Malware analysis and vulnerability discovering; CVE-2016-4116 DLL hijacking in Flash Player

Ladislav Bačo

Computer Security Incident Response Team Slovakia

TLP: Green

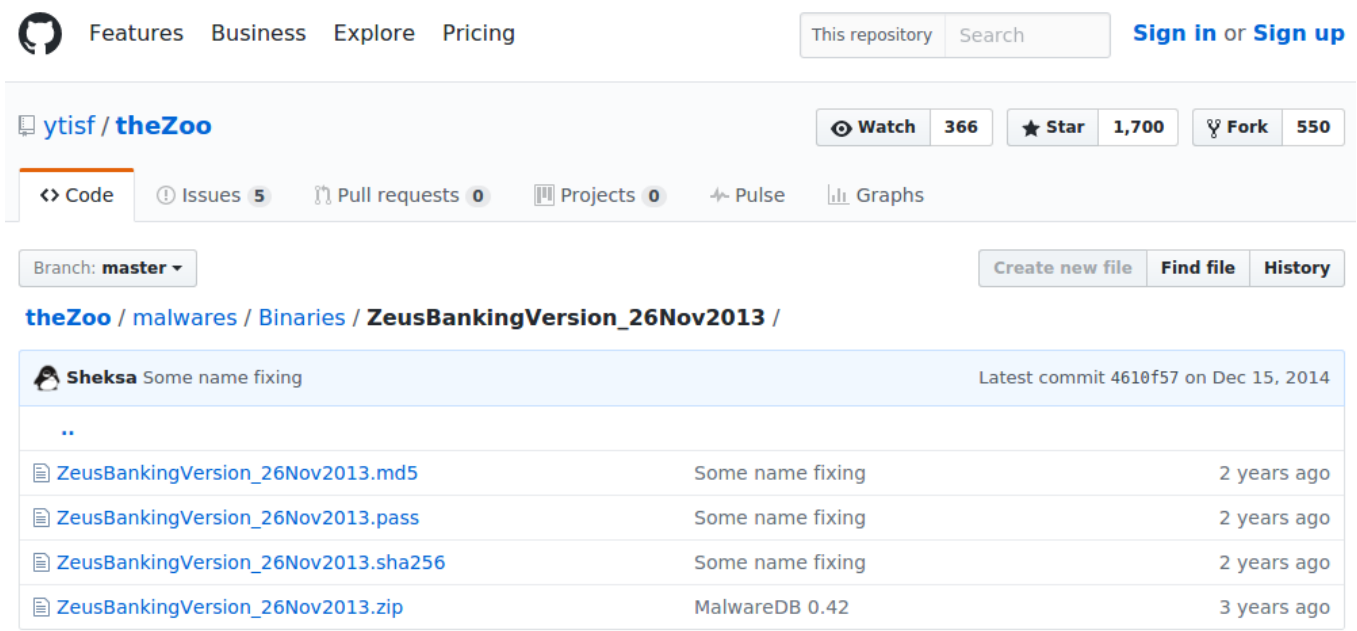
May 15, 2017

Agenda

- Story from one exercise
- DLL hijacking vulnerabilities
- CVE-2016-4116 Adobe Flash Player
- CVE-2016-1090 Adobe Reader
- 0-day vulnerabilities in Microsoft Windows and Google Chrome
- Is UAC trusted for common user?

Story from one exercise

- Preparation of forensics analysis task for one cyber exercise in SK
- Chosen old sample, well-known? Zeus trojan (VT 49/57)

