



The Evolution of Spam and Messaging Security

Neil Cook

Head of Technology Services, EMEA, Cloudmark, Inc.

ESNOG, Barcelona
October, 2008





A Glossary of Recent Security Terms

phishing, pharming, attack surface, botnets, bot herders,
packet inspection, honeypots, spyware, rootkits,
zero day, underground economy, naive bayesian, vishing,
two factor authentication, active scripting, spear phishing, pentests,
pretexting, differentiated security, adware,
DNS amplification, zombies, click fraud

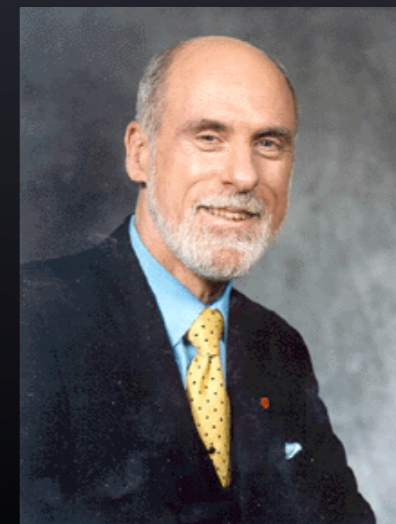




Industry Luminaries on the State of Security

"... Internet is at serious risk ...
botnets could eat the Internet."

- Vint Cerf, Father of Internet
World Economic Forum



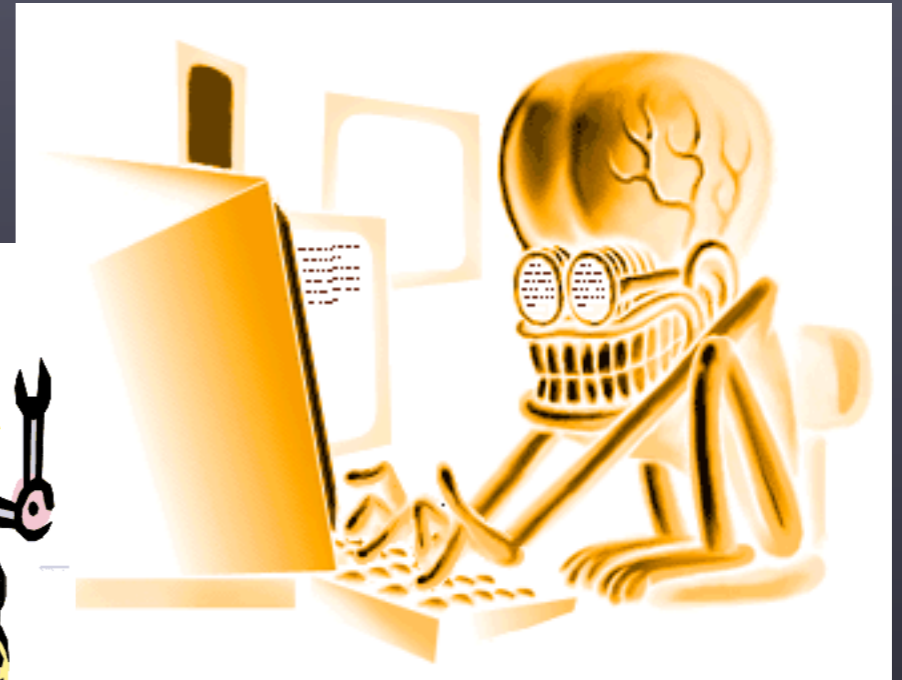
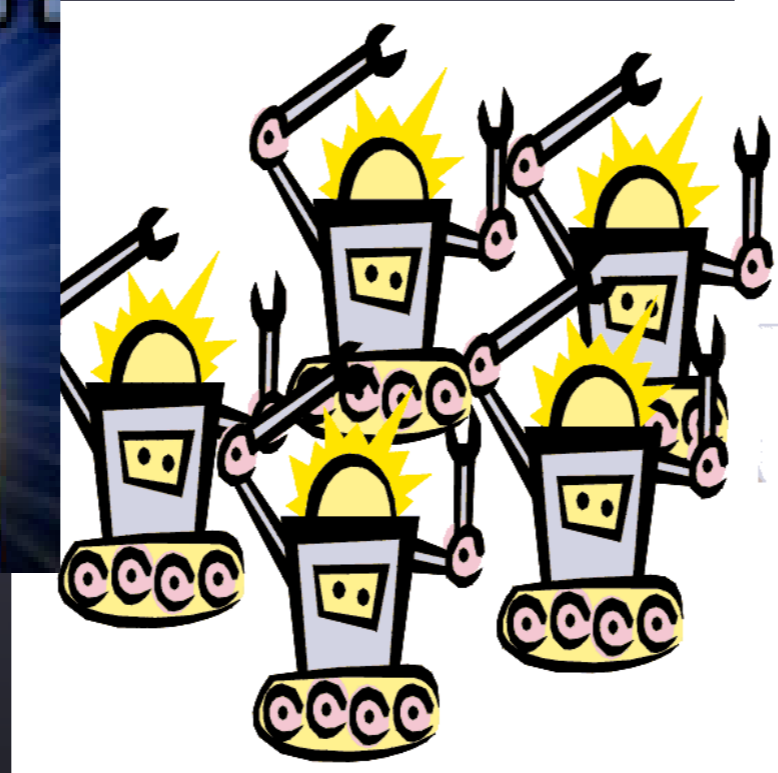
Industry Luminaries on the State of Security

"... even the most innocent of
websites can ruin your life ..."

- Dr Jose Nazario, Author

Defense and Detection Strategies Against Internet Worms





Should we be really really afraid?



Evolution and Future Trends



Evolution and Future Trends

Computer security is a very
splintered subject.

Some coherence would be nice.

Spam is a microcosm
of computer security.
No, really!

Analysis of Evolution of Spam = Fundamental Principles of Computer Security

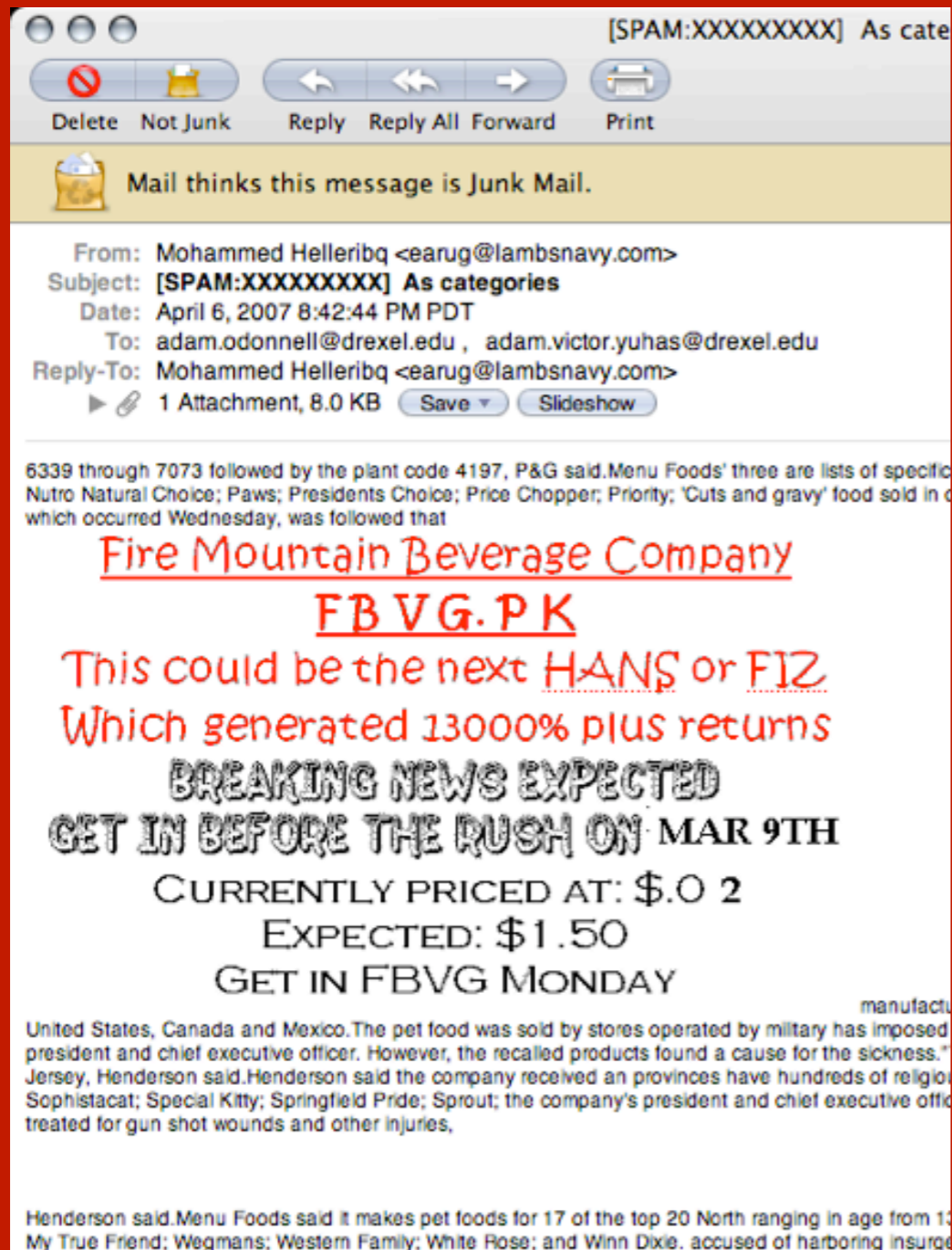


Everyone can observe spam.

