- Recomendaciones.
- Modo de infección.
- Como identificarlo.

Las pruebas han sido realizadas en un entorno controlado, especial para análisis de Malware.

Ing. Kennedy Sanchez
Ms. Infosec, Ms. MGP, Ps. Auditoria, Security+, Ptest Certified

Windows SMB vulnerability (MS17-010).


wannacry

- Sistemas Vulnerables a WannaCrypt 2.0

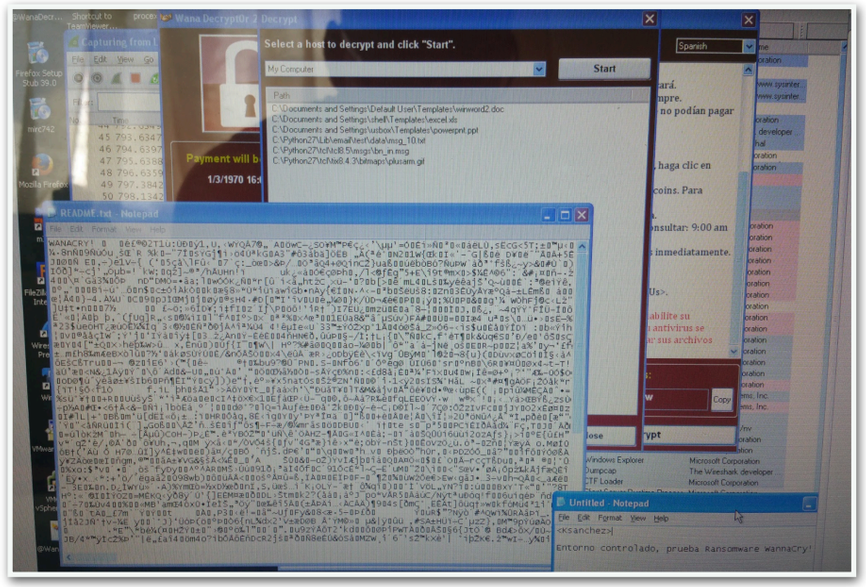
Vector: Todos las versiones de Windows antes de Windows 10 que no tengan el parcho **MS-17-010.**

- Metodo de Infección.

Explotation: El malware aprovecha una vulnerabilidad en el protocolo SMB y utiliza Eternalblue (exploits robados a la NSA).

Backdooring: El worm busca otros equipos en la red para ser infectados y corrompe los Shadow Copies de los equipos para que no se pueda hacer un recovery plan al sistema.

Crypto: Cada infección genera un llave (Keypair) RSA-2048.
Cada archivo es cifrado usando AES-128-CBC.



