

Reverse Engineering

for fun and profit :)

gynvael.coldwind/vx

/bin/whois

ReverseCraft

RE

pentesty

gynvael.coldwind//vx

vuln. research

code

/etc/motd

Reverse Engineering

Co to?

Po co to?

(w jakim celu się reversuje, przykłady)

Jak to?

(narzędzia, techniki)

/etc/motd

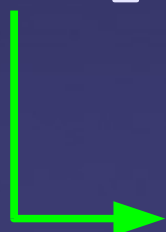
Reverse Engineering ???

*technika odwracania
inżynieria odwrotna
inżynieria wsteczna
analiza odwrotna
analiza wsteczna
programowanie zwrotne (???)*

Programowanie od tyłu?

Programowanie

koncept



projekt



kod



binarka

/etc/motd

Reverse Engineering

koncept



projekt



kod



binarka

/etc/motd

?

Anty RE = RE

?

? Nowe PC?

DLAZAMOST PIRACKIE FLAGI

Seria artykułów odkrywających między innymi tajniki zabezpieczeń, których druk rozpoczynany w tym numerze, stała się w naszej redakcji tematem wspaniałych dyskusji na łamach i czytelnicy bezprawnego rodnego poglądów na ten temat za-
Nie byłbym sobą, gdybym nie włożył kilku zdań, wyjaśniających co nie miały okazji zetknąć się z programem (np. kompilatora lub dobrej gry) wymaga ogromnego sił i czasu (mogą to być miesiące lub nawet lata pracy). Często ten produkt może być powielany (kopiuwany) i kadzi z kopii ma taką samą wartość użytkową jak oryginał. Pozwala to autorowi sprzedać program wielu użytkownikom i uzyskać godziwą rekompensatę za swój trud. Jednak nieuczciwy nabywca może także robić kopie i sprzedawać je na własną rękę, odciągając korzyści, które mu się nie należą (oczywiście odświadcza autorowi). Aby temu zapobiec, wielu autorów i firm produkujących oprogramowanie wstawia mające uniemożliwić zrobienie prawnej kopii. Od czasu gdy mam do czynienia z programami, które nie są tak łatwe do skopiowania, jak kiedyś, a między innymi także widać widać można znaleźć w artykule "Od środka", więc wracamy do redakcji "Bajtek".

Barżo szybko uzgodniliśmy, że nie można odrzucić dobrego, fascynującego artykułu tylko dlatego, że widać w nim zawarta może ulatwić złamanie zabezpieczenia programu i w konsekwencji jego skopiowanie wbrew woli autora. Nie można przecież mieć pretensji do producenta zapieki o to, że istnieje podpalacz. Gdyby zrezygnować z produkcji zapieki, to uciepiał na tym przede wszystkim zwykli użytkownicy, używający jej do zapieki własnych swoich codziennych potrzeb. A Czytelnicy "Bajtek" to przecież właśnie zwykli użytkownicy!

Jednak w tym dyskusji się nie zakończyła, gdyż jak się dało okazać, temat jest bardzo gorący. Bezpośrednim pretekstem stał się komentarz przytoczony do łask pirackich flag z kilku poprzednich numerów, oraz propozycja tytułu "Coś dla wspaniałych". Argumenty wplynęły dwutorowo: po pierwsze, widać w świecie powszechna zabawa, stymulująca i edukacyjna, próba sił między dwoma programistami, pośrednio mobilizująca do pogłębiania umiejętności. Wzrósł więc do tej zabawy i nazywamy ją po prostu "Pracę z obłąkami, piracka flaga na maszt!" Drugi nurt był praktyczny: bardzo wielu tzw. "apre-

Andrzej Pilaszek

ODSROKACZKI

Mало kto lubi programy, które przy pierwszym lepszym błędzie BREAK czyszczą całą pamięć komputera, nie pozostawiając po sobie żadnego śladu, albo "zawieszają się", zmuszając do wciśnięcia RESET. Sytuacja przestaje być zabawna, gdy mamy jakiś dobry program użytkowy, który program stosować do nietypowego sprzętu (lub gre do rzadkiego sportowego joysticka) lub gdy chcemy zmienić w programie wszystkie teksty angielskie na polskie, a program nie daje się zatrzymać.

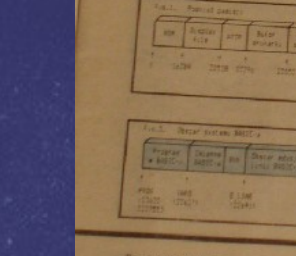
Chodziłbym przodkowiech w mikroelektronice tym artykuł. Kogoś wiec przedawca nie może nie mieć przy sobie informacji o swoim komputerze, jego konfiguracji, sposobie złączenia w pamięć poszczególnych RAM, w jakie systemy, itp. Podjęcie zabierania się do wywołania programu i bloków danych z pamięci "zawieszanie" sprzętu, tak, jak by się nie udało, nie jest to jednakże sposobem przydatnym, w specyficznym znaczeniu. Mamy nadzieję, że nasz wykład nie będzie na marne i ty także znajdziesz się dostatek bez przesady do każdego programu.