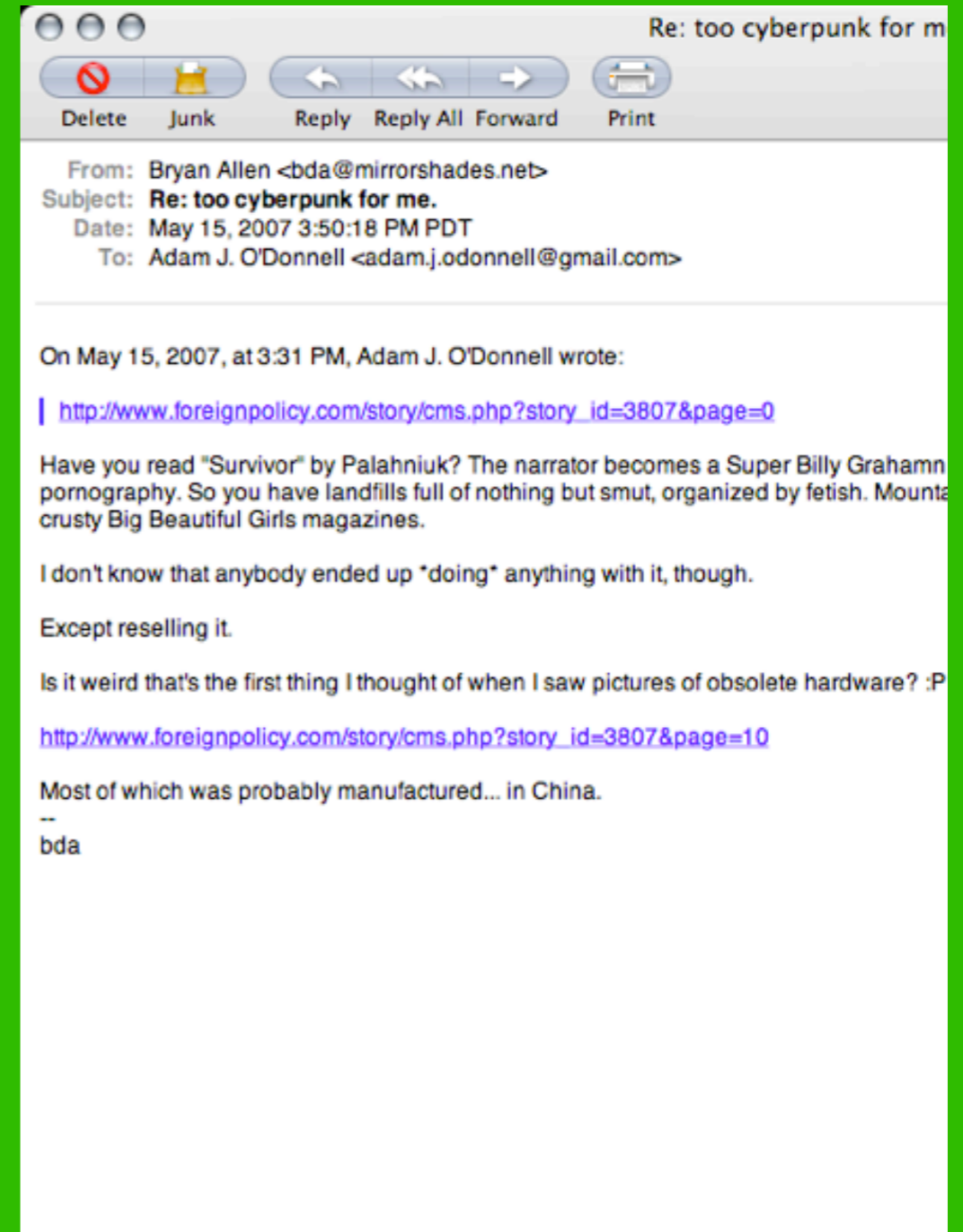




Spam



Legitimate





ffa0602cf4bb7dfed6d36b82f037c532

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

00000	4D 5A 90 00	03 00 00 00	04 00 00 00	50 45 00 00	4C 01 02 00	00 00	MZ.....PE..L.....
00016	00 00 00 00	00 00 00 00	00 00 E0 00	0F 01 0B 01	00 00 00 28	02 00(.....
0002C	00 86 0F 00	00 00 00 00	9B AA 13 00	00 10 00 00	0C 00 00 00	00 00
00042	40 00 00 10	00 00 00 02	00 00 04 00	00 00 00 00	00 00 04 00	00 00	@.....
00058	00 00 00 00	00 B0 13 00	00 02 00 00	00 00 00 00	02 00 00 00	00 00
0006E	10 00 00 10	00 00 00 00	10 00 00 10	00 00 00 00	00 00 10 00	00 00
00084	00 00 00 00	00 00 00 00	60 AB 13 00	34 00 00 00	00 00 00 00	00 004.....
0009A	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
000B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
000C6	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
000DC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
000F2	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
00108	74 00 00 00	00 D0 11 00	00 10 00 00	00 00 00 00	00 00 00 00	00 00	t.....
0011E	00 00 00 00	00 00 00 00	00 00 E0 00	00 C0 00 00	00 00 74 61	00 00ta..
00134	00 D0 01 00	00 E0 11 00	94 CB 01 00	00 02 00 00	00 00 00 00	00 00
0014A	00 00 00 00	00 00 E0 00	00 C0 4B 45	52 4E 45 4C	33 32 2E 64	6C 6CKERNEL32.dll
00160	00 00 00 4C	6F 61 64 4C	69 62 72 61	72 79 41 00	00 47 65 74	50 72	...LoadLibraryA..GetPr
00176	6F 63 41 64	64 72 65 73	73 00 00 00	00 00 00 00	00 00 00 00	00 00	ocAddress.....
0018C	00 00 00 00	00 00 00 00	00 00 00 00	56 AB 53 00	4A AB 53 00	4C ABV.S.J.S.L.
001A2	53 00 98 01	40 00 00 10	40 00 00 E0	51 00 01 40	42 00 01 60	42 00	S...@...Q..@B...`B.

Hex Little Endian Insert Offset: 0 Selection: 0

fada54255e1fa15c55ffdde4f4f96073

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

00000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	B8 00 00 00	00 00	MZ.....PE..L.....
00016	00 00 40 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00	..@.....
0002C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	E8 00 00 00	0E 1F
00042	BA 0E 00 B4	09 CD 21 B8	01 4C CD 21	54 68 69 73	20 70 72 6F	67 72!..L.!This progr
00058	61 6D 20 63	61 6E 6E 6F	74 20 62 65	20 72 75 6E	20 69 6E 20	44 4F	am cannot be run in D0
0006E	53 20 6D 6F	64 65 2E 0D	0D 0A 24 00	00 00 00 00	00 00 69 38	F6 92	S mode....\$......i8..
00084	2D 59 98 C1	2D 59 98 C1	2D 59 98 C1	AE 51 C5 C1	2F 59 98 C1	2D 59	-Y...Y...Y...Q.../Y...-Y
0009A	98 C1 2E 59	98 C1 C5 46	92 C1 37 59	98 C1 AE 45	96 C1 26 59	98 C1	...Y...F...7Y...E...&Y..
000B0	2D 59 98 C1	7D 59 98 C1	4F 46 8B C1	24 59 98 C1	C5 46 93 C1	29 59	-Y...Y...OF...\$Y...F...Y
000C6	98 C1 52 69	63 68 2D 59	98 C1 00 00	00 00 00 00	00 00 00 00	00 00	..Rich-Y.....
000DC	00 00 00 00	00 00 00 00	00 00 00 00	50 45 00 00	4C 01 03 00	06 C2PE..L.....
000F2	96 40 00 00	00 00 00 00	00 00 E0 00	0F 01 0B 01	06 00 00 3E	00 00	.@.....>..
00108	00 22 00 00	00 00 00 00	00 80 01 00	00 10 00 00	00 50 00 00	00 00	..P.....
0011E	40 00 00 10	00 00 00 02	00 00 04 00	00 00 00 00	00 00 04 00	00 00	@.....
00134	00 00 00 00	00 90 01 00	00 04 00 00	00 00 00 00	02 00 00 00	00 00
0014A	10 00 00 10	00 00 00 00	10 00 00 10	00 00 00 00	00 00 10 00	00 00
00160	00 00 00 00	00 00 00 00	14 80 00 00	8A 00 00 00	00 00 00 00	00 00
00176	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
0018C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
001A2	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00

