Reverse Engineering

for fun and profit :)

gynvael.coldwind//vx

/bin/whois

ReverseCraft

RE

pentesty

gynvael.coldwind//vx

vuln. research

code

Reverse Engineering

Co to?

Po co to?
(w jakim celu się reversuje, przykłady)

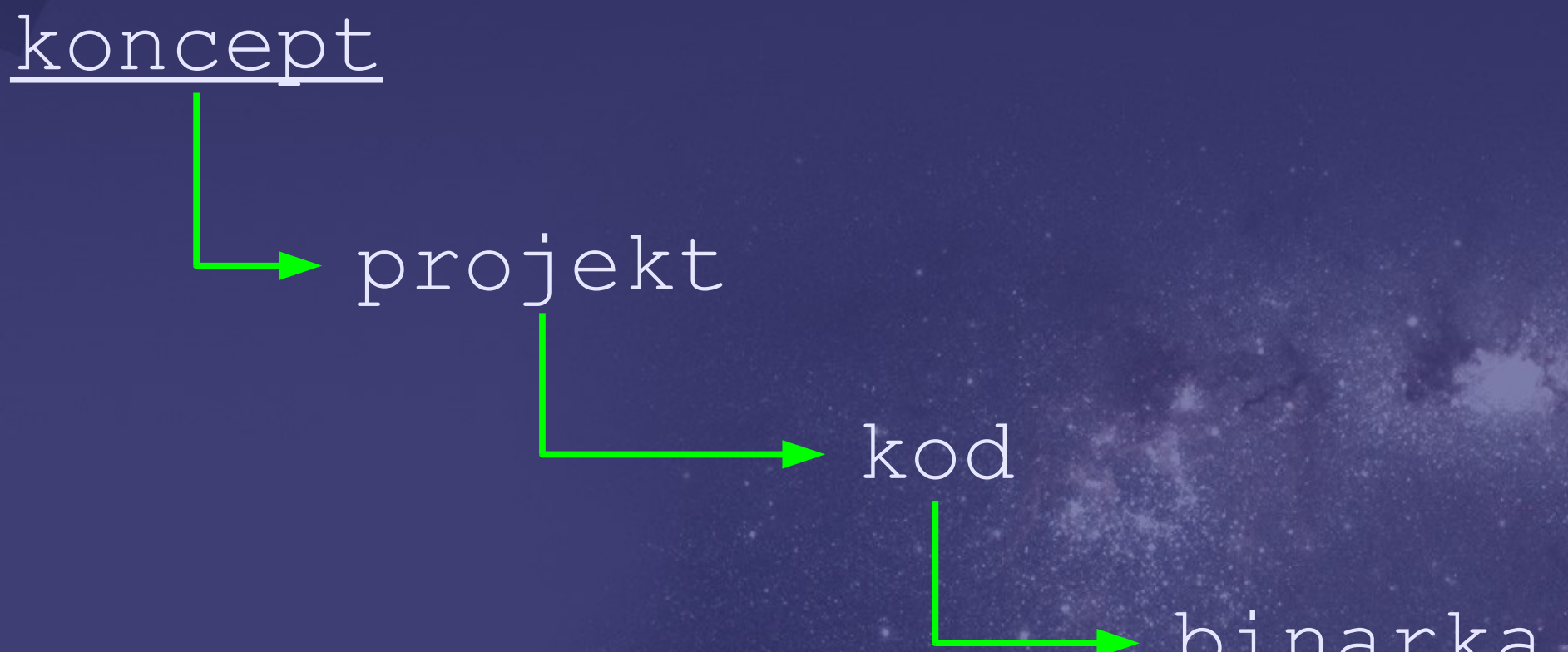
Jak to?
(narzędzia, techniki)

Reverse Engineering ???

