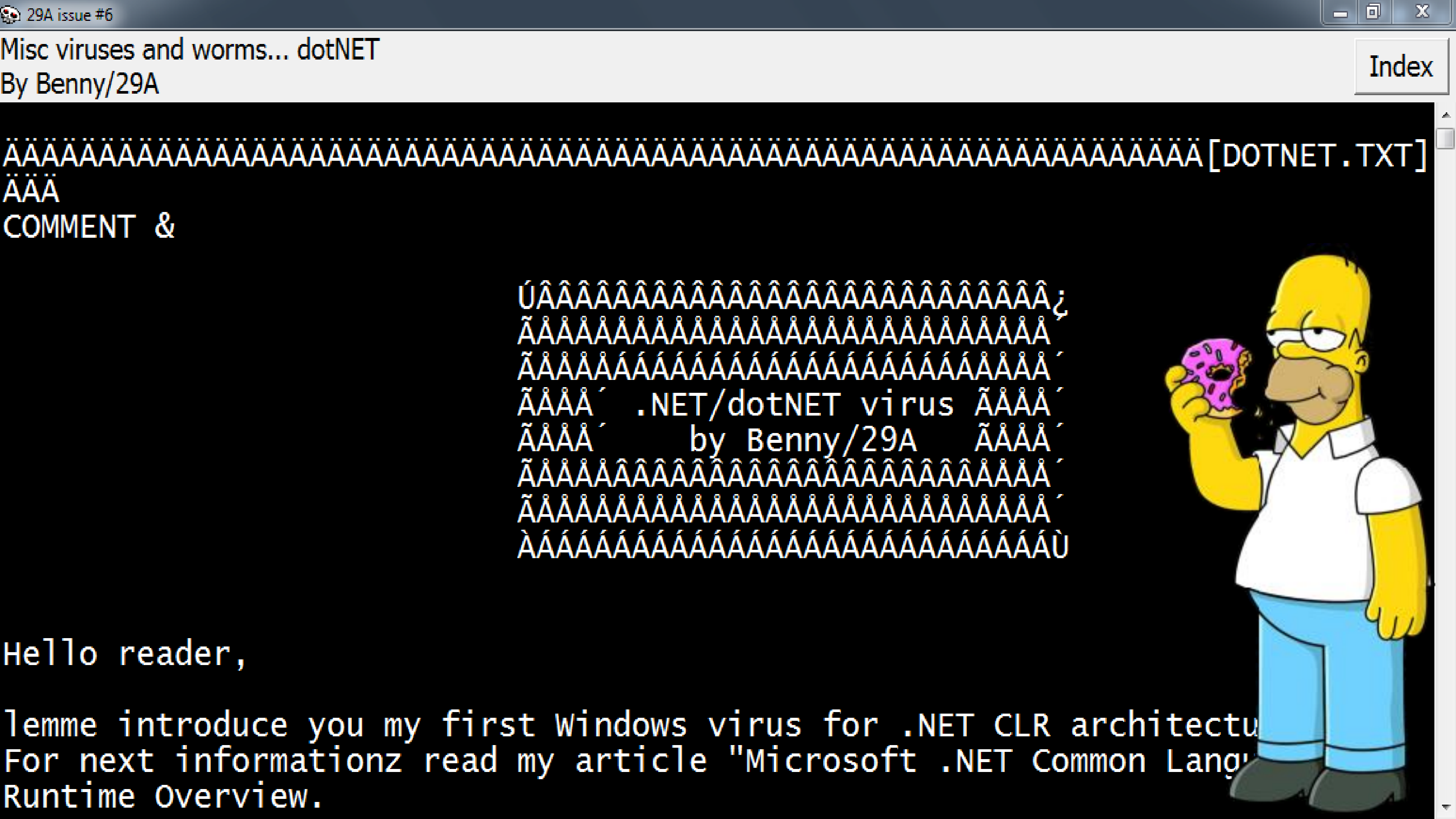
THE TAO OF .NET AND POWERSHELL MALWARE ANALYSIS

By Santiago M. Pontiroli, Roberto Martinez

GREAT

Virus Bulletin 2015



Misc viruses and worms... dotNET
By Benny/29A

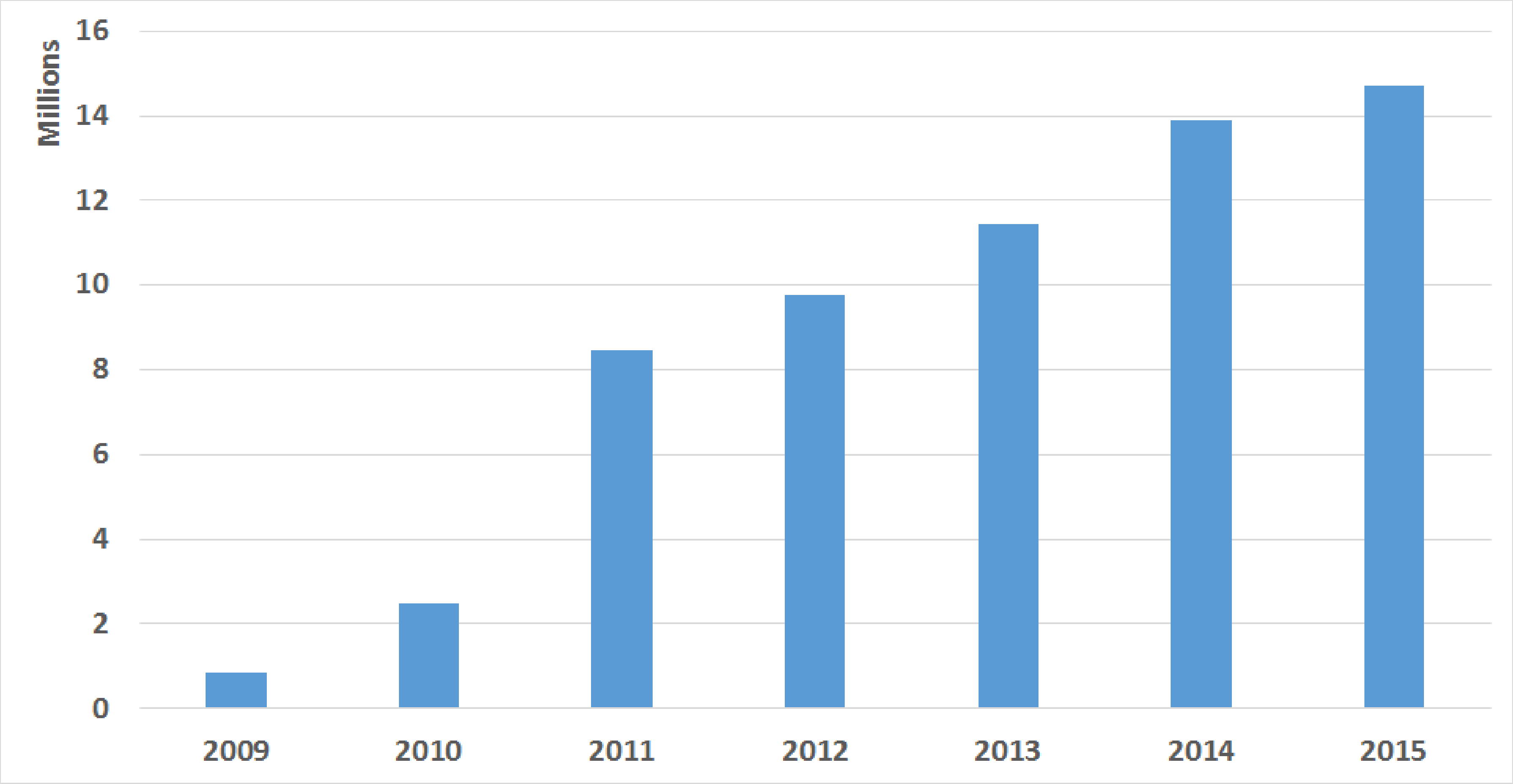
```
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ[DOTNET.TXT]
ÄÄÄ
COMMENT &

                           ÚÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂ¿
                           ÃÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅ´
                           ÃÅÅÅÅÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÅÅÅÅ´
                           ÃÅÅÅ´ .NET/dotNET virus ÃÅÅÅ´
                           ÃÅÅÅ´    by Benny/29A   ÃÅÅÅ´
                           ÃÅÅÅÅÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÅÅÅÅ´
                           ÃÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅÅ´
                           ÀÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÙ


Hello reader,

lemme introduce you my first Windows virus for .NET CLR architectu
For next informationz read my article "Microsoft .NET Common Lang
Runtime Overview.
```

WELL OVER 90% OF THE PCS IN THE WORLD HAVE SOME VERSION OF THE .NET FRAMEWORK INSTALLED.

