sAVEX

Virus infection by its exclusion

Alan Zaccardelle

alan.zaccardelle@eu.didata.com

DIMENSION DATA
www.dimensiondata.com

iAWACS Conference, 2010

DIMENSION DATA

DIMENSION DATA

DIMENSION DATA

DIMENSION DATA

DIMENSION DATA

DIMENSION DATA

The Anti-virus remains one of the most useful tools for fighting against and protecting computers from virus

However it is important to highlight that the actions performed by the end user could compromise the entire protection put into place by themselves or the organization to which they depend *(PDF and MSOffice are examples)*

Detect and Control

Because attacks tend to be more sophisticated, Anti-virus editors implements advanced protection features.

- Buffer Overlfow
- On Access Scanning
- Self protection or Access Protection controls to block threats that try disabling the Anti-virus
- RootKit detection
- Parental controls
- Firewall, Content filtering
- Phishing and Malwares protections
- Heuristic Malicious macro detections
- Multiple Engine scanner

Are there any Issues for the end user?
More or Less

Well, these new functions are effectively needed but, at what price ?

- Complex to configure as new features are implemented
- Systems and Applications performances decrease
- Users lose the choice of a good antiviral protection because nowadays choosing the best anti-virus software is more important than ever

- In most case, the Anti-Virus have some strange protection implementations or malwares' detection. They do not offer a well known protection as they should do *(even if you pay for the protection)*

sAVEX

security on **A**nti**V**irus **E**xclusions

The main objective of sAVEX is to show a simple way to exploit what it is been set. The infection by its own exclusion may remains the simplest way to a success.

Infection possible through

- Bad Anti-virus configuration
- A poor Anti-virus monitoring
- A funny escalation between Default/Low/High risks processes Anti-virus analysis
- An implementation of a already known exploit with Microsoft Macro that will remains difficult to detect from a "On Demand Scan" or "On Access Scan"

Protections & Infections

In order to validate this Proof of Concept, we have focused on a specific Anti-virus[1] and validated that it remains active and running without any suspicious alert.

Infection possible through

- No reverse engineered made on the application
- Update & administration tasks of the Anti-virus itself remain possible
- Use of known viruses without any code modification (direct use)

[1] McAfee VirusScan Enterprise 8.xi & Total Protection

Operating Systems & Applications

Condition of success

We have tested this Proof of Concept under some conditions:

- Administrative rights for Windows XP users
- Some actions/Steps will need administrator privileges to success
- Microsoft Windows XP, [Windows Vista, Windows Seven][a]
- Microsoft Office 2007 and McAfee Anti-virus up to date

[a] UAC may alert the user during the exploit the user's validation will be required

Those tests have been focused on the McAfee Anti-virus Protection[2] *But other solutions may have the same issues*[3].

- Infect a system with a well known virus based on local exclusions settings
- Infect a system that does not have any exclusions
- Make the virus persistent even after a policy enforcement
- Implement a global exclusion that excludes ALL hard-drives from "On Access Scanner" and "On Demand Scanner"

- We have installed the Anti-virus with standard settings
- Default Access Protection won't complicate the exploit success

[2] Because it was the easiest one and largely deployed

[3] I let Security Expert make it works

DIMENSION DATA

Business environment

The highest security risk

In a professional context, it is difficult for the anti-virus to find its position.

Security and Business Requirements

- The most powerful protection
- A complete set of detection features and options
- Compliant with all systems and applications
- Minimum of fault positive detections...

Business environment

Security Risks grow as evolutions are made

The installation of new product ranges, the change from out-of-date versions to more effective products with advanced detection features confront administrators with new problems:

Performance issues

- Systems and Applications overloads *(processor, memory, latencies,)*
- Applications and/or Operating systems that shut-down unexpectedly
- And finally a global Users' dissatisfaction around security tools installed on their systems

Root cause

The Anti-virus is often the root cause of these problems and is also blamed for these "degradations"

Private users

Impacted reduced for personal use

The Anti-virus in the personal user context is less vulnerable to these hazards than Corporate users and the only way to deal with this problem is:

- By completely re-installing the system or by buying a new one *(major mitigation for a normal user)*
- To set up the Anti-virus software as accurately[a] as possible depending on the applications that are impacted.