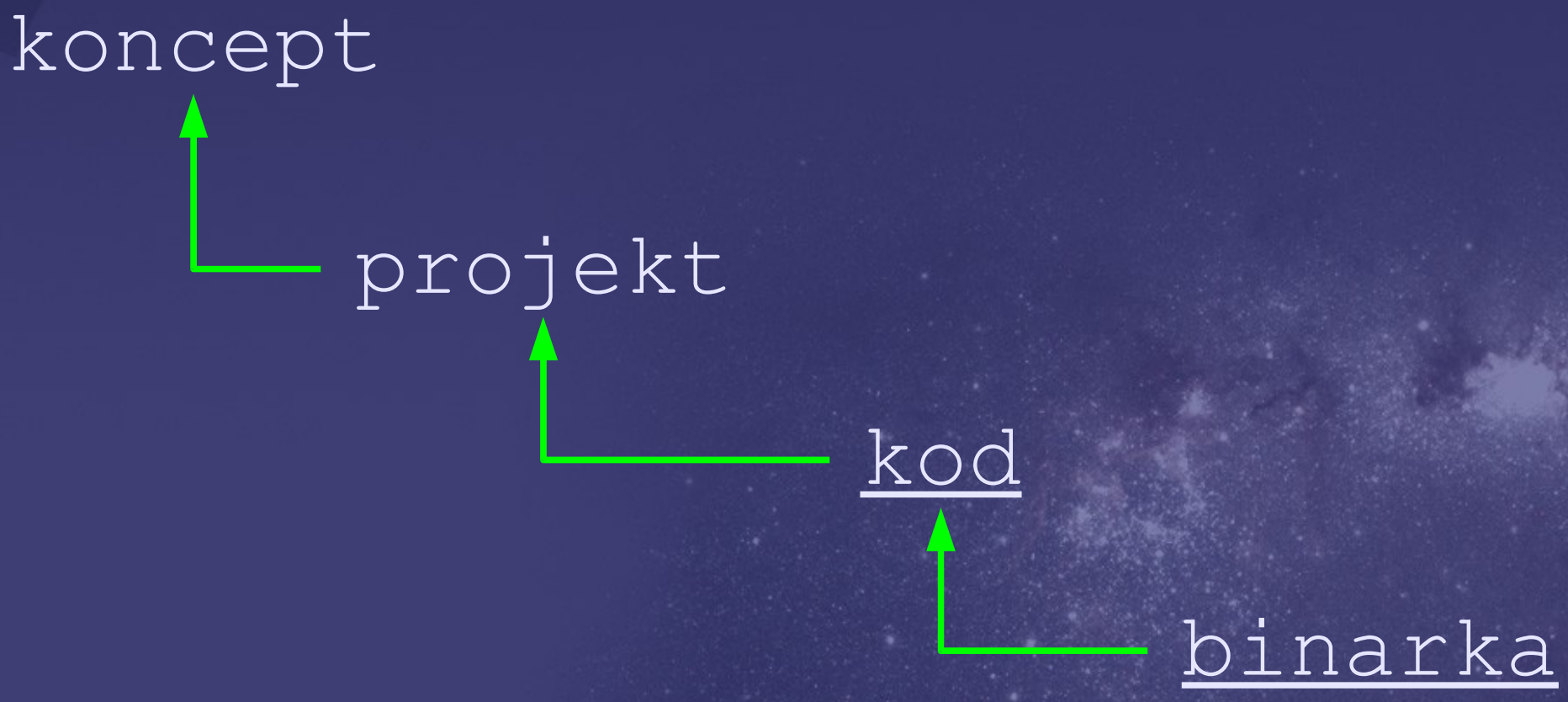
technika odwracania
inżynieria odwrotna
inżynieria wsteczna
analiza odwrotna
analiza wsteczna
programowanie zwrotne (???)

Programowanie od tyłu?

Programowanie



Reverse Engineering



?

Anty RE = RE

?

?Nowe RE?

