Export talk on Malware Analysis and Research:

Date: 10th July 2021

Time: 11:00 AM to 01:00 PM

Resource Person: Dr. Ashu Sharma, Sr. Malware Analyst, WatchGuard Technologies India.

Program Coordinator: Prof. Seema B. Joshi, Assistant Professor (Cyber Security), GTU-GSET

Objective of the Event:

The objective of this expert session was to learn and enhance skill of malware analysis and research.

About the Event:

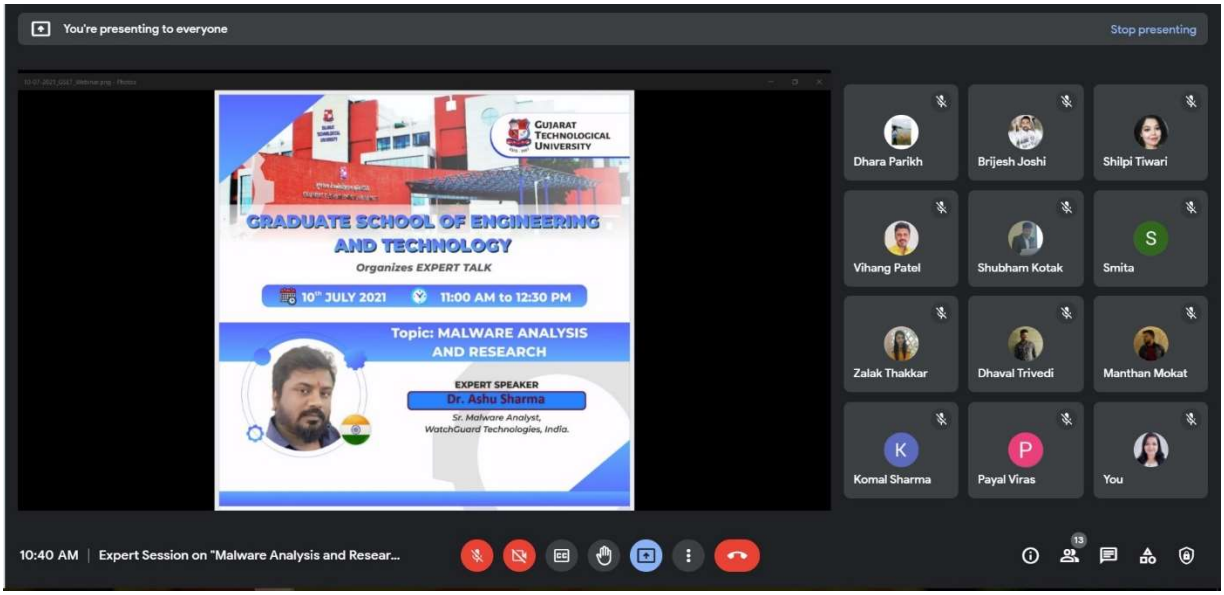
The expert session was conducted by Dr. Ashu Sharma. He had discussed the various malware detection techniques for the 2nd Generation malware. He had demonstrated the debugging techniques for signature identification of Ransomware. Also, the malware research challenges were discussed during the session.

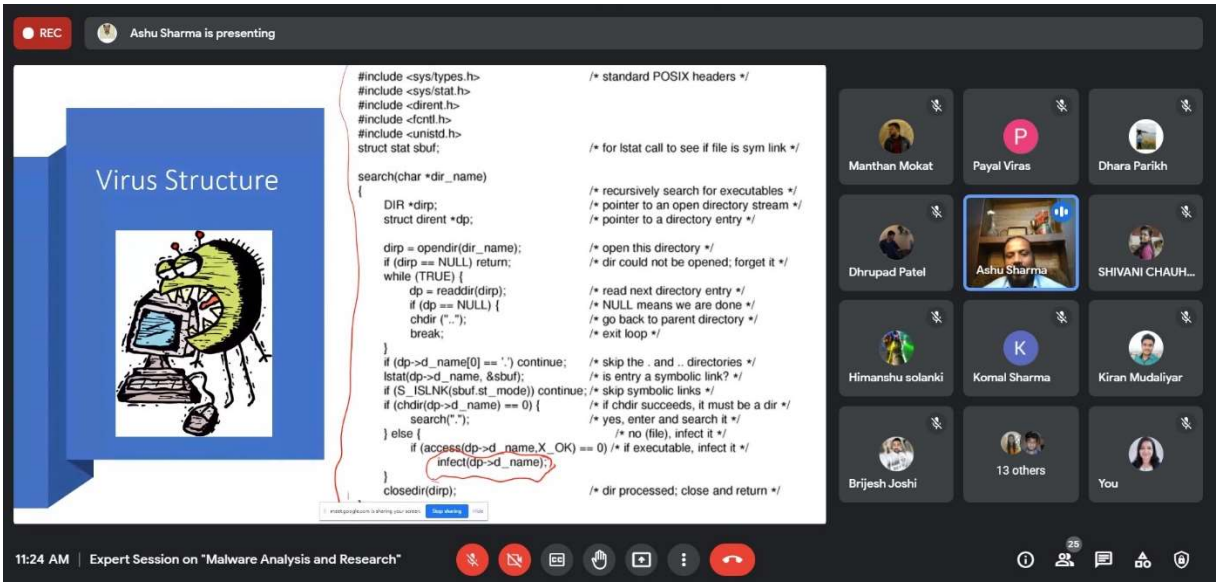
Targeted Audience: GTU-GSET Students of ME CE (Cyber Security).