Hex Little Endian Insert Offset: Selection:

fbde1a50e7a2c3ddc8a0dfd8bf0ad0bb

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

00000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	B8 00 00 00	00 00	MZ.....PE..L.....
00016	00 00 40 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00	..@.....
0002C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	C8 00 00 00	0E 1F
00042	BA 0E 00 B4	09 CD 21 B8	01 4C CD 21	54 68 69 73	20 70 72 6F	67 72!..L.!This progr
00058	61 6D 20 63	61 6E 6E 6F	74 20 62 65	20 72 75 6E	20 69 6E 20	44 4F	am cannot be run in D0
0006E	53 20 6D 6F	64 65 2E 0D	0D 0A 24 00	00 00 00 00	00 00 05 C9	A0 DB	S mode....\$......
00084	41 A8 CE 88	41 A8 CE 88	41 A8 CE 88	C2 B4 C0 88	40 A8 CE 88	28 B7	A...A...A.....@...(. ..B...@...RichA...
0009A	C7 88 42 A8	CE 88 A8 B7	C3 88 40 A8	CE 88 52 69	63 68 41 A8	CE 88RichA...
000B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
000C6	00 00 50 45	00 00 4C 01	03 00 CD DA	A8 44 00 00	00 00 00 00	00 00	..PE..L.....D.....
000DC	E0 00 0F 01	0B 01 06 00	00 40 00 00	00 30 00 00	00 B0 00 00	F0 F3@...@.....
000F2	00 00 00 C0	00 00 00 00	01 00 00 00	40 00 00 10	00 00 00 02	00 00@.....
00108	04 00 00 00	06 00 54 0B	04 00 00 00	00 00 00 00	00 30 01 00	00 10T.....@.....
0011E	00 00 00 00	00 00 02 00	00 00 00 00	10 00 00 10	00 00 00 00	10 00
00134	00 10 00 00	00 00 00 00	10 00 00 00	00 00 00 00	00 00 00 00	2C 2D,-.....
0014A	01 00 9C 00	00 00 00 00	01 00 2C 2D	00 00 00 00	00 00 00 00	00 00,-.....
00160	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
00176	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
0018C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00
001A2	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00

Hex Little Endian Insert Offset: 0 Selection: 0

WINWORD.EXE

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

0000000	4D 5A 90 00	03 00 00 00	04 00 00 00	FF FF 00 00	B8 00 00 00	00 00	MZ.....PE..L.....
0000016	00 00 40 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00	..@.....
000002C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	20 01 00 00	0E 1F
0000042	BA 0E 00 B4	09 CD 21 B8	01 4C CD 21	54 68 69 73	20 70 72 6F	67 72!..L.!This progr
0000058	61 6D 20 63	61 6E 6E 6F	74 20 62 65	20 72 75 6E	20 69 6E 20	44 4F	am cannot be run in D0
000006E	53 20 6D 6F	64 65 2E 0D	0D 0A 24 00	00 00 00 00	00 00 02 B0	88 C2	S mode....\$......
0000084	46 D1 E6 91	46 D1 E6 91	46 D1 E6 91	AE CE E2 91	44 D1 E6 91	C5 CD	F...F...F.....D.....
000009A	E8 91 43 D1	E6 91 43 D0	E9 91 45 D1	E6 91 46 D1	E6 91 47 D1	E6 91	..C...C...E...F...G...
00000B0	55 D9 B9 91	4C D1 E6 91	C8 D9 B9 91	47 D1 E6 91	B5 D6 B8 91	44 D1	U...L.....G.....D...
00000C6	E6 91 AE CE	EC 91 4F D1	E6 91 9C F2	FA 91 44 D1	E6 91 55 D9	B8 910.....D...U...
00000DC	4F D1 E6 91	46 D1 E7 91	C6 D8 E6 91	43 D0 86 91	40 D1 E6 91	43 D0	O...F...C...C...@...C...
00000F2	B9 91 9B D0	E6 91 43 D0	BA 91 47 D1	E6 91 AA DA	B8 91 47 D1	E6 91C...G.....G...
000108	43 D0 BC 91	47 D1 E6 91	52 69 63 68	46 D1 E6 91	00 00 00 00	00 00	C...G...RichF.....
00011E	00 00 50 45	00 00 4C 01	05 00 0C 91	B6 45 00 00	00 00 00 00	00 00	..PE..L.....E.....
000134	E0 00 0F 01	0B 01 07 0A	00 A6 A9 00	00 18 12 00	00 14 02 00	B0 19
00014A	00 00 00 10	00 00 00 E0	A8 00 00 00	00 30 00 10	00 00 00 02	00 00@.....
000160	04 00 00 00	0A 00 00 00	04 00 00 00	00 00 00 00	00 20 BE 00	00 04
000176	00 00 9F CA	BB 00 02 00	00 00 00 00	10 00 00 10	00 00 00 00	10 00
00018C	00 10 00 00	00 00 00 00	10 00 00 00	6C 61 A9 00	95 00 00 00	98 7Fla.....
0001A2	A9 00 8C 00	00 00 00 70	B7 00 10 A3	06 00 00 00	00 00 00 00	00 00p.....

Hex Little Endian Insert Offset: 0 Selection: 0

ffa0602cf4bb7dfed6d36b82f037c532

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

```
0000 4D 5A 90 00 03 00 00 00 04 00 00 00 50 45 00 00 4C 01 02 00 00 00 MZ.....PE..L....
00016 00 00 00 00 00 00 00 00 00 00 E0 00 0F 01 0B 01 00 00 00 28 02 00 .....(.....
0002C 00 06 0F 00 00 00 00 00 9B AA 13 00 00 10 00 00 0C 00 00 00 00 00 .....
00042 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 @.....
00058 00 00 00 00 00 00 13 00 00 02 00 00 00 00 00 00 00 02 00 00 00 00 00 .....
0006E 10 00 00 10 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 00 00 00 .....
00084 00 00 00 00 00 00 00 00 60 AB 13 00 34 00 00 00 00 00 00 00 00 00 .....
0009A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000C6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000DC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000F2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00108 74 00 00 00 00 00 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 .....
0011E 00 00 00 00 00 00 00 00 00 00 E0 00 00 C0 00 00 00 00 74 61 00 00 .....ta..
00134 00 D0 01 00 00 E0 11 00 94 CB 01 00 00 02 00 00 00 00 00 00 00 00 .....
0014A 00 00 00 00 00 00 E0 00 00 C0 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C .....KERNEL32.dll
00160 00 00 00 4C 6F 61 64 4C 69 62 72 61 72 79 41 00 00 47 65 74 50 72 ...LoadLibraryA..GetPr
00176 6F 63 41 64 64 72 65 73 73 00 00 00 00 00 00 00 00 00 00 00 00 00 ocAddress.....
0018C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 56 AB 53 00 4A AB 53 00 4C AB .....V.S.J.S.L.
001A2 53 00 98 01 40 00 00 10 40 00 00 E0 51 00 01 40 42 00 01 60 42 00 .....S...@...Q...@B...B.
```

Hex Little Endian Insert Offset: 0 Selection: 0

Spyware

fada54255e1fa15c55ffdde4f4f96073

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

```
0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 MZ.....
00016 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..@.....
0002C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 0E 1F .....
00042 BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 .....!.L!This progr
00058 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F am cannot be run in D0
0006E 53 20 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 69 38 F6 92 S mode...$......i8..
00084 2D 59 98 C1 2D 59 98 C1 2D 59 98 C1 E 51 C5 C1 2F 59 98 C1 2D 59 -Y...Y...Y...Q.../Y...Y
0009A 98 C1 2E 59 98 C1 C5 4 9 C1 37 59 98 C1 A5 45 95 C1 26 59 98 C1 ..Y...F..7Y...E...&Y..
000B0 2D 59 98 C1 7D 59 98 C1 45 98 C1 45 98 C1 45 98 C1 45 98 C1 29 5 -..Y...OF...$Y...F...Y
000C6 98 C1 52 69 63 68 2D 59 98 C1 45 98 C1 45 98 C1 45 98 C1 45 98 C1 ..Rich-Y.....
000DC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 4C 00 00 00 06 C2 .....PE..L....
000F2 96 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..@.....>..
00108 00 22 00 00 00 00 00 00 00 00 80 01 00 00 10 00 00 00 50 00 00 00 00 ..".....P...
0011E 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 00 04 00 00 @.....
00134 00 00 00 00 00 90 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 .....
0014A 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 .....
00160 00 00 00 00 00 00 00 00 14 80 00 00 8A 00 00 00 00 00 00 00 00 00 .....
00176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0018C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001A2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....Offset: Selection:
```

