



SNSCAT

What You Don't Know About Sometimes Hurts the Most

Dan Gunter & Solomon Sonya

Topics Covered

- What is SNSCat
- Why SNSCat Matters
- Module Overview & Demo
- Mitigation Strategies



blackhat
USA 2012



WHAT IS SNSCAT



**“Post penetration covert channel tool designed to
hide communication over social media sites and
confuse incident responders”**



Did you miss a key detail...

SNSCat exploits both the technology and incident responder



You said post penetration...isn't the access assumption a cheat?

Cobalt & Armitage are amazing projects that can leverage our project
(Check it out at <http://www.advancedpentest.com>)

Naïve Exfiltration



Weaknesses

- Looks suspicious
- Newer technology looks for this type of exfiltration
- Network security infrastructure can log session
- Attacker gives away IP

SNSCat Exfiltration



Weaknesses Exploited

- Data Loss Prevention vs encrypted/stego'd data
- Security infrastructure logs valid social media site traffic
- Attacker never sees victim
- Incident responders won't want to touch this
 - "More of a compliance issue" attitude

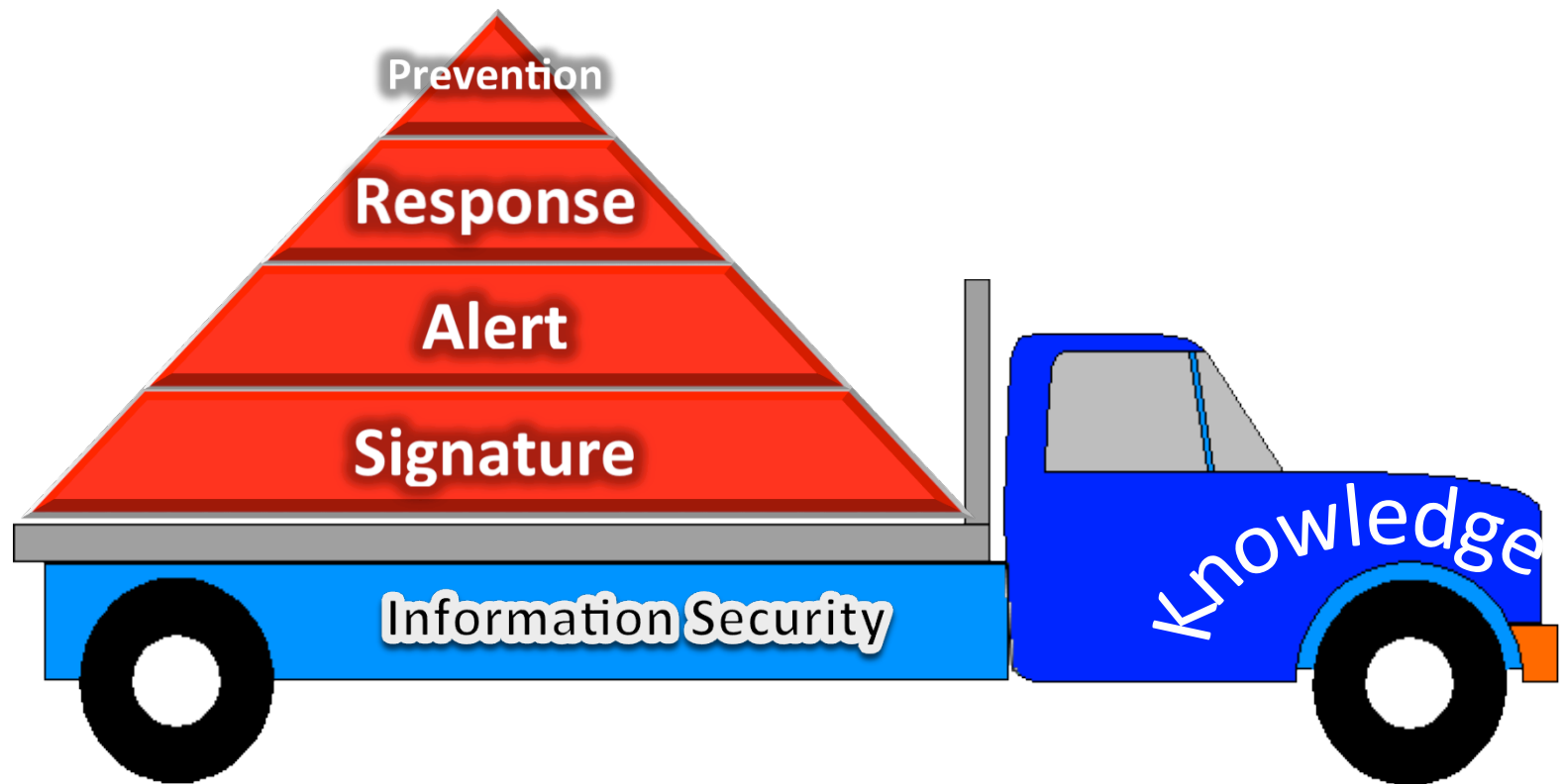


blackhat
USA 2012

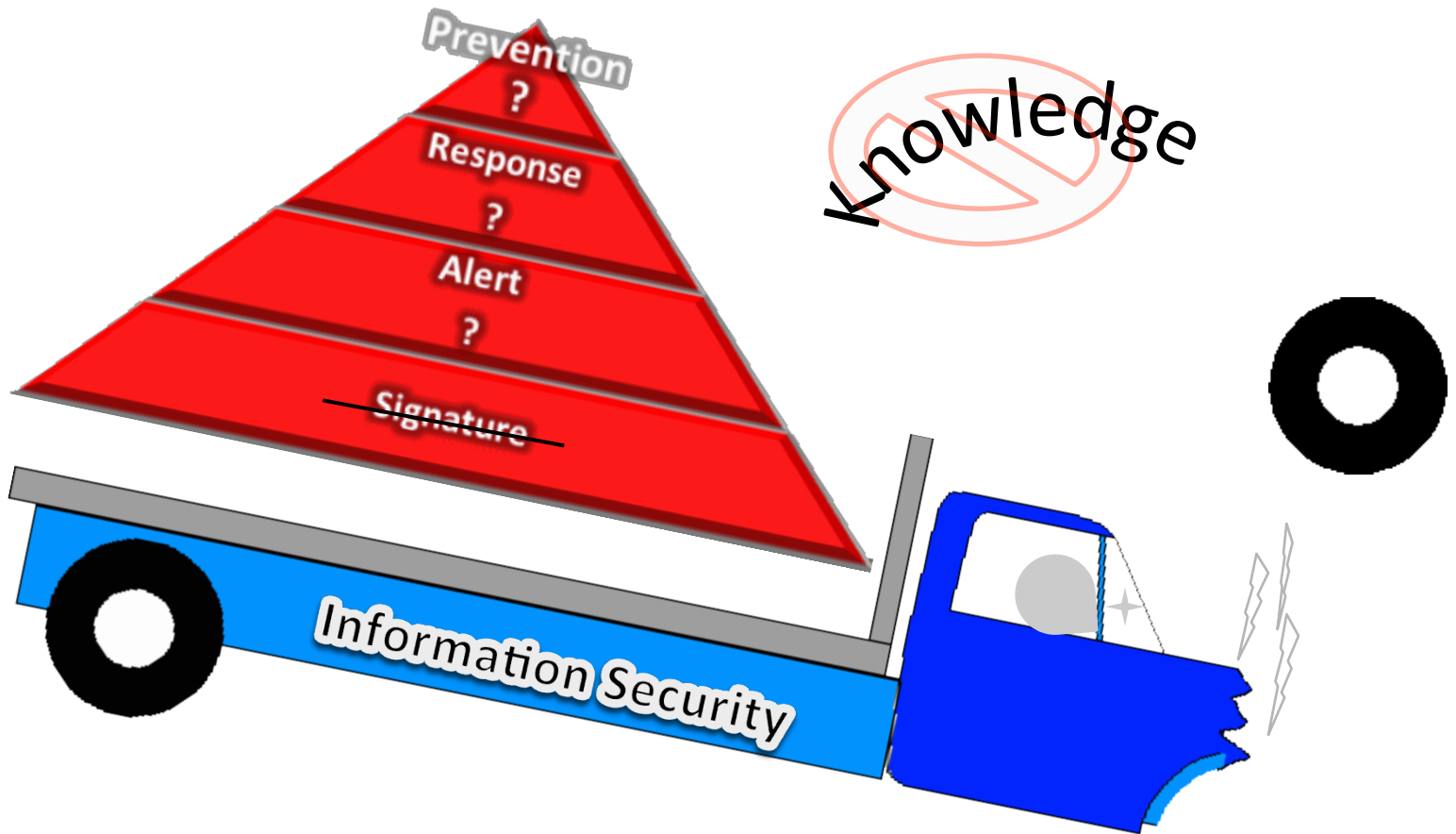


WHY SNSCAT MATTERS

Information Security Paradigm



What happens when Knowledge is Removed?



