„Scenowa nomenklatura”

Dla osoby, która dopiero zaczyna przygodę ze sceną PlayStation Vita, ilość tajemniczych pojęć może lekko przytłoczyć. W niniejszym krótkim poradniku, spróbuję przybliżyć najważniejsze.

Generacja I

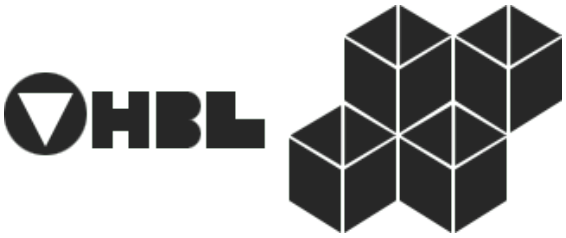
Czyli przeterminowane sposoby na uruchamianie oprogramowania.

EML Hack

Hak polegający na wywołaniu URI z poziomu aplikacji e-mail bądź kalendarza, umożliwia skopiowanie dowolnego pliku m.in. na kartę pamięci. Nigdy nie został do końca załatany i bez wątpienia był to kamień milowy w analizie środowiska.

Rejuvenate

Pierwszy sensowny hak konsoli PlayStation Vita. Niestety wymagał nie tylko licencji, programu PlayStation Mobile Developer Assistant (lub jego brata bliźniaka od Unity Technologies), ale i stałego połączenia z komputerem, przy obowiązkowym cyklicznym zgłaszaniu się do centrali w celu odnowy kluczy. Działa od wersji firmware **1.69** do **3.51** włącznie.



VHBL

Virtual Half-Byte Loader to w zasadzie exploit równoległy, ale wirtualizowanego środowiska PSP, a konkretnie określonych tytułów (różnych, w różnych wersjach i dla różnych wersji fw konsoli). Umożliwia uruchamianie homebrew z PSP (emulatory itp.).

Generacja II

Czyli aktualne sposoby na uruchamianie oprogramowania.

HENkaku i taiHEN

HENkaku jest łańcuchem exploitów, początkowo tylko dla firmware w wersji **3.60**, z „punktem wejścia” przez webkit (czyli de facto przez przeglądarkę internetową). W okolicach R6 została dodana obsługa modułów. Framework ten został ochrzczony taiHEN, więc możemy mówić o taiHENkaku, a nawet zamiennie z HENkaku ponieważ jest jego integralną częścią.

HENkaku umiera wraz z wyłączeniem konsoli i teoretycznie za każdym razem trzeba odwiedzać specjalnie przygotowaną stronę internetową, aby cieszyć się zhakowaną konsolą. Na szczęście szybko powstał **HENkaku Offline Installer**, który utylizuje EML i wystarczy przy każdym włączeniu konsoli uruchomić wbudowaną aplikację e-mail, która wczytuje pliki z karty pamięci lub pamięci wewnętrznej.

Ensō

Wybawienie dla wszystkich posiadaczy konsoli z firmware w wersji **3.60** przynosi dopiero **Ensō Installer**. Poprzez exploitowanie boot loadera (SBL) umożliwia uruchamianie HENkaku przy starcie konsoli bez żadnych dodatkowych czynności ze strony użytkownika. O ile firmware **3.61** i **3.63** załatały stare błędy w silniku przeglądarki, tak aż do **3.65** włącznie możliwe jest zachowanie Ensō (aktualizując fw z już zhakowanego 3.60 za pomocą specjalnego **programu**). Niestety, począwszy od **3.68**, **Ensō** przestał działać, ponieważ luka którą wykorzystywał, została załatana i ten stan rzeczy nie zmienił się aż do dziś.

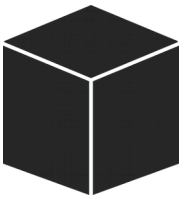
H-Encore i Memcore

Znając sposób generowania **klucza CMA** i szyfrowania PFS, można dostać się do konsoli preparując save'a do konkretnej gry, który exploituje już nie webkit tylko tę właśnie grę - wszystko wgrywane za pomocą **CMA** (są dwie mniej natarczywe alternatywy: QCMA i Open CMA), czyli przez aplikację komunikującą się z konsolą do przygotowywania i wgrywania kopii systemowej.

Na chwilę obecną **H-Encore** działa z grą Bitter Smile (PCSG-90096), wyłącznie na firmware od **3.56** do **3.68** włącznie (a więc póki co nie działa z **3.69** i nowszymi). Zaś **Memcore** który jest jego forkiem, powstał z myślą o starszych firmware (np. 3.60).

Pozostałe zagadnienia

Czyli różne pojęcia, niezwiązane bezpośrednio z exploitami.



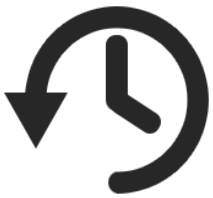
paczki VPK i PKG

Scenowe, czyli nieoficjalne programy dla PlayStation Vita i PlayStation TV instaluje się z plików *.vpk za pomocą managera plików (np. **VitaShell**). VPK to tak naprawdę zwyczajny ZIP i można je przygotować bądź edytować dowolnym archiwizatorem (7-Zip, WinRAR etc.). Manager plików jest instalowany razem z HENkaku lub w przypadku H-Encore, trzeba go sobie dograć do kopii systemowej.

Oficjalne programy (np. gry) są w podpisanych i zaszyfrowanych paczkach *.pkg. Aby takowe zainstalować należy użyć zmodyfikowanej aplikacji z debug kitów (wersji deweloperskich konsoli) lub pobrać programem **pkgj** (ewentualnie ściągnąć na komputerze i przepakować do VPK).

