Kelvin Chan

1/F, Block K, Kam Yee House,
Kam Ying Court, Ma On Shan,
Hong Kong

E-mail: kelvin1272011@gmail.com
Website: http://kelvinhack127.blogspot.hk/
Phone: +85263001293

EDUCATION

The Bachelor in Computer Science — 2014 — 2016

Hong Kong Baptist University

Higher Diploma in Network and Mobile Computing — 2011 — 2014

School of Continuing and Professional Studies, The Chinese University of Hong Kong

INTRODUCTION

Knowledge:

5 year compulsory subject:

- Computer Network (including CRC32 checksum)
- Operating System(Linux/Unix OS)
- Mobile Apps development(iOS/Android)
- Java / C / C++ programming

Self-learning subject:

- Windows x86 Ring3 level mechanism (especially anti- game cheating, anti-debug , etc)
- Windows x64 Ring0 level mechanism (especially anti- game cheating, anti-debug , etc)
- Windows Driver Programming
- x86 / x64 assembly language
- Intel IA-32 architecture

Responsible for project

1. Bypassing NProtect, TenProtect, X-Trap in the last few years. The difficulties is that anti-debug engine are always protect their target very well. such as, NProtect will inject DLL for protecting purpose, X-Trap will scan our process's windows signature. So we need to know more deep about our OS, such as kernel System call, SSDT Hook, many function for anti-debugging

2. And my undergraduate final year project is a anti-rootkit(ARK)tools in windows x86, there is a function that for different hook checking, such as Import/Export address table(IAT/EAT) Hook, enumerate System Callback, find a hidden process/thread/DLL image in our OS, so on. There is a difficulties that so hard to identify the hook is it be directly IAT hook or affected by other kernel module's EAT hook.

3. I also started my research on VT-x and try to use it on Windows software security, and at the end of the day, I am able to bypass windows7 PatchGuard by using a VT-x and make any software breakpoint or hook in kernel memory.

4. Defensing ransomware by injecting DLL into all process with x86/x64 compatability(including any commercial software , such as NProtect, QQ, Taobao protect engine, etc.) There are a difficulties that first is Windows User Access Control(UAC) will blocked our DLL loading ; Second is confront with commercial level protection.

5. 2016 April , I have been invited by Hong Kong security conference as a speaker, share a experience on anti-debugging and debugging related on Windows x86 platform.

PROJECT

Windows platform:
- Anti Rootkit in x86 platform
- Windows Driver for monitoring System hehaviour(mainly in file operation)
- Windows Driver for bypassing NProtect anti-debugging in 2016
- Windows Driver for TenProtect anti-debugging in 2015
- APT Attack handling in a bank
- Key-Chain Management System
- HongKong Ransomware detection on Windows platform (x86/x64)
-

Mobile platform
- Kitchen Remoter Ordering System in Android / iOS platform
- Pharmacy ordering apps in Andorid and iOS platform
- Casino VIP apps in Android and iOS platform
- Shopping web by using MYSQL and PHP

Hardware related:
- A train model by using Java in Hong Kong Productivity Council Exhibition

REFERENCES

kelvinhack127.blogspot.com