[a] An analysis is carried out when the incident occurs but then it is left untouched due to the low-risk factor or Risk Assessment issue

Undetectable known virus

Why make it complicated instead doing it simple

Learn more about the configuration

- Use specific local Anti-virus settings to infect the system when it is possible
- Use dedicated Anti-virus settings to infect the system
- Make the settings unchanged even after a system reboot or any Anti-virus policy enforcement[a]

[a] With McAfee ePolicy Orchestrator Agent - McAfee Framework

Infect the system

- Infect a system with a probability of success close to 100%

No encryption

All settings are in clear text

The exploit plays only with the registry to add or remove settings. All McAfee Antivirus settings are stored in the registry in a readable syntax.

McAfee Antivirus settings

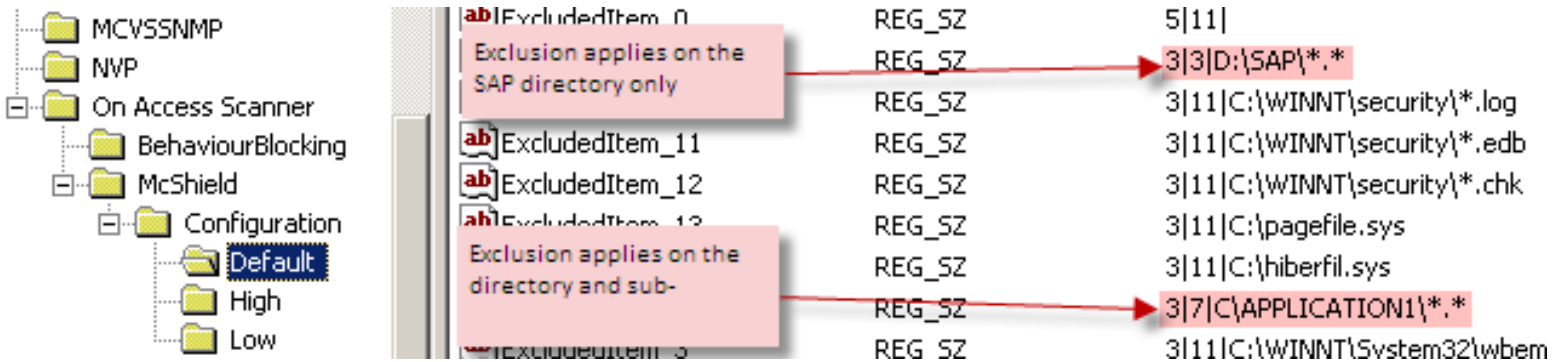
```
HKLM\SOFTWARE\McAfee\VSCore\On Access Scanner
HKLM\SOFTWARE\McAfee\VSCore\On Access Scanner\BehaviourBlocking
HKLM\SOFTWARE\McAfee\VSCore\On Access Scanner\McShield\Configuration\Default
HKLM\SOFTWARE\McAfee\VSCore\On Access Scanner\McShield\Configuration\High
HKLM\SOFTWARE\McAfee\VSCore\On Access Scanner\McShield\Configuration\Low
```

Current local Anti-virus settings

Guess on a poor Anti-virus administration

Potential vulnerabilities

The threat Analyzes potential vulnerabilities in the current Anti-virus' configurations



Current Exclusions

- An exclusion has been set on the full SAP directory for all types of file *(*.*)*
- An exclusion has been also set on the full APPLICATION1 directory and its subdirectories

Current local Anti-virus settings

Proof of Concept

Get Registry information

- Check registry key value for OnlyUseDefaultConfig[a]
- Check registry keys value for NumExcludeItems[b]
- If there are exclusions, they are called ExcludedItem_X. Check them and find a string that match (3|15[c]|...*.*) or (3|11[d]|...*.*)
- If it matches, the virus can stored and run from here

