Indice generale

Ringraziamenti ..... **ix**

Introduzione ..... **xi**

A chi è rivolto questo libro xiii
Come è organizzato questo libro xiv
L'autore xiv
Il revisore tecnico xiv

Parte I Il panorama delle cyberminacce avanzate **1**

Capitolo 1 Attacchi di livello governativo **3**

Cina 4
Titan Rain 4
Campagne di spionaggio di Hidden Lynx 5
Il report di Mandiant su APT1 6
Il cessate il fuoco del 2015 fra USA e Cina 6
Russia 8
Moonlight Maze 10
L'attacco all'Estonia 11
Il conflitto georgiano 12
Buckshot Yankee 13
Red October 14
Iran 15
I primi anni 16
La violazione di Gmail del 2011 18
Shamoon 19
Stati Uniti 21
Cripto AG 21
Stuxnet 23
The Equation Group 26
Regin 29

Corea del Nord 31
Unità 121 31
Cyberattacchi 32
Conclusioni 33

Capitolo 2 Attacchi di natura economica finanziati da Stati 35

Attacchi Distributed DoS contro istituzioni finanziarie 36
L'attacco Dozer 37
Ten Days of Rain 38
I Guardiani della Rivoluzione prendono di mira le banche statunitensi (2011-2013) 39
DarkSeoul 41
Attacchi russi contro l'Ucraina 43
Rapine per miliardi di dollari 44
Attacchi al sistema SWIFT 44
Lo schema di un furto finanziario della Corea del Nord 45
Reazione della Banca del Bangladesh 51
FASTCash: una rapina globale agli sportelli automatici 51
Odinaff: i cybercriminali imparano dagli hacker di livello governativo 53
Conclusioni 56

Capitolo 3 Attacchi ransomware 59

GoGalocker 60
SamSam 66
Ryuk 68
MegaCortex 69
EvilCorp 70
BitPaymer 71
Sotto accusa 71
WastedLocker 72
Collegamenti fra questi attacchi ransomware 74
Ransomware as a Service 79
L'attacco di DarkSide all'oleodotto 80
Misure di difesa 81
Conclusioni 83

Capitolo 4 Hacking elettorale 85

Le elezioni presidenziali ucraine del 2014 86
Lo schema dell'attacco elettorale ucraino 89
Figure false 89
Campagna di propaganda 89
DDoS e furto di dati 90
Manipolazione e divulgazione dei dati politici sottratti 91
Malware e dati elettorali falsi 91

Le elezioni presidenziali americane del 2016 91
Le elezioni presidenziali francesi del 2017.....98
Conclusioni 101

Parte II Ricerca e analisi di cyberminacce avanzate 103

Capitolo 5 Attribuzione degli attacchi 105

Classificazione in gruppi 106
Hacktivismo 106
Cybercriminalità.....107
Cyberspionaggio 110
Altro.....112
Attribuzione 112
Confidenza dell'attribuzione.....114
Processo di attribuzione.....115
Identificazione di tattiche, tecniche e procedure 117
Condurre analisi del fuso orario.....118
Errori di attribuzione.....122
Non identificate l'infrastruttura degli hacker sulla base del DDNS.....122
Non date per scontato che i domini ospitati sullo stesso indirizzo IP appartengano agli stessi hacker 123
Nello stabilire l'attribuzione non utilizzate domini registrati da broker.....124
Non stabilite l'attribuzione in base a strumenti di hacking pubblicamente disponibili 126
Suggerimenti per stabilire l'attribuzione 127
Creazione di profili delle minacce 128
Conclusioni 129

Capitolo 6 Distribuzione e comunicazioni del malware 131

Rilevamento dello spear-phishing 132
Informazioni di base sull'indirizzo 133
Il campo X-Mailer.....135
Il campo Message-ID.....136
Altri campi utili.....138
Analisi di siti dannosi o violati.....138
Rilevamento di comunicazioni segrete.....141
Shamoon e i file ADS (Alternative Data Stream) 141
Bachosens e uso improprio di un protocollo 143
Analisi del riutilizzo del codice del malware 146
WannaCry.....147
Il framework Elderwood per la distribuzione di exploit Zero-Day 149
Conclusioni 152

Capitolo 7 Caccia alle minacce tramite dati open source.....153

Utilizzo degli strumenti di OSINT 153
Proteggersi con l'OPSEC 154
Questioni legali 155
Strumenti di enumerazione dell'infrastruttura.....155
Farsight DNSDB 155
PassiveTotal.....156
DomainTools.....156
Whoisology 156
DNSmap 157
Strumenti di analisi del malware 157
VirusTotal.....157
Hybrid Analysis 159
Joe Sandbox.....159
Hatching Triage 160
Cuckoo Sandbox 161
Motori di ricerca 162
Formulazione delle ricerche.....162
Ricerca di parti di codice su NerdyData.....163
TweetDeck 164
Navigare nel Dark Web 164
Software VPN 166
Tracciamento delle indagini 166
ThreatNote 167
MISP.....168
Analyst1 168
DEVONthink 168
Analisi delle comunicazioni di rete con Wireshark 170
Utilizzo di framework di ricognizione.....170
Recon-ng.....171
TheHarvester.....172
SpiderFoot.....172
Maltego.....173
Conclusioni 173

Capitolo 8 Analisi di una minaccia concreta 175

La situazione.....175
Analisi del messaggio di posta elettronica.....176
Analisi del corpo dell'e-mail 178
Ricerca OSINT 180
Analisi del documento "esca" 183
Identificazione dell'infrastruttura di comando e controllo 185
Identificazione di eventuali file alterati 186
Analisi dei file eliminati.....187
Analisi del file dw20.t 188
Analisi del file netidt.dll 189

Indizi dal rilevamento delle signature 190
Ricerca sulle infrastrutture 193
Ricerca di domini aggiuntivi 194
DNS passivo 195
Visualizzare gli indicatori delle relazioni sulle violazioni 198
Risultati.....199
Creazione di un profilo della minaccia 201
Conclusioni 203

Appendice A Domande sulla profilazione delle minacce.....205

Appendice B Esempio di modello di profilo della minaccia 209

Note 211

Indice analitico.....229