

Ryan Brodsky

ICS 482

10/15/19

## InfoSec Lab: Crafting and Deploying Malware Using a Remote Access Trojan (RAT)

The collage consists of several overlapping screenshots from a virtual machine environment. The primary window is a Zenmap (Nmap) interface. The top screenshot shows the 'Ports / Hosts' tab with a list of open ports and their corresponding banner messages. The bottom screenshot shows the 'Hosts' tab with a list of hosts and their services. The right side of the collage shows a Windows 8.1 desktop with a Remote Access Trojan (RAT) running, displaying a command prompt and a file explorer window. The desktop background is a blue and black abstract design. The taskbar at the bottom shows the Start button, a search bar, and several application icons including Internet Explorer, File Explorer, and the Zenmap application. The system tray on the right shows the date and time as 5:44 PM on 10/15/2019.

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-access-trojan-rat

Assignments - ICS 482-01 Vuln... Mail - Ryan Brodsky - Outlook Crafting and D...

Crafting and Deploying Malware Using a Remot...

External Windows 8.1 Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

cmd - Shortcut

Zenmap

Target: 203.0.113.100 Profile: Intense scan

Command: nmap -T4 -A -v 203.0.113.100

Hosts Services

OS: Host

203.0.113.100

Starting Nmap 5.51 ( http://nmap.org ) at 2016-05-13 13:39 Eastern Summer Time

NSM loaded 57 scripts for scanning.

Initiating Ping Scan at 13:39

Completed Ping Scan at 13:39, 0.03s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 13:39

Completed Parallel DNS resolution of 1 host. at 13:39, 0.02s elapsed

Initiating SYN Stealth Scan at 13:39

Scanning 203.0.113.100 [1000 ports]

Discovered open port 23/tcp on 203.0.113.100

Discovered open port 3389/tcp on 203.0.113.100

Discovered open port 80/tcp on 203.0.113.100

Discovered open port 3306/tcp on 203.0.113.100

Discovered open port 25/tcp on 203.0.113.100

Discovered open port 21/tcp on 203.0.113.100

Discovered open port 443/tcp on 203.0.113.100

Discovered open port 5432/tcp on 203.0.113.100

Discovered open port 8180/tcp on 203.0.113.100

Completed SYN Stealth Scan at 13:39, 10.03s elapsed (1000 ports)

Initiating Service scan at 13:39

PORTS / HOSTS TAB

Hosts Services

OS: Host

203.0.113.100

21 tcp open ftp Microsoft Ftpd

23 tcp open telnet

25 tcp open smtp Microsoft ESMTP 7.0.6001.18000

80 tcp open http Apache httpd 2.2.14 ((Win32) DAV/2

443 tcp open http Apache httpd 2.2.14 ((Win32) DAV/2

1099 tcp open rmi Java RMI Registry

3306 tcp open mysql MySQL 5.0.51a-Jubun

3389 tcp open microsoft-rdp Microsoft Terminal Se

5432 tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

8180 tcp open http Apache Tomcat/Coyote JSP engine

OPEN PORTS WITH CORRESPONDING BANNER MESSAGES

5 Select Scan from the menu bar and then select Quit to close Z...

asked regarding Unsavd changes, select Close anyway.

cmd - Shortcut

Zenmap

Target: 203.0.113.100 Profile: Intense scan

Command: nmap -T4 -A -v 203.0.113.100

Hosts Services

OS: Host

203.0.113.100

21 tcp open ftp Microsoft Ftpd

23 tcp open telnet

25 tcp open smtp Microsoft ESMTP 7.0.6001.18000

80 tcp open http Apache httpd 2.2.14 ((Win32) DAV/2

110 tcp open pop3 Apache httpd 2.2.14 ((Win32) DAV/2

443 tcp open http Apache httpd 2.2.14 ((Win32) DAV/2

1099 tcp closed rmi Java RMI Registry

3306 tcp open mysql MySQL 5.0.51a-Jubun

3389 tcp open microsoft-rdp Microsoft Terminal Se

5432 tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

8180 tcp closed sampleflag999818

Windows 8.1 Enterprise Build 9600

5:44 PM 10/15/2019

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-965545/External%20Windows%208.1%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

### Crafting and Deploying Malware Using a Remote...

Test completed Pwd/Sec: 66 Tested: 18053 Time: 4:33

LAUNCHING THE ATTACK

11 After about 2-4 minutes, the attack will be completed and the will be displayed.

Test completed Pwd/Sec: 66 Tested: 18053 Time: 4:33

TARGET'S PASSWORD REVEALED - SUCCESS!

Note: Close the program by clicking the red X in the top right corner.

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-965545/External%20Windows%208.1%20Scoring

View Fullscreen Send Ctrl+Alt+Delete

### Crafting and Deploying Malware Using a Remote...

Test completed Pwd/Sec: 66 Tested: 18053 Time: 4:33

SAMPLEFLAG

Challenge Sample #1

5 Close the file by clicking the X in the right hand corner and close Explorer by clicking the X in the right hand corner.

