# Detection Techniques of Malware

Published date: July 27, 2015

## Technology description

### Background

Malware targeting enterprises has become highly sophisticated, lurking in a victim's machine for a long period of time. Malware often has complex logic to protect itself from being analyzed, and it conducts the attack in multiple steps, with each one guarded by a restricted condition. During this time, no sign of malicious activity is apparent until the intended target becomes reachable or a preset time frame is reached. According to Frost and Sullivan (2013), the United State experienced 55.7 percent of all malware incidents.

### Technology Summary

Researchers at Purdue University have developed a binary analysis engine, X-Force, which can detect malware attacks and reveal the malware's intent, behavior, and strategy. This technology monitors the execution of a binary through dynamic binary instrumentation, forcing the binary to ignore arbitrary conditional checks and supplying random values when inputs are needed. X-Force allows users to rapidly explore the behaviors of any unknown binary as it simply executes the binary without solving constraints. Furthermore, X-Force can also recover the execution from exceptions. Using this technique, users can easily handle binaries in a broader spectrum such as large, packed, or obfuscated binaries.

## Application area

Cybersecurity
Computational malware

## Advantages

More practical and extensible solution to malware attacks
Suitable for analyzing packed, obfuscated, and self-modifying binaries

## Institution

Purdue University

Inventors

Fei Peng
Xiangyu Zhang
Dongyan Xu
Zhui Deng