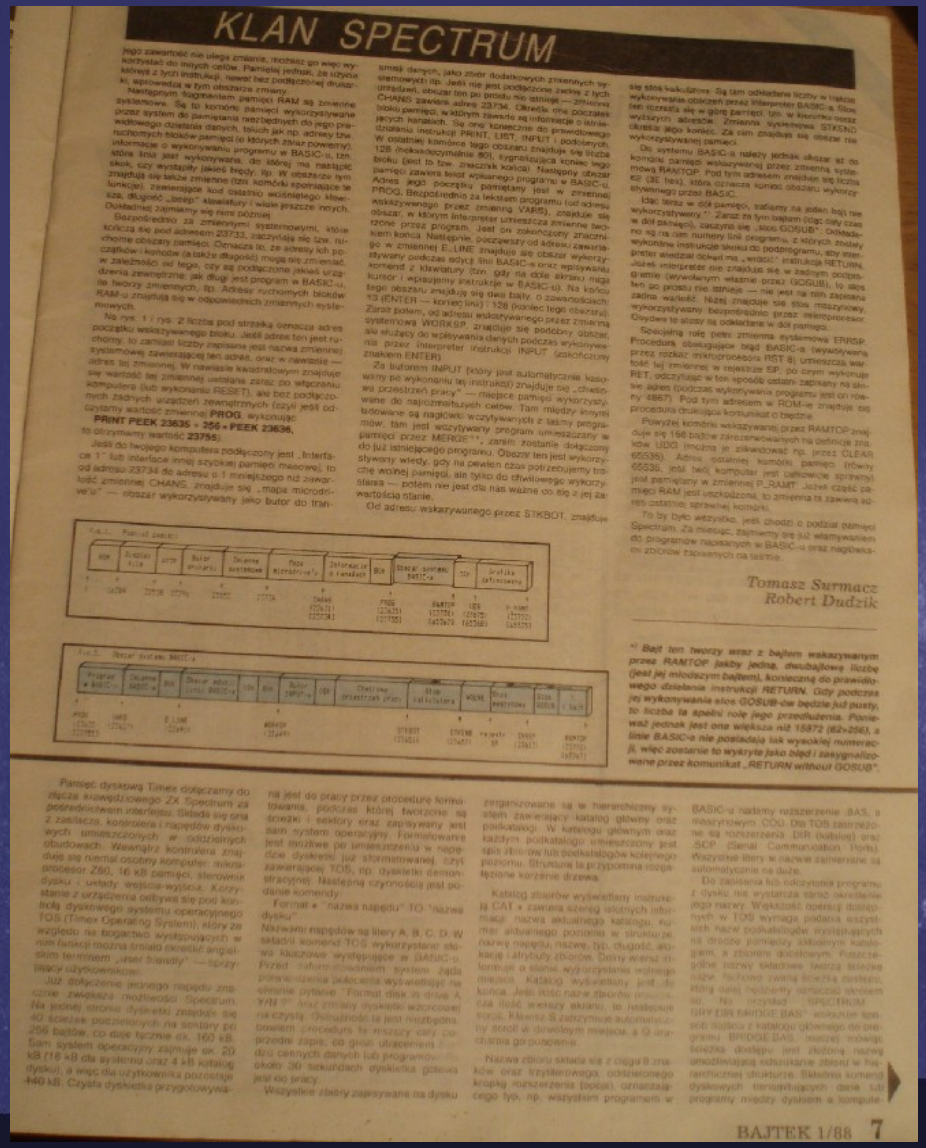
ZAMIAST PIRACKIEJ FLAGI

OD ŚRODKA cz. 1

TOS

Andrzej Pilaszek

6 BAJTEK 1/88



KLAN SPECTRUM

Tomasz Surmacz
Robert Dudzik

BAJTEK 1/88 7

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”

losowy screen znaleziony na google images

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

News flash dla wydawców/producentów:

WASZE ZABEZPIECZENIA NIE DZIAŁAJĄ I NIE BĘDĄ DZIAŁĄĆ.

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

Game server emu

Ultima Online

UOX, NOX, POL, RunUO, ...

Hobbyści


In Vas Mani - Greater Heal
In Nox - Poison
In Nox - Poison
Last target set.
An Nox - Cure
Celery looks ill.
3
1
2
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.
Socrates
Celery
H:
112
116
116
117
109
118
118
113
16
16
19
19
0

