.NET sample analysis, do you have more ?

Hugo RIFFLET
@l3m0ntr33

botconf 2016
The botnet fighting conference
30 NOVEMBER - 2 DECEMBER 2016
LYON - FRANCE
4th edition

QUICK'N DIRTY

.NET sample analysis, do you have more ?

Kevin Beaumont
@GossiTheDog
Suivre

Whatever this Office .pub malware is, it is funky. Uses Microsoft BITS to DL, signed 'by' Foxit. Analysis ongoing.

04:07 - 5 sept. 2016

http://cta.edu.pe/real/let.exe

.NET sample analysis, do you have more ?

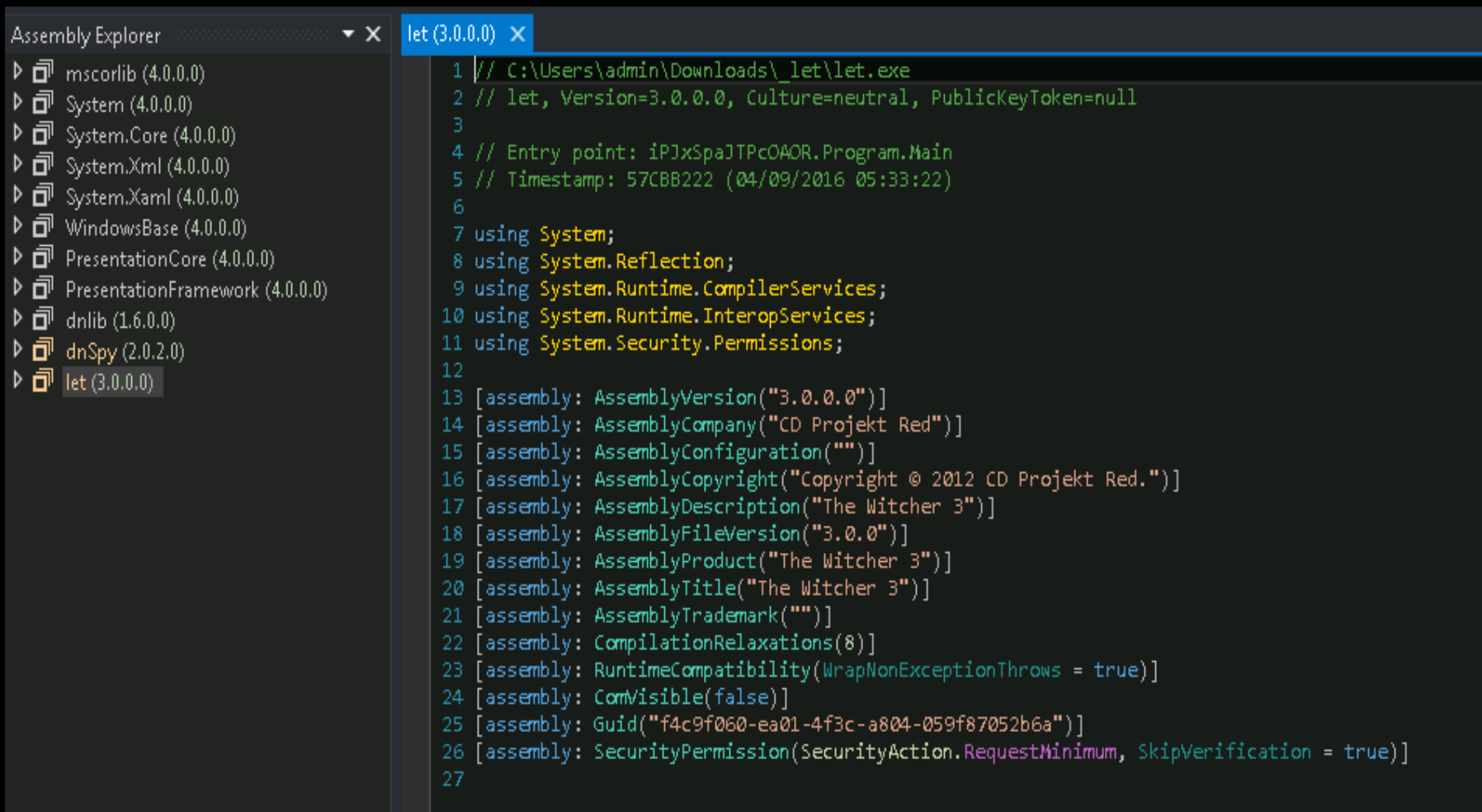## 1st Stage – let.exe
.NET sample

14d1c127f23b2440bfb59be830be7386530623d730e1c06190eca7da4c4bdc1c

SHA256:   14d1c127f23b2440bfb59be830be7386530623d730e1c06190eca7da4c4bdc1c

Nom du fichier :   let.exe

Ratio de détection :   45 / 57

Date d'analyse :   2016-09-26 18:48:53 UTC (il y a 2 mois)

.NET sample analysis, do you have more ?

