Problemas de Microsoft para corregir versiones antiguas de IE

Microsoft ha publicado una solución rápida para una vulnerabilidad en las versiones antiguas de su navegador Internet Explorer que está siendo utilizada activamente por atacantes para tomar el control de las computadoras.

La vulnerabilidad afecta a las versiones de IE 6, 7 y 8. Las últimas versiones del navegador, 9 y 10, no se ven afectados. La compañía de vez en cuando emite soluciones rápidas como medida de protección temporal mientras una actualización de seguridad permanente se desarrolla si una vulnerabilidad se considera especialmente peligrosa.

Microsoft publicó un aviso de advertencia del problema, que consiste en cómo IE accede a "***un objeto en la memoria que se ha eliminado o no se ha asignado correctamente.***" El problema corrompe la memoria del navegador, lo que permite a los atacantes ejecutar su propio código.

La vulnerabilidad puede ser explotada mediante la manipulación de una página web con el fin de atacar a los navegadores vulnerables, uno de los tipos más peligrosos de los ataques conocidos como descarga drive-by. Las víctimas sólo tiene que visitar el sitio manipulado para que su computadora se infecte. Para tener éxito, el atacante tendría que atraer a la persona a la página web atacante, que normalmente se realiza mediante el envío de un enlace malicioso por correo electrónico.

El proveedor de seguridad Symantec describe este escenario como un "***pozo de agua***", donde las víctimas se perfilan y luego

atraídos a visitar el sitio malicioso. Uno de los sitios descubiertos de haber sido manipuladas para entregar un ataque fue la del Consejo de Relaciones Exteriores.

El ataque se entrega en una pieza de software malicioso apodado Bifrose, una familia de malware detectado por primera vez alrededor de 2004. Bifrose crea una "***puerta trasera***" que permite a un atacante robar archivos desde un ordenador. Symantec escribió que los ataques con la vulnerabilidad de IE parece ser limitada y se concentra en América del Norte, lo que indica una campaña de ataque dirigido.

Desde los ataques en curso antes de la vulnerabilidad fue descubierta, Symantec dijo que "***sugiere un alto nivel de sofisticación que requiere el acceso a los recursos y habilidades que normalmente estarían fuera de la mayoría de las capacidades de los hackers***".