```
call
                                                                                                sub_314623
                                                                                         test
                                                                                                eax, eax
                                                                                                short loc_31306D
                                                                                         CIID
                                                                                                [ebp+arg_0], ebx
                                                                                                short loc 313066
                                                                                                eax, [ebp+var_70]
                                                                                                eax, [ebp+var_84]
                                                                                                short loc 313066
                                                                                                eax, [ebp+var_84]
                                                                                         push
                                                                                                681
                                                                                          push
                                                                                                es1
                                                                                          push
                                                                                                eax
                                                                                                edi
                                                                                         MOV
                                                                                                [ebp+arg_0], eax
                                                                                         call
                                                                                                sub_31486A
                                                                                          test
                                                                                                eax, eax
                                                                                                short loc 31306D
                                                                                         push
                                                                                                681
                                                                                         lea
                                                                                                eax, [ebp+arg_0]
                                    Introduction
                                                                                                esi, 1D0h
                                                                                          push
                                                                                                881
                                                                                          push
                                                                                                [ebp+arg_4]
                                                                                          push
                                                                                         call
                                                                                                sub 314623
                                                                                         test
                                                                                                eax, eax
                                                                                                 short loc_31306D
                                                                                                [ebp+arg_0], esi
                                                                                                short loc 31308F
                                      Malware Analysis
                                                                                                              ; CODE XREF: sub 312FD8
                                                                                                              : sub 312FD8+55
                                                                                                0 Dh
                                CSCI 4976 - Fall 2015
                                                                                                sub_31411B
                                                                                                              ; CODE XREF: sub 312FD8
                                                                                                              / sub 312FD8+49
                                          Branden Clark
                                                                                                sub 3140F3
                                                                                          test
                                                                                                eax, eax
                                                                                                short loc 31307D
                                                                                         call
                                                                                                sub_3140F3
                                                                                                short loc_31308C
                                                                                          THE
                                                                            loc_31307D:
                                                                                                              ; CODE XREF: sub 312FD8
                                                                                                sub_3140F3
                                                                                                eax, Offffh
                                                                                                eax, 80070000h
Malware - 09/01/2015
                                                       Introduction
                                                                            loc_31308C:
                                                                                                              ; CODE XREF: sub 312FD8
                                                        (cc)) BY-NC
                                                                                                [ebp+var 4], eax
```

push

edi

#### Lecture Overview

- 1. Syllabus
- 2. Course Overview
- 3. Basic Analysis

```
push
                         edi
                call
                         sub_314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                push
                push
                MOV
                         [ebp+arg_0], eax
                call
                         sub 31486A
                test
                         eax, eax
                         short loc_31306D
                push
                         681
                lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub_3140F3
                         eax, Offffh
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
                         [ebp+var 4], eax
```

#### Course Details

- Malware Analysis
  Course Number: CSCI 4976
  Credit Hours: 4
  - Semester / Year: Fall 2015
  - Meeting Days: Tuesday/Friday 12-2PM
  - Room Location: Sage 2112
  - Course Website: TODO
    - http://security.cs.rpi.edu/courses/malware-fall2015/
    - http://rpis.ec/malware
  - Prereqs:
    - CSCI 2500 Computer Organization
    - ECSE 2660 Computer Architecture, Networks, and Operating Systems

```
| call sub_3140F3 | and eax, 0FFFFn | or eax, 80070000h | Introduction | loc_31308C:
```

loc\_31307D:

loc 313066:

call

```
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi

push eax
push edi

mov [ebp+arg_0], eax
call sub_31486A
test eax, eax
jz short loc_31306D
push esi
lea eax, [ebp+arg_0]
push eax
mov esi, 1D0h
push esi
push esi
push esi
push ecax
mov esi, 1D0h
push esi
push ecax
test eax, eax
test eax, eax
test eax, eax
```

