

1.5.3 Nadějná legislativa v oblasti antiphishingu.....	38
Technické důsledky.....	38
Právní důsledky.....	39
1.6 Souhrn.....	39
1.7 Stručný přehled řešení.....	40
Jak se dělí spam.....	40
Historie virtuální kriminality.....	40
Co je phishing?.....	40
Podvod, pátrání a právo.....	41
1.8 Často kladené otázky.....	41
2. Jdeme na phish!.....	43
2.1 Úvod.....	43
2.2 Útok metodou falešná identita.....	45
2.2.1 Zrcadlo.....	45
2.2.2 Nastavení phishingového serveru.....	48
2.2.3 Založení anonymní schránky.....	52
Profi-triky.....	54
Man in the Middle.....	54
2.2.4 Příprava phishingového e-mailu.....	55
2.2.5 Příprava podfuku.....	58
2.2.6 Výsledky.....	61
2.3 Útok přesměrováním.....	61
2.3.1 Příprava e-mailu.....	62
2.3.2 Phishingový server a anonymní schránka.....	63
2.3.3 Příprava podfuku.....	64
2.3.4 Výsledky.....	66
2.4 Útok pomocí vyskakovacího okna.....	66
2.4.1 Vytvoření phishingového serveru.....	67
2.4.2 Příprava e-mailu.....	70
2.4.3 Příprava podfuku.....	71
Nástroje a pastičky.....	73
Kybernetika se neustále vyvíjí.....	73
2.4.4 Výsledky.....	74
2.5 Shmutí.....	74
2.6 Přehled řešení.....	75
Typy phishingových útoků.....	75
Útok za pomoci falešné identity.....	75

Útok přesměrováním.....	75
Útok vyskakovacím oknem.....	75
2.7 Často kladené otázky.....	75
3. E-mail: zbraň hromadného ničení.....	77
3.1 Úvod.....	77
3.2 Základy e-mailu.....	78
E-mailová záhlaví.....	78
Proces doručení e-mailu.....	81
Profi-triky.....	82
Základní komunikace SMTP.....	82
3.2.1 Anonymní e-mail.....	84
Falšování našich záhlaví.....	87
Otevřené přenosy a proxy servery.....	88
Obchodní triky.....	89
Phisherů přecházejí na bezdrátové připojení.....	89
Řetězení serverů proxy, cibulové routování a smíšené sítě.....	90
3.2.2 Sběr e-mailových adres.....	93
Nástroje, cíle a techniky sběru.....	94
Poznámky z podzemí.....	101
Potvrzení příjmu.....	101
Hackeři a internisté.....	101
3.2.3 Zasílání spamů.....	102
Obchodní nástroje.....	102
Anti-Antispam.....	104
3.3 Souhrn.....	108
3.4 Stručný přehled řešení.....	109
Základy e-mailu.....	109
Anonymní e-maily.....	110
Sběr e-mailových adres.....	110
Zasílání spamů.....	110
3.5 Často kladené otázky.....	111
4. Překročení hranice phishingu.....	113
4.1 Úvod.....	113
4.2 Web: stručné shrnutí.....	114
4.2.1 Dynamické HTML.....	114

4.3 Protokol pro přenos hypertextu (HyperText Transfer Protocol)	115
4.3.1 Žádejte a oni mají odpověď.....	115
4.3.2 Pole záhlaví HTTP (Message Header Fields).....	116
Nástroje a pastičky.....	119
Cross-Site Tracing.....	119
4.3.3 Stavové kódy.....	120
4.4 Ztracená důvěra.....	122
4.4.1 Úkol: přesměrování.....	123
Profi-triky.....	129
Načasování replay-attack.....	129
Profi-triky.....	135
Ironie IE.....	135
4.4.2 Úkol: Odrazení dotazu.....	149
4.4.3 Úkol: Odražené chybové stránky.....	160
4.5 Shmutí.....	165
4.6 Stručný přehled řešení.....	166
Nosiče útoků.....	166
Jak se vyhnout zákaznické anti-osvětě.....	166
Přesměrování.....	167
Dotazy.....	167
Stránky 404.....	167
4.7 Často kladené otázky.....	167
5. Odvrácená strana webu.....	169
5.1 Úvod.....	169
5.2 Co je to tedy ten dynamický jazyk HTML?.....	170
5.3 Když se z výhody stane trhlina.....	171
5.3.1 Opatrně s tím odkazem, Evžene.....	175
5.3.2 Taktika uhýbání.....	178
Profi-triky.....	179
Zatemněno kódy.....	179
#include <stdio.h>.....	180
5.3.3 Záplatování píchnuté pneumatiky.....	182
Chraňte se proti podvodníkům!.....	182
Nástroje a pastičky.....	188
Kde dvoufaktorová autentizace nemusí fungovat!.....	188
Směs oříšků.....	188
Kód mnoha barev.....	196

