Viruses and Malicious Code: A Community Defense Perspective

Presentation to the 5th Science in Savannah Symposium

September 19, 2002

Julie J.C.H. Ryan, D.Sc.

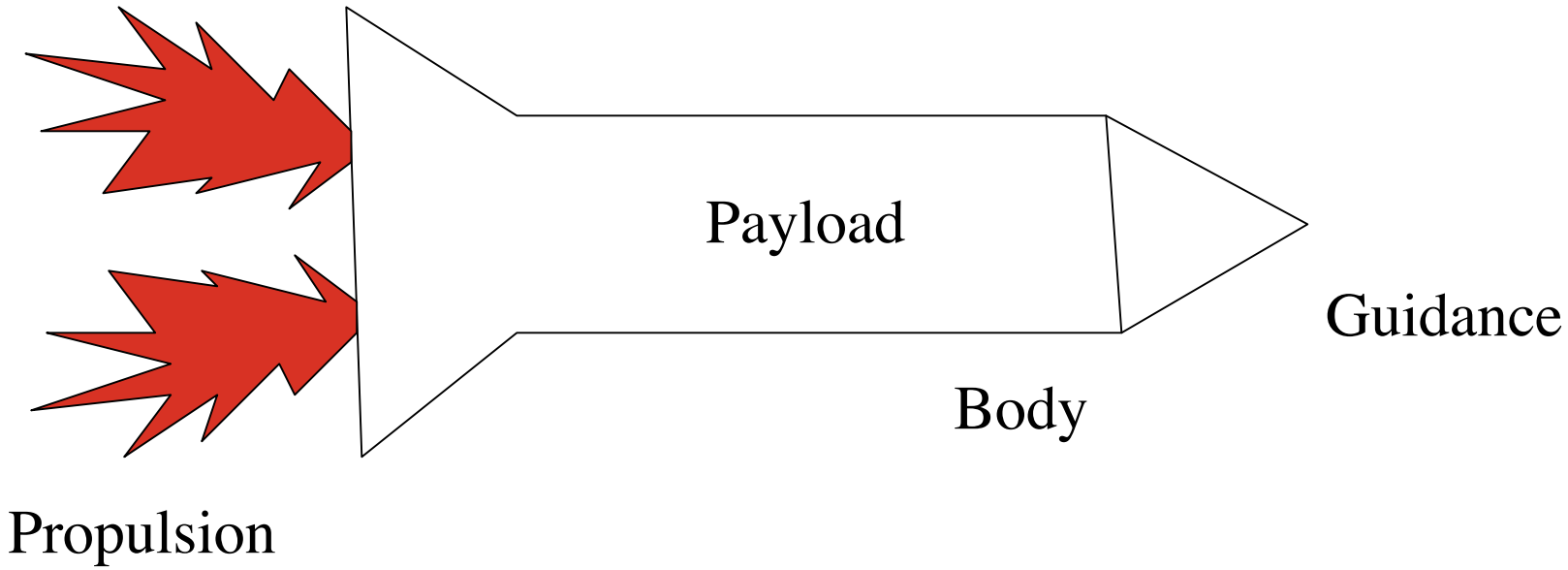
Assistant Professor, GWU

jjchryan@gwu.edu

Malicious Code

- What to call it?
  - "Virus" coined by Fred Cohen in 1984
    - Used to describe the nature of a specific type of software
  - "Malicious software"
    - More descriptive and includes more varieties
    - Trojan horses, easter eggs, worms, malicious macros
- All varieties of legitimate programming techniques
  - When used for nefarious purposes, called "malicious"
  - When used for good purposes, called "agents"
- Bottom line:
  - Software doesn't know good from bad -- it's the people behind the software
  - What you need to know
    - Any programming technique can be used for malicious purposes
    - Protecting yourself from malware isn't terribly difficult or technologically intense

