Malware
CSE 486 Fall 2022

Malware

- *Cryptovirology* by Young and Yung
- *The Art of Computer Virus Research and Defense* by Szor
  - Common theme since the turn of the millennium: stay in memory and don't go out to disk
- Elk Cloner in 1981 (Skrenta)
- “Virus” coined by Cohen in 1983 (“Information only has meaning in that it is subject to interpretation”)
  - https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html
- “Worm” came from John Brunner's *The Shockwave Rider* in 1975
  - Creeper in 1971 for TENEX systems
  - ANIMAL in 1975
  - Morris Worm in 1988
  - Code Red in 2001

Elk Cloner

Boot #	Behavior
10th	Overwrote the reset vector so that pressing CONTROL-RESET enters the Monitor program instead of DOS.
15th	Modified the video mode so that the text on the screen was inverted.
20th	Wrote to the speaker, causing a brief click to be heard.
25th	Modified the video mode so that the text on the screen flashed.
30th	Rearranged the characters that represent the file type of a file when the CATALOG command was executed
35th	Modified the value that represented

...

(from https://arxiv.org/pdf/2007.15759.pdf)

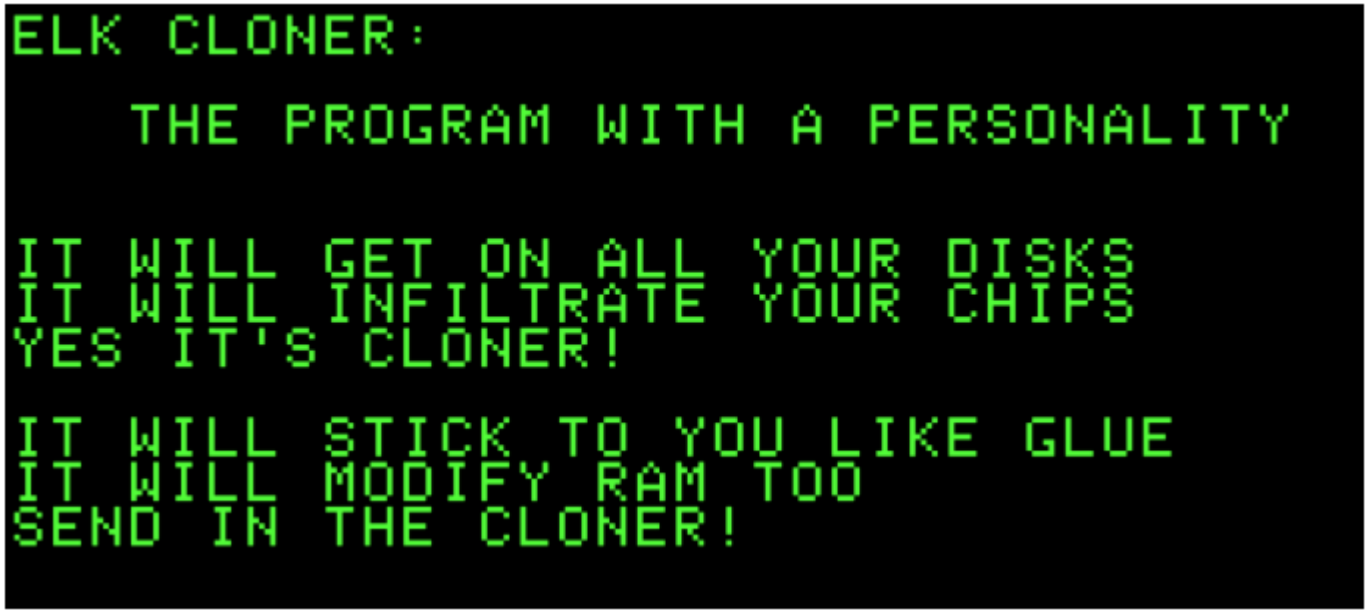
Elk Cloner (continued)

	the program instead.)
50th	Modified the reset vector so that pressing CONTROL-RESET caused the Elk Cloner poem to be displayed.
55th	Modified a constant in the diskette calibration code, causing the sound the disk calibration process made during the boot process to change. [4]
60th	Same as the 55th boot except that a different value was written to the constant in the disk calibration code.
65th	Overwrote the first instruction of the DOS command handler with a jump to the Monitor routine, so that the disk booted into the Monitor.
70th	Same as the 55th boot except that a different

...

