IOCs

Domains:

freewindowssoftware[.]com
filehubspot[.]com
digitalfilestores[.]com
afghannewsnetwork[.]com
newsindia[.]ddns.net
mmfaa[.]ddns[.]net
vmi296708[.]contaboserver[.]net
5-135-125-106[.]cinfuserver[.]com
mailupdater[.]net
nscinfo[.]ddns[.]net
vmi192147[.]contaboserver[.]net
mffatool[.]ddns[.]net
vmi532529[.]contaboserver[.]net
vmi420862[.]contaboserver[.]net
vmi475662[.]contaboserver[.]net
vmi388643[.]contaboserver[.]net
vmi369553[.]contaboserver[.]net
vmi512038[.]contaboserver[.]net
vmi312537[.]contaboserver[.]net
mfahost[.]ddns[.]net
vmi489177[.]contaboserver[.]net
vmi240582[.]contaboserver[.]net
vmi281634[.]contaboserver[.]net

HTA URLs:
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/html/
hxxps://londonkids[.]in/echoolz/assets/css/front/kwy/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/kwy/html5/
hxxps://londonkids[.]in/echoolz/assets/css/front/tfs/css/

hxxps://londonkids[.]in/echoolz/assets/css/front/tfs/html5/
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/DATE-OF-NEXT-INCREMENT-ON-UP-GRADATION-OF-PAY-ON-01-JAN-AND-01-JUL/css
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/PUBLICATION-OF-PART-II-ORDER-HRMS/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/kwy/2021-02-21%20MR(HS)-191-E1(DPC)/css
hxxps://iiieyehealth[.]com/fonts/times/files/Call-for-Proposal-DGSP-COAS-Chair-Excellance/css
hxxps://iiieyehealth[.]com/fonts/times/files/css/
hxxps://iiieyehealth[.]com/fonts/times/files/js/
hxxps://vedicwisdom[.]in/wp-content/uploads/2020/08/css2/
hxxps://vedicwisdom[.]in/wp-content/uploads/2020/08/css/
hxxps://vedicwisdom.in/wp-content/uploads/2019/13/hwo/DISCHARGE-DRILL/css/
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/ETPBs-Speed-Post-Booking/css/
hxxps://dice-academy.com/new/media/docs/hww/css/index.php
hxxps://ipa[.]co[.]in/assets/pdfs/cmaps/html/index.php
hxxps://demo[.]smart-hospital[.]in/uploads/hospital_content/logonw/html4/
hxxps://londonkids[.]in/admin/plugins/ckeditor/skins/moono/images/hidpi/EngrCoprsMatters/css/
hxxps://www.fincruitconsulting[.]in/js/cl/h-jquery/files/doc-d-01/html/1.hta
hxxps://fincruitconsulting[.]in/js/cl/h-jquery/files/doc-d-01/html/
hxxps://fincruitconsulting[.]in/js/cl/h-jquery/html/
hxxps://praditatech[.]com/dashboard/vendor/mike42/escpos-php/pdf/html
hxxp://demo[.]smart-hospital[.]in/uploads/hospital_content/mr/xml-http/1.hta
hxxp://culinarypassportatlanta[.]com/wp-content/uploads/2019/05/mr/files/cv/html/1.hta
hxxp://foreigngirlproblems[.]com/wp-content/uploads/2019/07/em_n/1.hta
hxxp://foreigngirlproblems[.]com/wp-content/uploads/2019/08/hta3_n/2.hta
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/html/jquery.txt
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/DATE-OF-NEXT-INCREMENT-ON-UP-GRADATION-OF-PAY-ON-01-JAN-AND-01-JUL/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/DATE-OF-NEXT-INCREMENT-ON-UP-GRADATION-OF-PAY-ON-01-JAN-AND-01-JUL/css/css.hta
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/css/css.hta
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/DATE-OF-NEXT-INCREMENT-ON-UP-GRADATION-OF-PAY-ON-01-JAN-AND-01-JUL/css
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/css/
hxxps://londonkids[.]in/admin/plugins/ckeditor/skins/moono/images/hidpi/EngrCoprsMatters/css/
hxxps://iiieyehealth[.]com/fonts/times/files/Call-for-Proposal-DGSP-COAS-Chair-Excellance/css/
hxxps://iiieyehealth[.]com/fonts/times/files/Call-for-Proposal-DGSP-COAS-Chair-Excellance/css/pdf.ico
hxxps://iiieyehealth[.]com/fonts/times/files/Call-for-Proposal-DGSP-COAS-Chair-