Game server emu

BNETD vs Blizzard

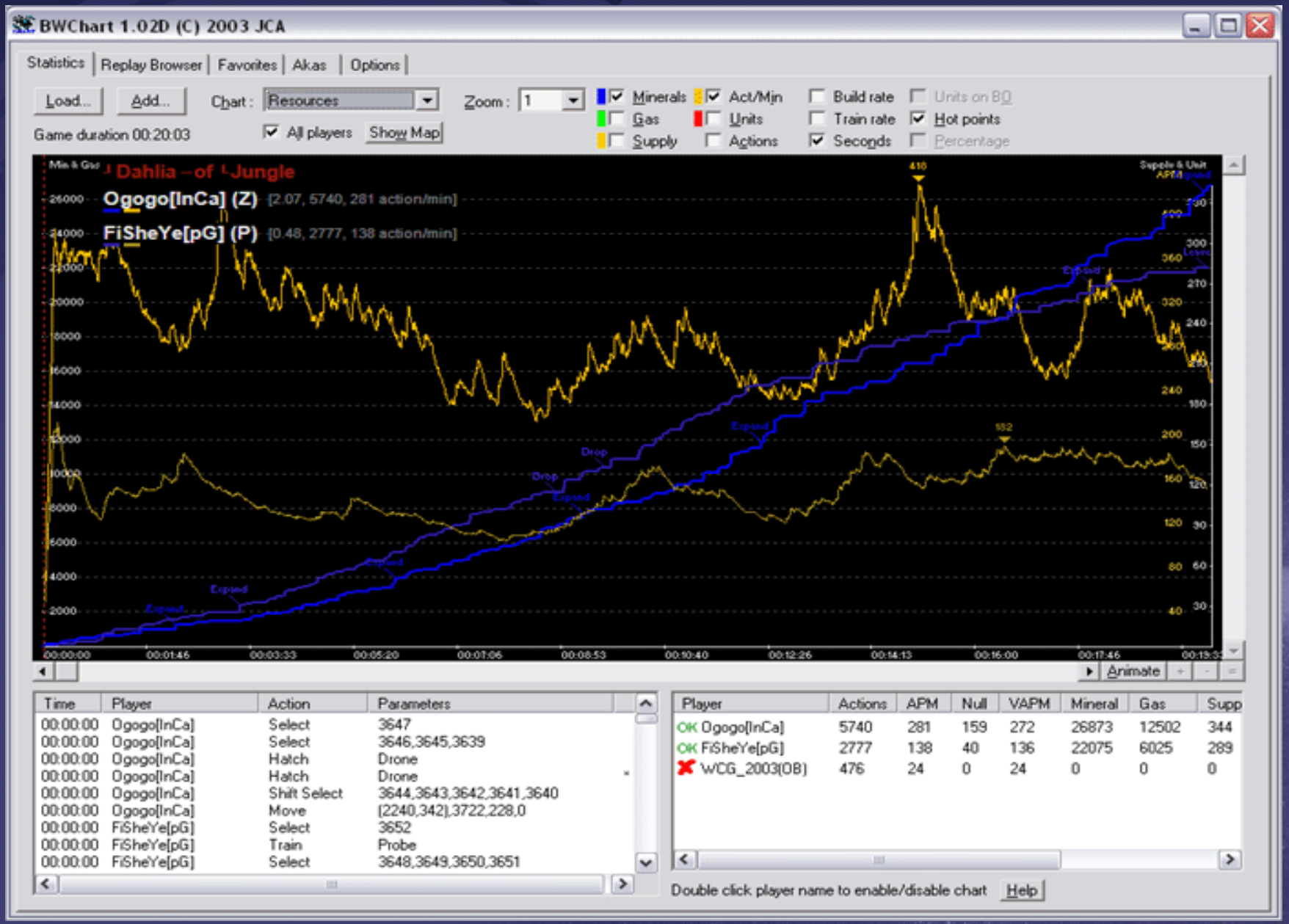
2002 -> 2005

PvPGN

Game utils & libs

BWAPI+BWSAL
BWChart
BWCoach
APMLive
Audio Replay
....

Hobbyści


BWChart 1.02D (C) 2003 JCA
Statistics
Replay Browser
Favorites
Akas
Options
Load...
Add...
Chart : Resources
Zoom : 1
Minerals
Gas
Supply
Act/Min
Units
Actions
Build rate
Train rate
Seconds
Units on BO
Hot points
Percentage
Game duration 00:20:03
All players
Show Map
Dahlia – of └Jungle
Ogogo[InCa] (Z) [2.07, 5740, 281 action/min]
FiSheYe[pG] (P) [0.48, 2777, 138 action/min]
Animate
Time
Player
Action
Parameters
00:00:00 Ogogo[InCa] Select 3647
00:00:00 Ogogo[InCa] Select 3646,3645,3639
00:00:00 Ogogo[InCa] Hatch Drone
00:00:00 Ogogo[InCa] Hatch Drone
00:00:00 Ogogo[InCa] Shift Select 3644,3643,3642,3641,3640
00:00:00 Ogogo[InCa] Move [2240,342],3722,228,0
00:00:00 FiSheYe[pG] Select 3652
00:00:00 FiSheYe[pG] Train Probe
00:00:00 FiSheYe[pG] Select 3648,3649,3650,3651
Player
Actions
APM
Null
VAPM
Mineral
Gas
Supp
OK Ogogo[InCa] 5740 281 159 272 26873 12502 344
OK FiSheYe[pG] 2777 138 40 136 22075 6025 289
WCG_2003(OB) 476 24 0 24 0 0 0
Double click player name to enable/disable chart
Help

Hobbyści


Worker stats for Question:
Total workers: 13
11 workers mining 5 patches. Avg:3.249
Total workers on gas: 0
Worker stats for ToT]Mondragon[:
Total workers: 10
9 workers mining 5 patches. Avg:3.492
Total workers on gas: 0
BO for Question:
8 Pylon (0:55)
11 Forge (1:40)
14 Cannon (2:10)
BO for ToT]Mondragon[:
9 Pool (1:06)
9 Extractor (1:22)
10 Overlord (1:30)
12 Zergling (1:50)
12 Zergling (1:50)
12 Zergling (1:50)
Question: 14 - Cannon (2:10)
Terran Command Center
Supplies Used: 1
Supplies Provided: 10
Total Supplies: 10
Supplies Max: 200
MENU
Replay Progress
Elapsed Time: 02:16
Speed: Fast

