Cybersecurity

Logic Bombs

CYBER.ORG

Logic Bomb

- Waits for a predefined event
  - Often left by someone with grudge
- Timebomb
  - Time or date
- User event
  - Logic bomb
- Difficult to identify
  - Difficult to recover if it goes off

Real-world logic bombs

- March 19, 2013, South Korea
  - Email with malicious attachment sent to South Korean organizations
  - Posed as bank email
  - Trojan installs malware
- March 20, 2013, 2pm local
  - Malware logic-bomb activates
  - Storage and master boot record (MBR) delected, system reboots
- Boot device not found.
  Please install an operating system on your hard disk.

Real-world logic bombs

- December 17, 2016, 11:53pm
- Kiev, Ukraine, high voltage substation
- Logic bomb begins disabling electrical circuits
  - Malware mapped out the control network
- Began disabling power at a predetermined time
- Customized for SCADA networks
  - Supervisory Control and Data Acquisistion

Preventing a logic bomb

- Hard to spot
  - Each is scenario is unique
  - No defined signature
- Process and procedures
- Electronic monitoring
  - Alert on changes to critical data
  - Host-based IDS
- Insider information
  - Knows where to hit, when most damaging, possibly how not to get caught
- Regular scanning/auditing
  - A malicious administrator can circumvent these approaches
- Backups and snapshots