

Kernel Downgrade w X360

Przedmowa...

Podczas bootowania zabezpieczenia X360 sprawdzają zawartość flasha uniemożliwiając prosty downgrade co w następstwie prowadziło by do wykorzystania exploitu w hypervisorze i wyciągnięcia kluczy CPU. Używając infectusa oraz prostych programów możemy ominąć to sprawdzanie i zabootować base kernel.

Downgrade możemy podzielić na dwie części. Pierwsza to przygotowanie obrazu downgradeującego stworzonego z dumpu Twojego flasha oraz z oryginalnych plików systemu 2.0.1888 (do ściągnięcia na #XBINS).

Częścią drugą jest szukanie odpowiedniego hasha dla drugiego bloku ładującego. To pozwoli nam uruchomić BK (base kernel, czyli 1888) a następnie uruchomić linuxa i wyciągnąć z CPU odpowiednie klucze..

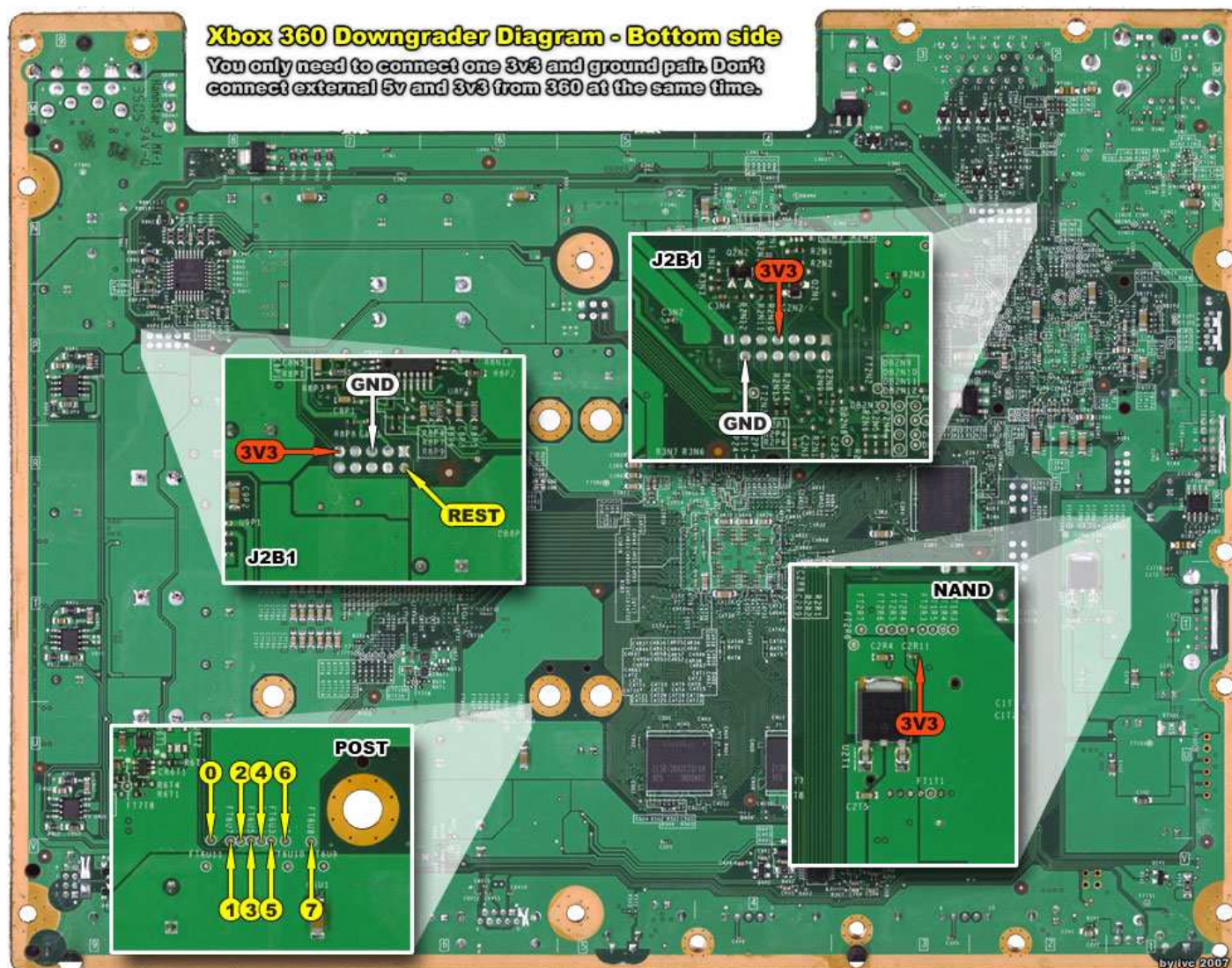
Zanim zaczniesz...

