Short Paper Review of:
An empirical study of real-world polymorphic code injection attacks

Citation:

Author(s) Affiliation(s):
- FORTH-ICS Greece
- I2R, Singapore
- Greek General Secretariat for Research and Technology under contract number PENED 03ED440

Claims:
- Present a study of > than 1.2 million polymorphic code injection attacks
  - Attacks targeted production systems
    - Real-world hosts not honeypots
    - over the course of 20 months
  - Captured using network-level emulation
- Results indicate limited use of sophisticated obfuscation
  - As well as high reuse of code among different malware families

Likes:
- I like the idea of network-level emulation as a way to capture attacks/malware.
- This paper was timley, right around this time the paper: “English Shellcode” was published: http://www.cs.jhu.edu/~sam/ccs243-mason.pdf which describes a system discusses the conversion from polymorphic code injection which could be detected up to that point because of the beleive that it must conform to specific standards to execute, to an almost English language like approach to shell code.
- Refreshing honesty about the up/down time of the sensors used.
- Interesting that the authors were able to identify variations of shellcode/malware not by the body which was encrypted but by the variations in encryptors.
Dislikes:

- Nemu “network level emulation software” sounds interesting but I was unable, upon cursory searching, to find anything more on it other than the two papers cited within this paper.

Repeat / Add to Work?

- I believe that this is a very important paper for others in the information security field to read. It has some very important facts about polymorphism and code reuse.

- Nemu / the process discussed in this paper is what I was initially outlining as future/add-on work for paper 18. The idea of identifying malware/families by their network level traffic patterns and attack characteristics.

- Overall I would say this was a good paper. I think that the authors could have presented the data in a more meaningful manor but the content was their, just a little hard to interpret.