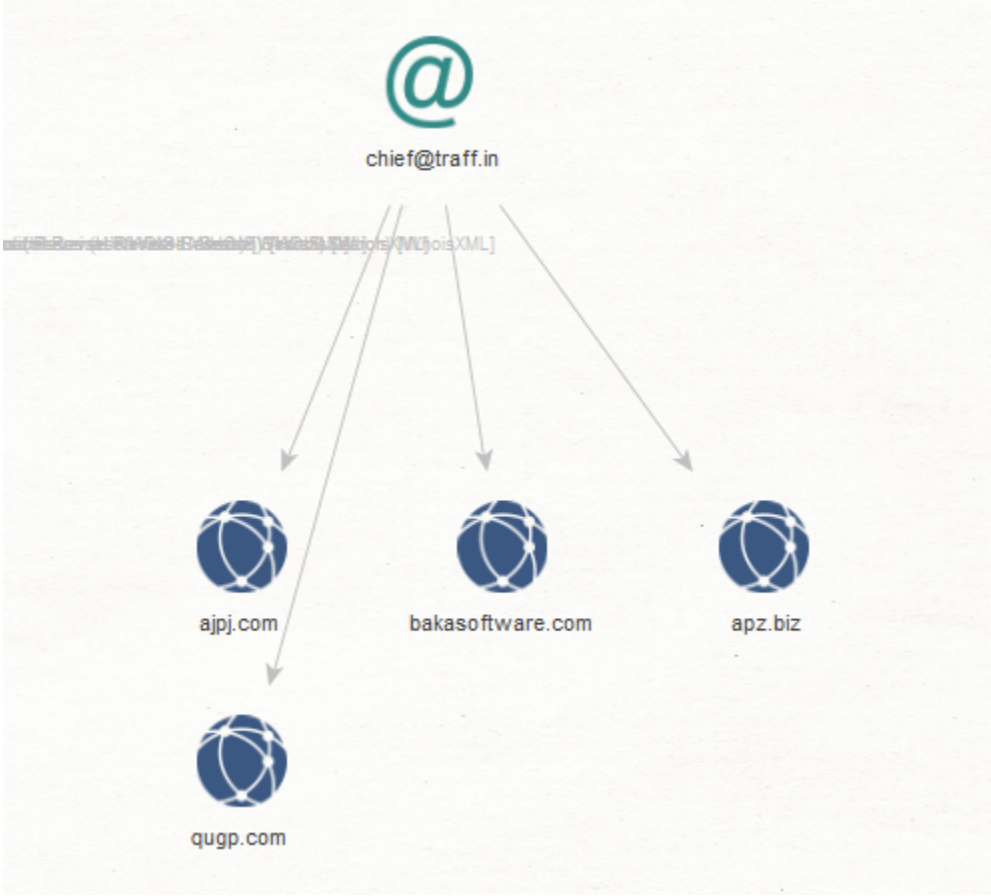
00. Exposing Bakasoftware - The Rogue Scareware Affiliate Network Circa 2008 - An OSINT Analysis

We've decided to take a deeper look at the Internet-connected infrastructure of the infamous scareware distributor circa 2008 with the idea to assist U.S Law Enforcement and the security community on its way to properly track down and monitor the rogue scareware distributor's infrastructure and eventually attempt to take it offline.

Sample malicious and rogue fraudulent domains known to have been involved in the campaign include:

bakasoftware.com
bakasoftware.net
bakadialer.com
zxrmedia.com
zaxargames.com

zxrmedia.com
zaxarstore.com
zaxargames.com
zaxarsearch.com
syscos15.ru
nidetafzy.ru
syscos19.ru
sendme13.ru
dysy.storial.ru
sendme12.ru
sendme9.ru
sendme8.ru
syscos30.ru
syscos18.ru