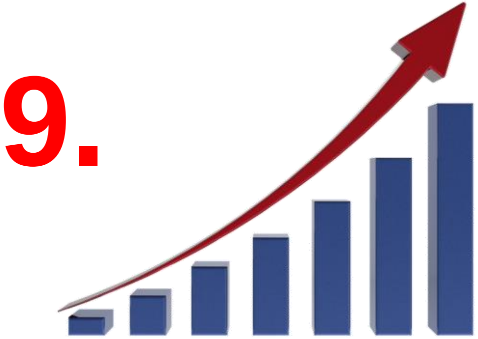
Microsoft®
.NET

Source: Microsoft

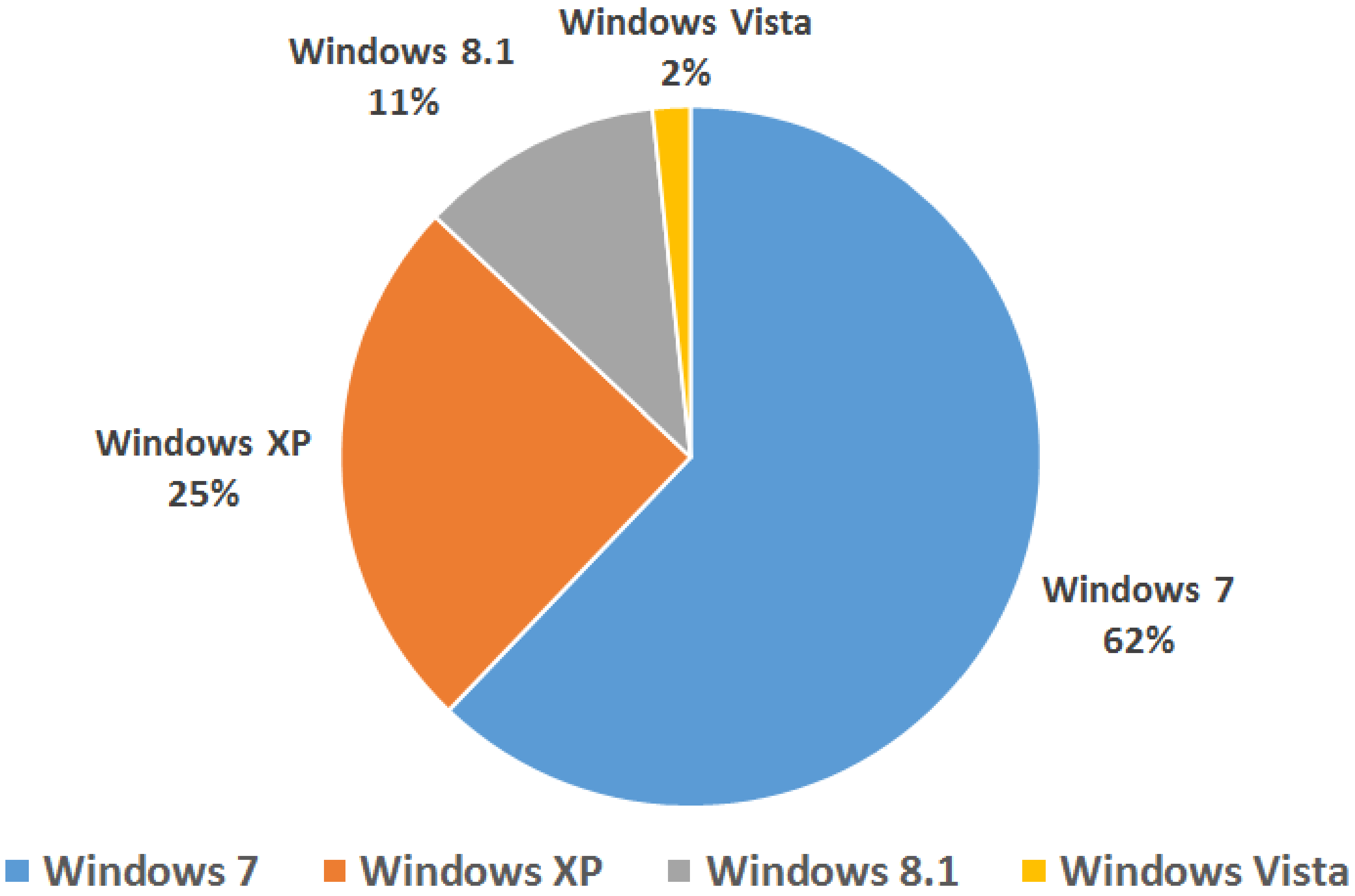
MSIL MALWARE – DETECTIONS YEARLY GROWTH



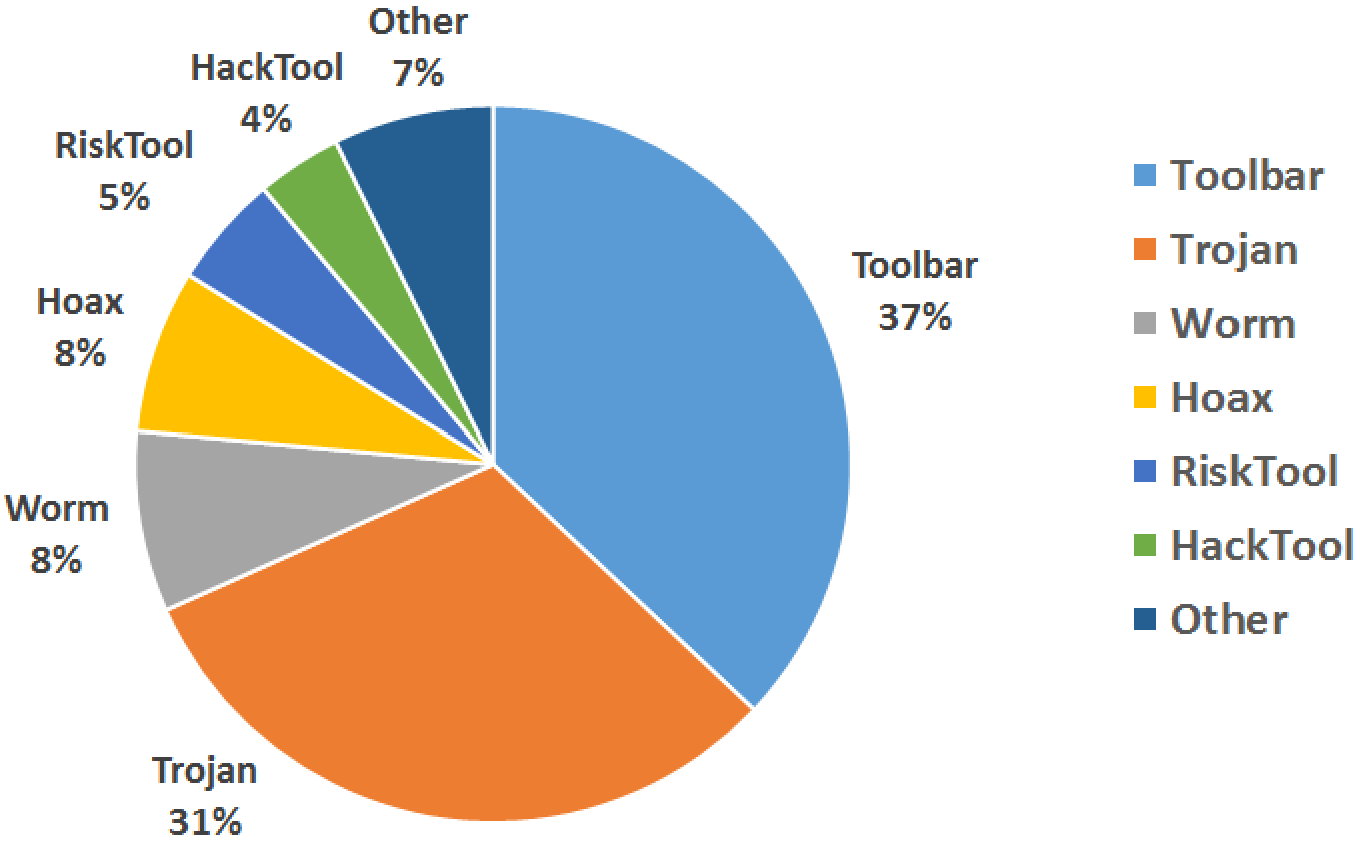
MORE THAN **14 MILLION UNIQUE DETECTIONS** OF MSIL MALWARE SO FAR IN 2015. **A 1600% GROWTH SINCE 2009.**



