ClubHACK 2010

Windows Icons : watch them closely or be screwed !

- Laboratoire de virologie et de cryptologie opérationnelles -
Corsaire
pas pirate

DAVID Baptiste & FILIOL Eric
bdavid@et.esiea-ouest.fr
filiol@esiea.fr

esiea recherche (C + V)^0

Agenda :

Introduction :

I) How the icons work on the desktop ?

II) Attack of icons by superposing !

III) Another attack : attack by background !

IV) Attacks on icons without icons !

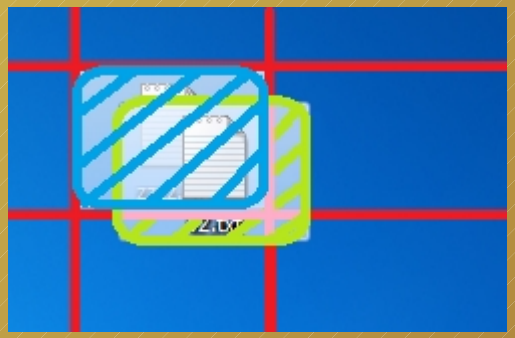
V) Attack the mouse to attack the icons !

VI) General Conclusion :

The main problem of this talk :

How to make the user believe that he is using his own icons ?!

Many questions about the possible actions on icons :



→ Which icon is selected by the mouse ?

→ What we can do with icons ?

→ Is the icon selection linked to the icon position ?

→ What can happen when you click on an icon ?

→ When I click on an icon, is it the right program which is launched ?

... How do we approach this problem ? …

I) How the icons work on the desktop.

Understanding the arrangement of icons on your desktop :

→The position of each icon is managed by a cartesian coordinate system of two dimensions.

→ The system's center of origin is located in the top left corner of the screen.

→ Windows exploration desktop has a special grid to place the icons.

A test to see how the priority of selection works on two icon positions :

→ Disable the icon coordinates to overlap them.

→ Create an algorithm in order to test which of the two icons has priority over the other.

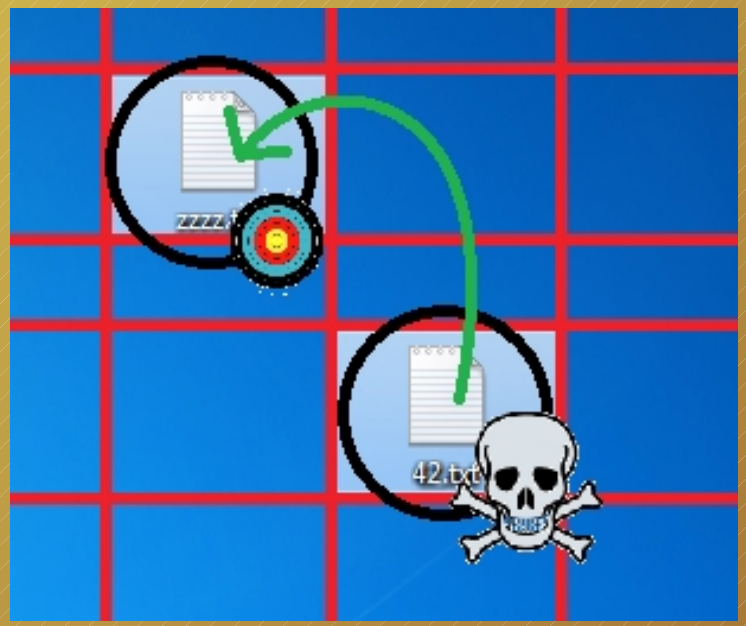
→ The experimental approach could be :

1) Store in a structure each icon's coordinates.

2) Identify the attacking icon (which overlaps) and the attacked icon (the one that will be overlapped).

3) Give the attacking icon the same coordinates as the attacked icon.

