



VACCINATION

THE ANTI-HONEYPOT APPROACH



WHOAMI

- Researcher @ Minerva Labs, an Israeli startup
- Big fan of breaking stuff and putting them back together
- Expert in calling experts when failing to put stuff back together
- Fluent in C, C#, Python, Java and... Arabic
- Twitter: [@Gal_B1t](https://twitter.com/Gal_B1t)



WHAT IS A HONEYPOT?

THAT LADY IN RED

- Honeypots are that first girl to appear in a Bond movie
- From far away they look like a catch
- Up close it is clear they ain't a bargain





SO....
WHAT IS A
ANTI-HONEYPOT?

NATURAL APPROACH FOR REPELLING ATTACKERS

- Can you tell the difference?



EVEN BUTTERFLIES TRY TO FIND HACKS





KNOW YOUR ENEMY'S FEARS - FOUR WAYS TO REPEL BAD GUYS

VIRTUALIZED\ANALYSIS ENVIRONMENT

```
push    NULL
push    .szWindowClassOllyDbg
call    [FindWindowA]
test    eax,eax
jnz     .debugger_found
```

```
push    NULL
push    .szWindowClassWinDbg
call    [FindWindowA]
test    eax,eax
jnz     .debugger_found
```

```
.szWindowClassOllyDbg    db "OLLYDBG",0
.szWindowClassWinDbg    db "WinDbgFrameClass",0
```

*Mark Vincent Yason
BH USA '07*

001D0778	50	push eax	
001D077C	FF 93 A9 09 00 00	call dword ptr ds:[ebx+9A9]	[ebx+9A9]:GetUserNameA
001D0782	09 C0	or eax,eax	
001D0784	74 53	je 1D07D9	
001D0786	FF 75 F8	push dword ptr ss:[ebp-8]	
001D0789	8D 85 F8 FB FF FF	lea eax,dword ptr ss:[ebp-408]	
001D078F	50	push eax	
001D0790	FF 93 A5 09 00 00	call dword ptr ds:[ebx+9A5]	[ebx+9A5]:CharUpperBuffA
001D0796	80 AD F8 FB FF FF 53	sub byte ptr ss:[ebp-408],53	
001D079D	75 3A	jne 1D07D9	
001D079F	80 AD F9 FB FF FF 41	sub byte ptr ss:[ebp-407],41	
001D07A6	75 31	jne 1D07D9	
001D07A8	80 AD FA FB FF FF 4E	sub byte ptr ss:[ebp-406],4E	
001D07AF	75 28	jne 1D07D9	
001D07B1	80 AD FB FB FF FF 44	sub byte ptr ss:[ebp-405],44	
001D07B8	75 1F	jne 1D07D9	
001D07BA	80 AD FC FB FF FF 42	sub byte ptr ss:[ebp-404],42	
001D07C1	75 16	jne 1D07D9	
001D07C3	80 AD FD FB FF FF 4F	sub byte ptr ss:[ebp-403],4F	
001D07CA	75 0D	jne 1D07D9	
001D07CC	80 AD FE FB FF FF 58	sub byte ptr ss:[ebp-402],58	
001D07D3	75 04	jne 1D07D9	
001D07D5	C6 45 FC 01	mov byte ptr ss:[ebp-4],1	
001D07D9	0F B6 45 FC	movzx eax,byte ptr ss:[ebp-4]	

53 41 4E 44 42 4F 58 ???

S A N D B O X !!!

HEAVILY FORTIFIED TARGETS

- Evading specific security products – the attacker's advantage
- Can't beat them all, but 90% of them is enough
- More in the live demo!



