Analýza škodlivého kódu a objavovanie zraniteľností

Ladislav Bačo

Computer Security Incident Response Team Slovakia

22. marec 2017

Škodlivý kód

- stotisíce nových vzoriek denne $\rightarrow$ automatizácia detekcie
- problém s neznámymi, ale aj s časťou známych vzoriek

Metódy analýzy malware

- Stroj, program: antivírus, sandbox
- Človek: analytik

Metódy analýzy malware

- Stroj, program: antivírus, sandbox
- Človek: analytik

- Základná statická analýza
- Behaviorálna analýza
- Dynamická analýza
- Pokročilá statická analýza – reverzné inžinierstvo

Identifikácia zraniteľnosti CVE-2016-4116

- príprava tréningovej úlohy
- staršia vzorka, dostatočne známa? (detekcia VirusTotal 49/57)

Identifikácia zraniteľnosti CVE-2016-4116

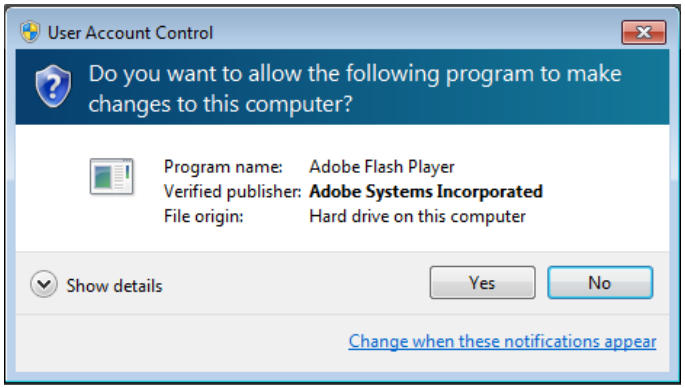
- príprava tréningovej úlohy
- staršia vzorka, dostatočne známa? (detekcia VirusTotal 49/57)

- rýchle overenie vzorky: behaviorálna analýza
- *(ukážka)*

Identifikácia zraniteľnosti CVE-2016-4116

- príprava tréningovej úlohy
- staršia vzorka, dostatočne známa? (detekcia VirusTotal 49/57)

- rýchle overenie vzorky: behaviorálna analýza
- *(ukážka)*
- podpísaný malvér?

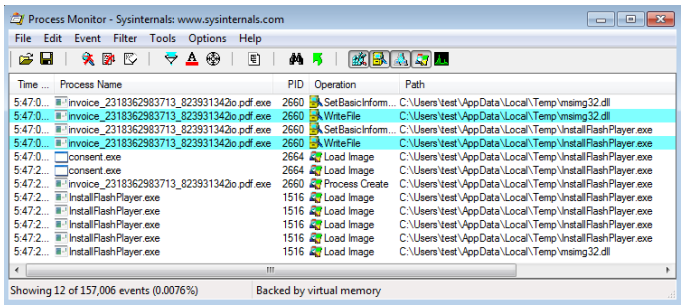


Identifikácia zraniteľnosti CVE-2016-4116

- čo sa stalo? $\rightarrow$ Process Monitor (procmon)

Identifikácia zraniteľnosti CVE-2016-4116

- čo sa stalo? → Process Monitor (procmon)



Time ...	Process Name	PID	Operation	Path
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	SetBasicInform...	C:\Users\test\AppData\Local\Temp\msimg32.dll
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	WriteFile	C:\Users\test\AppData\Local\Temp\msimg32.dll
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	SetBasicInform...	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	WriteFile	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:0...	consent.exe	2664	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	consent.exe	2664	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	invoice_2318362983713_823931342io.pdf.exe	2660	Process Create	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\msimg32.dll

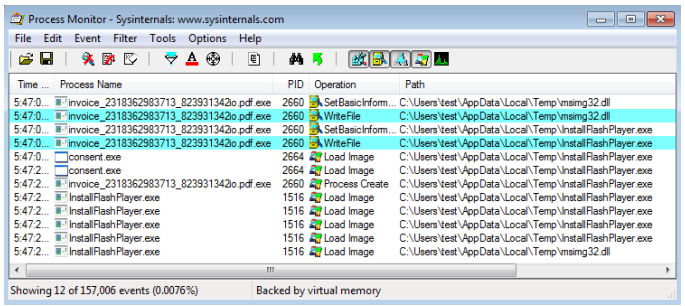
Showing 12 of 157,006 events (0.0076%)

Backed by virtual memory

- podozrivá knižnica `msimg32.dll`
- štandardné poradie vyhľadávania knižníc
- DLL hijacking

Identifikácia zraniteľnosti CVE-2016-4116

- čo sa stalo? → Process Monitor (procmon)



Time ...	Process Name	PID	Operation	Path
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	SetBasicInform...	C:\Users\test\AppData\Local\Temp\msimg32.dll
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	WriteFile	C:\Users\test\AppData\Local\Temp\msimg32.dll
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	SetBasicInform...	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:0...	invoice_2318362983713_823931342io.pdf.exe	2660	WriteFile	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:0...	consent.exe	2664	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	consent.exe	2664	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	invoice_2318362983713_823931342io.pdf.exe	2660	Process Create	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\InstallFlashPlayer.exe
5:47:2...	InstallFlashPlayer.exe	1516	Load Image	C:\Users\test\AppData\Local\Temp\msimg32.dll

Showing 12 of 157,006 events (0.0076%) Backed by virtual memory

- podozrivá knižnica `msimg32.dll`
- štandardné poradie vyhľadávania knižníc
- DLL hijacking
- stará vzorka exploituje zraniteľnosť Adobe Flash Player

CVE-2016-4116 = tisícdňový chrobák

- vzorka stará 876 dní
- zraniteľnosť stará 1670 dní
- neopravená $\rightarrow$ nahlásenie zraniteľnosti

CVE-2016-4116 = tisícdňový chrobák

- vzorka stará 876 dní
- zraniteľnosť stará 1670 dní
- neopravená $\rightarrow$ nahlásenie zraniteľnosti
- ZDI, Adobe PSIRT

CVE-2016-4116 = tisícdňový chrobák

- vzorka stará 876 dní
- zraniteľnosť stará 1670 dní
- neopravená $\rightarrow$ nahlásenie zraniteľnosti
- ZDI, Adobe PSIRT
- pridelený identifikátor CVE-2016-4116

Ďalší výskum

- automatizované testovanie DLL hijacking
- identifikovaná zraniteľnosť Adobe Reader
- nahlásenie zraniteľnosti $\rightarrow$ CVE-2016-1090

Ďalšie pokračovanie

- pri vývoji softvéru identifikované ďalšie zraniteľnosti
- inštalátor Google Chrome
- Microsoft Windows 7, knižnica ws2_32.dll
- *(ukážka)*

Možnosti zneužitia

- stiahnutie a spustenie zraniteľného softvéru
- inštalácia programov
- perzistencia, skrývanie sa v systéme (CIA)

Možnosti obrany

- premazávanie Downloads, %TEMP%
- kontrola podpisov
- spúšťanie dôveryhodných programov
- *(varovanie na stránke www.csirt.gov.sk)*

Otázky, diskusia.

Kontakt

Ladislav Bačo
Oddelenie NIKI

CSIRT.SK
WWW.CSIRT.GOV.SK

ladislav.baco@csirt.sk