Internet Security Threat Status

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 13

ravi.utsa@gmail.com
www.profsandhu.com

Industry Reports

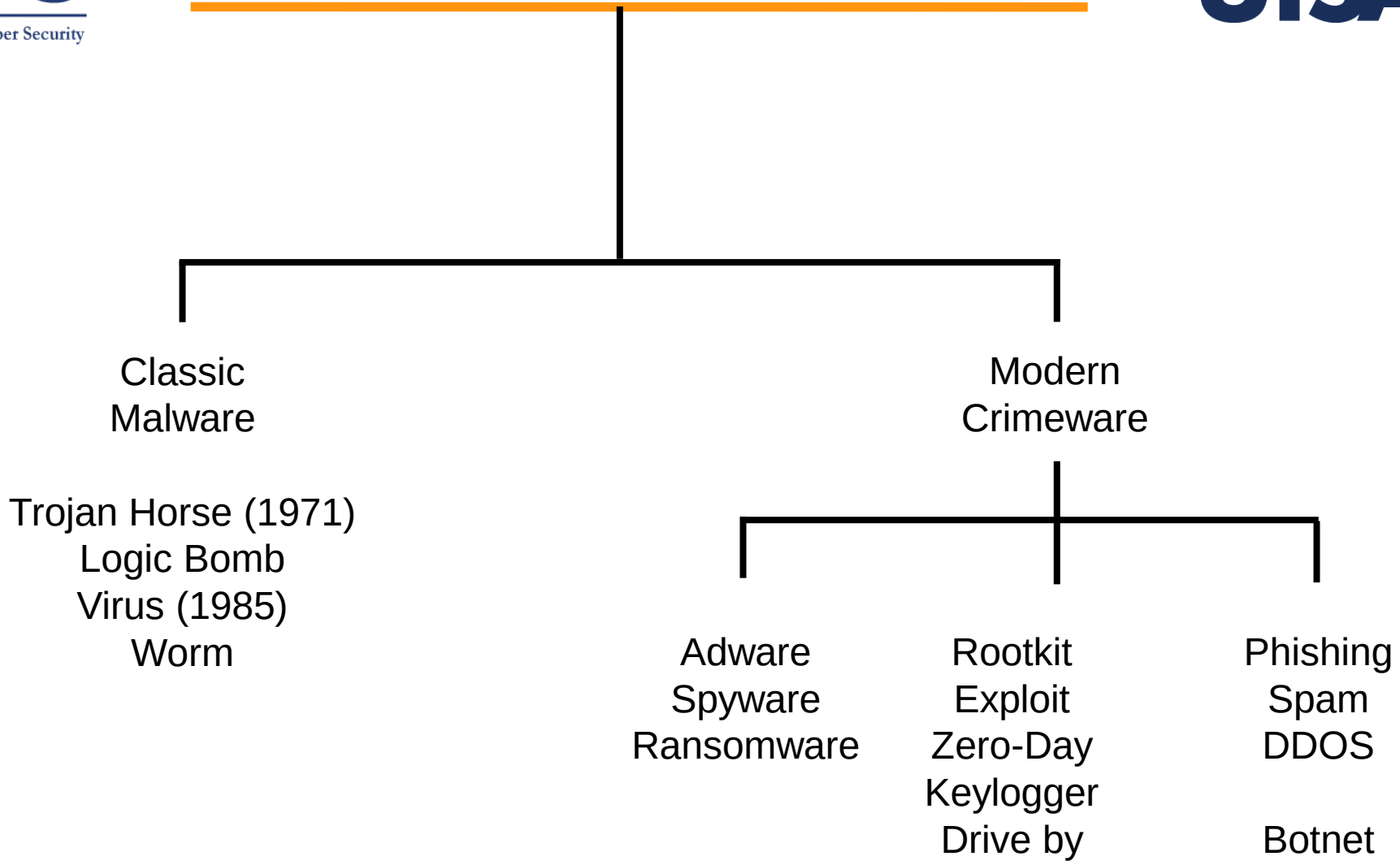
- Symantec Internet Security Threat Report
- AT&T Cybersecurity Insights Report
- Cisco Annual Security Report
- Dell Security Annual Threat Report
- Google Android Security Annual Report
- IBM X-Force Cyber Security Intelligence Index Report
- McAfee Labs Threat Predictions Report
- Verizon Data Breach Investigation Report
- ……

- Targeted attacks: Subversion/sabotage come to the fore
  - A notable shift towards more overt activity, with a decline in some covert activity
- Financial heists: Cyber attackers chase the big scores
  - Go for the bank, not for the bank customer
- Living off the land
  - Making use of resources at hand rather than malware/exploits
- Resurgence of email as favored attack channel
  - 1 in 131 emails were malicious, the highest rate in 5 years
- Ransomware with escalating demands
  - Average ransom in 2016 rose to $1,077, up from $294 in 2015
- New frontiers: IoT and cloud move into the spotlight
  - Security blind spot