5.4 Tajupné webové stránky.....	200
5.4.1 Cross-Site Request Forgery.....	201
Session riding.....	201
Slepá víra.....	211
Botnety prohlížečů.....	212
Útok na doménové klíče Yahoo!.....	222
5.5 Evoluce phishera.....	228
5.6 Souhrn.....	228
5.7 Stručný přehled řešení.....	229
Speciální funkce nebo trhliny.....	229
Techniky obcházení.....	229
Obchodní e-mail.....	229
Kryptografické implementace.....	229
Botnety prohlížečů.....	229
5.8 Často kladené otázky.....	230
6. Malware, stěhováci peněz a Ma Bell mimo provoz!.....	231
6.1 Úvod.....	231
6.2 Jízda na mule a praní špinavých peněz.....	232
6.2.1 Jak si phishers založí obchod.....	232
6.2.2 Proces přijímání peněz.....	233
Profi-triky.....	234
Přepravené a manipulace.....	234
Povinnosti manažera zásobování.....	234
6.2.3 Western Union.....	235
6.2.4 Závazky a pozice mul.....	235
Činnost v USA a platební karty.....	235
6.3 Phisheři telefonují domů.....	236
6.3.1 Definice dnešních telekomunikací.....	236
6.3.2 Přehled SIP.....	237
Komunikace pomocí SIP.....	238
6.3.3 Fašování identifikace volajícího.....	238
Obchodní triky.....	239
Zneužívání rovnocenných čísel.....	239
Převzetí sítě SBC.....	240
6.3.4 Anonymní telefonáty.....	242
6.3.5 Šílení phisheřů.....	243

6.4 Plazící se záplava	243
6.4.1 Malwarevroce 2004.....	244
Začátek roku 2004.....	244
Polovina roku 2004.....	244
Konec roku 2004.....	245
Trojské koně roku 2004.....	245
6.4.2 Malwarevroce 2005.....	246
Nástroje a pastičky.....	252
Den -1!.....	252
Hromadná pošta.....	252
Styl útoku.....	252
Pozorovaný vývoj.....	253
Botnety.....	254
Anonymní schránka.....	255
6.5 Jak dál s phishingem?	256
6.6 Souhm.....	257
6.7 Stručný přehled řešení	257
Jízda na mule a praní špinavých peněz.....	257
Phishers volají domů.....	257
Plazící se záplava.....	257
Jak dál s phishingem?.....	258
6.8 Často kladené otázky	258
7. Tak nashle a díky za phish!	259
7.1 Úvod.....	259
7.2 Ohlédnutí.....	260
Profi-triky.....	262
Rhybaření na farmě?.....	262
7.3 Na křídlech orla práva	262
7.3.1 Meziřesortní směnice.....	263
7.3.2 Výsledky.....	263
7.3.3 A co spam?.....	264
7.4 Dodavatelé antiphishingových nástrojů.....	265
Nástroje a pastičky.....	267
Řešení, která asi jen tak neprojdou.....	267
7.5 Statistiky pro budoucnost.....	269

7.6 Tracksploatace	272
7.6.1 Ukradneme jejich vlastní síť.....	273
Nástroje a pastičky.....	275
Osádka Defonicu.....	275
7.7 Pošlete mi phish!	276
7.8 Souhm	276
7.9 Stručný přehled řešení	276
Ohlednutí.....	276
Na křídlech orla práva.....	277
Statistiky pro budoucnost.....	277
Tracksploatace.....	277
7.10 Často kladené otázky	277
Rejstřík	279