Excellance/css/css.hta
hxxps://iiieyehealth[.]com/fonts/times/files/Call-for-Proposal-DGSP-COAS-Chair-Excellance/css
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/ETPBs-Speed-Post-Booking/css/style.css.hta
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/css/
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/ETPBs-Speed-Post-Booking/css/
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/js/jquery.txt
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/js/
hxxps://rarebooksocietyofindia[.]org/utils/assets/les/hwy/css/style7.css.hta
hxxps://ikiranastore[.]com/images/files/ist/doc/abc.hta
hxxps://ikiranastore[.]com/images/files/ist/doc/i.php
hxxps://ikiranastore[.]com/images/files/ist/doc/
hxxps://ikiranastore[.]com/images/files/ist/doc/Cir-Bfg-Int.docx
hxxps://ikiranastore[.]com/images/files/ist/doc/tingo7.rar
hxxps://ikiranastore[.]com/images/files/ist/doc/tingo.rar
hxxps://minervacollege[.]co[.]in/fonts/plugins/mrt/Image-7563/css2
hxxps://londonkids[.]in/preschool/video/emergency_vaccination/css/
hxxp://londonkids[.]in/preschool/video/Emergency_Vaccination/css
hxxp://londonkids[.]in/preschool/video/covid/css/super.hta
hxxp://cinfuserver[.]com/Emergency_Vaccination/css
hxxp://5-135-125-106[.]cinfuserver[.]com/Emergency_Vaccination/css/
hxxp://mailupdater[.]net/Covid_Vaccination/
hxxps://londonkids[.]in/preschool/video/covid_vaccination/
hxxp://filehubspot[.]com/css/hf/cy/07/
hxxp://filehubspot[.]com/css/hf/cy/ht2/
hxxp://filehubspot[.]com/css/hf/cy/07/1.hta
hxxp://filehubspot[.]com/css/hf/cy/ht2/2.hta
hxxp://filehubspot[.]com/css/hf/doc/image-2019-18.zip
hxxp://vedicwisdom[.]in/wp-content/uploads/2020/08/course/course.hta
hxxp://vedicwisdom[.]in/wp-content/uploads/2020/08/css.hta

hxxps://minervacollege[.]co.in/fonts/plugins/mrt/Image-7563/css2/
hxxp://minervacollege[.]co[.]in/fonts/plugins/crt/MoD-no.1750/css
hxxps://minervacollege[.]co[.]in/fonts/plugins/crt/MoD-no.1750/css
hxxp://minervacollege[.]co[.]in/fonts/plugins/mrt/image-7563/css2/css.hta
hxxps://minervacollege[.]co[.]in/fonts/plugins/kwy/BSF-Salary-2021
hxxps://minervacollege[.]co[.]in/fonts/plugins/mrt/Image-7563/css2/

hxxps://selforder[.]in/wp-content/uploads/wp-commerce/04/05/hzk/Tele-Directory(RSBs-ZSBs)/css/
hxxps://selforder[.]in/wp-content/uploads/wp-commerce/04/05/hzk/xml/

hxxps://dadsasoa[.]in/font/js/images/files/My-CV/css/css.hta
hxxps://dadsasoa[.]in/font/js/images/files/My-CV/css
hxxps://dadsasoa[.]in/font/js/images/files/United-States_Project_for_Promise/css/css.hta
hxxps://dadsasoa[.]in/font/js/images/files/United-States_Project_for_Promise/css

MargulasRAT download URLs:
hxxp://149[.]248.52.61/archive.rar
hxxp://149[.]248.52.61/archive7.rar

Allakore MSI infection URLs
hxxp://freewindowssoftware[.]com/store/video_locker.zip

C2 IPs and URLs:----------

CetaRAT
hxxp://164[.]68.104.126/htt_p
hxxp://161[.]97.142.96/htt_p
hxxp://109[.]236.85.152/htt_p
hxxp://173[.]249.41.175/h_t_t_p
hxxp://167[.]86.75.119/h_tt_p

DetaRAT
173[.]212.224.110:4145
173[.]249.50.230:1144

ReverseRAT
161[.]97.90.175:6666
173[.]249.50.230:1244
173[.]249.50.230:1289

MargulasRAT
149[.]248.52.61
149[.]248.52.61:8989
149[.]248.52.61:5656
149[.]248.52.61:2323

