

- 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 2.0

• Sistemas Vulnerables a WannaCrypt 2.0

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

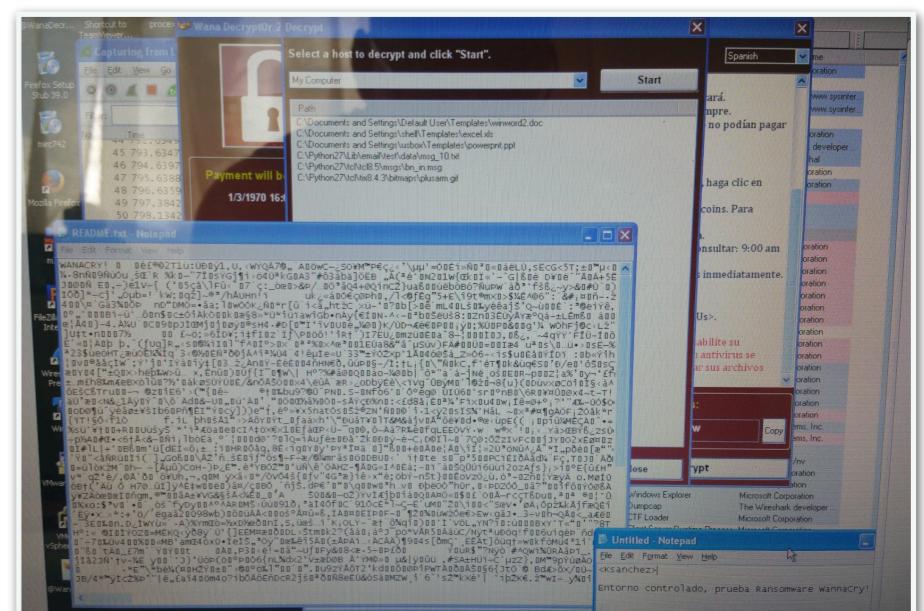


• Método de Infección.

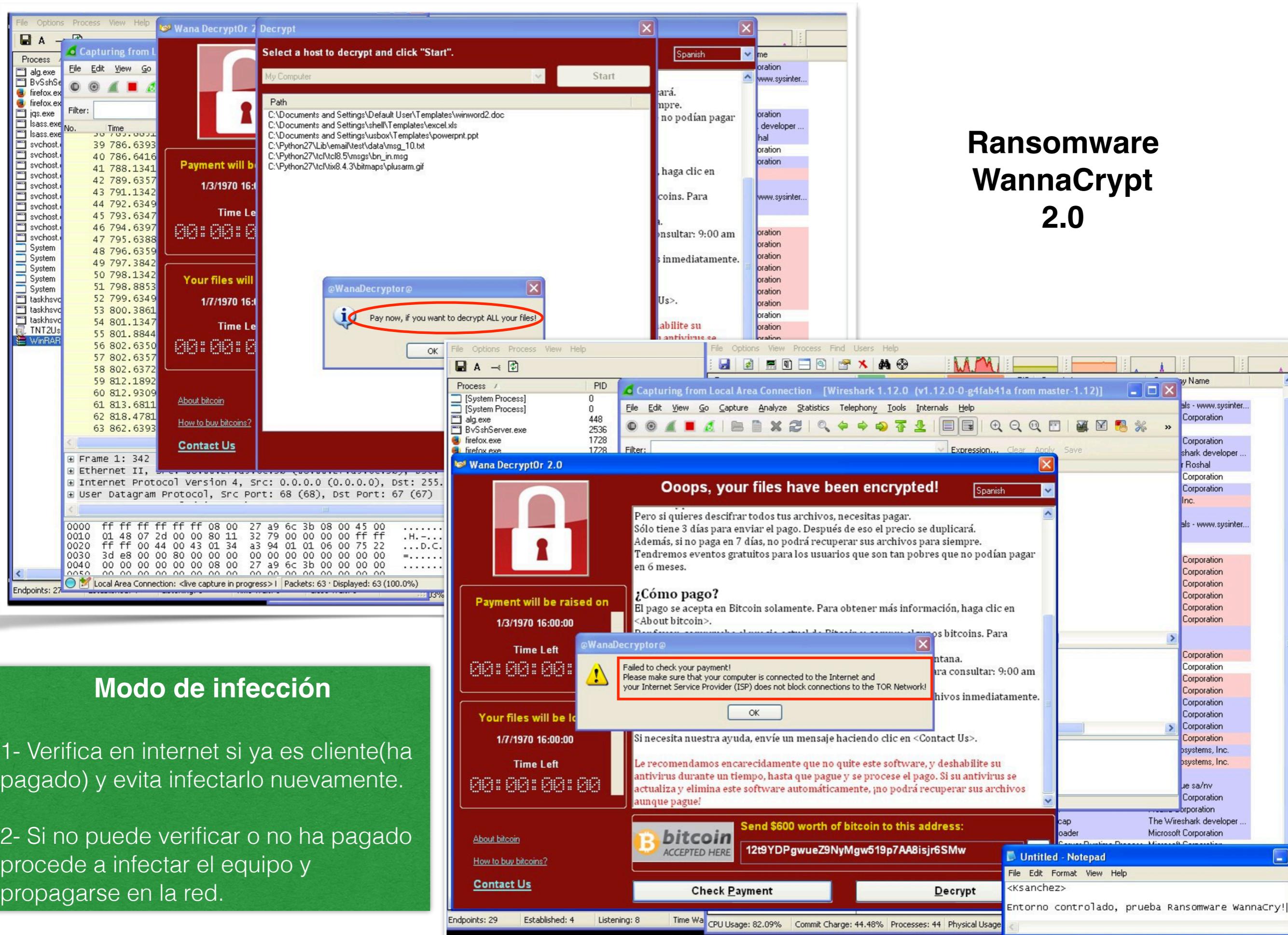
Exploitation: El malware aprovecha una vulnerabilidad en el protocolo SMB y utiliza Eternalblue (exploits robados a la NSA).