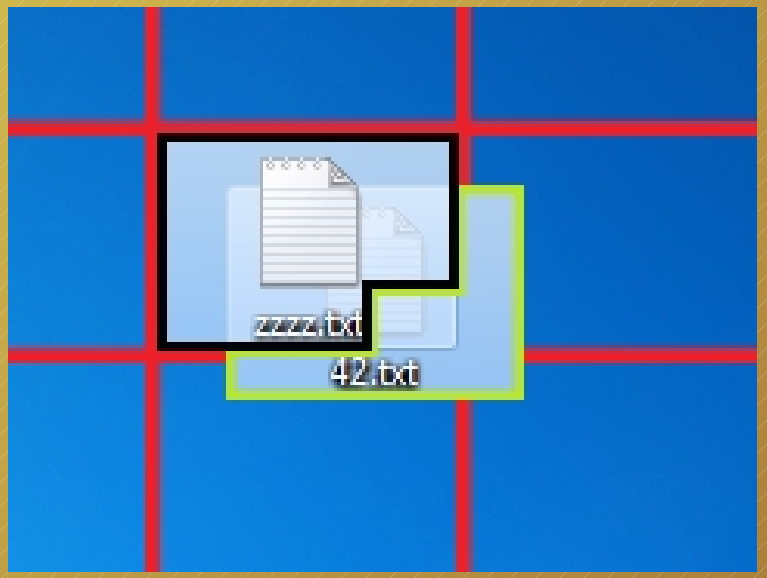
4) Observe the surface given by the mouse when hovering over the icons.



Test results:

From previously aligned icons :

→ Even if the alignment grid has been disabled, the priority of overlap is given to the icon located in the top left of the box.



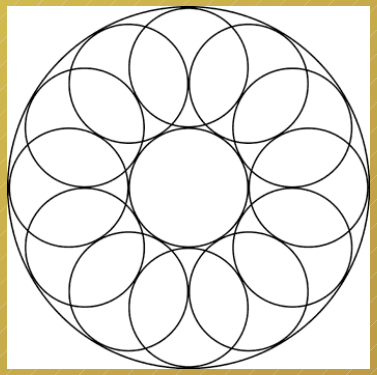
→ Surface determines priority.
(ie : a grid cell will not give priority to only one icon)

→ The center of the icon is not very significant.

→ The icon names, or programs they represent, have apparently no influence.

→ Presumably, most of the time, the user clicks on our attacking icon rather than the one that has been attacked.

II) Attack of icons by superposing :



Goals :

→ Try to create a trigger to launch a possible assailant program.

→ Overlap two icons in order to create confusion for the user.

Main tools :

→ Create an interaction between the icons by calling the List-View Controls Messages (LVM_) from the windows API.

→ Redirect the windows messages towards our program.

→ Prioritize the hovering of the mouse over our own icon instead of the attacked one.

→ Use an invisible icon !

How to create an invisible icon ?

→ Use icons of 32-bit color (16.7 million colors plus alpha channel transparency). (It has been possible since Windows XP).

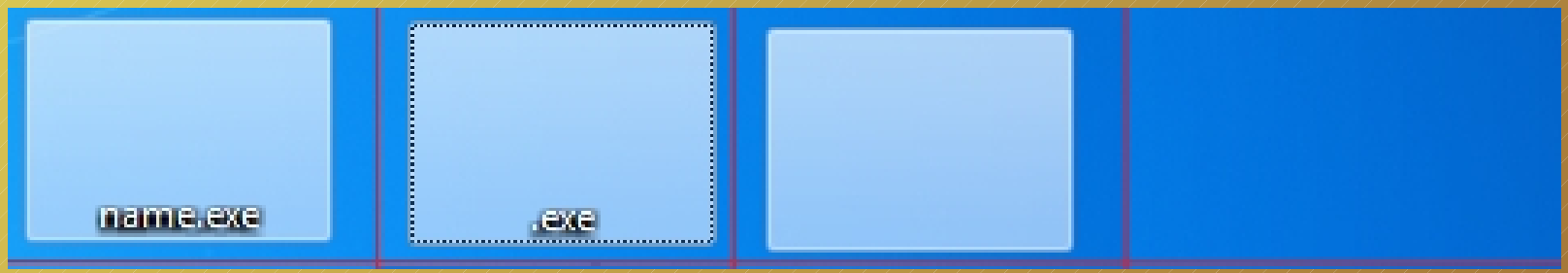
→ Possibility of using free icon creating software. Otherwise PNG (plus special header) will suffice to create icons.

→ Make the name of the icon which references the program invisible.
Rename the icon using the invisible character provided by the (extended) ASCII code 0xA0 (0160 in decimal).
Note : File names are written in UTF-16 format on Windows 7.

