

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

- 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)

The screenshot shows the GitHub interface for the repository 'ytisf/theZoo'. At the top, there are navigation links for 'Features', 'Business', 'Explore', and 'Pricing', along with a search bar and 'Sign in' or 'Sign up' buttons. Below this, the repository name 'ytisf / theZoo' is displayed, along with statistics: 366 Watchers, 1,700 Stars, and 550 Forks. Navigation tabs include 'Code', 'Issues' (5), 'Pull requests' (0), 'Projects' (0), 'Pulse', and 'Graphs'. A 'Branch: master' dropdown is visible, along with buttons for 'Create new file', 'Find file', and 'History'. The file list shows the path 'theZoo / malwares / Binaries / ZeusBankingVersion_26Nov2013 /'. The commit history table is as follows:

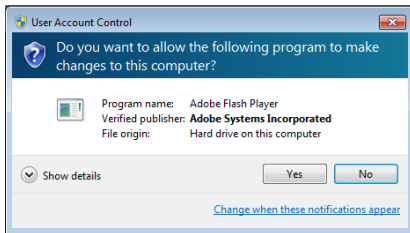
Commit	Author	Message	Time
..	Sheksa	Some name fixing	Latest commit 4610f57 on Dec 15, 2014
ZeusBankingVersion_26Nov2013.md5	Sheksa	Some name fixing	2 years ago
ZeusBankingVersion_26Nov2013.pass	Sheksa	Some name fixing	2 years ago
ZeusBankingVersion_26Nov2013.sha256	Sheksa	Some name fixing	2 years ago
ZeusBankingVersion_26Nov2013.zip	MalwareDB	0.42	3 years ago

Story from one exercise

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

Story from one exercise

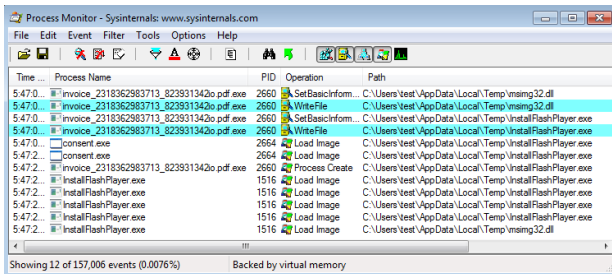
- Quick check of chosen sample: behavioral analysis
- (*demo*)
- signed malware



- What happened? → Process Monitor (procmon)

DLL hijacking vulnerability

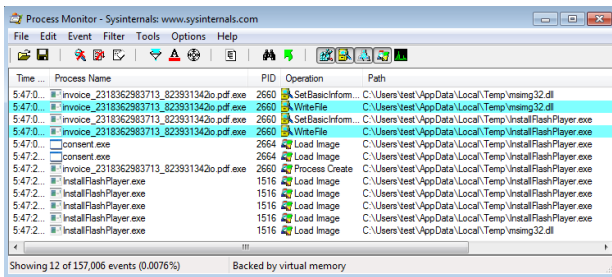
- What happened? → Process Monitor (procmon)



- 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 → 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

- automated testing of DLL hijacking vulnerabilities in installers
- identified another vulnerability in Adobe Reader
- report to Adobe PSIRT → 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
- Persistence, hiding malicious activities in the system (Vault7)

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

Questions, discussion.



Ladislav Bačo
Head of the NIKI department



ladislav.baco@csirt.sk