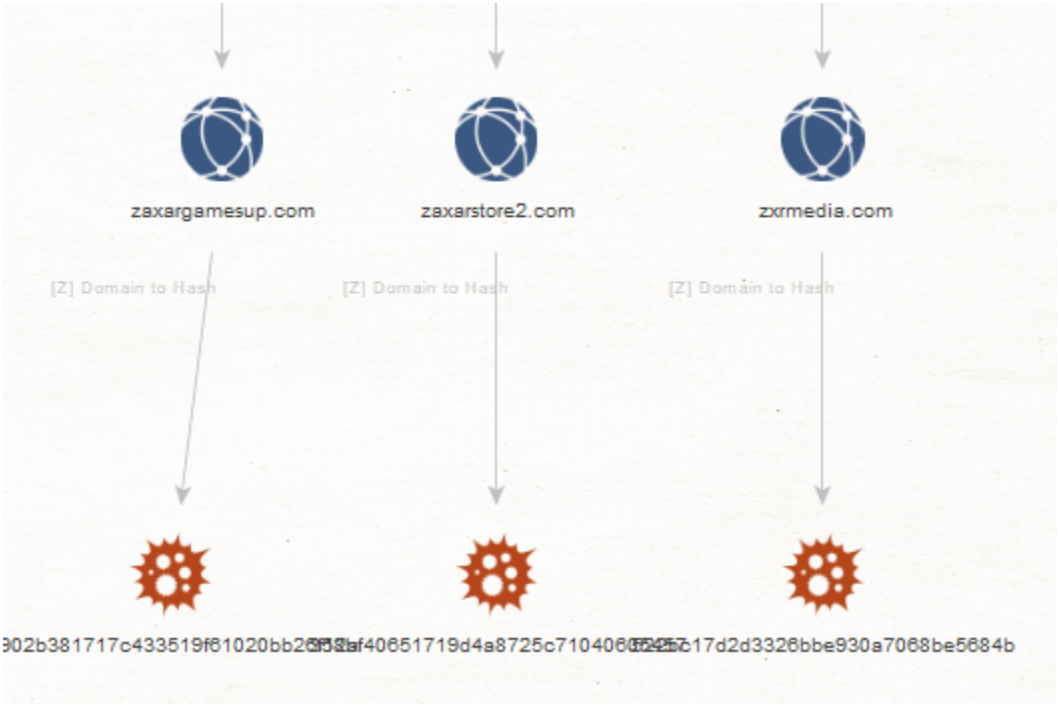


Related personally identifiable email address accounts known to have been involved in the campaign include:

chief@traff.in
support@zaxar.net
webgamesteam@hotmail.com

Related malicious and fraudulent domains known to have been involved in the campaign include:

bakasoftware.com
zaxargamesup.com
ajpj.com
zaxarstore2.com
zxrmedia.com
onlinea.net
zaxarsearch.com
zaxar.net
qugp.com
zaxargames.com
apz.biz
zaxarmail.com
zaxarstore1.com
zaxarstore3.com
zaxarstore4.com
pingip.net
zaxarstore.com



Related known responding IPs known to have been involved in the campaign include:

107.151.129.178
47.56.166.63
154.85.23.85
185.82.210.6
156.239.173.61
78.138.126.83
209.99.40.222
142.234.38.188
5.9.28.194
5.149.250.51
188.42.143.172
141.8.225.63
64.32.28.237
104.160.171.67
104.160.190.61
104.160.171.94
88.99.146.141
78.46.174.52
5.9.103.4
208.73.211.178

208.73.211.173
184.168.221.90
208.73.210.200
208.73.211.244
193.58.251.1
198.23.250.135
185.82.210.24
78.138.118.170
69.163.34.216
94.156.77.217
148.163.189.23
146.112.47.205
188.42.128.84
104.238.215.112
198.105.244.74
23.195.69.112
188.42.143.164
23.217.138.112
23.217.138.108
78.138.118.106
208.115.105.38
13.248.196.204
185.82.210.25
144.172.89.21
146.112.61.107
72.52.4.122
78.138.126.197
185.82.210.27
185.82.210.30
104.143.5.193
185.81.167.237
50.63.202.49
23.202.231.167
78.138.126.84
146.112.56.162
116.93.119.171

Related malicious MD5s known to have been involved in the campaign:

badd17d9ec5ddaf2c5d47407ae4a788b
522bc17d2d3326bbe930a7068be5684b
358bf40651719d4a8725c71040605457

d902b381717c433519f61020bb26f12a

We'll continue monitoring the campaign and we'll post updates as soon as new developments take place.