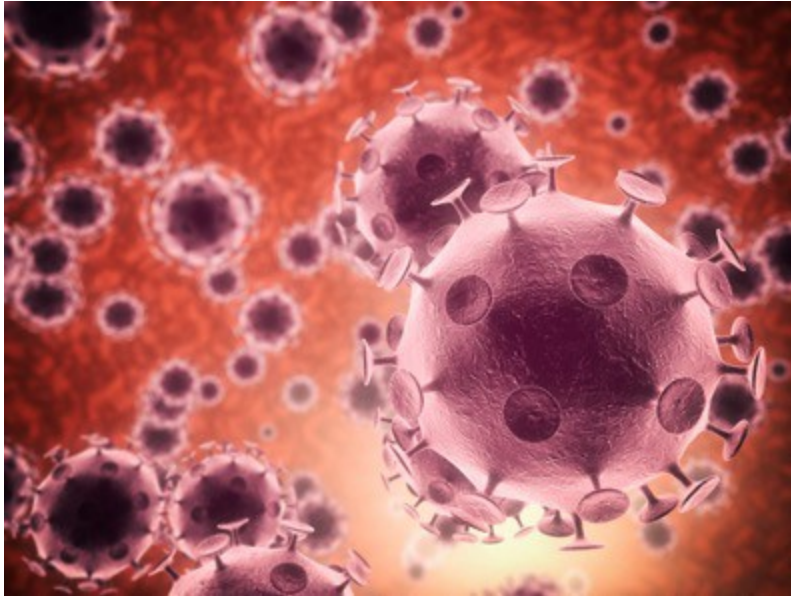


# Qbot testing malvertising campaigns?

 [medium.com/walmartglobaltech/qbot-testing-malvertising-campaigns-3e2552cbc69a](https://medium.com/walmartglobaltech/qbot-testing-malvertising-campaigns-3e2552cbc69a)

Jason Reaves

February 24, 2023



Jason Reaves

Feb 24

.

5 min read

By: Jason Reaves, Josh Platt, Jonathan McCay and Kirk Sayre

Malvertising has seen a significant uptick recently, the timing appears to coincide with Microsoft blocking most office files with macros downloaded from the web by default.

Brad Duncan put out an article showing screenshotter[3] being delivered via malvertising on Google Ads[1]. While investigating the listed C2 server, I noticed what appeared to be two naming conventions being used:

Ref:

The ones named Document show up in redirect chains that can be seen on UriScan:

Ref:

We can find emails uploaded to VirusTotal with some of these links onboard, a3c19a469f6a9337c8e33fb9249e6381eeebd5ab.

Good day,I really need your opinion on all these files in the attachment.VIEW FILES <hxxps://homepagego[.com/scd3b>Have a great dayBonjour M. Amadou,

Pivot to a QakBot

The TeamViewer named javascript files stand out as they appear to be based on a template of some kind, example:

ef930c5607b24cd1b106a944e62e67c5004795a5

A few interesting pieces of this file:

```
anExpression = 4 * (4 / 5) + 5;aSecondExpression = Math.PI * radius * radius;g = "w";f = "h";o = "p";heskkr = ".";p = ".co";s = "n";u = "i";ka = "ke";n = "t";
```

```
var today = new Date(); // Assign today's date to the variable today.j
```

```
var a = new Array(4);kRate.InstallProduct(sAssign);
```

These pieces can be pivoted on to find a similarly named javascript file:

44221d33eb4f6c9f7067cd7ddb1d8feb43ded30a

This file has some definite overlap in the template that was used:

```
anExpression = 4 * (4 / 5) + 5;aSecondExpression = Math.PI * radius * radius;g = "w";f = "h";o = "p";h = ".";p = "c";s = "n";u = "i";ka = "1";n = "t";
```

```
var today = new Date(); // Assign today's date to the variable today.
```

```
var a = new Array(4);k.InstallProduct(String.fromCharCode(Math.random()*0+104)+String.fromCharCode
```

The difference in this case however is what is downloaded:

```
hxxp://richtools[.]info/qqq.msi
```

Pivoting on the TLSH of this file also leads to another javascript file:

5ea8d40ca22df82aa4512bb359748dbbe1844ec8

```
var url = "hxxp://216.120.201[.]170/downloads/ZoomInstallerFull.msi"
```

This time possibly a Zoom theme? The first domain delivering qqq.msi was delivering this MSI package:

72cef301ca25db6f1aa42f9380ab12ae2e99a725

Inside this package resides a QakBot stager, the config encoding has been slightly changed[2] since the last time I checked:

```
def decode_data4(data): key =
hashlib.sha1(b'bUdiuy81gYguty@4frdRdpfko(eKmudeuMncueaN)').digest() rc4 =
ARC4.new(key) t = rc4.decrypt(data) tt = qbot_helpers.qbot_decode(t[20:]) return(tt)
```

Nothing too new just using multiple previously used methods to decrypt the config, parsing is also slightly different with the addition of a new flag value mixed in:

```
#Also now has an extra flag after the C2 node instead of just the preceding type
value
```

```
def parse_c2(data):
    out = ""
    if len(data) % 7 == 0:
        for i in range(0, len(data), 7):
            if i > 1:
                out += ', '
            (f, o1, o2, o3, o4, p) = struct.unpack_from('>BBBBBH', data[i:])
            out += ("{} | {}.{}.{}.{}:{}".format(f, o1, o2, o3, o4, p))
            if len(data[i+7:]) < 7:
                break
    elif len(data) % 8 == 0:
        for i in range(0, len(data), 8):
            if i > 1:
                out += ', '
            (f, o1, o2, o3, o4, p, ff) = struct.unpack_from('>BBBBBHB', data[i:])
            out += ("{} | {}.{}.{}.{}:{} | {}".format(f, o1, o2, o3, o4, p, ff))
            if len(data[i+8:]) < 8:
                break

    return out
```