short loc\_31306D [ebp+arg\_0], esi

sub 31411B

short loc 31308C

[ebp+var 4], eax

; CODE XREF: sub 312FD8

: CODE XREF: sub 312FD8

; CODE XREF: sub 312FD8

; CODE XREF: sub 312FD8

; sub 312FD8+55

sub 312FD8+49

sub\_314623

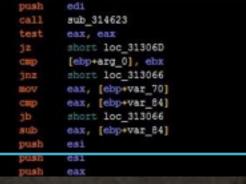
short loc\_31306D [ebp+arg\_0], ebx

eax, [ebp+var 70]

push

### Instructor

- Instructor: Dr. Bülent Yene
  - Office: Lally 310
  - Email: <u>yener@cs.rpi.ed</u>ı





loc\_31307D: ; CODE XREF: sub\_312FD8

call sub\_3140F3
and eax, OFFFFh
or eax, 80070000h

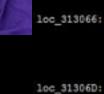
### Malware Mentors



Branden (Clark)



Aaron (Aidielse)



loc\_31306D:

push

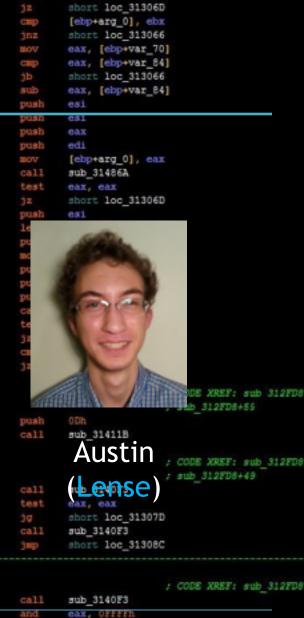
call

test

edi

sub\_314623

eax, eax



loc\_31307D:

eax, 80070000h



push edi
call sub\_314623
test eax, eax
jz short loc\_31306D
cmp [ebp+arg\_0], ebx
jnz short loc\_313066
mov eax, [ebp+var\_70]
cmp eax, [ebp+var\_84]
jb short loc\_313066
sub eax, [ebp+var\_84]
push esi

call

[ebp+arg\_0], eax

[ebp+arg\_4]

- Good to see lots of familiar faces!
- RPISEC meetings are <u>Friday 5-7 PM</u> in <u>DCC 324</u>
- Come learn other topics in computer security
  - Web hacking
  - Malware analysis
  - Reverse Engineering
  - Digital Forensics
  - So so much more
- Meet people from industry, get internships/jobs
- Read more <a href="http://rpis.ec">http://rpis.ec</a>

```
call sub_314623
test eax, eax
jz short loc_31306D
cmp [ebp+arg_0], esi
jz short loc_31308F

; CODE XREF: sub_312FD8
; sub_312FD8+55

push ODh
call sub_31411B

; CODE XREF: sub_312FD8
; sub_312FD8+49
```

[ebp+var 4], eax

: CODE XREF: sub 312FD:

loc 313066:

loc\_31306D:

loc 31308C:

#### Office Hours

- Office hours:
  - Wed 7-10 PM @ Sage 5101
- Come hang out at RPISEC hack nights!
  - Ask questions, get extra help with the class
  - Collaborate on Projects/Labs Labs Labs
  - Work on security projects, challenges,
     etc

```
loc_31307D:
call sub_
```

loc 31308C:

push

edi sub\_314623 eax, eax

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax sub\_31486A

short loc 31306D

eax, [ebp+arg\_0]

all sub\_3140F3
nd eax, Offffn
r eax, 80070000h

short loc 31308C

[ebp+var 4], eax

sub 312FD8+55

; CODE XREF: sub 312FD8

# Digital Office Hours (IRC)

short loc 31306D [ebp+arg 0], ebx eax, [ebp+var 84] short loc 313066

push

edi sub 314623

- The RPISEC IRC http://rpis.ec [ebp+arg\_0], eax
  - server: irc.rpis.ec
  - port: 6667 (6697 for SSL)
  - room: #rpisec

esi, 1D0h [ebp+arg\_4] sub 314623 test eax, eax short loc 31306D [ebp+arg\_0], esi short loc 31308F