Application to Network Forensics

Knowledge

- Starts by identifying artifact of the attacker
 - Clues the system has been compromised
 - Connection data (IP, DNS, time, duration, count)
 - Unknown Traffic that is “very unusual...”

Signature

- Develop mechanism to detect footprint

Response

- Search enterprise, mitigate discoveries

Prevention

- Release methods to prevent reoccurrence

Covert Channels via Stego & Crypto

- Covert Channel
 - Protocol Abuse
 - Storage or timing based
 - Steganography = Art of hiding data in carrier images
 - Pretty much anywhere data can fit
- Cryptography
 - Plaintext, Encrypted Text

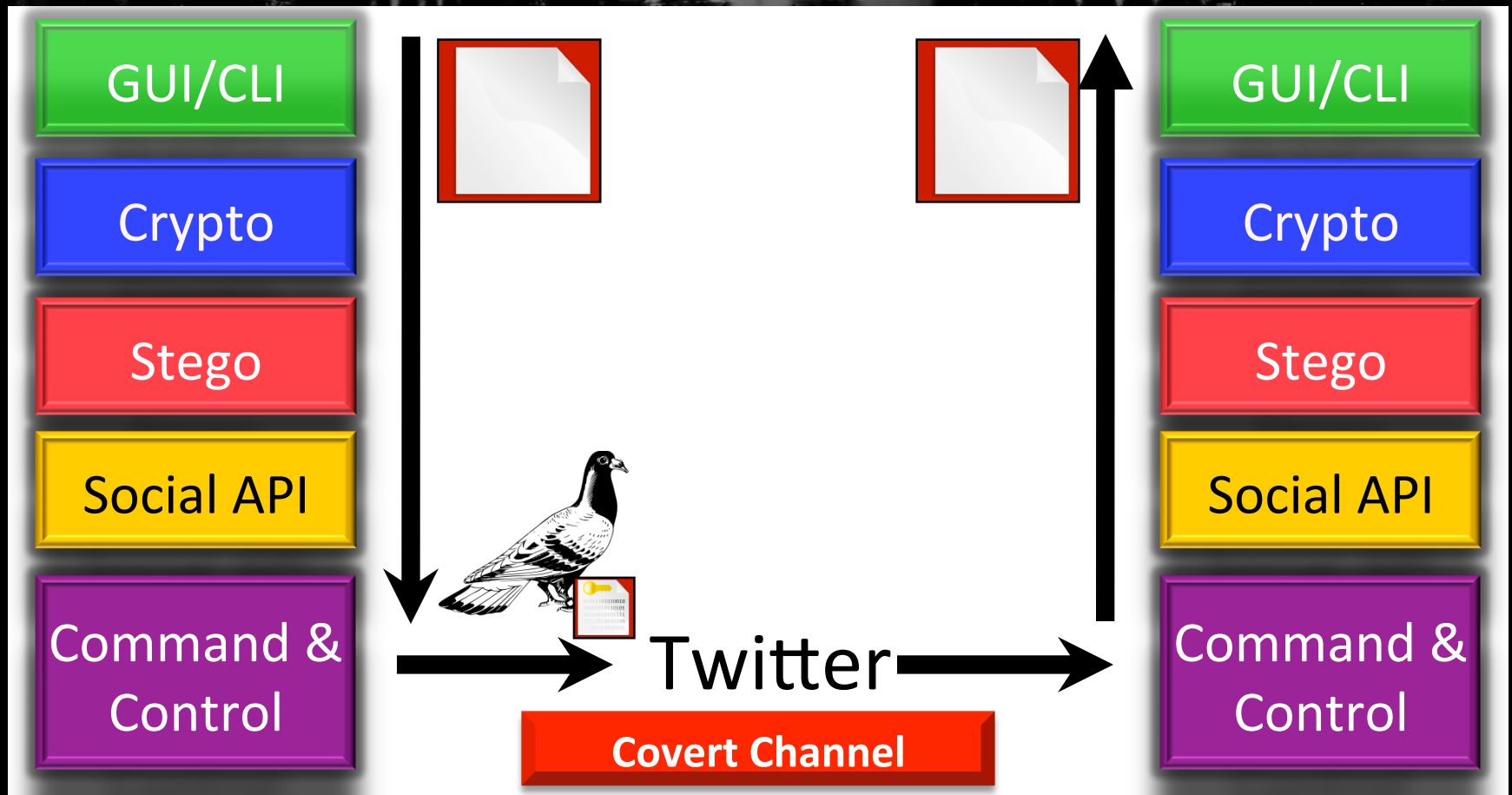


blackhat
USA 2012



MODULE OVERVIEW

Graphical Overview





blackhat
USA 2012

GUI/CLI Demo

Modules & Concepts

```
mbpro1s-MacBook-Pro:snsca2 mbpro1$ java -jar X0rCrypto.jar
Usage: X0r.jar
    -e <filepath> <keypath> [output file]
    -eS <message byte values> <key>
    -d <filepath> <keypath> [output file]
    -dS <cipherText byte values> <key>
    -g <Key Byte Size> [output file]
    -gS <Key Byte Size>
mbpro1s-MacBook-Pro:snsca2 mbpro1$
```


Modules & Concepts

```
mbpro1s-MacBook-Pro:snsca2 mbpro1$ java -jar X0rCrypto.jar -g 10 secretkey
mbpro1s-MacBook-Pro:snsca2 mbpro1$ hexdump secretkey
00000000 e6 ff 36 b3 d4 8f 18 c2 9d d7
0000000a
```



Steganography Module Video



Q: How do you deal with compression?

A: It depends!

Modules & Concepts

Social API Module

