AN EMPIRICAL STUDY OF REAL-WORLD POLYMORPHIC CODE INJECTION ATTACKS

M. Polychronakis, K. Anagnostakis, E. Markatos in *2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)*, 2009

A presentation by Adrian Jamieson

An Overview

- Polymorphic code is code that, when injected using a remote attack, is mutated so every attack has a unique pattern.

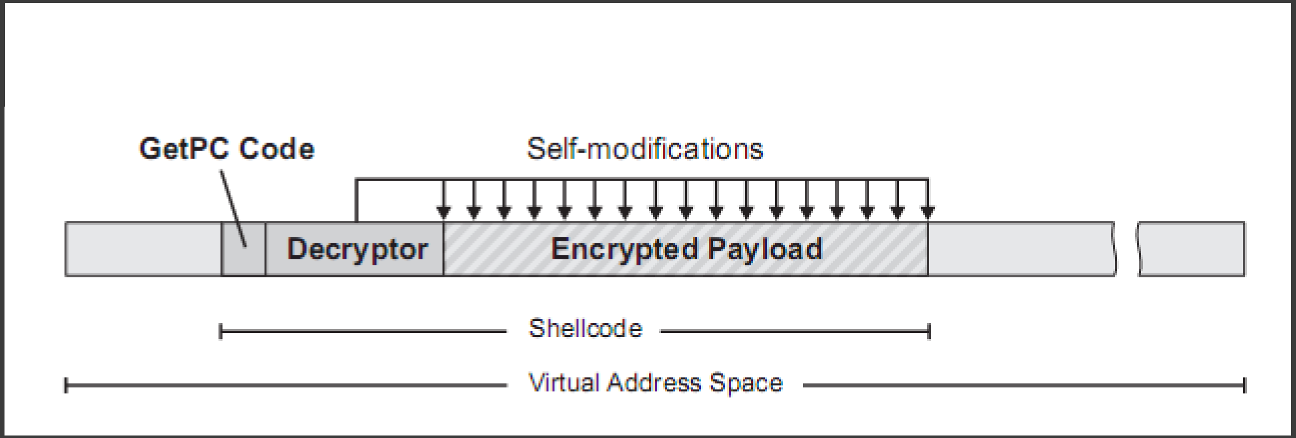
- The paper is an in-depth analysis of the structure of polymorphic code attacks.

The Good

- A good breakdown of how polymorphic attacks work.

- The intended purpose of the study was to “*focus on the analysis of the structure and operation of the attack code, as well as the overall attack activity in relation to the targeted services.*”

An Example



- Paper describes characteristics of each part very effectively.
  - The initial attack
  - The decryptor
  - The encrypted payload

- Achieves what is says on the tin.

The Bad

- *“We should note that for all captured attacks, nemu was able to successfully decrypt the original shellcode, while so far has resulted to **zero false positives**.”*
  - Really?
  - No clear definition of what polymorphic code is.
  - *“...so far has resulted to zero false positives.”*
  - Definitions game.

Bad

- No other means of detection
  - Is GetPC and patterns enough?
  - Truly polymorphic code would be extremely difficult to trace and perhaps use methods other than the one described.

- Everything you've ever wanted to know about polymorphic code injection attacks!
  - Paper is basically a text-book about polymorphic code injection attacks.
  - Nothing about how to detect or how to prevent.

Question

- Is it possible to make truly polymorphic code? Should we be worried about it?