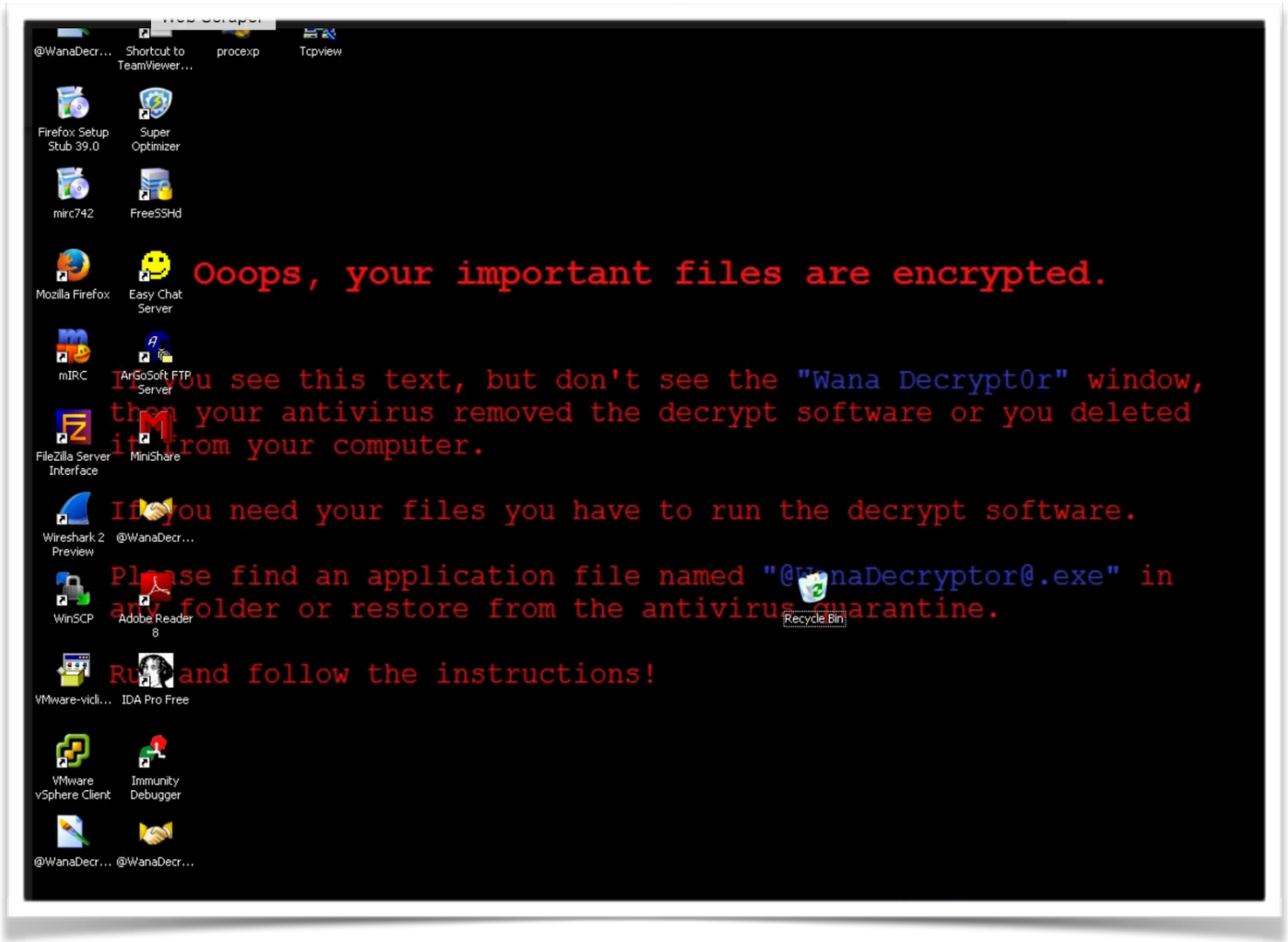
Ransomware WannaCrypt 2.0

Modo de infección

1- Verifica en internet si ya es cliente(ha pagado) y evita infectarlo nuevamente.

2- Si no puede verificar o no ha pagado procede a infectar el equipo y propagarse en la red.

• Pantalla PC Infectada.