[a] Under HKLM/SOFTWARE/McAfee/VSCore/On Access Scanner/McShield/Configuration

[b] Under HKLM/SOFTWARE/McAfee/VSCore/On Access Scanner/McShield/Configuration/Default|Low|High

[c] Current Directory and subdirectories

[d] Current Directory only

Dedicated Anti-virus settings 1/2

Excluded all types of file on any drives

Potential vulnerable exclusions

- To be able to forge dedicated exclusions, Access Protection needs to be turn off in order to not alert the user. Check the APEnabled value [a]
- If Activated, Mcshield service must be stop with SYSTEM account *(*sc.exe from microsoft will help)
- Create a forged Anti-virus exclusions to bypass the real time[b] detection

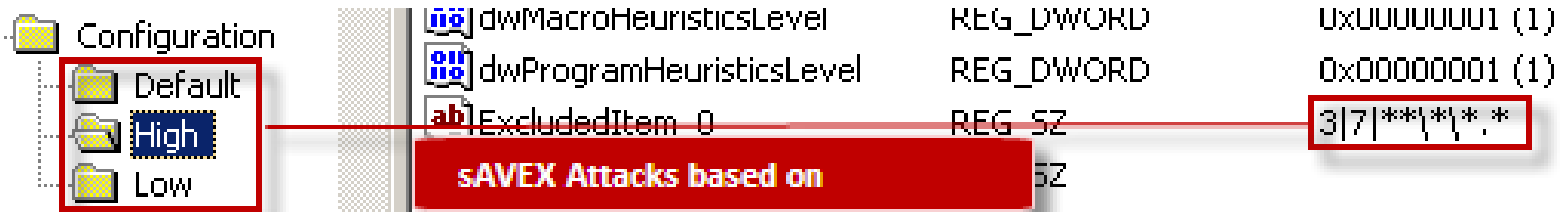
---

[a] Under HKLM/SOFTWARE/McAfee/VSCore/On Access Scanner/BehaviourBlocking/

[b] Can be set also for scheduled scan tasks

Dedicated Anti-virus settings 2/2

Proof of Concept



Full hardrives' exclusions

This exclusion allows virus to be undetectable from any directories and subdirectories and also on any drivers

