**Yara Rule for Emotet**

**(CS-5202)**

**2021-2022**

**Amit Ranjan Sahoo**

**MT20ACS492**

**AREA DIRECTOR NAME FACULTY NAME**

**Dr. Debashish Sengupta Dr Ashu Sharma**

The below string is behaves like a spyware

$a="CreateObject"

$b="Root Entry"

$c="autoopen"

These are root level privileges. Usually these are used in trojan backdoor

$d="word/media/image1.pngPK"

$e="word/theme/theme1.xmlPK"

These links are looking malicious.

$f="bypass"

$g="prog0ramm"

These are some keyword which look like phishing strings