			push	edi	
			call	sub_314623	
			test	eax, eax	
			jz	short loc_31306D	
			CHID	[ebp+arg_0], ebx	
			Jnz	short loc_313066	
			BOV	eax, [ebp+var_70]	
			CHIP	eax, [ebp+var_84]	
			jb	short loc_313066	
			sub	eax, [ebp+var_84]	
			push	esi	
			push	eax	
			push	edi	
			BOV	[ebp+arg_0], eax	
			call	sub_31486A	
			test	eax, eax	
			jz	short loc_31306D	
			push	esi	
			lea	eax, [ebp+arg_0]	
	Basic Anal		push	eax	
	Rasic Anal		mov	esi, 1D0h	
	Dusit Anat	<b>Y</b> JIJ	push	esi	
			point	[ebp+arg_4]	
			push	edi	
			call	sub_314623	
			test	cax, cax	
			jz cmp	<pre>short loc_31306D [ebp+arg_0], esi</pre>	
			jz	short loc_31308F	
	Malware Anal	vcic			; CODE XREF: sub 312FD
	Malwalt Alla	LY SIS			sub 312FD8+55
			push	ODh	-
			call	sub_31411B	
	CSCI 4976 - Fal			-	
		loc_31306D:			: CODE XREF: sub 312FD
					sub 312FD8+49
	Branden Cla	nrk –	call	sub_3140F3	
	Dianach ciù		test	eax, eax	
			3a	short loc_31307D	
			call	sub_3140F3	
			jmp	short loc_31308C	
		loc_31307D:			: CODE XREF: sub_312FD
			call	sub_3140F3	
			and	eax, OFFFFh	
RPISEC - 08/29/2014	Meeting Title		OT	eax, 80070000h	1
	Meeting Title	loc_31308C:			CODE XREF: sub_312FD
		200-0700.001	BOV	[ebp+var_4], eax	
				and a second second	

### Overview

• Your malware analysis VM

**Meeting Title** 

• Static Analysis

RPISEC - 08/29/2014

• Dynamic Analysis

push edi sub\_314623 test eax, eax short loc\_31306D CID [ebp+arg\_0], ebx 1nz short loc\_313066 eax, [ebp+var\_70] BOV eax, [ebp+var\_84] CHO short loc 313066 sub eax, [ebp+var\_84] push 081 C31 push push eax push edi [ebp+arg\_0], eax nov call sub\_31486A test eax, eax short loc\_31306D push 631 lea eax, [ebp+arg\_0] push eax esi, 1D0h NOR push 881 push [ebp+arg\_4] push edi call sub 314623 test cax, cax abort loc\_31306D cmp [ebp+arg\_0], esi short loc 31308F loc 313066: ; CODE XREF: sub 312FD8 ; sub 312FD8+55 puan 0 Dh call sub\_31411B loc\_31306D: ; CODE XREF: sub 312FD8 / sub 312FD8+49 call sub\_3140F3 test eax, eax short loc\_31307D call sub\_3140F3 short loc\_31308C 1000 loc\_31307D: ; CODE XREF: sub 312FD8 sub\_3140F3 and eax, OFFFFh eax, 80070000h 2 loc\_31308C: ; CODE XREF: sub 312FD8

[ebp+var\_4], eax

10V

## Virtual Machines

RPISEC - 08/29/2014

- What is a virtual machine?
   Simply, a computer in your computer
   Really, a (usually) segregated virtual environment that emulates reating in the second se
  - •There are different types/methods that we'll discuss later

				7 sub 312FD8	+49
		call	sub_3140F3		
		test	eax, eax		
		ja.	short loc 31307	D	
		call	sub 3140F3		
		jmp	short loc_31308	C	
	/				
	loc_31307D:	call	sub_3140F3	; CODE XREF:	sub_312FD8
		and	eax, OFFFFh		
			eax, 80070000h		
Meeting Title					3
	loc_31308C:			; CODE XREF:	sub 312FD8

push

call

test

CHO

inz

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]

