# WEBIMPRINTS

Empresa de pruebas de penetración

Empresa de seguridad informática

http://www.webimprints.com/seguridad-informatica.html

# Macro Malware

# Macro Malware

Según Webimprints una empresa de pruebas de penetración, esta amenaza actualizada está dirigida a los usuarios de las grandes organizaciones que con frecuencia utilizan macros. Cuidadosamente elaborado y correos electrónicos de ingeniería social atraen a los usuarios abrir documentos aparentemente legítimos y luego activar la macro. Los blancos más populares de malware macro son documentos de Microsoft Office, especialmente los archivos de Word. Word permite macros se ejecuten de forma automática, por ejemplo, cuando un usuario abre un documento, lo cierra, o crea una nueva. Estos comandos son utilizados comúnmente por macros legítimas y maliciosas.

# Como funciona Macro Malware

Según expertos de **proveedor de pruebas de penetración**, el camino a una infección del sistema amplia a través de macro malware comienza típicamente con un archivo adjunto de correo electrónico hecho de aparecer como algo legítimo, a menudo de ingeniería social para adaptarse al usuario de destino. Las líneas de asunto comunes incluyen frases tales como solicitud de pago, la notificación de mensajería, hoja de vida, factura de venta, o la confirmación de la donación. El texto del mensaje coincide con la línea de asunto suficiente para que el usuario abra el archivo adjunto abierto, incluyendo firmas y logotipos de aspecto oficial.

# Como funciona Macro Malware

Una vez abierto, las características de seguridad de Microsoft Office se advierten a los usuarios que el archivo contiene macros y pregunta si quieren que les permitan. Algunos de estos archivos tienen gran proclamación de texto que están protegidos y que las macros debe estar habilitarse macros para verlos. Si el usuario hace clic en "Activar", el código malicioso se ejecuta, dejando caer un descargador de malware en el sistema que traerá en la carga útil de malware real, y luego, entonces a menudo eliminar sí mismo después comenta Mike Stevens profesional de empresa de seguridad informática.

# Macro Malware

Comenta Mike Stevens de **empresa de seguridad informática** uno de los mayores cambios en la macro malware desde la última gran infestación es su capacidad actual para ocultar, por lo que es mucho más difícil de detectar. Los autores de malware macro han adoptados varias técnicas de otros tipos de malware, incluyendo la adición de código basura y escribir cadenas cifradas complejas. Código de basura es sólo código que no está destinado a ejecutar, pero se puede generar con facilidad y cambiarse con frecuencia para derrotar a los algoritmos de detección de la firma y confundir a los investigadores de amenazas.

# Macro Malware

La simplicidad y la facilidad de codificación macros hacen accesibles a una amplia gama de criminales con conocimientos mínimos de tecnología. Como resultado, el potencial alcance y la eficacia de macro de malware significan que las empresas deben volver a educar a los usuarios sobre esta amenaza. Además, el sistema operativo y las aplicaciones deben mantenerse al día, y la configuración de seguridad de macros en todos los productos de Microsoft Office se debe establecer en alto. Aplicaciones de correo electrónico no deben abrir automáticamente los archivos adjuntos menciono Mike Stevens de empresa de seguridad informática.

# CONTACTO

www.webimprints.com

538 Homero # 303
Polanco, México D.F 11570
México
México Tel: (55) 9183-5420

DUBAI

702, Smart Heights Tower, Dubai

Sixth Floor, Aggarwal Cyber Tower 1
Netaji Subhash Place, Delhi NCR, 110034
India
India Tel: +91 11 4556 6845