I KNOWZ SOFTWARE ENGEENIRINGZ

- Bugs in implementation of infection markers
- Abusing proper mechanisms

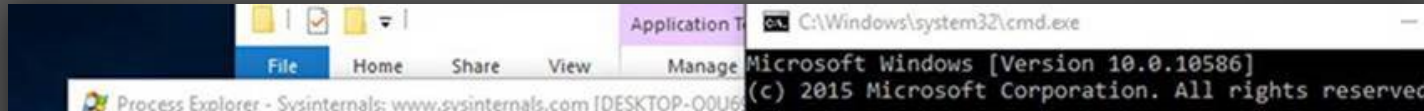


SYLVAIN SARMÉJEANNE
2/2016

```
push offset ValueName ; "completed"
push [ebp+hKey] ; hKey
setz [ebp+var_15]
mov [ebp+cbData], esi
00923073 FFD3 CALL EBX kernel32.CreateMutexA
0092307A 8945 80 MOV DWORD PTR SS:[EBP-80],EAX
0092307D FF15 DC109200 CALL DWORD PTR DS:[9210DC] ntdll.RtlGetLastWin32Error
00923083 8945 8C MOV DWORD PTR SS:[EBP-74],EAX
00923086 E8 062D0000 CALL 009226A91
00923088 8BF8 MOV EDI,EAX
0092308D FF15 D8109200 CALL DWORD PTR DS:[9210D8] kernel32.GetCommandLineA
00923093 56 PUSH ESI
00923094 8DB5 90000000 LEA ESI,DWORD PTR SS:[EBP+90]
0092309A 8945 88 MOV DWORD PTR SS:[EBP-78],EAX
0092309D E8 7EF8FFFF CALL 00923620
009230A2 8BC6 MOV EAX,ESI
009230A4 8B35 70129200 MOV ESI,DWORD PTR DS:[921270] msvcrt._stricmp
009230AA C70424 B4159200 MOV DWORD PTR SS:[ESP],9215B4 ASCII "rundll32.exe"
009230B1 50 PUSH EAX
009230B2 FFD6 CALL ESI
009230B4 85C0 TEST EAX,EAX
009230B6 8B1D A4129200 MOV EBX,DWORD PTR DS:[9212A4] SHLWAPI.StrStrIA
009230BC 59 POP ECX
009230BD 59 POP ECX
009230BE 75 42 JNZ SHORT 00923E02
009230C0 68 C0B09300 PUSH 93B0C0 ASCII "zaqtqk"
009230C5 FF75 88 PUSH DWORD PTR SS:[EBP-78]
009230C8 FFD3 CALL EBX
009230CA 85C0 TEST EAX,EAX
009230CC 74 34 JE SHORT 00923E02
009230CE 817D 8C B7000001 CMP DWORD PTR SS:[EBP-74],0B7
009230D5 74 23 JE SHORT 00923DFA
009230D7 837D 8C 05 CMP DWORD PTR SS:[EBP-74],5
009230DB 74 1D JE SHORT 00923DFA
009230DD FF75 80 PUSH DWORD PTR SS:[EBP-80]
009230E0 FF15 B4109200 CALL DWORD PTR DS:[9210B4] kernel32.CloseHandle
009230E6 E8 E1F8FFFF CALL 009236CC
009230EB 85C0 TEST EAX,EAX
009230ED 74 0B JE SHORT 00923DFA
009230EF 68 B0B00000 PUSH 0BB8
009230F4 FF15 B0109200 CALL DWORD PTR DS:[9210B0] kernel32.Sleep
009230FA 6A 00 PUSH 0
009230FC FF15 D4109200 CALL DWORD PTR DS:[9210D4] kernel32.ExitProcess
EBX=7C80EB3F (kernel32.CreateMutexA)
```

```
lea eax, [ebp+var_80]
call myCheckIDInRegistry
test al, al
jz short loc_4043B5
```


...AND SPORA RANSOMWARE!



The "HoeflerText" font wasn't found.



The web page you are trying to load is displayed incorrectly, as it uses the "HoeflerText" font. To fix the error and display the text, you have to update the "Chrome Font Pack".

Manufacturer: Google Inc. All Rights Reserved

Current version: Chrome Font Pack **53.0.2785.89**

Latest version: Chrome Font Pack **57.2.5284.21**

Update



<https://github.com/MinervaLabsResearch/SporaVaccination>

РУССКИЕ*

- Be careful with what you wish for when vaccinating!
- Russian keyboard:
 - Some malware will avoid to infect you
 - Others are comrade-targeted malware

*Russians



HOW BAD GUYS KNOW WHEN TO BUG OUT?

STATIC WINDOWS ARTIFACTS

- Registry keys
- Registry values
- Files
- Folders

Can be created

```
def create_file(f, t):  
    """  
    create file or folder if it doesn't exist  
    """  
    print "\t+ creating {0}".format(f)  
    try:  
        if os.path.exists(f):  
            print "\t+ {0} already exists!\n".format(f)  
        else:  
            if t == "file":  
                open(f, 'w')  
            elif t == "folder":  
                os.mkdir(f)  
            print "\t+ {0} was created!\n".format(f)  
    except Exception as e:  
        error_on_create(f, e)
```

DYNAM

- Processes
- Mutexes
- Windows
- Requires d
 - Run 1,000
 - More cl

```
def create_exe(name):  
    dest_file = temp_folder + name  
    shutil.copyfile(src_proc, dest_file)  
  
def run_exe(command):  
    try:  
        subprocess.Popen(command)  
    except Exception as e:  
        print "Got exception {0} while creating {1}".format(e, command)  
    return  
  
if __name__ == '__main__':  
    processes_to_mimic = [  
        "\\Wireshark.exe",  
        "\\OLLYDBG.exe",  
        "\\vmttoolsd.exe",  
        "\\mspaint.exe"  
    ]  
  
    for proc_name in processes_to_mimic:  
        create_exe(proc_name)  
        run_exe(temp_folder + proc_name)  
    while True:  
        pass
```

LOW LEVEL X86 TRICKS

- “Red Pill” (Joanna Rutkowska, 11/2004)

```
1 int swallow_redpill () {  
2     unsigned char m[2+4], rpill[] = "\x0f\x01\x0d\x00\x00\x00\x00\xc3";  
3     *((unsigned*)&rpill[3]) = (unsigned)m;  
4     ((void(*)())&rpill)();  
5     return (m[5]>0xd0) ? 1 : 0; // return 1 if in VM  
6 }
```

- Why bother?





PROS & CONS



DEMO TIME!



<https://github.com/G4LB1T/TC2017>

QUESTIONS?

