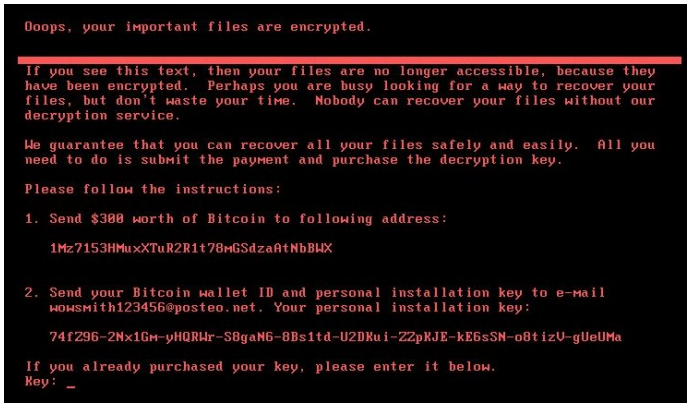
Petya: los expertos en seguridad te explican el ataque

Ayer un ransomware, bautizado como Petya, se expandió por equipos de todo el mundo en muy pocas horas, como ya hiciera hace unas semanas el WannaCry. Este tipo de ataques nos recuerdan que nuestra información es mucho más vulnerable de lo que creemos cuando interactuamos día a día con nuesrtos dispositivos.

Diversas empreasde seguridad han querido dar su opinión al respecto y explicar la situación y aquí tienes la información, para conocer un poco más del malware Petya:



–**Trend Micro**: La entrada inicial de este ransomware en el sistema implica el uso de la herramienta **PsExec**, una herramienta oficial de **Microsoft** utilizada para ejecutar procesos en sistemas remotos. También utiliza la **vulnerabilidad de EternalBlue - previamente empleada en el ataque de WannaCry-** que se dirige a una vulnerabilidad en Server Message Block (SMB) v1. Una vez en un sistema, esta variante Petya utiliza el proceso rundll32.exe para ejecutarse por sí misma. Este ransomware añade entonces una tarea programada, que reinicia el sistema después de al menos una hora.

-Kaspersky Lab: Los **cibercriminales están pidiendo 300 dólares en Bitcoins por facilitar la "llave" o clave que descifrará los datos secuestrados**, y el pago a través de una cuenta unificada de Bitcoin. A diferencia de **WannaCry**, esta técnica podría funcionar porque los ciberdelincuentes han pedido a las víctimas que envíen sus números de cuenta por correo electrónico a "wowsmith123456@posteo.net" para confirmar las transacciones. Sin embargo, desde Kaspersky Lab se ha detectado que esta cuenta de correo electrónico ya ha sido cerrada, lo que hace que el descifrado sea imposible.

–**Fortinet**: Este nuevo malware **forma parte de una nueva ola de ataques ransomware multi-vector, que hemos llamado "ransomworm"**, y que aprovecha determinados exploits. El ransomworm está diseñado para moverse a través de múltiples sistemas de forma automática, en lugar de permanecer quieto. Parece que el ransomworm Petya está utilizando vulnerabilidades actuales similares a las que fueron explotadas durante el ataque de Wannacry. De forma preventiva, Fortinet recomienda establecer una rutina para aplicar los parches del Sistema Operativo, el Software y el Firmware de todos los dispositivos. Además de instalar algún antivirus.

–**Eset**: Las investigaciones indican que el ataque habría comenzado en Ucrania, el país más afectado al momento. Se puede observar que Ucrania es el país más afectado mientras que e**n Latinoamérica, el de mayor impacto, hasta el momento es Argentina**.