Zacznijmy więc od podstaw pamięci. Zaczniemy pamięć podzielona jest na dwa główne części: ROM i RAM. ROM zapisuje dane o adresie RAM natomiast zapisuje 16384 - 65536. Zawieszanie RAM nie będzie się na razie zajmować, więc za to pamięć przywrócić się do podstawowej pamięci RAM. Jest ona podzielona na bloki spełniające różne funkcje w systemie BASIC a tryb 1).

Pamięć dyskową ZX Spectrum została zrealizowana z myślą o współpracy z magnetofonem lub magnetofonem. Nie oznacza to, że używane są taśmy, ale to, że prace nad dyskami. Pamięć dyskową do ZX Spectrum powstały w wielu firmach i charakteryzują się różnorodnością zastosowanych w nich rozwiązań technicznych. Jednym z najciekawszych urządzeń tego typu jest 3-człownik wyciągnięty z firmy Timez, umożliwiając jednocześnie podłączenie do Spectrum 4 magnetofonów dyskowych - sterowanych wspólnym kontrolerem. Użytkownik zwykle w ten sposób szybko i niezawodnie dostaje do ponad 500 kb dodatkowej pamięci.

tego zawieszono nie dlatego, że nie było wywołano do innych celów. Pamięć pamięć, że istnieje możliwość, że ten adres jest zajęty przez inny program. Pamięć pamięć, że ten adres jest zajęty przez inny program. Pamięć pamięć, że ten adres jest zajęty przez inny program.

Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.

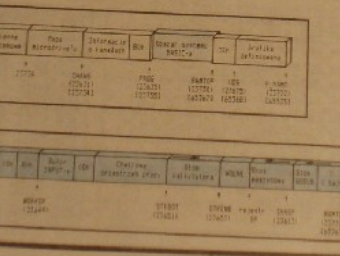


Pamięć dyskową Timez odłączamy do dysku zwanego ZX Spectrum. Pamięć dyskową Timez odłączamy do dysku zwanego ZX Spectrum. Pamięć dyskową Timez odłączamy do dysku zwanego ZX Spectrum.

KLAN SPECTRUM

Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.

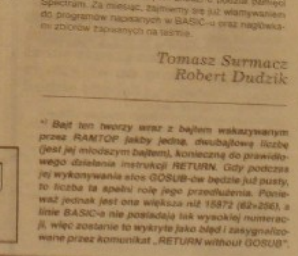
Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.



Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.

Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.

Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.



Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku. Przebiegamy przez procedury formatowania dysku.

7

kto reversuje?

Kto reversuje?

Hobbyści
Profesjonaliści
Researcherzy
Black Market

Cracking

crackme
keygenme
*me

(czyli to co wczoraj
na warsztatach ;>)

komercyjne
oprogramowanie

zabezpieczenia
antypirackie:
?@!#%@#\$%^
(next slide)

Hobbyści - „zabezpieczenia”



EA Spore (SecuROM=1 of 5 @ amazon, 1.7mln @ TPB)

Hobbyści - „zabezpieczenia”



**Ubisoft Assassins Creed 2 – Single player req. con. to serv.
crackers made an emu lol.**

Hobbyści - „zabezpieczenia”

News flash dla wydawców/producentów:

**WASZE ZABEZPIECZENIA NIE DZIAŁAJĄ
I NIE BĘDĄ DZIAŁAĆ.**

Przestańcie wkurzać płacącego klienta.

Game mods

„I might have gone a different way...”
Riddick

<http://diablo.phx.pl/awake/>
New Storyline, New spells, New monsters
New unique monsters, New base items,
New unique items, New quests
New graphics, New music, New sounds
New movies, Shared Experience

Hobbyści – game mods



Hobbyści – game mods



Hobbyści

Game server emu

Ultima Online

UOX, NOX, POL, RunUO, ...

Hobbyści

In Vas Mani - Greater Heat

In Rox - Poison

In Rox - Poison

Last target set.

An Rox - Cure

Celery looks ill.

some damage has been healed : 47

You should throw it now!

You are frozen and cannot move.

You are already casting a spell. [18]

You have not yet recovered from casting a spell.

Please, wait, resynchronizing.

Resynchronization complete.

You are already casting a spell. [12]

You are frozen and cannot move.