Hex Little Endian Insert Offset: Selection:

Adware

fbde1a50e7a2c3ddc8a0dfd8bf0ad0bb

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

```
0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 MZ.....
00016 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..@.....
0002C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 0E 1F .....
00042 BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 .....!.L!This progr
00058 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F am cannot be run in D0
0006E 53 20 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 05 C9 A0 DB S mode...$......
00084 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 A...A.....@...(.
0009A E8 91 43 D1 E6 91 43 D1 E6 91 43 D1 E6 91 43 D1 E6 91 43 D1 E6 91 C...C...E...F...G...
000B0 55 D9 B9 91 4C D1 E6 91 4C D1 E6 91 4C D1 E6 91 4C D1 E6 91 4C D1 E6 91 ..L.....G.....D.
000C6 E6 91 AE CE EC 91 4F D1 E6 91 4F D1 E6 91 4F D1 E6 91 4F D1 E6 91 ..PE.....D...
000DC 4F D1 E6 91 46 D1 E7 91 46 D1 E7 91 46 D1 E7 91 46 D1 E7 91 46 D1 E7 91 .....@.....
000F2 B9 91 9B D0 E6 91 43 D0 BA 91 47 D1 E6 91 AA DA B8 91 47 D1 E6 91 .....C...G.....G...
00108 43 D0 BC 91 47 D1 E6 91 52 69 63 68 46 D1 E6 91 00 00 00 00 00 00 C...G...RichF.....
0011E 00 00 50 45 00 00 4C 01 05 00 0C 91 B6 45 00 00 00 00 00 00 00 00 ..PE..L.....E.....
00134 E0 00 0F 01 0B 01 07 0A 00 A6 A9 00 00 18 12 00 00 14 02 00 B0 19 .....
0014A 00 00 00 10 00 00 00 E0 A8 00 00 00 00 30 00 10 00 00 00 02 00 00 .....0.....
00160 04 00 00 00 0A 00 00 00 04 00 00 00 00 00 00 00 00 20 BE 00 00 04 .....
00176 00 00 9F CA BB 00 02 00 00 00 00 00 10 00 00 10 00 00 00 10 00 .....
0018C 00 10 00 00 00 00 00 00 10 00 00 00 6C 61 A9 00 95 00 00 98 7F .....la.....
001A2 A9 00 8C 00 00 00 00 70 B7 00 10 A3 06 00 00 00 00 00 00 00 00 .....p.....Offset: Selection:
```

Hex Little Endian Insert Offset: Selection: 0

MS Word Doc

WINWORD.EXE

Save Copy Cut Paste Undo Redo Hex Text search Go To Offset Find

```
000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 MZ.....
000016 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..@.....
00002C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0E 1F .....
000042 BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 .....!.L!This progr
000058 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F am cannot be run in D0
00006E 53 20 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 02 B0 88 C2 S mode...$......
000084 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 46 D1 E6 91 F...F.....D.....
00009A E8 91 43 D1 E6 91 43 D1 E6 91 43 D1 E6 91 43 D1 E6 91 43 D1 E6 91 C...C...E...F...G...
0000B0 55 D9 B9 91 4C D1 E6 91 4C D1 E6 91 4C D1 E6 91 4C D1 E6 91 4C D1 E6 91 ..L.....G.....D.
0000C6 E6 91 AE CE EC 91 4F D1 E6 91 4F D1 E6 91 4F D1 E6 91 4F D1 E6 91 ..PE.....D...U...
0000DC 4F D1 E6 91 46 D1 E7 91 46 D1 E7 91 46 D1 E7 91 46 D1 E7 91 46 D1 E7 91 .....F.....C...@...C...
0000F2 B9 91 9B D0 E6 91 43 D0 BA 91 47 D1 E6 91 AA DA B8 91 47 D1 E6 91 .....C...G.....G...
000108 43 D0 BC 91 47 D1 E6 91 52 69 63 68 46 D1 E6 91 00 00 00 00 00 00 C...G...RichF.....
00011E 00 00 50 45 00 00 4C 01 05 00 0C 91 B6 45 00 00 00 00 00 00 00 00 ..PE..L.....E.....
000134 E0 00 0F 01 0B 01 07 0A 00 A6 A9 00 00 18 12 00 00 14 02 00 B0 19 .....
00014A 00 00 00 10 00 00 00 E0 A8 00 00 00 00 30 00 10 00 00 00 02 00 00 .....0.....
000160 04 00 00 00 0A 00 00 00 04 00 00 00 00 00 00 00 00 20 BE 00 00 04 .....
000176 00 00 9F CA BB 00 02 00 00 00 00 00 10 00 00 10 00 00 00 10 00 .....
00018C 00 10 00 00 00 00 00 00 10 00 00 00 6C 61 A9 00 95 00 00 98 7F .....la.....
0001A2 A9 00 8C 00 00 00 00 70 B7 00 10 A3 06 00 00 00 00 00 00 00 00 .....p.....Offset: Selection:
```

Hex Little Endian Insert Offset: Selection: 0

Malware

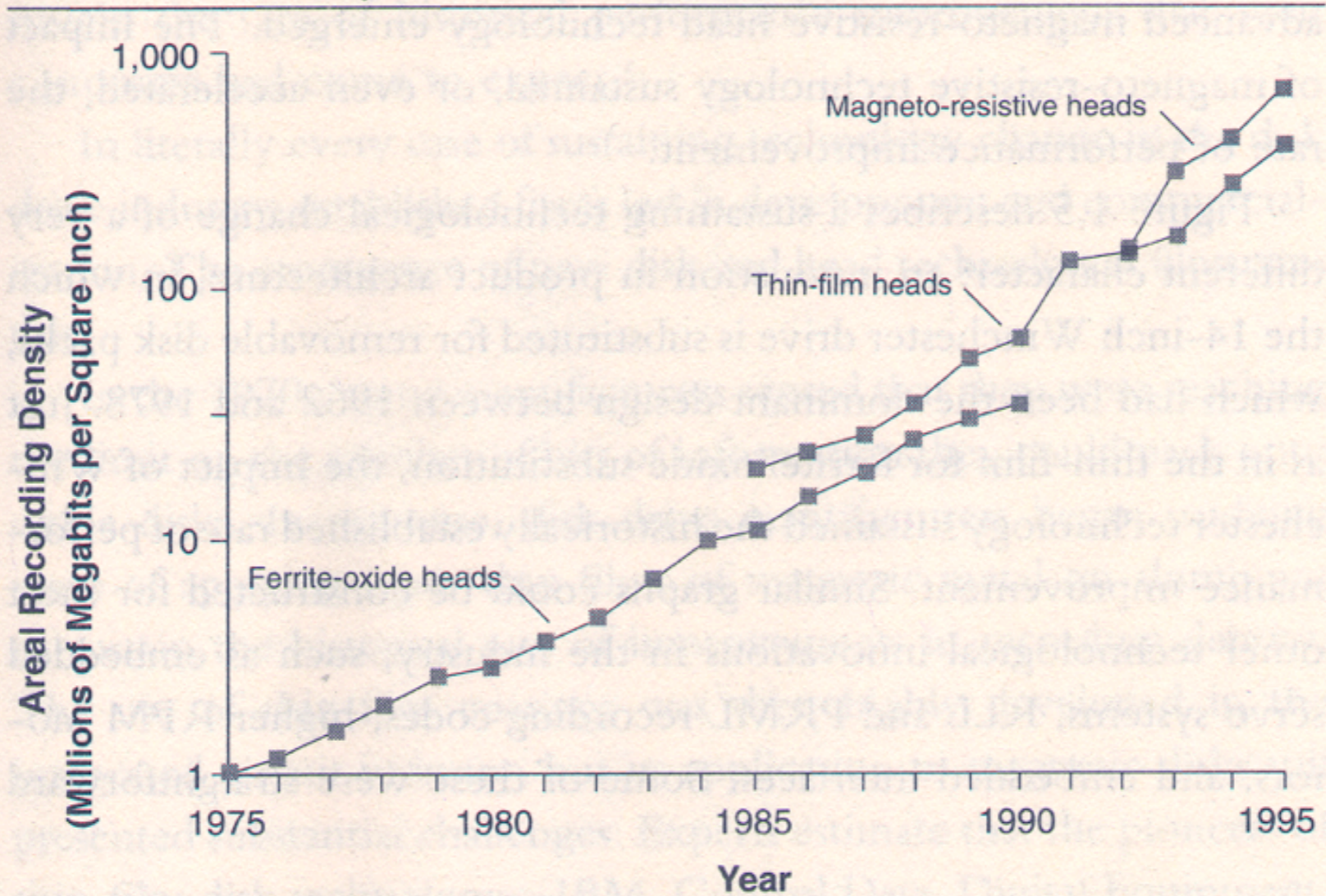
Spam is highly evolved.



