Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad

Análisis y Detección de Malware

Raúl Acosta Bermejo

Temario

1. Introducción
   - 1.1. Definiciones y taxonomias de malware
     Rootkits, Botnets, Virus y Gusanos, Keyloggers, Troyanos, Ransomware.
   - 1.2. Historia y evolución del malware.
   - 1.3. Antivirus, antimalware.
     VirusTotal,
   - 1.4. Reportes de seguridad y de malware.
2. Análisis de malware
   - 2.1. Introducción
     Formatos de ejecutables.
   - 2.2. Extracción de información
     - 2.2.1. Herramientas: Dependency Walker, PeiD, IDA Pro, etc.
     - 2.2.2. Elementos: strings, librerias, funciones y API calls.
   - 2.3. Firmas de malware
     - 2.3.1. Hash, Ssdeep, Sdhash, Yara
     - 2.3.2. Pakers.
   - 2.4. Ingenieria inversa
     - 2.4.1. Metodología, desensamblado y decompilación.
     - 2.4.2. Herramientas: Radare, Capstone, etc.
   - 2.5. Debuggers y técnicas antidebugging
     Ejecución simbólica
   - 2.6. Técnicas de ataque del malware
     - 2.6.1. Inyeción de código, buffer overflow
     - 2.6.2. Hooking, RET2, ROP.
     - 2.6.3. Shellcode
     - 2.6.4. Vulnerabilidades en archivos binarios
   - 2.7. Ataques de red
     - 2.7.1. DoS, DGA, Amplificación.
     - 2.7.2. Sybilattack, Smurf, fraggle, naptha.
   - 2.8. Ofuscación
     - 2.8.1. Packers, motores metamorficos.
   - 2.9. Detección de malware mediante algoritmos de ML y mineria de datos.
     Ngrams, CFG, Markov, etc.
3. Detección de malware
   - 3.1. Sistemas de Detección y Prevención de Intrusos (del inglés IDS)

De host y de red.

3.2. Detección mediante las acciones del malware
  3.2.1. Bitacoras de procesos, de red, de registros (Windows registry)
3.3. Detección de comportamientos mediante opcodes, syscalls, program profiling, code metrics.
3.4. Detección de malware mediante algoritmos de ML y mineria de datos.
3.5. Análisis forense
  3.5.1. Captura de memoria de un proceso y del kernel.
  3.5.2. Herramientas: Volatility.
3.6. Técnicas avanzadas: introspección.

4. Análisis de amenazas
  4.1. Modelos de amenazas Árboles (ataque, falla), Diagrama Ataque-Defensa
  4.2. Countermeasures: Antivirus, IDS-Host, Programación Segura
5. Repositorios de malware
  5.1. Definición y API REST.
  5.2. VirusShare, VirusSign, VirusTotal, Contagio, etc.
6. Laboratorio de malware
  6.1. Sandboxing, Containers, Honeypots
  6.2. Cuckoo