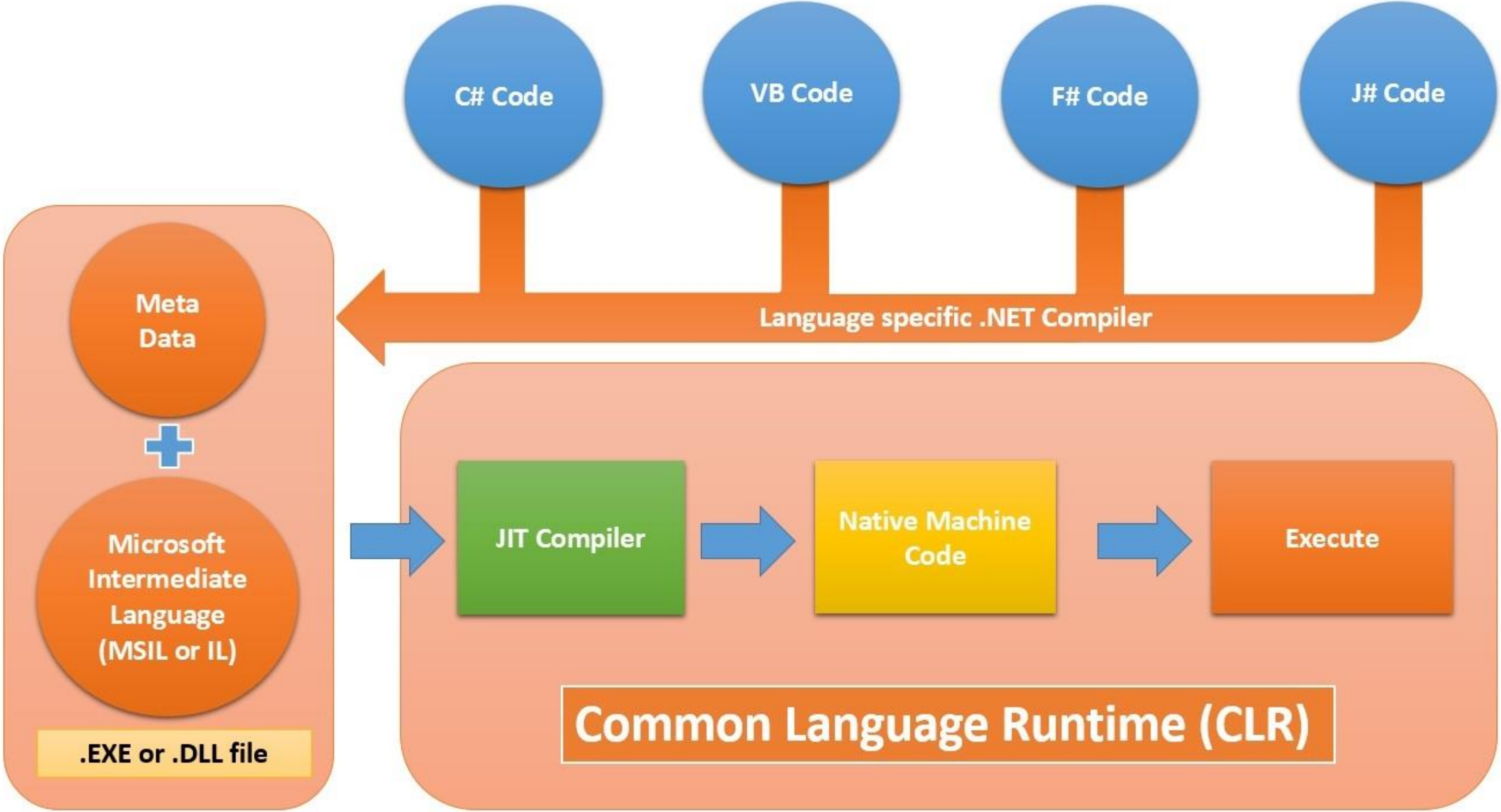
MOST ATTACKED OPERATING SYSTEMS



THE USUAL SUSPECTS

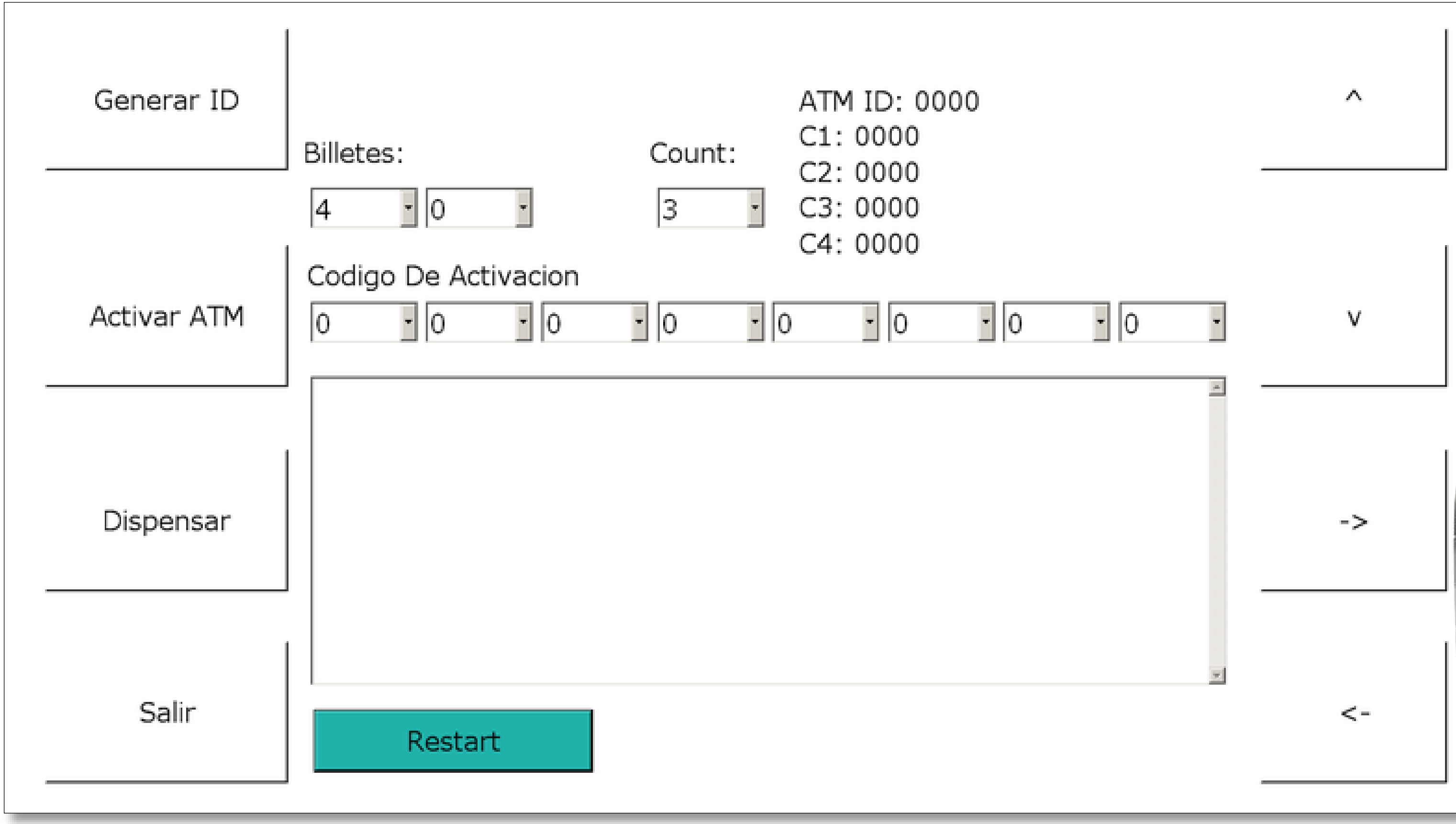


TROJANS…


C# Code
VB Code
F# Code
J# Code
Language specific .NET Compiler
Meta Data
Microsoft Intermediate Language (MSIL or IL)
.EXE or .DLL file
JIT Compiler
Native Machine Code
Execute
Common Language Runtime (CLR)