→ Remove icon extensions if present :
In the Windows registry about the key :

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

→ Put it to 0 to display the extension.
→ Put it to 1 to hide the extension.



Using this result to create a trigger :

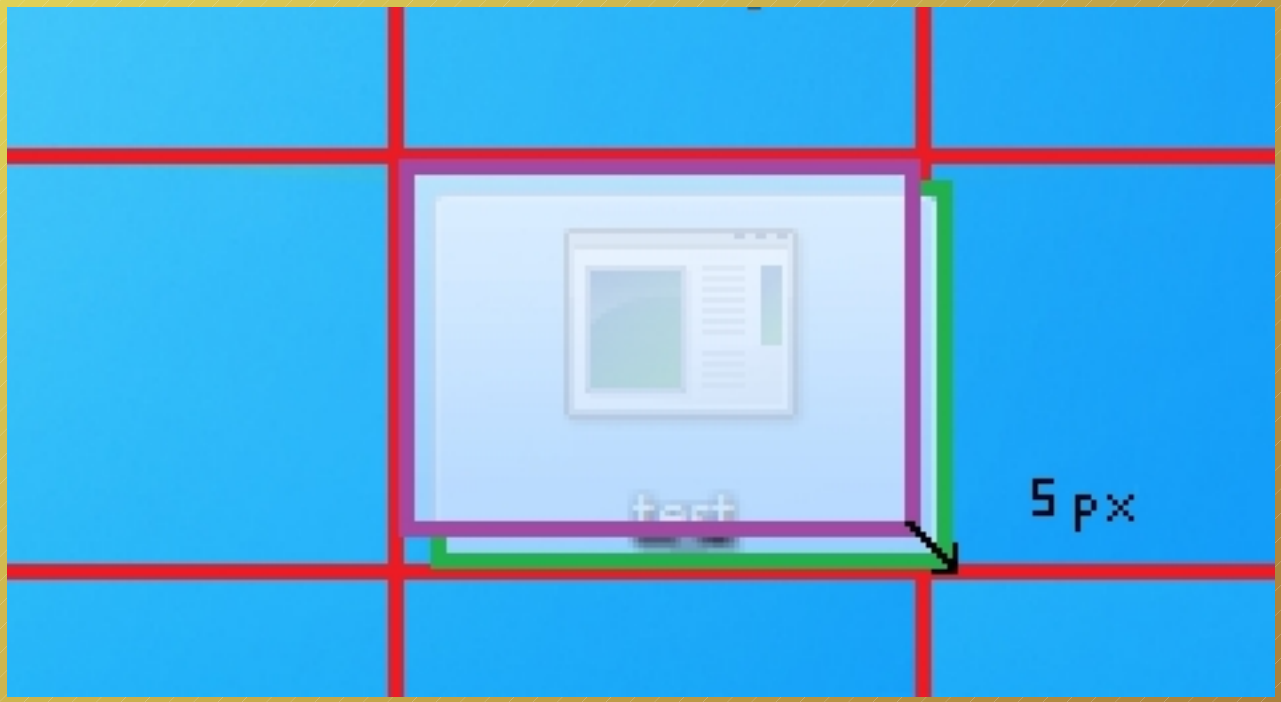
→ Create a transparent icon (possible by the alpha channel).

→ Hide the name of the icon.

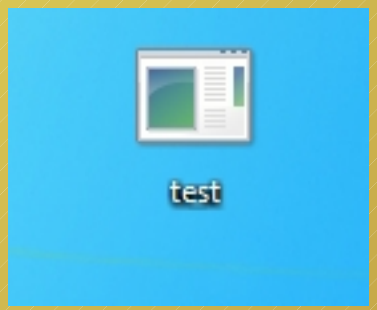
→ Create the recovery.

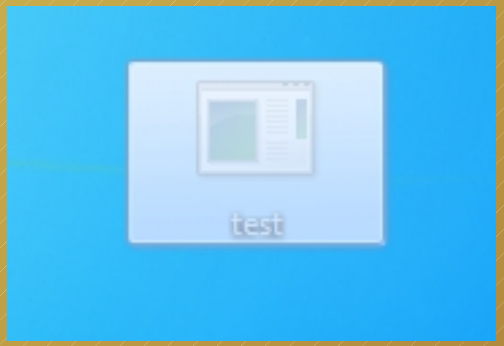
→ Update the desktop.