[ebp+var\_84]

short loc 31306D

eax, [ebp+arg\_0]

- Way faster than emailing back and forth
- Some of us are usually on at ridiculous hours sub\_3140F3
  - basically a 24/7 channel

; CODE XREF: sub 312FD: sub\_3140F3 : CODE XREF: sub 312FD

short loc 31307D sub 3140F3

short loc 31308C

[ebp+var 4], eax

7 sub 312FD8+49

loc\_31307D:

### **Options of Last Resort**

- Email us
  - malware\_ta@cs.lists.rpi.edu
    - temporarily down
  - malware\_ta@rpis.ec
    - use this for now

```
[ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var 84]
                         short loc 313066
                         eax, [ebp+var_84]
                         [ebp+arg_0], eax
                call
                         sub 31486A
                 test
                         eax, eax
                         short loc 31306D
                 push
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                 push
                 push
                         [ebp+arg_4]
                 call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, Offffh
                         eax, 80070000h
```

push

test

edi sub\_314623

eax, eax

short loc\_31306D

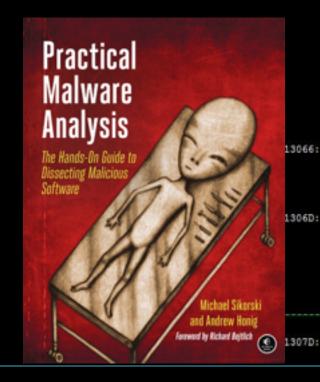
### Required Textbooks

push edi
call sub\_314623
test eax, eax
jz short loc\_31306D
cmp [ebp+arg\_0], ebx
jnz short loc\_313066
mov eax, [ebp+var\_70]
cmp eax, [ebp+var\_84]
jb short loc\_313066
sub eax, [ebp+var\_84]
push esi
push esi

Practical Malware Analysis by Michael Sikorski and

**Andrew Honig** 

- ISBN 978-1593272906

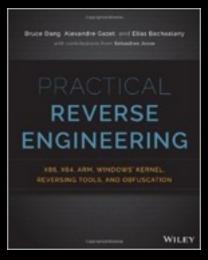


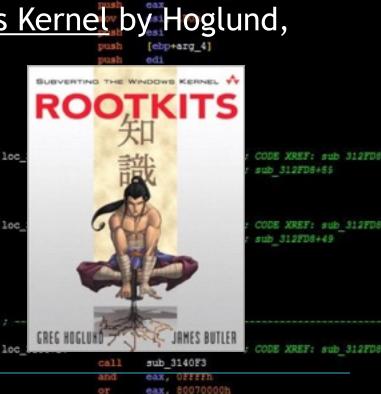
```
sub 31486A
test
        eax, eax
        short loc 31306D
lea
        eax, [ebp+arg_0]
        esi, 1D0h
push
        881
push
        [ebp+arg_4]
push
call
        sub 314623
test
        eax, eax
        short loc_31306D
        [ebp+arg 0], esi
        short loc 31308F
                          ; CODE XREF: sub 312FD8
                          ; sub 312FD8+55
push
call
        sub 31411B
                         ; CODE XREF: sub 312FD8
                         ; sub 312FD8+49
call
        sub 3140F3
test
        eax, eax
        short loc 31307D
call
        sub_3140F3
        short loc 31308C
THE C
                         ; CODE XREF: sub 312FD8
        sub 3140F3
```

eax, Offffh

### Suggested Textbooks

- Practical Reverse Engineering by Dang, Bachaalany
  - ISBN 978-1118787311
- Rootkits: Subverting the Windows Kernel by Hoglund, Butler
  - ISBN 978-0321294319





push

call

test

edi

sub 314623

short loc 31306D

[ebp+arg\_0], ebx short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

short loc 31306D

eax, [ebp+arg\_0]

