Logic Bombs

Blown to Bits

Gwynedd Mercy University

Cindy Casey, Gwynedd Mercy University

Logic Bombs

- Programming code purposely inserted into a system that sets off malicious function (payload) when some specified condition (trigger) is met.
- Logic Bombs are often referred to as Slag Code.
- To be considered a logic bomb, the payload should be unwanted and unknown.

Time Bombs

- Subclass of Logic Bombs
- Piece software that is dormant until specific date or time causes malicious payload to be executed.
- Examples:
  - US Army Reserves
  - Chernobyl Virus
  - South Korean Banks and Media Outlets

US Army Servers

- US Army Reserve IT contractor in Fort Bragg, North Carolina.
- Inserted malicious code into payroll systems after his employers lost the contract.
- Written to activate at a specific time - days after the handover.
- Executed November 24, 2014 (date new company started).
- Over 200,000 Army reservists had to wait weeks for pay.
- Sentenced 2 years prison, 3 years supervised released, ordered to pay $1.5 million in restitution

Chernobyl Virus (CHI)

- One of the most dangerous viruses in history.
- Trigger Date:
  - ✓ Anniversary of 1986 Chernobyl nuclear accident Ukraine
  - ✓ April 26th
- Payload
  - ✓ Overwrote PC’s HD completely destroying it’s contents
  - ✓ Overwrote BIOS preventing the PC from starting

South Korea Cyberattack

- Wiped HD and MBR of at least three banks and two media companies simultaneously.
- Over 30,000 machines compromised
- Malware consisted of four files:
  - AgentBase.exe triggered the wiping.
  - March 20, 2013 at 2pm (2013-3-20 14:00:00).
  - When clock on PC hit 14:00:01, wiper script was triggered.

South Korea Cyberattack

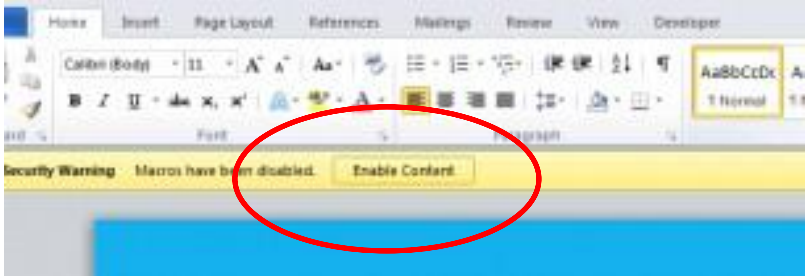
Wiper Script	Action
SYSTEM= ’$UNAME –s’ If [$SYSTYPE = “SunOS”] then dd_for_sun elif [$SYSTYPE = “AIX”] then dd_for_aix elif [$SYSTYPE = “HP-UX”] then dd_for_hp elif [$SYSTYPE = “Linux”] then dd_for_linux else exit	UNAME (UNIX Name) - reveal what OS is running -s (kernel name – used if no UNAME is specified) if the system is Solaris (Sun Microsystems UNIX) then write over (wipe data) We see the same command for AIX (IBM UNIX), HP_UX (Hewlett UNIX), and Linux operating systems Else (otherwise) Exit

Friday the 13th

- 1998 Jerusalem virus - created to mark the 40th anniversary of creation of the Jewish state.
- Trigger date: Friday the 13th
- Programs and files being used would be infected and eliminated.
- Infected files with COM, EXE or SYS extensions.
- Increases in size whenever file is executed.

Did You Just Say Virus?

- A computer virus can also behave like a logic bomb by releasing its payload at a predetermined time or date.
- Example:
  - WM/Theatre.A or Taiwan Theater Virus
    - Preset to activate on the first day of any month.
    - Downloaded via an infected Word document.
    - Program destroys system's hard drive.



Security Warning Macros have been disabled.

Piggybacking

Trojans

- Logic Bombs can be embed in code within a fake application, or Trojan horse.
- The logic bomb is executed when the fraudulent software is launched.

Keyloggers

- A keylogger captures your keystrokes.
- The logic bomb is designed to wait until you visit a website that requires you to login with your credentials.
- This triggers the logic bomb to execute the keylogger and capture your credentials.

Triggers and Payload

Triggers

- Specific date/time
- Countdown
  - Similar to time bomb but does not rely on system’s clock
- Third Party Triggering
  - MS Word
- Booting up System
- Buffer overflow
  - Occurs when program attempts to put more data in a buffer than it can hold
- Location

Payload (Destructive Part of Code)

- Wipe/Destroy Data
- Activate keylogger
- Lock or freeze machine
- Change system configurations
- Phone home
- Destroy centrifuges!

