S ovladačem do jádra!

Martin Dráb
martin.drab@email.cz

Úvod a cíle přednášky

- Od 64bitových verzí Windows Vista je nutné ovladače digitálně podepisovat důvěryhodným certifikátem, aby je operační systém vpustil do jádra
  - Na 32bitových verzích to vyloženě nutné není, ale vyplatí se také.
- Cílem přednášky je prezentovat čtyři různé způsoby, jak ovladač do jádra dostat:
  - cestu historickou,
  - cestu pro vývojáře,
  - cestu legitimní,
  - cestu nelegitimní.

Cesta historická

- Windows XP, Windows Server 2003 SP0
- Digitální podpis důvěryhodným certifikátem není nutný. Pro jisté živly však může být zajímavé dostat svůj kód do jádra i neoficiálními cestami.
- Asi hlavně teoretický model
- Přímý zápis kódu do fyzické paměti
  - Objekct **\Device\PhysicalMemory**
  - Paměťově mapovaný soubor
  - Na novějších verzích Windows přístupný jen z režimu jádra.

Cesta historická II

- Deskriptor zabezpečení objektu \Device\PhysicalMemory dovoluje administrátorům pouze čtení. Je ale možné získat i oprávnění WRITE_DAC.
- Následný postup:
  - najít ve fyzické paměti jádro (či nějaký ovladač)
  - modifikovat jej
  - vyvolat modifikovaný kód.
  - Lepší je najít kus kódu, který se vykonává zřídka, ale lze jej zavolat na požádání (málo využívané systémové volání).

Cesta historická III

- **Problémy**
  - Nevíme, zda kód, který modifikujeme, není právě vykonáván
  - Většina jádra žije ve stránkované paměti, takže může být teoreticky odmapována na disk či přemístěna ve fyzické paměti jinam
    - Příklad se síťovou kartou
  - Dnes už zajímavé asi jen pro pamětníky
  - Bezpečnostní produkty o tom vědí
    - Ale některé špatně hlídaly (DrWeb).
- **Podobné**
  - Útok na stránkovací soubor (page file attack)

Cesta pro vývojáře

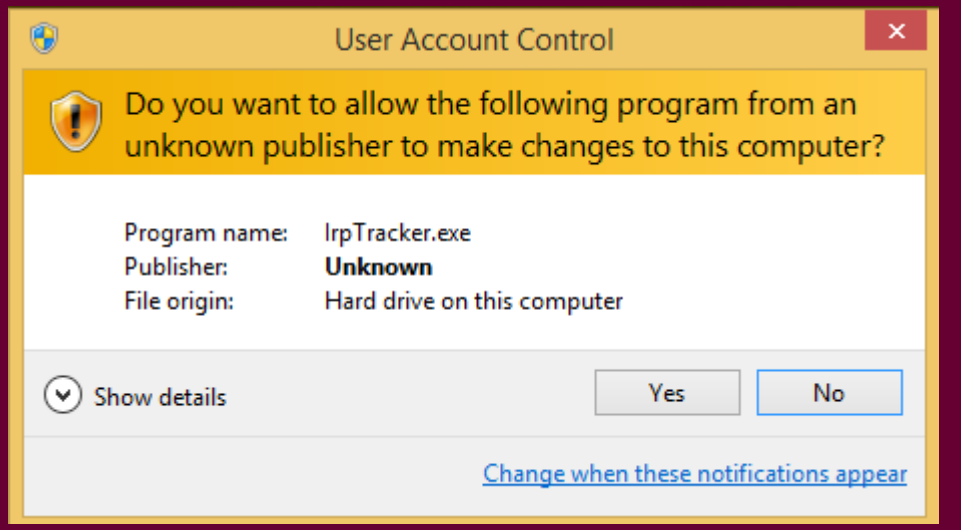
- Kupovat certifikát kvůli hraní si/učení se je moc drahé a zdlouhavé.
- Windows lze nastavit tak, že do jádra pustí ovladače podepsané tzv. Self-signed certifikáty.
  - Bcdedit /set TESTSIGNING ON
  - Certifikát musí být v TRCA (Trusted Root Certificate Authorities)
  - Změna konfigurace vyžaduje restart stroje
  - Úplný zákaz kontroly podpisu ovladačů
    - lze nastavit, ale nedpoporučuje se

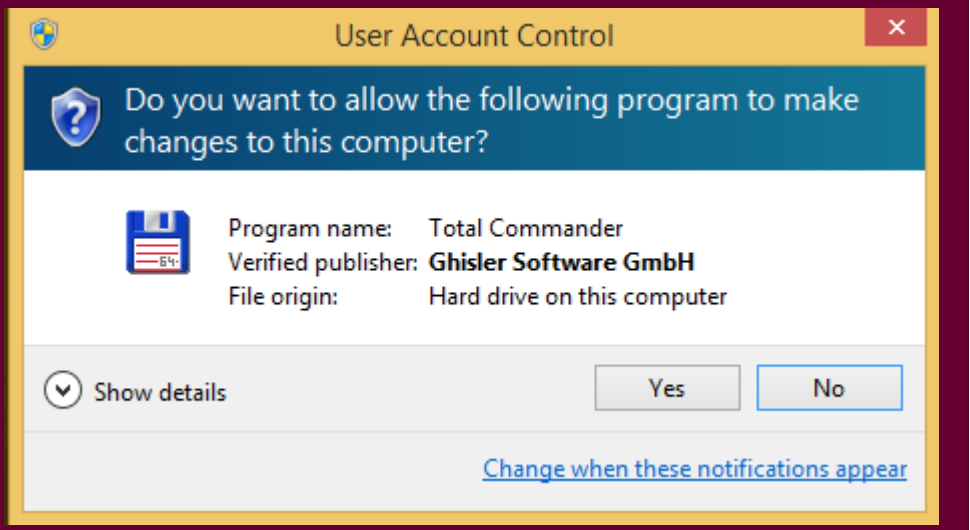
Cesta legitimní

- Pořídit (koupit) certifikát od autority, které Microsoft dovolil vydávat certifikáty pro podepisování ovladačů jádra.
- VeriSign, GlobalSign, …
  - ne všechny vydávají pro obyčejné lidi
- Symantec (přeprodej VeriSignu)
- Založeno převážně na mých zkušenostech (Symantec).

