INDICATOR SHARING

Threat Actor Selling Cobalt Strike Cryptor, Claims Will Bypass Most Security Sensors

TLP:WHITE

Jan 17, 2023

Recently, DeepSeas Darkweb team discovered a post from a credible XSS crime forum account selling access to a cryptor for a cracked version of Cobalt Strike 4.7.2 and claims it will bypass several popular security sensors.

The threat actor is offering subscription access to the cryptor service at tiered prices depending on which security control the buyer wishes to bypass:

$5,000	Basic Build
$8,000	Sentinel One, Windows Defender, Kaspersky, and Sophos
$15,000	Crowdstrike, CarbonBlack, Cylance Protect

The threat actor has the username of r1z, and is a known and credible access and cobalt strike seller on multiple forums. R1z has been active since around June 2022 and has previously offered unauthorized access via compromised Confluence, Microsoft Exchange, SonicVPN, and VMWare accounts.

Indicators of Compromise:

The following Indicators of Compromise have been entered into Health-ISAC's automated sharing platform for those members ingesting automated threat indicators.

1worldsync[.]com

aracelicolin[.]org[.]mx

assistironline[.]net

beechdesigngroup[.]com

breadoflifetabernacle[.]com

burmancoffee[.]com

dentalofficeathens[.]gr

dexacoin[.]net

dunkandjump[.]com

filorga[.]com

galonivan[.]com[.]br

hcss[.]nl

hozoboz[.]com

lyngsfjord[.]com

nickthomm[.]com

serialowy[.]pl

shareddata[.]org

skymedia360[.]com

thetripgoeson[.]com

tonyevers[.]com

91[.]92[.]136[.]20

23d3d8cd3a5b8e4703a9b91970d790d1

785fcb9380b4c2310c2200790641bc73

bbbfab2763b717178141f0561584d087

cadb91ac90f52e27c0acae43b79aa202

1worldsync[.]com/xmlrpc[.]php

aracelicolin[.]org[.]mx/xmlrpc[.]php

assistironline[.]net/xmlrpc[.]php

beechdesigngroup[.]com/xmlrpc[.]php

breadoflifetabernacle[.]com/xmlrpc[.]php

burmancoffee[.]com/xmlrpc[.]php

dentalofficeathens[.]gr/xmlrpc[.]php

dexacoin[.]net/xmlrpc[.]php

dunkandjump[.]com/xmlrpc[.]php

filorga[.]com/xmlrpc[.]php

galonivan[.]com[.]br/xmlrpc[.]php

hcss[.]nl/xmlrpc[.]php

hozoboz[.]com/xmlrpc[.]php

lyngsfjord[.]com/xmlrpc[.]php

nickthomm[.]com/xmlrpc[.]php

serialowy[.]pl/xmlrpc[.]php

shareddata[.]org/xmlrpc[.]php

skymedia360[.]com/xmlrpc[.]php

thetripgoeson[.]com/xmlrpc[.]php

tonyevers[.]com/xmlrpc[.]php

Reference(s)	securityondemand
Threat Actor	Cyber Criminal

Threat Indicators

1worldsync.com	FQDN
aracelicolin.org.mx	FQDN
assistironline.net	FQDN
beechdesigngroup.com	FQDN
breadoflifetabernacle.com	FQDN
burmancoffee.com	FQDN
dentalofficeathens.gr	FQDN
dexacoin.net	FQDN
dunkandjump.com	FQDN
filorga.com	FQDN
galonivan.com.br	FQDN
hcss.nl	FQDN
hozoboz.com	FQDN
lyngsfjord.com	FQDN

nickthomm.com	FQDN
serialowy.pl	FQDN
shareddata.org	FQDN
skymedia360.com	FQDN
thetripgoeson.com	FQDN
tonyevers.com	FQDN
91.92.136.20	IP Address
23d3d8cd3a5b8e4703a9b91970d790d1	MD5
785fcb9380b4c2310c2200790641bc73	MD5
bbbfab2763b717178141f0561584d087	MD5
cadb91ac90f52e27c0acae43b79aa202	MD5
1worldsync.com/xmlrpc.php	URL
aracelicolin.org.mx/xmlrpc.php	URL
assistironline.net/xmlrpc.php	URL
beechdesigngroup.com/xmlrpc.php	URL
breadoflifetabernacle.com/xmlrpc.php	URL
burmancoffee.com/xmlrpc.php	URL
dentalofficeathens.gr/xmlrpc.php	URL
dexacoin.net/xmlrpc.php	URL
dunkandjump.com/xmlrpc.php	URL
filorga.com/xmlrpc.php	URL
galonivan.com.br/xmlrpc.php	URL
hcss.nl/xmlrpc.php	URL
hozoboz.com/xmlrpc.php	URL
lyngsfjord.com/xmlrpc.php	URL
nickthomm.com/xmlrpc.php	URL
serialowy.pl/xmlrpc.php	URL
shareddata.org/xmlrpc.php	URL
skymedia360.com/xmlrpc.php	URL
thetripgoeson.com/xmlrpc.php	URL
tonyevers.com/xmlrpc.php	URL

Incident Date
1673585999

Alert ID 6df8d8af

View Alert

Tags r1z, Cobalt Strike

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**