Source: ISpeakDotNet

BRINGING CYBERCRIME TO THE REAL WORLD



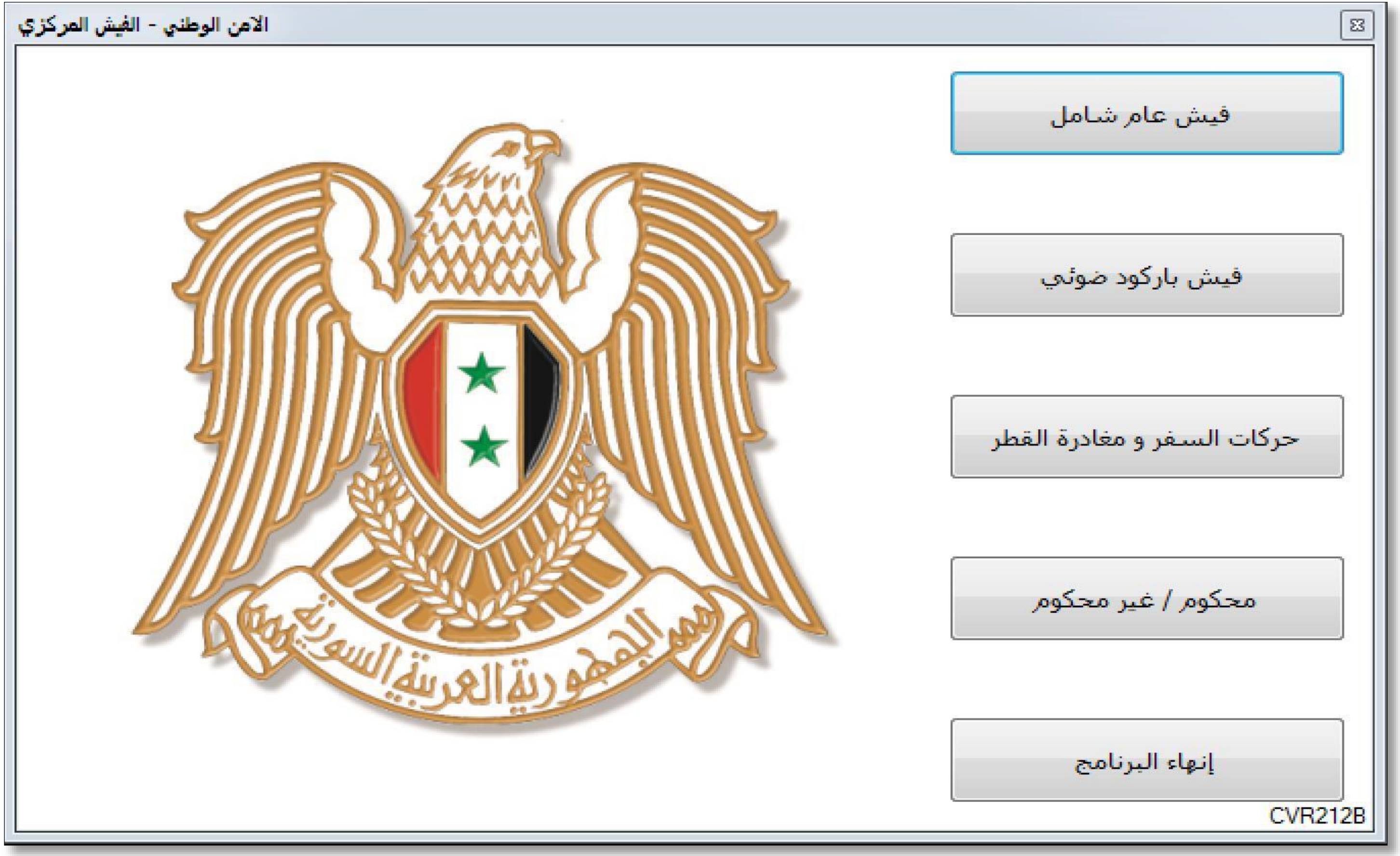
Billetes: 4 0

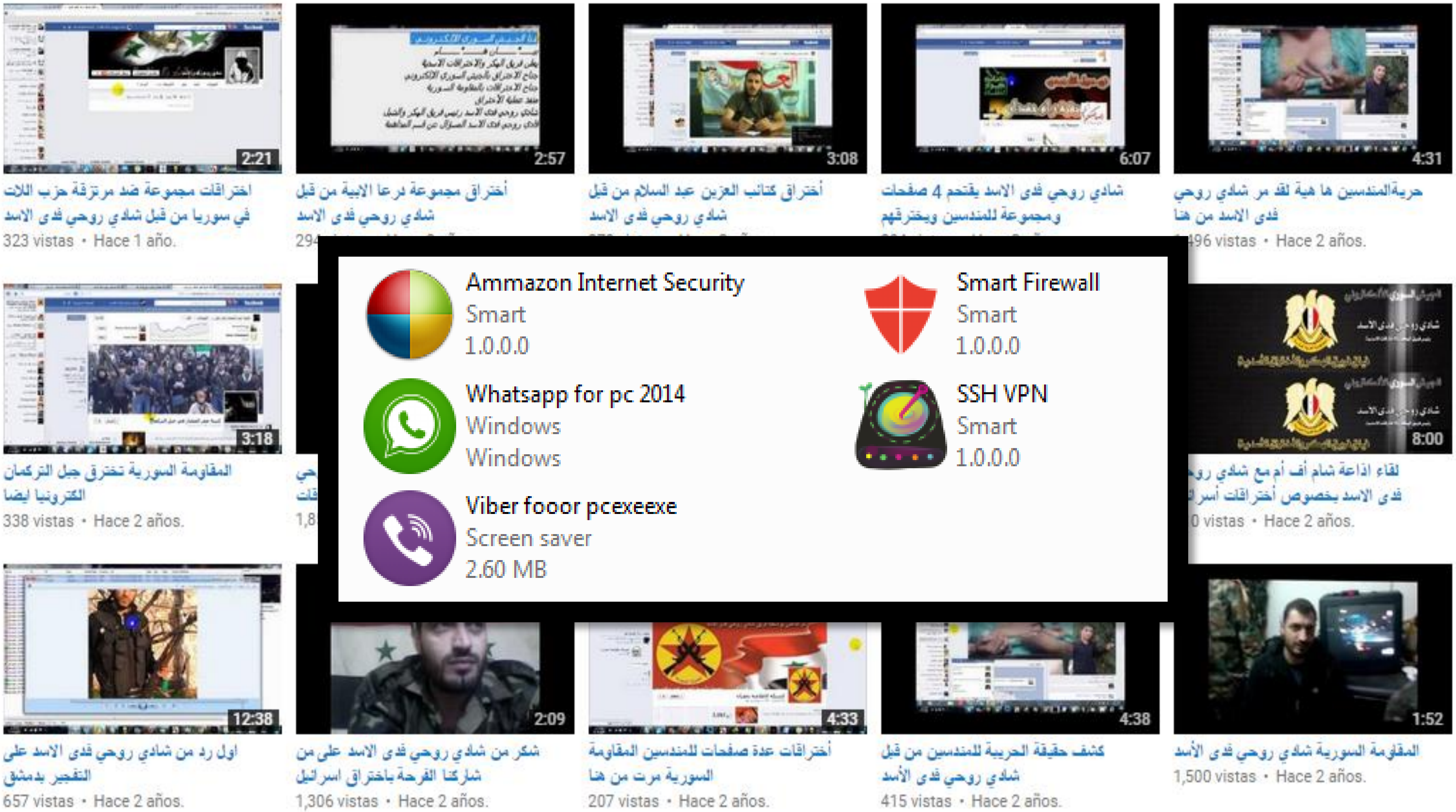
Count: 3

ATM ID: 0000
C1: 0000
C2: 0000
C3: 0000
C4: 0000

Codigo De Activacion
0 0 0 0 0 0 0 0

PERSISTENT THREATS - SYRIAN MALWARE


الامن الوطني - الفيش المركزي
فيش عام شامل
فيش باركود ضوئي
حركات السفر و مغادرة القطر
محكوم / غير محكوم
إنهاء البرنامج
الجمهورية العربية السورية
CVR212B



اختراقات مجموعة ضد مرتزقة حزب اللات في سوريا من قبل شادي روحي فدى الاسد

323 vistas • Hace 1 año.

أختراق مجموعة درعا الابية من قبل شادي روحي فدى الاسد

294

أختراق كتائب العزين عبد السلام من قبل شادي روحي فدى الاسد

شادي روحي فدى الاسد يقتحم 4 صفحات ومجموعة للمندسين ويخترقهم

حريةالمندسين ها هية لقد مر شادي روحي فدى الاسد من هنا

