843,736 malicious programs detected and neutralized on users' computers;
- 96,702,092 heuristic verdicts registered.

2011/05/20_11:46	crong.ce.ms/index.php?Q5LhrtRWbRBGznrZMzdNVCswBWm7FmMbrQf+GhDW59eCqCCLiDU+oANG4lDsfFids3ilDS7REaYxSSRAp3rCaFrDO6CMXeAkPxpRiQwd6QE=	188.229.88.102	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	43134	
2011/05/20_11:46	ezzo.ce.ms/index.php?Q9fhCNTlbT9Gq3p+M11NlStXBai7MmMrrbv+RxBN566C3SDfiLk+7g0O4jXssliCswClGy5BEWE/B5zEoDLMYIXhO/qMZ+CvPyBRyQXF6UI=	46.161.11.100	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	29073	
2011/05/20_11:46	crong.ce.ms/index.php?Q5LhrtRWbRBGznrZMzdNVCswBWm7FmMbrQf+GhDW59eCqCCLiDU+oANG4lDsfFids3ilDS7REaYxSSRAp3rCaFrDO6CMXeAkPxpRiQwd6QE	188.229.88.102	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	43134	
2011/05/20_11:46	hamshoofpti.ce.ms/index.php?Q6XhH9RUbbdGvXqnM71NtSvIBZ+762Pbrd3+bRDv57KCBCABiLI+SgOk4kjsV1gds0el4C6XEfo/UpjEqZDCqlV+Ow+MJ+AJP7RRqQyL6YI=	46.161.11.100	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	29073	
2011/05/20_11:46	hgegeermon.ce.ms/index.php?Qx3hDtT/bf1GkXq7MwtNtys8BZC7d2NArQf+mBDgS1yCkACJGo+hwNf4ijsu1jusxqlzi4qEaowp576pVbKCvo1O2SM0uCxP2FRKgxQ6ao=	188.229.88.102	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	43134	
2011/05/20_11:46	khcelolo.ce.ms/index.php?Q+rhz9TMbS1GY3q6M2xNGysPBYi7HWMyrZf+yxDs5yWC9yBjF4+CAP74hPsUFgOpyWIli7HEWA/N56JpNfMjFplO8mM7+DzPxNRjgyL6QQ=	188.229.88.102	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	43134	
2011/05/20_11:46	khcelolo.ce.ms/index.php?Q73hLtTHbeFGSXp9M1SNYyveBRy7gSNyrrVP+nxAk59aCFyAtiF8+1gMb4hDs2lj8s3ilzy4KEEg/8pm8oH7MAlXfOxWM0uCiPwhRdwyS6eI=	188.229.88.102	-	fake AV	AdamsNames Limited / person2007@adamsnames.com	43134	

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

How they look like?

- The fake anti-malware pretend a critical infection
- A bogus scan is launched play-acting the file system is being scanned
- Too many alerts messages are displayed to panic the user
- Several “critical” infections are detected



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

Tricks by scammers to spread rogue malware

- Spam on discussion forums
- Rogue malware scanners can be seen even in TV commercials
- Running an affiliate program to spread the fake scanners
- Social networks
- Malicious banner advertisement
- Well known domain name compromised

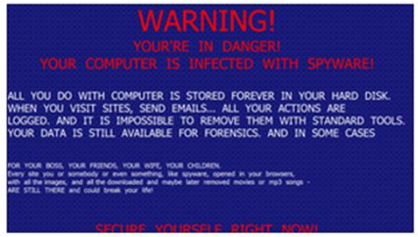
28 February 2011 Last updated at 12:55 GMT

London Stock Exchange site shows malicious adverts

Booby-trapped adverts that hit visitors with fake security software have been discovered on the London Stock Exchange (LSE) website.

Analysis of the LSE site suggests that over the last 90 days, about 363 pages had hosted malware.

The LSE said its site was now safe and an investigation showed that ads provided by a third party were the culprit.