Omega Logic Bomb

- Disgruntled former network administrator Tim Lloyd.
- Malicious code led to the deletion of $10 million dollars in production programs.
- As a result, company was forced to dismiss 80 employees.
- Lloyd was convicted of computer sabotage and sentenced to 41 months in prison.

How Lloyd’s Logic Bomb Worked

Code	Action
F:	Event that triggered the bomb - logging onto central file server
F:\LOGIN\LOGIN 12345	Logged in a fictitious user (backdoor)
CD/PUBLIC	Changed Directory to public folder containing programs
FIX.EXE/Y F:\*.*	Run program called FIX which deleted everything
Purge F:\/ALL	Prevent recovery of deleted files

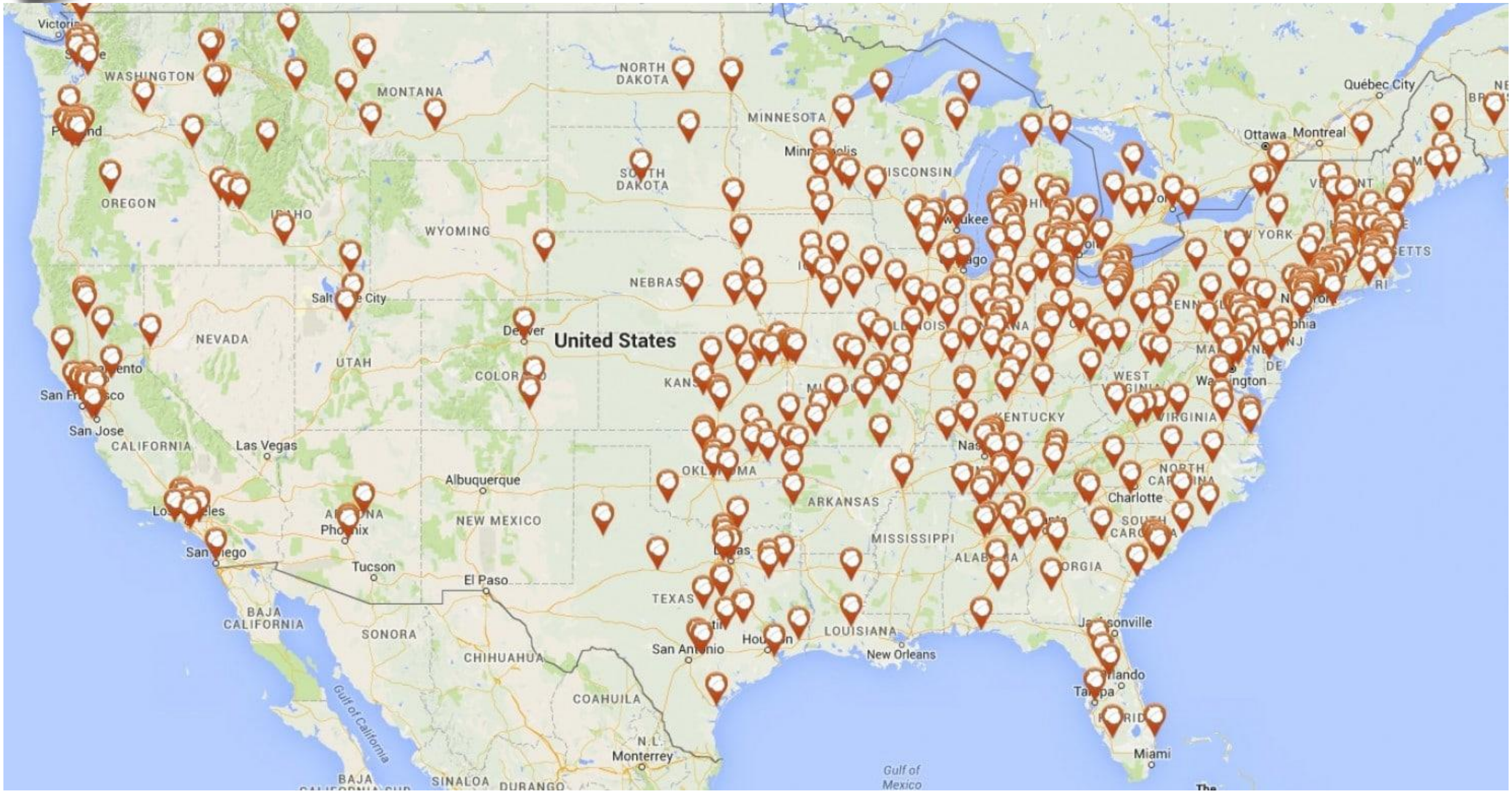
Cyberespionage, Cyberwarfare, and Cyberterrorism