Virtual Machir	nes		call test jz cmp jnz mov cmp jb sub push	<pre>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 esi</pre>	1
• Why are we using	g a virtu	al ma	ch		
-Safety, reliability, c	onsistency	it's ea	test CV/	eax, eax short loc_31306D	
Jarcey, renability, e	onsistency,	, it sta	Joh	esi eax, [ebp+arg_0]	
-Keep the malware i	n a contair	ned env	iror		
			push	esi [ebp+arg_4]	
-Snapshots			push	edi	
			call test	sub_314623 eax, eax	
<ul> <li>Completely 100% re</li> </ul>	vert the VM	to an ear	lier	state state	
<ul> <li>If things go bad, no</li> </ul>	ono caros		jz	[ebp+arg_0], esi short loc_31308F	
	Une Cares	loc_313066;			; CODE XREF: sub 312FD8
					; sub_312FD8+55
			call.	0Dh sub_314118	
		loc_31306D:			; CODE XREF: sub_312FD8 ; sub_312FD8+49
			call	sub_3140F3	
			test	eax, eax short loc_31307D	
			call	sub_3140F3	
			jmp	short loc_31308C	
		100 919070.			. OADE VOEE, AND SISENS
		loc_31307D:	call	sub_3140F3	; CODE XREF: sub_312FD8
			and	eax, OFFFFh	
RPISEC - 08/29/2014	Meeting Title		OT	eax, 80070000h	4
	Meeting Hite	loc_31308C:			; CODE XREF: sub_312FD8
				F-3	

## Virtual Machines

#### • What's in mine?

- -Free Microsoft IE testing VM license
- Lots of free tools all pre-setup for you (C: tools)
  - Common ones are linked on the desktop
  - symlinks to desktop and tools directory in cygwin home dir

push

call

test

CHO

inz

00.8

call

Ces

edi

eax.

eax.

081

es1 eax

edi

sub 314623

short loc 31306D

[ebp+arg\_0], ebx

short loc\_313066
eax, [ebp+var\_70]
eax, [ebp+var\_84]
short loc 313066

[ebp+arg\_0], eax

sub 31486A

[cbp+var 84]

loc 31306D

loc\_31308C

- •debuggers, disassemblers, analyzers, unpackers, compilers... the list goes on
- You'll know them all soon enough the state of the state

		1 010070-			
		loc_31307D:	call	sub_3140F3	; CODE XREF: sub_312FD8
			and	eax, OFFFFh	
				eax, 80070000h	
RPISEC - 08/29/2014	Meeting Title				5
	3	loc_31308C:			; CODE XREF: sub 312FD8
			THOMP.	febrewar 41, ea	*

### Overview

- Your malware analysis VM
- Static Analysis

RPISEC - 08/29/2014

Dynamic Analysis

push edi sub\_314623 test eax, eax short loc\_31306D CID [ebp+arg\_0], ebx 1nz short loc\_313066 eax, [ebp+var\_70] BOV eax, [ebp+var\_84] CHO short loc 313066 sub eax, [ebp+var\_84] push 081 C31 push push eax push edi nov [ebp+arg\_0], eax call sub\_31486A test eax, eax short loc\_31306D push 681 lea eax, [ebp+arg\_0] push eax esi, 1D0h NOR push 881 push [ebp+arg\_4] push edi call sub 314623 test cax, cax short loc\_31306D cmp [ebp+arg\_0], esi short loc\_31308F loc 313066: ; CODE XREF: sub 312FD8 ; sub 312FD8+55 puan 0 Dh call sub\_31411B loc\_31306D: ; CODE XREF: sub 312FD8 / sub 312FD8+49 call sub\_3140F3 test eax, eax short loc\_31307D call sub\_3140F3 short loc\_31308C 1000 loc\_31307D: ; CODE XREF: sub 312FD8 sub\_3140F3 and eax, OFFFFh eax, 80070000h Meeting Title 6 loc\_31308C: ; CODE XREF: sub 312FD8 [ebp+var\_4], eax

10V

## Static Analysis

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\_70] cmp eax, [ebp+var\_84] jb short loc\_313066 sub eax, [ebp+var\_84] push esi

eax

681

nush

esi, 1D0h

[ebp+arg\_4]

- Analyzing a sample without executing any code
- Safe(r)Infer functionality
- Provides good pointers to guide dynamic and advanced analysis

Meeting Title

• Lots of tools involved!

		eax, eax		
		short loc_31306D		
guic	le (	dynam	İC	
c_313066:				sub 312FD
-			sub 312FD8	+55
	push	0 Dh		
	call	sub_31411B		
c_31306D:			CODE XREF:	sub 312FD
-			sub 312FD8	+49
	call	sub_3140F3		
	test	eax, eax		
	ja	short loc_31307D		
	call	sub_3140F3		
	j≡p	short loc_31308C		
c_31307D:			CODE XREF:	sub 312FD
	call	sub 3140F3	room Hotara I	-
	and	eax, OFFFFh		
		eax, 80070000h		7
c_31308C:			CODE XREF:	sub 312FD
	mov	[ebp+var_4], eax		

