

Hacking .NET Applications: The Black Arts



USA + 2011
EMBEDDING SECURITY

Jon McCoy

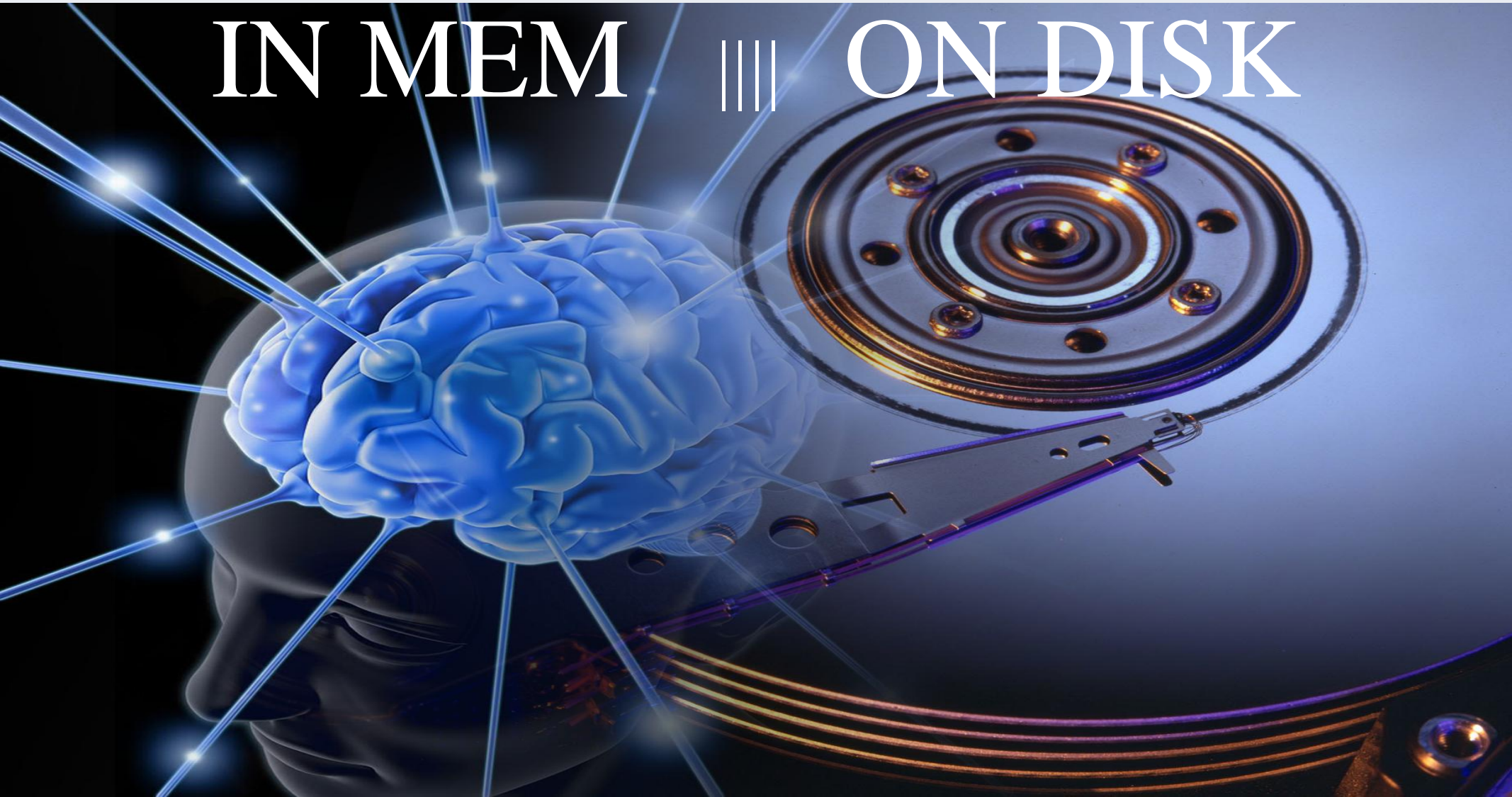
www.DigitalBodyGuard.com

TOPICS

- ◆ How-To Attack .NET Applications
- ◆ Tools and Methodology of Attacking
- ◆ Overcome “secure” .NET Applications
- ◆ Building KeyGen/Crack/Hacks/Malware
- ◆ Reverse Engenering for Protection