Make the undetectable virus Persistent 1/2

Block the policy enforcement

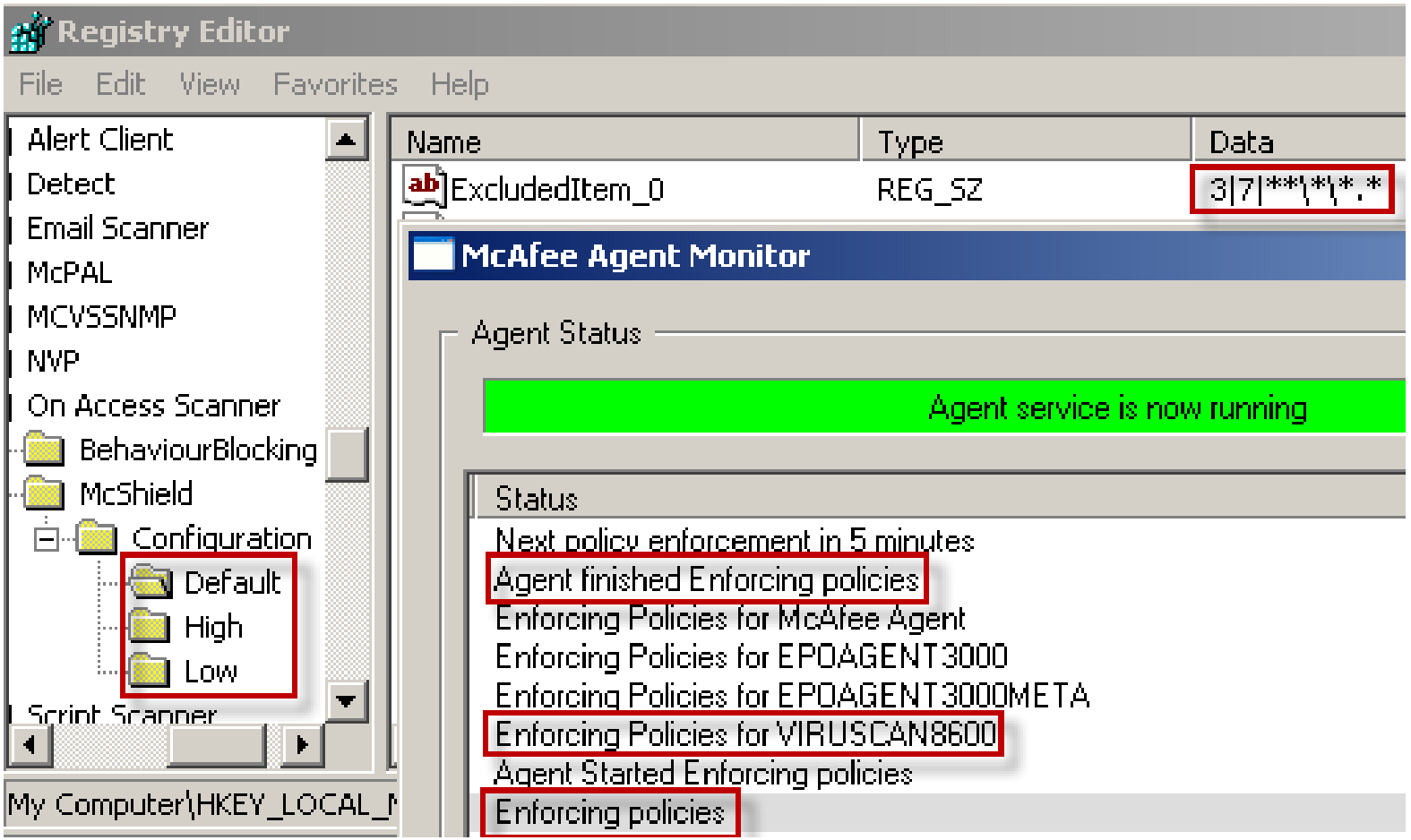
Access Protection won't detect any of these changes

- Make sure your full Harddrive exclusions are set
- Change Registry keys ACL to block any McAfee policy enforcement that would reset to a trusted configuration
- Deny System account access on the "Default|Low|High" key and sub-keys. In this way, McAfee won't be able to apply any future changes. Current applied policies will remain even after a reboot[a]

[a] You will get another security Proof of Concept ;)

Make the undetectable virus Persistent 2/2

Block the policy enforcement



Even if sAVEX is a McAfee Proof of Concept, it is important to have few little ideas to detect or block such of activities.

- Restrict registry access to some identified persons
- Logs any registry access
- Centralize, Correlate and monitor Logs (Antivirus, Operating system events,)
- Implement a periodic scan task from other Anti-virus that are not installed on systems (Online scan, Rescue Antivirus LiveCD, Logon scripts,)
- Wait for an update *(HotFix, Patch or DAT)*

DIMENSION DATA

- Not complicate at all
- Not high technical knowledge to understand and implement
- Known virus might be reactivated by this attack *Conficker, ZeuS...*

We have designed a detailed operational technique to infect a system from its current Anti-virus' exclusions

Basic infection

- From local exclusions configuration
- From dedicated Anti-virus settings

Advanced infection

It is also possible to combine virus infection from a specific High Risk process to a Low Risk or even a Default one according to the less restrictive exclusion.

Some Anti-virus are not affected by this attack

- Settings are stored in an encrypted file and not accessible from registry
- Encryption keys belong to the current installation SID
- Precomputed exclusion file from a computer *A* won't work on the computer *B*

Many thanks for your attention