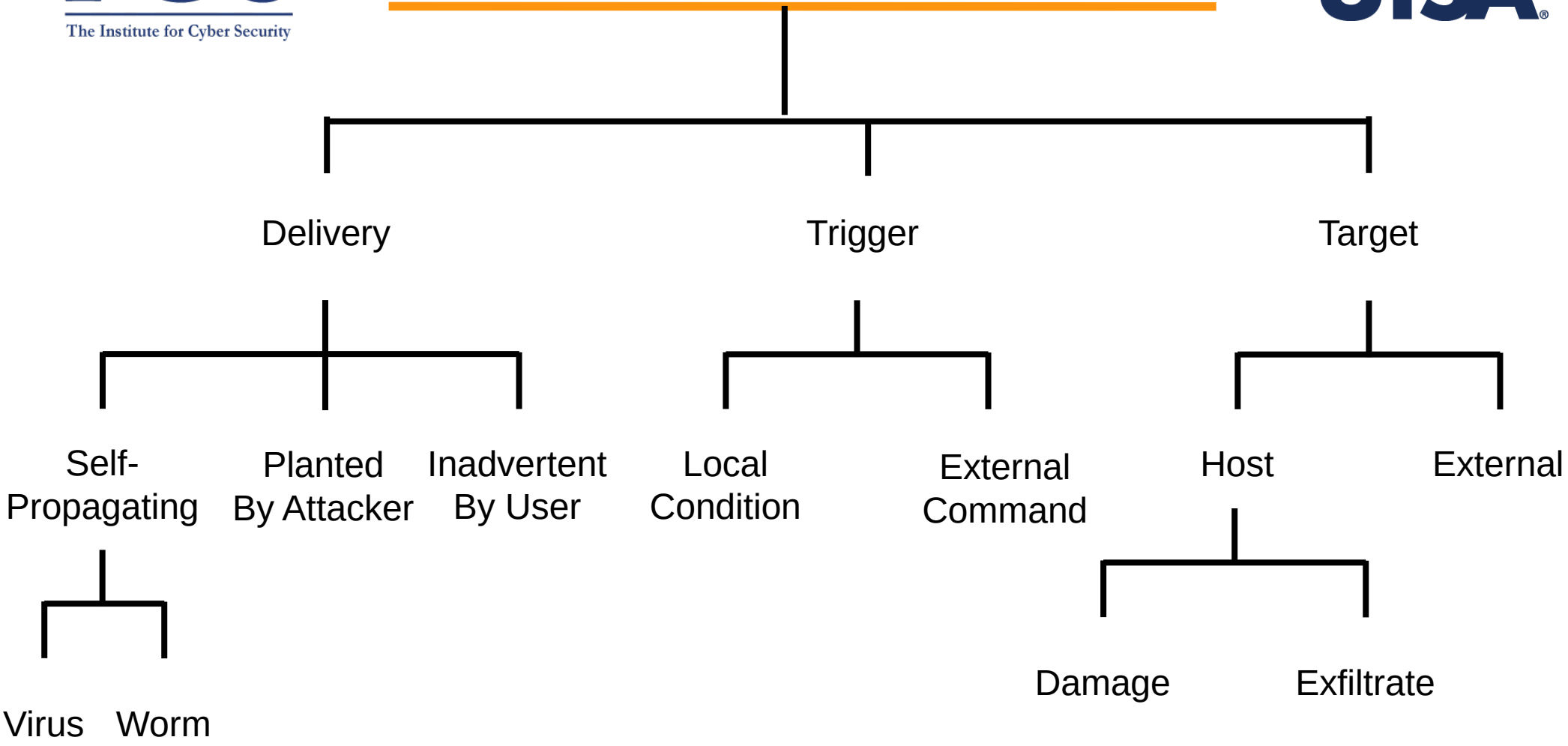
- A new zero-day vulnerability was discovered on average each week (total 54)
  - Doubled from 2014
- Over half a billion personal records were stolen or lost
  - Companies choosing not to report the number of records lost increased by 85 percent
- Major security vulnerabilities in 75% of popular websites
  - 15% of legitimate websites have critical vulnerabilities
- Spear-phishing targeting employees increased 55%
  - 43% of all attacks targeted at small businesses
- Ransomware increased 35%
  - Moved beyond PCs to smart phones, Mac, and Linux systems
- Symantec blocked 100 million fake tech support scams
  - First reported in 2010

- Big numbers
  - Pages 10-12 of report

Malware


Classic Malware
Trojan Horse (1971)
Logic Bomb
Virus (1985)
Worm
Modern Crimeware
Adware
Spyware
Ransomware
Rootkit
Exploit
Zero-Day
Keylogger
Drive by
Phishing
Spam
DDOS
Botnet

Malware


Delivery
Trigger
Target
Self-Propagating
Planted By Attacker
Inadvertent By User
Local Condition
External Command
Host
External
Virus
Worm
Damage
Exfiltrate