Static Analysis			push call test jz cmp jnz mov cmp jb sub 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] esi	
• Can be an easy wa			test	eax, eax	
-URLs, filename	s, regisi	lty ke	ys	esi eax, [ebp+arg_0]	
<ul> <li>But it's not alway</li> </ul>	s so eas	5y!	push mov push push call test	eax, [dsp=arg_0] eax esi, 1D0h esi [ebp+arg_4] edi sub_314623 eax, eax	
			jz cmp jz	<pre>short loc_31306D [ebp+arg_0], esi short loc_31308F</pre>	
		loc_313066;	push call		: CODE XREF: sub 312FD8 : sub_312FD8+55
		loc_31306D:			CODE XREF: sub_312FD8 sub_312FD8+49
			call test jg call	<pre>sub_3140F3 eax, eax short loc_31307D sub_3140F3 short loc_31308C</pre>	
		;	jup		CODE XREF: sub_312FD8
		100_313010:	call	sub_3140F3	CODE AMER BUD STREDG
RPISEC - 08/29/2014	Meeting Title	loc_31308C:	or	eax, OFFFFn eax, 80070000h [ebp+var_4], eax	CODE XREF: sub_312FD8

## Hands on

• VM time!

#### If your VM isn't working, don't working, Just jot down the tools and the process. We'll resolve any issues and review at office hours!

push

call

test

CID

1nz

BOV

CHO

SUD

push

push

push

nov

call

test

push

lea

push

push

push

test

jg call edi

esi

eax

edi

681

eax esi, 1D0h

681

sub 314623

short loc\_31306D

[ebp+arg\_0], ebx

short loc 313066

eax, [ebp+var\_70]

eax, [ebp+var\_64]

short loc 313066

eax, [ebp+var\_84]

[ebp+arg\_0], eax

short loc\_31306D

eax, [ebp+arg\_0]

[ebp+arg\_4]

eax, eax

sub 3140F3

short loc\_31307D

sub\_31486A

eax, eax

			jmp	short loc_3130	8C			
		loc_31307D:			; CODE XREF:	sub_312FD		
			call	sub_3140F3				
			and	eax, OFFFFh				
				eax, 80070000h				
RPISEC - 08/29/2014	Meeting Title					9		
	3	loc_31308C:			; CODE XREF:	sub 312FD		
			BROWN P	Tehnastar 41	27			

### Overview

• Your malware analysis VM

Meeting Title

• Static Analysis

RPISEC - 08/29/2014

• Dynamic Analysis

push edi sub\_314623 test eax, eax short loc\_31306D CID [ebp+arg\_0], ebx 1nz short loc\_313066 eax, [ebp+var\_70] BOV eax, [ebp+var\_84] CHO short loc 313066 sub eax, [ebp+var\_84] push 081 C31 push eax push edi [ebp+arg\_0], eax nov call sub\_31486A test eax, eax short loc\_31306D push 681 lea eax, [ebp+arg\_0] push eax esi, 1D0h NOR push 881 push [ebp+arg\_4] push edi call sub 314623 test cax, cax abort loc\_31306D cmp [ebp+arg\_0], esi short loc 31308F loc 313066: ; CODE XREF: sub 312FD8 ; sub 312FD8+55 puan 0 Dh call sub\_31411B loc\_31306D: ; CODE XREF: sub 312FD8 / sub 312FD8+49 call sub\_3140F3 test eax, eax short loc\_31307D call sub\_3140F3 short loc\_31308C 1000 loc\_31307D: ; CODE XREF: sub 312FD8 call sub\_3140F3 and eax, OFFFFh eax, 80070000h 10 loc\_31308C: ; CODE XREF: sub 312FD8

[ebp+var\_4], eax

# Dynamic Analysis

Analyze what happens when the sample is executed

push

call

test

CHO

inz

CHO

test

call

100

Cal.

loc\_31307D:

loc 31308C:

eax, eax

sub\_3140F3 short loc\_31308C

short loc\_31307D

edi

eax,

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]

eax, eax

- Are files made, processes created, websites contacted, files downloaded/ executed, etc
- Shows you the effect the malware has on the system/network

**Meeting Title** 

BUD_314023		
eax, OFFFFh		
eax, 80070000h		
		11
	CODE	XREF: sub 3
[ebp+var 4], eax		_

; CODE XREF: sub 312FD:

## Hands on

• VM time!