eax, eax

#### Grade Breakdown

- Labs 48%
  - 12 labs @ 4% each
  - Lab attendance is MANDATORY as the first p must be checked off in person
- Malware Analysis 42%
  - 3 Projects @ 10% each
  - Final Project @ 12%
  - Like a big lab, but over a few weeks
- Quizzes 10%
  - **10 quizzes** @ 1% each
  - Small, quick, easy, from the reading loc 31307D:

```
test
        eax, eax
        short loc 31306D
        [ebp+arg_0], ebx
        short loc 313066
        eax, [ebp+var 70]
        eax, [ebp+var_84]
        short loc 313066
        eax, [ebp+var_84]
        [ebp+arg_0], eax
call
        sub 31486A
        short loc 31306D
      art is due and
        [ebp+arg_4]
call
        sub 314623
test
        eax, eax
        short loc 31306D
        [ebp+arg 0], esi
        short loc 31308F
                         ; CODE XREF: sub 312FD8
                         ; sub 312FD8+55
push
        sub 31411B
                        ; CODE XREF: sub 312FD8
                        ; sub 312FD8+49
        sub 3140F3
        eax, eax
        short loc 31307D
        sub_3140F3
        short loc 31308C
THE C
                        ; CODE XREF: sub 312FD:
```

push

edi sub\_314623

loc 313066:

sub\_3140F3

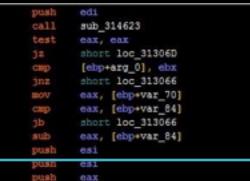
eax, 80070000h

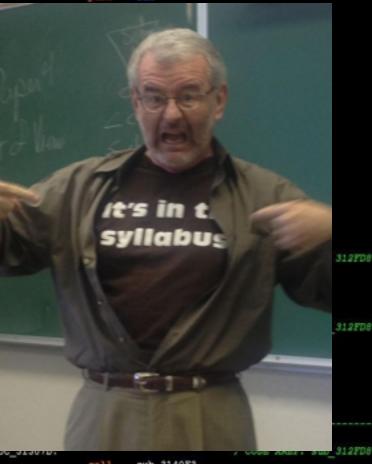
# Syllabus

READ THE SYLLABUS

Well written, full of details

• It's on the course website rpis.ec/malware







[ebp+var 4], eax

#### Lecture Overview

- 1. Syllabus
- 2. Course Overview
- 3. Basic Analysis

```
push
                         edi
                call
                         sub_314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                push
                         esi
                push
                MOV
                         [ebp+arg_0], eax
                call
                         sub 31486A
                test
                         eax, eax
                         short loc_31306D
                push
                         681
                lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc_31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub_3140F3
                         eax, Offffh
                         eax, 80070000h
                                          ; CODE XREF: sub 312FD8
```

## A typical (RPISEC) Class

- Designed and orchestrated by RPISEC (students)
- Other courses
  - CSCI 4968 Modern Binary Exploitation
  - CSCI 4971 Secure Software Principles
  - CSCI 4972 / 6963 Malware Analysis (Spring 2013)
  - CSCI 4974 / 6974 Hardware Reverse Engineering

loc 31308C:

```
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C

;
loc_31307D: ; CODE XREF: sub_312FD8
call sub_3140F3
and eax, OFFFFR
or eax, 80070000h
```

[ebp+var 4], eax

: CODE XREF: sub 312FD

sub\_3140F3

push

edi sub 314623

short loc 31306D

[ebp+arg 0], ebx

eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

eax, [ebp+arg\_0]

esi, 1D0h

[ebp+arg\_4]

### Course Roadmap

```
push edi
call sub_314623
test eax, eax
jz short loc_31306D
cmp [ebp+arg_0], ebx
jnz short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
```

esi, 1D0h

[ebp+arg\_4]

sub 314623

sub 3140F3

short loc\_31306D [ebp+arg\_0], esi short loc\_31308F

eax, eax

test

- Practical Malware Analysis textbook
  - Basic analysis, debugging, reverse engineering, Malware behavior, Windows internals

- Windows Kernel + Rootkits
  - kernel basics, debugging, behavior, stealth
- push ODh
  call sub\_314118

