Počítačové viry a bezpečnost počítačových systémů
Protokol z předmětu (2b)

Tématická oblast: Analýza malware – statická analýza

Přednášející: prof. Ing. Ivan Zelinka, Ph.D.; Ing. Jan Plucar

Jméno a číslo studenta: Daniel Trnka, TRN0038
Datum vypracování: 19. 4. 2019

Zadání:

1) Seznamte se s technikami užívanými k ověřování itegrity souborů.
   Vytvořte hashe MD5, SHA1 a SHA256 pomocí Vámi zvoleného offline nástroje.
   Zde vložte screenshoty Vašeho nástroje:

```
C:\Users\User\Desktop\pvbps-cv06>certutil -hashfile Sample4 MD5
MD5 hash of Sample4:
e5b84f2ef76fb9a52acc743110839924
CertUtil: -hashfile command completed successfully.

C:\Users\User\Desktop\pvbps-cv06>certutil -hashfile Sample4 SHA1
SHA1 hash of Sample4:
b00dc958347b43cb06a8ec35fb0d6bfa790c7c5c
CertUtil: -hashfile command completed successfully.

C:\Users\User\Desktop\pvbps-cv06>certutil -hashfile Sample4 SHA256
SHA256 hash of Sample4:
affc45da0602ebd4b7685b9be635d64e06b81bb64ee3470a88a186a7525db382
CertUtil: -hashfile command completed successfully.
```

2) Seznamte se s nástroji pro extrakci řetězců (stringů) z exe souborů:
   Strings: https://technet.microsoft.com/en-us/sysinternals/strings.aspx
   BinText: https://softfamous.com/bintext/
   Jeden z nástrojů si zvolte, proveďte extrakci řetězců z vašeho vzorku a nalezněte veškeré obsažené webové URL.
   URL adresy zkopírujte zde:
   Sample1:
   http://vguarder.91i.net/SETUPX.EXE

   Sample2:
   http://www.smartassembly.c

   Sample3:
   http://avrill.ucoz.ru, v UTF-16

   Sample4:
   nic nenalezeno

   Sample5:
   http://schemas.microsoft.com/SMI/2005/WindowsSettings (xml namespace)
   http://leimer.name/

3) Seznamte se s on-line službou https://www.virustotal.com/. Přes službu analyzujte Váš malware.
Pro tento úkol byl vybrán vzorek 5, protože obsahoval na VirusTotal i informaci o chování programu v sandboxu.

a. Zjistěte alespoň 3 názvy, pod kterými je Váš malware identifikován.
Vypište:
HackTool:Win32/KMSAuto.f35123f2
a variant of Win32/HackKMS.A
Hacktool.Keygen
HackTool:Win64/Keygen
Hack.Tool/Gen-Crack
W32/Keygen.DX!tr
jinak převážně generický trojan

Dle detekce a komentářů se může jednat o keygen či aktivátor systému Windows 7 Enterprise.

b. Zkopírujte další získané informace, které považujete za zajímavé pro analýzu malware:
Malware byl zkompilován v 2009-08-16. Vzorek využívá funkci LoadLibrary, takže může v době běhu načítat další knihovny za běhu. Dále pravděpodobně volá funkci CreateFileW, DeleteFileA/W a spouští aplikaci pomocí ShellExecuteExA z knihovny SHELL32.dll. Dále využívá funkci ShowWindow, takže může například skrýt grafické okno.

Je cílen pro 64bitovou architekturu. Jedná se nejspíše o grafickou aplikaci, která obsahuje několik zdrojů (resources) včetně ikonky, které jsou lokalizované pro anglický jazyk.

Vzorek je zabalen pomocí packeru nazvaného jako rar. Jedná se o samorozbalovací archiv, který obsahuje soubory, které byly následně analyzovány ručně:
bie_kms.exe
start.bat
Tento skript spouští Windows skript slmgr.vb pro správu Windows licence a nastavuje aktivační klíč pro Windows 7 Enterprise. Následně spouští proces bie_kms.exe, který pravděpodobně slouží jako Key Management Service (KMS) pro ověření licence. Následně je znovu spuštěn skript slmgr.vb, kterému se předá adresa serveru KMS 127.0.0.1. Následně se kontroluje úspěch aktivace pomocí obsahu souboru %systemroot%\check.txt. Poté je proces bie_kms.exe zabit a všechny soubory včetně check.txt jsou smazány.