#### If your VM isn't working, don't working, Just jot down the tools and the process. We'll resolve any issues and review at office hours!

push

call

test

CT D

1nz

BOV

CHO

sub

push

push

push

mov call

test

push

lea

push

push

push

test

jg call edi

esi

eax

edi

681

eax esi, 1D0h

681

sub 314623

short loc\_31306D

[ebp+arg\_0], ebx

short loc 313066

eax, [ebp+var\_70]

eax, [ebp+var\_64]

short loc 313066

eax, [ebp+var\_84]

[ebp+arg 0], eax

short loc\_31306D

eax, [ebp+arg\_0]

[ebp+arg\_4]

eax, eax

sub 3140F3

short loc\_31307D

sub\_31486A

eax, eax

			jup.	08C	
		loc_31307D:			; CODE XREF: sub 312FD8
			call	sub_3140F3	
			and	eax, OFFFFh	
				eax, 800700008	h
RPISEC - 08/29/2014	Meeting Title				12
	3	loc_31308C:			; CODE XREF: sub 312FD8
		-	MACON P.	Labourna 41	

Lab			push call test jz cmp jnz mov cmp jb sub 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 esi	1
<ul> <li>Friday 09/04, sa</li> <li>Problems will be today</li> </ul>			See push mov push	you start of the s	aw
<ul> <li>Must answer a fe sample</li> </ul>		loc_313066;	cmp jz	[ebp+arg_0], esi short loc_31308F	; CODE XREF: sub 312FD8
-See the PMA C	hapter l	_abs fo	Dr	exam	oles
		loc_31306D:	call test jg call jmp		: CODE XREF: sub_312FD8 ; sub_312FD8+49
		loc_31307D:	call	sub_3140F3	; CODE XREF: sub_312FD8
RPISEC - 08/29/2014	Meeting Title	loc_31308C:	or mov	eax, OFFFFh eax, 80070000h	13 : CODE XREF: sub_312FD0

## Additional Material

### • Related Readings:

- Practical Malware Analysis
  - Chapter 1. Basic Static Analysis
  - Chapter 2. Malware Analysis in Virtual Machines
  - Chapter 3. Basic Dynamic Analysis

#### The chapter outlines make a great reference

push

call

test

CHID

jnz mov

CHO

SUD

push

push

push

nov

call

test

push

lea

push

push

call

test

edi

881

C31

eax

edi

681

eax

edi

eax.

sub 314623

sub 314623

short loc\_31306D

[ebp+arg\_0], ebx

short loc 313066

eax, [ebp+var 70]

eax, [ebp+var\_64] short loc\_313066

eax, [ebp+var\_84]

[ebp+arg\_0], eax

short loc\_31306D

eax, [ebp+arg\_0]

short loc 31306D

sub\_31486A

eax, eax

		loc_313066:			; CODE XREF: sub 312FD ; sub_312FD8+55
			push	ODh	
			call	sub_31411B	
		loc_31306D:			; CODE XREF: sub_312FD
					; sub 312FD8+49
			call	sub_3140F3	
			test	eax, eax	
			30	short loc_3130	70
			call	sub_3140F3	
			3mp	short loc_3130	3C
		loc_31307D:			; CODE XREF: sub_312FD
			call	sub_3140F3	
			and	eax, OFFFFh	
				eax, 80070000h	
Malware - 09/01/2015	Introduction				14
	(cc)) EV-NC	loc_31308C:			; CODE XREF: sub_312FD
	1 /		mov	[ebp+var 4], et	LX.

## References

ush	edi
all	sub_314623
est	eax, eax
z	short loc_31306D
ango	[ebp+arg_0], ebx
nz	short loc_313066
voi	eax, [ebp+var_70]
ango	eax, [ebp+var_84]
b	short loc 313066
nuite -	eax, [ebp+var_84]
ush	esi
01510	051

1. Sikorski, Michael, and Andrew Honig. Practical Malware Analysis the Hands-on Guide to Dissecting Malicious Software. San Francisco: No Starch, 2012. Print.

Advanced Statio

Malware - 09/08/2015

		jz	short loc_31306D
		push	esi
		lea	eax, [ebp+arg_0]
		push	eax
		mov	esi, 1D0h
		push	esi
		push	[ebp+arg_4]
		push	edi
		call	sub_314623
		test	eax, eax
		jz	abort loc_31306D
		cap	[ebp+arg_0], esi
		jz	short loc_31308F
	loc_313066:		; CODE XREF: sub 312FD
			; sub 312FD8+55
		push	ODh
		call	sub_31411B
	loc_31306D:		; CODE XREF: sub 312FD
	-		; sub_312FD8+49
		call	aub_3140F3
		test	eax, eax
		ja.	short loc_31307D
		call	aub_3140F3
		jmp	short loc_31308C
	loc_31307D:		; CODE XREF: sub_312FD
		call	sub_3140F3
		and	eax, OFFFFh
			eax, 80070000h
c Analysis			15
	loc_31308C:		; CODE XREF: sub_312FD
		mov	[ebp+var_4], eax