About Me:

As cybercrimes are becoming more and more prevalent nowadays, being a cyber security graduate, I am confident that I can contribute to the diligent act against cybercrimes to provide a better and safe future.

"Life will always give you choices – Choosing the right one will be more beneficial in long-term than choosing the best one "

Name : Dilip C Nair *Nationality* : Indian

B. Tech : Computer Science and Engineering

M. Tech : Information and Network Security

dilipn6@gmail.com *+918136980540*

LinkedIn *Current Location*

Career Goal : "To become a Cyber Security Professional"

Knowledge and Skills

- Reverse Engineering and Malware Analysis using REMnux or Windows VM
- Finding the file type using file utility in REMnux and using Trid for more information.
- PE File format
- Loading the malware in DetectItEasy and checking for all the sections it has and checking for entropy of each sections to check whether its packed or not.
- Parsing the the PE file header using CFF Explorer to find the Image base and Entry point offset
- Checking for TLS Callbacks
- Looking at its import table
- Virustotal
- Static analysis using tools like Pecheck and Peframe in REMnux and PE studio in Windows VM
- Searching for ASCII strings in malware using strings utility and xorsearch for encoded strings
- Signsrch utility in REMnux for identifying Cryptographic signatures
- Dynamic analysis using Procmon, Regshot, InetSim, fakedns, wireshark, netcat and procdot analysis.
- Unpacking malware
- Reverse engineering using IDA
- Assembly Level Debugger with xdbg
- User mode and Kernel mode
- Setting breakpoints on API calls and DLL Entry
- Memory Map, Call stack, CPU registers in xdbg
- Malware Obfuscation and Anti-Debugging
- Windows APIs and x86 assembly language
- Finding Indicators of Compromise

Tools

file, trid, die, CFF explorer, PEiD, binee, IDA, xdbg, Pecheck, Peframe, signsrch, clamscan(clamav), yara-rules, bbcrack, floss, PE Studio, procmon, regshot, Inetsim, fakedns, wireshark, netcat, procdot, fake-ng, UPX etc…

Accomplishments

- As a part of post-graduation (M.Tech), I have developed a security-based desktop application using ***.NET – WPF(MVVM)***.
- I have named it as ***Restriction Based System (RBS)*** which comes under the class of Intrusion Detection Systems
- It has a monitoring engine that runs in the background and scans for the system activities like currently running processes and file system changes.
- The admin can keep restrictions on processes and files in the system.
- RBS will monitor for the violation of these restrictions and will trigger an alert in the system if any violation occurs.
- The admin can also get alerts through emails if he wants to.
- Double click here to view my project portfolio ⟶ 

Experience

- Worked at Cognizant for **ERSS** team – Enterprise Risk and Security Assessment (5 months).
- My job was **DR testing** (Disaster recovery testing). Here you simulate a disaster and test how an application responds to it. After testing, we submit a DR report to the client.
- Simulating a disaster basically means, simulating **denial of service**.
- Cognizant offers DR testing services to clients all over the world.
- Clients come and check their applications for Disaster Resilience.
- Presently I am an Art of Living Volunteer conducting and organizing Art of Living programmes across Kerala, India.

Misc. Details

Full Name : Dilip Chakkingal Nair

Nationality : Indian

Native State : Kerala

Date of birth : 16-September-1992

Gender : Male

Marital Status : Unmarried

Languages Known : English, Hindi and Malayalam

M.Tech (2015 – 2017) : Nirma University, Ahmedabad, Gujarat, India

B.Tech (2010 – 2014) : University of Calicut, Kerala, India