Attacking/Cracking

IN MEM |||| ON DISK



ATTACK OVERVIEW



Attack on Disk

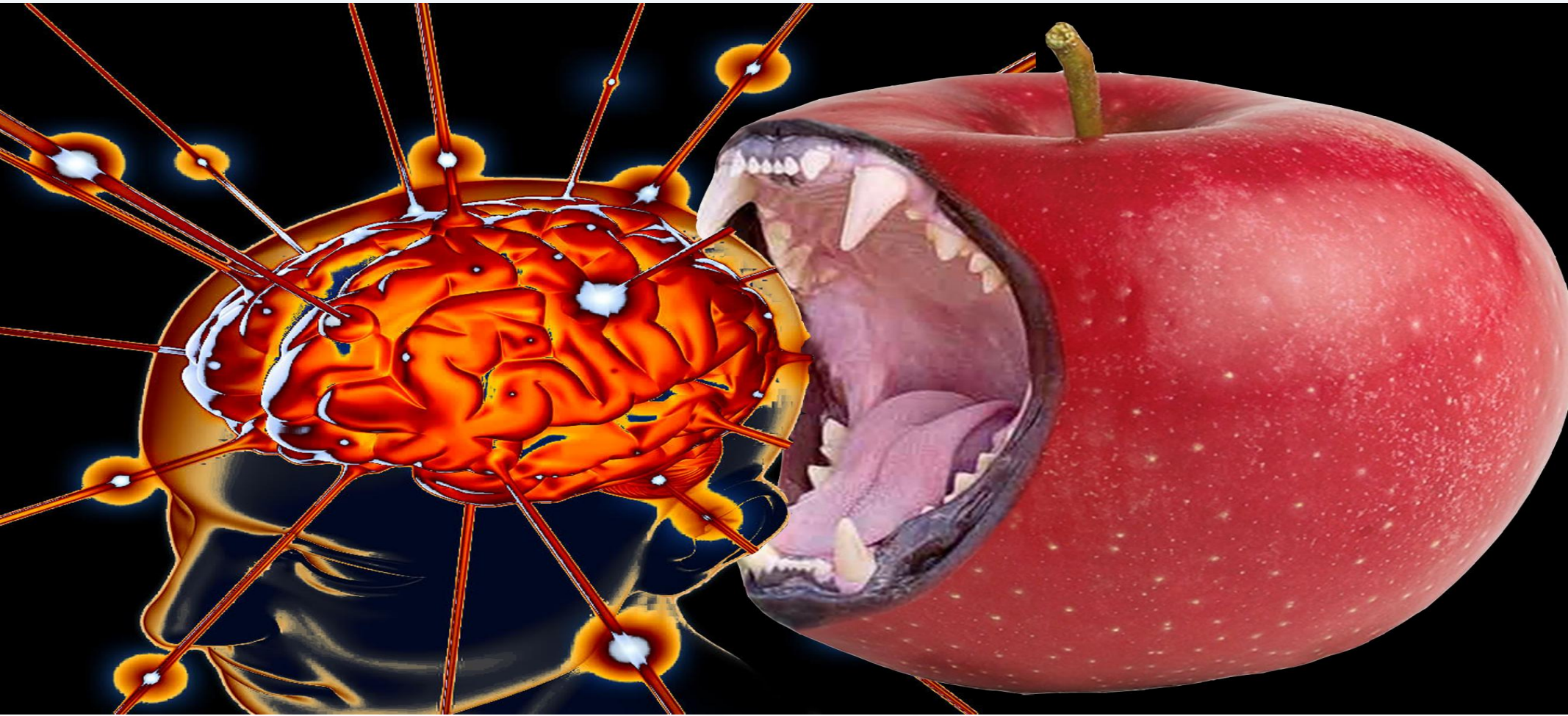
- Access Logic
- Infect Logic
- Hook Logic
- Decompile
- Recompile
- Debug