→ Let the user click.



→ With a very small gap distance (1 pixel).






Laboratoire de virologie et de cryptologie opérationnelles -
Corsaire
pas pirate

Demo

Conclusion on this attack :

Good points :

→ The possibility of hovering icons can create an interesting confusion for the user.

→ The trigger created is modulated in utilization by the user himself.

→ By selecting the attacked icon, it is possible to know which application is clicked by the user on the desktop and react accordingly.

→ If the user decides to move the icon, he also moves the hovering icon in an invisible way for him.

Bad Points :

→ The user can quickly see and counteract the attack by making a re-alignment of icons on the grid.

→ There could be some problems about the displaying of the transparent icon.

→ If there are two icons, it is not always certain that your icon is selected by the user.

Ideas to solve problems :

→ Problem about the re-alignment of icons on the grid :

→ Watch the call of the right click of the mouse and prevent the use of re-alignment.

→ Problem about the offset distance :

→ Try to be the nearest to the targeted icon (Depends on the percentage of clicks that you want).

→ Problem about the displaying of the transparent icon :

→ Normally on a stable system there are no problems.
→ Refresh the desktop or reboot.

III) Another attack : attack by background !

Objective :

Let the user believe that he is clicking on the icon of his program.

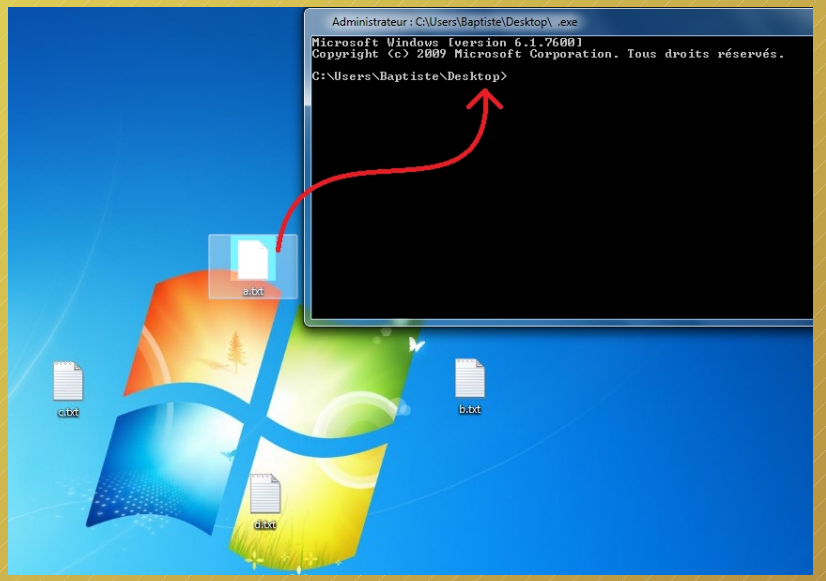
Main tools :

→ Use the wallpaper of the desktop.

→ Put forward our attacking icons instead of attacked icons, on the desktop.

→ Do not directly depend on the alignment of icons on the grid.

→ Use of transparent icons.



The different stages of the attack :

→ First : take the position of the icons.

→ Second : remove any windows in the foreground.

→ Third : reduce the taskbar.

→ Fourth : take the screenshoot.

→ Fifth : restore the taskbar.

→ Sixth (and for each icon attacked) :

- → Remove the icon or the program represented.
- → Put our transparent icon on the desktop.
- → Add one invisible character at the end of the new transparent icon's name.
  (Prevents the crush of icons)

→ Seventh : put the screenshot taken at the fourth step as wallpaper.


Laboratoire de virologie et de cryptologie opérationnelles -
Corsaire
pas pirate

Demo

Conclusion on this attack :

Good points :

→ The attack is easy to implement.

→ We no longer depend on the priority of hovering, nor the alignment of icons on the grid.

→ Opportunity to react accordingly to the original icon called by the user.

→ The trigger will be launched each time the user tries to click on his icons.

Bad Points :

→ Taking the screenshot can be done quickly but it is necessary to minimize all windows.

→ If the user tries to move icons, he will see the problem.

→ There may be some problems about the displaying of the transparent icon.