Celery
H: [Health Bar]

Socrates
[Status Bar]

112
116
116
117
109
118
118
113
16
16
19
19
0

Hobbyści

Game server emu

BNETD vs Blizzard

2002 -> 2005

PvPGN

Game utils & libs

BWAPI+BWSAL

BWChart

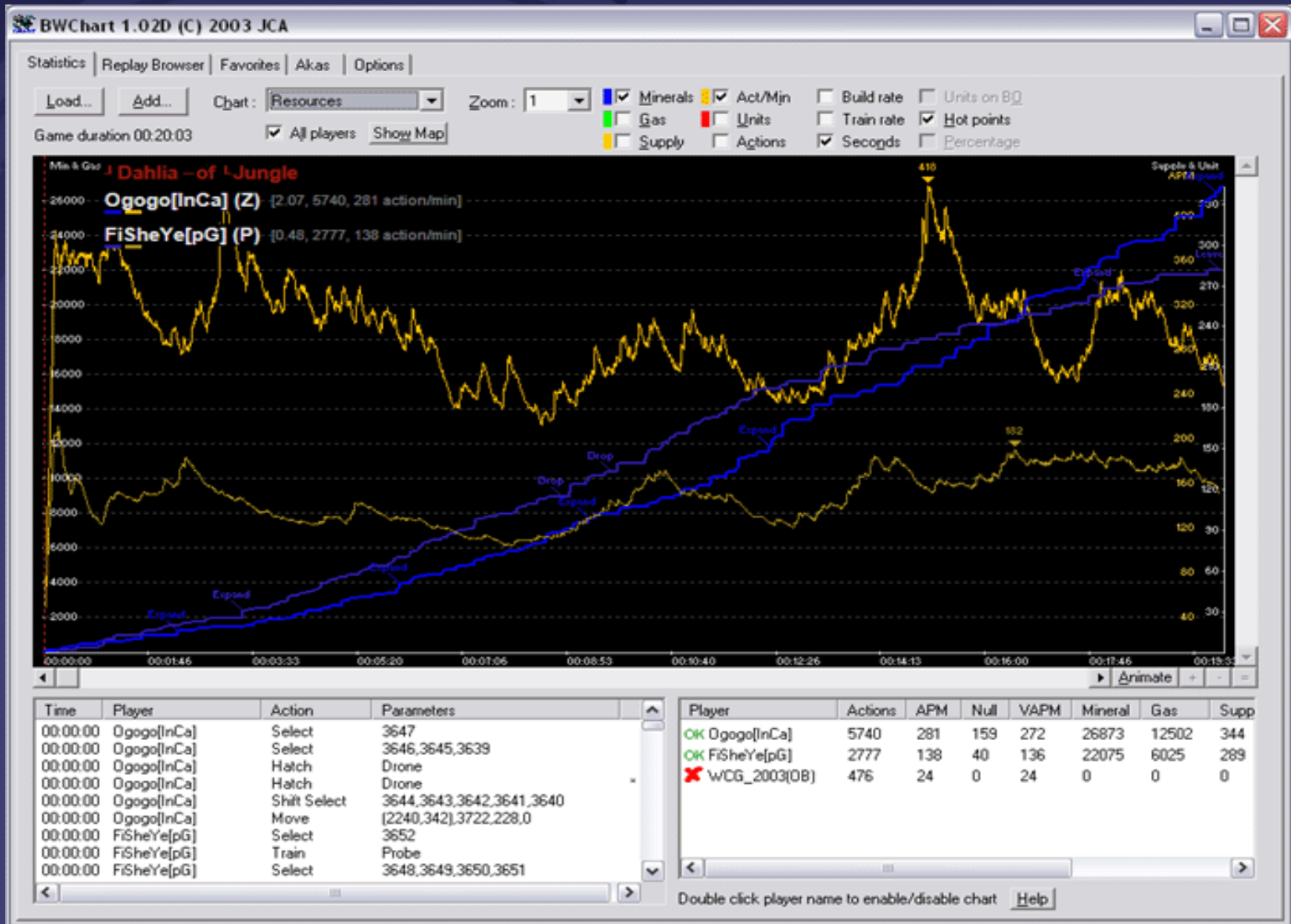
BWCoach

APMLive

Audio Replay

....

Hobbyści



Hobbyści

Question: 100 M(+670), 0 G(+0) - 14/17
production facilities: 1(0)
Units queued: 0 (0 M 0 G)
Avg # Units queued: 0.200 (10.000 M 0.000 G)
Units building: 1 (50 M 0 G)
of idle production facilities: 0, avg: 0.127
Overall macro rating: 5971, avg: 5520.151

ToT|Mendragon: 520 M(+670), 0 G(+0) - 10/17
Hatcheries: 1(0)
Idling larva: 1, Avg: 1433
Units working: 0 (150 M 0 G)
Overall macro rating: 5612, avg: 5655.685

Worker stats for Question:
Total workers: 13
11 workers mining 3 patches, Avg: 3.249
Total workers on gas: 0
Total idle workers: 2

Worker stats for ToT|Mendragon:
Total workers: 10
9 workers mining 3 patches, Avg: 3.492
Total workers on gas: 0
Total idle workers: 0

BO for Question:
6 - Pylon (0:55)
11 - Forge (1:40)
14 - Cannon (2:10)