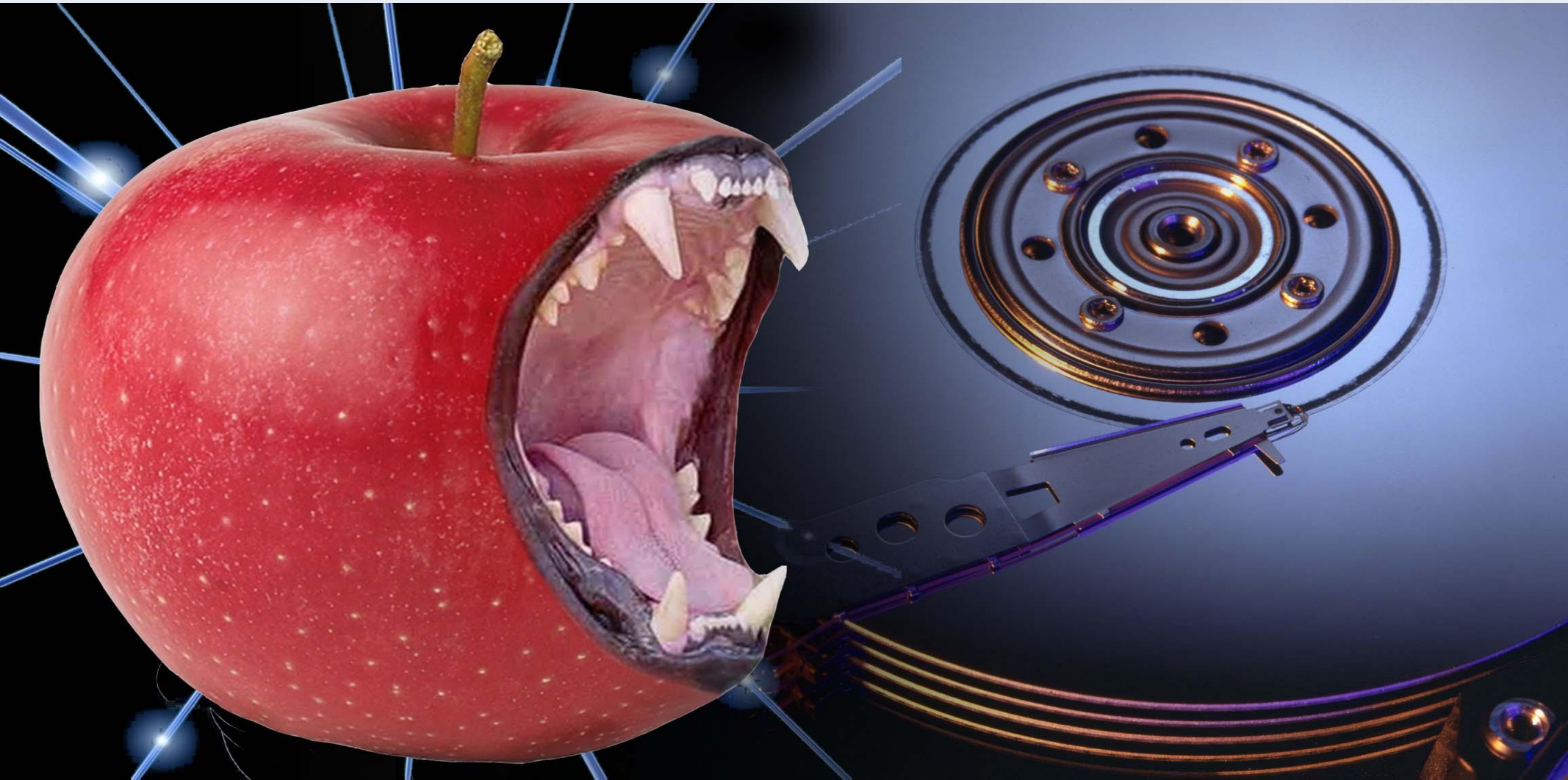
Attack in Memory/Runtime

- Injecting Structure
- Navigating Structure
- Editing/Controlling Structure

ATTACKING .NET APPLICATIONS: AT RUNTIME



ATTACKING ON DISK



101 – DECOMPILERS

DEMO

GrayWolf – IL_Spy – Reflector



101 - Recon

Windows Media Center

- Core File Location

C:\Windows\ehome\ehshell.dll

- StrongName KEY

d:\w7rtm.public.x86fre\internal\strongnamekeys\fake\windows.snk

- Registry CurrentUser OR LocalMachine





SOFTWARE\Microsoft\Windows\CurrentVersion\Media Center\

- Web Host Address

www.microsoft.com/WindowsMedia/Services/2003/10/10/movie

101 - ATTACK ON DISK

Connect/Open - Access Code

-  Decompile - Get code/tech
-  Infect - Change the target's code
-  Exploit - Take advantage
-  Remold Application - WIN

