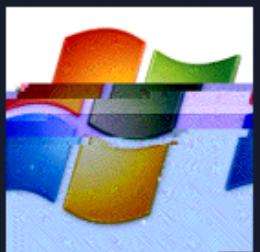


EternalBlue: el exploit que cambió la ciberseguridad

X



Blue

Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

Easy 30 min



Patricio Burattini

Imagina un salón oscuro en las entrañas de la Agencia de Seguridad Nacional de Estados Unidos (NSA) hacia mediados de la década de 2000.

Allí, un equipo de criptógrafos y analistas rebuscaba vulnerabilidades en protocolos críticos de Windows: encontraban fallos, los documentaban... y en lugar de alertar a Microsoft, los guardaban celosamente en su arsenal para operaciones de inteligencia.

Uno de esos hallazgos fue una grieta profunda en el protocolo de archivos y comunicaciones SMBv1, capaz de ejecutar código arbitrario en sistemas remotos.

La NSA le llamó internamente “EternalBlue” y lo conservó en secreto por años, preparándolo como una poderosa herramienta de intrusión



Patricio Burattini

A mediados de abril de 2017, un misterioso grupo bautizado Shadow Brokers sorprendió al mundo filtrando un paquete llamado FuzzBunch, en el que se incluía EternalBlue.

Microsoft, que para entonces ya había sido alertada por la NSA del robo inminente, publicó el 14 de marzo de 2017 el boletín de seguridad MS17-010, con parches que corregían varias vulnerabilidades críticas en SMBv1.

Sin embargo, muchas organizaciones tardaron en aplicarlos: el mantenimiento de sistemas heredados y la falta de conciencia dejaron millones de máquinas expuestas.



Pocos días después de la filtración, el 12 de mayo de 2017, estalló WannaCry, un ransomware que se aprovechó de EternalBlue para propagarse de manera autónoma entre equipos con Windows sin parchear.

En cuestión de horas, hospitales en el Reino Unido detuvieron cirugías, fábricas en España paralizaron líneas de producción y usuarios de todo el mundo vieron sus archivos cifrados a cambio de un rescate en bitcoin.

Fue la primera gran demostración de la letalidad de un exploit nacido en inteligencia de Estado, convertido en arma masiva por ciberdelincuentes.



Patricio Burattini

Pero WannaCry no fue el único.

El 27 de junio de 2017, NotPetya utilizó de nuevo EternalBlue como vector de entrada, esta vez disfrazado de un ataque contra Ucrania que rápidamente cruzó fronteras y causó más de mil millones de dólares en daños, afectando desde compañías logísticas hasta centrales eléctricas.

Y aunque Microsoft amplió los parches de emergencia incluso para sistemas fuera de soporte (Windows XP, 8, Server 2003), la sombra de EternalBlue persistió.



Patricio Burattini

Con el tiempo, investigadores de seguridad portaron EternalBlue a prácticamente todas las versiones de Windows desde 2000 hasta 2018, integrándolo en Metasploit y en varias herramientas de pentesting.

A día de hoy, en entornos corporativos mal gestionados o en dispositivos de IoT olvidados, sigue siendo posible ejecutar código arbitrario con un solo paquete SMB especialmente construido.

SMBv1, hoy desaconsejado y muchas veces bloqueado en cortafuegos internos, pasó a enseñarse en todas las formaciones de ciberseguridad como un caso de estudio clásico.



Patricio Burattini

La repercusión de EternalBlue cambió la industria:

- **Cultura de parches inmediata:** arrancó la práctica de aplicar parches críticos en 48 horas.
- **Desactivación de SMBv1:** Microsoft tomó la drástica medida de renunciar a un protocolo que llevaba funcionando desde 1992, recomendando su exclusión total.
- **Debate ético sobre vulnerabilidades de Estado:** hizo saltar las alarmas al revelarse que la NSA había “almacenado” agujeros en software en vez de corregirlos, cuestionando el equilibrio entre seguridad nacional y protección ciudadana.
- **Conciencia global:** gobiernos y empresas comprendieron que la superficie de ataque no era sólo un asunto de IT, sino de continuidad de negocio y seguridad pública



Patricio Burattini

Hoy, ocho años después de su filtración, EternalBlue sigue siendo un recordatorio de que un solo exploit sin gestionar puede desencadenar crisis globales.

Para conmemorarlo como se merece, en mi portfolio van a encontrar un write-up acerca de Blue, una máquina de tryhackme inspirada en éste exploit que va a quedar tallado en la memoria de todos.

MEDIUM: <https://bit.ly/4k8ISot>

WRITE-UP: <https://bit.ly/43EXYLM>