BO for ToT|Mendragon:
9 - Pool (1:06)
9 - Extractor (1:22)
10 - Overlord (1:30)
12 - Zergling (1:56)
13 - Zergling (1:58)
13 - Zergling (1:58)

Question, 14 - Cannon (2:10)

Terran Command Center
Supplies Used: 1
Supplies Provided: 10
Total Supplies: 10
Supplies Max: 200

Replay Progress
Elapsed Time: 02:16
Speed: Fast

StarCraft (1998) **by Blizzard Entertainment**

**"Have Stim? No, Shield!"
Buffer overflow in map (UMS) loader found
by Deathknight 4 years go.**

"A new glitch found by Deathknight, a buffer overflow, has opened new limitless possibilities for the UMS map making with Starforge, making Starcraft map editing far superior to even Warcraft3 editing."

<http://sc.gosugamers.net>

StarCraft (1998) **by Blizzard Entertainment**

"Have Stim? No, Shield!"
Buffer overflow in map (UMS) loader found
by Deathknight 4 years go.

It was patched by version 1.13b

***"The UMS community did lose a useful tool, as
the bug permitted them some nifty legitimate
UMS functionality."***

<http://sc.gosugamers.net>

Hobbyści

Game remake

Fallout Online

<http://fonline2238.blogspot.com/>

Freesynd

<http://freesynd.sourceforge.net/>

Hobbyści



Hobbyści



Hobbyści

Porty gier

OpenTTD

JJFFE

Frontier: First Encounters

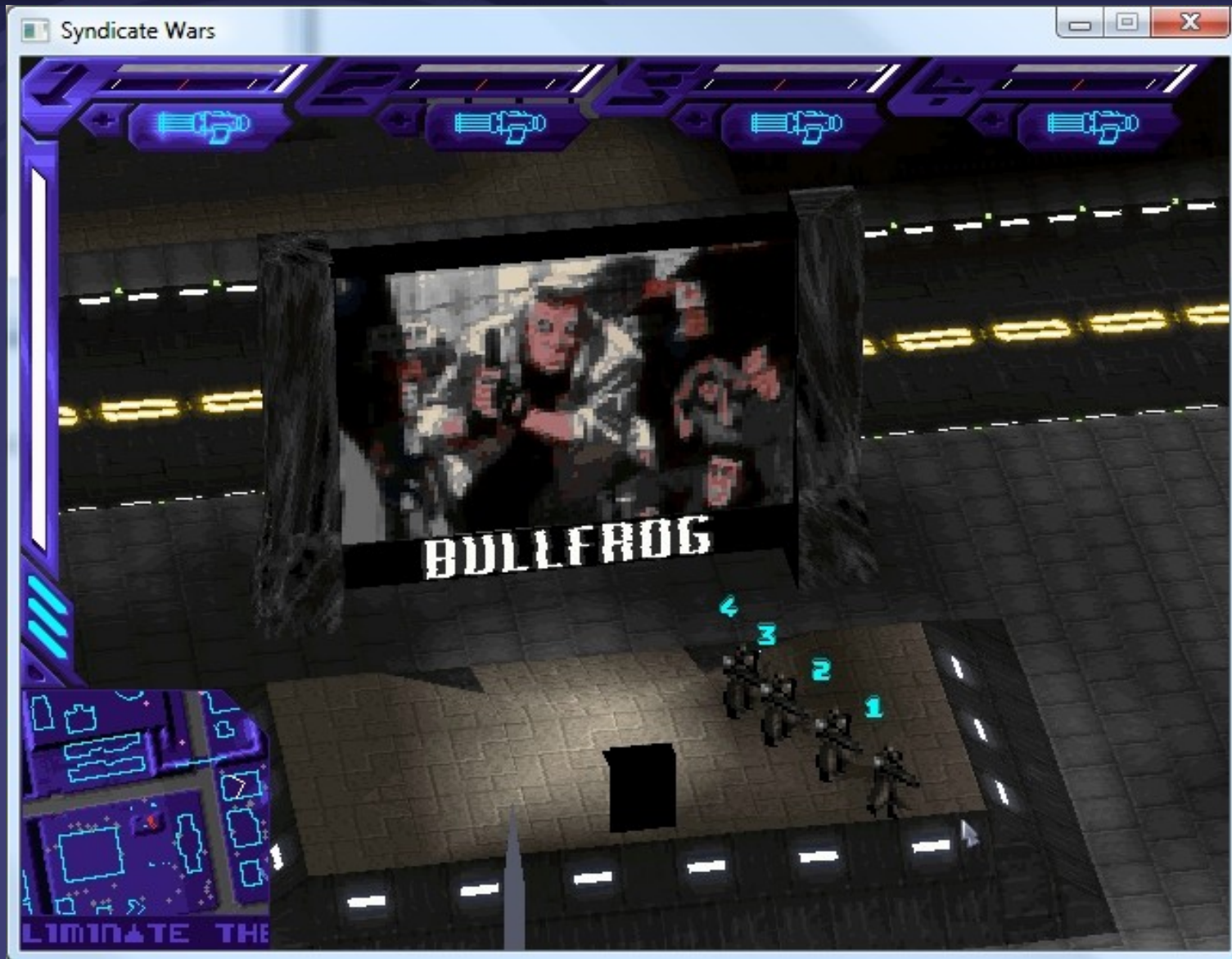