EpicenterRAT:
173[.]249.50.230:1245

Allakore

164[.]68.104.126
161[.]97.142.96
167[.]86.83.29
144[.]91.65.100
173[.]249.50.230
144[.]91.91.236
173[.]212.224.110
mmfaa[.]ddns[.]net
144[.]91.65.100:4145
144[.]91.65.100:3245
144[.]91.91.236:4140
164[.]68.104.126:4140
164[.]68.104.126:3245
173[.]212.224.110:4140
144[.]91.91.236:4145
173[.]249.50.230:3245
173[.]249.50.230:4145

ActionRAT C2:
hxxp://mmfaa[.]ddns[.]net/classifieds/update.php
hxxp://mmfaa[.]ddns[.]net/classifieds/classifieds.php
hxxp://149[.]248.52.61/weisenborn/updation.php
hxxp://149[.]248.52.61/weisenborn/aziroboro.php
hxxp://mfahost[.]ddns[.]net/classical/beacon.php
hxxp://mfahost[.]ddns[.]net/classical/update.php
hxxp://nscinfo[.]ddns[.]net/classification/update.php
hxxp://nscinfo[.]ddns[.]net/classification/classification.php
hxxp://mffatool[.]ddns[.]net/knightrider/update.php
hxxp://mffatool[.]ddns[.]net/knightrider/knightrider.php
hxxp://144[.]91.65.100/classification/updatecs.php
hxxp://144[.]91.65.100/classification/classification.php
hxxp://144[.]91.91.236/crus/update.php
hxxp://144[.]91.91.236/crus/beacon.php
hxxp://173[.]212.224.110/krowd/update.php
hxxp://173[.]212.224.110/krowd/beacon.php
hxxp://144[.]91.65.100/classics/abnormal.php
hxxp://144[.]91.65.100/classics/updetion.php
hxxp://144[.]91.65.100/classics/update.php
hxxps://afghannewsnetwork[.]com/classification/update.php
hxxps://afghannewsnetwork[.]com/classification/classification.php

hxxps://afghannewsnetwork[.]com/classification/updatecs.php

njRAT C2s
149[.]248.52.61:87
149[.]248.52.61
149[.]248.52.61:89

Lilith RAT:
173[.]249.50.230:1238
hxxp://muzicmirchi[.]000webhostapp[.]com/resources/Hello.NKU

Meterpreter shells
71bbf2394fe4909a6ce0f7085ca41f21cf5e05e3d761620e4d7f307183fb1e1b
852612666095aec2e9f3456ec4f8a9566be2c690c8583aff6055d180507d5476

167[.]86.70.194:9091
167[.]86.70.194:9092

Custom Revershell :
956f0f369082068ef24b76ec162cfc2119adbffda94e33e41b40f39d2f192ffe
161.97.90.175:8080

File Searcher Plugin:
hxxp://mfahost[.]ddns[.]net/soccer/info.php
hxxp://mfahost[.]ddns[.]net/soccer/read_cmd.php
hxxp://mfahost[.]ddns[.]net/soccer/file_scan.php
hxxp://mfahost[.]ddns[.]net/soccer/file_move.php

Google drive IOCs

Decoy document URL:
hxxps://drive.google.com/file/d/1EwjS2lnsktVryzN06UNiaj0b_ETCkcJq/view?usp=sharing

hxxps://londonkids[.]in/admin/plugins/ckeditor/skins/moono/images/hidpi/EngrCoprsMatters/css/
hxxps://drive[.]google[.]com/file/d/1Qa8P15CjcP_IXOVdZIPE95dtp0yTJaLa/view
hxxps://i.ibb.co/bLDvJWq/Whatsapp-Image-7.jpg

Associated email ids:
gillufarooq[at]gmail[.]com
jseck6047[at]gmail[.]com

Phishing URLs:
hxxp://149[.]248.52.61/webmail[.]gov[.]in/verification/KAVACH/

Other Malicious URLs:
hxxp://culinarypassportatlanta[.]com/wp-content/uploads/2019/05/mr/files/cv/mycv.zip
hxxp://culinarypassportatlanta[.]com/wp-content/uploads/2019/05/mr/files/CV/MyCV.zip
hxxp://culinarypassportatlanta[.]com/wp-content/uploads/2017/05/css/sub/crus/beacon.php