Analýza souboru **bie_kms.exe** na virustotal.com:
Soubor je zabalen pomoci packeru:
PEiDPECompact 2.xx --> BitSum Technologies
Program je zkompilován pro 32bitovou architekturu.
Využívá funkce:
VirtualFree
LoadLibraryA
VirtualAlloc
GetProcAddress
Tato kombinace je podezřelá, protože v době běhu může pomocí LoadLibrary načítat další dynamické knihovny za běhu. Dále je například možné pomocí

funkce VirtualAlloc alokovat paměť s oprávněním pro spouštění, takže je tak možné dynamicky vytvořit (rozbalit) instrukce také za běhu programu. Pravděpodobně jsou zde tyto funkce kvůli použitému packeru.
Z dynamické analýzy na VirusTotal lze například vidět, že jsou v době běhu nahrány tyto knihovny:
kernel32
user32
rpcrt4.dll
mswsock.dll
ws2_32.dll
WS2HELP.dll
hnetcfg.dll
C:\WINDOWS\System32\wshtcpip.dll
WS2_32.dll
Seznam nemusí však být kompletní, pokud malware v době běhu detekoval, že běží v sandboxu, nebo příliš krátkou dobu. Dále byly otevřené další DLL soubory, které mohly být do procesu namapované manuálně bez využití funkce LoadLibrary.

Sice se jedná o protokol statické analýzy, ale VirusTotal poskytuje i zajímavý výsledek pro dynamickou analýzu, kdy se zaznamenávalo chování aplikace Sample5 v sandboxu.
Vzorek komunikoval s nějakou lokální aplikací po TCP portu 49163, což nejspíš souvisí s Key Management Service a procesem **bie_kms.exe**.

Vzorek zapsal do těchto souborů (nejspíše byly vytvořeny při rozbalení samorozbalovacího archivu):
%TEMP%\rarsfx0\bie_kms.exe
%TEMP%\rarsfx0\start.bat
%WINDIR%\check.txt – soubor byl vytvořen skriptem slmgr.vb a obsahuje výsledek potvrzení licence windows

Vytvořený soubor bie_kms.exe byl také následně spuštěn.
Společně se souborem start.bat byly na konci smazány.

Byly také spuštěny služby:
SPPSvc
sppuinotify

Z registru byly například odstraněny adresy DNS serverů.
<HKLM>\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{6a52be73-ec8e-4f63-a268-7517a50dcb38}\DhcpNameServer

Závěr:

Statická analýza je vhodná pro prvotní analýzu malware. Lze například zjistit používané funkce nebo řetězce či data programu. Malware ale ve většině případu ukládá např. URL adresu v obfuskované podobě, aby právě předešel takové jednoduché statické analýze pomocí programu string. Pouhá inkrementace každého znaku URL adresy způsobí, že nepůjde na první pohled najít. Například ve vzorku 3 nebyla pomocí string nalezena žádná URL adresa, protože je soubor vytvořen pomocí packeru AutoIt. Ve vzorku 1 byla nalezena přímo URL adresa pravděpodobně dalšího malware, který se stáhne do počítače oběti. Doména nemá v současné době žádný záznam v DNS.
Vzorek 5 byl nejzajímavější a byl proto vybrán pro druhý úkol. Malware byl některými antiviry detekován jako keygen. V komentářích se objevilo, že se jedná o aktivátor pro systém Windows 7 Enterprise. Vzorek byl samorozbalovací rar archiv obsahující bat skript a spustitelný soubor. Skript spouštěl soubor, který pravděpodobně plnil funkci pro ověření Windows licence. Skript následně provedl aktivaci licence vůči tomuto serveru. Zajímavosti je, že spustitelný proces byl také zabalen pomocí jiného packeru. Z tohoto důvodu pravděpodobně obsahoval pouze funkce pro nahrání dynamické knihovny za běhu, nebo pro alokaci paměti, která navíc umožňuje nastavit i příznak povolující vykonávání kódu.