SWARS Port

Hobbyści



OpenTTD: 2002->2004 Port, potem Remake

Hobbyści



Syndicate Wars Port by unavowed & gynvael
5 years, >1mln lines of assembly
<http://swars.vexillium.org/>

Cheaty do gier

Map hack

Wall hack

Auto* hack

etc...

Hobbyści

Malware

**Taaa... kiedyś ludzie to
robili for fun...**

29A

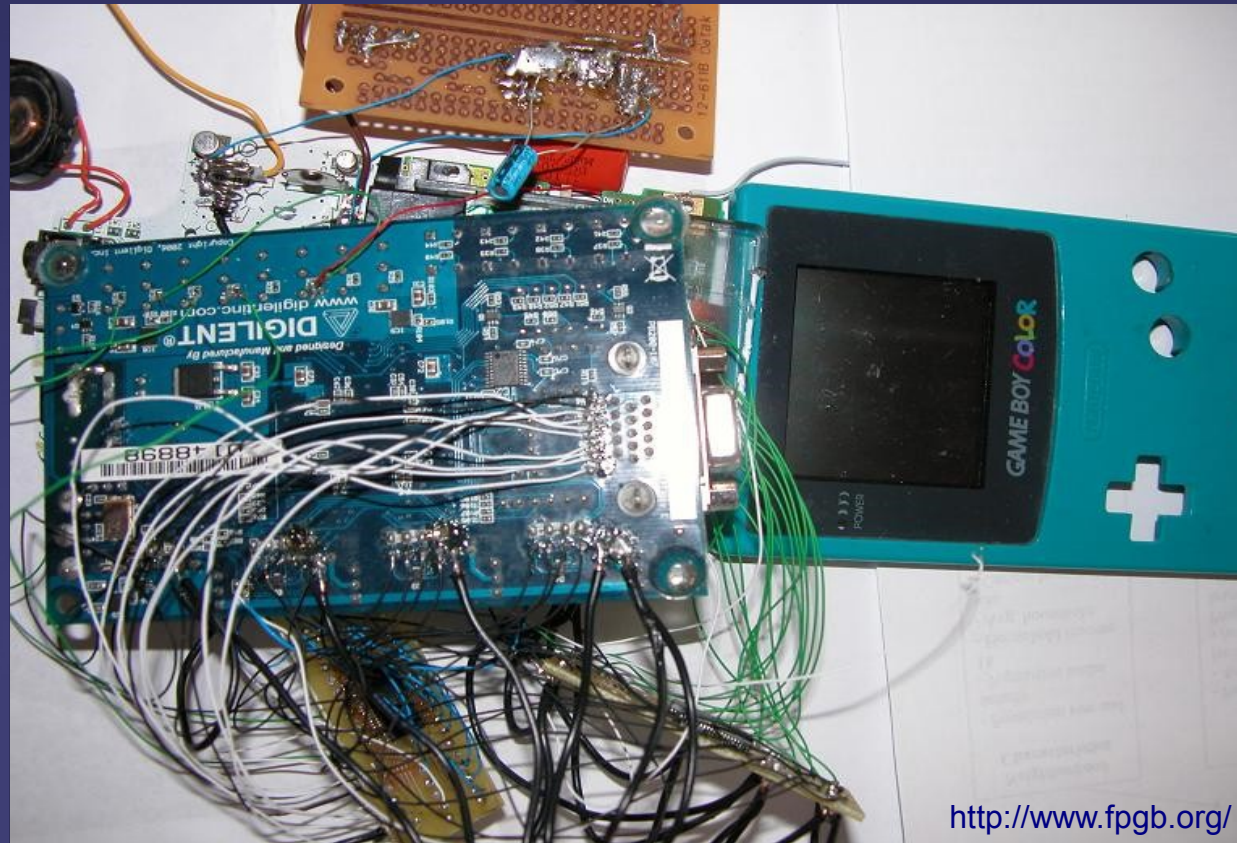
Hobbyści

Vulnerability Research

for fun
and
profit :)

(PWN2OWN)

Hardware/firmware mods



ROM

CARD

Hardware/firmware mods & homebrew

photo by GeRm305



Hobbyści

Hardware/firmware mods & homebrew

<http://hackaday.com/>

Analiza malware

AV

Instytucje finansowe

botnet shutdown

bywa zabawnie:

SQL, FTP, XOR

Vulnerability Research

idef

zdi

inne programy

no more free bugs

Profesjoniści

Hardware Weakness Research

smart card
TPM

black sheep wall

Profesjoniści

Lokalizacja

**Devi nie zawsze
dadzą źródła :(**

Zmianny niesupportowanego softu



screen poglądowy, przedstawiający losową aplikację działającą w systemie MS-DOS

Dokumentowanie

Firma X zrobiła soft

Firma Y go kupiła

Firma Y potrzebuje kompatybilny soft

Firma X nie udostępnia formatu

Firma Y wynajmuje RE

Malware

Banker:

1. Ukradnij dane
2. Wyślij je na server
3. Owner robi przelew

Czy to działa?

