CERIAS

the center for education and research in information assurance and security

Controlled Malware Behavior Analysis

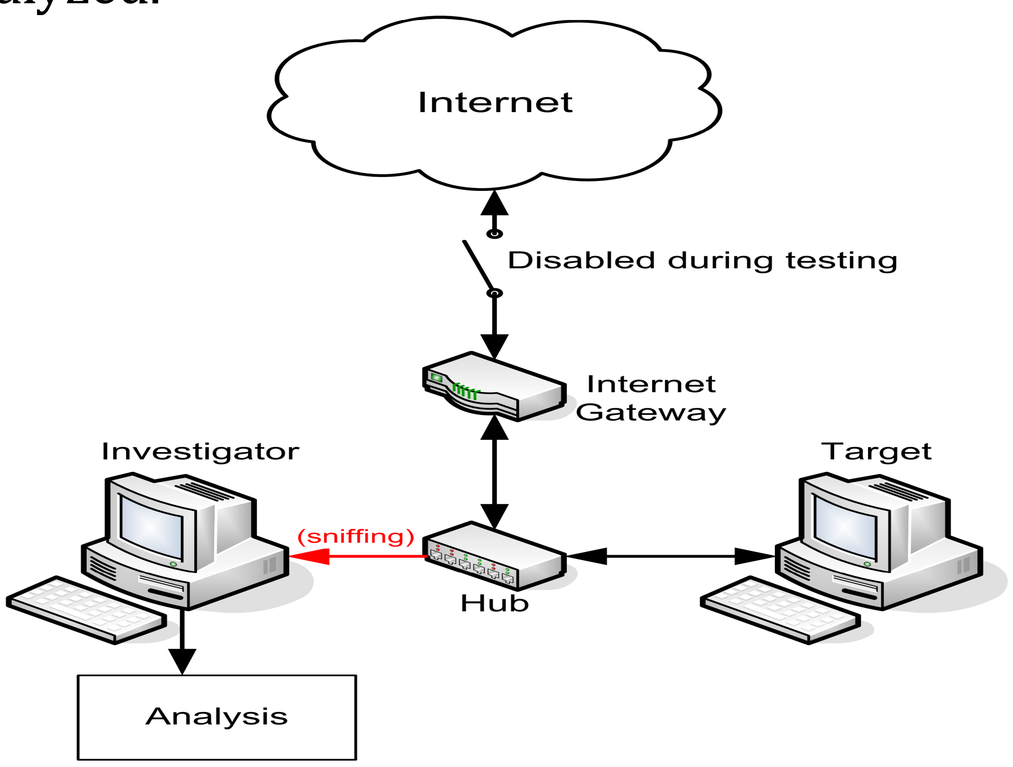
James E. Goldman, Sean C. Leshney*, Bradley J. Nabholz, Deepak R. Nuli, Nicklas R. Peelman

OVERVIEW

In coordination with the Indianapolis division of the FBI, the Malware Analysis Team is developing standardized architectures and processes with which to isolate, observe, analyze, contain, and eradicate malware of various types. Specialized tools will be developed to support the various phases of this mission. Of particular interest are complex trojans that can be installed on victims' computers and used at will in the execution of a variety of crimes.

PROBLEM

- Malware is a relatively new attack combining elements of classic viruses with new tactics – and worse, motivation – for stealing information and transmitting it to a remote location.
- When dealing with these new, evolved forms of malware, detection via signatures is not enough. Instead, the changes made to the local system, and attempts to contact the "outside world" must be captured and analyzed.



PROCESS

- In a controlled and isolated environment, launch malware on a target/victim computer.
- Using another workstation to sniff the network or "listen in," record any outgoing connection attempts by the victim computer.
- Analyze the connection records for patterns, giving insight into the malware's behavior.
- Develop tools able to detect newly discovered malware.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center