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.



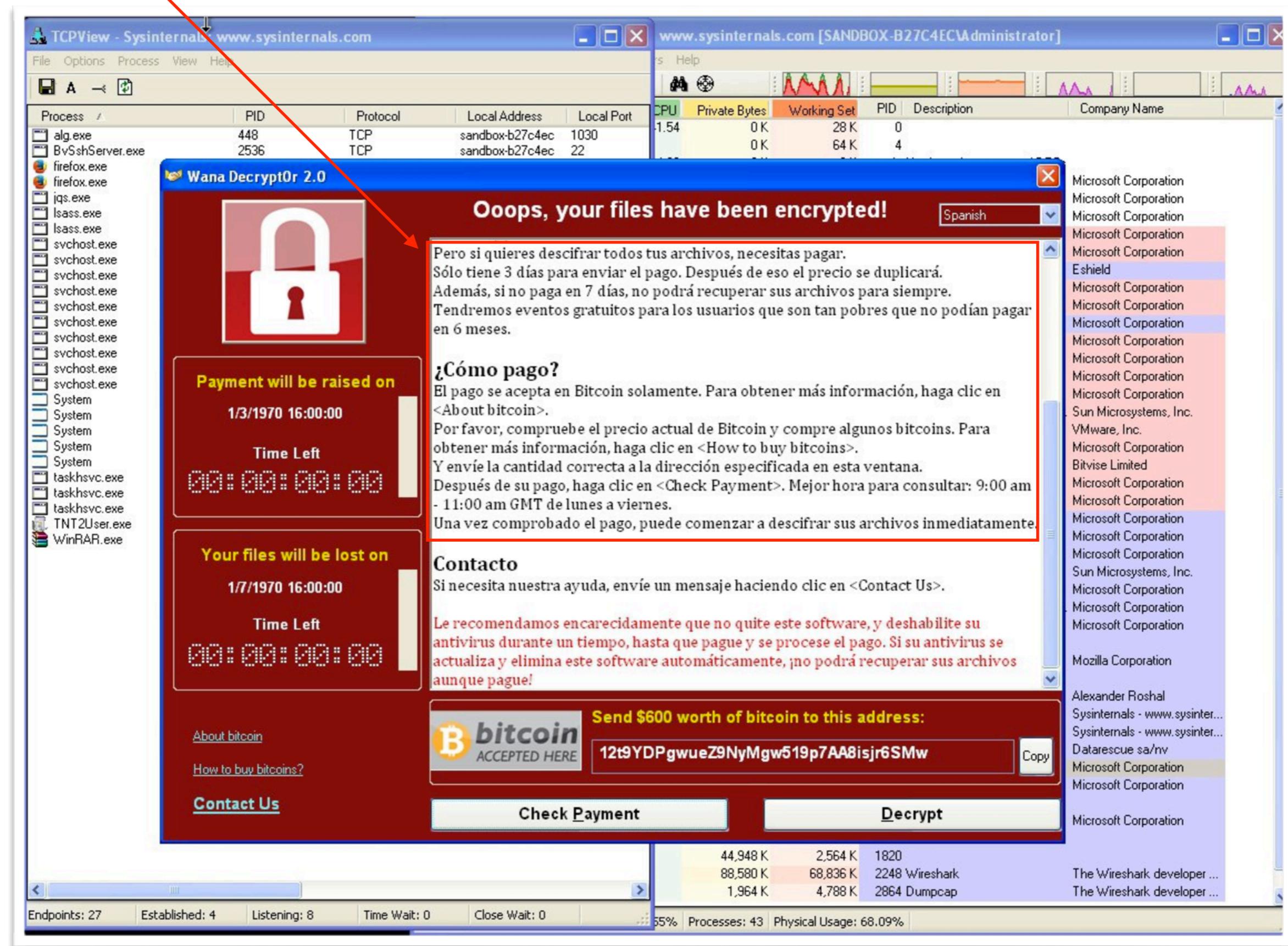
Si detecta una pantalla de este tipo, removerla de la red. Aunque probablemente las demás ya estén infectadas.