Black Market



znalezione w jakimś trojanie, photo z prezentacji [lcewall'a](#)

PERFECT FOR BANKS.

Unica do Brasil: IE6, IE7, Firefox e Internet Explorer 8!



Windows®

Internet Explorer® 8

QUER MAIS?
PERFEITA

To ate sem palavras ;D

Pegando 18 Bancos

Todas as Telas forão refeitas.

Nova Tela do Unibanco, Banco BMG, America Express, Sicredi, Caixa, Real com senha de 3, Credicard Citi, Credicard Itau, Uol pra spam, Serasa, PayPal, Dofus, Itau Personalite, Banrisul, Itau, Bradesco, Brasil e Santander!

Itau pegando Ate Saldo!

Bradesco Entrando na conta!

Bay: vaikarai_7@hotmail.com

Perfeitaaa \o/

Black Market

Vulnerability Research

**Drive-by download
(mpack)**

Worms

Researchers

Nowe techniki RE

Np. nowa lepsza dekompilacja ;)

Nowe techniki Anty RE

np. packery

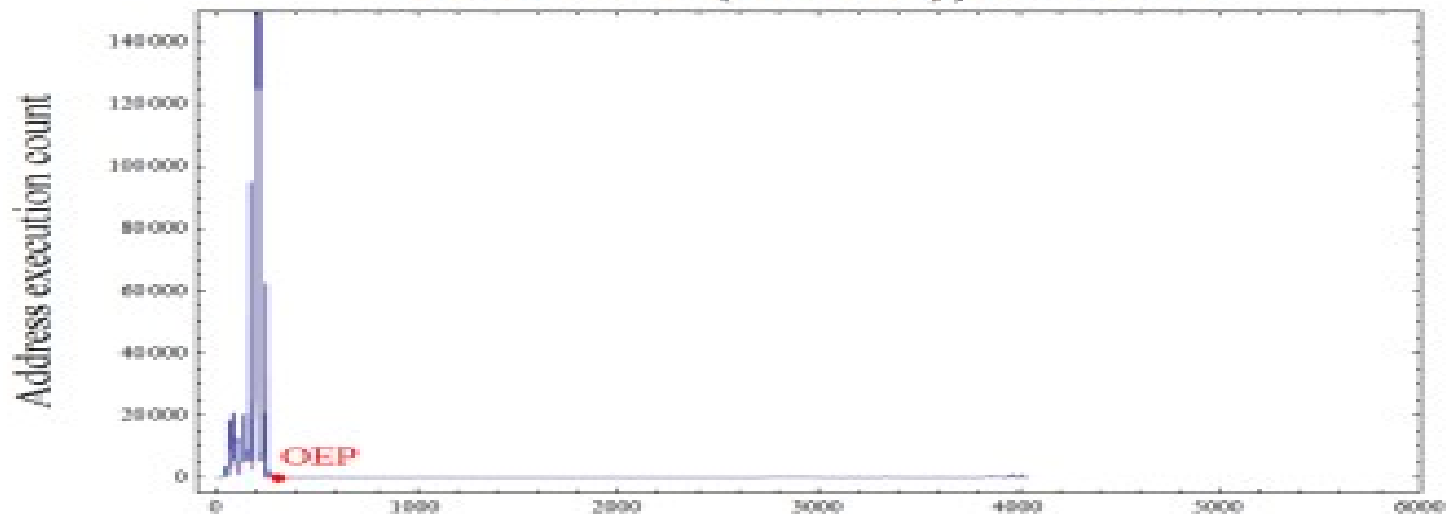
**kod i dane są szyfrowane
w momencie uruchomienia są deszyfrowane
utrudnia analizę
(czasem tylko o 5 sekund ;p)**

