Operation Shady RAT

Tim Duffy
4/2/12

What is Shady RAT?

- Shady RAT (Remote Administration Tool) is an ongoing series of attacks that started in 2006
- Potentially one of the largest ever cyber-attacks
- Targeted phishing attack using custom code
- 71 organizations in 14 different countries were attacked between 2006 and 2011

21	
US Federal Government	6
US State Government	5
US County Government	3
Canadian Government	2
Vietnam Government	1
Taiwan Government	1
US Government Contractor	1
United Nations	1
Indian Government	1

6	
Construction/ Heavy Industry	3
Steel Industry	1
Energy	1
Solar Power	1

13	
Electronics Industry	3
Computer Security	2
Information Technology	2
Satellite Communications	2
News Media	2
Information Services	1
Communications Technology	1

13	
Defense Contractor	13

6	
Real Estate	2
Accounting Industry	2
Agriculture	1
Insurance	1

12	
International Sports	5
Economics/ Trade	2
Think Tanks	2
International Government/ Economics/ Trade	1
Political Non-Profit	1
US National Security Non-Profit	1

Source: McAfee

How Does Shady RAT Work?

Three Stage Attack:

1) **Phishing Attack and Trojan Installation**

2) Execution Of the Trojan

3) Data Collection

Stage 1: Phishing

- Individuals are sent a malicious file via email

- Excel files use an exploit that corrupts memory in such a way that function calls can be made

- Opening the file drops a clean version of the document, and installs a trojan file.

How Does Shady RAT Work?

Three Stage Attack:

1) Phishing Attack and Trojan Installation

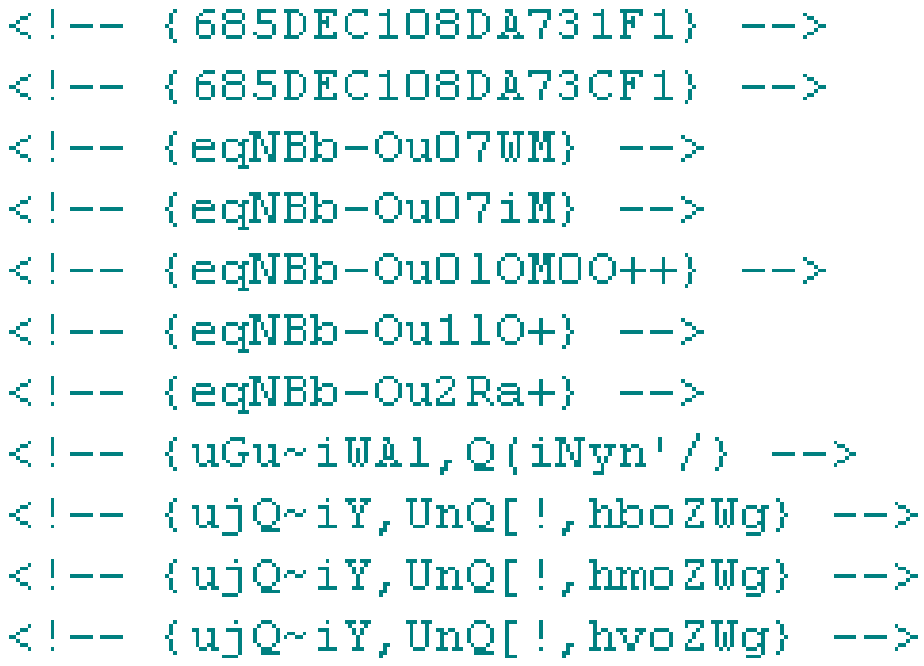
2) Execution Of the Trojan

3) Data Collection

Stage 2: Executing the Trojan

- The Trojan connects to a website hardcoded in itself.
  - Site is an HTML file with some random content

- Steganography is used to hide commands (such as run *FILE*, or *connect to IP:PORT)* from plain view
  - Encrypted commands were hidden in comments
  - Bits representing the commands were mathematically built into the pixels of an image



```
<!-- {685DEC108DA731F1} -->
<!-- {685DEC108DA73CF1} -->
<!-- {eqNBb-Ou07WM} -->
<!-- {eqNBb-Ou07iM} -->
<!-- {eqNBb-Ou01OMDO++} -->
<!-- {eqNBb-Ou11O+} -->
<!-- {eqNBb-Ou2Ra+} -->
<!-- {uGu~iWAl,Q(iNyn'/} -->
<!-- {ujQ~iY,UnQ[!,hboZWg} -->
<!-- {ujQ~iY,UnQ[!,hmoZWg} -->
<!-- {ujQ~iY,UnQ[!,hvoZWg} -->
```

Some commands for the trojan were encrypted, converted to base-64 encoding, and put in the HTML comments

Other commands were hidden within the bits of an image (ex: the 2 least significant bits of each pixel)

How Does Shady RAT Work?

Three Stage Attack:

1) Phishing Attack and Trojan Installation

2) Execution Of the Trojan

3) Data Collection

Stage 3: Data Collection

- When a Trojan receives a *connect* command, it establishes a remote shell

- An attacker at a remote site can directly issue shell commands to a compromised computer

The Trojan periodically checks the server for commands (such as *uploading/downloading a file from the server, running a file, or sending a report*)

Sources

http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109

http://www.verisigninc.com/sv_SE/products-and-services/network-intelligence-availability/idefense/public-vulnerability-reports/articles/index.xhtml?id=832

http://www.symantec.com/connect/blogs/truth-behind-shady-rat

http://www.computerworld.com/s/article/9218910/_Shady_RAT_hacking_claims_overblown_say_security_firms?taxonomyId=82&pageNumber=2

www.mcafee.com/us/resources/white.../wp-ope**rat**ion-**shady-rat**.pdf