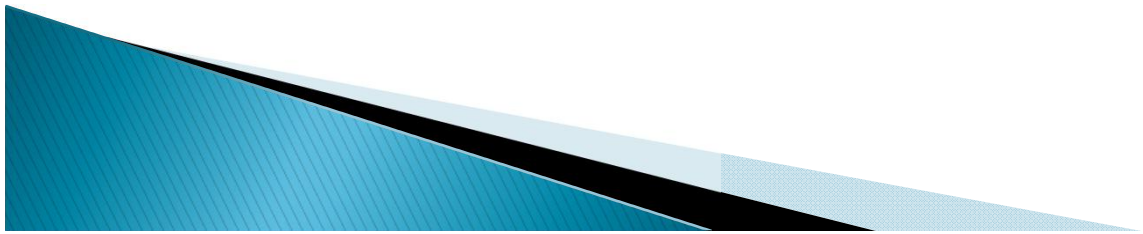
The infection kicked off warnings from a fake security program

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (1)

- Let's study how a common fake malware scanner works
- We will study the one behind this URL:

somrtype.com/scn/f7068a638392089bf9c6462f3c816e37/0540f0d2bb566d0ed0d80150e2b728ef/3656b9eddb95cfb9d7f013ed46b015a2

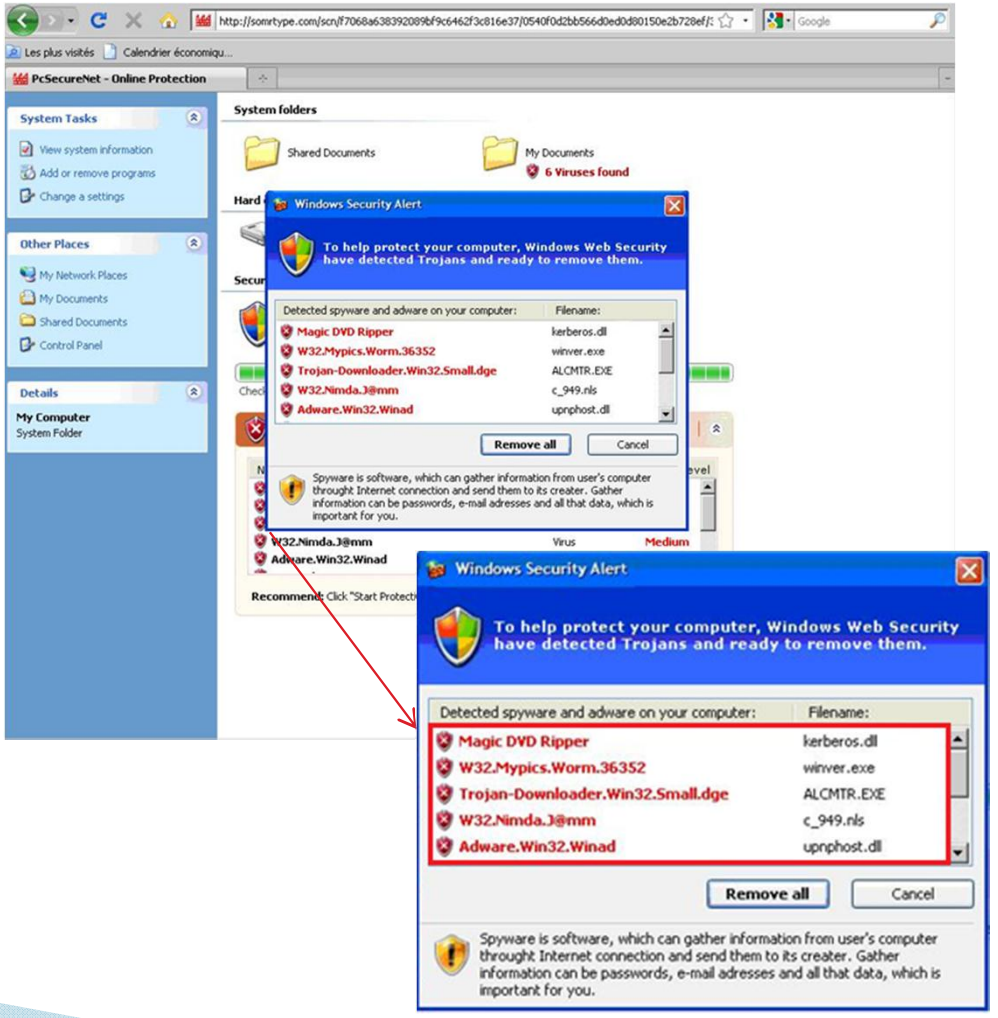


A case study (2)