496 vistas • Hace 2 años.

المقاومة السورية تخترق جبل التركمان الكترونيا ايضا

338 vistas • Hace 2 años.

لقاء اذاعة شام أف أم مع شادي رو
فدى الاسد بخصوص أختراقات أسرا

0 vistas • Hace 2 años.

Ammazon Internet Security
Smart
1.0.0.0

Smart Firewall
Smart
1.0.0.0

Whatsapp for pc 2014
Windows
Windows

SSH VPN
Smart
1.0.0.0

Viber fooor pcexeexe
Screen saver
2.60 MB

اول رد من شادي روحي فدى الاسد على التفجير بدمشق

657 vistas • Hace 2 años.

شكر من شادي روحي فدى الاسد على من شاركنا الفرحة باختراق اسرائيل

1,306 vistas • Hace 2 años.

أختراقات عدة صفحات للمندسين المقاومة السورية مرت من هنا

207 vistas • Hace 2 años.

كشف حقيقة الحريبة للمندسين من قبل شادي روحي فدى الأسد

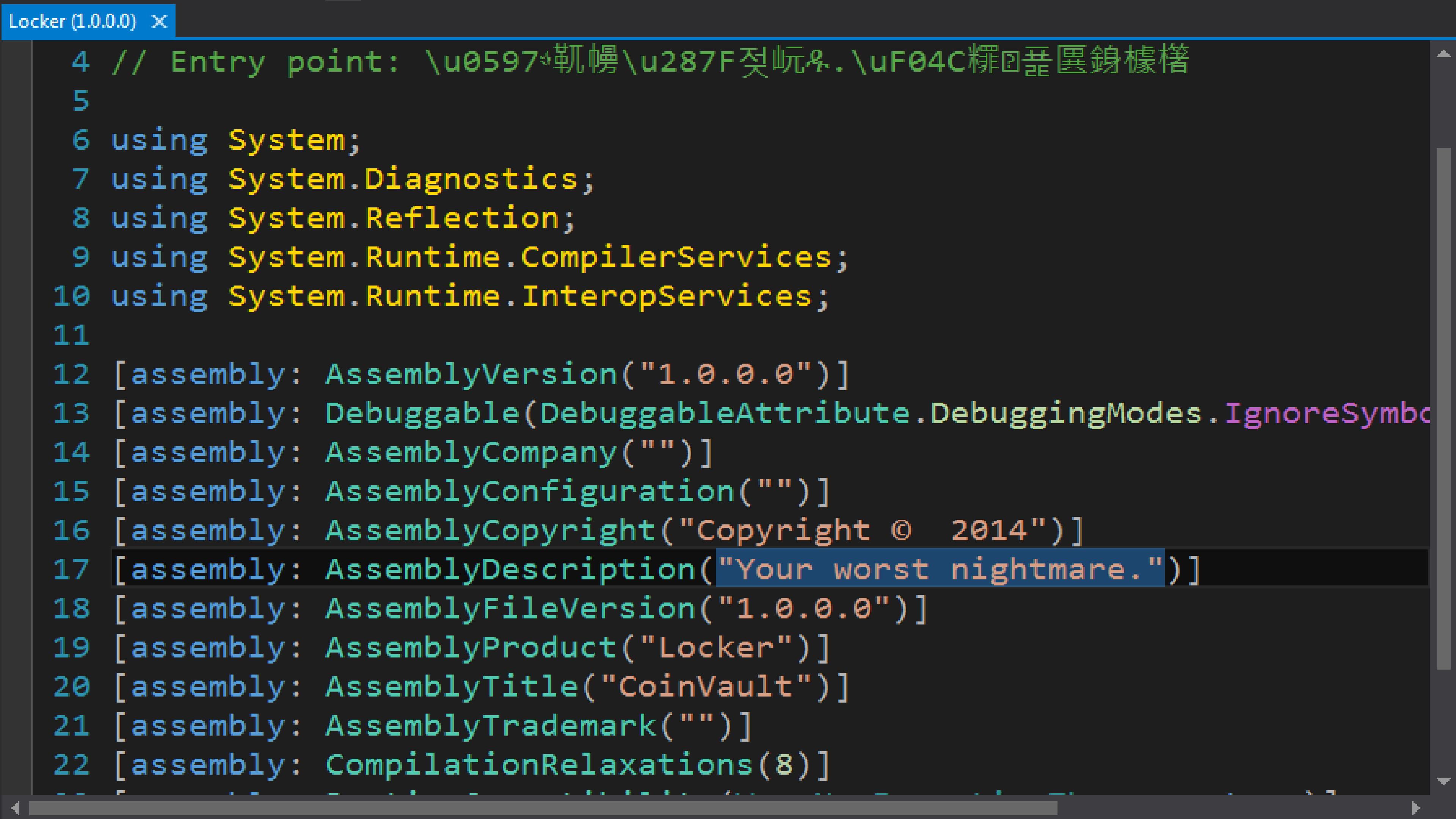
415 vistas • Hace 2 años.

