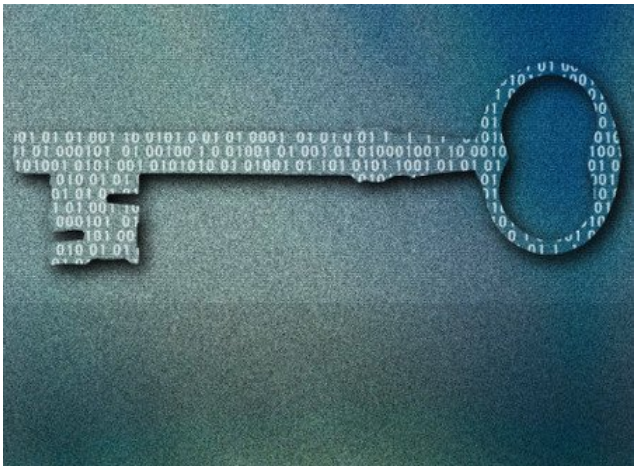
Malware ‘Skeleton Key’ Desbloquea Las Redes Corporativas



En la actualidad existen diferentes amenazas que afectan la seguridad en un sitio web, comprometiendo los datos mas sensibles de una empresa o de los usuarios. Existen diversas herramientas que se pueden encontrar en la web para vulnerar los diferentes sitios. Ademas de las diversas herramientas, se lanzan a menudo programas maliciosos como el malware, recientemente ha sido descubierto «**Skeleton Key**«, el cual es capaz de eludir la autenticación en sistemas de Active Directory, de acuerdo con investigadores de Dell.

Según los investigadores de seguridad, el **malware «Skeleton Key»** permite a los ciberdelincuentes eludir los sistemas de AD que sólo implementan un sistema de autentificación. El equipo dice que los hackers pueden utilizar una contraseña de su elección para registrarse como cualquier usuario, antes de escudriñar en la red (desbloquear las redes corporativas) y hacer lo que les plazca. **Skeleton Key** fue descubierto en la red de un cliente que utiliza contraseñas para el acceso a los servicios de correo electrónico y VPN. El malware, una vez desplegado como un parche en memoria en el **controlador de dominio AD de un sistema**, le dio a los cibercriminales acceso sin restricciones a los servicios de acceso remoto. Sin embargo, los usuarios legítimos pudieron continuar con normalidad, ignorando felizmente de la presencia del malware o suplantación.

«Evitar la autenticación Clave del esqueleto también permite a los actores amenaza con acceso físico al inicio de sesión y desbloquear los sistemas de autenticación de los usuarios en contra de los controladores de dominio de AD comprometidos», dicen los investigadores de CTU.

Esto significa que un atacante puede pasar por cualquier usuario sin alertar a los demás o restringir el acceso de los usuarios legítimos. ¿Por qué molestarse? La respuesta es simple. Puede que no sea el tipo más sofisticado de ataque, pero su característica principal es el bajo perfil.

Sin duda esto es algo preocupante, ya que empleados molestos podrían hacerse pasar por sus jefes y tomar información importante y sensible que se podría usar con alguna finalidad distinta al objetivo de la empresa. Sin embargo, existe otra debilidad en el software malicioso, la necesidad de una redistribución constante para operar **cada vez que se inicia el controlador de dominio**. También se cree que Skeleton Key sólo será compatible con las versiones de Windows de 64 bits.

«Entre las ocho horas y ocho días de un reinicio, los actores de amenazas utilizan otros tipos de malware de acceso remoto ya desplegados en la red de la víctima para redistribuir Skeleton Key en los controladores de dominio», dice el equipo de seguridad.

El malware no transmite el tráfico de red, por lo que puede ser más difícil de detectar por los sistemas de prevención de intrusos IDS/IPS. En estos casos, es necesario reiniciar para resolver el problema. Para evitar que el malware que afecta a

su red, la autenticación de dos pasos es el mejor camino a seguir.