ZouAV for PWN2KILL

Core Algorithm Approach

Alan Zaccardelle

alan.zaccardelle@eu.didata.com

DIMENSION DATA
www.dimensiondata.com

iAWACS Challenge, 2010

DIMENSION DATA

Objectives

- Attack must stay undetectable[a] by the Anti-virus
- Disable Anti-virus protection and make it permanently successful
- Use EICAR virus sample to validate the attack even after a reboot

[a] Known as Malicious activity, Malwares, Virus, Trojan, Unwanted Programs,...

DIMENSION DATA

Easy Candidates

- AVAST
- AVG
- AVIRA
- F-Secure
- G-Data
- McAfee
- Microsoft-SE
- TrendMicro
- Safe'n'Sec

Complex Candidates

- BiteDefender
- Kaspersky
- NOD32
- DrWeb
- Symantec

Main Approach

- Execute a program that requests an Administrator privilege
- Modify some Access Control List to block Anti-virus processes' execution
- Disable the Anti-virus by using local available tools and trusted application from the Software Protection analysis
- Implement a Powerful and a Simple Attack at the same time

DIMENSION DATA

Core Algorithm

Attack implementation for Easily Anti-virus List

Processes' identification

- Identify Anti-virus processes to implement a generic attack
- Identify the Installation path of the Anti-virus
- Set restricted Access Control List on specific Anti-virus files

Easy Candidates

- Easy Candidates list Anti-virus were disabled without any detection
- The disabled protection remains persistent even after reboots or updates

Antivirus Alerts Management

- Some Anti-virus do not even display a Security Alert
- One of them displays a System Safe status in the GUI Console

Core Algorithm

Attack implementation for Complex Anti-virus List

Some of them remains a little bit sophisticated from the Easy list. They load drivers from Kernel or make other integrity check to make sure that they still activated and operational. It is not always possible to stop the Application service but it works as easy as we did in the previous Anti-virus list.

Other Candidates

- This generic attack can be implemented also for those Anti-virus from assumptions and conditions
- SYSTEM privileges are needed, therefore a simple Windows Service implementation has been tested
- Technical knowledges are required to implement the attack from a Kernel driver for more sophisticated attack[a]

[a] Currently out of my technical knowledge

DIMENSION DATA

Core Algorithm

Attack implementation for Complex Anti-virus List

Antivirus disabled

- Kaspersky has been disabled with windows administrative tools such as *calcs.exe*
- *NOD32, BitDefender, DrWeb*[a] *and Symantec* have to be tested again

[a] If SelfProtection is off, DrWeb moves to the Easy Anti-virus List

As today[1], Symantec detected *ZouAV Application & ZouAV Windows Service* as a non trusted application and blocked[2]. But the version that has been tested for Kaspersky should work without any alert.

[1] 2010-05-03

[2] SONAR detection module

Easy Candidates

- AVAST Disabled
- AVG Disabled
- AVIRA Disabled
- F-Secure Disabled
- G-Data Disabled
- McAfee Disabled
- Microsoft-SE Disabled
- TrendMicro Disabled
- Safe'n'Sec Disabled

Complex Candidates

- BiteDefender To be tested
- Kaspersky Disabled
- NOD32 To be tested
- DrWeb To be tested
- Symantec To be tested

- Not a sophisticated attack
- Not technical knowledges to understand
- Simple and powerful at the time
- Denial of Service possible on the Windows UAC components
- All Antivirus are vulnerable to this attack
- Virus Database Signature may have fault positive alerts
- The user will remains the last security point of failure
- ZouAV[a] is not an idiot ;)

[a] Doing things as an idiot

DIMENSION DATA

Questions & Answers

iAWACS / PWN2KILL 2010

Alan ZACCARDELLE

EPITECH
DIMENSION DATA
Eric FILIOL