- Logic bombs have been suspected in several cyberespionage attacks.
- Examples:
  - ✓Electrical Power incidents in Ukraine
  - ✓Stuxnet

Cyberwarfare

- Infrastructure has become an attack vector.
  - Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA) Systems now on network.
- Once code injected – IT host no longer needed.
- SHODAN finds connected devices on Internet.
- 2016 Ukrainian electrical power outage in Kiev.
- Stuxnet targeted SCADA systems nuclear power plant in Iran.

Squirrel Attacks



Map where squirrels have knocked out part of the power grid since 1987. Source: https://cybersquirrel1.com/

From Car Bombs to Logic Bombs

- Appeal:
  - ✓Inexpensive
  - ✓Large impact
    - Disrupt Infrastructure
    - Harm people
  - ✓Anonymity
  - ✓Easily obtainable

Sybil Logic Bomb Scenario

- Detailed risk scenario developed at Cambridge University.
- Described an insider who modified source code in a regular upgrade of the fictitious Sybil Company.
- Constructed using past cyber attacks.
- Logic Bomb designed to slowly corrupt data backups via small errors in the systems (so small that they aren’t initially noticeable).
- Demonstrated over the course of few years damages could range from 4.5 to $15 trillion dollars.

Sybil Logic Bomb Scenario

- According to the scenario, the damage caused by the Sybil Logic Bomb could have been mitigated through the following measures:
  - Reporting near misses
  - Dual-source technologies
  - Limit plug swappable technologies
  - Defending against insider attacks
- Between 58-70% of all security incidents are attributed to insiders!

Restrict sensitive information access to only those that need it.

Report suspicious activity or workers immediately.

Diffusing a Logic Bomb

- ✓ Evacuate the area (remove infected host)
- ✓ Keep the evidence
- ✓ Restore the data
- ✓ Verify backup before restoring
- ✓ Play with system time (turn back)
- ✓ Examine all processes and logs
- ✓ Defense-in-depth approach

Prevention

- ✓ Least privilege
- ✓ Secure system configurations
- ✓ Baseline of processes
- ✓ Check scheduler
- ✓ Up-to-date Anti-virus
- ✓ Patches, updates
- ✓ Review log patterns
- ✓ Keep records of modifications and who installed (date and request)
- ✓ Hash functions on entire files in the production library

Questions?

Cindy Casey, Gwynedd Mercy University
casey.cindy@gmercyu.edu

References

[1] M. E. Kabay, "Logic Bombs: Dangerous Cargo," [Online]. Available: http://www.mekabay.com/nwss/116q--logic_bombs_%281%29.pdf.

[2] A. S. Bist, "Detection of Logic Bombs," INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH, pp. 777-779, 2014.

[3] N. Robillard, "Defusing a Logic Bomb," 2004. [Online]. Available: https://www.giac.org/paper/gsec/3504/diffusing-logic-bomb/105715.

[4] J. F. Ido Dubrawsky, CompTIA Security+ Exam, Burlington: Syngress, 2007.

[5] D. Karl, "Stuxnet the world's dirtiest digital bomb," 2016. [Online]. Available: http://www.abc.net.au/science/articles/2011/11/01/3353334.htm.

[6] W. M. H. John Rittinghouse, in Cybersecurity Operations Handbook, Burlington, Elsevier, 2003, p. 6.

[7] S. Gaudin, "Case Study of Insider Sabotage: The Tim Lloyd/Omega Case," Computer Security Journal, 15 2 2000.

[8] Oildom, "Costly Insider Security Breaches," 11 2009. [Online]. Available: http://pgjonline.com/2009/11/17/costly-insider-security-breaches/.

[9] Cambridge Centre for Risk Studies, "Sybil Logic Bomb Cyber Catastrophe Scenario," University of Cambridge, Cambridge, 2014.

[10] K. Zetter, "Logic Bomb Set Off South Korea Cyberattack," 21 3 2013. [Online]. Available: http://www.wired.com/2013/03/logic-bomb-south-korea-attack/.

[11] M. Schwartz, "How South Korean Bank Malware Spread," 25 3 2013. [Online]. Available: http://www.darkreading.com/attacks-and-breaches/how-south-korean-bank-malware-spread/d/d-id/1109239?.

[12] Dell, "Wiper Malware Analysis Attacking Korean Financial Sector," 21 3 2013. [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/.