Hobbyści

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 Warcraf3 editing."

http://sc.gosugamers.net

Hobbyści

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

Game remake

Fallout Online
http://fonline2238.blogspot.com/

Freesynd
http://freesynd.sourceforge.net/

Hobbyści


PRAY
PRAY
Dement
Eevee
CoolD.
Nikopol
I count eighteen..
Ghosthack
Alpha
BigFucker
SmartCheetah
Blady
RedSix
Mike Grizzly
Heiskanen
Rocco S
matrix
pepper
Jack
Slaughter03
• Nails: Sir, if I may? I think we need to split to units when defending the cathedral.
• Dement: PRAY
• Dement: OBEY
• Ghosthack: FOLLOW
• Mike Grizzly: PRAISE THE HOLY FLAME
• Dement: UNITY
• Nikopol: speak, brother Nails.
• Nails: How many are we? Let's see..
• Nikopol: what do you think what to do to defend our home?
• CoolD.: 17!
• Nails: I count eighteen..
INV
EINZEL
HP
078
029
MAP
CHA
PIP
FIX
Skill ex

Hobbyści

Porty gier

OpenTTD

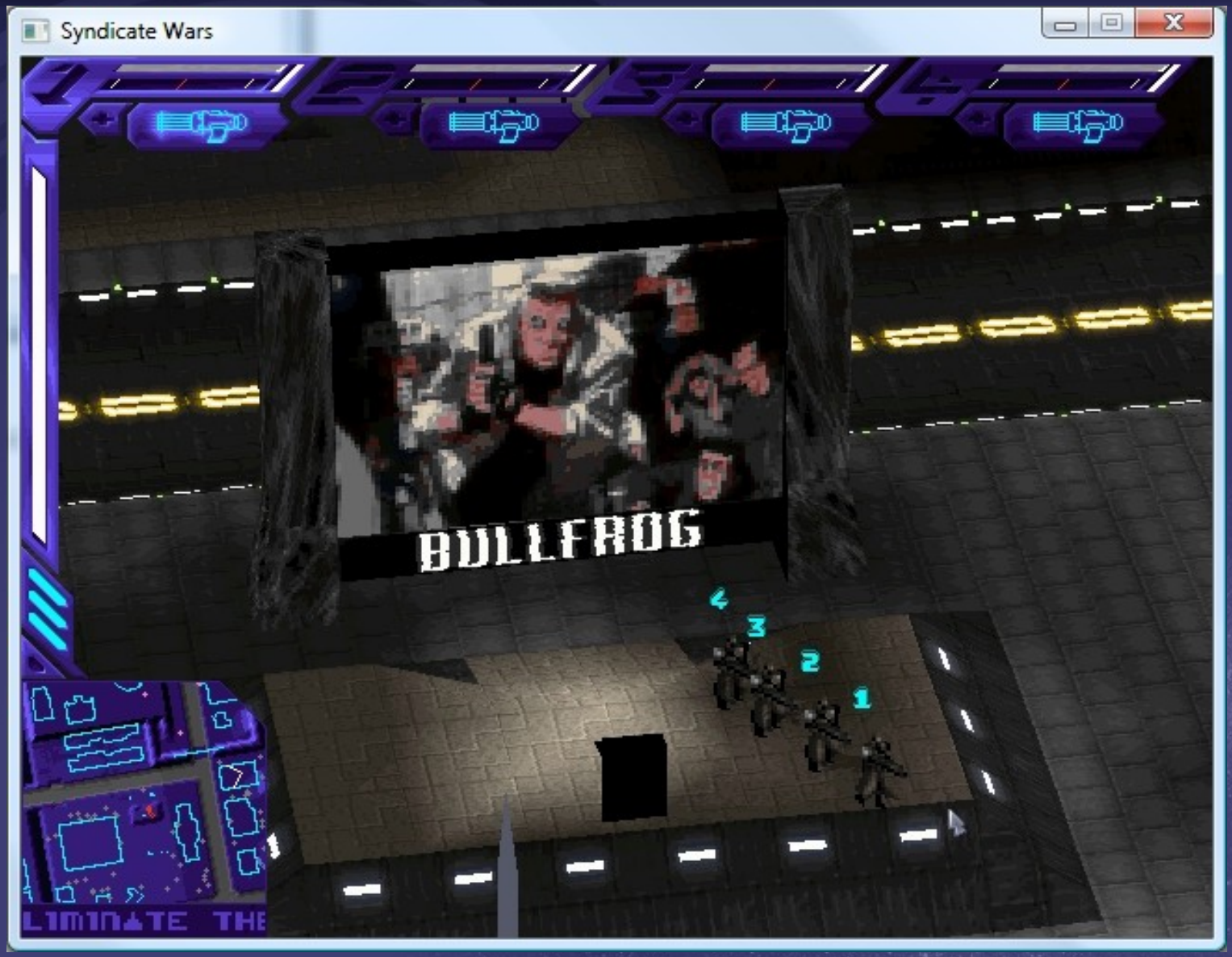
JJFFE
Frontier: First Encounters

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...

Malware

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

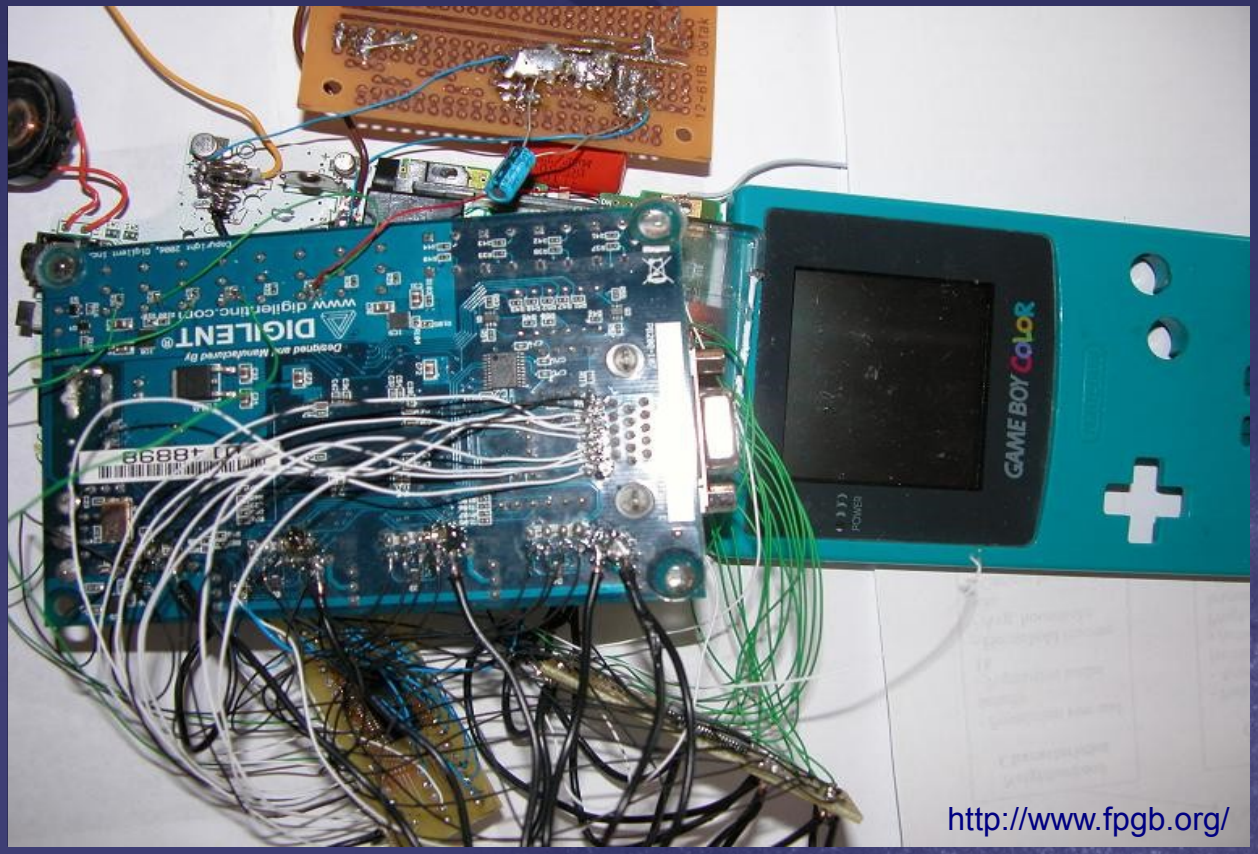
29A

Vulnerability Research

for fun
and
profit :)

(PWN2OWN)

Hardware/firmware mods



ROM

CARD

Hardware/firmware mods & homebrew

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

Hardware Weakness Research

smart card
TPM

black sheep wall

Lokalizacja

Devi nie zawsze dadzą źródła :(

Zmianny niesupportowanego softu

screen poglądowy, przedstawiający losową aplikacje 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 zrobi przelew

Czy to działa?

