

O b s a h

Zoznam použitých grafických značiek	6
Predhovor	7
1. Úvodom	9
1.1 BotNety	10
1.2 O úroveň vyššie	12
1.3 Možnosti BotNetov	13
2. Metódy komunikácie	16
2.1 Metóda komunikácie Ports & IP Connectivity	17
2.1.1 Možnosti detekcie.....	21
2.1.2 Detekcia firewallom.....	22
2.1.3 Technológia NAT.....	23
2.2 Metóda prístupu na server HTTP/S, FTP.....	25
2.2.1 HTTP.....	25
2.2.2 HTTPS.....	27
2.2.3 Detekcia HTTP/S	27
2.2.4 FTP.....	28
2.2.5 Sťahovanie/nahrávanie	29
2.3 Ako zostať v anonymite	30
2.3.1 Použitie Proxy Serveru.....	31
2.4 Stavíme BotNety.....	33
2.4.1 Multi BotNets	34
3. Dobývanie systému	38
3.1 Od šírenia po stiahnutie.....	38
3.1.1 Vytváranie plánu koncových skupín	40
3.1.2 Výber mediačných serverov.....	49
3.1.3 Koncové stiahnutie	50
3.2 Infiltrácia do operačného systému	52
3.2.1 Získavanie práv operačného systému	53
3.2.2 Windows Integrity Levels	55
3.3 Infikovanie operačného systému	58
3.3.1 Ukladanie do systému.....	58
3.3.2 Prístup k HIVES.....	63
3.3.3 Konfigurácia databázy registrov – spúšťanie.....	67
3.3.4 Modifikácia databázy registrov.....	86

4. Algoritmizácia	110
4.1 Príklady algoritmizácie.....	110
4.2 Detekčný obraz.....	116
4.2.1 Zneužitie detekčného obrazu.....	120
5. Zakrývanie stôp	128
5.1 Malware sa dostal do detekčnej databázy	128
Záver	132
Summary	133
Literatúra.....	134
O autorovi.....	135
Vecný register.....	136