Departamento de Ciencias de la Computación
Universidad de las Fuerzas Armadas-ESPE

Taller No° 2

Investigación acerca Amenazas

Integrantes: José Sanmartín
Yeshua Chiliquinga
Carrera / Asignatura: Ingeniería de Software / Ingenieria de la Seguridad
NRC: 23358
Fecha: 27 de Mayo de 2025

Spyware: Definición

El spyware es un tipo de software malicioso que "intenta monitorear silenciosamente el comportamiento de los usuarios, registrar sus hábitos de navegación web o robar sus datos sensibles, como contraseñas" (Egele et al., 2007, p. 233). Su funcionamiento consiste en instalarse de forma oculta en el sistema del usuario, interceptar y registrar información confidencial sin consentimiento, y transmitirla a terceros, generalmente con fines comerciales o maliciosos. Utiliza técnicas como el análisis dinámico y la ofuscación de código para evitar ser detectado por herramientas tradicionales de seguridad.

Ilustración Representativa

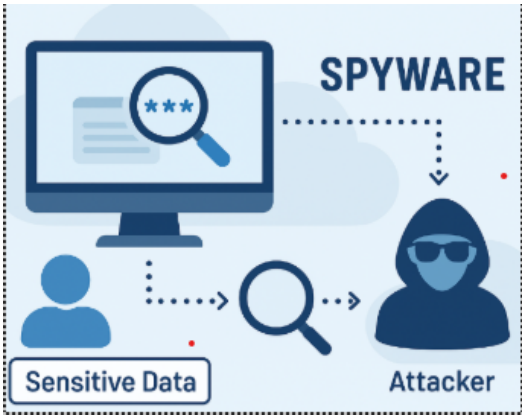

Imagen 1: Representación conceptual del spyware

Estadísticas Recientes

En el tercer trimestre de 2024, se observó un aumento del 166 % en las detecciones de spyware, impulsado por amenazas avanzadas como NGate, que se dirige a datos NFC para retiros en cajeros automáticos. La firma iVerify identificó infecciones por el spyware Pegasus en 7 de 2,500 dispositivos escaneados. El costo global del cibercrimen alcanzó los $9.5 billones en 2024, con un crecimiento proyectado del 15 % anual hasta 2025.

Casos de Estudio o Ejemplos

Pegasus (Spyware Examples, 2024)

[leftmargin=*]**Año de aparición:** Mediados de la década de 2010 **Desarrollado por:** NSO Group, empresa tecnológica israelí **Modo de operación:**

- Se dirige a dispositivos iOS y Android
- Utiliza exploits de "cero-clic" para infectar sin interacción del usuario
- También se propaga vía spear-phishing
- Una vez instalado, permite el monitoreo completo del dispositivo

- **Impacto:**
  - Utilizado contra periodistas, activistas y políticos
  - Ha comprometido docenas de teléfonos de alto perfil
  - Representa una amenaza a los derechos humanos y libertades civiles

DarkHotel (Jerry, 2024)

[leftmargin=*]**Año de aparición:** Identificado en 2014, con infecciones desde 2008 **Lugar de aparición:** Corea del Sur **Modo de operación:**

- Apunta a ejecutivos hospedados en hoteles de lujo
- Usa redes Wi-Fi inseguras para atacar
- Falsifica certificados para instalar software malicioso
- Registra pulsaciones de teclas mediante keyloggers

- **Impacto:**
  - Roba datos financieros y propiedad intelectual
  - Ha comprometido información confidencial a nivel empresarial
  - Subraya la amenaza del ciberespionaje dirigido

Métodos para Combatir el Spyware

Herramientas

Herramientas como Malwarebytes, Spybot Search
Destroy, Kaspersky, Bitdefender, ESET y Norton pueden detectar y eliminar spyware. Es fundamental mantenerlas actualizadas.

Buenas Prácticas

- Mantener los sistemas operativos actualizados para evitar vulnerabilidades
- No instalar software de fuentes no verificadas
- Usar bloqueadores de pop-ups y eliminar extensiones sospechosas
- Cambiar contraseñas después de una infección
- Realizar análisis completos del sistema regularmente

Conclusiones

Pegasus se considera uno de los spyware más peligrosos por su uso a nivel estatal y su capacidad de vigilancia extrema. Su existencia plantea cuestionamientos éticos profundos y amenazas a la privacidad y libertad. La mejor defensa es la educación del usuario, el uso de herramientas confiables y una actitud proactiva ante las amenazas cibernéticas. En 2024, el spyware tuvo un impacto notable y creciente, lo que exige medidas reforzadas de seguridad digital en todos los niveles.

Referencias Bibliográficas

- Egele, M., Kruegel, C., Kirda, E., Yin, H.,
  Song, D. (2007). *Dynamic spyware analysis*. USENIX Annual Technical Conference.
- Chakian, F. N.,
  García, B. S. (2011). *Definición e implantación de un sistema de monitoreo y reporte de la seguridad lógica en un data center*. Universidad Católica Andrés Bello.

- Spyware Examples (2024). *The 5 worst attacks of all time*. SoftwareLab. https://softwarelab.org/blog/spyware-examples/
- Jerry. (2024). *The 5 most notorious spyware attacks*. Safernet. https://safernetvpn.com/the-5-most-notorious-spyware-attacks/
- Skoudis, E., Zeltser, L. (2004). *Malware: Fighting malicious code*. Prentice Hall Professional.
- Ligh, M., Adair, S., Hartstein, B., Richard, M. (2010). *Malware analyst's cookbook and DVD: Tools and techniques for fighting malicious code*. Wiley Publishing.
- ESET. (2024). *Reporte de Ciberamenazas 2024*. https://www.eset.com/la/blog/ciberseguridad/estadisticas-ciberamenazas-2024/