المقاومة السورية شادي روحي فدى الأسد

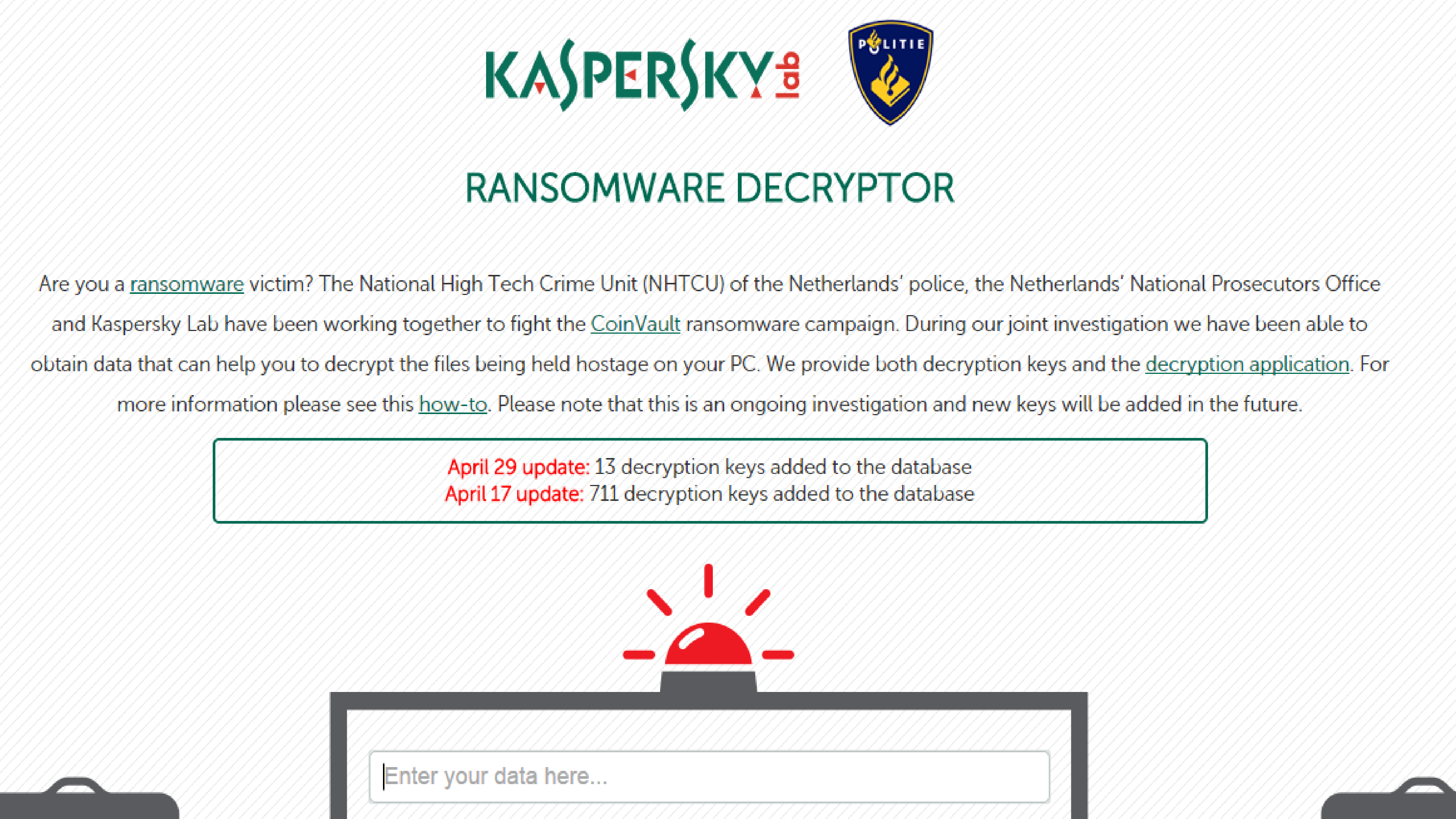
1,500 vistas • Hace 2 años.

YOUR FILES HAVE BEEN ENCRYPTED!

CoinVault®



```
// Entry point: \u0597ᢀ軏幱\u287F癸岏ᛍ.\uF04C糶⍰䜌匽鋿檬橧

using System;
using System.Diagnostics;
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;

[assembly: AssemblyVersion("1.0.0.0")]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbo
[assembly: AssemblyCompany("")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCopyright("Copyright ©  2014")]
[assembly: AssemblyDescription("Your worst nightmare.")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: AssemblyProduct("Locker")]
[assembly: AssemblyTitle("CoinVault")]
[assembly: AssemblyTrademark("")]
[assembly: CompilationRelaxations(8)]
```



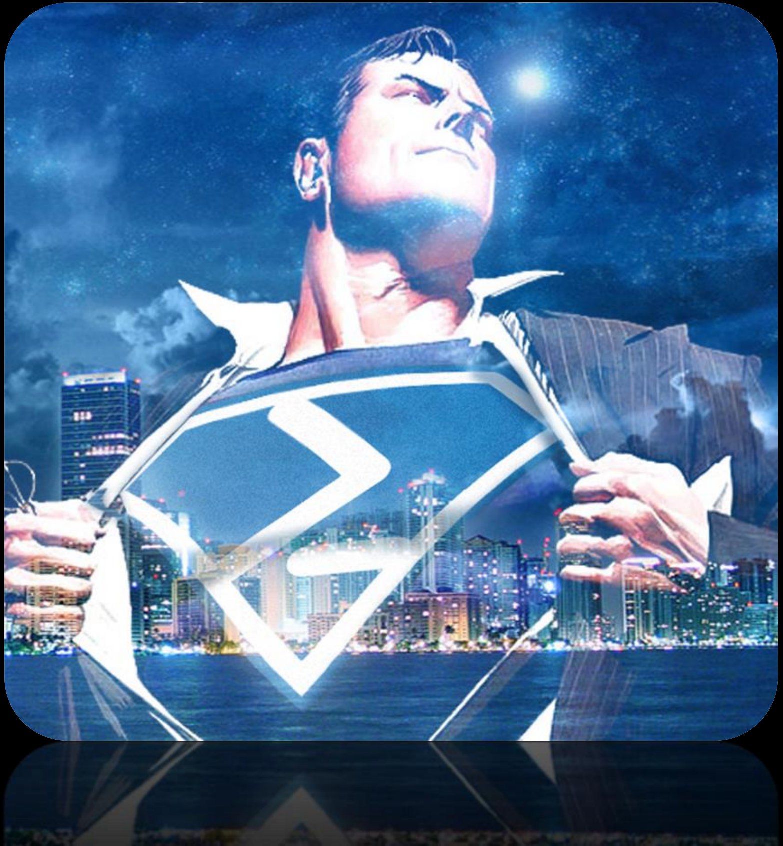
RANSOMWARE DECRYPTOR

Are you a ransomware victim? The National High Tech Crime Unit (NHTCU) of the Netherlands' police, the Netherlands' National Prosecutors Office and Kaspersky Lab have been working together to fight the CoinVault ransomware campaign. During our joint investigation we have been able to obtain data that can help you to decrypt the files being held hostage on your PC. We provide both decryption keys and the decryption application. For more information please see this how-to. Please note that this is an ongoing investigation and new keys will be added in the future.

