**Yara Rule for PsiXbot**

**(CS-5202)**

**2021-2022**

**Anurag Chowdhury**

**MT20ACS496**

**AREA DIRECTOR NAME FACULTY NAME**

**Dr. Debashish Sengupta Dr Ashu Sharma**

The below string is behaves like a spyware

$a= "PeekMessage"

$b= "GetMessage"

$c= "DispatchMessage"

$d= "GetUserName"

The below string looks malicious

$e= "L-V3"

$f= "86B("

The below strings represents that a RDP connection is being created and the string WTSUnRegisterSessionNotification" is used to suppress notification.Probably a spyware

$g= "WTSSendMessage"

$h= "WTSEnumerateServers"

$i= "WTSUnRegisterSessionNotification"

$j= "WTSVirtualChannelOpen"

$k= "WTSFreeMemory"

$l= "WTSDisconnectSession"

The below Strings Detects that it is a behaviour or nomaclature of malware. KillAV string will atempt to disable the AV

$m= "KillAv"

$n= "Ransomeware"

$o= "Psix"

$p= "BotModules"

$q= "Malware.exe"