- After pasting the URL into a web browser a fake message says the computer is under risk of malware and virus attacks.
- A system requires an fast check
- The System Security fake malware will perform a bogus scan

A case study (3)

- A counterfeit windows security alert is created
- The fake scan starts
- Too many infections are showed to the user



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (4)

- Let's see how this fake anti-malware operates
- We get the web page using CLI commands.

```
C:\>wget http://somrtype.com/scn/f7068a638392089bf9c6462f3c816e37/0540f0d2bb566d0ed0d80150e2b728ef/3656b9eddb95cfb9d7f013ed46b015a2
--17:45:07--  http://somrtype.com/scn/f7068a638392089bf9c6462f3c816e37/0540f0d2bb566d0ed0d80150e2b728ef/3656b9eddb95cfb9d7f013ed46b015a2
          => `3656b9eddb95cfb9d7f013ed46b015a2.1'
Resolving somrtype.com... 213.155.22.193, 213.163.65.2, 194.54.83.163
Connecting to somrtype.com|213.155.22.193|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

    [   <=>                                                                 ] 40'827        54.17K/s

7:45:08 (54.01 KB/s) - `3656b9eddb95cfb9d7f013ed46b015a2.1' saved [40827]
```

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (5)

- The file is a kind of hash
- It contains an encrypted webpage

```
(54.01 KB/s) - `3656b9eddb95cfb9d7f013ed46b015a2.1' saved [40827]
```