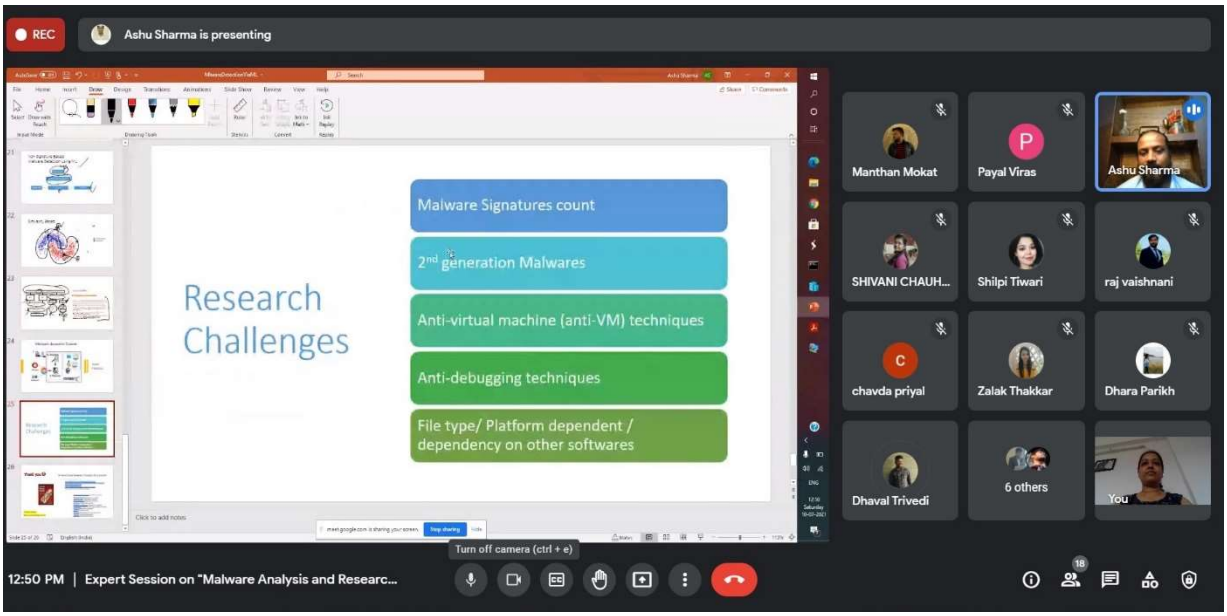
Outcomes:

At the end of this event, students were able to apply the knowledge of malware detection techniques using various tools and techniques.

Event Photographs:




REC
Ashu Sharma is presenting
Virus Structure
#include <sys/types.h> /* standard POSIX headers */
#include <sys/stat.h>
#include <dirent.h>
#include <fcntl.h>
#include <unistd.h>
struct stat sbuf; /* for lstat call to see if file is sym link */
search(char *dir_name)
{ /* recursively search for executables */
DIR *dirp; /* pointer to an open directory stream */
struct dirent *dp; /* pointer to a directory entry */
dirp = opendir(dir_name); /* open this directory */
if (dirp == NULL) return; /* dir could not be opened; forget it */
while (TRUE) {
dp = readdir(dirp); /* read next directory entry */
if (dp == NULL) { /* NULL means we are done */
chdir (".."); /* go back to parent directory */
break; /* exit loop */
}
if (dp->d_name[0] == '.') continue; /* skip the . and .. directories */
lstat(dp->d_name, &sbuf); /* is entry a symbolic link? */
if (S_ISLNK(sbuf.st_mode)) continue; /* skip symbolic links */
if (chdir(dp->d_name) == 0) { /* if chdir succeeds, it must be a dir */
search("."); /* yes, enter and search it */
} else { /* no (file), infect it */
if (access(dp->d_name,X_OK) == 0) /* if executable, infect it */
infect(dp->d_name);
}
closedir(dirp); /* dir processed; close and return */
Manthan Mokat
Payal Viras
Dhara Parikh
Dhrupad Patel
Ashu Sharma
SHIVANI CHAUH...
Himanshu solanki
Komal Sharma
Kiran Mudaliyar
Brijesh Joshi
13 others
You
11:24 AM | Expert Session on "Malware Analysis and Research"


REC
Ashu Sharma is presenting
Research Challenges
Malware Signatures count
2nd generation Malwares
Anti-virtual machine (anti-VM) techniques
Anti-debugging techniques
File type/ Platform dependent / dependency on other softwares
Manthan Mokat
Payal Viras
Ashu Sharma
SHIVANI CHAUH...
Shilpi Tiwari
raj vaishnani
chavda priyal
Zalak Thakkar
Dhara Parikh
Dhaval Trivedi
6 others
You
Turn off camera (ctrl + e)
12:50 PM | Expert Session on "Malware Analysis and Researc...