```
mbpro1s-MacBook-Pro:snscat2 mbpro1$ java -jar TwitterAPI.jar -h
Usage: twitter.jar
    -upload <username> <password> <file path> <status msg>
    -downloadall <username> <download path>
    -downloadnew <username> <download path>
    -getallfilenames <username>
    -getnewfilenames <username>
    -reinventory <image link> <download path> <Twitter Handle>
    -new <filename> <username>
mbpro1s-MacBook-Pro:snscat2 mbpro1$
```


Modules & Concepts

Social API Module

```
mbpro1s-MacBook-Pro:snsca2 mbpro1$ java -jar TwitterAPI.jar -downloadall NatureL0ver121 ./
1
mbpro1s-MacBook-Pro:snsca2 mbpro1$ ls
483068539.jpg      485242079.jpg      490285734.png      490286035.png
483068564.jpg      485242185.jpg      490285799.png      501713039.png
485092307.jpg      485245500.jpg      490285855.png      501713119.png
485234569.jpg      485257662.jpg      490285906.png      NatureL0ver121.txt
485234670.jpg      489309766.jpg      490285992.png      TwitterAPI.jar
mbpro1s-MacBook-Pro:snsca2 mbpro1$
```

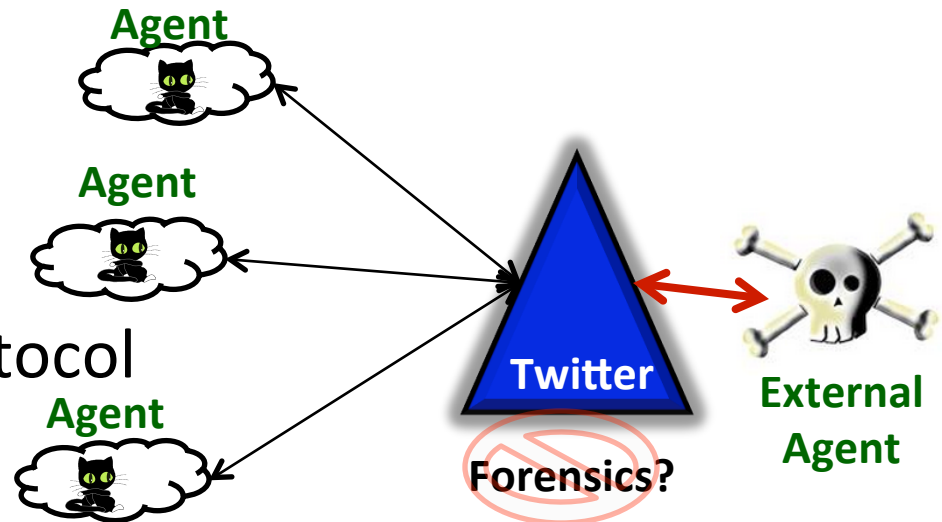

Modules & Concepts

Social API Module

```
mbpro1s-MacBook-Pro:sncat2 mbpro1$ cat NatureL0ver121.txt
501713119.png
501713039.png
490286035.png
490286035.png
490285992.png
490285906.png
490285855.png
490285799.png
490285734.png
489309766.jpg
485257662.jpg
485245500.jpg
485242185.jpg
485242079.jpg
485234670.jpg
485234569.jpg
485092307.jpg
483068564.jpg
483068539.jpg
mbpro1s-MacBook-Pro:sncat2 mbpro1$
```