File Edit Format View Help

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1
    <script type="text/javascript" src="/new_engine/encrypters/base64.js"></script>
Ks8E7vZ1Stb/HBq+a+Sx3xwN0WPBotmphGPKkTyqs8/ZwdTgZaFWyTI/+LRIamdBUVHJzA+bk6ZjJWB+h1x9KgwHm3tLI4
e0YxhAeY1jV7HGZLyA2AFLjdbCvdmfgvC/lPihJ8Wgs3BJHm0oBRuqPvR1UsVWN1G1B92OglcsaONUsN7v+nuIDAh5DxP9
XgkHweY8D3WgHtRDc+NJA+hOtMME6zlg028Bdzyih6CGD+/Dqqt6BWhfA59wYOQVK3yJydD+ddfM0JI+Kjs/54Ik/WXsGK
PDXNsBugkJn6Mnl+d2wvHSgWQgXr56LKYntbq6THXkzEENQtI95tXLjrRz6PeBuHAekJI4WCxPZWKY4mE43+B9CHFZoDxD
DIc5occ9qyN3J31UBdJlnedeJ8TYxxbsC2t1vV9m0bUCan88DyG/JAtkgUv/dG6LvS2UcOSwovoTCP7lxzXgGXZM1L0wdj
hhO06RfEqka5X9ksFFv8xNHD/Mqha5HAoh1s+cEAzaCkOcZgTS7MRn1uGETrQRJ/NvjIZ5bK2/zbmXwsmj9YEepiah2w7c
0GkJO4rYvJPwRoK29pO1wccmFFxgMCwImuu7EKjXRQ0MvbDhOYJjlPTHx31iC0vKcnD6Ec8BjCW4XaMvRIhxl3nJBdfe+s
erDRdkAOoXKnO42FpMBHdWqqu5Kk/R93AHEyGeOJGesns9Y9akHOdZ+9smjFo8ZTPC1367OpNJkfyJKy/ApnBfOvf9NdrC
C15H/CStkO7/g4VnAL0Mq+RCWnXRIaHSBs5YpspzICi8G70PUoXgDPSeLJvnxHLnjR72lDfTpUMo+3g+G9yHj2PA9J2WIc
zxzRwim/ff1aE8NfyTUHBHMkZ+sIJBfAosns7NGAiz65cmvuZVcl3qw+yPdZxWuwFOgePFNIGdO1qKvrRuk2gWXtNZf2pE
Bmt+Fn4r/dAnMvPj7VNnZAglzqfeAeZpIGvC4lxu2MNsH7tBzth8Mr7lULAE8RsNl8rIyQBr15QxXSaQxfqkLHE8zkIMhE
hBJhFFOSxqisiNdMQCmiRUphDuYsI8HRvanZCB+r9CMWEyJdEqJsmqQ93xIOL1egC+fKV+FRZHR6WSkCq74srrTbS9wlFi
M/dgJEdGDFuxKxjR7wgY+94DJ9BRCpBNepDkRxliozHPPKnPGNW5H+CfDLl13tz6M7Ai0hE6cYtsHb5wvFlxirJD0NHhUM
zmbfeDGb4M5c14ar71dnMLAZVZfsxwdsJBlAfhrZBZcsk9sJtN65NuAfag+50CdewD9pq52zm6pWVF6Ubom87nP3hvz1IH
Lbh/vqOTmowjzTgBxvhoKjknShdodk7xhvchuIg8yElD7O1pgycDeWBgxZ5jlT+JdR4zcCNpm3cyJdQVkiSI7X+LStJ+pw
CO7OlhXy2rAlJDZf6KgooUQt/V/tLjwnL1KMA8jN6hrCxVJdiAejAOtbPZz1a2g7kGHHdj3MrcuIqPhgE7Uuy6wELSpkcx
QfR60blw5LG3TzYHDdbFduBK5ymw1amZqRMMEUGIwObxp7Ya16HumFCa8a3xw02eI3R+SQaJmVEtUNFaAYlxPc+aUjI3mk
zHchJYhAXfvJIjkWx17lSrfCNcJHFuGneRSJdZTXB1fciBAfuris5iHCS0A5G2O6Jfa3p1Ig21JP9rQ+RUnrLGPSMvISYb
arX3nKtt09Sn8kBQuwdt5WLvjs4cwaJPnY49HG65SEptTAEKUNJyKzocBA2QYUjXcSxB4NvSX3nhfa/LuxU3J8aKw/eSJc
/VNJNe+0DQTslgpLJoFsgdAFAUMpusZ7lsNOCBjHd7eVdyNEPQbKPRYzEsQHmJ/H9Znt8Tnz7rW9q0gG2uHmdDXIEQuQ7y