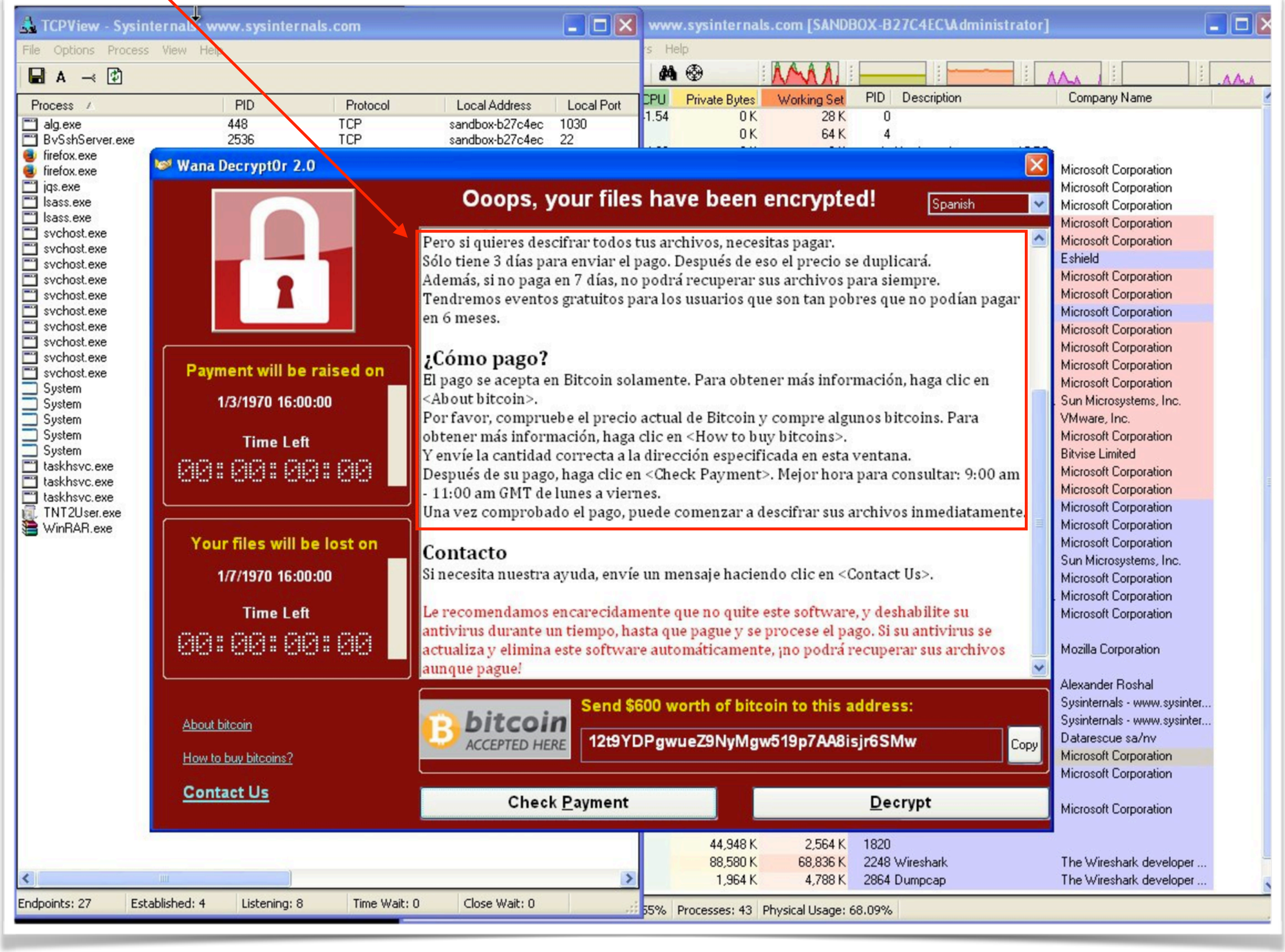
Today, ransomware is one of the biggest cyber threats in 2016. To avoid becoming a victim, you need to take action now to protect your computer systems. Waiting could cost you money, hassle, and negative publicity.

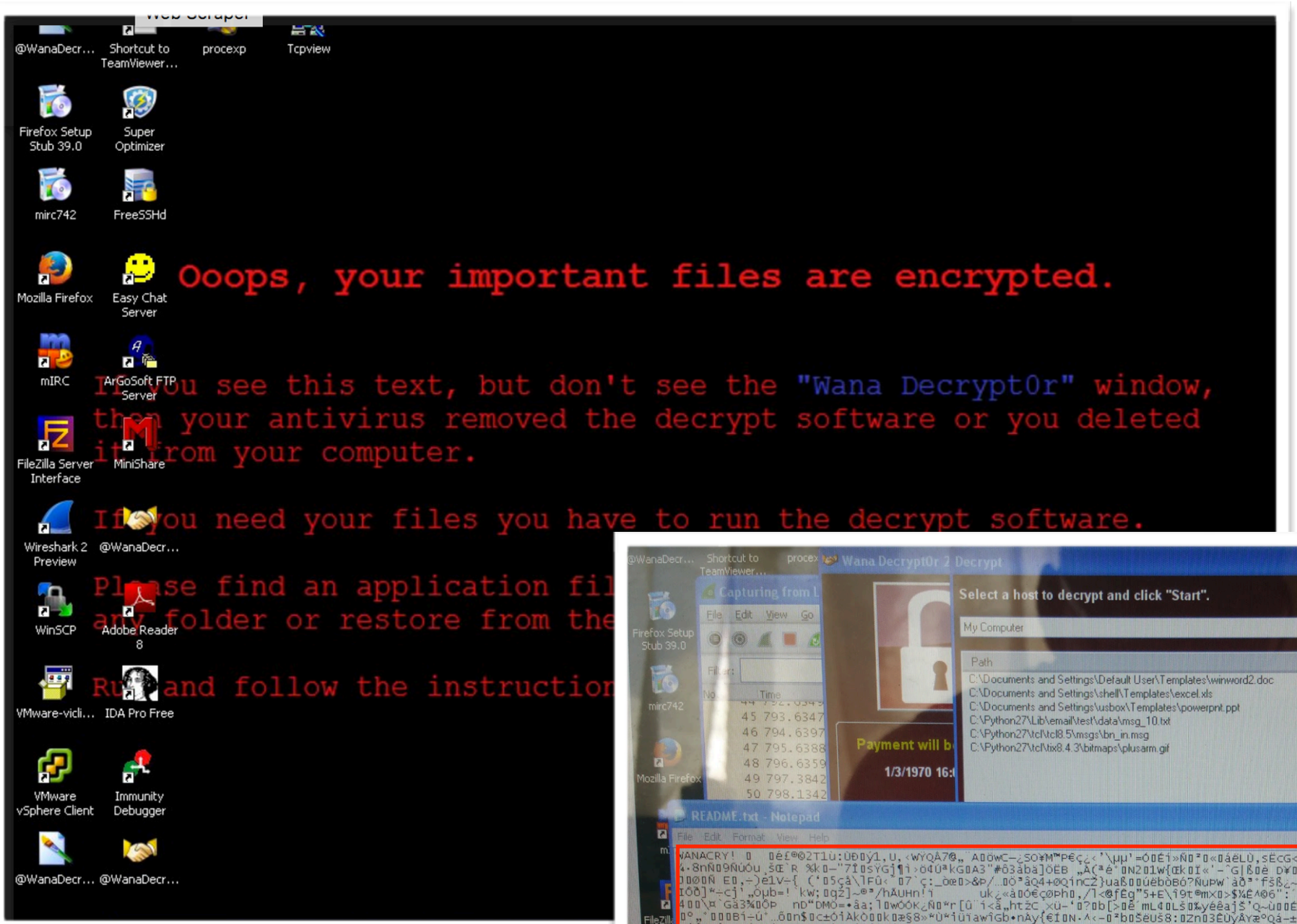
Si detecta una pantalla de este tipo, removerla de la red. Aunque probablemente las demás ya estén infectadas.

