

Spis treści

PODZIĘKOWANIA	11
---------------------	----

WPROWADZENIE	12
--------------------	----

CZĘŚĆ I. PRZEGLĄD ZAAWANSOWANYCH CYBERZAGROŻEŃ	17
--	-----------

1	
ATAKI PROWADZONE PRZEZ ORGANIZACJE PAŃSTWOWE	19
Chiny	20
Titan Rain	21
Kampanie szpiegowskie Hidden Lynx	21
Raport firmy Madiant na temat grupy APT1	22
Zawieszenie broni pomiędzy USA a ChRL w 2015 r.	23
Rosja	25
Moonlight Maze	27
Konflikt z Estonią	29
Konflikt z Gruzją	30
Buckshot Yankee	31
Red October	32
Iran	34
Wczesne lata	34
Atak na usługę Gmail w 2011 r.	36
Shamoon	39
Stany Zjednoczone	41
Crypto AG	41
Stuxnet	43
Grupa Equation	47
Regin	50

Korea Północna	53
Jednostka 121	53
Cyberataki	54
Podsumowanie	55

2

ATAKI FINANSOWE PROWADZONE PRZES HAKERÓW RZĄDOWYCH	56
Rozproszone ataki DoS w sektorze finansowym	57
Atak z użyciem narzędzia Dozer	58
Atak Ten Days of Rain	59
Korpus Strażników Rewolucji Islamskiej obiera za cel amerykańskie banki (2011 – 2013)	60
DarkSeoul	63
Rosyjskie ataki przeciwko Ukrainie	66
Miliardowe kradzieże	67
Ataki na system SWIFT	67
Model kradzieży finansowych stosowany przez Koreę Północną	68
Reakcja Banku Bangladeszu	75
FASTCash — globalna kradzież bankomatowa	76
Odinaff — cyberprzestępcy uczą się od hakerów rządowych	78
Podsumowanie	81

3

SZYFROWANIE DLA OKUPU	83
Atak GoGalocker	85
Atak SamSam	91
Atak Ryuk	93
Atak MegaCortex	95
Grupa EvilCorp	95
Wirus szyfrujący BitPaymer	96
Akt oskarżenia	97
Ataki WastedLocker	98
Odnajdywanie powiązań między atakami	100
Ataki szyfrujące jako usługa	106
Atak grupy DarkSide na rurociąg	107
Metody obrony	109
Podsumowanie	111

4

HAKOWANIE WYBORÓW	113
Wybory prezydenckie na Ukrainie w 2014 r.	114
Model ataku zastosowany wobec ukraińskich wyborów prezydenckich	117
Faktyczne tożsamości internetowe	118
Kampanie propagandowe	118
Ataki DDoS i kradzież danych	119
Faktyzowanie wykradzionych informacji politycznych i ich publikacje	120
Szkodliwe oprogramowanie i faktyczne wyniki wyborów	120

Wybory prezydenckie w USA w 2016 r.	120
Wybory prezydenckie we Francji w 2017 r.	128
Podsumowanie	132

CZĘŚĆ II. WYKRYWANIE I ANALIZA ZAAWANSOWANYCH CYBERZAGROŻEŃ 135

5 PRZYPISYWANIE ATAKÓW PRZECIWNIKOM 137

Klasyfikacja grup zagrożeń	138
Haktywiści	138
Cyberprzestępcy	139
Szpiegostwo cyfrowe	142
Nieznani	144
Atrybucja	146
Pewność przypisania sprawstwa	147
Proces przypisywania sprawstwa	149
Identyfikacja metod, technik i procedur	151
Prowadzenie analizy stref czasowych	153
Błędy atrybucji	157
Nie określaj agresora na podstawie danych z dynamicznego systemu nazw domenowych	158
Nie traktuj domen uruchomionych pod tym samym adresem IP jako należących do tego samego agresora	158
Nie używaj do atrybucji domen zarejestrowanych przez brokerów	160
Nie próbuj określić sprawcy ataku na podstawie publicznie dostępnych narzędzi hakerskich ...	162
Wskazówki	163
Tworzenie profili zagrożeń	165
Podsumowanie	166

6 SPOSOBY ROZPOWSZECZNIA SZKODLIWEGO OPROGRAMOWANIA I JEGO METODY KOMUNIKACJI 167

Wykrywanie personalizowanych wiadomości phishingowych	168
Podstawowe informacje o adresie	169
Informacja o użytym programie pocztowym	172
Identyfikator wiadomości	174
Pozostałe przydatne pola	175
Analiza szkodliwych lub przejętych przez hakerów stron internetowych	176
Wykrywanie skrytej komunikacji	179
Nadużycie mechanizmu Alternate Data Stream podczas ataku Shamoons	180
Nadużycie protokołów komunikacyjnych przez wirusa Bachosens	182
Analiza wielokrotnego wykorzystania szkodliwego kodu	186
Atak WannaCry	186
Platforma dystrybucji exploitów Elderwood	189
Podsumowanie	193

POSZUKIWANIE INFORMACJI O ZAGROŻENIACH W OGÓLNODOSTĘPNYCH ŹRÓDŁACH 194

Używanie narzędzi OSINT	195
Stosowanie zasad bezpieczeństwa operacyjnego	195
Wątpliwości natury prawnej	196
Narzędzia do enumeracji elementów infrastruktury	197
Farsight DNSDB	197
PassiveTotal	198
DomainTools	198
Whoisology	198
DNSmap	199
Narzędzia do analizy szkodliwego oprogramowania	199
VirusTotal	200
Hybrid Analysis	201
Joe Sandbox	202
Hatching Triage	203
Cuckoo Sandbox	203
Wyszukiwarki	204
Tworzenie zapytań	205
Poszukiwanie próbek kodu za pomocą wyszukiwarki NerdyData	205
Narzędzie TweetDeck	207
Przeglądanie zasobów ciemnej strony internetu	207
Oprogramowanie VPN	209
Narzędzia wspomagające organizowanie informacji zebranych podczas śledztwa	210
ThreatNote	210
MISP	211
Analyst1	212
DEVONthink	212
Analizowanie komunikacji sieciowej za pomocą narzędzia Wireshark	214
Korzystanie z platform rozpoznawczych	215
Recon-ng	215
TheHarvester	216
SpiderFoot	217
Maltego	217
Podsumowanie	218

ANALIZA RZECZYWISTEGO ZAGROŻENIA 219

Kontekst	219
Analiza wiadomości e-mail	220
Analiza nagłówka	220
Analiza treści wiadomości	223
Analiza publicznie dostępnych źródeł informacji (OSINT)	225

Analiza dokumentu pułapki	229
Identyfikacja infrastruktury sterowania i kontroli	231
Identyfikacja zmodyfikowanych plików	232
Analiza pobranych plików	234
Analiza pliku dw20.t	234
Analiza pliku netidt.dll	236
Korzystanie ze wskazówek silników detekcji	237
Analiza infrastruktury	240
Odszukanie dodatkowych domen	241
Rekordy pasywnego DNS	242
Wizualizacja powiązań między wskaźnikami włamania	246
Wnioski	247
Tworzenie profilu zagrożenia	249
Podsumowanie	252
 A	
PYTANIA POMOCNICZE DO TWORZENIA PROFILU ZAGROŻENIA	253
 B	
PRZYKŁADOWY SZABLON PROFILU ZAGROŻENIA	257
 PRZYPISY KOŃCOWE	259