Co będzie Ci potrzebne:

- 1) X360 z Infectusem, Downgrade PCB oraz flasher infectusa w najnowszej wersji.
- 2) Program Degraded
- 3) Narzędzie downgradeujące (iDGTool, infectus.dll i SiUSBXp.dll
- 4) 360 NAND Tool w wersji 0.87
- 5) Oryginalne pliki z dashboarda 1888, znajdujące się w archiwum 1888.FS.rar
- 6) Dump Twojego flasha wykonany za pomocą infectusa.

Wszelkie potrzebne programy możesz znaleźć na stronie infectusa.

Możesz także wylutować rezystor R6T3. Odradzam to jednak początkującym ponieważ rezystor jest mały i trudny do wylutowania. Spalanie się bezpieczników (eFuse) w CPU to nie problem ale jeżeli masz zamiar robić upgrade'y kilka razy dla eksperymentów lub będziesz chciał go wylutować, rób to ostrożnie!

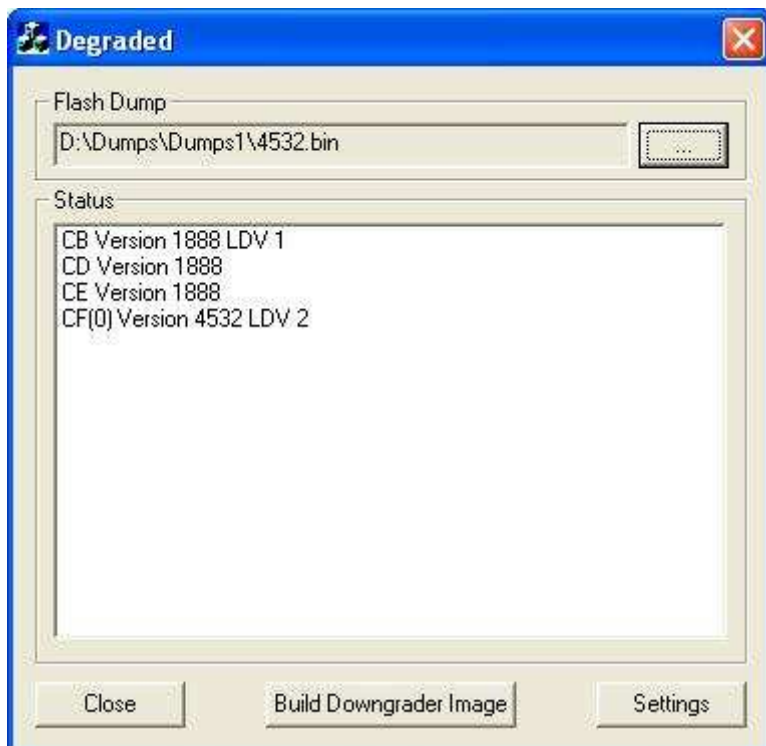


Na schemacie widzimy 3V3 (3.3V). Ten punkt jest używany dla płytki downgradeującej dla infectusa. „Domowe” płytki wymagają 5V które możemy np. wziąć z infectusa.

Chip zainstaluj wg. NAND Flashera. Dolutuj do tego żyłkę z JTAG Reset do punktu Adress 0 na infectusie oraz POST Bus do infectusa (lub dodatkowej płytki) od adresów 10 do 17.

