Earth Baxia Uses Spear-Phishing and GeoServer Exploit to Target APAC

SHA256 Hashes Detection
916f3f4b895c8948b504cbf1beccb601ff7cc6e982d2ed375447bce6ecb41534
Trojan.VBS.RIPCOY.ZTLI
4edc77c3586ccc255460f047bd337b2d09e2339e3b0b0c92d68cddedf2ac1e54
Trojan.VBS.RIPCOY.ZTLI
6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbed3094612a6696a40c664ce
Trojan.VBS.RIPCOY.ZBLI
1e6c661d6981c0fa56c011c29536e57d21545fd11205eddf9218269ddf53d448
Trojan.VBS.RIPCOY.ZCLI
4ad078a52abeced860ceb28ae99dda47424d362a90e1101d45c43e8e35dfd325
Trojan.VBS.RIPCOY.ZTLI
04b336c3bcfe027436f36dfc73a173c37c66288c7160651b11561b39ce2cd25e
Trojan.VBS.RIPCOY.ZTLI
c78a02fa928ed8f83bda56d4b269152074f512c2cb73d59b2029bfc50ac2b8bc
Trojan.Win64.DULLDOWN.ZTLH.component
1c13e6b1f57de9aa10441f63f076b7b6bd6e73d180e70e6148b3e551260e31ee
TrojanSpy.SH.DULL.ZTLH
9b50e888aaec0e4d105a6f06db168a8a2dcf9ab1f9deeff4b7862463299ab1ca
Trojan.Win64.SWORDLDR.ZTLH
d23dd576f7a44df0d44fca6652897e4de751fdb0becc6b14b754ac9aafc9081c
Trojan.Win64.SWORDLDR.ZTLH
d3c1ada67f9fe46dfb11f72c1754667d2ccd0026d48d37b61192e3d0ef369b84
Trojan.Win64.SWORDLDR.ZYLH
e9854ab68dad0a744925118bfae4ec6ce9c4b7727e2ad6763aa50b923991de95
Backdoor.Win64.COBEACON.ZTLH.enc
b3b8efcaf6b9491c00049292cdff8f53772438fde968073e73d767d51218d189
Backdoor.Win64.EAGLEDOOR.ZTLH
cef0d2834613a3da4befa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8
Backdoor.Win64.EAGLEDOOR.ZTLH
061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7
Backdoor.Win64.EAGLEDOOR.ZTLH
1c26d79a841fdca70e50af712f4072fea2de7faf5875390a2ad6d29a43480458
Backdoor.Win64.COBEACON.ZTLH.enc

Domains Description
recordar-simmco.s3.sa-east-1.amazonaws[.]com Decoy download site
wordpresss-data.s3.me-south-1.amazonaws[.]com Decoy download site
ecgglass-arq.s3.sa-east-1.amazonaws[.]com Decoy download site
souzacambos.s3.sa-east-1.amazonaws[.]com Decoy download site
cooltours.s3.sa-east-1.amazonaws[.]com Decoy download site
xiiltrionsoledadprod.s3.sa-east-1.amazonaws[.]com Decoy download site
app-dimensiona.s3.sa-east-1.amazonaws[.]com Decoy download site
bjj-files-production.s3.sa-east-1.amazonaws[.]com Decoy download site
footracker-statics.s3.sa-east-1.amazonaws[.]com Decoy download site
proradead.s3.sa-east-1.amazonaws[.]com Decoy download site
s3-contemp.s3.sa-east-1.amazonaws[.]com Decoy download site
homologacao-sisp.s3.sa-east-1.amazonaws[.]com Decoy download site
doare-assets.s3.sa-east-1.amazonaws[.]com Decoy download site
kcalmoments.s3.me-south-1.amazonaws[.]com Decoy download site
speedshare.oss-cn-hongkong.aliyuncs[.]com The next decoy download site
360photo.oss-cn-hongkong.aliyuncs[.]com The next decoy download site
bobs8.oss-cn-hongkong.aliyuncs[.]com The next decoy download site
status.s3cloud-azure[.]com The final decoy download site
api.s2cloud-amazon[.]com The final decoy download site
visualstudio-microsoft[.]com COBEACON C&C
us2.s3bucket-azure[.]online COBEACON C&C
static.trendmicrotech[.]com COBEACON C&C
rocean.oca[.]pics COBEACON C&C
static.krislab[.]site COBEACON C&C
ms1.hinet[.]lat COBEACON C&C
msa.hinet[.]ink EAGLEDOOR C&C

IPs Description
167.172.89[.]142 EAGLEDOOR C&C
167.172.84[.]142 EAGLEDOOR C&C
152.42.243[.]170 Download site
188.166.252[.]85 Download site