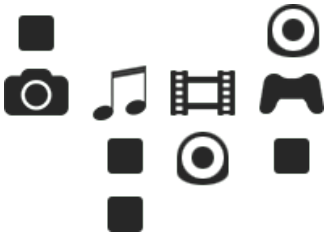
moduły i pluginy

Moduły (lub jak kto woli określenia: pluginy, wtyczki) są to programy ładowane na żądanie np. przy starcie systemu lub konkretnej gry, które działają w tle. Ich natywnymi dla Vita'y formatami są *.skprx i *.suprx, zależnie od przeznaczenia i poziomu uprawnień. Ich użycie definiuje się w pliku "ur0:/tai/config.txt". Po więcej informacji odsyłam do stosownego **poradnika**.



Modoru

Jest to **aplikacja** służąca do downgrade'u, czyli wgrania starszego firmware niż obecnie zainstalowany. A więc można zainstalować np. firmware 3.60, będąc na 3.68. Warunkami są jednak: zhakowana konsola i wersja fw z jaką konsola wyjechała z fabryki – niższa lub równa tej, którą użytkownik chce wgrać (są bowiem PSV, które fw „bazowy" mają 3.68 i na takich nie da się wrzucić nawet 3.65).



Adrenaline

Adrenalina jest to aplikacja wykorzystująca wbudowany wirtualizator konsoli PlayStation Portable (to dzięki niemu możliwa jest emulacja gier z PSX i wirtualizacja gier, a nawet całego CFW PSP). Nie wymaga aktywacji konsoli i wyparła wszystkie stosowane do tej pory rozwiązania (VHBL, ARK CFW etc.).

Drogowskaz

Na koniec garść porad i mała mapa dla potencjalnych podróżników po świecie nieoficjalnego oprogramowania.

- **Jeśli** posiadasz konsolę z fw w wersji **3.69 lub nowszą** to… póki co nie ma żadnego exploitu, który umożliwia uruchamianie niepodpisanego kodu dla Vita'y. Ponoć są już złamane także 3.70, ale żaden sposób nie został jak dotąd opublikowany.

- **Jeśli** posiadasz konsolę z fw w wersji **3.67** lub **3.68** to należy wgrać **H-Encore**, a jeśli zależy ci na uruchamianiu konsoli od razu z „aktywnym hakiem" to potem użyj **Modoru**, aby zejść do fw **3.65** lub **3.60** (o ile rzecz jasna to możliwe) i móc zainstalować **Ensō**.

- **Jeśli** posiadasz konsolę z fw w wersji **3.65** to należy wgrać **H-Encore**, a następnie **Ensō**.

- **Jeśli** posiadasz konsolę z fw w wersji **3.61** lub **3.63** to należy najpierw zaktualizować do **3.65**, by potem wgrać **H-Encore**, a następnie **Ensō**.

- **Jeśli** posiadasz konsolę z fw w wersji **3.60** to należy wgrać **HENkaku**, a następnie **Ensō**.

- **Jeśli** posiadasz konsolę z fw w wersji **3.57** lub starszą to należy najpierw zaktualizować do **3.60**, by potem wgrać **HENkaku**, a następnie **Ensō**.

O ile na PSTV **aktualizacja możliwa jest z USB**, o tyle na PSV trzeba się bawić w proxy i nieoficjalne serwery aby nie skończyć z najnowszym firmware.

PlayStation Vita i PlayStation TV niczym się nie różnią w materii hakowania. Jedynymi dodatkowymi czynnościami na kadłubku są **edycja białych list** (bez czego nie uruchomisz nawet 95% oryginalnych gier) i dodatkowe moduły które oszukują gry, które używają nieobecnych w PSTV i DS3/DS4 **czujników ruchu** i **kamery**.

Najlepszym firmware jest **3.60** ponieważ zadziałają na nim wszystkie moduły. Jednocześnie, jakiegoś wielkiego sensu trzymać się akurat tej wersji nie ma, ponieważ najważniejsze wtyczki działają również na 3.65 i nowszych (**reF00D**, **Storage Manager**, **NoNpDrm**, **NoPsmDrm**, **rePatch reDux0** itd.).

Nie używaj aplikacji, które modyfikują tablicę partycji (zmiana rozmiaru partycji, ich ilości etc.) ponieważ w przyszłości utrudnisz sobie lub nawet uniemożliwisz zastosowanie jakiegoś programu (jak np. Modoru czy też przywracanie fw z poziomu **recovery**).

Emulacja na PSV/PSTV wciąż jest w powijakach i najlepsze emulatory dostępne są na… PSP via Adrenaline. **RetroArch** często bywa problematyczny („wywrotki", problemy z plikiem konfiguracyjnym, niska jakość emulacji platform 16bit i nowszych), a wiele innych emulatorów jest portami jego „rdzeni". Mimo wszystko znajdziesz również porządny **ScummVM** czy nawet **BasiliskII** (emulator Apple II).

Scena tej konsoli dorobiła się też sporej ilości portów gier z PC (i tych oficjalnych gdzie udostępniono kod źródłowy np. Quake'ów i tych homebrew jak np. **chałupnicze Zeldy**).

Najlepszym źródłem oprogramowania na tę konsolę są zasoby **GitHub** (skompilowane oprogramowanie znajdziesz pod linkiem "releases") i **VitaDB**.

Berion
dla CDRinfo.pl @2019-03-06