Fakulta elektrotechniky a informatiky
Vysoká škola báňská - Technická univerzita Ostrava

Cvičení 7

POČÍTAČOVÁ OBRANA A ÚTOK - POU

Drive-by download

- Nevyžádané stahování obsahu z internetu
  - Stažení takového obsahu, který uživatel schválil, aniž by věděl (nebo porozuměl) co vše bude staženo
  - Stažení obsahu z internetu bez vědomí uživatele (při návštěvě webové stránky)
  - Škodlivý kód ukryt na webové stránce nebo v HTML emailu

Drive-by install

- podobná událost týkající se spíše instalace sw než stažení obsahu
- termíny často zaměňované

Drive-by download

- Škodlivý kód na webové stránce
  - vložen přímo na stránku
  - doručen např. reklamním systémem či jiným obsahem 3. stran
  - obvykle zjišťuje typ OS, verze OS, prohlížeče včetně doplňků, verze Javy, Flashe, …
  - stažení exploitu zneužívajícího zranitelnosti detekované verze a doručení škodlivého kódu na zařízení oběti útoku

Drive-by download - průběh

- 1. Fáze – Vstupní bod (entry point)
  - návštěva nakažené webové stránky
- 2. Fáze – Distribuce (distribution)
  - přesměrování na stránku ovládanou hackery
  - malware balen do „exploit kitů“, které mohou využít slabiny v instalovaných SW tisíci různými způsoby
- 3. Fáze – Využití (Exploit)
  - na přesměrované webové stránce proběhne zjištění OS, SW, prohlížeče, video přehrávače, … pro nalezení bezpečnostní díry

Drive-by download - průběh

- 4. Fáze – Infekce (infection)
  - infekce proběhne jakmile je nalezeno a zneužito nalezené slabé místo
- 5. Fáze – Vykonávání (Execution)
  - Malware vykonává svoji činnost

- Např.:
  - Malware Zbot je stvořen k přístupu k emailům nebo bakovním účtům
  - Ransomware je typ malweru, který zabraňuje přístupu k souborům (např. do doby, než za osvobození souborů proběhne výkupné)

Drive-by download - Obrana

- aktualizace(všechny bezpečnostní záplaty)
  - útoky zneužívající zranitelnosti nultého dne (Zero-day attack) bývají obvykle využívány k cíleným útokům, které lze daleko lépe zpeněžit
- antivirus
  - lze zachytit většinu ze známých hrozeb
- sandbox
  - izolace prohlížeče od zbytku zařízení
- zákaz JavaScriptu
  - škodlivý kód však může být umístěn v Javě nebo Flashi

Drive-by download - Obrana

- omezená práva prohlížeče
  - zabrání tak cca 50% útoků
- Linux
  - na OS Windows je vedeno nejvíce útoků
- Důvěryhodné weby
  - používání důvěryhodných webů snižuje riziko nákazy
- AppLocker
  - pro výběr spustitelných programů

Drive-by download - Příklad

- okolo 50 milionů uživatelů postiženo Drive-by download útokem
- weby zobrazující reklamu společnosti revive-adserver
- např. i web pražského letiště byl vystaven nebezpečí
- zneužita byla zranitelnost Adobe Flash Playeru
- do PC byl stažen trojský kůň
- měnil PC v zombie

Windows Script Host (WSH)

- určen pro vytváření skriptů ve Windows
- poprvé ve Windows 95
- plnohodnotné skriptovací prostředí
  - VBScript
    - používá „WScript“ objekty
    - přípona .vbs
  - JScript
    - přípona .js
    - JavaScript od firmy Microsoft (ECMAScript)
  - WSF (Windows Script File)
    - soubor kombinující VBScript a JScript

Drive-by download - protokol

Počítačová obrana a útok
Protokol z předmětu

Tématická oblast: Drive-by download

Přednášející: prof. Ing. Ivan Zelinka, Ph.D., Ing. Jan Plucar
Cvičící: Ing. Jiří Znoj

Jméno a číslo studenta:
Datum vypracování:

Zadání:

1) Seznamte se s útokem typu drive-by download, konkrétně s jeho JavaScript verzí.
2) Seznamte se s Windows komponentou Windows Script Host (WSH).
3) Naprogramujte spustitelnou(exe) aplikaci, která provede jednoduchou, ale škodlivou akci.
4) V JavaScriptu vytvořte skript, který po spuštění stáhne Vaši exe aplikaci a přímo ji spustí.
5) Odzkoušejte a vypracujte závěr protokolu.

Postup řešení:

1) **Seznamte se s WSH, především se podívejte na možnosti vzdálené komunikace a přístupu k shellu z JavaScriptu.**
2) **Vytvořte spustitelnou „exe" aplikaci, která provede Vámi zvolenou škodlivou akci. Aplikace nezobrazí žádné okno, ani jiným způsobem uživatele viditelně neupozorní.**
3) **Vytvořenou aplikaci zkopírujte na webový server, který je součástí dodaného VirtualBox testovacího prostředí.**
4) **Vytvořte JavaScriptový kód, který po spuštění stáhne Vámi vytvořenou (škodlivou) aplikaci a tuto aplikaci spustí. Skript uložte do souboru s koncovkou „.js" na disk testovacího prostředí.**
5) **Spusťte skript, ověřte a zhodnoťte útok. Poznatky doplňte do závěru a odpovězte na otázky v závěru.**
(Ve virtuálním prostředí je nainstalováno Visual Studio. Proto je pravděpodobné, že se systém Windows zeptá, přes jaký software JavaScript soubor otevřít . Zvolte „Microsoft Windows Based Script Host" - tato volba je v systému výchozí.)

Nápověda:

- Tento kód můžete uložit do JS souboru a otestovat jeho spuštění:
WScript.CreateObject("WScript.Shell").Run("calc.exe", 0, false);

- Užitečné funkce rozšiřující možnosti JS na systémech Windows:
WScript.CreateObject(WScript.Shell)
WScript.CreateObject(MSXML2.XMLHTTP)
WScript.CreateObject(ADODB.Stream)
GetSpecialFolder(...)

Závěr:

- **Při odevzdávání přiložte Vaše zdrojové kódy JS skriptu a škodlivé aplikace (neposílejte binární soubory, jen zdrojový kód!).**

- **Do protokolu vložte alespoň 2 screenshoty vaší práce.**
- **Odpovězte na následující otázky:**
  - **V čem spočívá nebezpečí plynoucí z provedeného útoku?**
  - **Tento útok můžeme považovat za následníka macro útoků pro Office soubory. Porovnejte tento útok s macro viry a popište rozdíly. V čem je tento útok pro uživatele záludnější?**
  - **Vyzkoušejte spustit vytvořený JS skript v prohlížeči a to jak lokálně, tak vzdáleně. Co jste zjistili?**
  - **Popište možnosti obrany.**

Dále můžete zahrnout vlastní poznatky.