April 29 update: 13 decryption keys added to the database
April 17 update: 711 decryption keys added to the database

FBI
FBI

POWERSHELL - THE HOLY GRAIL



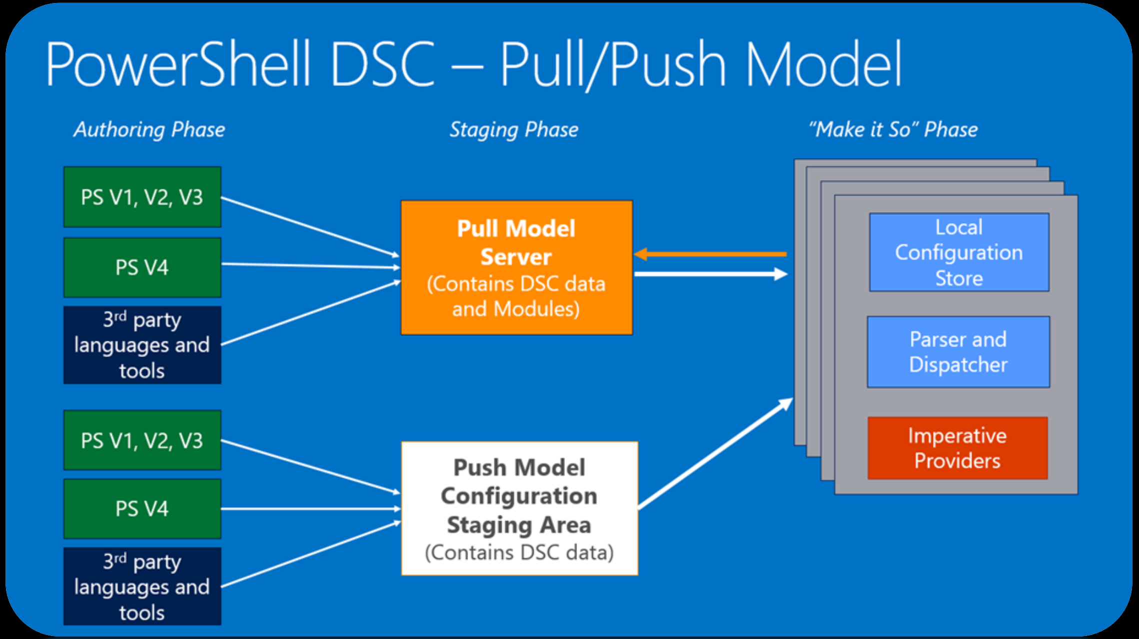
- Revolutionary shell and scripting language
- Based on .NET
- Compatible with many available tools and extensions
- Capable of using available instrumentation (COM, ADSI, WMI, ADO, XML, Text, …)

GIVE ME THE POWER

- **Microsoft's ecosystem supports PowerShell integration.**
- **Management for SQL Server, Sharepoint, Active Directory, Azure.**

POWERSHELL DSC TAKES ON LINUX

- **Provides Push/Pull configuration.**
- **Management Platform for several major Linux distributions.**



PowerShell DSC – Pull/Push Model

Authoring Phase

Staging Phase

"Make it So" Phase

PS V1, V2, V3

PS V4

3rd party languages and tools

Pull Model Server
(Contains DSC data and Modules)

PS V1, V2, V3

PS V4

3rd party languages and tools

Push Model Configuration Staging Area
(Contains DSC data)

Local Configuration Store

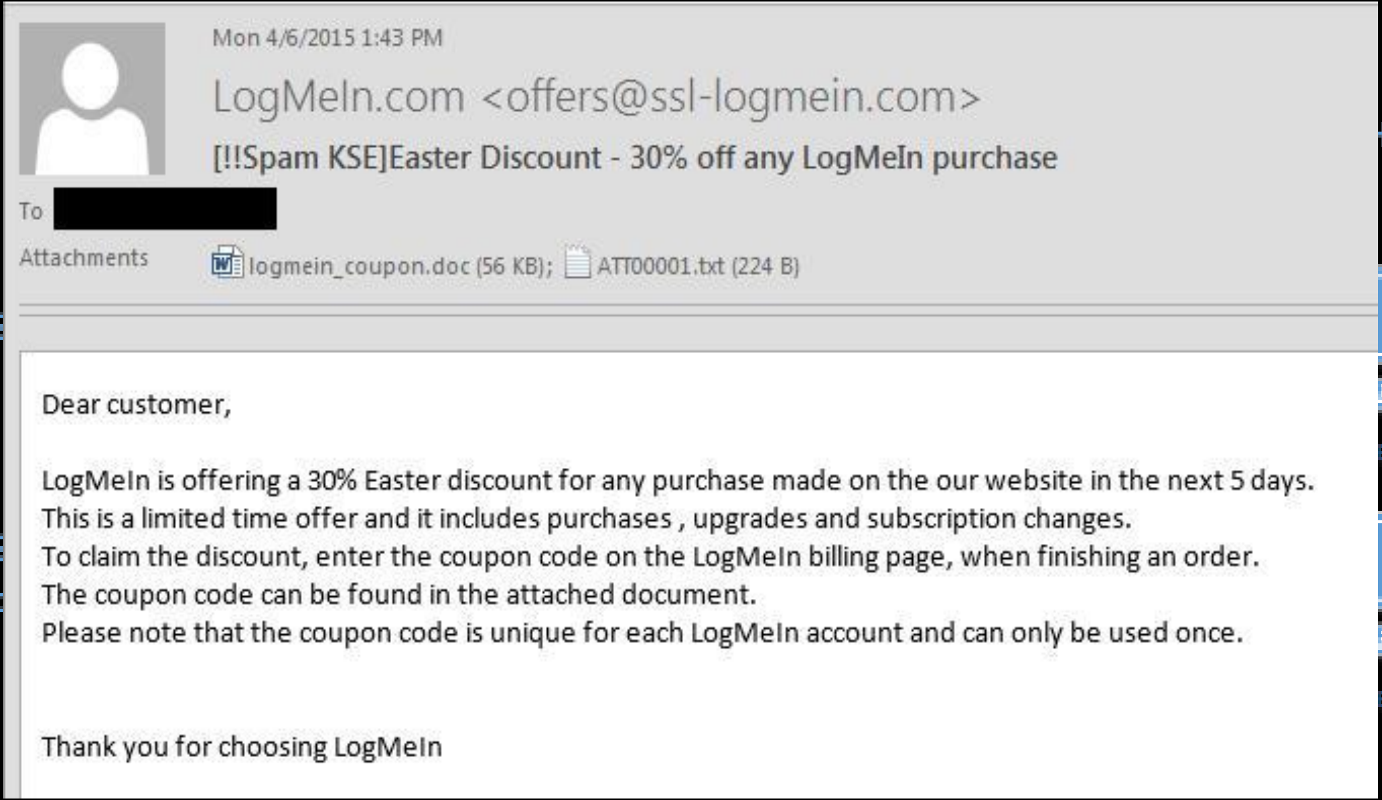
Parser and Dispatcher

Imperative Providers

POWERSHELL AS A SECURITY WEAPON

PowerS

PowerS
wit



Mon 4/6/2015 1:43 PM

LogMeIn.com <offers@ssl-logmein.com>

[!!Spam KSE]Easter Discount - 30% off any LogMeIn purchase

To [redacted]

Attachments logmein_coupon.doc (56 KB); ATT00001.txt (224 B)

Dear customer,

LogMeIn is offering a 30% Easter discount for any purchase made on the our website in the next 5 days.
This is a limited time offer and it includes purchases , upgrades and subscription changes.
To claim the discount, enter the coupon code on the LogMeIn billing page, when finishing an order.
The coupon code can be found in the attached document.
Please note that the coupon code is unique for each LogMeIn account and can only be used once.