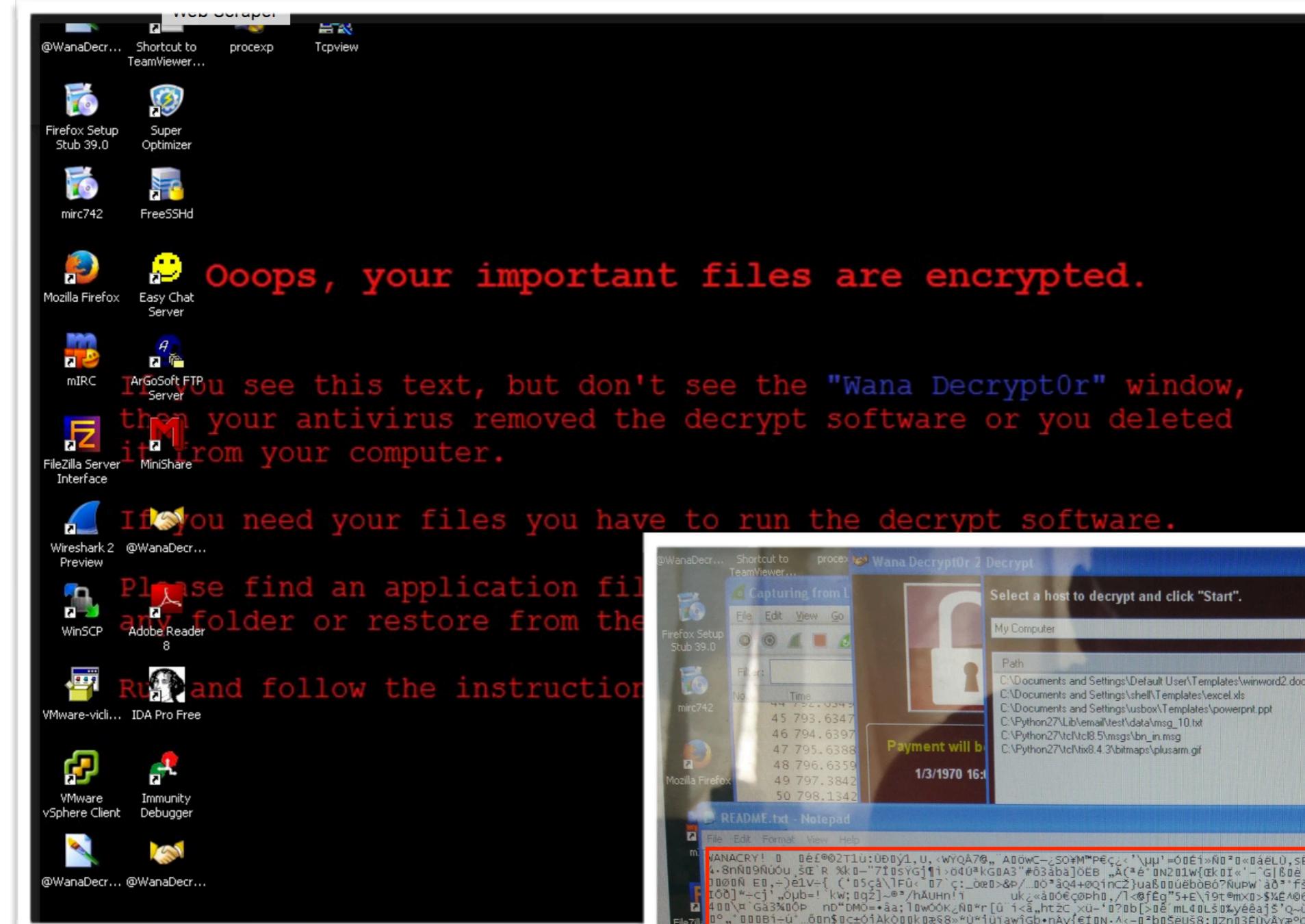
Today, ransomware is one of the biggest cyber threats in 2016. To avoid becoming a victim, you need to take action now to protect your computer systems. Waiting could cost you money, hassle, and negative publicity.