Ideas to solve problems :

→ Problem about taking the screenshot :

→ Wait until there are no windows on the foreground to act.
→ Take the screenshot when the computer shuts down and make the change when the computer restarts.
→ Take the screenshot when the computer starts.

→ Problem about the movement of icons :

→ Update the icon positions at regular short intervals of time.
→ Position icons to their own position all the time .

→ Problem about the displaying of the transparent icon :

→ Why not try to not use them ?...

IV) Attacks on icons without icons !

Objective :

Hide icons and make the user believe that they are still there.

Why and how ?

→ Icons have got constrained positions, some problems about displaying, alignment, reorganization...They could be a real pain !

→ Use the wallpaper to reproduce the appearance of a normal desktop.

→ Don't mind about icons.

Realization of the attack :

→ First : minimize all windows.

→ Second : reduce the taskbar.

→ Third : take the screenshot.

→ Fourth : replace the taskbar.

→ Fifth : put the screenshot taken at the fourth step as wallpaper.

→ Sixth : disable the display of desktop elements.

→ Seventh: start the process to detect the solicitation of icons by the mouse.


Laboratoire de virologie et de cryptologie opérationnelles -
Corsaire
pas pirate

Demo

Conclusion on this attack :

Good points :

→ The attack is easy to implement.

→ Just watch and react to the movement of the mouse.

→ It's enough that the user clicks on the desired locations on the desktop to launch the malware.

→ Possibility of alternating the "true" and the "false" desktop.

Bad Points :

→ The desktop seems a bit stuck and static.

→ Moving the icons is forbidden to the user.

Ideas to solve problems :

→ Problem about the static nature of the office :

→ Take a screenshot for each icon in selection mode. Use these to manage each icon.

→ Alternate between the real and the fake desktop to seem more real (before and after a click on it, for example).

→ Realize a keyboard handling to manage the calls by keyboard for the icons.

→ Problem about the impossible movement of icons :

→ Toggle between the true or the fake desktop.

→ Manage the left/right click of the mouse.

V) Attack the mouse to attack the icons !

Objective :

Focusing on the mouse to launch the attack rather than on the icons.

Main tools :

→ Using icons as an advantage not as a constraint.

→ Hook the mouse to manage the launch of the trigger.

→ Do not use the functions on the icons directly.

Plan of the attack :

→ Take the position of each icon.

→ Place a hook on the keyboard and on the mouse :
  → Prevent the use of the double click.
  → Prevent the use of the key enter (to launch the program directly).
  → Prevent the use of the right click and the function run or open.

→ When a signal, which must be intercepted by the hook, is present :
  → Check if an icon is situated where the user has double clicked.
  → Launch our malicious application.
  → Do not spread the intercepted signal !

→ Or else let the signal pass.

→ Update the position of icons.


Laboratoire de virologie et de cryptologie opérationnelles -
Corsaire
pas pirate

Demo

Conclusion on this attack :

Good points :

→ The attack is easy to implement.

→ The desktop icons are unchanged.

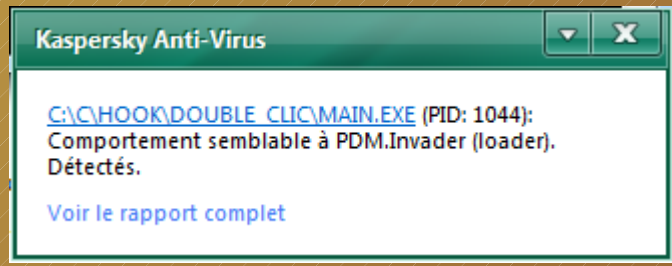
→ We let the icons go free. The action is completely invisible for the user.

→ Interactions between the movement, the selections, and information under the icons are no longer prevented.

→ Very fluid.

Bad Points :

→ Some antiviruses can sometimes dislike the operation (information message).



VI) General Conclusion :

→ The use of icons as a trigger is not ready to stop.

→ There are many different ways and approaches possible to create this kind of trigger.

→ We are between social engineering and basic viral action.

→ Use in order to make a bad joke or to hide an unexpected trigger.

→ Users without a functional desktop are quickly lost !

DAVID Baptiste & FILIOL Eric
bdavid@et.esiea-ouest.fr
filiol@esiea.fr

Thank you very much for your attention.

If you have any questions, I would be happy to answer them...