Cesta legitimní II

- Výhody:
  - nemusíte být hacker,
  - lze podepsat i jiné formáty (EXE, DLL...), aplikace se pak jeví důvěryhodně.
- Nevýhody:
  - nejedná se o charitu (pár set dolarů),
  - proces ověření identity je celkem drsný,
  - není to Alza.





Cesta legitimní III

- Žádost o vydání certifikátu
  - Webový formulář
  - Výběr algoritmů
    - RSA, SHA-1, SHA-2
  - Třeba vyplnit spoustu osobních údajů
    - Většina se pak na výsledném certifikátu neobjeví,
    - Slouží zřejmě pro snadnější ověření vaší identity.
  - Po úspěšném odeslání začíná manuální fáze celé objednávky

Ověření identity

- Výměna emailů s příslušnými odděleními VeriSignu a Symantceu
  - Velmi zdvořilí
  - Neoblomní
- Prohlášení o tom, že právě vy žádáte o vydání certifikátu (včetně čísla objednávky)
  - Fotokopie dokladu totožnosti (pas)
  - Vlastnoruční podpis ověřený „notářem“ (Notary Public)
  - Lze pořídit na ambasádě USA (není to charita)
  - Je dobré nepodvádět

Ověřování identity

- Po odevzdání prohlášení (nešifrovaný a nepodepsaný email) je řada na těch druhých.
- Trvá to celkem dlouho (zvláště přes Vánoce).
- Ověřují i, zda osoba, která ověřila váš podpis, k tomu měla oprávnění.

Závěrečná fáze

- Ověřovací telefonát
  - Na vše stačí odpovědět ANO
- Po jeho úspěšném absolvování se stanou dvě věci:
  - zmizí pár set dolarů,
  - do pár hodin přijde certifikát emailem, popř. link, kde si jej lze vyzvednout (automaticky se nainstaluje).

Podivnosti

- Komunikace probíhá na dvou frontách:
  - s živými lidmi,
  - s robotem kontrolujícím, zda jsou včas splněny náležitosti.
  - Probíhá v podstatě nezávisle na sobě.
- Je třeba rozlišovat, zda komunikujete se Symantecem či VeriSignem:
  - vaše objednávka nemá v obou systémech stejné číslo
  - každý váš email obvykle vyřizuje někdo jiný,
  - při uvedení špatného čísla objednávky dochází ke zmatku
- Pozor na SHA-2.
- Cross-signing.

Cesta nelegitimní

- Používáno autory malware
- V zásadě ale „nemožnost“ získat certifikát nevadí, protože:
  - ovladače jiných výrobců podepsány jsou,
  - programátoři ovladačů se při ošetřování vstupů mohou dopustit chyby,
  - příslušný certifikát lze ukrást.
- **Příklad:** DriveCrypt, VirtualBox

Problém

- Aplikace při komunikaci s ovladačem předává vstupní data v bufferu.
- Vstup může obsahovat odkazy (adresy) na další buffery v prostoru aplikace
- Ovladač musí v rámci přijetí požadavku:
  - ověřit, že vstupní buffer (a případné další buffery) nachází v prostoru, kam má aplikace přístup,
  - postupně kopírovat vstupní data tam, kam aplikace nemůže (aby je nemohla měnit ovladači „pod rukama“).

Zneužití

- Najít ovladač, který špatně ověřuje platnost vstupů
- Přibalit jej ke svému dílu
- Nainstalovat jej do systému a zneužít zranitelnost.
- **Příklad:** VirtualBox 1.6.2, ovaldač VboxDrv.sys dovoluje zapsat na libovolnou adresu.
- Zápis do proměnné určující, zda se mají při načtení ovladače do jádra kontrolovat digitální podpisy:
  - Ntoskrnl.exe!g_CiEnabled (Windows Vista/7)
  - Ci.dll!Cig_CiOptions (Windows 8 a novější), chráněno pomocí KPP (Patchguard)
- Po načtení svého (škodlivého) ovladače je možné digitální podpisy opět vynucovat.

Užitečnost certifikátu

- Podepsání ovladačů k Apple USB Ethernet Adapter
- Tvorba vlastních ovladačů a utilit (opensource):
  - VrtuleTree
  - IRPMon
- Možnost podepsat ovladač někomu jinému
  - nekomerční/opensource použití,
  - chci vidět zdrojový kód,
  - přístup je individuální.

Zdroje

- **Practical Windows Code and Driver Signing**
  - http://www.davidegrayson.com/signing/
- **KMCS Walkthrough**
  - http://msdn.microsoft.com/en-us/library/windows/hardware/dn653569(v=vs.85).aspx
- **Digital Signatures for Kernel Modules on Windows**
  - http://msdn.microsoft.com/en-us/library/windows/hardware/dn653559(v=vs.85).aspx
- **Dsefix**
  - http://www.kernelmode.info/forum/viewtopic.php?f=11&t=3322&hilit=dsefix

Závěr

- **Martin Dráb**
- **Email:** martin.drab@email.cz
- WWW: http://www.jadro-windows.cz