Nowe techniki Anty Anty RE

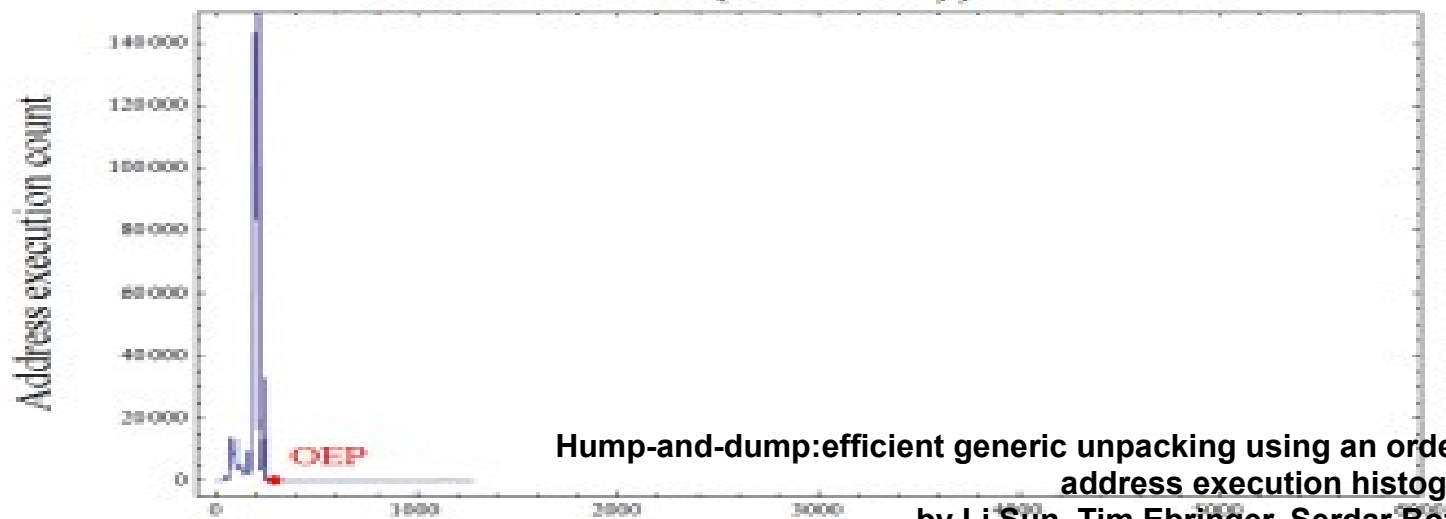
**Hump and Dump
w dużym skrócie:
skoro deszyfrowanie kodu
jest w pętli, to niedługo
po końcu pętli następuje
skok do OEP**

Researchers

UPack 0.399 (calc.exe), liner scale



UPack 0.399 (date.exe), liner scale



Hump-and-dump: efficient generic unpacking using an ordered address execution histogram
by Li Sun, Tim Ebringer, Serdar Boztas

Researchers

Nowe techniki Anty Anty Anty RE

Rozszczepić pętle!

**np. każdą iterację uruchamiać
z innego adresu**

Researchers

**Nowe techniki
Anty Anty Anty ... RE**

**Wykrywać identyczne
sekwencje uruchamianych
instrukcji!**

etc, itd, itp

Prawo?

technika chińskiego muru

Reverser który zrewersuje fragment programu chronionego prawem autorskim i użyje go w swoim programie łamie prawo (bo skopiował nie swój kod).

Np. dlatego w projekcie WINE niechętnie przyjmują reverserów (Microsoft mógłby się wtedy „przyczepić”).

Stąd... metoda chińskiego muru!
(Columbia Data Products, ReactOS)

RE a prawo Polskie

Art. 75.

([http://pl.wikisource.org/wiki/Prawo_autorskie_\(ustawa\)](http://pl.wikisource.org/wiki/Prawo_autorskie_(ustawa)))

2. **Nie wymaga zezwolenia uprawnionego:**

(...)

2) **obserwowanie, badanie i testowanie funkcjonowania programu komputerowego w celu poznania jego idei i zasad przez osobę posiadającą prawo korzystania z egzemplarza programu komputerowego, jeżeli, będąc do tych czynności upoważniona, dokonuje ona tego w trakcie wprowadzania, wyświetlania, stosowania, przekazywania lub przechowywania programu komputerowego,**

3) **zwielokrotnianie kodu lub tłumaczenie jego formy w rozumieniu art. 74 ust. 4 pkt 1 i 2, jeżeli jest to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego z innymi programami komputerowymi, o ile zostaną spełnione następujące warunki:**

a) **czynności te dokonywane są przez licencjobiorcę lub inną osobę uprawnioną do korzystania z egzemplarza programu komputerowego bądź przez inną osobę działającą na ich rzecz,**

Toolset ?

Debuggery
Disassemblery
Dekompilatory
Monitory
Sygnatory
Emulatory
Inne

HW level

Firmware, Hardware

vs

**oscyloskop
programator
lutownica ;)**

BIOS level

OS Loader, Bootkit

VS

BOCHS

IDA Pro

Ralf Brown's Int/Port List

Kernel level

OS Kernel, Drivers, R0 Rootkits

VS

WinDBG

IDA Pro

Ralf Brown's Int/Port List

Virtual PC / VMWare

WDK

App level

Aplikacje, malware, R3 rootkity

VS

WinDBG, OllyDbg

IDA Pro

MSDN

Virtual PC / VMWare / VirtualBox

WDK, kompilator R3

ProcMon, ProcExp., PeID

Ent, Excphook, etc

VM level

Aplikacje

VS

IDA Pro

JAD, Jasmin, SWF Decompiler, flasm
etc...

