

Amenazas Persistentes Avanzadas

* * * * *

Antonio Villalón
Director de Seguridad – S2 Grupo

 **libres**

© Antonio Villalón Huerta, 2016

© De esta edición:

Nau Llibres

Periodista Badía 10. 46010 València

Tel.: 96 360 33 36

Fax: 96 332 55 82

E-mail: nau@naullibres.com

web: www.naullibres.com

Diseño y maquetación:

Pablo Navarro, Nerina Navarrete y Artes Digitales Nau Llibres

Diseño de cubierta e ilustración:

S2 Grupo

ISBNs Nau Llibres

ISBN_papel: 978-84-16926-09-1

Depósito Legal: V-2614-2016

ISBN_ePub: 978-84-16926-10-7

ISBN_mobi: 978-84-16926-11-4

ISBN_PDF: 978-84-16926-12-1

Impresión: Safekat

Quedan rigurosamente prohibidas, sin la autorización por escrito de los titulares del «Copyright», bajo las sanciones establecidas por las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidas la reprografía y el tratamiento informático.



Para Raquel, Teresa y Lucía

Índice

Antes de comenzar	11
Prólogo	13
1. Introducción	15
1.1. Inteligencia.....	15
1.2. Necesidades de información	18
1.3. Ciberinteligencia	19
1.4. Amenazas Persistentes Avanzadas	21
1.5. CNO, SIGINT, APT.....	24
1.6. Seguridad tradicional.....	26
2. Actores principales	29
2.1. Atribución	30
2.1.1. Evidencias.....	31
2.1.2. TTP	32
2.1.3. Planificación	34
2.1.4. Necesidades de información.....	34
2.1.5. El problema de la atribución	36
2.2. Los estados.....	39
2.2.1. USA/FVEY	41
2.2.2. China	47
2.2.3. Rusia.....	54
2.2.4. Alemania.....	60
2.2.5. Francia.....	62
2.2.6. Israel.....	64
2.3. Los grupos.....	67
2.3.1. China: APT1	68
2.3.2. USA: TAO	69
2.3.3. Rusia: APT28.....	70
2.3.4. ¿Quién falta en la lista?.....	70
3. Las campañas y el malware	73
3.1. Stuxnet	74
3.2. Duqu	76
3.3. Shady RAT	76

3.4. Flame	77
3.5. Red October	78
3.6. NetTraveler	79
3.7. CARETO	80
3.8. UROBUROS.....	81
4. Arquitectura de la amenaza	83
4.1. Arquitectura externa.....	84
4.2. Arquitectura interna.....	87
4.3. Técnicas de evasión avanzadas	89
4.4. Ficheros portadores	91
4.5. (Supuesta) anatomía de un C2	92
5. Ciclo de vida de una APT	97
5.1. Reconocimiento.....	100
5.2. Intrusión	103
5.3. Persistencia	107
5.3.1. Movimiento lateral.....	108
5.3.2. Movimiento externo	110
5.3.3. Exfiltración sin tráfico saliente	111
6. Detección del compromiso	113
6.1. Contrainteligencia.....	114
6.2. Tecnologías de detección.....	115
6.3. Detección del compromiso.....	117
6.4. SIGINT: detección de movimiento externo	118
6.5. SIGINT: detección de movimiento lateral.....	123
6.6. TECHINT.....	126
6.7. OSINT	130
6.8. HUMINT	133
6.8.1. Intercambio de información.....	133
6.8.2. HUMINT clandestina.....	135
7. Gestión del incidente	139
7.1. Introducción	140
7.2. Consideraciones previas.....	142
7.3. Preparación	143
7.4. Respuesta	145

7.4.1. Identificación.....	148
7.4.2. Contención	149
7.4.3. Erradicación.....	151
7.4.4. Recuperación.....	151
7.5. Lecciones aprendidas.....	152
7.6. Ejemplo práctico.....	154
8. Otra vuelta de tuerca	159
8.1. Sabotaje	159
8.2. Redes aisladas.....	161
8.3. La amenaza humana	162
8.4. Amenazas volátiles.....	167
8.5. Amenazas en firmware	168
8.6. Malware en dispositivos móviles	170
8.7. Esteganografía.....	172
8.8. Exfiltración multicast	173
9. Conclusiones	177
10. Anexo: Anomalías HTTP	181
10.1. Resumen	181
10.2. Introducción: Detección de anomalías.....	181
10.3. Anomalías HTTP.....	183
10.4. Adquisición de datos	185
10.5. Análisis estadístico univariable	187
10.6. Análisis estadístico multivariable.....	190
10.7. Análisis basado en conocimiento.....	194
10.8. EL CAMPO TIME.....	195
10.9. El campo URL.....	197
10.10. Aprendizaje automático.....	201
10.11. Mejoras al esquema	203
11. Anexo: Acrónimos	207
12. Referencias.....	211