Thank you for choosing LogMeIn

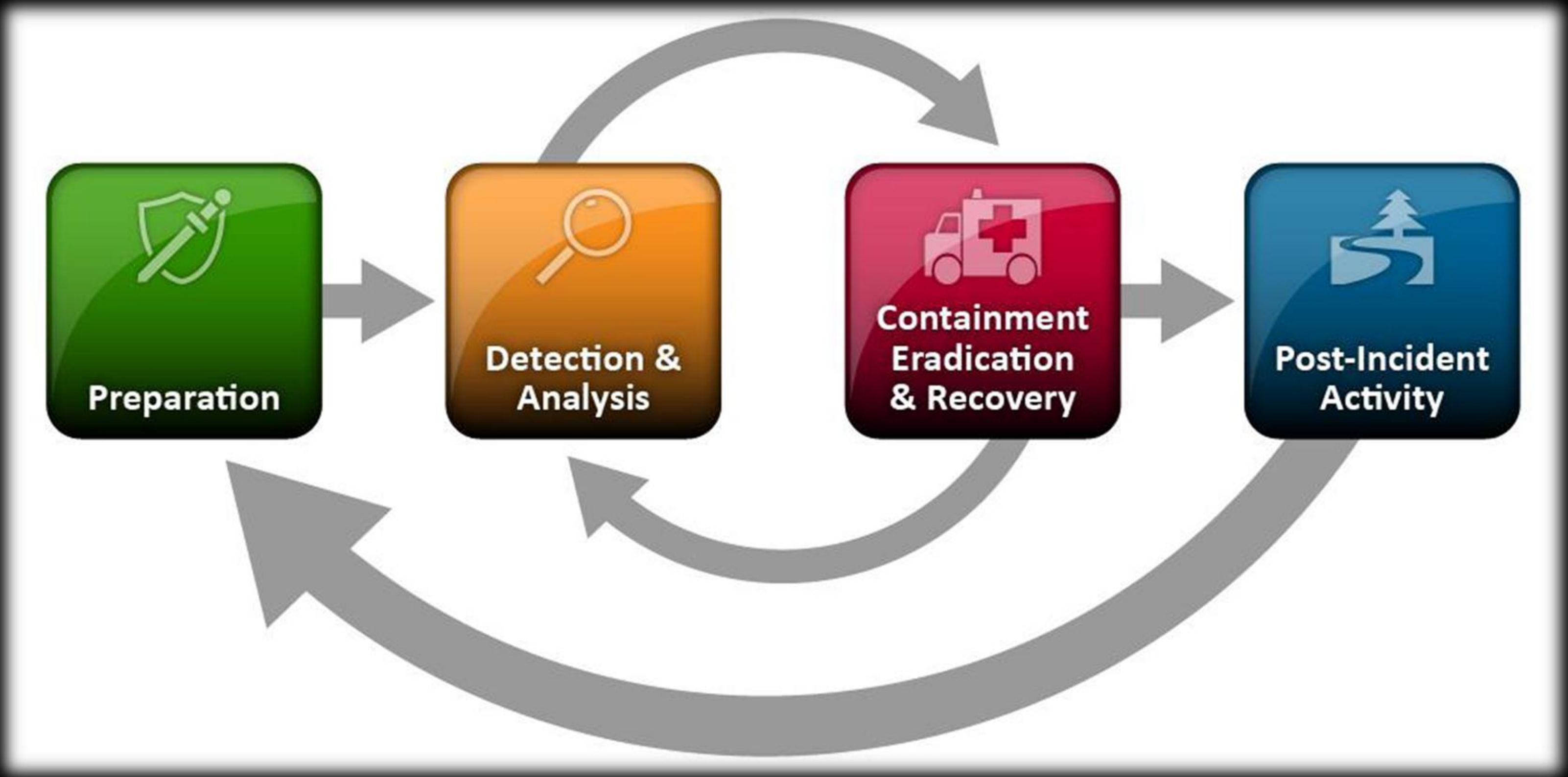
http://www.powershellmagazine.com/2014/03/06/accidental-sabotage-beware-of-credssp/

THE ATTACKER'S ARSENAL

- Social Engineering Toolkit
- Veil Framework
- PowerUp
- PowerView
- PowerShell Empire

- Nishang
- Metasploit
- Powercat

HUNTING EVIL - A FORENSICS APPROACH

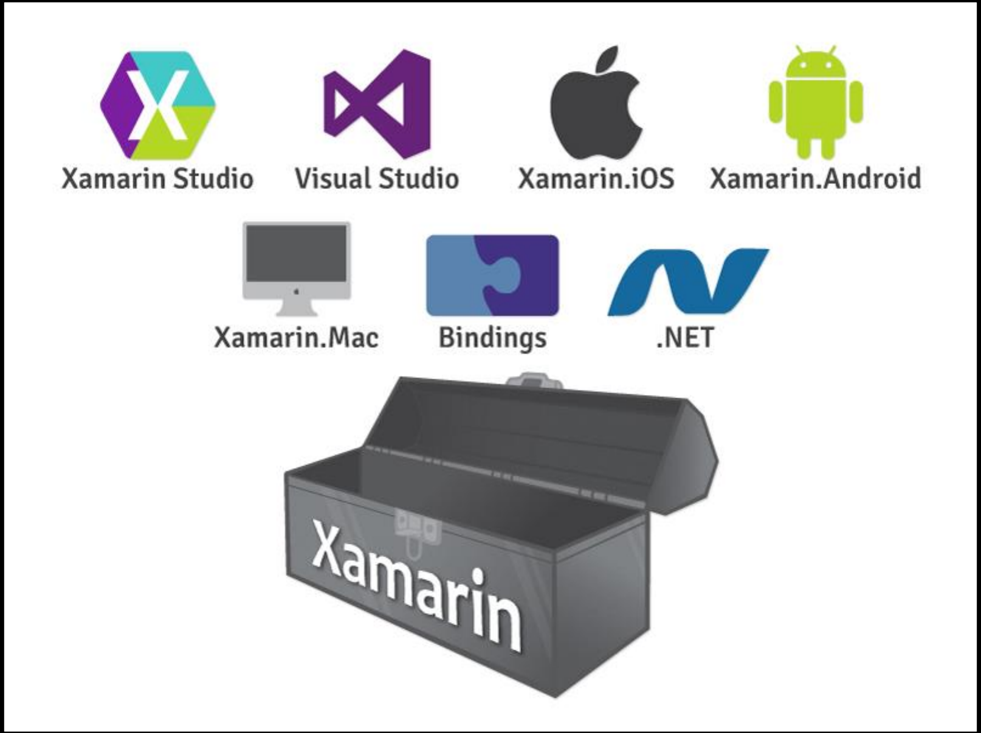


ANTI-FORENSICS

- **Use of web clients to download the payloads**
- **Assembling of malicious binaries in memory**
- **Bypassing PowerShell’s execution policy is easy!**
- **Use of legitimate DLL´s and windows tools**

TRENDS - MULTIPLATFORM THREATS

```
<applet width="1" height="1" id="Secure Java A
```



```
<param name="STUFF" value="">
<param name="OSX" value="http://name.domain.org/nickname/set/mac.bin">
<param name="LINUX" value="http://name.domain.org/nickname/set/nix.bin">
```

BECOME ONE WITH THE TAO

"KNOWING IS NOT ENOUGH;
WE MUST APPLY.
WILLING IS NOT ENOUGH;
WE MUST DO."

Questions / Comments?
Follow us on Twitter
@spontiroli
@r0bertmart1nez

THANK YOU!