Tworzenie obrazu downgradeującego

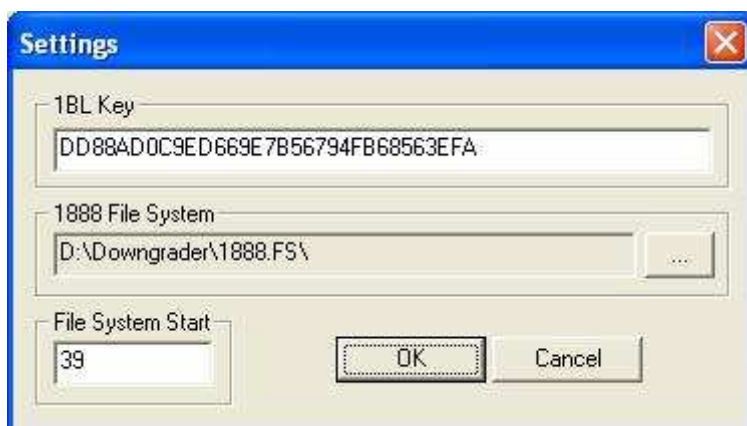
Aby stworzyć odpowiedni obraz uruchom program Degraded:



Wejdź w ustawienia (settings):

Wpisz:

- 1) **1BL Key** - "DD88AD0C9ED669E7B56794FB68563EFA"
- 2) **1888 File System** Folder gdzie rozpakowałeś 1888.FS.rar.
- 3) **File System Start** Powinno być ustawione na 39.



Klik na OK a następnie na "...” aby otworzyć obraz swojego Flasha. Program pokaże nam informacje o Twojej konfiguracji.

Aby stworzyć potrzebny nam plik kliknij na „Build Downgrader Image” i wybierz gdzie zapisać plik.

Niestety czasami proces może zakończyć się niepowodzeniem.

Bardzo rzadko zdarza się, że bajt nie został poprawnie wykryty. W takiej sytuacji program zaczyna szukanie bajtu od nowa, znajduje poprawny i przełącza się na następny.

Jeżeli proces zostanie zatrzymany przez ukończeniem możesz ponowić całość używając dodatkowych komend:

```
Idgtool SS Plik X YY..YY
```

x- liczba znalezionych bajtów
y- odnalezione bajty

Czyli, jeżeli szukanie zakończy się tak:

```
H[8 4F700DF50BB8B8EF22XXXXXXXXXXXXXXXXXX] M 17933 A 17932 D 1 : 0 NEXT
```

Oznacza to, że znalezionych jest 8 bajtów (4F700DF50BB8B8EF) tak więc w komendzie wpisz:

```
idGTool 1 1888.bin 8 4F700DF50BB8B8EF
```

Spowoduje to ponowne sprawdzanie z punktu gdzie się zakończyło

```
Pairing Data 0x38695E 02  
H[16 00000000000000000000000000000000]  
Initial Hash:  
H[8 4F700DF50BB8B8EFXXXXXXXXXXXXXXXXXX]  
Turn on your Xbox, press any key when the RRoD starts
```

Jeżeli bajty będą złe program będzie działał w kółko nie odnajdując następnego bajtu.

W końcu...

Twoja konsola powinna się uruchomić a Ty masz do wyboru język dashboarda itd. Teraz powinieneś zrobić upgrade do wersji Kernela 4532 i wyciągnąć klucze z CPU.

Na samym końcu należy wyczyścić pozostałości po downgrade. 2BL (sekcja CB) zawiera spreparowane wersje LDV. Naprawisz to uruchamiając program NAND Flash dump tool. Możesz to zrobić na dwa sposoby:

- 1) Spachować sekcje LDV sekcji CB na 0
- 2) Dodaj 1 do jednej lub obydwóch sekcji CF

Znane problemy:

Czasami iDGTool przywiesza się gdy zaczyna szukać hasha, a jest to spowodowane stanem w jakim znajduje się Infectus. Wyłącz konsolę, wyciągnij kabel USB z infectusa, wyciągnij kabel zasilający konsoli, włóż go z powrotem, włóż kabel USB i powinno działać.