Automating SNSCat

- Botnet Functionality
- Basics:
 - Controller
 - Dropper/Agent
 - Communication Protocol
- Fully Modular
 - Downloader, Uploader, Parser Modules
 - Establish Connected Agents
 - Exchange Commands, View Updates





Botnet Module Demo



blackhat
USA 2012



MITIGATION

Mitigation Strategies

- Accept that network-based Data Loss Prevention has limits
- Separate non-critical assets from critical assets
- Move beyond the boundary
- Image Compression/Alteration



QUESTIONS?



SNSCAT

What You Don't Know About Sometimes Hurts the Most

Dan Gunter & Solomon Sonya

Contact: SNSCat2012@gmail.com

blackhat
USA 2012



blackhat
USA 2012



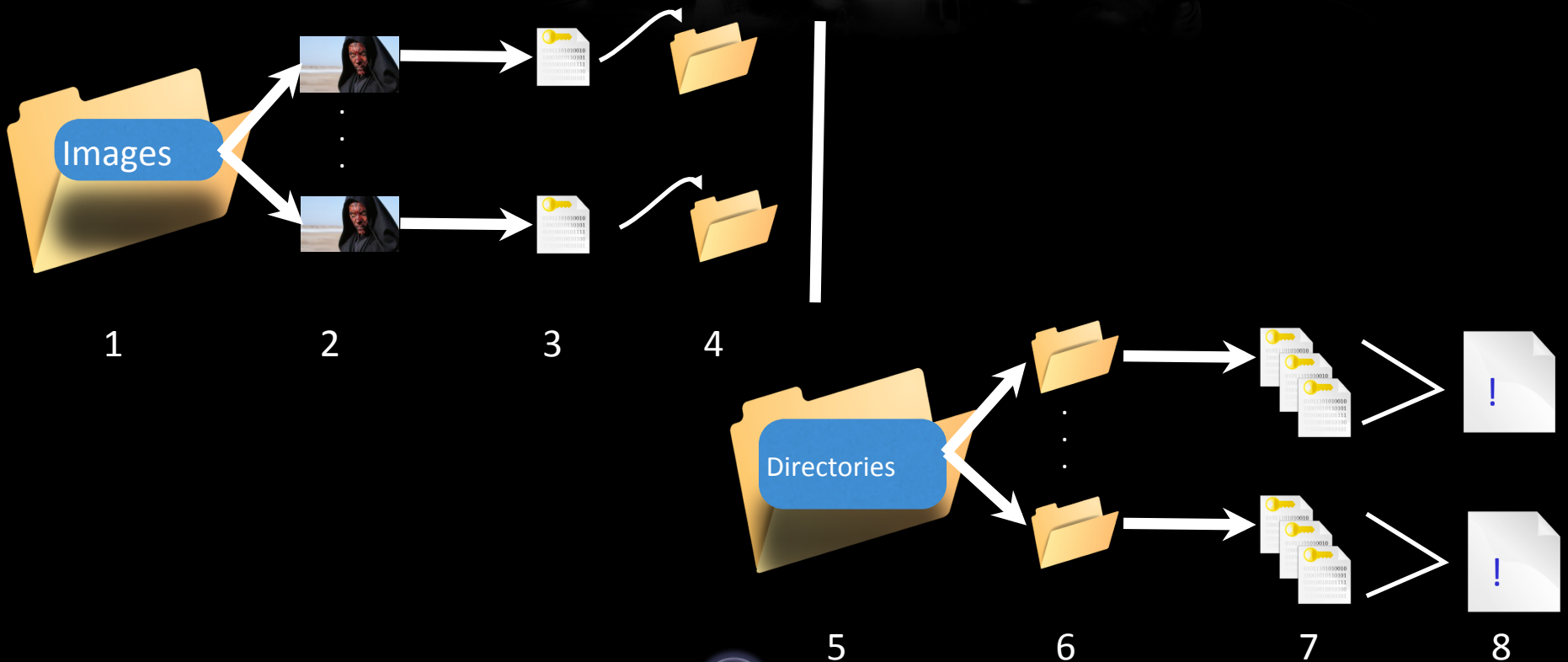
Hidden Slides (Backup)