Black Market

znalezione w jakimś trojanie, photo z prezentacji Icewall'a

Black Market

Vulnerability Research

Drive-by download (mpack)

Worms

Nowe techniki RE

Np. nowa lepsza dekompilacja ;)

Nowe techniki
Anty RE

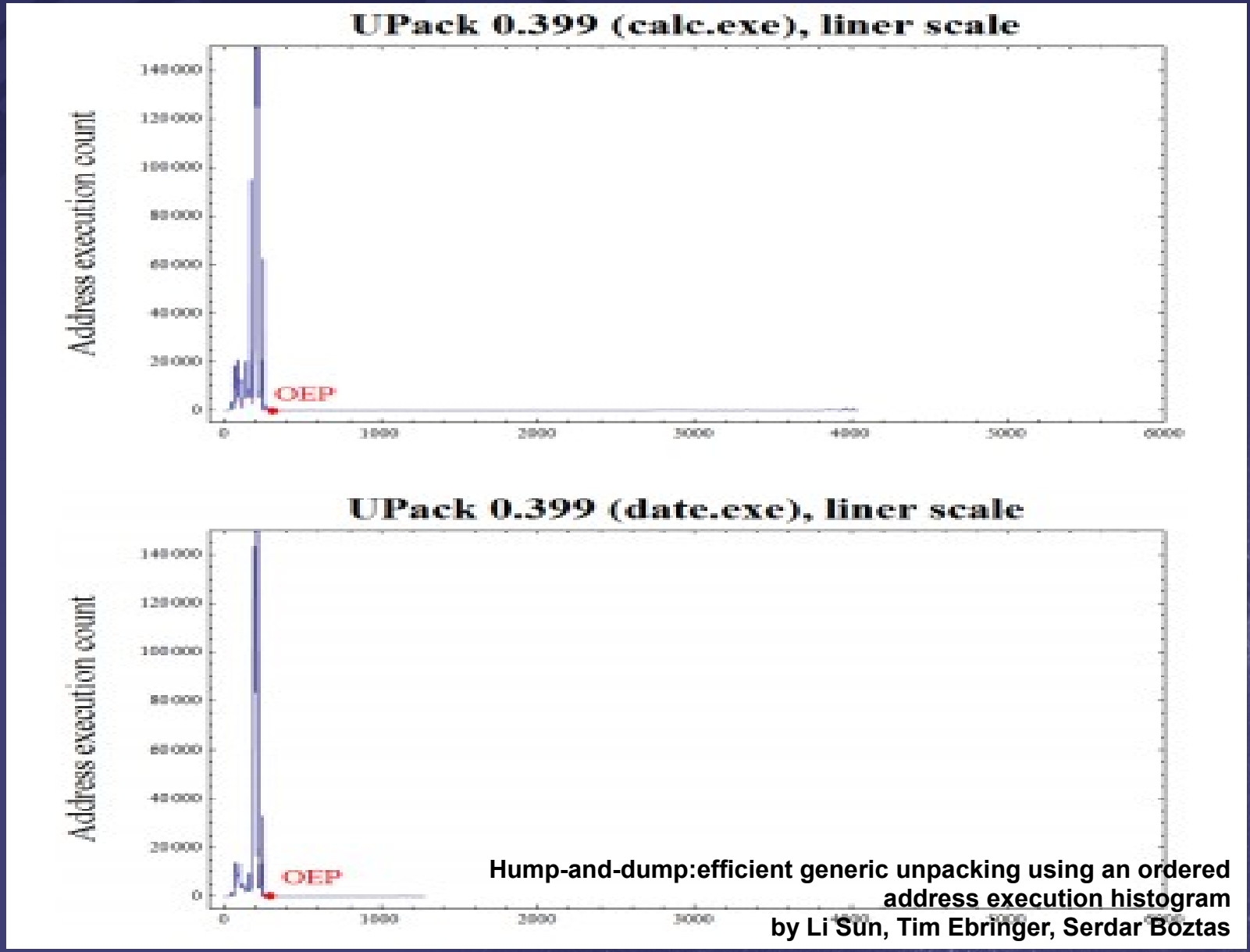
np. packery

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



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

Nowe techniki
Anty Anty Anty RE

Rozszczepić pętle!

