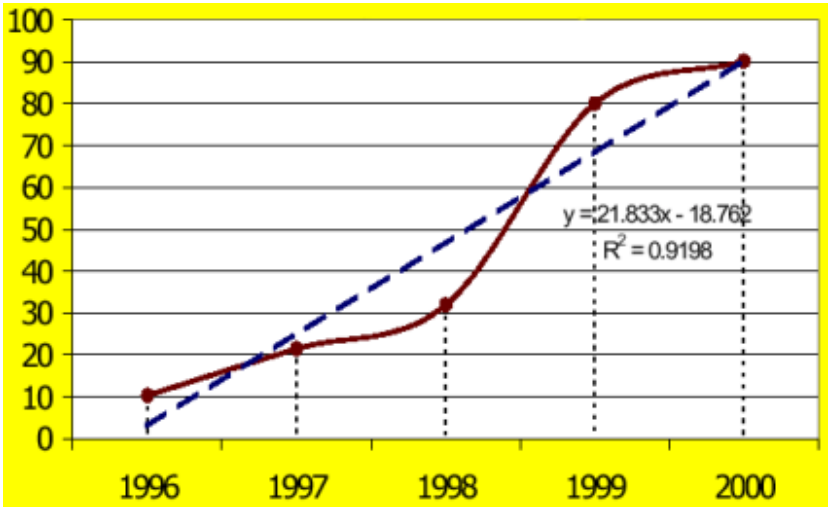
Apžvalga
Virusų siautėjimas 2000-aisiais

Virusų antpuoliai nesiliauja nepaisant įstaigų tinklo administratorių ar kito IT personalo pastangų. Ši apžvalga pabandys parodyti šių metų pokyčius lyginant su ankstesniais.

Palyginimas

Metai	Užkrėstų kompiuterių skaičius Iš 1 tūkst. kompiuterių per vieną mėnesį
1996	10
1997	21
1998	32
1999	80
2000	**90**

Iš šios lentelės matosi, kad virusų ataką patiriančių kompiuterių kiekis kasmet nuolat auga - maždaug po 10 vienam tūkstančiui kompiuterių. 199-aisiais įvykęs kiekybinis šuolis parodo naujos eros - makro ir el.pašto virusų paplitimą. Žemiau grafiškai pailiustruojama virusų dinamika.



Pateikiame vartotojų nuomonę apie padėties pasikeitimą:

Nuomonė	Visi	MS-Word	MS-Excel
Gerokai blogiau	41%	19%	6%
Kažkiek blogiau	35%	21%	8%
Maždaug tokia pati	15%	36%	51%
Šiek tiek geriau	5%	15%	20%
Daug geriau	2%	7%	6%
Nežinau	<1%	1%	9%

Iš šios lentelės matome, kad manoma bendroji padėtis blogėja, nors "Word" ir "Excel" makro virusai baugina jau mažiau.

Dažniausi kenkėjai

Virusų pasaulyje priskaičiuojama jau devynios galybės (jau kalbama apie netolimą 50 tūkst. virusų ar jų variantų skaičių). Tačiau kai kurie jų aplanko kompiuterių naudotojus dažniau nei kiti. Pateikiamas dažniausiai "erzinusių" virusų sąrašas:

Vieta	Pavadinimas	2000 pradžia	1999 pabaiga	1999 pradžia
1.	W97M/Melissa	14.83	33.48	92.86
2.	VBScript	14.76	30.04	
3.	Worm, unspecified	13.83	5.89	
4.	Macro Viruses, unspecified	11.74	14.38	18.63
5.	JS/Kak.Worm	6.48	4.49	0.04
6.	W32/PrettyPark	5.61	0.30	0.07
7.	W97M/Marker	3.82	0.77	0.01
8.	VBS/Freelinks	3.31	0.09	
9.	X97M/Laroux	2.54	0.46	0.04
10.	WIN32/Ska (Happy99)	2.02	0.46	0.18
11.	O97M/Tristate	2.00	0.60	0.11
12.	W97M/Ethan	1.78	1.25	0.21
13.	W32/ExploreZip	1.63	0.21	1.12
14.	W97M/Class	1.35	0.43	0.13
15.	W97M/Locale	1.19	0.01	
16.	W97M/Cap	0.79	0.08	0.03
17.	Trojan Programs	0.62	0.30	0.18

Manau, neturėtų nieko stebinti, kad ištisai pirmauja makro virusai, tačiau tarp populiariausių jau randame ir "VBScript" bei "JavaScript" virusų. Iš populiariausių sąrašo išnyko kelties (boot) sektoriaus bei failų virusai. Pateikiame sumarinę lentelę pagal virusų rūšis

.

Viruso rūšis	2000 pradžia	1999 pabaiga	1999 pradžia
Macro	51,374	112,423	351,623
VB Script	27,066	19,847	3
JavaScript	8,160	1,265	185
File	3,114	73,488	779
Boot	277	14,580	196
Other	0	4,1379	3,861

Pavojingumas

Virusai ne tik plinta ir "nervina", bet ir sukelia darbo sutrikimus. Pateikiama lentelė pagal virusų pavojingumą. Kitoje lentelėje parodoma, keik laiko truko virusų pašalinimo darbai (buvo sustabdytas serverių darbas).