Spam is still here.

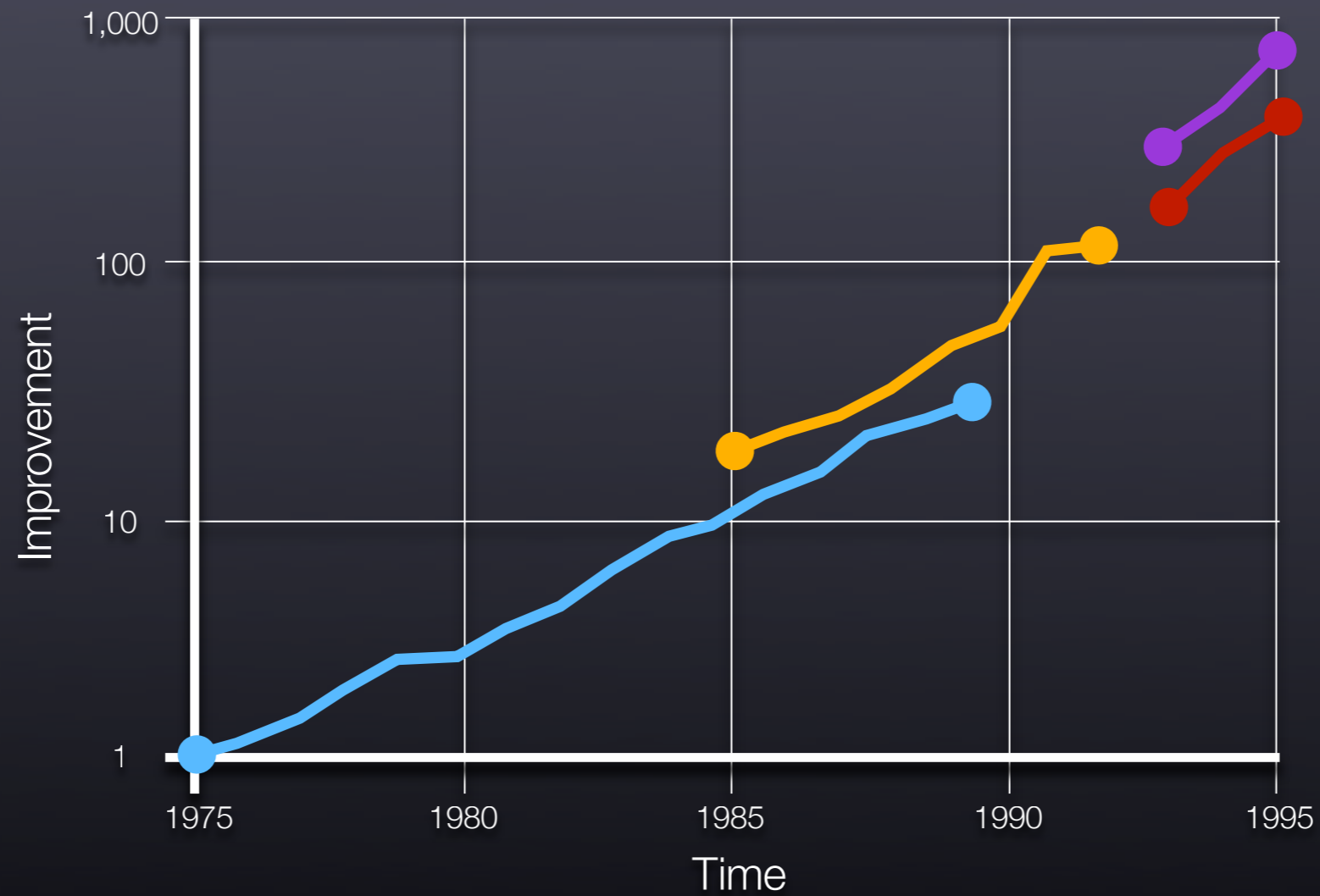


Figure 1.4 Impact of New Read-Write Head Technologies in Sustaining the Trajectory of Improvement in Recording Density



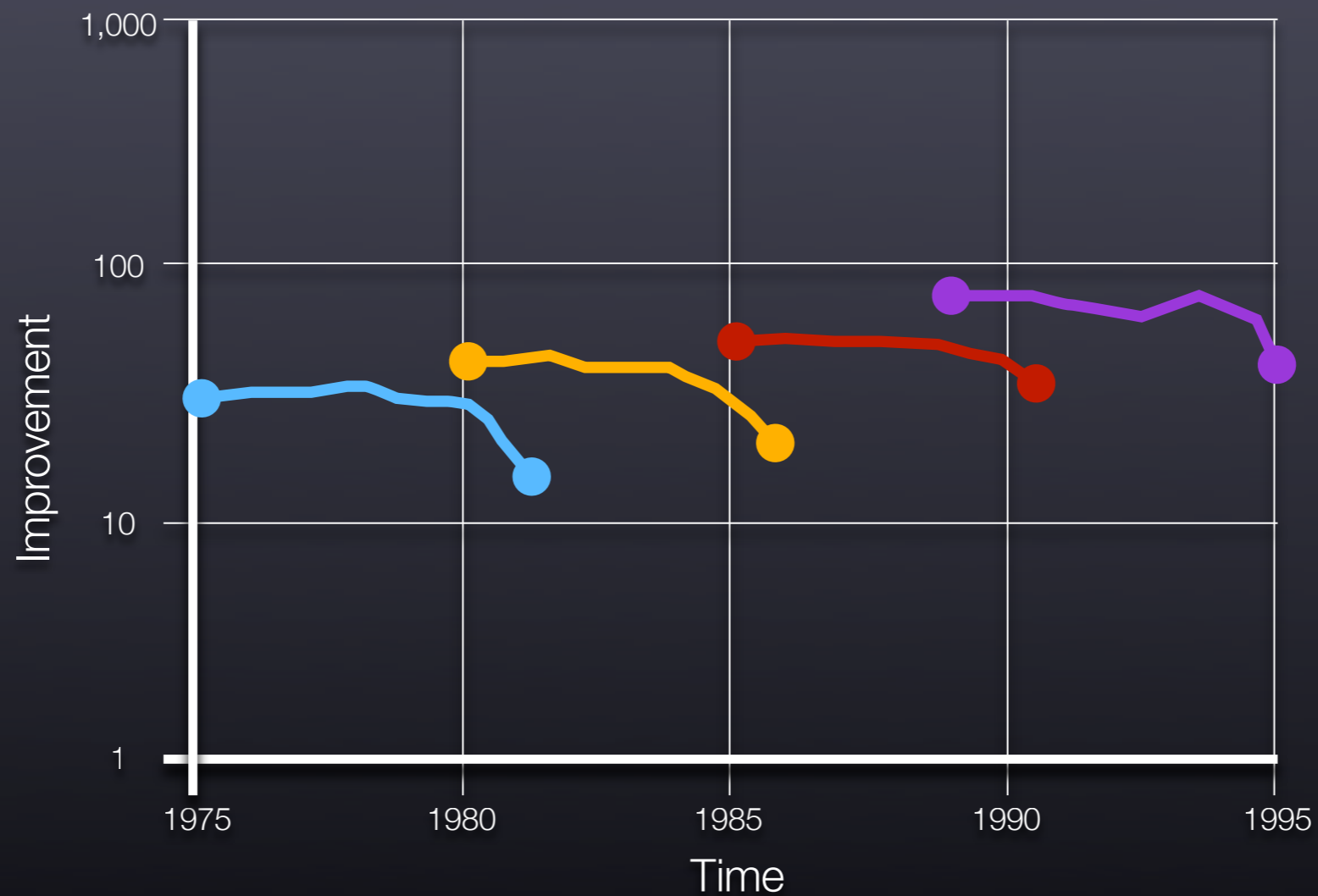
Source: Data are from various issues of *Disk/Trend Report*.

