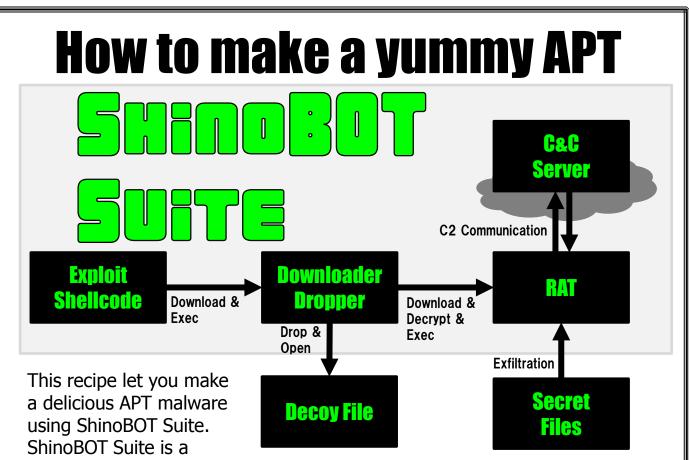


RSENAL



Copyright © Sh1n0g1 2013-2014



tool-kit to help pen-testers simulate a sophisticated APT campaign with a few steps, just like a bouillon cube. Cook it, try it, and let your friend or foe eat it!

Yield:	Dozens Infected Computers
Category :	Targeted Attack
Prep Time :	5 min
Cook Time	: 5 min

Ingredients

1

- 1 ShinoBOT Suite ShinoDownloader.exe ShinoBOT.exe
- 1 Decoy File (size < 50KB)
- 1 Password to encrypt the RAT
 - Attacker's PC to access C&C Server (only browser needed)

Direction

PDF

1.1

×

w, 1

J

R

STEPO PREPARATION

- 1. Prepare 1 decoy file. A legitimate documents.
- 2. Download ShinoBOT Suite from <u>ShinoSec.Com</u>

STEP1 ENCRYPT THE RAT

- 1. Execute ShinoBOTSuite.exe.
- 2. Choose the RAT.
- 3. You can set your encryption key or password (via Set Ascii)
- 4. Press [Encrypt] and [Next Step]

STEP2 UPLOAD THE RAT

- 1. Choose the upload server (default ShinoMal.mooo.com)
- 2. Press [Upload] and [Next Step]

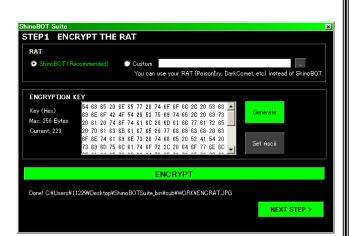
ep2 UPLOAD THE I al Path of the RAT	TAI
	/Suite_bin¥sub¥WORK¥ENCRAT.JPG
oload Server	
ShinoMAL (Recommended)	Upload Manually (Input the URL to download your encrypted RAT)
	UPLOAD
of Encrypted RAT	
L of Encrypted RAT	
L of Encrypted RAT	

TIPS

The encrypted RAT is hidden in the kitten image. So you can upload it in some image sharing server instead of ShinoMal.mooo.com.



Copyright © Sh1n0g1 2013-2014



STEP3 CREATE DOWNLOADER

- Select your decoy file.
 Otherwise you can use the default one.
- 2. Press [Create Downloader] and [Next Step]

STEP4 UPLOAD THE DOWNLOADER

- **1.** Select the upload server
- 2. Press [Upload] and [Next Step]

STEP5 CREATE THE EXPLOIT

- **1.** Choose the icon path.
- 2. Press [Create] and [Exit].
- 3. The shortcut will appear on your desktop.

ShinaBOT Suite Image: Step3 CREATE DOWNLOADER Local Path of the RAT C#Users#11229#Desktop#ShinaBOTSuite_bin#sub#WORK#ENCRAT.JPG URL of Encrypted RAT Image: Step502 Eytes http://shinabl.mooo.com/files/938df3e64ba6d5de_53DA90B3img.jpg Image: Step502 Eytes DecoyFile File Size:5502 Eytes C#Users#11229#Desktop#ShinaBOTSuite_bin#sub#WECOY#NSA_Certificate_Extension_RFC7169.txt C#Users#11229#Desktop#ShinaBOTSuite_bin#sub#WECOY#NSA_Certificate_Extension_RFC7169.txt File Name 2 Download File Name *tmp:/F9F09BF.tmp RAT File Name KB79590579.exe CREATE DOWNLO ADER Path of Downloader C#Users#11229#Desktop#ShinaBOTSuite_bin#sub#WORK#ShinaDownloader.exe C#Users#11229#Desktop#ShinaBOTSuite_bin#sub#WORK#ShinaDownloader.exe NEXT STEP

ep4 UPLOAD THE DOV		
	INLOADER	
al Path of the Downloader		
Users¥11229¥Desktop¥ShinoBOTSuite	bin¥sub¥WORK¥ShinoDownloader.exe	
Upload Server		
ShinoMAL (Recommended)	Upload Manually (Input the URL to download	your encrypted RAT)
File Name (http://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	/%filename%)	
_dlwdr		
	UPLOAD	
	UPLOAD	
IRL of Downloader		
ttp://129-199-192-16-1-akamaiedge.mo	ooo.com/files/dd9341cc833788bc_53DA938A_d	lwdr
you can download your Downloader, it n	eans that it is OK. If not please retry	
	Download Test	
		NEXT STEP >

ShinoBOT Suite	×
Step 5 CREATE THE EXPLOIT (.LNK)	
URL of the Downloader	
http://129-199-192-16-1-akarnaiedge.mooo.com/files/dd9341cc833788bc_53D	A938A dlwdr
	······
Shortcut Parameter	
File Name	
NSA_Certificate_Extension_RFC7169	
lcon Path %SystemRoot%¥System32¥imageresdⅡ	Icon Index 97
x3ystemPublik-3ystem22+imageres.uii	37
CREATE	
Shortcut Path	
C#Users¥11229¥Desktop¥NSA_Certificate_Extension_RFC7169.txt.lnk	
Now, you get your weapon! Enjoy with it.	Exit

NUTRITION NOTE

ShinoBOT Suite contains cryptography, steganography, DGA (used in the RAT SHinoBOT.exe), shortcut attack, icon camouflage, etc. Anyway, it is very healthy.

You can send the shortcut in phishing mail. Most mail server allow the shortcut on the ZIP folder. When the victim click the shortcut, he or she will infected by the RAT without detected.

Bon Appétit‼

Copyright © Sh1n0g1 2013-2014