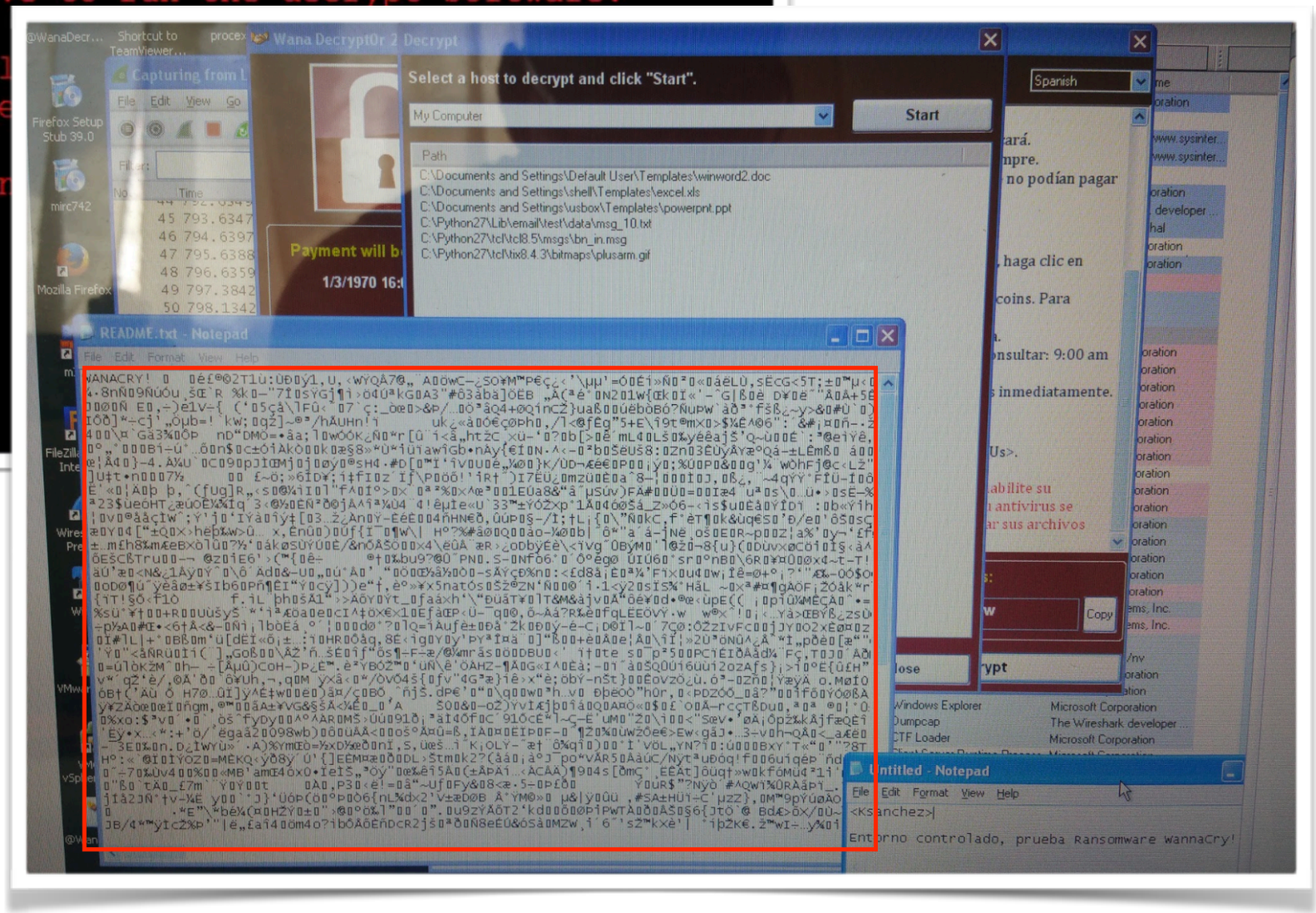
Algunas medidas preventivas:

- Realizar copias de seguridad en medios externos y que no estén permanente conectados.
- Ajustar reglas de Firewall, antimalwares y carpetas compartidas.
- Ajustar filtros de seguridad en el navegador
- Activar Firewall de los sistemas operativos (no importa que tengan Firewall de hardware).
- Actualizar sistemas operativos y antimalwares.
- Educar a los usuarios para que no abran archivos adjuntos si no están seguros que sea legítimo.
- Desactivar macros.

- **Asistencia de pago para descifrar la información.**







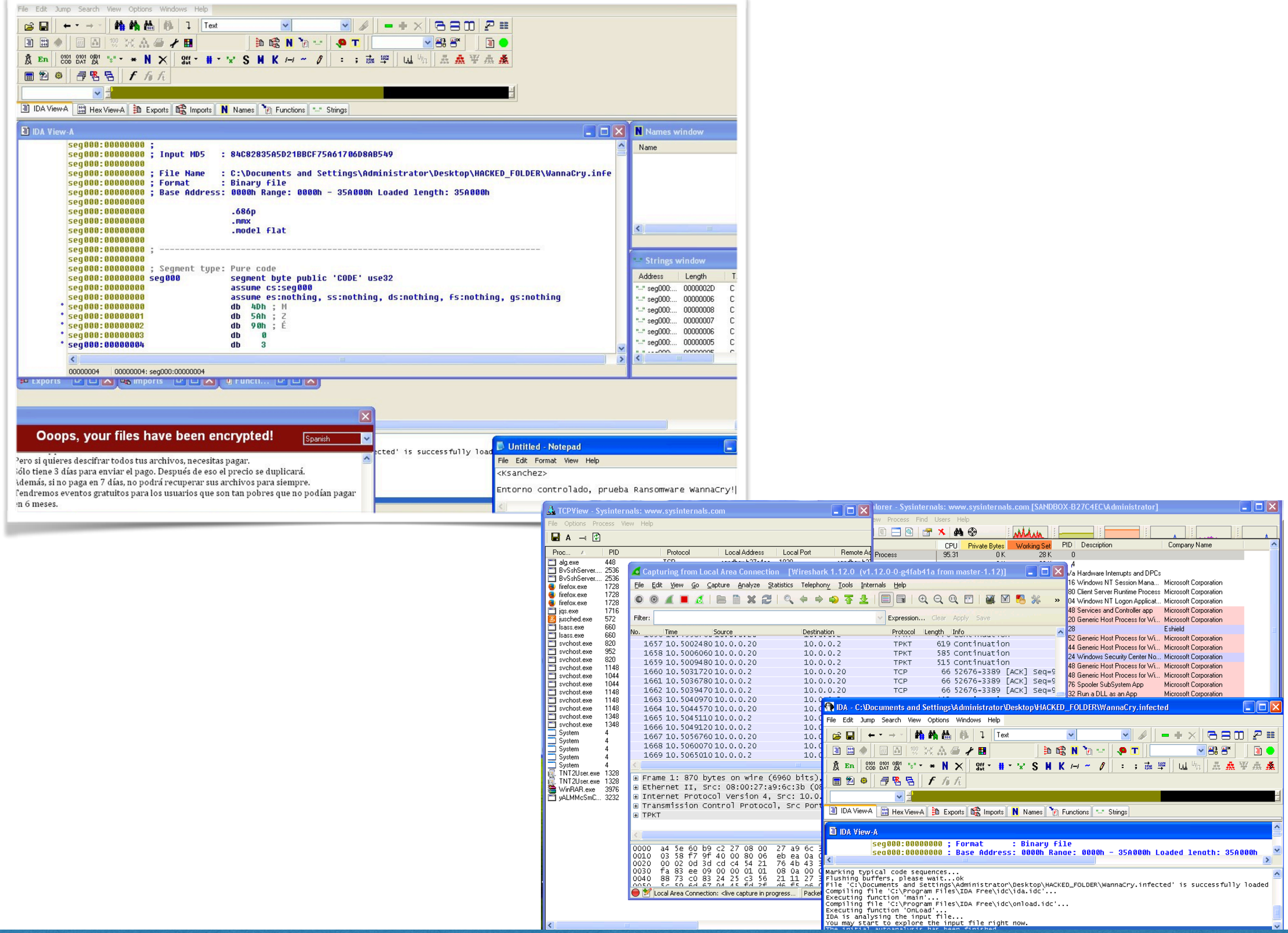
Resultado.

