Instituto Politécnico Nacional
Centro de Investigación en Computación
Laboratorio de Ciberseguridad

Autor inicial: Raúl Acosta Bermejo.

Análisis de Malware

72 hrs. / 36 Clases

Temario

1. Introducción — 6 hrs. / 3 clases
   - 1.1. Historia y evolución del malware.
   - 1.2. Definiciones y taxonomias de malware
     Rootkits, Botnets, Virus y Gusanos, Keyloggers, Troyanos, Ransomware.
     Congresos (Defcon)
     Reportes de seguridad y de malware, Infografias.
2. Repositorios de malware — 4 hrs. / 2 clases
   - 2.1. Definición y API REST.
   - 2.2. Casos de estudio
     VirusShare, VirusSign, VirusTotal, Contagio, etc.
3. Laboratorio de malware — 8 hrs. / 4 clases
   - 3.1. Inroducción
     - 3.1.1. Entorno controlado
     - 3.1.2. Sandboxing, Containers, Honeypots
   - 3.2. Casos de Estudio
     - 3.2.1. Cuckoo
     - 3.2.2. Joe Sandbox
     - 3.2.3. Sandboxie
   - 3.3. API REST
4. Tecnicas del malware — 8 hrs. / 4 clases
   - 4.1. Técnicas de Defensa contra el malware
     Funciones hash, funciones fuzzy, CTPH (context triggered piecewise hashing)
     Ejemplos Ssdeep, Sdhash.
     Antivirus, antimalware. Ejemplos: VirusTotal, Hybrid Analysis
   - 4.2. Técnicas de Ataque del malware
     - 4.2.1. Inyeción de código, buffer overflow
     - 4.2.2. Hooking, RET2, ROP.
     - 4.2.3. Shellcode
     - 4.2.4. Vulnerabilidades en archivos binarios
   - 4.3. Ataques de red
     - 4.3.1. DoS, DGA, Amplificación.
     - 4.3.2. Sybilattack, Smurf, fraggle, naptha.
5. Análisis Estático de Malware — 20 hrs. / 10 clases
   - 5.1. Introducción

Formatos de ejecutables.
Firmas de malware (Hash, Ssdeep, Sdhash)

5.2. Ingenieria inversa
5.2.1. Metodología, desensamblado y decompilación.
5.2.2. Herramientas: Radare, Capstone, etc.
5.3. Extracción de información
5.3.1. Herramientas: Dependency Walker, PeiD, IDA Pro, etc.
5.3.2. Elementos: strings, librerias, funciones y API calls.
5.4. Debuggers y técnicas antidebugging
Ejecución simbólica
5.5. Ofuscación
5.5.1. Packers, motores metamorficos.
5.6. Técnicas avanzadas: introspección.

6. Análisis Dinámico de Malware — 20 hrs. / 10 clases
6.1. Introducción
6.1.1. Hooking
6.2. Volcado de memoria
6.2.1. De procesos
6.2.2. Del kernel del sistema operativo
6.3. Captura de datos
6.3.1. System Calls (SysCall)
6.3.2. API Calls
6.4. Agentes
6.4.1. Monitoreo de las comunicaciones
6.4.2. Monitoreo de operaciones: archivos, puertos, etc.

7. Temas Avanzados — 6 hrs. / 3 clases
7.1. Análisis forense
7.1.1. Captura de memoria de un proceso y del kernel.
7.1.2. Herramientas: Volatility.

Bibliografía

1. “Malware Analyst’s Cookbook and DVD”, Tools and Techniques for fighting malicious code.
    a. Autores: Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard.
    b. Editorial: Wiley Publishing Inc, 2011.
2. “Practical Malware Analysis”.
    a. Autores: Michael Sikorski, Andrew Honig.
    b. Editorial Wiliam Pollock, 2012.
3. “Learning Malware Analysis”, Explore the concepts, tools, and techniques to analyze and investigate Windows malware.
    a. Autores: Monnappa K A.
    b. Editorial Packet Publishing, 2018.
4. “HACKING EXPOSED MALWARE & ROOTKITS: MALWARE & ROOTKITS SECURITY SECRETS & SOLUTIONS”,
    a. Autores: Michael DAVIS, Sean BODMER, Aaron LEMASTERS.
    b. Editorial: McGraw Hill. 2nd edition 2017.
5. “Malware: Fighting Malicious Code”,
    a. Autores: Ed Skoudis,Lenny Zeltser.
    b. Editorial : Pearson, 2003.
6. “Rootkits: Subverting the Windows Kernel”,
    a. Autores: Greg Hoglund, James Butler.
    b. Editorial: Addison Wesley Professional.
7. “Practical Binary Analysis”, Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly.
    a. Autores: Dennis Andriesse.
    b. Editorial No Starch Press San Francisco, 2019.
8. “Learning Linux Binary Analysis”,
    a. Autor: "elfmaster"
    b. Editorial: O'Neill, Packt Publishing, 2016.

========== FIN DEL DOCUMENTO ==========