THE WEAK SPOTS



Flip The Checks



Cut The Logic



Controlling Objects



Accessing Value



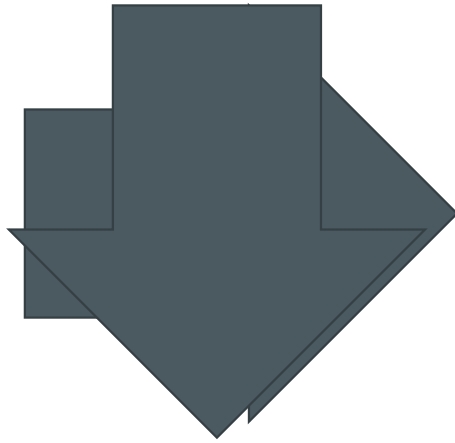
Set Value is “True”



SET VALUE TO "TRUE"

~~bool Registered = false;~~

~~If(a != b)~~



IL – Intermediate Language

Code of the Matrix |||| NEW ASM

1	ldarg.0		78	stloc.2		174	ldobj	System.IntPtr	235	stloc.3	
2	movsb	System.Void System.Random.Next(System.IntPtr)	79	ldloc.2		175	ldloc.0		236	stloc.3	
7	stloc.0		80	ldc.i4.0		177	ldc.i4.0	10000	237	brtrue	IL_01e8 ret
8	ldc.i4.4		81	ldstems	System.IntPtr	182	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	242	ldarg.0	
9	movsr	System.IntPtr	85	dup		187	add		248	stloc.1	
14	stloc.1		87	ldobj	System.IntPtr	188	stobj	System.IntPtr	244	ldc.i4.2	
15	ldloc.1		92	ldloc.1		199	ldarg.0		245	ldstems	
16	ldc.i4.0		98	ldc.i4.0	10	194	ldloc.1		246	rem	
17	ldloc.0		99	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	195	ldc.i4.0		247	stloc.2	
18	ldc.i4.0	10	100	add		196	ldstems		248	ldc.i4.1	
20	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	101	stobj	System.IntPtr	197	rem		249	ldstems	
25	ststems		105	ldloc.2		198	ldloc.2		250	add	
26	ldloc.1		107	ldc.i4.1		199	ldc.i4.3		251	ldc.i4.0	01F
27	ldc.i4.1		108	ldstems	System.IntPtr	200	ldstems		255	eq	
28	ldloc.0		116	dup		201	add		258	ldc.i4.0	
29	ldc.i4.0	100	114	ldobj	System.IntPtr	202	ldc.i4.0	0000	259	eq	
31	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	115	ldloc.0		207	eq		261	stloc.3	
35	ststems		120	ldc.i4.0	100	208	ldc.i4.0		262	stloc.3	
37	ldloc.1		122	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	210	eq		268	brtrue	IL_01e8 ret
38	ldc.i4.2		127	add		212	stloc.3		268	ldarg.0	
39	ldloc.0		128	stobj	System.IntPtr	213	ldloc.3		269	stloc.1	
40	ldc.i4.0	1000	133	ldloc.2		214	brtrue	IL_01e8 ret	270	ldc.i4.3	
45	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	134	ldc.i4.2		215	ldarg.0		271	ldstems	
50	ststems		135	ldstems	System.IntPtr	220	ldloc.1		272	rem	
51	ldloc.1		140	dup		221	ldc.i4.1		273	stloc.2	
52	ldc.i4.3		141	ldobj	System.IntPtr	222	ldstems		274	ldc.i4.0	
53	ldloc.0		145	ldloc.0		223	rem		275	ldstems	
54	ldc.i4.0	10000	147	ldc.i4.0	1000	224	ldloc.2		276	add	
55	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	152	callvirt	System.IntPtr System.Random.Next(System.IntPtr)	225	ldc.i4.2		277	ldc.i4.0	010
59	ststems		157	add		226	ldstems		282	eq	
65	ldarg.1		158	stobj	System.IntPtr	227	add		284	ldc.i4.0	
68	movsb	System.Void System.Random.Next(System.IntPtr)	169	ldloc.2		228	ldc.i4.0	00	285	eq	
70	stloc.0		184	ldc.i4.3		230	eq		287	stloc.3	
72	ldc.i4.4		185	ldstems	System.IntPtr	232	ldc.i4.0		288	stloc.3	

REGISTRATION CHECK

■ KeyGens

&

■ Cracks

IT CAN'T BE THAT EZ

NO

What can stop this!!

UNPROTECTED/PROTECTED



IT CAN'T BE THAT EZ



NO

YES

What can stop this!!!

MALWARE FIGHT



Androsa File Protector

Version 1.4.4

Copyright © AndrosaSoft 2009

 **black hat** USA + 2011

MORE INFORMATION @:
www.DigitalBodyGuard.com

FIN = 1