6 Get the information for below Challenge Flag by using the same techniques from the previous steps.

Challenge #2

7 Double-click on the Malware folder on the Windows 8.1 desktop.

Test completed Pwd/Sec: 66 Tested: 18053 Time: 4:33

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-access

Assignments - ICS 482-01 Vuln... Mail - Ryan Brodsky - Outlook Crafting and Deploying Malware Using a Remote Access

### Crafting and Deploying Malware Using a Remote Access

Spooft extensions  
Users  
changelog.txt  
comet.db  
config.ini  
DarkComet.exe  
flag3.txt  
GeoIP.dat  
readme\_help.txt  
sampleflag.txt  
sqlite3.dll

SAMPLEFLAG

11 Get the information for below Challenge Flag by using the same techniques from the previous steps.

Challenge #3

12 Type `exit` and press Enter.

13 Double-click on `DarkComet.exe` to launch the program.

External Windows 8.1 Scoring

View Fullscreen Send Ctrl+Alt+Delete

flag3.txt - Notepad

File Edit Format View Help

flag:717999

Search DarkComet

Type	Size
File folder	
File folder	
File folder	
File folder	
File folder	
File folder	
File folder	
Text Document	8.1 KB
Data Base File	88 KB
Configuration settin...	8 KB
Application	11,547 KB
Text Document	1 KB
DAT File	1,171 KB
Text Document	3 KB
Text Document	1 KB
Application extension	511 KB

Windows 8.1

Type here to search

5:54 PM 10/15/2019

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-access

Assignments - ICS 482-01 Vuln... Mail - Ryan Brodsky - Outlook Crafting and Deploying Malware Using a Remote Access

### Crafting and Deploying Malware Using a Remote Access

Firefox Malware on Desktop

Run as administrator  
Troubleshoot compatibility  
Pin to Start  
7-Zip  
CRC SHA  
Share with  
Pin to Taskbar  
Send to  
Cut  
Copy  
Create shortcut  
Delete  
Rename  
Properties

External Windows 8.1 Scoring

View Fullscreen Send Ctrl+Alt+Delete

Create a new stub - Installer version < v5.0 >

Application Tools

Documents

File Home Share View Manage

Search Documents

Name	Date modified	Type	Size
ca_setup.exe	7/29/2015 8:55 PM	Application	8,051 KB
desktop.ini	2/12/2015 12:00 PM	Configuration sett...	1 KB
firefox.exe	10/15/2019 6:56 PM	Application	349 KB
ggg4win-2.3.1.exe	4/25/2016 1:34 AM	Application	26,133 KB
img7.jpg	6/18/2013 8:56 AM	JPEG image	155 KB

5 Items 1 Item selected 349 KB

Windows 8.1

Type here to search

5:57 PM 10/15/2019



The collage consists of several screenshots from a video tutorial. The top row shows a Windows 8.1 desktop with a 'Crafting and Deploying Malware Using a Remote Desktop' window. The middle row shows a Windows Server 2008 desktop with a 'Crafting and Deploying Malware Using a Remote Desktop' window. The bottom row shows a Windows 8.1 desktop with a 'Crafting and Deploying Malware Using a Remote Desktop' window. The right side of the collage shows a Windows 8.1 desktop with a 'Crafting and Deploying Malware Using a Remote Desktop' window. The bottom row also includes a 'DarkComet RAT Console' window showing a list of users and a 'DarkComet RAT' window showing a list of files.

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-access

Assignments - ICS 482-01 Vuln... Mail - Ryan Brodsky - Outlook Crafting and Deploying Malware

### Crafting and Deploying Malware Using a Remote Access Tool

Target: blueprint.jpg (1/4)

FILE TRANSFER

14 Click the Refresh button to view the stolen files on the attacker's system.

File Manager: [SERVER / administrator], Socket: [1120]

Name	Type	Size	File creation
My Music	Folder		12/30/1899
My Pictures	Folder		12/30/1899
My Videos	Folder		12/30/1899
blueprint1.jpg	JPEG image	0.00 Bytes	4/26/2018
blueprint2.jpg	JPEG image	0.00 Bytes	4/26/2018
blueprint3.jpg	JPEG image	0.00 Bytes	4/26/2018
blueprint4.jpg	JPEG image	0.00 Bytes	4/26/2018
blueprint5.jpg	JPEG image	0.00 Bytes	4/26/2018
desktop.ini	Configuration sett...	276.00 Bytes	4/26/2018

File Manager: [SERVER / administrator], Socket: [1120]

Name	Type	Size	File creation
My Music	Folder		12/30/1899
My Pictures	Folder		12/30/1899
My Videos	Folder		12/30/1899
blueprint1.jpg	JPEG image	1.80 MB	2/26/2018
blueprint2.jpg	JPEG image	171.56 KB	2/26/2018
blueprint3.jpg	JPEG image	55.25 KB	2/26/2018
blueprint4.jpg	JPEG image	107.01 KB	2/26/2018
blueprint5.jpg	JPEG image	107.01 KB	2/26/2018
desktop.ini	Configuration sett...	276.00 Bytes	4/26/2018

18 items 1 item selected 11.2 MB

cmd - Shortcut

6 items

Windows 8.1

Type here to search

6:02 PM 10/15/2019

External Windows 8.1 Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-access

Assignments - ICS 482-01 Vuln... Mail - Ryan Brodsky - Outlook Crafting and Deploying Malware

### Crafting and Deploying Malware Using a Remote Access Tool

BLUEPRINT #1

21 Get the information for the below Challenge Flag by using the same techniques from the previous steps.

Challenge #4

22 Get the information for the below Challenge Flag by using the same techniques from the previous steps.

Challenge #5

23 Get the information for the below Challenge Flag by using the same techniques from the previous steps.

Challenge #6

Press the STOP button to complete the lab.

Public Documents

Local Disk (C:) > Users > Public > Public Documents

My Videos

blueprint1.jpg

blueprint2.jpg

blueprint3.jpg

blueprint4.jpg

blueprint5.jpg

8 items 1 item selected 1.80 MB

Windows 8.1

Type here to search

6:04 PM 10/15/2019