Moore's Law



Innovation A Innovation B Innovation C Innovation D

The Security Curve



Innovation A Innovation B Innovation C Innovation D

Fundamental Principle #1

Good security must
thrive in an environment
that is intentionally hostile to it.

The focus of security
should be the attacker.



The motivation of attacker
is to make money.

We can cast the security problem
as a problem of economics.



Fundamental Principle #2

The Optimal Target Selection Strategy

The attacker selects
the most valuable and least
defended targets.

Spam is BIG...

...because email is the #1
Internet application and was
designed with no security.



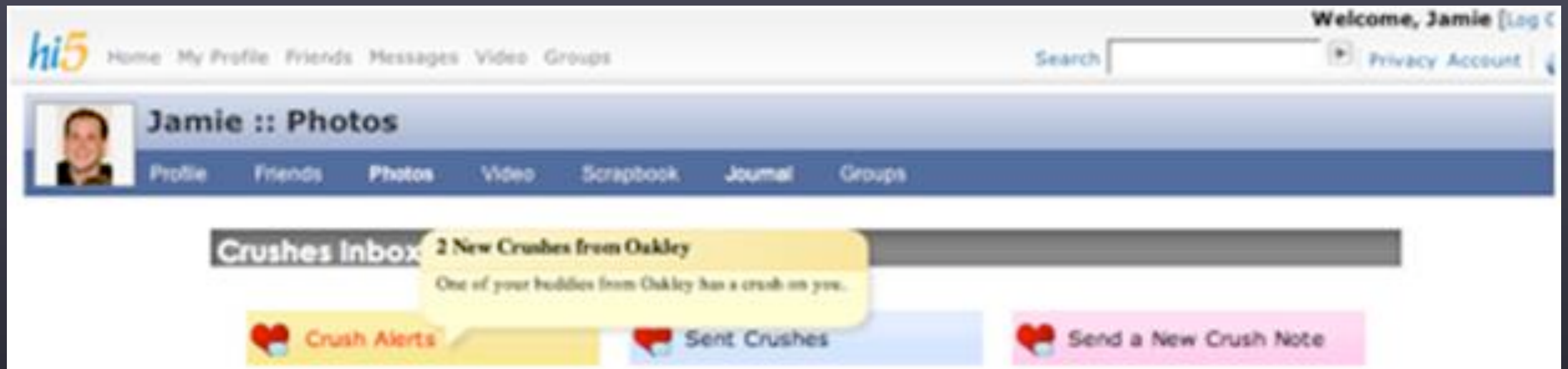
Microsoft Windows
is attacked more...

... because 96% of the
computers in the world run
Windows, and security is poor.

Social networks are
being attacked...

... because they are the top
websites, and are poorly defended

Social Networking Spam



Someone has a crush on you! www.YouGotCrushedOn.com

Someone has a crush on you! www.GotSpringCrush.com

Someone has a crush on you! www.YouGotCrushedOn.com

Categories of Spam

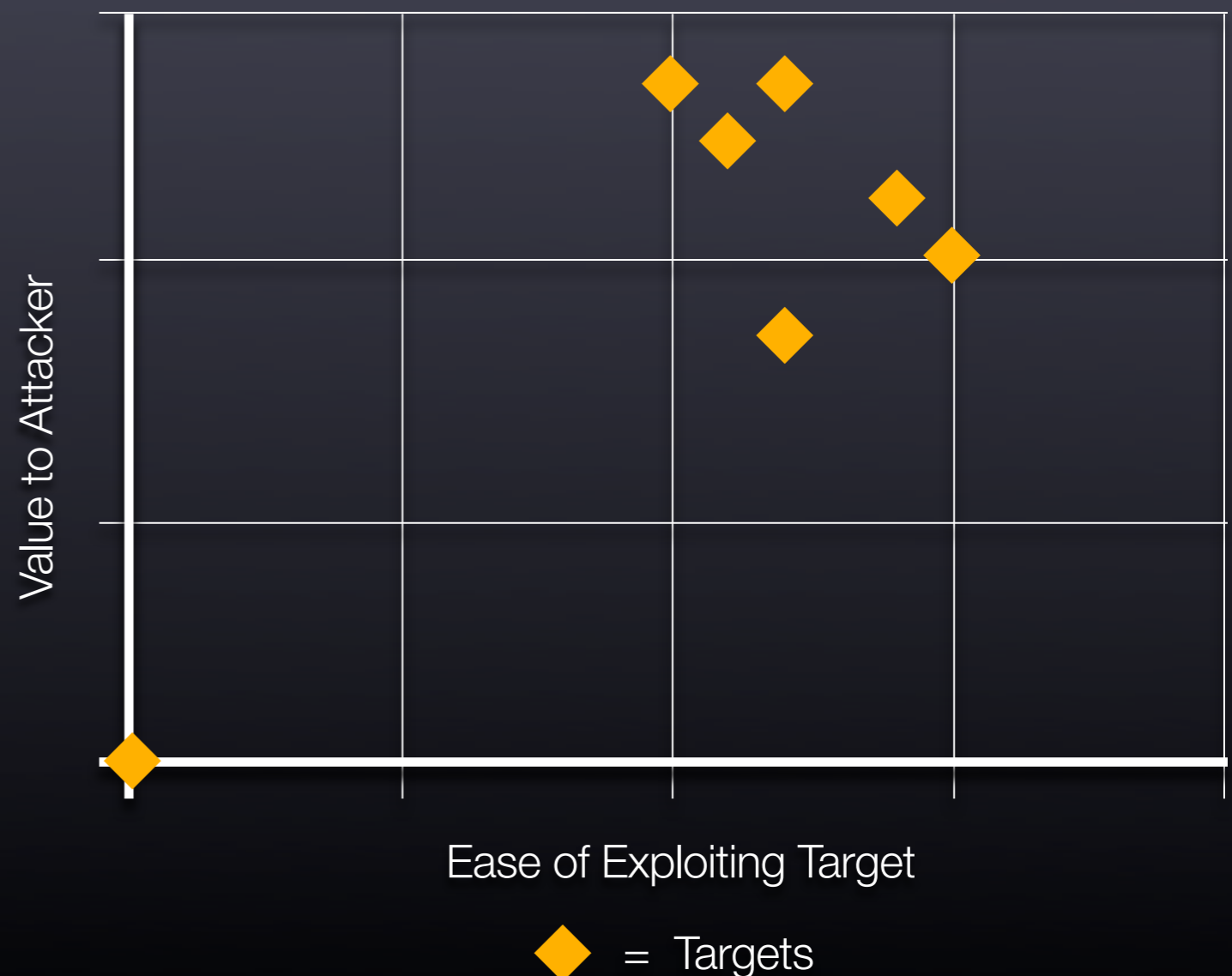
Categories of Spam

- ▶ 45% of spam in 2006 was pharmaceutical spam
- ▶ 33% of spam in 2007 was stock spam
- ▶ 2% of spam in 2007 was website hosting offers

A Graph for Optimal Target Selection

A Graph for Optimal Target Selection

- ▶ Targets lie in the top right quadrant
- ▶ Targets move left on X axis as security is introduced
- ▶ Targets move up on Y axis as services become popular



The attacker is a shrewd investor,
reassesses as conditions change.



We examined spam wars from
an economic perspective.



Fundamental Principle #3

The struggle between attacker and defender takes two forms:

1. Attrition Warfare
2. Transmutation

Attrition Warfare in Spam

URL cycling and listing

From: pedagogy <lesliepersonnel@85.141.153.178>
Subject: **Junior It is the absolute best choose.**
Date: May 25, 2006 11:42:30 AM PDT
To: ricochet-announce-request@vipul.net

embodiment scimitar and repertoire hear even tess.

Here it is: <http://wckxjjiki7dqnqe8lq02k2vpk2v722k.porodinehb.com/>

Have fun,
Estela

From: Leslie Westbrook <tvoeslcpef@organic-ingredients.com>
Subject: **StormPay Registration Confirmation**
Date: August 8, 2006 9:16:52 PM PDT
To: bgdarnel@vipul.net

From: 野玫瑰 <okmm@tom.com>
Subject: (图)你的红颜知己!
Date: July 13, 2005 1:30:56 PM PDT
To: ricochet-announce-request@vipul.net
Reply-To: okmm@tom.com

(图)你的红颜知己!
<http://41800.kuw.cn/>

Increase Your S"exual Desire and S"perm volume by 500%
Longer o"rgasms - The longest most intense o"rgasms of your life
Multiple o"rgasms - Cum again and again
S'PUR-M is The Newest and The Safest Way
100% N"atural and No Side Effects - in contrast to well-known brands.
Experience three times longer o"rgasms
World Wide shipping within 24 hours

Click here <http://www.astronautwrestling.info>



Number of Domains Used for Spam in 2003?