Viruso pavadinimas	Dažnumas	Nukentėjusių PK skaičius
VBS/LoveLetter.A	123	456,570
W97M/Melissa	9	22,350
Other	6	6,355
X97M/Laroux	3	8,150
W32/Funlove	2	1,900
W97M/Ethan	2	4,200
W97M/Marker	2	6,050
W95/CIH	1	1,100
WIN32/Ska (Happy99)	1	1,200
JS/Kak.Worm	1	500
W97M/Class	1	1,500
W32/PrettyPark	1	1,500
Iš viso:	**152**	**511,375**

Valandos	Dažnis	%
0	55	36%
1	3	2%
2	6	4%
3	4	3%
4	4	3%
5	9	6%
10	23	15%
20	13	9%
30	20	13%
40	0	0%
50	14	9%
100	1	1%
200	0	0%
300	0	0%
400	0	0%
500	0	0%
1,000	1	1%
Iš viso:	**152**	**>100%**

Toliau reikia pasiaiškinti, kokį poveikį darbui padarė virusai (aišku, neskaitant pinigų ir llaiko jų antpuolių pasekmėms pašalinti)

Poveikis	Dažnis	%
Darbo efektyvumo sumažėjimas	209	70%
Pažeisti failai	196	66%
Negalima dirbti su PK	150	50%
Nėra prieigos prie duomenų	145	49%
Sutrikimai dirbant su failais	132	44%
Prarasti duomenys	119	40%
Pranešimai ekrane, mirguliaviams ir kt.	99	33%
Vartotojo konfidencialumo pažeidimas	65	22%
Sutrikimai išsaugant duomenis	61	30%
"Smigo" sistema	57	19%
Nestabilus programų darbas	41	14%
Sutrikimai spausdinant	28	9%
Nesukėlė jokių problemų	25	8%
Nežinau	8	3%
Rūpestis kitu praradusiu darbą	7	2%
Kitoks	1	<1%
Iš viso	**299**	**>100%**

