

ReversalCraft

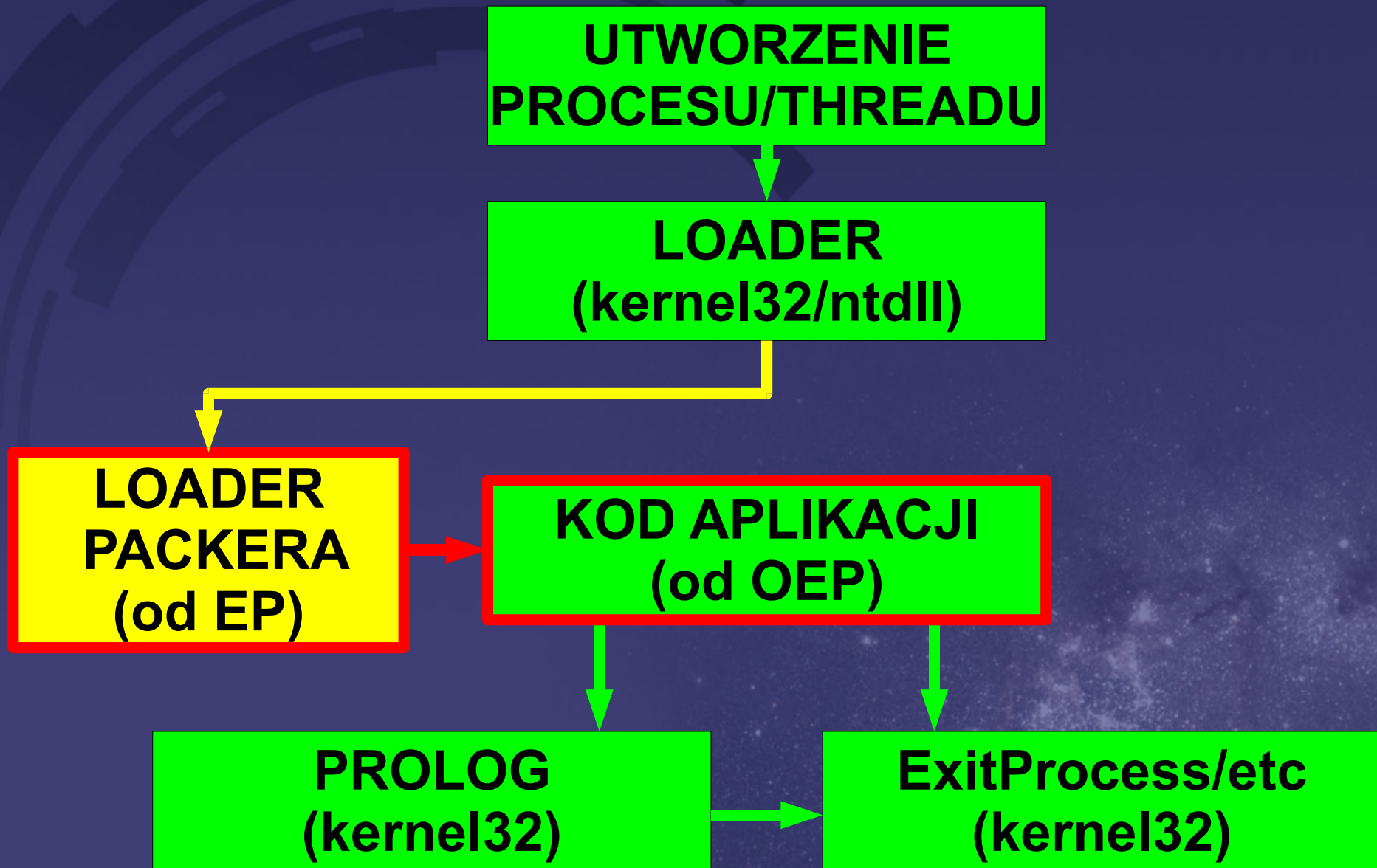
by gynvael.coldwind//vx

006 – OEP i rzuty pamięci

Strony projektu:

<http://re.coldwind.pl/>
<http://www.uw-team.org/>

Przypomnienie packerów/protektorów...



Dwa ważne pytania

Kiedy trzeba znaleźć OEP ?

Jak znaleźć OEP ?

OEP nieistotne – co zrzucić ?

Całą pamięć procesu!

Tylko jeden moduł PE!

Fragment pamięci!

OEP nieistotne – kiedy zrzucić ?

Podczas działania programu
(jeżeli program chodzi w pętli)

Po trafieniu w breakpoint
(BP na API!)

Po zakończeniu procesu

OEP nieistotne – narzędzia do dumpowania:

TraceHook v0.0.2

(cała pamięć, po określonym czasie lub przy zakończeniu działania aplikacji)

TotalDump / HiperDump

(cała pamięć, podczas działania lub wstrzymania aplikacji)

Szukamy OEP #1

Coś co już znamy:
analiza loadera!

Szukamy OEP #2

Memory/hardware breakpoint na stos

Szukamy OEP #3

EIP zmienia sekcję

Szukamy OEP #4

(gritz to Icewall)

**BP na API używane w
prologu kompilatora**

Szukamy OEP #5

(gritz to IceWall)

BP na API wykorzystywane w loaderze packera:

VirtualAlloc

VirtualProtect

VirtualFree



Dziękuję za uwagę :)

Strony projektu:

<http://re.coldwind.pl/>
<http://www.uw-team.org/>