Data level

Protokoły sieciowe, formaty plików

VS

Hex workshop

Ent

Dużo kartek papieru :)

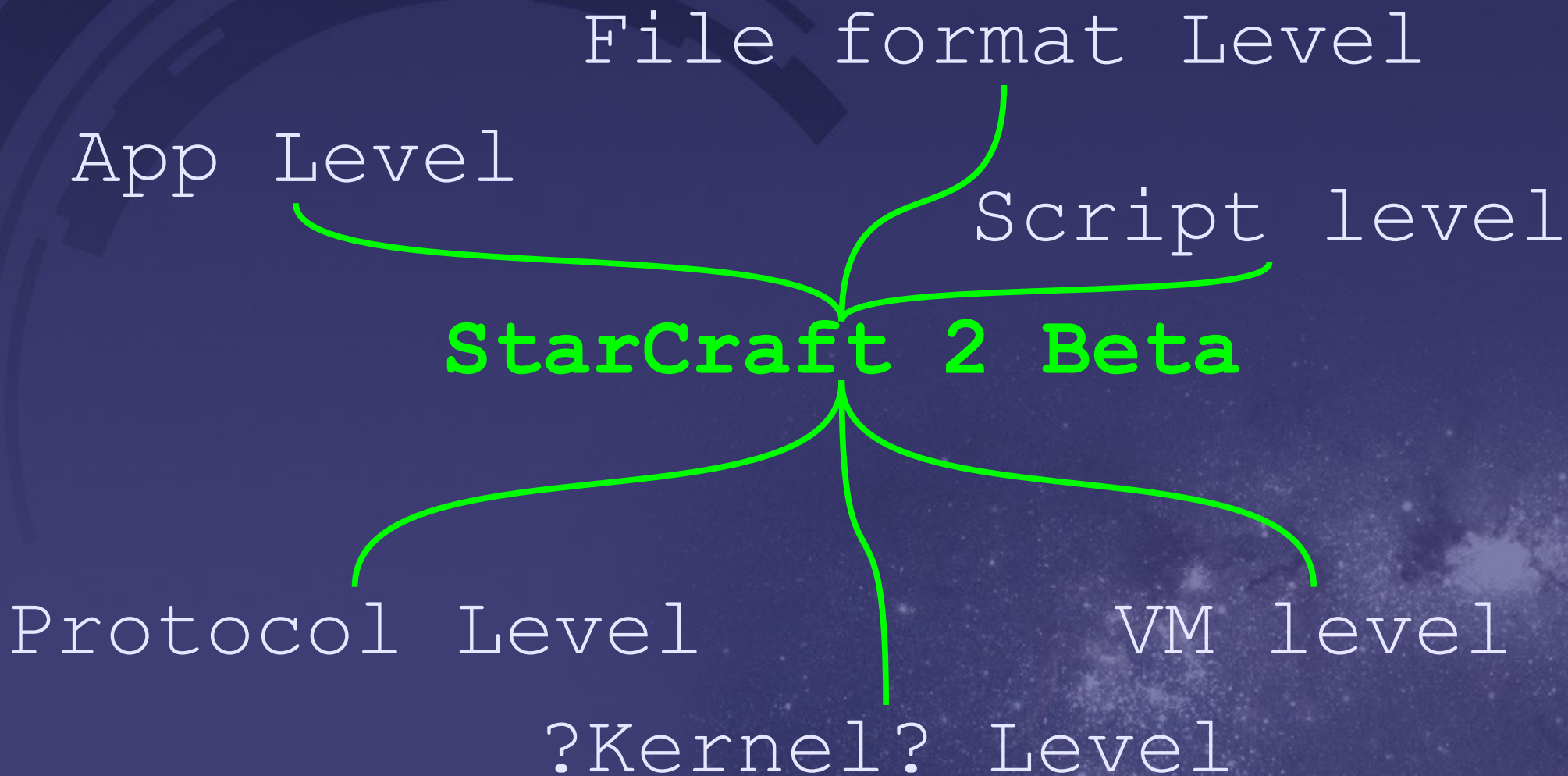
Mix w jednym projekcie?

Mix leveli?

Ba!

StarCraft 2 Beta!

StarCraft 2 Beta





Podsumowanie

Kontakt:

<http://gynvael.coldwind.pl/>
<mailto:gynvael@coldwind.pl>



Pytania?

Kontakt:

<http://gynvael.coldwind.pl/>
<mailto:gynvael@coldwind.pl>



Dziękuję za uwagę :))

Kontakt:

<http://gynvael.coldwind.pl/>
<mailto:gynvael@coldwind.pl>