  ; CODE XREF: sub\_312FDi
  ; sub\_312FD8+49

; sub 312FD8+55

- Modern malware threats
  - APTs (Advanced Persistent threats), nation-state sponsored

loc\_31306D:

#### Goals for This Course

```
push edi
call sub_314623
test eax, eax
jz short loc_31306D
cmp [ebp+arg_0], ebx
jnz short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
```

[ebp+arg 4]

short loc 31308C

sub 3140F3

- This will be a very applied, hands on course
  - No data structures, algorithms, cryptography, or cyber policy
  - Every lecture after this you're expected to bring your laptop!
- We will cover technically challenging material rarely touched upon in other classes
  - As an individual you will leave with all the skills necessary to identify, extract, and analyze all features of modern malicious software.

```
Introduction
```

loc\_31307D:

loc 313066:

sub 312FD8+55

: CODE XREF: sub 312FU

### Course Terminology

jz short loc\_31306D

cmp [ebp+arg\_0], ebx

jnz short loc\_313066

mov eax, [ebp+var\_70]

cmp eax, [ebp+var\_84]

jb short loc\_313066

sub eax, [ebp+var\_84]

push esi

push esi

push eax

push edi

mov [ebp+arg\_0], eax

eax, [ebp+arg\_0]

[ebp+arg 4]

sub 31411B

short loc 31308C

sub 314623

push

#### Machine

 A computer, server, sometimes refers to CPU

#### Binary

- An executable such as an .EXE, ELF, MachO or other code containers that run on a machine

loc\_31306D:

loc\_31307D:

loc 31308C:

- Other names: program, application, service (sometimes)

#### Malware

- A piece of software that is intended to perform unwanted activities on a machine
- More as we go along!

call sub\_3140F3
and eax, OFFFFR
or eax, 80070000h

18
; CODE XREF: sub\_312FD:

/ sub 312FD8+55

; sub 312FD8+49

: CODE XREF: sub 312FD6

#### What is malware?

- Some common names...
  - Trojan, virus, worm, RAT, rootkit
    - A piece of software that is intended to unwanted activities on a machine
- Some examples of malicious behavior...
  - Serving ads, stealing data, consuming resources
  - Others?

```
### AND COMPANY OF THE STATE OF OF THE STATE
```

[ebp+var 4], eax

push

test

edi sub 314623

eax, eax

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax sub\_31486A

short loc 31306D

[ebp+arg 4]

sub 314623

short loc 31306D

loc 31308C:

#### [ebp+arg 0], ebx Why do people write mal

- Morris Worm
  - On accident
    - Purpose: "gauge the size of the internet"
    - What happened: Fork bomb



eax, Offffh eax, 80070000h

[ebp+var 4], eax

push

edi sub 314623 eax, eax

short loc 31306D

[ebp+var 84]

[ebp+arg\_0], eax sub 31486A eax, eax

short loc 31306D

eax, [ebp+arg\_0]

[ebp+arg 4]

sub 314623

### Why do people write mal

- In the 90s
  - For the lulz / glory
  - Spread to other machines & display a message



push

sub 314623

short loc\_31306D [ebp+arg\_0], ebx

[ebp+var 84]

[ebp+arg\_0], eax sub\_31486A

short loc 31306D

eax, [ebp+arg\_0]

eax, 80070000h

### Why do people write ma

- Today
  - \$\$\$
- Organizations buy malware
  - Steal passwords, credit cards, bank intellectual property, trade secrets
  - They can use this info or sell it

```
[ebp+arg_0], eax
        sub 31486A
        eax, eax
        short loc 31306D
        eax, [ebp+arg_0]
        esi, 1D0h
        [ebp+arg_4]
call
        sub 314623
                         ; CODE XREF: sub 312FD8
                         : sub 312FD8+55
push
call
        sub 31411B
                         ; CODE XREF: sub 312FD8
                         ; sub 312FD8+49
        sub 3140F3
        eax, eax
        short loc 31307D
        sub 3140F3
        short loc 31308C
                         ; CODE XREF: sub 312FD8
        sub_3140F3
```

