ACKER-est



Hiding on Windows Platforms

Martin Dráb

martin.drab@email.cz

Agenda

- Areas of interest
 - **Windows** registry
 - **Network communication**
- Attacker's point of view
- No extra knowledge required



<link href="/Themes/HackerFes
<link href="/Themes/HackerFes</pre>

</head>

<a href="/RM.Localiz
/
<a href="/RM.Localiz</pre>

/article></div>
</div>
</div>
<div class="citation">
"Pokud znáš nepřítele a ...
'okud neznáš nepřítele ani seb.
</div>
</div>
<a class="gopas-link" hrel-

<div class="title">

</header>

<div class="navbar">

<div class="bomb">

<vib

span class= Icon-b

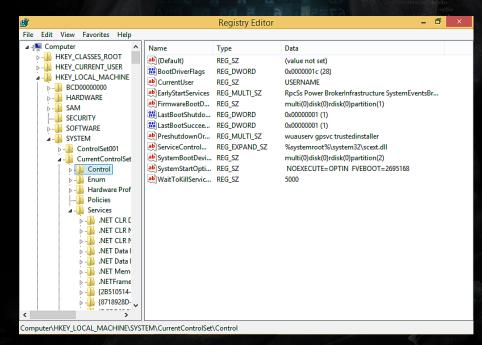
<span class= icon-bi

HACKERFest 2015

Windows Registry

Windows Registry – basic info

- Configuration storage similar to file systems
 keys = directories
 - ✓ values = files
- Typed, small sized data
- Stored on disk, lives in RAM





Filtering Registry Operations

- Driver-supplied callbacks (CmRegisterCallback(Ex))
 - Invoked before and after a registry operation in context of the thread taht irequested it
 - Multiple callback registrations allowed (layered model)
- Modes of operation
 - (gather information about each operation)
 - Solution Block (the requestor receives an error)
 - Modify (operation parameters and/or results can be changed)
 - Emulate (the whole operation is performed by the filter driver)



RegHider

- Hides registry keys
 - QueryKey and EnumerateSubkeys operation modified in order not to report given registry keys
- Reports nonexistent registry values
 - © Operations on these values are emulated
 - Each value may be visible either systém-wide, or only to certain processes



Detection

- Special registry operations
- Offline analysis
 - Offline Registry Library
 - Parsing registry files directly (e.g. chntpw)
- Online analysis
 - Registry tree is stored in memory (usually)
 - It can be read directly (without using any system routines)



k href="/Themes/HackerFest
k href="/Themes/HackerFest

</head>

<a href="/RM.Localiz
/
<a href="/RM.Localiz</pre>

21.

<a class="hackerfest-log

</header>

<div class="navbar">

<div id="countdown"></d</pre>

<vib\>

span class="icon-be snan class="icon-be

<span class="icon-backgrain con-backgrain class="icon-backgrain class="icon-backgra

HACKERFest 2015

Network Communication

ddiv classe "citation"
"Pokud ariss nepfie
Pokud nearids nepfie", a «div»
«a classe" gopas "tille", «div classe" tille", «span classe" dut

el cos-«Ineader p «div class» navbar «div class» bomb «div class» navbar mr «div class» navbar mr «div class» container

<span class from Abution (div class from coll (div class from article class from detribute)

:li class="first">

li> i>

>

ntml lang="cs-CZ" class ntml lang="cs-CZ" class ntml charset="utf-8" <https://intlines.com/charsets/titles/ <!--[if tt IE 9]>

secnpt src= /Lore/shapes/scru

content="Orchard" name

funk href="/Themes/Hackerre

think href="/Themes/Hackerre

GOPAS

Network Basics

header

TCP/UDP header

WFP (Vista, W7)

WFP (W8 and later)

Applications

Kemel components

Transport layer (TCP, UDP)

Network layer (packets)

> Link layer (frames)

Ethemet header

IPv4/IPv6

Data

HACKER est 2015



Winsock Kernel

- A socket-like interface for the kernel world
 - Usual socket calls (socket(), bind(), connect(), listen())
 - Used in the same way as in usermode
 - An easy way how a driver can comminucate over network
- Implementation details



Raw Ethernet Frames

- Kernel dirvers are able to send raw ethernet frames over network, thus bypassing any packet filters placed above
- Difficulty: easy (PoC at least)
 - ☑ Just get the ndisprot sample from the WDK package
 - © Delete few lines of code and it will work
 - ☐ Fill in the IP header correctly



s/article></div>
</div>
</div>
</div>
</div>
</div

<pre>"Pokud znáš nepřítele a c

</div>
</div>
</div>

</div
</div
</div
</di>
</dr>
</pr>
</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

</pr>

HACKERFest 2015

File Systems

Driver and Device Objects

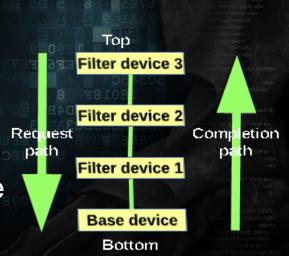
- Driver object
 - Gathers all necessary information about certain device driver, such as addresses of routines servicing various types of requests
- Device object
 - Receives requests from applications and other drivers
 - A driver owning the device is responsible for handling incomming requests



Device Stacks

When a driver needs to see requests comming to a particular device (of another driver), it can **attach** its own device object **above** that device and form a **device stack**

- ³ Requests usually sent to the top device
- [™] Unknown requests passed down
- All drivers in the stack should keep their manners





<link href="/Themes/HackerFe
<link href="/Themes/HackerFe</pre>

Where to Attach?

os enos"=eeelo vib> ebeert doublius"=eeelo aloitaes File system

</article></div>

filter drivers

class="citation">

Filter Manager

class="title"> span class="date">| span> slass="beckerfest

File system driver (NTFS)

Volume stack

Volume Snapshots

ReadyBoost

Bitlocker

Volume Manager Storage stack Partition Manager

TrueCrypt

Disk Class Driver

USB Storage Driver

Disk stack

USB filter drivers

7EF67F67

USB Storage Driver

USB filter drivers

USB hub

USB stack

HACKER est 2015

GOPAS

Implications

© Problems of a lower attacher

- Hardware dependencies
- Software encryption
- No context information
- Direct (S)ATA/SCSI commands
- Writting a basic FS parser is quite easy

Games Tips & Tricks

- Build your own file system
- Take advantage of symbolic links (such as drive letters)



HACKERFest | 2015

Conclusion

References

- □ Demo projects (may be updated in the future)
 - https://github.com/MartinDrab/Hackerfest2015
- - http://dfrws.org/2008/proceedings/p26-dolan-gavitt.pdf
 - http://amnesia.gtisc.gatech.edu/~moyix/suzibandit.ltd.uk/MSc/Registry
- - "==eQD vib http://www.jadro-windows.cz/download/ntfsdoc-0.5.zip
 - http://www.jadro-windows.cz/download/fat.zip





HACKERFest | 2015

www.hackerfest.cz www.gopas.cz