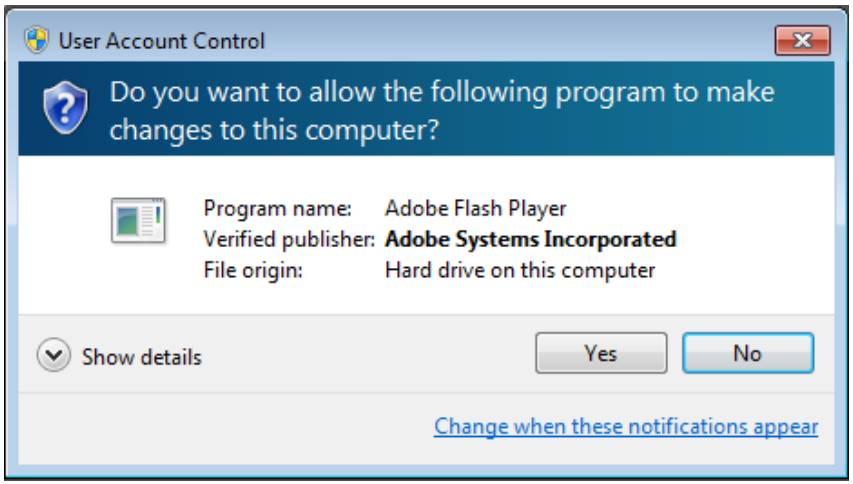


Story from one exercise

- Quick check of chosen sample: behavioral analysis
- *(demo)*

Story from one exercise

- Quick check of chosen sample: behavioral analysis
- *(demo)*
- signed malware

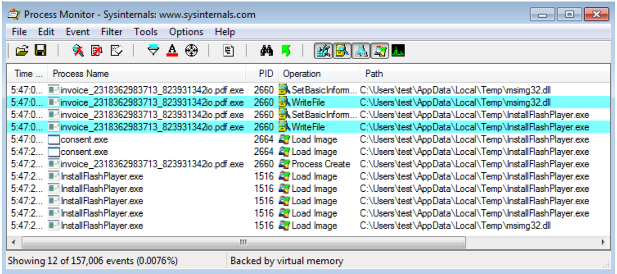


DLL hijacking vulnerability

- What happened? $\rightarrow$ Process Monitor (procmon)

DLL hijacking vulnerability

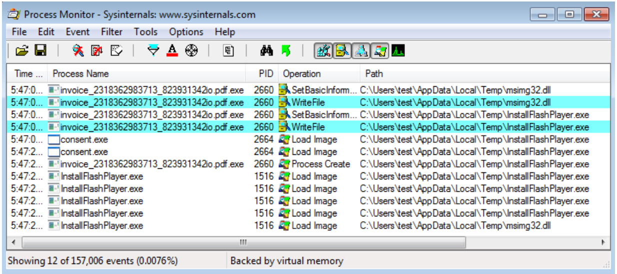
- What happened? → Process Monitor (procmon)



- Suspicious library `msimg32.dll`
- Dynamic-link library search order
- DLL hijacking

DLL hijacking vulnerability

- What happened? → Process Monitor (procmon)



- Suspicious library `msimg32.dll`
- Dynamic-link library search order
- DLL hijacking
- the old sample has exploited the vulnerability in Adobe Flash Player

CVE-2016-4116 = "1000-day old bug"

- Sample age: 876 days
- Vulnerability in Adobe Flash Player: 1670 days
- Still present in newer versions $\rightarrow$ report and responsible disclosure

CVE-2016-4116 = "1000-day old bug"

- Sample age: 876 days
- Vulnerability in Adobe Flash Player: 1670 days
- Still present in newer versions → report and responsible disclosure
- ZDI, Adobe PSIRT

CVE-2016-4116 = "1000-day old bug"

- Sample age: 876 days
- Vulnerability in Adobe Flash Player: 1670 days
- Still present in newer versions → report and responsible disclosure
- ZDI, Adobe PSIRT
- CVE-2016-4116

Further research

- automated testing of DLL hijacking vulnerabilities in installers
- identified another vulnerability in Adobe Reader
- report to Adobe PSIRT $\rightarrow$ CVE-2016-1090

Story continues. . .

- during software development we identified another two vulnerabilities
- Google Chrome installer
- Microsoft Windows 7, library ws2_32.dll loads library given in registry `HKLM\SYSTEM\CurrentControlSet\services\WinSock2\Parameters`
  - `rasadhlp.dll` in Windows 7
  - `C:\Windows\System32\rasadhlp.dll` in Windows 8.1, 10
- *(demo)*

Story continues. . .

- during software development we identified another two vulnerabilities
- Google Chrome installer
- Microsoft Windows 7, library ws2_32.dll loads library given in registry `HKLM\SYSTEM\CurrentControlSet\services\WinSock2\Parameters`
  - `rasadhlp.dll` in Windows 7
  - `C:\Windows\System32\rasadhlp.dll` in Windows 8.1, 10
- *(demo)*
- report to Google on Feb 04, 2017
  - "We don't consider physically local attacks to be in Chrome's threat model"

Story continues. . .

- during software development we identified another two vulnerabilities
- Google Chrome installer
- Microsoft Windows 7, library ws2_32.dll loads library given in registry `HKLM\SYSTEM\CurrentControlSet\services\WinSock2\Parameters`
  - `rasadhlp.dll` in Windows 7
  - `C:\Windows\System32\rasadhlp.dll` in Windows 8.1, 10
- *(demo)*
- report to Google on Feb 04, 2017
  - "We don't consider physically local attacks to be in Chrome's threat model"
- report to Microsoft on Feb 03, 2017
  - "loading binaries from the application directory is by design. . . . does not meet the bar for security servicing."

Abusing the DLL hijacking vulnerabilities

- After downloading and executing vulnerable programs
- Installation of programs: executing malicious code with admin privileges
- "bypass" the UAC and legitimize the malicious code using trusted signature
  - as in PoCs
  - programatically simulate "Run as admin" via `HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers`
- Persistance, hiding malicious activities in the system (Vault7)

Protection and prevention

- Periodically cleaning the Downloads dir, %TEMP%
- Verifying the signatures
- Executing only trusted software
- *0-days: warning at website www.csirt.gov.sk*

Questions, discussion.

Kontakt

Ladislav Bačo
Head of the NIKI department

ladislav.baco@csirt.sk