Anatomy of A Cyberattack

Here's how a computer invader plans and launches an attack on information systems:

1 **Recon** Invader uses information-gathering programs and techniques to sniff traffic at the network gateway, then scans ports for vulnerable services.

2 **Profile Target** Invader gets passwords, then identifies machines and software running on the network.

3 **Attack** Invader gains root or administrative privilege of unclassified systems, then seeks and modifies information.

4 **Cover Tracks** Invader hides the evidence trail and slips away.

5 **Wait for Results** Invader watches CNN to see what damage he wrought.

"The weak areas [of the above scenario] are in predicting when someone is gathering information for a later attack. And, once we've been attacked, the problem is in recovery," says Dennis McCallam, senior technologist at Herndon, Va.-based Logicon Inc., the IT contracting division of Los Angeles-based defense contractor Northrop Grumman Corp.

For the past year, Logicon has been working with the Air Force Research Laboratory (AFRL) in Rome, N.Y., to develop real-time analysis and recovery capability.

The result is something they call the resilient network: intuitive data hiding and recovery agents that will recognize when key data is erased or replaced with bogus data. Then that data or computational process is replaced with the untouched version, and the administrator is alerted.

The administrator starts by specifying the most essential data or processes that need protection – say air traffic patterns that, if interrupted, could lead to a collision or crash. The agents then camouflage the data by hiding it under fake file names and fake extensions in unlikely places on the network. At the first sign of data destruction or unauthorized tampering, the agent follows its path back to the clean data, copies and replaces it and alerts administrators.

"Our work represents a new vision in information infrastructure command and control that goes way beyond the protect-and-detect technologies [such as firewalls and intrusion detection systems] that came out in the '80s and '90s," says Joe Giordano, technical adviser to the AFRL. "This is active response, the linchpin to active forensics and protection."

Researchers are working on ways to tie the algorithm into other technologies also in research, including advanced forensics and a tracking system to follow a live evidence trail.

Don't be surprised if these algorithms eventually wind up in the private sector.

The AFRL developed the first intrusion detection algorithm, which spun out to the private sector when several former Air Force researchers founded the first intrusion detection company, WheelGroup, which was later acquired by San Jose-based Cisco Systems Inc.

– Deborah Radcliff