Appendix A – VexTrio IOCs & PacketWatch Query

```
womanflirting.life
bonustop-price.life
allprizeshub.life
greatbonushere.top
prizes-topwin.life
a.crystalcraft.top
logsmetrics.com
webdatatrace.com
marybskitchen.com
prom-gg.com
go.clicksme.org
machinetext.org
getquery.org
quaryget.org
greenpapers.org
dailytickyclock.org
tiktok.megastok.top
tiktok.supersbows.us
tiktok.tomorrows.top
tiktok.superbowsm.top
antibotcloud.com
hixastump.com
d.strouchridun.top
```

```
http.host:(womanflirting.life OR bonustop-price.life OR allprizeshub.life OR
greatbonushere.top OR prizes-topwin.life OR a.crystalcraft.top OR
logsmetrics.com OR webdatatrace.com OR marybskitchen.com OR prom-gg.com OR
go.clicksme.org OR machinetext.org OR getquery.org OR quaryget.org OR
greenpapers.org OR dailytickyclock.org OR tiktok.megastok.top OR
tiktok.supersbows.us OR tiktok.tomorrows.top OR tiktok.superbowsm.top OR
antibotcloud.com OR hixastump.com OR d.strouchridun.top)
```

Appendix B – CrowdStrike Query for ‘Martini’ files

```
FileName=martini.exe OR FileName=martini.sys OR FileName=viragt64.sys
```