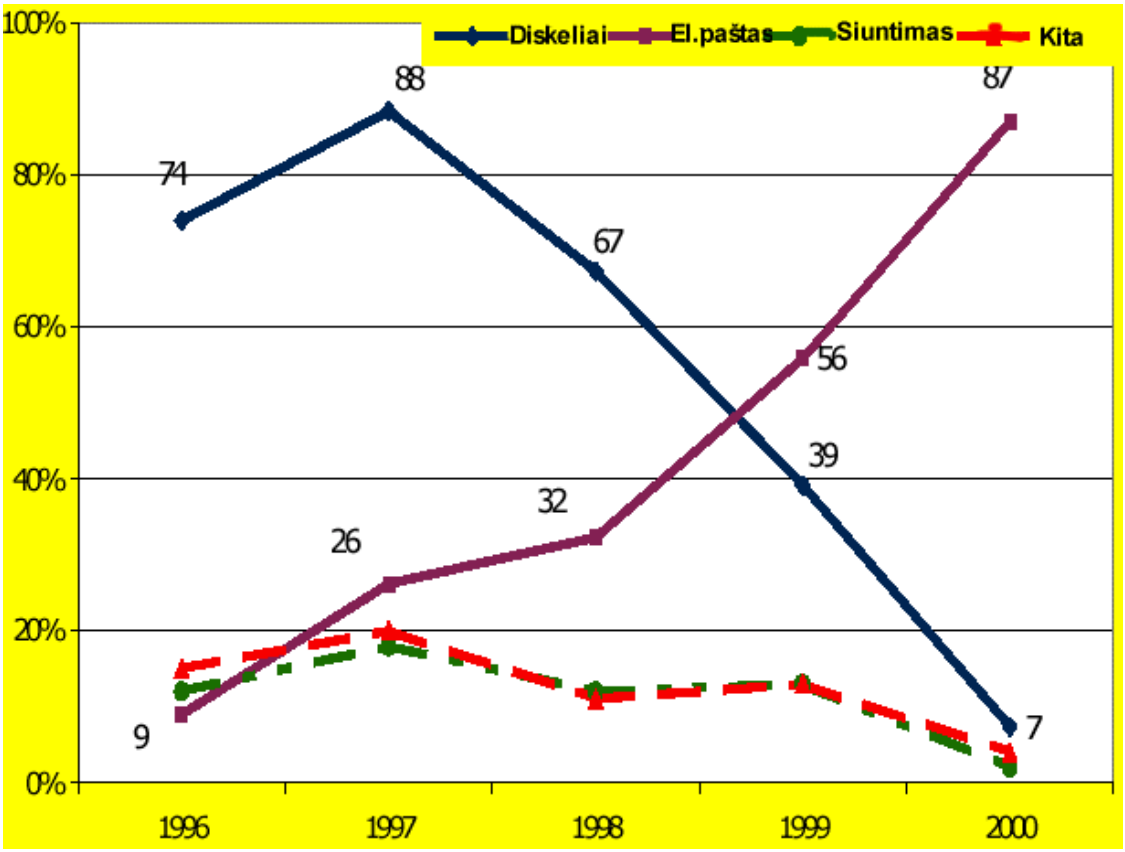
Užkrėtimo šaltinis

Kiltis	1996	1997	1998	1999	2000
El.laiško priedai	9%	26%	32%	56%	87%
Diskeliai (iš namų)	36%	42%	36%	25%	4%
Neaiški	15%	7%	5%	7%	2%
Diskeliai (kiti)	21%	27%	21%	9%	2%
Internetas/BBS/ISP	10%	16%	9%	11%	1%
Kita nei nurodyta	0%	0%	0%	2%	1%
Kažkokia kita	0%	5%	1%	1%	1%
Paimta iš vidinio tinklo	2%	2%	3%	2%	1%
Iš platinamo CD	0%	1%	2%	0%	1%
Diskeliai: demonstraciniai	11%	8%	4%	2%	<1%
Automatinis PĮ platinimas	0%	2%	1%	0%	<1%
Diskeliai: iš tinklo administratoriaus	1%	3%	1%	0%	<1%
Diskeliai: iš piktavalio asmens	0%	1%	1%	0%	<1%
Diskeliai: neaiški PĮ	2%	4%	2%	0%	<1%
Naršymas po WWW	0%	5%	2%	3%	0%
Diskeliai: iš serviso asmens	3%	3%	3%	2%	0%

Sugrupavus pagal pagrindines grupes, gausime:

Kiltis	1996	1997	1998	1999	2000
Diskeliai	74%	88%	67%	39%	7%
El.paštas	9%	26%	32%	56%	87%
Atsisiuntimas	12%	18%	12%	13%	2%
Kita	15%	20%	11%	13%	4%

Grafinis polyčių pasikeitimas:



Antivirusinių programų efektyvumas

Pagrindinė apsaugos nuo kompiuterių virusų priemonė yra antivirusinės programos. Šioje lentelėje nurodoma, kurios jų buvo dažniausiai efektyviai naudotos (virš 100% todėl, kad kai kurios firmos naudoja ne vieną antivirusinę programą):

Produktas	Dažnis	%
Network Asociates (McAfee)	161	54%
Symantec Corp (Norton)	124	32
Computer Associates	34	11%
Command Software	13	4%
Trend Micro (OfficeScan)	7	2%
Kitos	7	2%
Nenaudota	3	1%
Nežinomos	2	1%
Kaspersky Lab (AVP)	1	<1%
F-Secure	1	<1%
Alladin Knowledge Systems (eSafe Protect)	1	<1%
Norman Data Defense	1	<1%
Intel	1	<1%
Sophos Plc	1	<1%
Iš viso	**297**	**> 100%**

Apibendrinimas

Kasmet vis daugiau kompiuterių nukenčia nuo kompiuterių virusų, kirminų, "Trojos arklių" ir kitų piktybiškų programų. Tai reiškia papildomas išlaidas, didesnį pavojų duomenims bei darbo kokybei.

Beveik išnyko kelties (boot) sektoriaus virusai. Tai gali būti paaiškinama paplitusiu antivirusinių programų naudojimu, kurios gana gerai apsaugo nuo šios rūšies blogiečių. Be to, nereikia pamiršti, kad didžioji dauguma kompiuterių naudotojų dirba "Windows" 9x/NT/2000 terpėse, kuriose 1) kelties virusų plitimo galimybės mažesnės; 2) vis rečiau naudojami diskeliai (išaugp duomenų apimtys ir jie dažnai tiesiog netelpa į diskelius); 3) :Windows" terpė pasidarė didesnis "taikinys" virusams.

Smarkiai padidėjo Internetu (el.paštu, WWW ir kt.) plintančių virusų. Tai nenuostabu, nes plačiai naudojamos "Microsoft" firmos "Outlook" programos (kaip ir "Word" ir kitos MS Office" programos turi programavimo terpę, kurioje galima vykdyti "Visual Basic" arba "VBScript" kalbomis parašytą kodą. Tai sukėlė "Melissa", "I llove you" el.pašto virusų epidemijas. Jų ypatybė - pasaulyje paplinta akimirksniu ir užkrečia milžinišką kiekį kompiuterių.

Tai kelia didesnį poreikį antivirusinei programinei įrangai, kuri sugebėtų stipriau pasipriešinti ***nežinomiems*** kenkėjams. Dažnai, jei užtvara pralaužta, naudos iš AV programų mažai. Iš pasyvaus stebėjimo (kad ir turint 70% padengima AV produktais) reikia pereiti prie aktyvios gynybos - filtravimo, veikimo ribojimo, programų režimų nustatymo, "smėlio dėžių" ir kitų metodų.saugesnio Didesnį dėmesį skirti ne darbo vietų PK, o "įvadams" - apsaugos skydams (firewall), "proksiams", el.pašto serveriams, Interneto protokolams ir kt.- t.y. stengiantis "nuskinti" virusus iki patenkant į įstaigą.