



RIESGOS EN LA RED: TIPOS DE MALWARE

Guía Técnica de Identificación de Amenazas y Seguridad de Sistemas

1. CONCEPTO GENERAL DE MALWARE

Acrónimo de "*Malicious Software*" (Software Malicioso), el **Malware** hace referencia a cualquier código, programa o script diseñado maliciosamente para infiltrarse en un sistema, evadir controles de acceso, robar información confidencial, dañar archivos o comprometer la integridad y disponibilidad de la infraestructura tecnológica de un usuario o entidad.

Para **MEGANET TELECOMUNICACIONES S.A.S.**, la seguridad digital es un pilar fundamental. Por ello, a continuación se detallan las principales amenazas de malware identificadas en la red:

2. TIPOS COMUNES DE MALWARE (PARTE I)

Spyware (Software Espía):

Diseñado específicamente para rastrear, registrar y espiar las actividades del usuario sin su autorización. El spyware captura contraseñas mediante registradores de teclas (keyloggers), rastrea hábitos de navegación y exfiltra información de formularios. Suele instalarse de forma encubierta agrupado con software gratuito o troyanos.

Adware (Software Publicitario):

Software programado para mostrar o descargar publicidad de manera automática e intrusiva en forma de ventanas emergentes (pop-ups) o banners dentro de los programas. Si bien algunos adwares solo causan molestias comerciales, con frecuencia incluyen rutinas de spyware para recopilar datos de mercadeo del usuario.

Bot (Robot Informático) y Botnets:

Código malicioso diseñado para realizar tareas automatizadas en línea bajo las instrucciones de un atacante remoto. Cuando múltiples dispositivos son infectados con estos bots, conforman una "Botnet" (Red de computadores zombis), la cual es utilizada para lanzar ataques masivos de denegación de servicio (DDoS) o envío de spam a gran escala.

Ransomware (Secuestro de Información):

Una de las amenazas más dañinas de la actualidad. Este software cifra (encripta) los archivos del disco duro del usuario utilizando algoritmos complejos y bloquea el acceso al sistema operativo, exigiendo el pago de un rescate económico (usualmente en criptomonedas) para entregar la clave de descifrado.

**Scareware (Software de Coerción/Temor):**

Malware diseñado para engañar al usuario mediante el miedo. Genera ventanas emergentes falsas que simulan ser advertencias del sistema operativo o alertas de virus del computador. Estos mensajes advierten de daños críticos y solicitan de forma urgente la descarga o compra de un programa específico para "solucionar" el problema, infectando el equipo en el proceso.

Rootkit:

Herramientas altamente sofisticadas diseñadas para modificar componentes del sistema operativo central a fin de abrir una puerta trasera (backdoor) permanente. Esto otorga al atacante control total y privilegios de administrador de forma remota, ocultando su presencia de los programas antivirus tradicionales y del administrador de tareas.

Virus Informático:

Código ejecutable que se adjunta de forma maliciosa a un programa o archivo legítimo del host. Requiere de la acción deliberada del usuario (abrir el archivo infectado) para activarse y propagarse. Puede causar desde daños leves (mostrar imágenes molestas) hasta la destrucción de archivos de sistema de forma masiva.

Troyano (Caballo de Troya):

Malware que se presenta ante el usuario como un programa legítimo e inofensivo (como un juego, utilidad o archivo de audio), pero que en segundo plano ejecuta operaciones dañinas aprovechando los privilegios de ejecución del usuario. A diferencia de los virus, los troyanos no se replican por sí mismos.

Gusanos (Worms):

Códigos maliciosos autónomos que tienen la capacidad de replicarse y propagarse de forma independiente a través de los recursos de red compartidos y conexiones a internet, explotando fallas de seguridad del sistema. Su impacto principal es la saturación del ancho de banda y la ralentización de las redes corporativas y hogareñas.

Hombre en el Medio (MitM / Man-in-the-Middle):

Ataque donde el perpetrador intercepta silenciosamente la comunicación entre el dispositivo del usuario y el servidor de destino. Permite capturar credenciales de acceso, transacciones financieras y datos confidenciales.

Hombre en el Móvil (MitMo / Man-in-the-Mobile):

Variante del ataque MitM aplicada a teléfonos inteligentes. Permite a los atacantes interceptar y leer silenciosamente mensajes SMS de autenticación de doble factor (2FA) enviados por bancos, comprometiendo cuentas bancarias y portales corporativos.



3. SÍNTOMAS FRECUENTES DE INFECCIÓN POR MALWARE

Independientemente del tipo de software malicioso que haya comprometido el sistema de su hogar u oficina, existen patrones de comportamiento anómalos que alertan sobre una infección:

- **Ralentización del Sistema:** Disminución notable en la velocidad de la computadora y aumento injustificado en el uso de la memoria RAM y el procesador (CPU).
- **Fallas y Bloqueos Recurrentes:** La computadora se congela, muestra pantallas azules o cierra los programas de forma repentina.
- **Navegación Lenta o Redireccionada:** La velocidad de carga de internet disminuye significativamente y los navegadores cambian su página de inicio o abren pestañas publicitarias no solicitadas de manera constante.
- **Modificación y Desaparición de Archivos:** Archivos modificados sin su consentimiento, carpetas encriptadas o eliminación espontánea de bases de datos y documentos.
- **Comportamiento Extraño del Escritorio:** Aparición de iconos desconocidos, barras de herramientas nuevas en el navegador o ejecución de procesos sospechosos en segundo plano.
- **Envío Automático de Correos:** Mensajes enviados desde sus cuentas de correo electrónico o redes sociales a sus contactos sin su conocimiento o consentimiento.

Pauta Crítica de Acción:

Si detecta uno o más síntomas en su equipo de cómputo, desconecte inmediatamente el dispositivo de la red Wi-Fi o cableada para evitar la propagación del malware en la red local y realice un escaneo completo utilizando una herramienta antivirus licenciada y actualizada.

4. MEDIDAS Y RECOMENDACIONES DE MEGANET TELECOMUNICACIONES S.A.S.

Para resguardar sus activos de información en nuestra red de internet de alta velocidad, aconsejamos:

- **Instalar Antivirus y Firewalls locales:** Configure soluciones activas de protección y mantenga activo el cortafuegos del sistema operativo.
- **Verificar Enlaces y Descargas:** No descargue programas desde enlaces enviados en redes sociales o correos de dudosa procedencia. Utilice siempre los portales oficiales de los desarrolladores.
- **Actualizar Dispositivos:** Mantenga al día el firmware de sus enrutadores, teléfonos móviles y computadoras.