Novel Information Attacks

From “Carpet Bombings” to “Smart Bombs”
Traditional malware:
• Developed to create massive computer epidemics
• At the early stages of epidemics provides plenty of information for attack mitigation

Modern anti-virus products:
• Developed for massive attacks leading to epidemics, rather than targeted attacks
• Mainly employ binary signatures to detect malware (viruses, network worms etc.).
• The database of binary signatures is ever increasing due to new attacks and mutating malware

Novel malware such as StuxNet worm:
• Developed to create single attacks against high value target (industrial and government facilities)
• Does not create epidemics thus do not provide data for attack mitigation: the first instance of attack could also be the last instance
• The malware is highly specialized for particular environment of the target
Information for malware analysis and attack mitigation comes too late for the high value target.
What do we know about the StuxNet:

Internationally:
• Majority of attacks happened in Iran ["W32.Stuxnet Dossier" Symantec Corporation, October 2010]
• On July 7 2010, StuxNet might have shut down an Indian satellite that was operated by vulnerable remote terminal units [Jeffery Carr, “Did The Stuxnet Worm Kill India’s INSAT-4B Satellite?”, Forbes.com, September, 2010]

Generally, a targeted attack, such as StuxNet worm represents a threat of a great importance:
• The mass utilization of remote and automatic control systems at strategic objects as nuclear power plants, gas and oil production and transportation...
• Such control systems incorporate a large number of interconnected industrial controllers and operator stations…
• Systems that are particularly vulnerable to targeted attacks such as StuxNet worm
What do we know about the StuxNet:

- Control electronics (PLC)
- Process control computer
- INTERNET
- Deployment
- Propagation
- Activation, execution
- Erroneous control decisions
- Actuators
- Control valves
- Destructive control actions
- Destructive control actions
Our Current Work

Problem:

• A new trend in computer attacks is a stealthy targeted attack
• These attacks are aimed at high value targets within the national infrastructure that is much more dangerous and much more difficult to mitigate than traditional computer epidemics
• Existing computer security products, by design, fail to prevent targeted, industry oriented attacks.

The proposed solution:

• We propose a new cyber-security technology that detects attacks by identifying and classifying goals of an attacker (malware).
• Our technology does not rely on large signature data base that minimizes the use of computer resources and associated costs.
• Our technology addresses both traditional massive attacks and low and slow targeted attacks on industrial and government facilities.
What is done

- Observing malicious behaviors
- Specifying malicious functionalities
- Developing functionality recognition technology
- Preventing the attack spread

What we want to do

- Detecting potential goals of the attack
- Specifying malicious functionalities
- Utilizing functionality recognition technology
- Immunizing high value targets