sXzE89fE0iEbOXe3FNmOZZP9OnH0jqLZJVjmjNfL2jfaalBkARqMADiBKaaYVoTmke1ideGJAg7QV4ivAB8uSBCj1XpBGf
XI5ms0DwO+Q5ODVEakMDKIeueYc2T+mDdehCb3+XPQBhsVmeJT3vpq0cayWT+Eh2+lScySGJUFnUp2VLQ0WuMPYPftR9TL
Dhlq2AMTN/cgPZkEExTpL9l1cC3U3ZDsYU6zkSvfBFYvphhJJSXp0EmidWsHXa61MBjbEWIxqT3bXsL1xsUXXve5uHRzar
G6bFaSl2fbZYpR9J4roRaNu5Mx78lsXLW2R/fkl5F1JHNuh89IGP+K+yxar83LrM+wZqbgm28yyEPIlIGYQEKvvAmeLGQC
UjEC4PDQ8VxmoqPZZDv7Kqhon4cBHx2hqO30bgJWkXOYeTWErIWdpQrcg49Eke0CutgYph6caVx7icvTqo0taBAuqnp3MT
KX/aCaBmAwMnJ+tIgafiNovUeCQsptxPRyLsFbrS+dswFNfEwmCvfrbqVTsj+Pbk11ir7SO7f75rkFwNMvxrNSGueKbfbY
J3bu6X9m/v5JwfmFfkwAFrBxDgVV/9tYqd3pPVcxbJOLh/Btrv7nk3zi1uXJ2vSS1RX0lMFDAWxSEaV6TO2wsrl2xxmADv
BHu2CnJ+IkixmrW03GAzuFrMt8NvbyUZfukxIK4FAitjuEbYcMkjAnRqih5DKre4nD6jG7qexbkCiylP5BGRCDfmBwzEBT
t8B9OYwNwNH9hkD7Vlqfms5HqgpulqLpMuNXKs/zkxRrWonUjTAfD1VpdCgh9rr4jSptea0fB1xWZS9qenHlol0dsJmIS9
I69b5y74L3+aYSgHrdx3vmmFECZt5PetOjgcbUEu5kQPT1GvElYv9blngHIhhB2RAHEbHyJ5FC2v6Clow9VkDck8fEz43y
sBQCQMgPmuqvg26/r7EKeix31gBaXeWWeu5rQ5rXhdfdgK5+KnY2QexRy6lH3v/bgE+rMXzd0/W8jezyukevnJnslSwlpE
SPlOl3GmObg3WQTbtsfc7U0BT+3ao+Vwu/4E8uBtbifmYnpWPcy572/9tFPm0PY0rRGhe/4+Sd+kBNyAgTZXwzgPZRIsCl
```

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (6)

- Let's open it using more user-friendly software
- We can understand more clearly what is happening in here
- Some javaScript code waiting to be executed in x_xtea.js and base64.js files
- The long variable is being decoded using simply base64 algorithm. Then the result was passed to TEA algorithm using the password "test"

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
        <script type="text/javascript" src="/new_engine/encrypters/x_xtea.js"></script>
        <script type="text/javascript" src="/new_engine/encrypters/base64.js"></script>
        <script type="text/javascript">
        var ymndkzpgcosjqtiwblfeahxuvr='DtmlOvjF9iOGZJ+kI8UPHz6kF9Izwdk46SXUsVjgkLIwjwdpSVkNdoe5Eqn3iFitFmhlSNAV+RmLKU/Qyz
 document.write(TEAdecrypt(base64Decode(ymndkzpgcosjqtiwblfeahxuvr), 'test'));
</script>
```