(from https://arxiv.org/pdf/2007.15759.pdf)

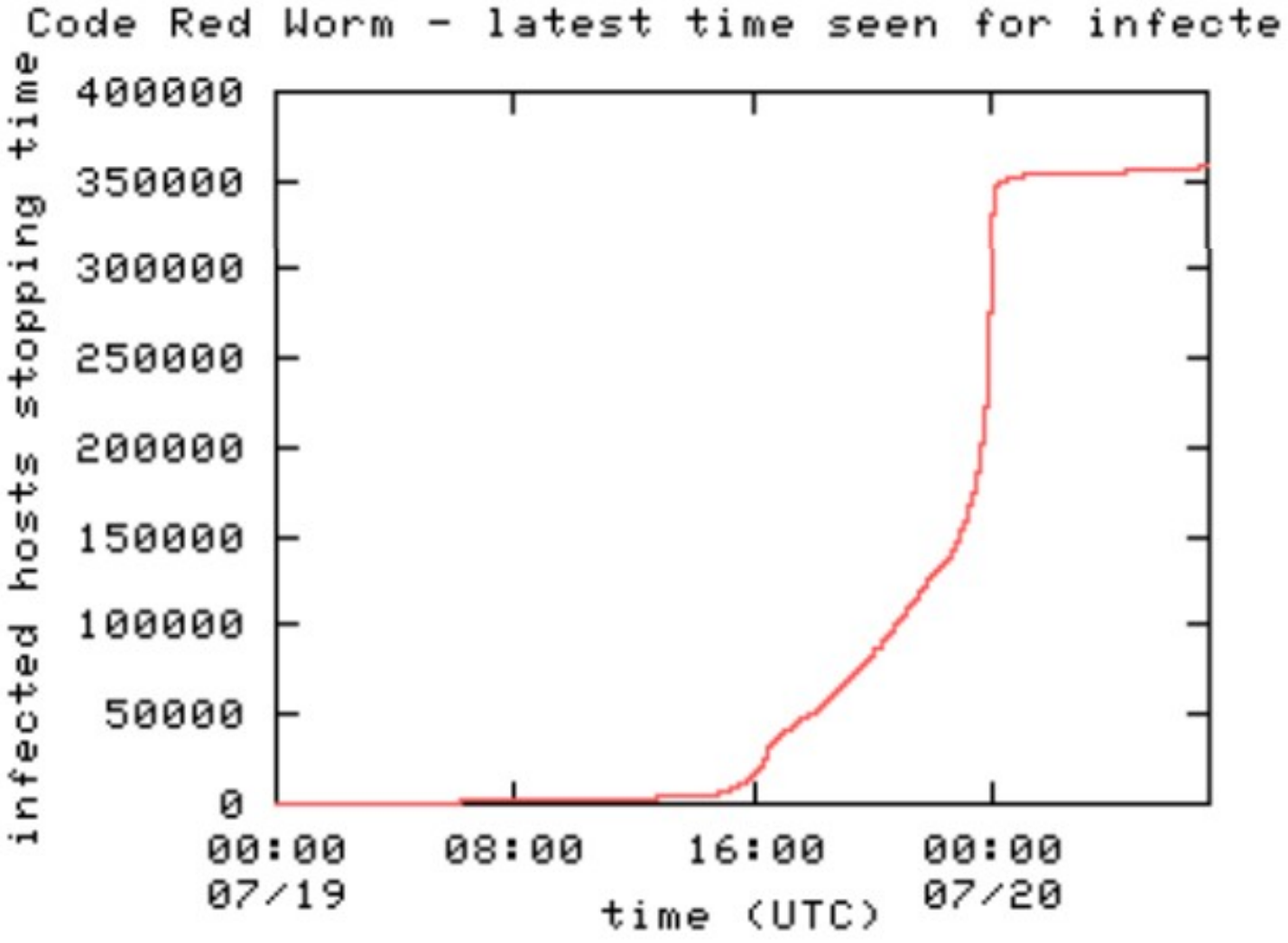
Elk Cloner poem



Code Red

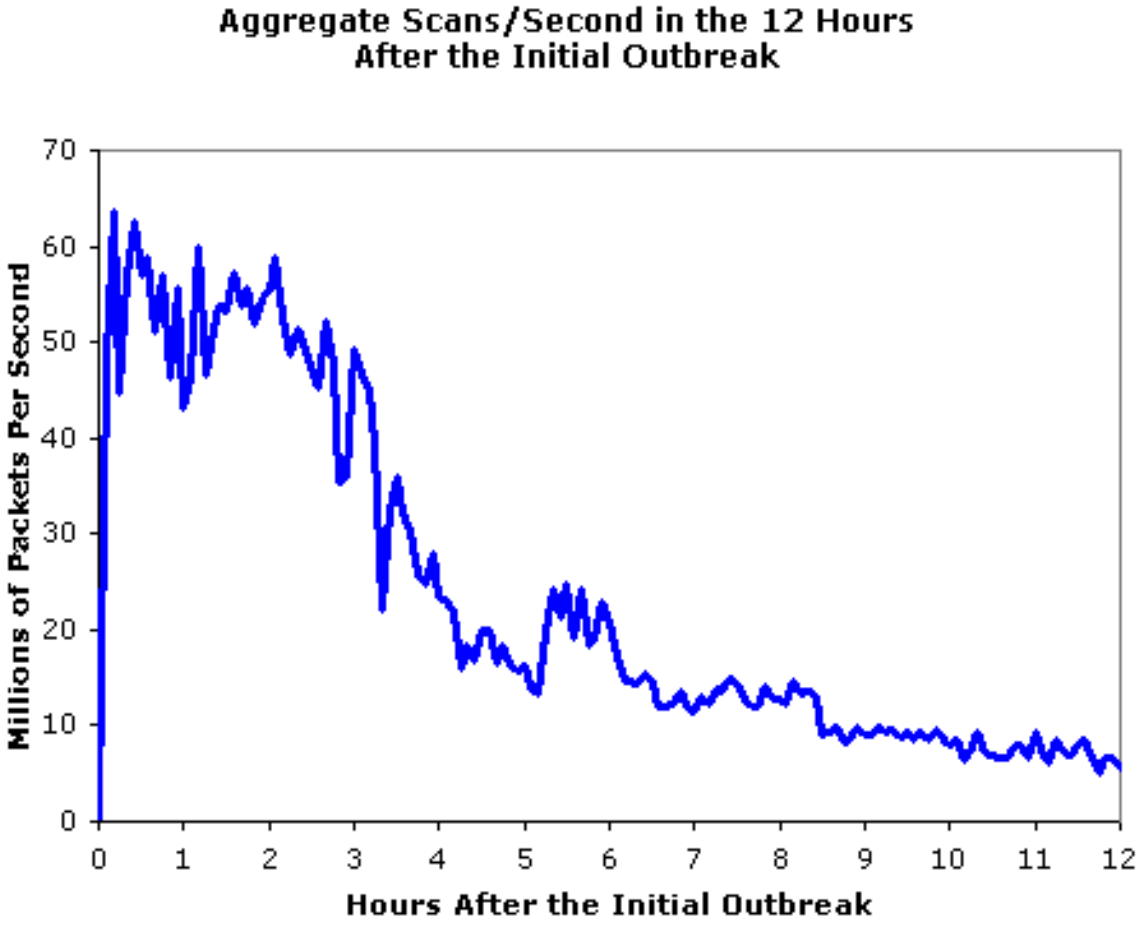
```
GET /default.ida NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u
7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%
u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 200 190
```

Code Red



From: https://www.cs.ucf.edu/~czou/research/codered.pdf

Slammer



Over 75K machines in 10 minutes.
(From: https://www.caida.org/catalog/papers/2003_sapphire/)

Witty Worm

```
rand(){
    # Note that 32-bit integers obviate the need for
    # a modulus operation here.
    X = X * 214013 + 2531011;
    return X; }
srand(seed){ X = seed; }
main(){
 1.     srand(get_tick_count());
 2.     for (i=0; i < 20,000; ++i)
 3.         dest_ip ← rand()[0...15] || rand()[0...15];
 4.         dest_port ← rand()[0...15];
 5.         packetsize ← 768+rand()[0...8];
 6.         packetcontents ← top of stack;
 7.         sendto();
 8.     if(open(physicaldisk, rand()[13...15]))
 9.         overwrite_block(rand()[0...14] || 0x4e20);
10.         goto 1;
11.     else goto 2; }
```

Figure 2: Pseudocode of the Witty worm

From: https://www.icir.org/vern/papers/witty-imc05.pdf

Stuxnet

Stuxnet