.NET sample analysis, do you have more ?

.NET sample analysis, do you have more ?

2ⁿᵈ stage – Olympic Worker
Always .NET

.NET sample analysis, do you have more ?


```
{} OlympicWorker.Tools
    EncryptionSettings @0200
    RunPE @02000009
```

```
18 [assembly: AssemblyCopyright("Copyright ©  2016")]
19 [assembly: AssemblyDelaySign(false)]
20 [assembly: AssemblyDescription("")]
21 [assembly: AssemblyFileVersion("1.0.0.0")]
22 [assembly: AssemblyKeyName("")]
23 [assembly: AssemblyProduct("OlympicWorker")]
24 [assembly: AssemblyTitle("OlympicWorker")]
25 [assembly: AssemblyTrademark("")]
26 [assembly: CompilationRelaxations(8)]
27 [assembly: RuntimeCompatibility(WrapNonExceptio
28 [assembly: ComVisible(false)]
29 [assembly: Guid("4825e303-3b70-4d83-afa4-1e7b8e
30 [assembly: SecurityPermission(SecurityAction.Re
31
```

```
MvOjBIbXByV4QME_TZ(object) : object @06000062
O9jtVNbQ3oW         (object, int, object, int, int) : void @06000075
pUO0T          eU5(object) : object @0600005C
R76Yy          bject) : bool @06000052
Run(int, string, byte[], bool, byte[], out uint) : bool @06000053
rwOBWIbLQBQ29OOMoU7(object) : object @06000056
sEQYU5bwGH2Wgo8LVjh(object, IntPtr) : int @06000078
```

.NET sample analysis, do you have more ?

```
42    // Token: 0x06000009 RID: 9 RVA: 0x00002148 File Offset: 0x00000348
43    [MethodImpl(MethodImplOptions.NoInlining)]
44    public static void DoWork()
45    {
46        try
47
48
49
50
51
52
53
54
55
56
57
58
59
60
```

Name	Value	Type
▲ ● encryptionSettings	{OlympicWorker.Tools.EncryptionSettings}	OlympicWorker.Tools.Encr
● CompatibleMode	false	bool
● DeleteZoneID	true	bool
● DownloadExecute	false	bool
● DownloadURL	""	string
● EOFData	{byte[0x00000000]}	byte[]
● EnableFakeError	false	bool
● EnableStartup	false	bool
● ExecutionDelay	0x00000000	int
● FakeErrorMessage	""	string
● FakeErrorTitle	""	string
● FakeErrorType	Asterisk	System.Windows.Forms.M
● HideFile	false	bool
● InjectProtectionModule	false	bool
● InjectionTarget	0x00000003	int
● InstallFile	false	bool
● InstallPath	0x00000000	int
● MarkAsSystem	false	bool
● MutexString	"SsXwHEDushUCDkgXlkkK"	string
● ProcessName	""	string
● StartupKey	""	string

Locals

.NET sample analysis, do you have more ?

3rd stage – Native PE32 file

MD5,086C7DAC6F6C25E8E1B6A804CB78A4B8
- 0 results on VT on september
- Now detected by 42 AV vendors

virustotal

SHA256:	2af3610b33b952a14fcfa6efb0392c083f1db1e3b23...
Nom du fichier :	data.exe
Ratio de détection :	42 / 56
Date d'analyse :	2016-12-01 15:02:39 UTC (il y a 1 minute)

☰ Analyse   🔍 File detail   ⓘ Informations supplémentaires   💬 C

Antivirus	Résultat	
ALYac	Trojan.Keylogger.NBD	20161201

I have no time to do anything.

.NET sample analysis, do you have more ?

If someone has already made a study of .NET samples and/or classification (packer, dropper,…) i will be happy to go further.

Please free to contact me @l3m0ntr33