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

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

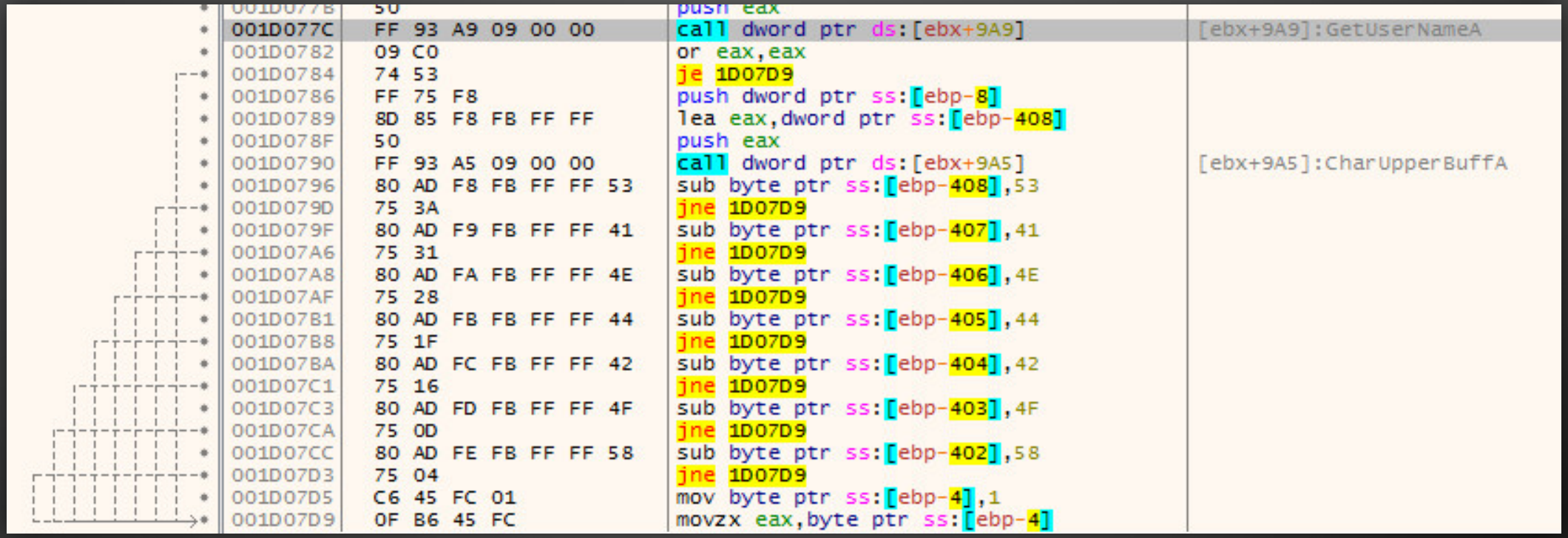
VIRTUALIZED\ANALYSIS ENVIRONMENT

```
    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



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

S A N D B O X !!!

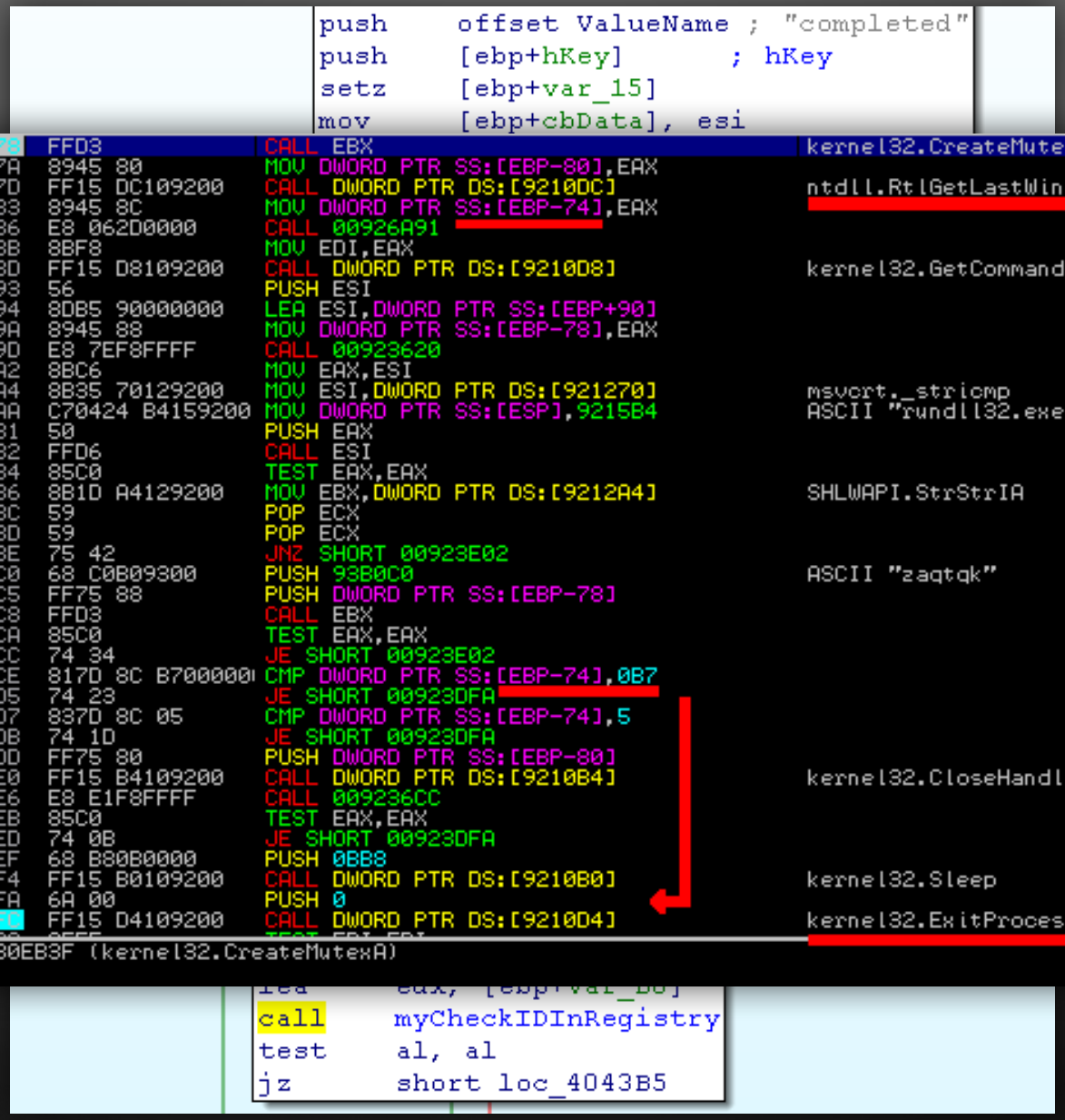
HEAVILY FORTIFIED TARGETS

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

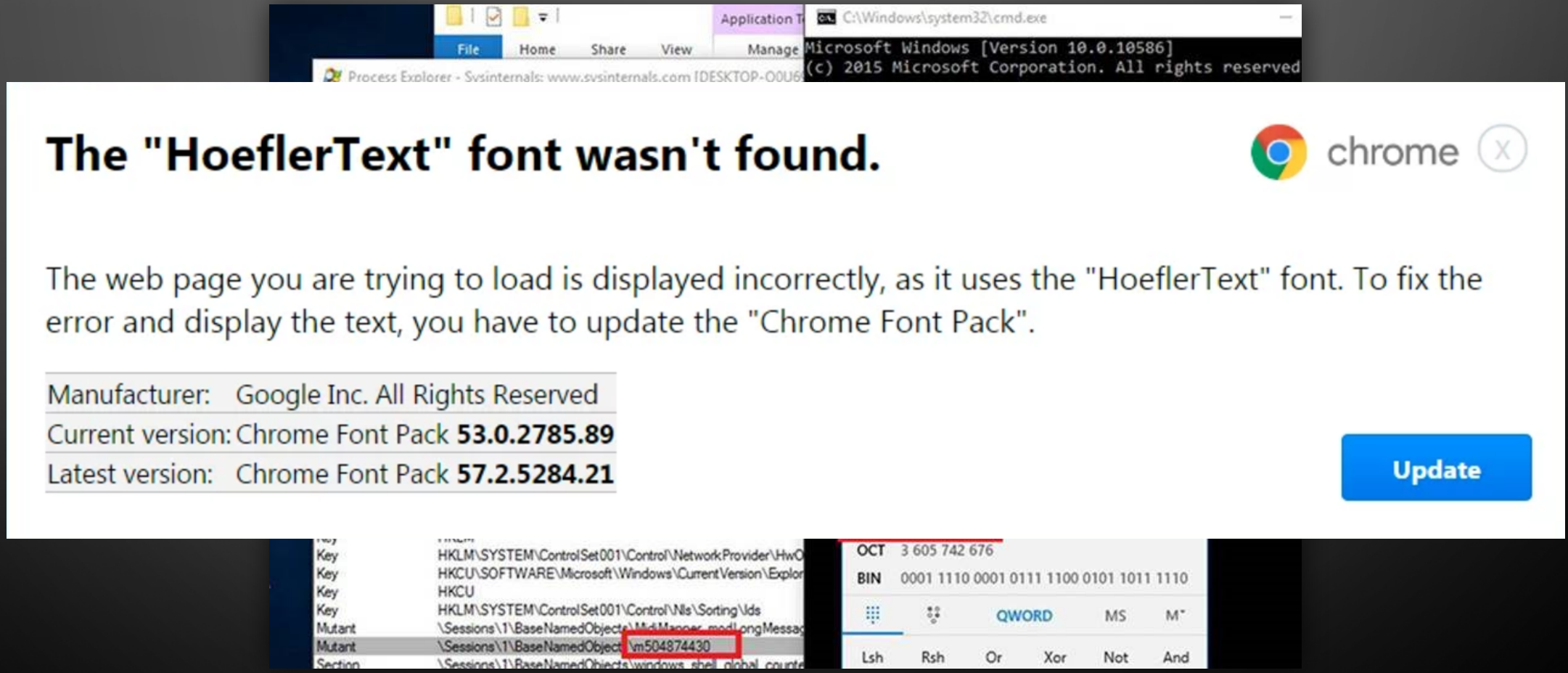
I KNOWZ SOFTWARE ENGEENIRINGZ

- Bugs in implementation of infection markers
- Abusing proper mechanisms

SYLVAIN SARMÉJEANNE
2/2016



…AND SPORA RANSOMWARE!



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 ke
- Registry va
- Files
- Folders

Can be crea

```
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 1,0
  - 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",
        "\\vmtoolsd.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?