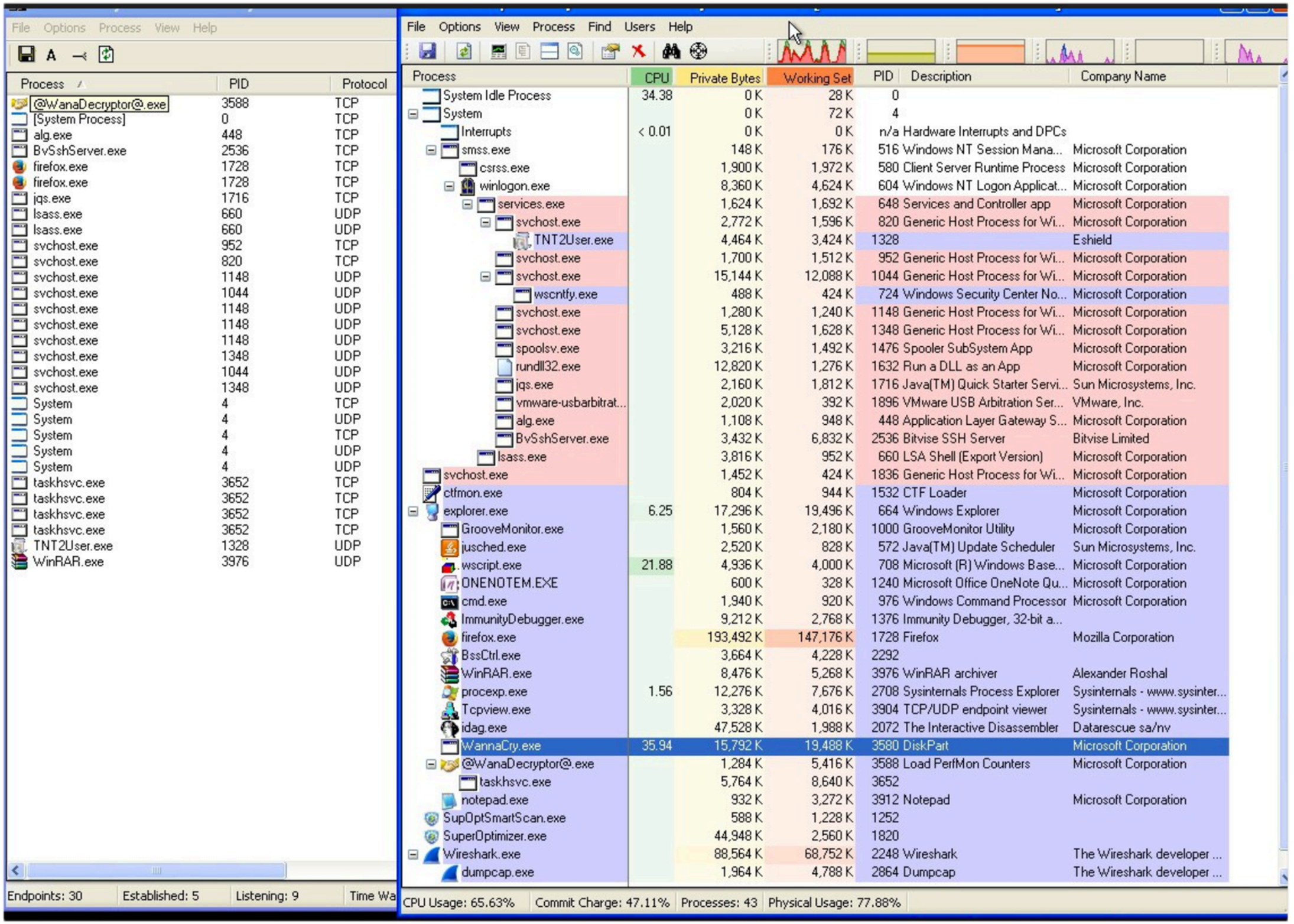
- Equipo infectado y propagación en la red, en busca de documentos compartidos y vulnerabilidades en protocolo SMB.