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (7)

- When we change the document.write function by an alert one we get a screenshot of the deobfuscated code

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1
/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
   <meta http-equiv="Content-Language" content="en" />

   <meta http-equiv="Cache-control" content="Public" />
   <title>PcSecureNet - Online Protection</title>

   <link rel="icon" href="/Images/favicon.gif" type="image/gif"/>
     <script type="text/javascript">
          var rand = "22396c263473f49fb955c51e971650dc7e1d8c27";
          var strategy = {preLandingTemplate: "<table cellpadding=\"0\" cellspacing=\"0\"
align=\"center\" width=\"395px\">\r\n<tr>\r\n<td>\r\n<table width=\"378px\" cellpadding=\"0\"
cellspacing=\"0\" style=\"position:relative; top:28px; left:24px\">\r\n <tr>\r\n <td width=\"6px\"
height=\"5px\"><img src=\"/new_engine//landings/04/img/left_top.gif\" width=\"6\"\r\n
height=\"5\" alt=\"\" border=\"0\"></td>\r\n <td style=\"border-top:#d3d3d3 1px solid;\"><img
src=\"/new_engine//landings/04/img/right_top.gif\" width=\"5\"\r\n height=\"5\" alt=\"\" border=\"0
\"></td>\r\n </tr>\r\n <tr>\r\n <td height=\"95px\" width=\"5\" style=\" border-left:#d3d3d3
1px solid\"><img\r\n src=\"/new_engine//landings/04/img/spacer.gif\" width=\"1\" height=\"1\"
alt=\"\" border=\"0\"\r\n </td>\r\n <td align=\"center\" valign=\"middle\">\r\n <table
width=\"80%\" height=\"75px\" border=\"0\" cellpadding=\"0\" cellspacing=\"0\"\r\n style=\"font-
size:12px\">\r\n <tr>\r\n <td align=\"left\">Operating system:</td>\r\n <td align=\"left\"
height=\"25px\" id=\"os_label\"></td>\r\n </tr>\r\n <tr>\r\n <td align=\"left\" height=\"25px
\">Internet browser:</td>\r\n <td align=\"left\" id=\"browser_label\"></td>\r\n </tr>\r\n
<tr>\r\n <td align=\"left\" height=\"25px\">Scan time:</td>\r\n <td align=\"left\"
id=\"scantime_label\"></td>\r\n </tr>\r\n </table>\r\n\r\n </td>\r\n <td style=\"border-
right:#d3d3d3 1px solid\"><img src=\"/new_engine//landings/04/img/spacer.gif\"\r\n width=\"1\"
height=\"1\" alt=\"\" border=\"0\"></td>\r\n </tr>\r\n <tr>\r\n <td height=\"5px\"><img
src=\"/new_engine//landings/04/img/left_bottom.gif\" width=\"6\" height=\"5\" alt=\"\"\r\n
border=\"0\"></td>\r\n <td style=\"border-bottom:#d3d3d3 1px solid; font-size:1px\"><img\r\n
src=\"/new_engine//landings/04/img/spacer.gif\" width=\"1\" height=\"1\" alt=\"\" border=\"0
\">\r\n </td>\r\n <td><img src=\"/new_engine//landings/04/img/right_bottom.gif\" width=\"5\"
height=\"5\" alt=\"\" border=\"0\"></td>\r\n </tr>\r\n</table>\r\n<div style=\"width:100px;
position:relative; top:40px; left:30px; font-size:20px; color:#727272;\">\r\n <div id=\"dot2\"\r\n
style=\"width:20px; height:22px; background:url(/new_engine//landings/04/img/green_dot.jpg)
no-repeat; font-size:20px; color:#727272; position:relative; top:3px; left:0px; float:left;
visibility:hidden\"></div>\r\n <div id=\"stage1\" style=\"visibility:hidden\"> Stage 1</div>\r
\n</div>\r\n<div id=\"check1\"\r\n style=\"font-size:14px; font-weight:bold; position:relative;
top:50px; left:55px; visibility:hidden\">\r\n Checking firewall status\r\n</div>\r\n<div
style=\"position:relative; top:65px; left:54px\"><img id=\"scroll1\"\r\n src=\"/new_engine//landings
/04/img/anim-line.gif\"\r\n style=\"visibility:hidden\" width=\"304\" height=\"15\" alt=\"\" border=\"0
\">\r\n</div>\r\n<div id=\"way1\" style=\"font-size:10px;position:relative; top:70px; left:56px;
visibility:hidden\">Sending data\r\n to server\r\n</div>\r\n<table id=\"fire_dis\" cellpadding=\"0\"
cellspacing=\"0\" height=\"33px\" width=\"303px\"\r\n style=\"font-size:10px;position:relative;
top:60px; left:56px; visibility:hidden\">\r\n <tr>\r\n <td width=\"303px\" height=\"4\"><img
src=\"/new_engine//landings/04/img/red_top.jpg\" width=\"303\"\r\n height=\"4\" alt=\"\"
border=\"0\"></td>\r\n </tr>\r\n <tr>\r\n <td background=\"/new_engine//landings/04/img
/red_bg.jpg\">\r\n <div style=\"position:relative; top:2px; left:13px;width:270px; height:25px;
background:url(/new_engine//landings/04/img/x.jpg) no-repeat; color:#FFFFFF; padding-left:28px;
font-size:14px; font-weight:bold; padding-top:3px\">\r\n Firewall protection disabled\r\n
</div>\r\n </td>\r\n </tr>\r\n <tr>\r\n <td width=\"303px\" height=\"4\"><img
src=\"/new_engine//landings/04/img/red_bottom.jpg\" width=\"303\"\r\n height=\"4\" alt=\"\"
border=\"0\"></td>\r\n </tr>\r\n</table>\r\n<div style=\"width:100px; position:relative;
top:90px; left:30px; font-size:20px; color:#727272;\">\r\n <div style=\"width:22px; height:20px;
background:url(/new_engine//landings/04/img/red_dot.jpg) no-repeat; font-size:20px;
color:#727272; position:relative; top:3px; left:0px; float:left; visibility:hidden\"\r\n id=\"dot1
\"></div>\r\n <div id=\"stage\" style=\"visibility:hidden\"> Stage 2</div>\r\n</div>
\r\n<div id=\"check\"\r\n style=\"font-size:14px; font-weight:bold; position:relative; top:100px;
left:55px; visibility:hidden\">\r\n Checking installed security software\r\n</div>\r\n<div
```

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (8)

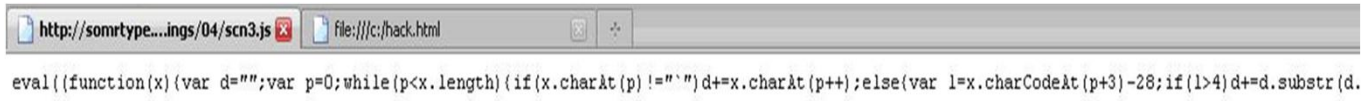
- Playing a while with the path /new_engine/landings/04/ let us know another interesting javaScript page scn3.js

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta http-equiv="Content-Language" content="en" />

    <meta http-equiv="Cache-control" content="Public" />
    <title>PRODUCT_NAME - Online Protection</title>

    <link rel="icon" href="/Images/favicon.gif" type="image/gif"/>
        <script type="text/javascript">
                var rand = "7e2a602d0618a2f1a674c25596ac4e1dea169fe1";
                var strategy = {preLandingTemplate: "<table cellpadding=\"0\" cellspacing=\"0\" align=\"center\" width=\"395px\">\
                var downloadUrl = "";
        </script>
        <script type="text/javascript" src="PATH/scn3.js"></script>

</head>
<body>
<div id="loading" style="display:none">
    <div class="loading-indicator">
      <img height="50" width="50" style="margin-right: 8px; float: left; vertical-align: top;" src="/Images/loading.gif"/>
      <br/>
      <span id="loading-msg">Initializing Virus Protection System...</span></div>
</div>

</body>
</html>
```

