Playing with Sandbox
- AVTokyo style -

All your sandboxes are belong to us

Daiki FUKUMORI
daikifukumori @ gmail.com
Speaking of Sandbox

In 2009, Shibuya.pm

「Native Client Hacks」

http://www.atmarkit.co.jp/fsecurity/column/ueno/58.html
Let me show you the conclusion first as they are the same from last time.

Wrap-up

Sandboxes become strong every time they are broken.

Enjoy SandBoxing!

Daiki Fukumori
<daikifukumori@gmail.com>
Example of Malware Analysis Sandbox

Anubis

viCHECK.ca

GFI ThreatTrack™

VirSCAN.org

ThreatExpert

COMODO
Creating Trust Online™

FORTINET®

virusTotal

Malware
For example: VirusTotal

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>AheLab-V3</td>
<td>Spymir82.Zbot</td>
<td>20130803</td>
</tr>
<tr>
<td>AntiVir</td>
<td>TR/Spy.Zbot, ejine.1</td>
<td>20130803</td>
</tr>
<tr>
<td>Anty-AVL</td>
<td>Trojan.Win32.Zbot.gen</td>
<td>20130803</td>
</tr>
<tr>
<td>Avast</td>
<td>Wi20.Anti-Malware [Tg]</td>
<td>20130803</td>
</tr>
<tr>
<td>AVG</td>
<td>Generic26:GLX</td>
<td>20130803</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Trojan.Generic.KO 67396</td>
<td>20130803</td>
</tr>
</tbody>
</table>

**Pattern matching**

**Behavior detection (By using Cuckoo)**
Mechanism of Malware Analysis Sandbox

User

Upload

Sandbox

Execute

Report
- Changed files
- Changed registries
- Network access

Internet access

Download additional files

Attacker’s site
Action of common sandboxes

- Execute samples, infect for real
- Report changes of files, registries, etc.
- Capture network access
- API execution record
Recent malware’s characteristics

• So-called “downloader” or “dropper”
• To Escape from detection, there is a minimum function in 1\textsuperscript{st} binary file.
• 2\textsuperscript{nd} binary file can execute arbitrary command

Cannot define malware until operational command comes from C&C server
Cannot define malware until operational command comes from C&C server

Sandboxes have no choice but accessing Internet
From attacker’s perspective

- Do not want their method to be detected by researchers.
- Want to stop their malware if it is test environments.
RAT - Cerberus

Create New Server

Settings:
- Basic Options
- Server Installation
- Boot Methods
- Add file
- Anti Debugging
- Misc. Options
- Display message
- Black list
- Overview
- Create server

Anti Debugging:
- Anti Virtual PC
- Anti VMWare
- Anti VirtualBox

- Attempt to avoid the following Sandbox's
  01 - Sandboxie
  02 - ThreatExpert
  03 - Anubis
  04 - CW/Sandbox
  05 - JoeBox
  06 - Norman Sandbox

If the server is ran inside of a sandbox or virtual machine, it will not run in order to prevent its detection.
Check ProductId

```assembly
push 0      ; lpType
push 0      ; lpReserved
push offset ValueName ; "ProductId"
mov eax, [esp+120h+hKey]
push eax ; hKey
call RegQueryValueExA_0
lea eax, [esp+10Ch+Data]
cmp eax, offset a55274640267306 ; "55274-640-2673064-23950"
jnz short loc_4072FD
```

```
loc_4072FD:
lea   eax, [esp+10Ch+Data]
cmp   eax, offset a76487644317703 ; "76487-644-3177037-23510"
jnz   short loc_40730C
```

```
loc_40730C:
lea   eax, [esp+10Ch+Data]
cmp   eax, offset a76487337842995 ; "76487-337-8429955-22614"
jnz   short loc_40731B
```
If “remote-control virus” is executed in a sandbox

ERROR

ERROR: Unable to resume thread with handle "0x00000744"
Sandboxes are the lovables

- No “Visual C++ Redistributable Package”
- No “.NET Framework”
How to execute “remote-control virus”

1. Download .NET Framework and install it
2. Upload custom-made agent
3. Install the sample
Error, because the generated report was too big
Playing with Sandbox — AVTokyo style
How to run “remote-control virus”

1. Upload custom-made agent
2. Download .NET Framework and install it
3. Install the sample
4. Take screen-capture and upload it
All your sandboxes are belong to us
[ Removed ]
Malware analysis sandbox without internet access
AV Tracker