These numbers give us a perspective of how much hackers can make off of your data. But what does it actually cost a business to experience a data breach or loss of vital information? New findings from Juniper Research suggests that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. Furthermore, the average cost of a data breach in 2020 will exceed $150 million, as more business infrastructure gets connected.

Now, there are even more ways to get ransom out of the victim or the victim organization. Attackers can use Vouchers, BitCoins, Paysafecard, MoneyPak, UKash, CashU, and MoneXy to demand payment. All of this makes it easier to collect and easier for the victim to pay. However, just like with any monetary crime – the more victims pay, the more attacks we will be seeing. *So, whatever you do – avoid paying that ransom; if you can.*

MALWARE LAB


IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
seg000:00000000 ;
seg000:00000000 ; Input MD5 : 84C82835A5D21BBCF75A61706D8AB549
seg000:00000000 ; File Name : C:\Documents and Settings\Administrator\Desktop\HACKED_FOLDER\WannaCry.infe
seg000:00000000 ; Format : Binary file
seg000:00000000 ; Base Address: 0000h Range: 0000h - 35A000h Loaded length: 35A000h
.686p
.mmx
.model flat
seg000:00000000 ; Segment type: Pure code
seg000:00000000 seg000 segment byte public 'CODE' use32
assume cs:seg000
assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
db 4Dh ; M
db 5Ah ; Z
db 90h ; É
db 0
db 3
Names window
Name
Strings window
Address
Length
Ooops, your files have been encrypted!
Spanish
Pero si quieres descifrar todos tus archivos, necesitas pagar.
Sólo tiene 3 días para enviar el pago. Después de eso el precio se duplicará.
Además, si no paga en 7 días, no podrá recuperar sus archivos para siempre.
Tendremos eventos gratuitos para los usuarios que son tan pobres que no podían pagar
en 6 meses.
Untitled - Notepad
File Edit Format View Help
<Ksanchez>
Entorno controlado, prueba Ransomware WannaCry!
TCPView - Sysinternals: www.sysinternals.com
Capturing from Local Area Connection [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]
IDA - C:\Documents and Settings\Administrator\Desktop\HACKED_FOLDER\WannaCry.infected
Marking typical code sequences...
Flushing buffers, please wait...ok
File 'C:\Documents and Settings\Administrator\Desktop\HACKED_FOLDER\WannaCry.infected' is successfully loaded
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.