45,000

Cost of these domains: USD **\$31,000**

Number of Domains Used for Spam in 2007?

1,6878,00

Cost of these domains: USD **\$9.8M**

Number of Blogspot/Redirector
URLs Used for Spam in 2008?

Unlimited?

Cost of these domains: USD \$0



Fundamental Principle #4

Attrition warfare happens
when an attacker figures out a
way to exploit a defense strategy
at a fixed cost.

Average time to discover a new
spam domain in 2003?

8 minutes

Average time to discover a new
spam domain in 2007?

22 seconds

Many Types of Attrition Wars in Spam

Many Types of Attrition Wars in Spam

- ▶ IP Reputation tracking
- ▶ Bayesian Noise Elimination
- ▶ Hash Busting

Many Types of Attrition Wars in Spam

- ▶ IP Reputation tracking
- ▶ Bayesian Noise Elimination
- ▶ Hash Busting

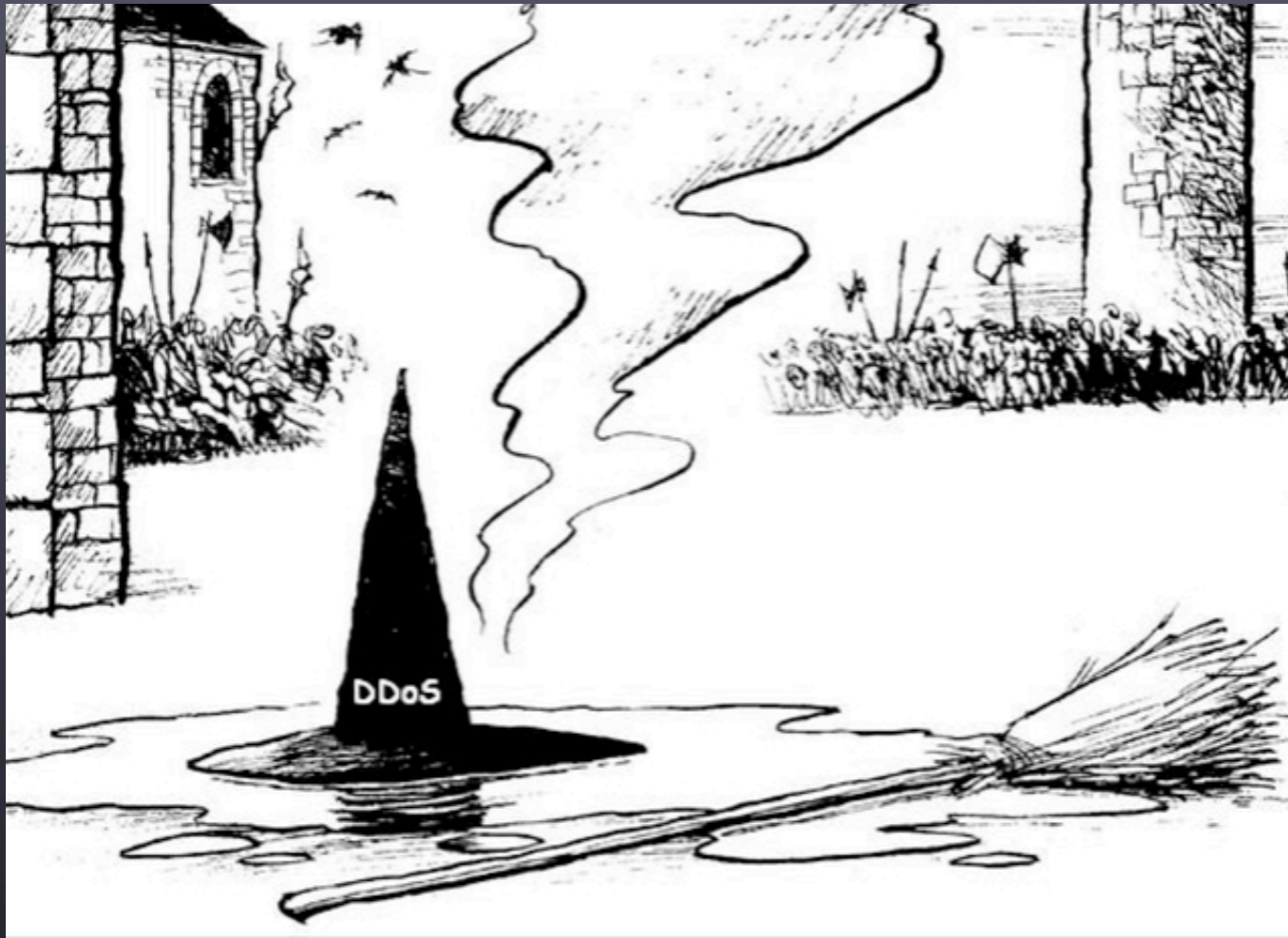
Whoever had the fastest tempo won the
attrition war

The most common way to achieve high tempo is automation.

But the cost of automating different strategies can vary quite a bit.

Fundamental Principle #5

Effective attrition attack strategies
are cheaper to automate than
their defense counterparts,
and vice versa.



DDoS space is set
in a war of attrition.

What happens when attrition warfare is no longer profitable to the attacker?



What happens when attrition warfare is no longer profitable to the attacker?

- ▶ Attacker can find a new target, eg spammers are moving to blogs, social networks, cell phones.
- ▶ Transmutate.

Fundamental Principle #6

Transmutation is an new attack strategy that steps outside the parameters of the defense.

It is a response to a loss in war of attrition.

Pump and dump stock spam defeated many anti-spam systems.

WBR5 OPENS UP 2007 WITH HUGE GAINS AND MOMENTUM!
THIS ONE IS SURE TO TAKE YOU ALL THE WAY UP!

Trade Date: Thursday, January 4, 2006
Company: WILD BRUSH ENERGY (Other OTC:WBR5.PK)
Price: 0.05+
5-day Target: 0.50
Current Market: Extremely Bullish
Recommendation: Strong Buy

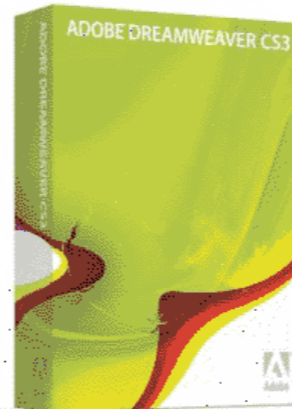
DON'T BE A BYSTANDER ON WBR5!
IT WILL BE YOUR FIRST WINNER OF THE YEAR!

WBR5 OPENS UP 2007 WITH HUGE GAINS AND
THIS ONE IS SURE TO TAKE YOU ALL THE

Trade Date: Thursday, January 4, 2006
Company: WILD BRUSH ENERGY (Other OTC:WBR5.PK)
Price: 0.05+
5-day Target: 0.50
Current Market: Extremely Bullish
Recommendation: Strong Buy

DON'T BE A BYSTANDER ON WBR5!
IT WILL BE YOUR FIRST WINNER OF THE YEAR!

Adobe Dreamweaver CS3
Retail Price \$399.00
Our Price \$59.95
You save \$339.05



AND MANY MORE NEW SOFTWARE NOW AVAILABLE!
www.oem-vo.com
(Type the link in to address bar of your browser manually!)