np. każdą iteracje uruchamiać z innego adresu

Nowe techniki
Anty Anty Anty ... RE

Wykrywać identyczne sekwencje uruchamianych instrukcji!

etc, itd, itp

technika chińskiego muru

Reverser który zreversuje 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))
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
Sygnatury
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

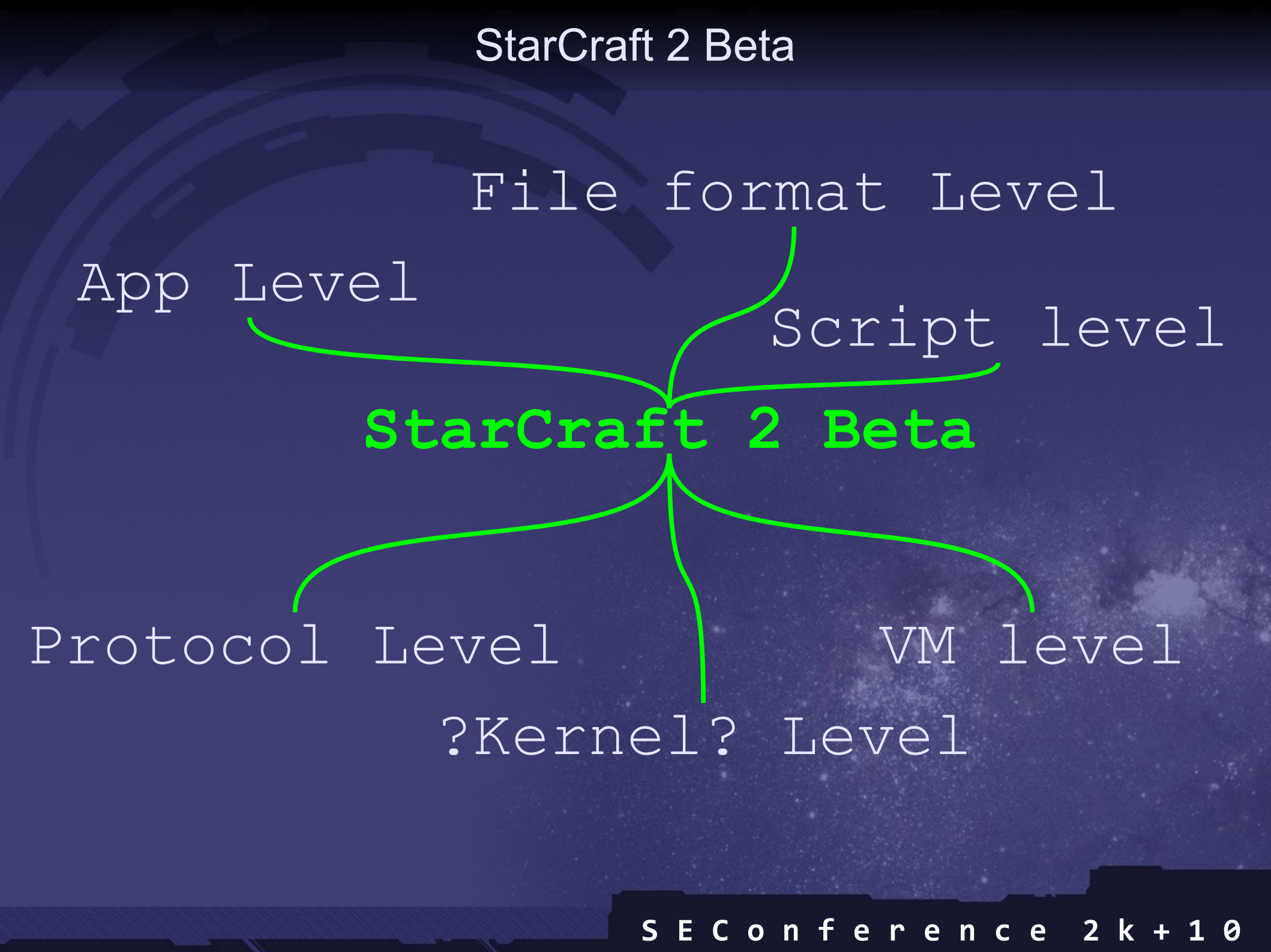
Hex workshop
Ent
Dużo kartek papieru :)

Mix leveli?

Ba!

StarCraft 2 Beta!

StarCraft 2 Beta


File format Level
App Level
Script level
StarCraft 2 Beta
Protocol Level
VM level
?Kernel? Level

Podsumowanie

Kontakt:

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

Pytania?

Kontakt:

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

Dziękuje za uwagę :)

Kontakt:

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