AN EMPIRICAL STUDY OF REAL-WORLD POLYMORPHIC CODE INJECTION ATTACKS

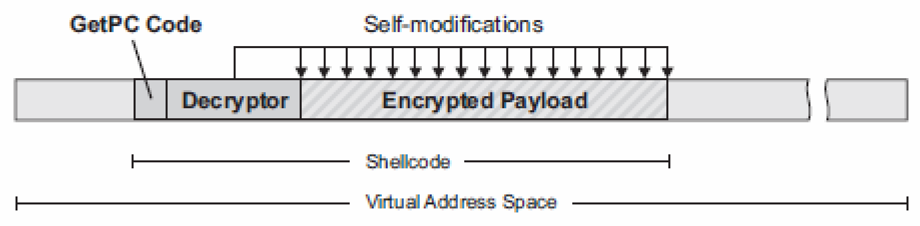
M.Polychronakis, K. Anagnostakis, E.Markatos

Published for the Second USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)

Presented by Chao Jiang

INTRODUCTION

The paper presents a study of more than 1.2 million polymorphic code injection attacks and focus on the analysis of the structure and operation of the attack codes.



- Shellcode
- GetPC code
- Encrypted Payload

"When polymorphism is applied to remote code injection attacks, the initial attack code is mutated so that every attack instance acquires a unique pattern, thereby making fingerprinting of the whole breed a challenge." – Third paragraph of Introduction

APPRECIATIVE COMMENT

The paper focuses on analysis the attack activity in relation to the targeted network services, the structure of the polymorphic shellcode used, and the different operations performed by its actual payload.

- Well explanation of how polymorphic code works
- Figures and Bar chart
- Good analysis techniques

CRITICAL COMMENT

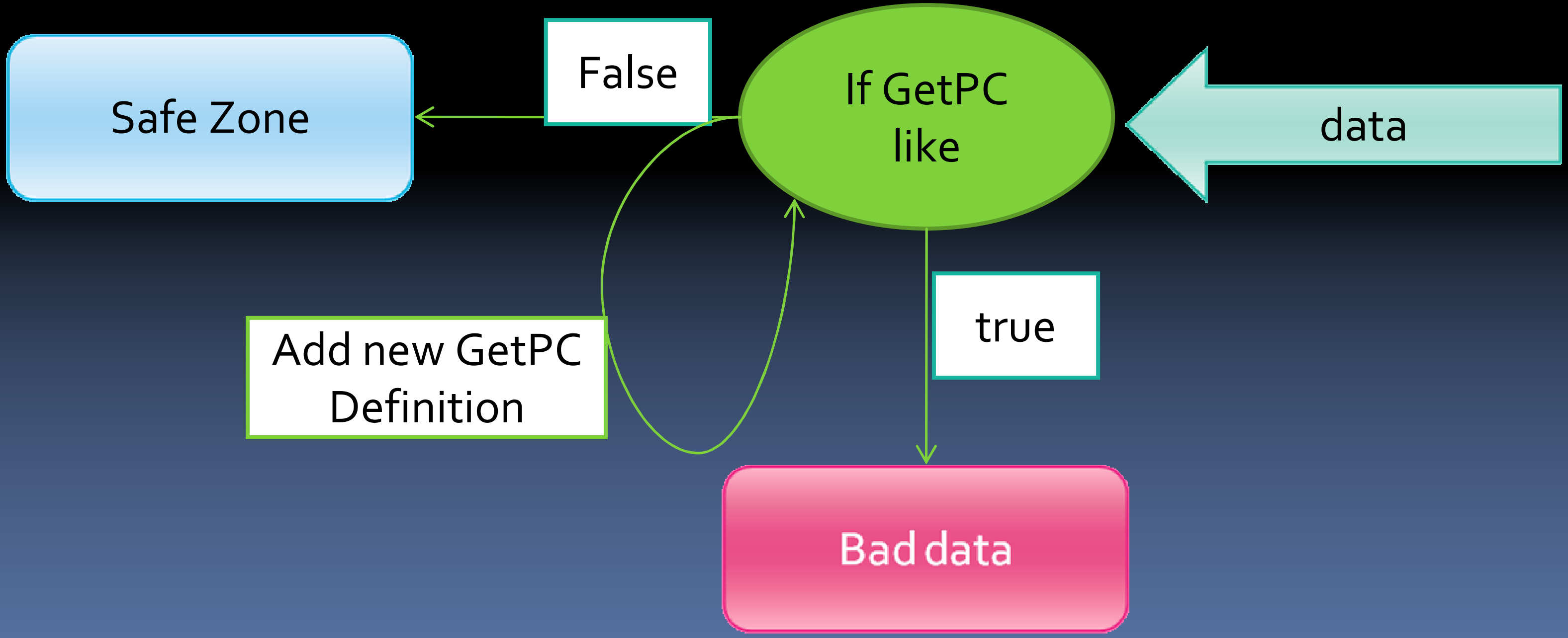
“When polymorphism is applied to remote code injection attacks, the initial attack code is mutated so that every attack instance acquires a unique pattern, thereby making fingerprinting of the whole breed a challenge.”

Analysis on 1.2 million records but talking about fingerprinting of the whole breed?

How to detect? Perhaps more explanation or more study?

QUESTION

Is GetPC the only way to detect polymorphic code? Can we use that to prevent from polymorphic attacks?


Safe Zone
False
If GetPC like
data
Add new GetPC Definition
true
Bad data