

## Predhovor

Obsah tejto publikácie vznikol ako doplnkový materiál pre priblíženie fungovania problematiky, princípov sieťových štruktúr a podštruktúr, spolu so zavedením ich infikovaných koncových bodov. Učebný materiál je určený aj pre akreditované predmety a môžu z neho čerpať priaznivci podobných kurzov či spriaznených disciplín.

Predložený učebný text vznikol na základe dlhoročných skúseností z oblasti IT bezpečnosti, konkrétne z rozsiahlych znalostí Operačného Systému platformy Microsoft Windows, praktických testov a návrhov malwaru, testov bezpečnostných utilít alebo tvorením pomocných nástrojov pre opravu, obnovu a podobne. Text bol ďalej zakonponovaný do odvetví ako hacking, cracking, bezpečnostné prieniky a obrany proti nim pre platformy spomínaného Operačného Systému.

Obsahom materiálov je ozrejmiť základné fungovanie BotNetov, popísať metódy a možnosti aktivity vírusov, popísať metodiku komunikácie, ale aj vytknúť výhody a nevýhody jednotlivých postupov komunikácie koncových BootNet bodov, popísať spôsoby „zavádzania sa do systému“, ktorými disponujú malware, možnosti devastácie systému, popis bugov a ich využitie malwarom.

Pokračovaním tejto publikácie bude kniha „*BotNets 2*“, ktorej obsah má dopodrobna v jednotlivých blokoch konkrétnych kódov priblížiť metodiky fungovania vírusov, spôsoby krytia v systéme, vykonávanie útokov, ako aj spôsoby obrany voči antivírusovým a antispywarovým programom.



# Obsah

<b>1. Úvod</b> .....	<b>5</b>
1.1. <i>BotNets</i> .....	8
1.2. <i>O úroveň vyššie</i> .....	9
1.3. <i>Možnosti BotNetov</i> .....	10
<i>Zhrnutie</i> .....	11
<b>2. Metódy komunikácie</b> .....	<b>12</b>
2.1. <i>Metóda prístupu Ports &amp; IP connectivity</i> .....	12
<i>Príklady</i> .....	11
2.1.1. <i>Možnosti detekcie</i> .....	15
2.1.2. <i>Detekcia Firewallom</i> .....	15
2.1.3. <i>Problém NAT</i> .....	15
2.2. <i>Metóda prístupu na server HTTP/S, FTP</i> .....	18
2.2.1. <i>HTTP</i> .....	19
<i>Komunikácia koncového bota</i> .....	19
<i>Komunikácia útočníka</i> .....	20
2.2.2. <i>HTTPS</i> .....	20
2.2.3. <i>Detekcia HTTP/S</i> .....	20
2.2.4. <i>FTP</i> .....	21
<i>Komunikácia koncového bota</i> .....	21
2.2.5. <i>Možnosti detekcie</i> .....	20
2.2.6. <i>Detekcia firewallom</i> .....	20
2.3. <i>Zostávame v anonymite</i> .....	23
<i>Útok z cudzieho počítača</i> .....	23
<i>Útok cez verejné siete</i> .....	23
2.3.1. <i>Použitie proxy serveru</i> .....	24
2.4. <i>Stavíme BotNety</i> .....	25
<i>Príklady</i> .....	25
2.4.1. <i>Multi BotNets</i> .....	26
<i>Zhrnutie</i> .....	28
<b>3. Dobývanie systému</b> .....	<b>29</b>
3.1. <i>Od šírenia po stiahnutie</i> .....	29
3.1.1. <i>Vytvárame plán koncových skupín</i> .....	30
<i>Umenie klamu</i> .....	32
<i>Kamufláž</i> .....	33
<i>Príklady</i> .....	33
3.1.2. <i>Výber mediačných serverov</i> .....	37
<i>Rezervácia mediačných serverov</i> .....	38
3.1.3. <i>Koncové stiahnutie</i> .....	39

3.2. Infiltrácia do operačného systému .....	40
<i>Systémové volania Win. API's</i> .....	41
3.2.1. Dobývanie práv operačného systému .....	41
3.2.2. Windows Integrity Levels .....	43
<i>Spúšťame sa ako Administrátor</i> .....	43
<i>Právo Elevate</i> .....	43
<i>Prístup k System Integrity Level</i> .....	45
3.3. Infikovanie operačného systému .....	46
3.3.1. Ukladáme sa do systému .....	46
<i>Administrátor alebo Guest</i> .....	47
<i>Kam sa uložiť</i> .....	47
<i>Skrývame sa za zložky</i> .....	49
3.3.2. Prístup k HIVES .....	50
<i>Štruktúra HIVES</i> .....	51
3.3.3. Konfigurácia databázy registry - Spúšťanie .....	52
<i>Registrové</i> .....	53
<i>Zložkové</i> .....	62
<i>Úlohové</i> .....	63
<i>Súborové</i> .....	63
<i>Injecting (Hooking)</i> .....	64
<i>Biosové</i> .....	64
<i>Zavedenie ovládačov/služieb do núdzového režimu</i> .....	65
3.3.4. Modifikácia databázy registry .....	66
<i>Modifikácia systémového prostredia</i> .....	66
<i>Modifikácia zoznamu nainštalovaných aplikácií</i> .....	69
<i>Blokovanie správcu úloh - Task Manager</i> .....	70
<i>Blokovanie editora registry - Regedit</i> .....	71
<i>Blokovanie príkazového riadka - Cmd</i> .....	71
<i>Blokovanie Run Command</i> .....	72
<i>Blokovanie User Account Control</i> .....	72
<i>Obídenie prístupu cez windows firewall</i> .....	73
<i>Mazanie inicializovaných koncoviek spustiteľných súborov</i> .....	74
<i>Objects Hijacking</i> .....	75
<i>Zhrnutie</i> .....	81
<b>4. Algoritmizácia .....</b>	<b>82</b>
4.1. <i>Píklady algoritmizácie</i> .....	82
4.2. <i>Detekčný obraz</i> .....	87
4.2.1. <i>Zneužitie detekčného obrazu</i> .....	90
<i>Zhrnutie</i> .....	95
<b>5. Zakrývanie stôp .....</b>	<b>96</b>
5.1. <i>Malware sa dostal do detekčnej databázy</i> .....	96
<i>Scan test</i> .....	96
<i>Heuristická analýza</i> .....	96
<i>Zhrnutie</i> .....	98
<b>6. Záver .....</b>	<b>102</b>
6.1. <i>Acknowledgement</i> .....	102
6.2. <i>O autorovi</i> .....	102
6.3. <i>Odkazy</i> .....	103