proactive
Information security.

# Ayudamos a Proteger sus Activos de Información


## ProActive News Vol.1

## ¿Qué pasó con la NSA?

El 14 de abril redes sociales y portales sobre seguridad se hacían eco de una inquietante filtración. La noticia señalaba como víctima a la NSA *National Security Agency* (NSA) organismo de seguridad de los Estados Unidos de Norteamerica y como protagonistas al grupo de hackers conocidos como ***The Shadow Brokers*** quienes a través de un t*weet* exponían un enlace que dejaba al descubierto un arsenal de exploits que hasta entonces solo estaba a disposición de los agentes de la NSA.

## ¿En qué consistió la filtración?

Entre la información filtrada se dio a conocer una variedad de exploits, algunos *Zero Days* y también una plataforma llamada "*FuzzBunch*", esta última muy similar a plataforma de Metasploit, en la cual es posible cargar módulos y configurar parámetros como "RHOST" y "LHOST" para obtener fácilmente una ***shell*** reversa sin interacción de terceras partes.

## ¿Estoy seguro? ¿Qué exploits se han liberado?

En realidad uno nunca sabe que tan segura se encuentra la infraestructura de su organización, menos aún si no práctica de manera habitual un Test de Intrusión para medir de alguna manera a que se encuentra expuesta. No obstante esta filtración sin lugar a dudas amplió horizontes a la hora de llevar a cabo intrusiones, a continuación se expone un resumen que deja expuesta la información sobre los exploits descubiertos:

| EXPLOIT | DESCRIPCION | ACTUALIZACIÓN | SERVICIO | PLATAFORMA |
|---|---|---|---|---|
| Easypi | Exploit para Lotus cc:Mail | - | LOTUS MAIL | Windows NT, 2000, XP, 2003 |
| Eclipsedwing | Exploit SMB para 2000, 2003 y XP | MS08-067 | SMB | Windows 2000, XP, 2003 |
| Educatedscholar | Exploit SMB | MS09-050 | SMB | Windows Vista. 2008 |
| Emeraldthread | Exploit SMB para XP y 2003 dropea un implant al estilo de Stuxnet | - | SMB | Windows XP, 2003 |

| EXPLOIT | DESCRIPCION | ACTUALIZACIÓN | SERVICIO | PLATAFORMA |
|---|---|---|---|---|
| Erraticgopher | Exploit para SMB, probado en XP y 2003. Zero day, no será parcheado | - | SMB | Windows XP, 2003 |
| Eskimoroll | Exploit para Kerberos contra controladores de dominio con plataformas Windows Server 2000, 2003, 2008 y 2008 R2 | MS14-068 | KERBEROS SERVIC | Windows 2000, 2003, 2008 |
| Esteemaudit | Exploit remoto afecta al protocolo RDP (Remote Desktop) en plataformas Windows Server 2003 y XP, instala un implant. Probado, funciona con autenticación por SmartCard. Zero day, no será parcheado. | - | RDP | Windows XP, 2003 |
| Eternalblue | Exploit para SMBv1 probado y funcionando. Remoto, no requiere autenticación, funciona contra Windows Server 2008 R2 | MS17-010 | SMB | Windows XP, 2003, Vista, 2008, 7 |
| Eternalchampion | Exploit SMB. Funcional. Corregido en CVE-2017–0147. | CVE-2017-0146 & CVE-2017-0147 | | Windows |
| Eternalromance | Exploit remoto para SMB1 afecta a plataformas Windows XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2. Probado, funciona. | MS17-010 | SMB | Windows XP, 2003, Vista, 2008, 7 |
| Eternalsynergy | Exlploit de ejecución remota de codigo para SMB | MS17-010 | SMB | Windows 8, 2012 |
| Ewokfrenzy | Exploit para Lotus Domino 6 & 7 | - | LOTUS DOMINO | Windows |
| Explodingcan | Exploit para Microsoft IIS 6. explota WebDav solo en Windows Server 2003, no será parcheado. | - | IIS6.0 | Windows 2003 |
| Zippybeer | Exploit contra controlador de dominio Microsoft, Requiere autenticación | - | SMB | Windows |

Desde el laboratorio de **ProActive**, realizamos una prueba de concepto utilizando uno de los más peligrosos *exploits* liberados denominado ***EternalBlue***, para ver el video siga el enlace:

*https://drive.google.com/file/d/0B38did9zITfESmRLNHRCNFhvSGs/view?usp=sharing*

Con objeto de mantenerlo actualizado y protegido, quedamos a vuestra disposición para asesorarlo en cuanto a la detección de vulnerabilidades en su plataforma que puedan ser explotadas por los recientes exploits filtrados.

Obtenga mayor información sobre nuestros servicios y productos, póngase en contacto con nosotros:

Web: www.proactive.consulting

Mail: contacto@proactive.consulting

Tel: +595 (981) 478-921

Twitter: @ProActive_py