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (9)

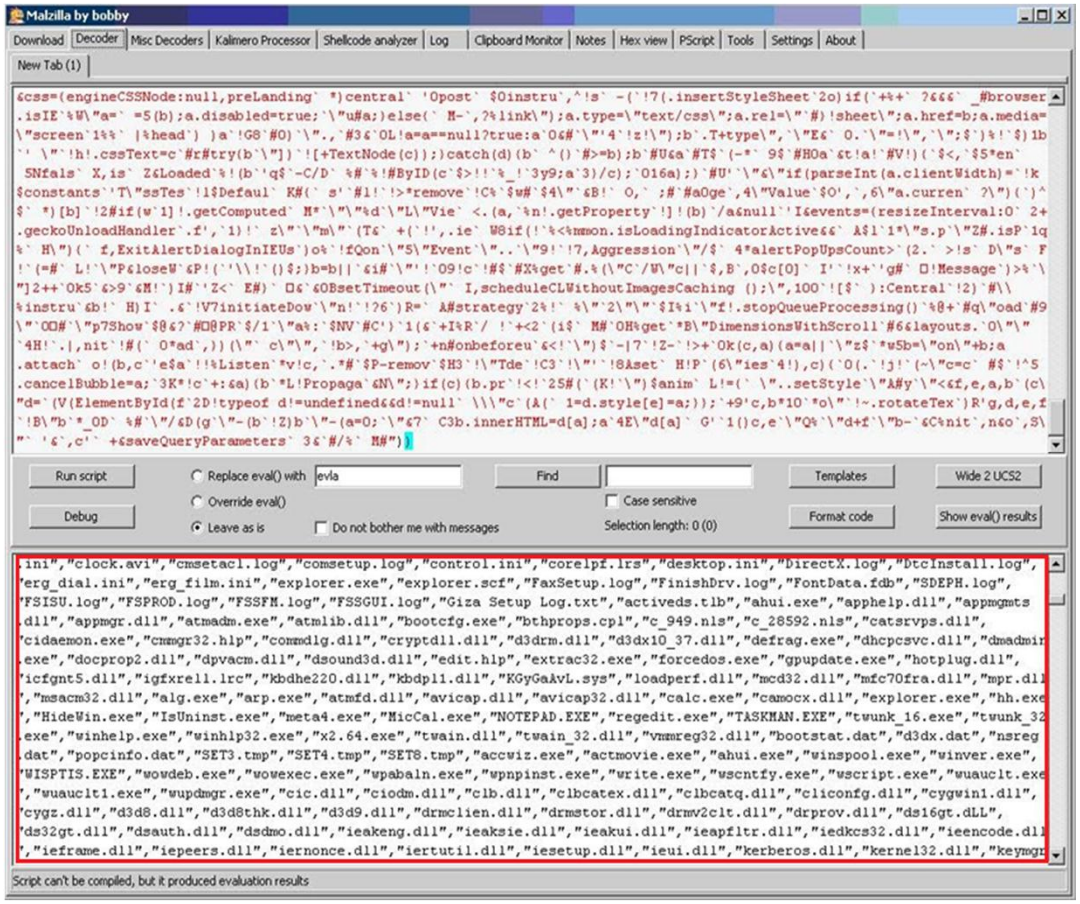
- After viewing the file contents I get another encoded webpage
- This time I used Malzilla. This good piece of code is very useful to be used in exploring malicious webpages