The Differences

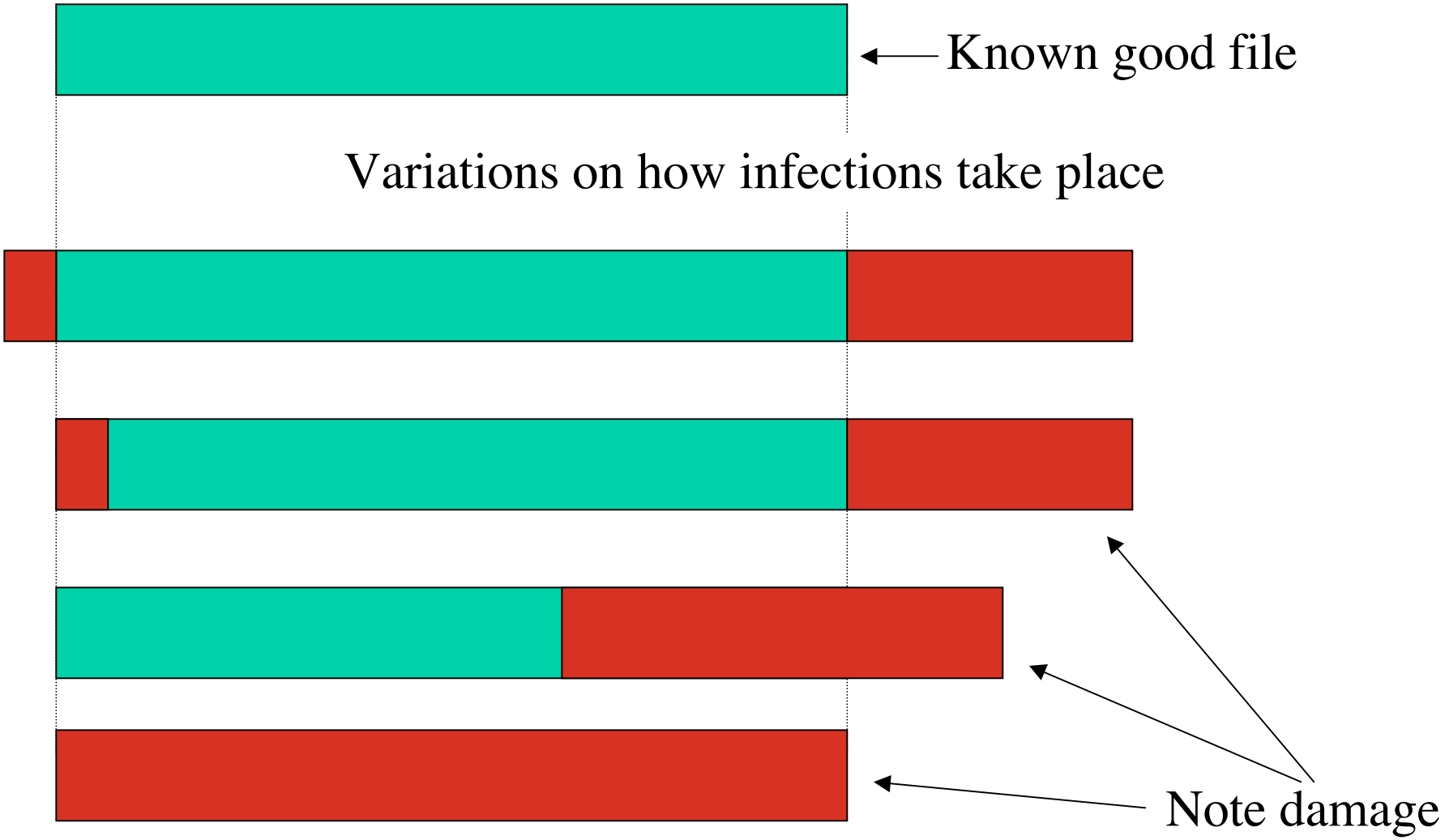


A virus relies on other files and users to provide both guidance and propulsion -- it hitch-hikes a ride