File Options Process View Help
Process PID Protocol
@WanaDecryptor@.exe 3588 TCP
[System Process] 0 TCP
alg.exe 448 TCP
BvSshServer.exe 2536 TCP
firefox.exe 1728 TCP
firefox.exe 1728 TCP
jqs.exe 1716 TCP
lsass.exe 660 UDP
lsass.exe 660 UDP
svchost.exe 952 TCP
svchost.exe 820 TCP
svchost.exe 1148 UDP
svchost.exe 1044 UDP
svchost.exe 1148 UDP
svchost.exe 1148 UDP
svchost.exe 1148 UDP
svchost.exe 1348 UDP
svchost.exe 1044 UDP
svchost.exe 1348 UDP
System 4 TCP
System 4 UDP
System 4 TCP
System 4 UDP
System 4 UDP
taskhsvc.exe 3652 TCP
taskhsvc.exe 3652 TCP
taskhsvc.exe 3652 TCP
taskhsvc.exe 3652 TCP
TNT2User.exe 1328 UDP
WinRAR.exe 3976 UDP
Endpoints: 30 Established: 5 Listening: 9 Time Wa
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 34.38 0 K 28 K 0
System 0 K 72 K 4
Interrupts < 0.01 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 148 K 176 K 516 Windows NT Session Mana... Microsoft Corporation
csrss.exe 1,900 K 1,972 K 580 Client Server Runtime Process Microsoft Corporation
winlogon.exe 8,360 K 4,624 K 604 Windows NT Logon Applicat... Microsoft Corporation
services.exe 1,624 K 1,692 K 648 Services and Controller app Microsoft Corporation
svchost.exe 2,772 K 1,596 K 820 Generic Host Process for Wi... Microsoft Corporation
TNT2User.exe 4,464 K 3,424 K 1328 Eshield
svchost.exe 1,700 K 1,512 K 952 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 15,144 K 12,088 K 1044 Generic Host Process for Wi... Microsoft Corporation
wscntfy.exe 488 K 424 K 724 Windows Security Center No... Microsoft Corporation
svchost.exe 1,280 K 1,240 K 1148 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 5,128 K 1,628 K 1348 Generic Host Process for Wi... Microsoft Corporation
spoolsv.exe 3,216 K 1,492 K 1476 Spooler SubSystem App Microsoft Corporation
rundll32.exe 12,820 K 1,276 K 1632 Run a DLL as an App Microsoft Corporation
jqs.exe 2,160 K 1,812 K 1716 Java(TM) Quick Starter Servi... Sun Microsystems, Inc.
vmware-usbarbitrat... 2,020 K 392 K 1896 VMware USB Arbitration Ser... VMware, Inc.
alg.exe 1,108 K 948 K 448 Application Layer Gateway S... Microsoft Corporation
BvSshServer.exe 3,432 K 6,832 K 2536 Bitvise SSH Server Bitvise Limited
lsass.exe 3,816 K 952 K 660 LSA Shell (Export Version) Microsoft Corporation
svchost.exe 1,452 K 424 K 1836 Generic Host Process for Wi... Microsoft Corporation
ctfmon.exe 804 K 944 K 1532 CTF Loader Microsoft Corporation
explorer.exe 6.25 17,296 K 19,496 K 664 Windows Explorer Microsoft Corporation
GrooveMonitor.exe 1,560 K 2,180 K 1000 GrooveMonitor Utility Microsoft Corporation
jusched.exe 2,520 K 828 K 572 Java(TM) Update Scheduler Sun Microsystems, Inc.
wscript.exe 21.88 4,936 K 4,000 K 708 Microsoft (R) Windows Base... Microsoft Corporation
ONENOTEM.EXE 600 K 328 K 1240 Microsoft Office OneNote Qu... Microsoft Corporation
cmd.exe 1,940 K 920 K 976 Windows Command Processor Microsoft Corporation
ImmunityDebugger.exe 9,212 K 2,768 K 1376 Immunity Debugger, 32-bit a...
firefox.exe 193,492 K 147,176 K 1728 Firefox Mozilla Corporation
BssCtrl.exe 3,664 K 4,228 K 2292
WinRAR.exe 8,476 K 5,268 K 3976 WinRAR archiver Alexander Roshal
procexp.exe 1.56 12,276 K 7,676 K 2708 Sysinternals Process Explorer Sysinternals - www.sysinter...
Tcpview.exe 3,328 K 4,016 K 3904 TCP/UDP endpoint viewer Sysinternals - www.sysinter...
idag.exe 47,528 K 1,988 K 2072 The Interactive Disassembler Datarescue sa/nv
WannaCry.exe 35.94 15,792 K 19,488 K 3580 DiskPart Microsoft Corporation
@WanaDecryptor@.exe 1,284 K 5,416 K 3588 Load PerfMon Counters Microsoft Corporation
taskhsvc.exe 5,764 K 8,640 K 3652
notepad.exe 932 K 3,272 K 3912 Notepad Microsoft Corporation
SupOptSmartScan.exe 588 K 1,228 K 1252
SuperOptimizer.exe 44,948 K 2,560 K 1820
Wireshark.exe 88,564 K 68,752 K 2248 Wireshark The Wireshark developer ...
dumpcap.exe 1,964 K 4,788 K 2864 Dumpcap The Wireshark developer ...
CPU Usage: 65.63% Commit Charge: 47.11% Processes: 43 Physical Usage: 77.88%