- Attacked the Iranian nuclear program
- Multiple ways of spreading
- Attempt to limit spread, several attempts
- Not as buggy as malware typically is
- Attacked very specific centrifuges with a very specific frequency

Interesting types of malware

- Macroviruses
  - “ON ERROR RESUME NEXT”
  - https://bontchev.nlcv.bas.bg/papers/macidpro.html
- Botnets
  - Command and Control (C&C), from IRC and hierarchical to fastflux and beyond
- Targeted threats
  - E.g., Tibetan exile community, Syria/Egypt, Mexico
  - Google “Citizen Lab” or watch “Black Code”

Research: Anomaly detection

- A Sense of Self for Unix Processes (Forrest *et al.* in 1996)

Resources

- *Practical Malware Analysis* by Honig and Sikorski
- http://www.forensicswiki.org/wiki/Tools

Conferences you should check out

- IEEE Symposium on Security and Privacy (Oakland)
- USENIX Security Symposium
  - Also check out the workshops like FOCI and WOOT
- ACM Conference on Computer and Communications Security (CCS)
- Network and Distributed System Security Symposium (NDSS)
- Privacy-Enhancing Technologies Symposium (PETS)
  - Also PoPETS
- Also RAID for intrusion detection, DFRWS for forensics, CSF for policy and theory, Eurocrypt and Crypto, Blackhat, DEFCON, phrack, 2600 magazine, WPES and WEIS