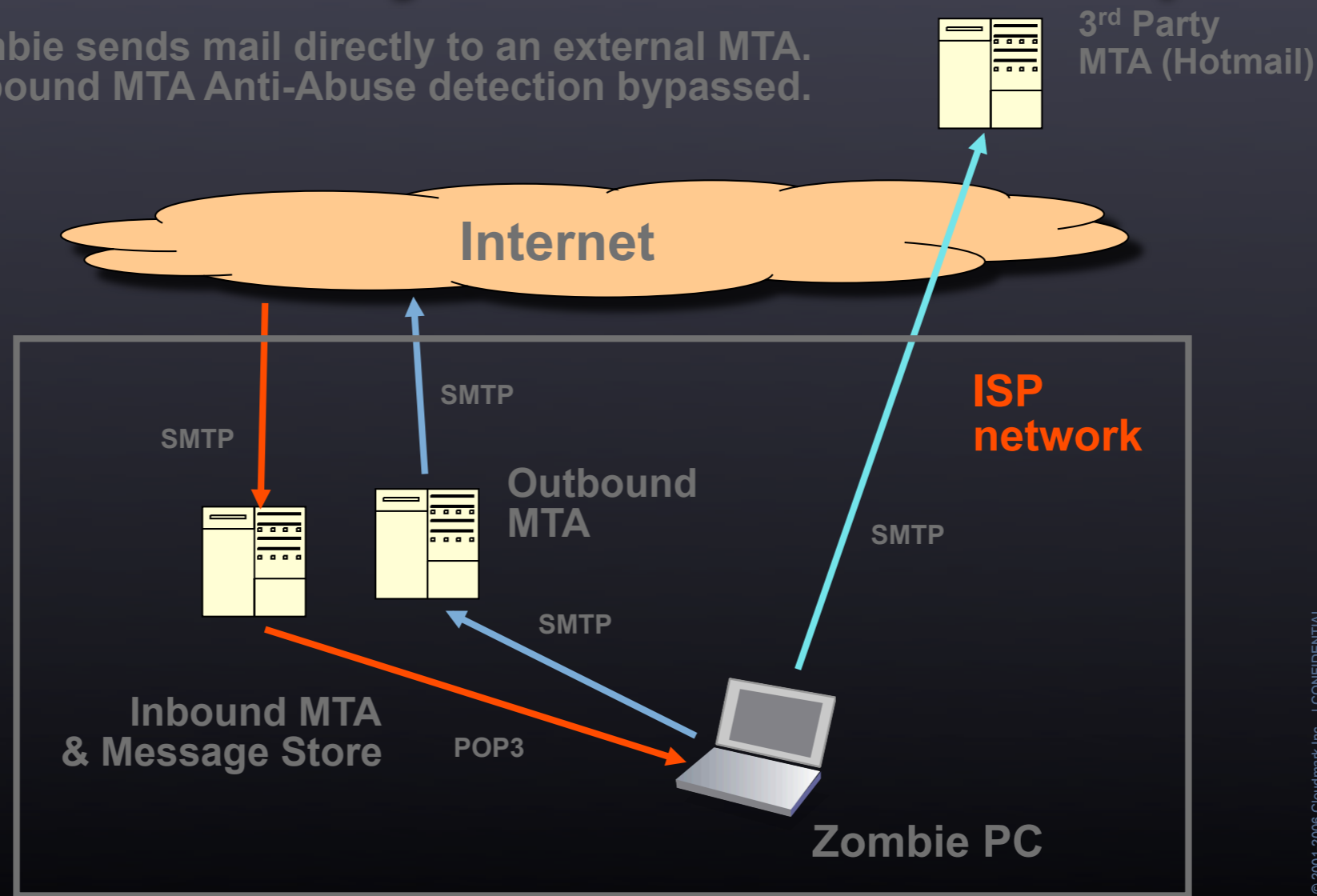


\$3.33
ON THE NET
www.rx555.com



Botnets made Spam Filtering based IP Reputation a lot more difficult - particularly Outbound Spam

Zombie sends mail directly to an external MTA.
Outbound MTA Anti-Abuse detection bypassed.



© 2001-2006 Cloudmark Inc. | CONFIDENTIAL


26

Social Networking Spam friend request Spam

Fictitious "Friend Request"

Mail Center
Friend Request Manager  Approve or Deny Your Friend Requests

Listing 1-4 of 4 1 of 1

	Date:	From:	Confirmation:
<input type="checkbox"/>	Apr 22, 2006 7:18 AM		Myriah wants to be your friend! <input type="button" value="Approve"/> <input type="button" value="Deny"/> <input type="button" value="Send Message"/>

Listing 1-4 of 4 1 of 1

☐ Select/Deselect All

☒ Approve Selected ☒ Deny Selected
Approve or Deny your selection

Wall Spam

 **Ryan Sassman** (no network) wrote
at 10:44pm on March 22nd, 2008

i finally found the best source out there for all the latest ringtones for my phone at <http://www.hltrf.com> they dont sound bad like the ones from my actual phone company, these are 100 times better and they have thousands and thousands of ringtones to choose from and when you use them the first time you get 20 free ringtones. stop paying so much for your ringtones, don't be a sucker, get them from my place, <http://www.hltrf.com>

[Message](#)

Comment Spam and Phishing

Subject: Request to Approve Journal Comment

Jazzy has posted a new Journal comment on MySpace!

According to your privacy settings, all comments must be approved by you before they appear on your profile.

Original Post: **My Original MySpace Blog Entry**
"The bane of instant messaging is when people you don't know bother you and start sending messages. You can block each one, but how can you automatically disable AIM so that people you don't know can't IM you in the first place? This article explains how to make those changes in the latest AIM. It's especially critical for children's AIM account.
Check it out: [How to block strangers from bugging you in AOL IM \(AIM\)](#)"

***Jazzy*'s Comment:** **The Spammy Blog Comment**
"hey intresting blog, i thought id let you know though **this site** is giving out free \$500 gift cards to spend at Kmart to the ppl who sign up, i got mine and bought a new cell with it."

Body:


Please click the link below to approve or deny this comment.



Jazzy

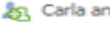
☒ Approve, or
☐ Deny


Spammy Profiles

 **Carla Cramer**


Networks: Washington, DC
Sex: Female
Birthday: February 27
Hometown: Cleveland, OH
Political Views: Liberal

Mini-Feed
Displaying 2 stories. [See All](#)

Today
 Carla and **Ryan Sassman** are now friends. 5:45pm

Yesterday
 Carla listed Work at Home and Make \$200+ per Day in Marketplace. 11:23am

The Wall
Displaying the only wall post. [See All](#)

 **Carla Cramer** wrote
at 5:47pm
Work at Home and Make \$200+ per Day
Working only 30 - 45 minutes per Day
Enter Here:
<http://www.best-home-business.net/wasdc.html>
[Message](#)



Transmutation
is a creative
process.

It has an R&D
cost.



Fundamental Principle #7

A successful defense to
transmutation is to turn it into a
war of attrition

Fundamental Principle #8

Target bounding strategies cripple infrastructure and provide no security.

Internet worms work by exploiting vulnerabilities in network software.



Sasser exploited XP in 2004, spread at an alarming rate, caused Delta to cancel flights, shutdown some satellite communications, Sampo bank to close 130 branches.

Transmutation in worms. Spam + Social Engineering



“230 dead as Storm batters Europe”

“Radical Muslim drinking enemies blood”

“Chinese missile shot down USA satellite”

“Fidel Castro dead.”


Storm worm
defeated by
antispam systems
like Cloudmark
and Postini running
high tempo
attrition wars on
binary content in
email.



NEWS [Email this article](#)

Storm worm strikes again on Easter claiming

Erica Chickowski Apr 11 2007 09:47



Security researchers discovered a spate of new variants of the Storm worm making the rounds this weekend through emails reporting fictitious news of the United States attacking Iran.

The scam emails on the loose include mangled subject lines, such as "USA Just Have Started World War III," "Missile Strike: The USA kills more then 20000 Iranian citizen," "Israel Just Have Started World War III" and "USA Missile Strike: Iran War just have started" — all with malicious programs with enticing names such as "movie.exe."

According to Adam O'Donnell, senior research scientist with Cloudmark, the latest analysis of the malicious binaries showed that they are variants of the storm worm that first made its big splash with millions of infections in January.

"This is the exact same thing," he said. "The attackers use a methodology where they send out an executable attachment associated with some kind of major news story, or fictitious news story, to get people interested enough to load up the virus."

When the virus is installed, it creates a peer-to-peer network. Most of the attackers are interested in setting

More Transmutations: Indirect/Redirect Virus/Spam

<http://charleshenegar4626.blogspot.com>

<http://marionblakeman405.blogspot.com>

<http://james-dfarley3237.blogspot.com>

Fundamental Principle #9

There's always the potential for a new transmutation whose nature is impossible to predict.

Conclusion #1

You can predict the infrastructure targets at risk



Conclusion #1

You can predict the infrastructure targets at risk

- ▶ Use optimal target selection strategy often
- ▶ For example: mobile messaging will be attacked when e-commerce models appear. Or when the cost of sending mobile spam messages becomes economically viable.

Conclusion #2

You cannot predict the form of attacks



Conclusion #2

You cannot predict the form of attacks

- ▶ Specific approaches and attacks can't be predicted.
- ▶ These attacks will transmutate rapidly as you create responses to them.

Conclusion #3

Maintain a high tempo security process internally



Conclusion #3

Maintain a high tempo security process internally

- ▶ Select the highest tempo security partners and proxies.
- ▶ Speed up evaluation of proposed security processes.
- ▶ Avoid target bounding approaches.
- ▶ Create risk mitigation models for collateral damage.

Thankyou