Antivirus Tracker

<table>
<thead>
<tr>
<th>IP</th>
<th>POSTS</th>
<th>COUNTRY</th>
<th>DATE/title</th>
<th>IRC</th>
<th>IP Tables</th>
<th>API</th>
<th>.Status</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>81.181.247.146</td>
<td>81.181.247.146</td>
<td>China</td>
<td>6th Jun 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80.13.75.21</td>
<td></td>
<td>France</td>
<td>27th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82.245.40.203</td>
<td></td>
<td>France</td>
<td>29th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.130.56.11</td>
<td></td>
<td>Austria</td>
<td>20th Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.130.56.12</td>
<td></td>
<td>Austria</td>
<td>20th Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.130.56.14</td>
<td></td>
<td>Austria</td>
<td>17th Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.130.56.16</td>
<td></td>
<td>Austria</td>
<td>15th Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.130.56.23</td>
<td></td>
<td>Austria</td>
<td>7th Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.130.56.26</td>
<td></td>
<td>Austria</td>
<td>6th Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80.13.75.21</td>
<td></td>
<td>France</td>
<td>28th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>217.86.133.28</td>
<td></td>
<td>Germany</td>
<td>7th Jun 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.95.48.100</td>
<td></td>
<td>United States</td>
<td>19th Oct 08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91.199.104.3</td>
<td></td>
<td>Romania</td>
<td>16th Oct 08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91.199.104.4</td>
<td></td>
<td>Romania</td>
<td>16th Oct 08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01.199.104.15</td>
<td></td>
<td>Romania</td>
<td>16th Oct 08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.126.133.131</td>
<td>[*] 64-126-133-131.static.bwtelecom.net</td>
<td>United States</td>
<td>19th Aug 08</td>
<td>HOME-OF-DOS</td>
<td>Dave</td>
<td>Windows 5.1</td>
<td>CWSandbox</td>
<td></td>
</tr>
<tr>
<td>88.135.42.70</td>
<td></td>
<td>Germany</td>
<td>7th Jun 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.145.241.17</td>
<td></td>
<td>Germany</td>
<td>15th Oct 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216.245.222.15</td>
<td>[*] 15-222-225-216.reverse.lat.net</td>
<td>United States</td>
<td>19th Aug 08</td>
<td>HOME-OF-DOS</td>
<td>Dave</td>
<td>Windows 5.1</td>
<td>CWSandbox</td>
<td></td>
</tr>
<tr>
<td>46.102.243.70</td>
<td></td>
<td>Romania</td>
<td>28th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>208.118.60.155</td>
<td></td>
<td>United States</td>
<td>26th Feb 10</td>
<td>rtrrle</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109.74.154.83</td>
<td></td>
<td>Slovakia</td>
<td>28th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95.148.33.57</td>
<td></td>
<td>Slovakia</td>
<td>15th Jun 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66.129.97.254</td>
<td>[*] 66.129-97.254</td>
<td>United States</td>
<td>26th Jan 12</td>
<td>HOME-OF-DOS</td>
<td>Dave</td>
<td>Windows 5.1</td>
<td>GFI Sandbox</td>
<td></td>
</tr>
<tr>
<td>72.66.146.112</td>
<td>[*] static-72-66-146-112.tampmill.tos-verian.net</td>
<td>United States</td>
<td>26th Jan 12</td>
<td>JONATHAN-CSSD</td>
<td>SIP</td>
<td>Windows 5.1</td>
<td>GFI Sandbox</td>
<td></td>
</tr>
<tr>
<td>212.8.67</td>
<td>muzuki.kaspersky-labs.com</td>
<td>United States</td>
<td>20th Oct 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91.103.66.1</td>
<td>aol.kaspersky-labs.com</td>
<td>United States</td>
<td>15th Jun 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91.103.66.2</td>
<td>asie2-kaspersky-labs.com</td>
<td>United States</td>
<td>15th Jun 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91.103.66.3</td>
<td>ase2-kaspersky-labs.com</td>
<td>United States</td>
<td>15th Jun 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91.103.66.4</td>
<td>ase3-kaspersky-labs.com</td>
<td>United States</td>
<td>15th Jun 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>149.20.63.65</td>
<td>[*] 149-20-63-65</td>
<td>United States</td>
<td>26th Jan 12</td>
<td>LAB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>149.20.63.5</td>
<td></td>
<td>United States</td>
<td>26th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>169.164.111.198</td>
<td></td>
<td>United States</td>
<td>28th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>193.71.68.2</td>
<td>norman.norman.no</td>
<td>Norway</td>
<td>26th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81.131.173.102</td>
<td></td>
<td>Norway</td>
<td>26th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81.23.107.120</td>
<td></td>
<td>Norway</td>
<td>22nd Feb 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>124.92.234.19</td>
<td></td>
<td>Malaysia</td>
<td>6th Jun 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>202.160.74.29</td>
<td>[*] 202-160-74-29</td>
<td>Malaysia</td>
<td>6th Jun 18</td>
<td>XANNY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>204.93.130.132</td>
<td></td>
<td>United States</td>
<td>27th Jan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>174.133.89.70</td>
<td>[*] 46.95.85.ee.static.theplanet.com</td>
<td>United States</td>
<td>19th Aug 08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>174.133.89.72</td>
<td>46.95.85.ee.static.theplanet.com</td>
<td>United States</td>
<td>17th Oct 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>174.133.89.74</td>
<td>46.95.85.ee.static.theplanet.com</td>
<td>United States</td>
<td>6th Jun 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>174.133.89.84</td>
<td>46.95.85.ee.static.theplanet.com</td>
<td>United States</td>
<td>22nd Oct 09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Access from all over the world
Wrap-up

• possible to retrieve lots of information from sandboxes
• possible to detect sandboxes by using combination of the information
• Anti-Sandbox is simple
  * WindowsID
  * User ID
  * Delay
  (Sandboxes are reverted in a timely manner)
All your sandboxes are belong to us
Three important things when you play with sandbox
1. Big heart

Sandboxes are really unstable. Result may change every time.

Don’t blame their error!
2. Patience

Sandyboxes are really slow.
It takes long time getting the result.
(more than a month in a worst case)

Look with a warm eye!
3. Prioritize

Sandboxes last really short time as they get reverted all the time. We have to do essential tasks efficiently.

Life is really short!
Sandboxes showed me all about life
Enjoy Sandboxing!!!

Wrap-up

Sandboxes become strong every time they are broken

ご清聴ありがとうございました

Enjoy SandBoxing!

Daiki Fukumori
<daikifukumori@gmail.com>