An Empirical Study of Real-world Polymorphic Code Injection Attacks

Michalis Polychronakis, Kostas G. Anagnostakis, Evangelos P.Markatos

Published in 2nd *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)*, 2009.

Presented by Zhen Li

Introduction

- The article was contributed after analysis more than 1.2 million shellcode attacks by using network-level emulation , detected over more than 20 months.
- The article focus on the analysis of the structure and operation of the attack code.
- And overall attack activity in relation to the targeted services

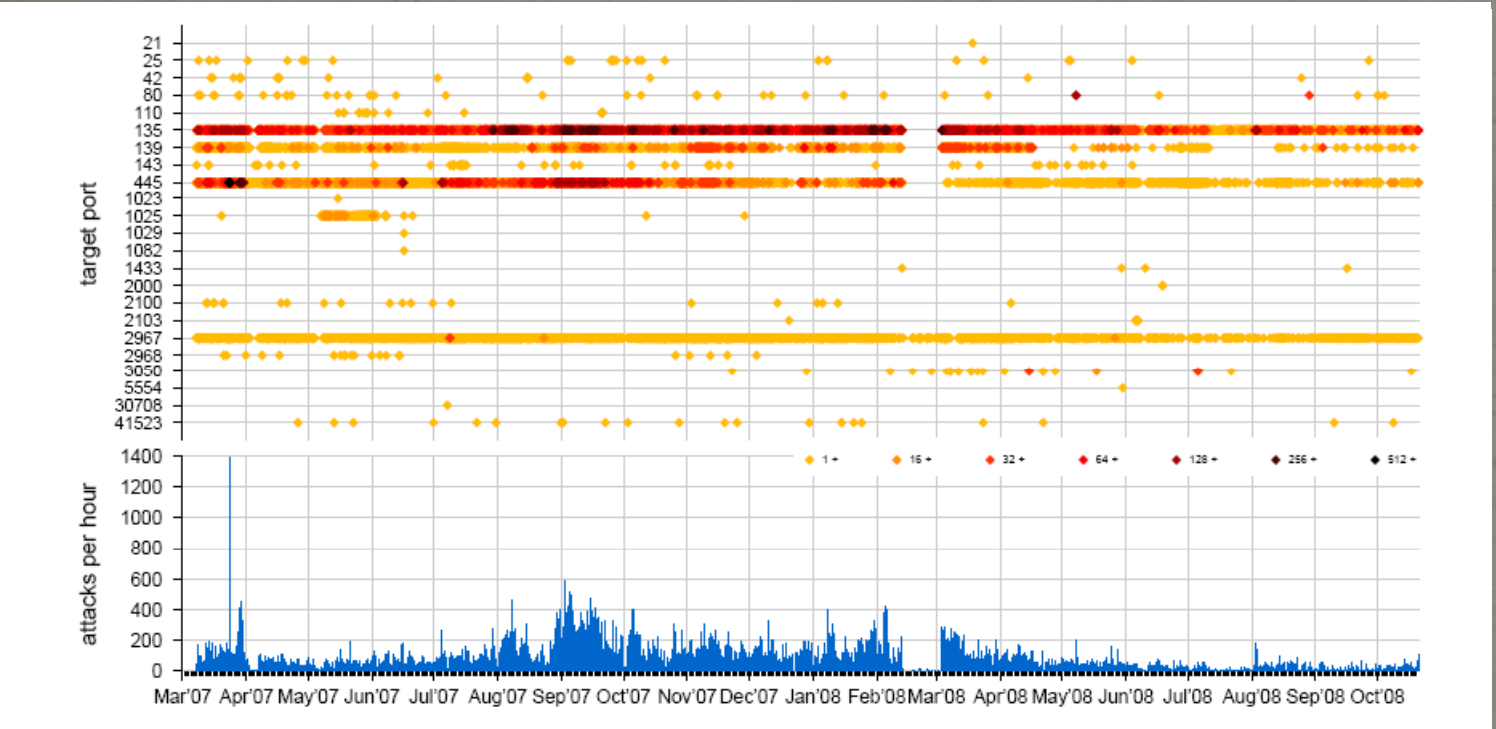
Appreciative comment

- Well explain attack activity relate to targeted services by using figures.

- Colorful
- Nice pattern structure

- Authors has very good analysis skill.

Appreciative comment



Using color to represent number of attacks, and Highlight most frequency attacked ports

135,139,445,2976 were highly exploited in the wild

Critical comment

- "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."

- Zero false positives only mentioned once in whole article
- Less definition of zero false positives.
- What is that mean?

Critical comment

		Actual condition	
		Infected	**Not infected**
Test result	**Test shows "infected"**	True Positive	False Positive (i.e. infection reported but not present) **Type I error**
	Test shows "not infected"	False Negative (i.e. infection not detected) **Type II error**	True Negative

From Wikipedia

Zero false positive means: does not make a mistake, all shell codes captured are truly shell code.

Question

- Are the zero false positive important ? Does detector have to care about that?