- Alg behind LSB
- • Convert Source Data to bytes
- • `data[] = convertSourceToBytes();`
- • Determine indices to place each bit
- • **Populate embed location**
- • **`embedSize = sizeof(source data bytes) * 8;`**
- • **`indexLoc[] = new int[embedSize];`**
- • **`locations[] = populateLocations(indexLoc, carrierFileSize);`**
- • **Embed, re-compose, upload**

Hidden Slide (Embed Bits)

- Embed Bits
- position = 0;
- for(i; embedSize...)
- {
- currByte = embedData[i];
- arr[0] = (currByte >>> 7) & 1;
- ...
- arr[7] = (currByte >>> 0) & 1;
- for(j < 8)
- {
- indexToMod = locations[position++];
- carrierByteToMod = carrier[indexToMod];
- carrierByte_LSB_Cleared = carrierByteToMod & 0xFE;
- **newByte_LSB = (byte)(carrierByte_LSB_Cleared | arr[j]);**
- carrier[indexToModify] = newByte_LSB;
- ...
- }
- ...
- }
- • **Extraction: populate locations > extract bits > shift bits > save byte**
- • **Re-Composing: carrier image > fragment > compress > Source Data**

ReCompose Pictogram!!!



SNSCat Framework version 2.0 - BETA

- Action
- Source Data
- Encryption
- Carrier Image
- Upload / Download
- JAR Interaction Content
- Cookie JAR
- Implant Communications

Settings Connected Agents Network Commands

Drop Box

Drop Box

Modules

Download Bin: F:\Blackhat\FINAL\StegoMakerWorkspace\Download

Client Top Folder: F:\Blackhat\FINAL\StegoMakerWorkspace\Client Registration

Acct Synchronization: F:\Blackhat\FINAL\StegoMakerWorkspace\Acct Sync

Parse Directory: F:\Blackhat\FINAL\StegoMakerWorkspace\Parse

Connection Data: F:\Blackhat\FINAL\StegoMakerWorkspace\Connection Data

Connected Clients

Account Name:

Account PW:

Account Type:

Added Accounts

[Twitter] snscaat_implant1

[Twitter] snscaat_implant2

[Twitter] snscaat_implant3

Number of Connected Clients: 3

ServerSocket

8080

Number of Connected Agents: 0

Downloader Activation Update Interval

☒ Sec ☐ Min ☐ Hr

Next Update at: Not Started

Connectivity Status

Drop Box Info: Complete

External Modules: Complete

Socket Connection: Open

Update Interval: Established

Downloader Module: Connected

Uploader Module: Connected

Parser Module: Connected

Send Network Command to Implants

Select

0 B

0 B

1

1

None Selected

Commands

SNSCat Framework version 2.0 - BETA

- Action
- Source Data
- Encryption
- Carrier Image
- Upload / Download
- JAR Interaction Content
- Cookie JAR
- Implant Communications

Settings Connected Agents Network Commands

Commands

Broadcast Acct: sncatBroadcast Broadcast PW: 123456

Acct Type: Twitter.com

Add Command

Remove All

Browse Carrier Image: joMakerWorkspace\JARs\Upload\CanvasFiles.png

Tag: Awesome Day Friday

Carrier Size: 0 B Command(s) Size: 0 B

Remove	Cmd: 0	Parameters: systeminfo	Response: Implant Account
Remove	Cmd: 0	Parameters: dir /s c:/	Response: Implant Account
Remove	Cmd: 2	Parameters: c:\Special Documents*	Response: Implant Account

Command Recipients

Broadcast Account

[Twitter] sncat_implant1
[Twitter] sncat_implant2
[Twitter] sncat_implant3

Network Traffic

Send Network Command to Implants

Select

0 B

0 B

1

1

None Selected

Commands

Upcoming Features

- PKI to validate commands only sent from the Controller
- Larger dispersal (Twitter, Facebook, Youtube)
- Embed stego in Audio and Video Files
- Exchange Large File Types
- Explore Smart Phone platforms

Hidden Slides (Importing Modules)

- Building Modules
- • GUI/CLI Conventions
- • Not really any specifics
- • The sky is the limit

Hidden Slides (Modules)

- Crypto Module Conventions
- • -e <filename> <keyfile> -- encrypts file with key
- • -d <filename> <keyfile> -- decrypts file with key
- • -g -- generates key(s) and stores in TMP
- • -h -- help

Hidden Slides (Additional Modules)

- Depends on what the audience would like to see