push

edi

short loc\_31306D [ebp+arg\_0], ebx

loc\_31307D:

loc\_31306D:

eax, 80070000h

## Why do people write ma

- Future?
  - Cyber warfare, intelligence gathering
- Nation-states
  - Stuxnet
    - Highly advanced
    - Multiple Windows 0-days
    - Targeted and physically destroyed Iranian nuclear centrifuges
  - CNO (Computer Network Operations)
    - CND Defense
    - **CNE** Exploitation
    - CNA Attack

```
[ebp+arg_0], eax
call
        sub 31486A
        short loc 31306D
lea
        eax, [ebp+arg_0]
        esi, 1D0h
        [ebp+arg_4]
call
        sub 314623
test
        eax, eax
        short loc_31306D
        [ebp+arg 0], esi
        short loc 31308F
                         ; CODE XREF: sub 312FD8
                         ; sub 312FD8+55
```

short loc 31306D [ebp+arg 0],

```
; CODE XREF: sub 312FD8
                         ; sub 312FD8+49
call
        sub 3140F3
        eax, eax
        short loc 31307D
        sub 3140F3
        short loc 31308C
```

push

sub\_3140F3

[ebp+var 4], eax

; CODE XREF: sub 312FD8

loc\_31307D:

loc 313066:

### Malware over time

```
push
        short loc_31306D
        [ebp+arg 0], ebx
```

- 1988 Morris Worm exploits use of gets() in finger daemon
- 1990 Mark Washburn develops first polymorphic malware
- 2001 Code Red worm exploits a MS web server vulnerability to hit hundreds of thousands of computers
- 2004 Vundo trojan displays popups and advertising
- 2005 Sony infects CDs with a rootkit to prevent music piracy
- 2008 Koobface RAT spreads via infected Facebook and Myspace profiles
- 2008-2010 Stuxnet employs four Windows Odays to spread through Iranian nuclear refinery control system networks
- 2013 Mandiant publishes evidence on APT1, a Chinese cyber espionage campaign dating as early as 2005
- 2015 Duqu2 targets McAfee with advanced, modularized memory only malware

Introduction (cc)) BY-NC

loc\_31307D:

sub 3140F3

### Why analyze malware?

- Detect and respond to intrusions
  - Threat analysis
    - Host & Network signatures
    - What's the damage?
      - Who/What is infected?
  - Threat prevention
  - Threat removal

```
short loc_31306D
                         [ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var 70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         [ebp+arg 0], eax
                         sub 31486A
                         eax, eax
                         short loc 31306D
                         eax, [ebp+arg_0]
                         esi, 1D0h
                         [ebp+arg_4]
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
```

[ebp+var 4], eax

: CODE XREF: sub 312FD8

push

test

edi sub\_314623

eax, eax

loc\_31308C:

### Additional Material

- Related Readings:
  - Practical Malware Analysis
    - Introduction
    - Chapter 0. Malware Analysis Primer

```
short loc_31306D
                         [ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                 push
                         esi
                push
                         [ebp+arg_0], eax
                call
                         sub 31486A
                 test
                         eax, eax
                         short loc_31306D
                 push
                         681
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                 push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
                         eax, Offffh
                         eax, 80070000h
                                                      26
```

push

test

edi sub\_314623

eax, eax

#### Lecture Overview

- Syllabus
- Course Overview
- Basic Analysis

```
push
                         edi
                call
                         sub_314623
                test
                         eax, eax
                         short loc_31306D
                CIID
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                push
                         esi
                push
                         edi
                         [ebp+arg_0], eax
                MOV
                call
                         sub 31486A
                test
                         eax, eax
                         short loc_31306D
                push
                         681
                lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                 push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc_31308F
                                          ; CODE XREF: sub 312FD8
loc 313066:
                                          : sub 312FD8+55
                         0 Dh
                push
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub 3140F3
                         eax, Offffh
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```