A worm contains all elements itself -- it is self-propelled and self-guided

Most people refer to all malware as viruses without distinguishing between types

Virus Infections



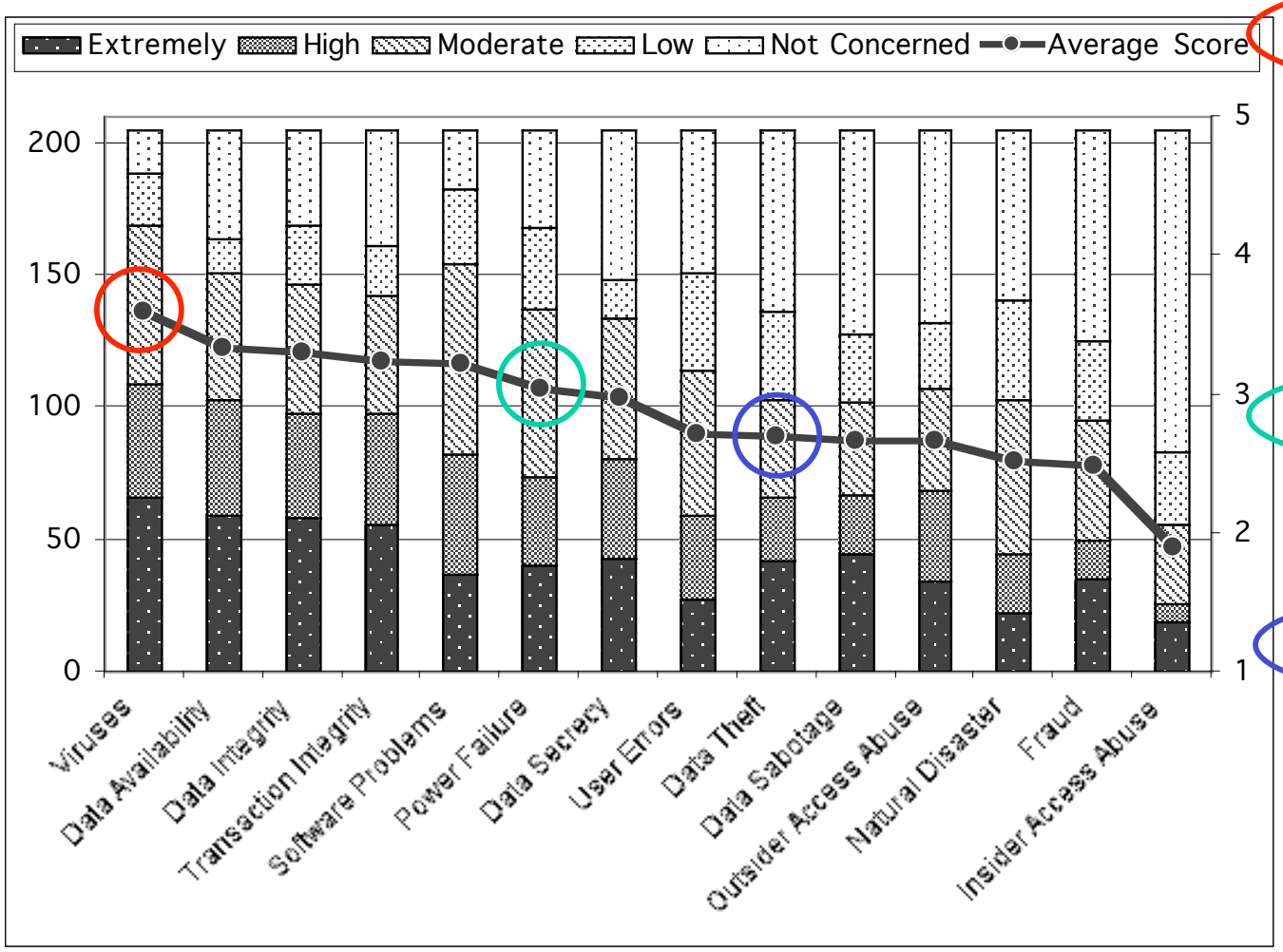
Recent Statistics

- August 2002 Wildlist
  - 203 viruses in the 'wild' on the most active list
  - Ones that were reported most:

Freq	Name	Aliases
47	W32/BadTrans.B-mm	29020
46	W32/SirCam.A-mm	-
44	W32/Magistr.A-mm	28672; Disembowler
40	W32/Nimda.A-mm	-
36	W32/Goner.A-mm	-
36	W32/Klez.H-mm	-
35	W32/Hybris.B-mm	Hybris.23040-mm
35	W32/Klez.E-mm	-
35	W32/Magistr.B-mm	32768
34	W32/MTX-m	Apology; Matrix
32	W32/Funlove.4099	-
27	VBS/Haptime.A-mm	Help
26	W32/Nimda.E-mm	-
24	W32/Aliz.A-mm	-
24	W32/BadTrans.A-mm	13312
23	VBS/VBSWG.X-mm	HomePage; SST
23	W32/Elkern.C	WQK.C
23	W32/Gibe.A-mm	-
22	JS/Kak.A-m	-
22	VBS/LoveLetter.A-mm	BugFix; I-Worm
22	W95/CIH.1003	CIH.A; Spacefiller
21	W32/MyParty.A-mm	-
19	W32/FBound.C-mm	-
16	VBS/LoveLetter.AS-mm	Plan.A
16	W32/Hybris.D-mm	Hybris.25088-mm
16	W32/Ska.A-m	HAPPY99
16	W95/Spaces.1445	Busm.1445
16	W97M/Marker.C	Spooky.C
15	O97M/Tristate.C	Crown.B
15	W97M/Thus.A	Thursday.A

Source:
http://www.wildlist.org/WildList/200208.htm

Small Business Concerns Overall Ranking



Scale is from 1 to 5, where 1 equates to "Not Concerned" and 5 equates to "Of Extreme Concern"

3.60 Viruses

3.33 Data Availability

3.30 Data Integrity

3.23 Transaction Integrity

3.22 Software Problems

3.04 Power Failure

2.98 Data Secrecy

2.71 User Errors

2.69 Data Theft

2.67 Data Sabotage

2.67 Outsider Access Abuse

2.52 Natural Disaster

2.49 Fraud

1.90 Insider Access Abuse

Technology Use

Technology Tools			Percentages		
	Yes	No	Yes	No	
Anti-Virus Software	182	27	87.1%	12.9%	
Data Backup System	157	52	75.1%	24.9%	
System Access Control	152	57	72.7%	27.3%	
Power Surge Protectors	147	62	70.3%	29.7%	
Redundant Systems	95	114	45.5%	54.5%	Less than 50% use
Shredders	93	116	44.5%	55.5%	
Data Segregation	60	149	28.7%	71.3%	
Firewalls	54	155	25.8%	74.2%	
Encryption	53	156	25.4%	74.6%	
Intrusion Detection Systems	47	162	22.5%	77.5%	Less than 25% use
System Activity Monitor	33	176	15.8%	84.2%	
Facility Access Control	30	179	14.4%	85.6%	
Security Evaluation System	24	185	11.5%	88.5%	
Dial Back Modem	21	188	10.0%	90.0%	
Media Degaussers	7	202	3.3%	96.7%	

Use of Remedies

- Remarkably few people understand how AV software works
  - Actually, it shouldn't be necessary that they do
  - This currently impinges on the effectiveness of stopping malware infections
- Current AV software requires frequent updates
  - Works by pattern matching through signatures
  - Signature must be known a priori in order for detection to occur
  - Many users don't know this, or don't bother to update
- There are some non-technical controls that can greatly reduce infection rates
  - Turning off auto-run and macro launches
  - Only accepting executables from trusted sources
  - Limiting file sharing
  - Not using "preview" capabilities in email clients
  - Not automatically launching .vbs files without checking them out first

4 Recommendations

- Awareness, awareness, awareness
- Training and education
- “Push” AV definitions
- A distant fourth: exotic solutions
  - Auto-immune system for computers
    - Research being done in New Mexico
  - Central analysis center sampling network traffic
    - Auto-analyze and push new definitions to users
    - Research done at IBM Watson Research Lab

Contact Information

Julie J.C.H. Ryan, D.Sc.
1776 G. Street NW #110
Washington DC, 20052
jjchryan@seas.gwu.edu
http://www.seas.gwu.edu/~infosec/

The George Washington University is an NSA Certified Center of Academic Excellence in Information Assurance Education and meets the Federal Training Standards for Information Systems Security Professionals (NSTISSI 4011). We offer Graduate Certificate, Master's, and Doctoral level education in Information Security Management for professionals from all educational backgrounds. GWU is located in the heart of Washington DC very near the White House and other government offices.