Algunas medidas preventivas:

- Realizar copias de seguridad en medios externos y que no estén permanentemente 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.

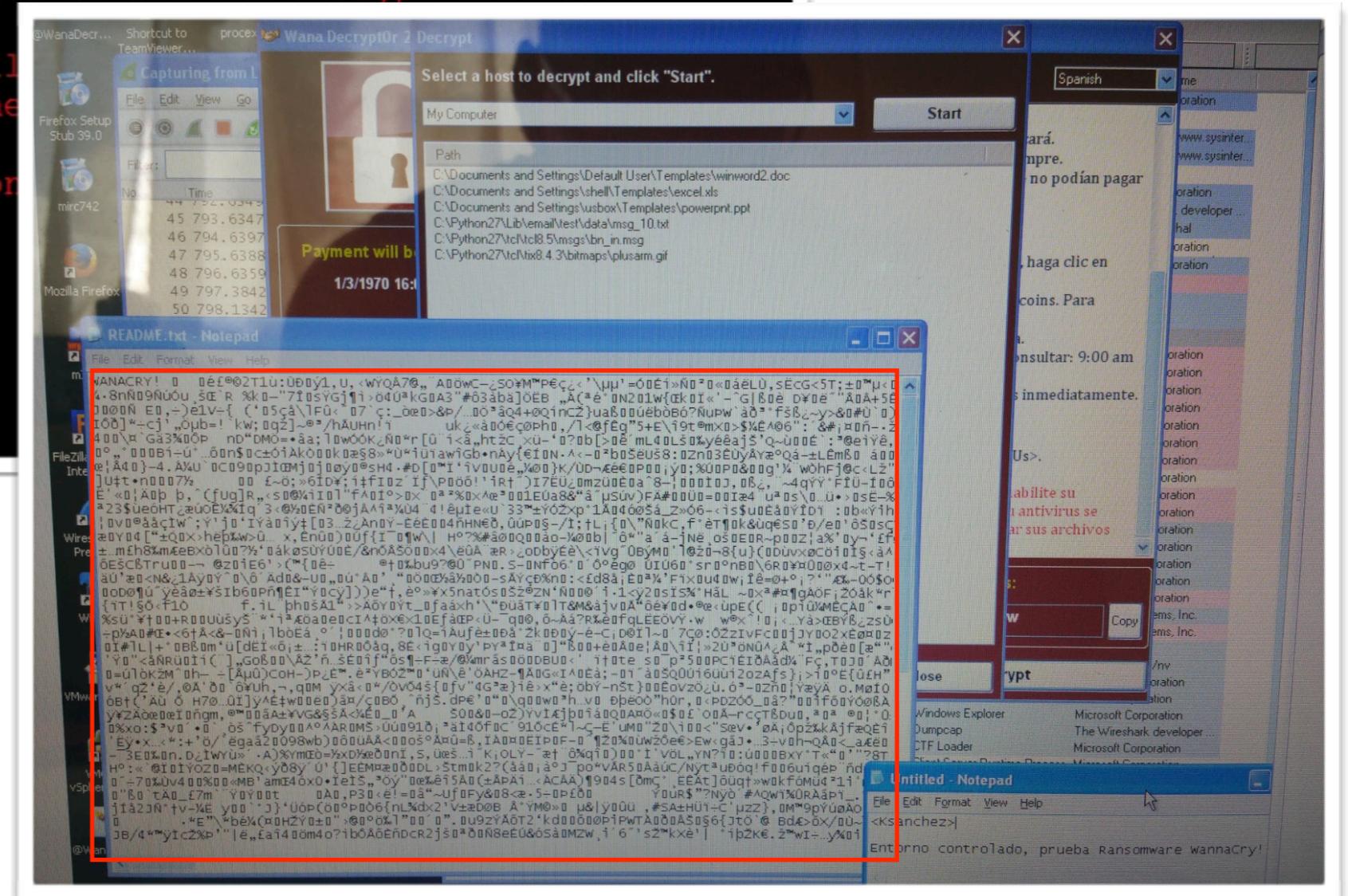
• Asistencia de pago para descifrar la información.





Resultado.

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



ESSENTIAL GUIDE TO: RANSOMWARE: DETECTING THREATS AND PROTECTING YOUR DATA

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