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

A case study (10)

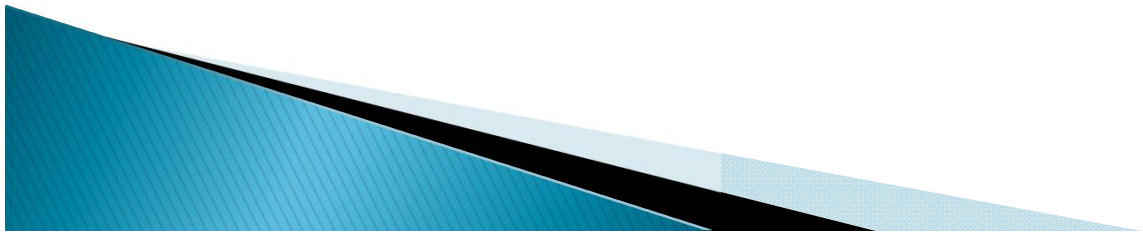
- Copying the code into the decoder option got me in seconds the deobfuscated webpage contents
- We can clearly see the list of files being used for the fake antivirus, trying to convince the victim that the box is being scan to search “malicious” programs



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

How to prevent them?

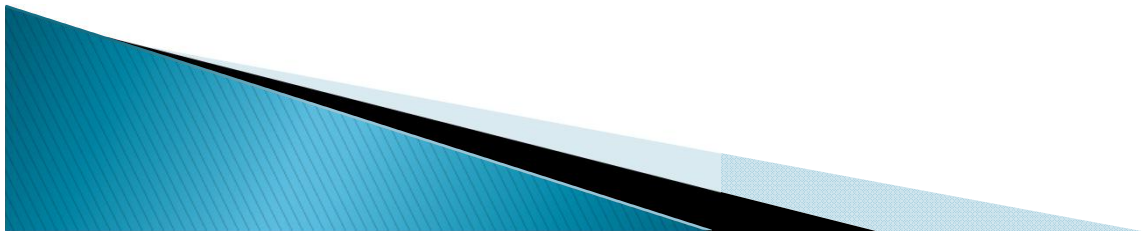
- Users should pause before clicking on a window or strange pop-ups
- Users should make sure that they run up-to-date legitimate antimalware software
- Updated Web browser with antiphishing features
- Patched applications and Operating system
- Auto-update features should be enabled



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

References

- SecureList – http://www.securelist.com/en/analysis/204792170/Monthly_Malware_Statistics_March_2011
- MalwareDomainList – http://www.malwaredomainlist.com
- Malzilla – http://malzilla.sourceforge.net
- The Inquirer – http://www.theinquirer.net/inquirer/news/2029425/london-stock-exchange-website-hacked-malware-ads



HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

Questions?

brian.mariani@htbridge.ch