QakBot config:

```
{'CONF1': b'10=BB12\r\n3=1675090602\r\n', 'C2': '1 | 24.9.220.167:443 | 1,1 |  
92.239.81.124:443 | 1,1 | 12.172.173.82:32101 | 1,1 | 162.248.14.107:443 | 1,1 |  
213.31.90.183:2222 | 1,1 | 217.128.200.114:2222 | 1,1 | 71.31.101.183:443 | 1,1 |  
81.229.117.95:2222 | 1,1 | 184.68.116.146:2222 | 1,1 | 86.130.9.183:2222 | 0,1 |  
92.154.45.81:2222 | 1,1 | 70.64.77.115:443 | 1,1 | 24.71.120.191:443 | 1,1 |  
86.225.214.138:2222 | 1,1 | 86.165.225.227:2222 | 0,1 | 172.90.139.138:2222 | 1,1 |  
92.207.132.174:2222 | 1,1 | 70.160.80.210:443 | 1,1 | 58.162.223.233:443 | 1,1 |  
47.61.70.188:2078 | 0,1 | 119.82.122.226:443 | 0,1 | 84.35.26.14:995 | 1,1 |  
73.36.196.11:443 | 1,1 | 24.123.211.131:443 | 0,1 | 23.251.92.57:2222 | 0,1 |  
208.180.17.32:2222 | 1,1 | 75.156.125.215:995 | 1,1 | 47.196.203.73:443 | 0,1 |  
173.178.151.233:443 | 1,1 | 198.2.51.242:993 | 1,1 | 103.12.133.134:2222 | 0,1 |  
86.194.156.14:2222 | 0,1 | 88.126.94.4:50000 | 1,1 | 75.191.246.70:443 | 1,1 |  
76.80.180.154:995 | 1,1 | 174.104.184.149:443 | 1,1 | 12.172.173.82:465 | 1,1 |  
92.154.17.149:2222 | 1,1 | 77.124.33.54:443 | 0,1 | 173.18.126.3:443 | 1,1 |  
27.0.48.205:443 | 1,1 | 197.1.12.81:443 | 0,1 | 86.250.12.217:2222 | 0,1 |  
93.238.63.3:995 | 0,1 | 201.244.108.183:995 | 1,1 | 86.176.37.65:443 | 0,1 |  
72.80.7.6:995 | 1,1 | 47.34.30.133:443 | 1,1 | 5.193.24.225:2222 | 0,1 |  
50.68.204.71:993 | 1,1 | 67.61.71.201:443 | 1,1 | 49.245.127.223:2222 | 0,1 |  
12.172.173.82:50001 | 1,1 | 90.162.45.154:2222 | 1,1 | 87.56.238.53:443 | 0,1 |  
73.165.119.20:443 | 1,1 | 200.109.207.186:2222 | 0,1 | 37.14.229.220:2222 | 1,1 |  
12.172.173.82:990 | 1,1 | 121.121.100.207:995 | 0,1 | 66.191.69.18:995 | 1,1 |  
74.92.243.113:50000 | 1,1 | 94.70.92.137:2222 | 0,1 | 142.119.127.214:2222 | 0,1 |  
181.118.206.65:995 | 1,1 | 50.68.204.71:995 | 1,1 | 31.120.202.209:443 | 1,1 |  
41.62.225.148:443 | 0,1 | 72.88.245.71:443 | 1,1 | 76.170.252.153:995 | 1,1 |  
184.68.116.146:3389 | 1,1 | 109.149.148.161:2222 | 0,1 | 136.35.241.159:443 | 1,1 |  
92.8.190.175:2222 | 0,1 | 91.68.227.219:443 | 1,1 | 69.159.158.183:2222 | 0,1 |  
27.109.19.90:2078 | 1,1 | 206.188.201.143:2222 | 0,1 | 50.68.204.71:443 | 1,1 |  
69.119.123.159:2222 | 1,1 | 181.118.183.2:443 | 0,1 | 172.248.42.122:443 | 1,1 |  
90.78.138.217:2222 | 1,1 | 83.7.54.167:443 | 0,1 | 12.172.173.82:2087 | 1,1 |  
75.143.236.149:443 | 1,1 | 69.133.162.35:443 | 1,1 | 130.43.172.217:2222 | 0,1 |  
27.99.45.237:2222 | 1,1 | 125.20.112.94:443 | 1,1 | 85.59.61.52:2222 | 1,1 |  
47.16.76.122:2222 | 0,1 | 12.172.173.82:995 | 1,1 | 79.26.203.25:443 | 0,1 |  
87.202.101.164:50000 | 1,1 | 86.207.227.152:2222 | 0,1 | 98.175.176.254:995 | 0,1 |  
105.184.103.7:995 | 0,1 | 190.249.231.121:443 | 0,1 | 65.95.85.172:2222 | 1,1 |  
86.172.79.135:443 | 0,1 | 76.64.202.88:2222 | 0,1 | 109.11.175.42:2222 | 1,1 |  
89.115.196.99:443 | 1,1 | 109.148.227.154:443 | 0,1 | 173.76.49.61:443 | 1,1 |  
175.139.129.94:2222 | 0,1 | 103.141.50.151:995 | 1,1 | 183.87.163.165:443 | 1,1 |  
75.98.154.19:443 | 1,1 | 31.53.29.161:2222 | 0,1 | 213.67.255.57:2222 | 1,1 |  
85.241.180.94:443 | 1,1 | 151.65.168.222:443 | 0,1 | 87.221.197.113:2222 | 0,1 |  
70.77.116.233:443 | 1,1 | 184.68.116.146:2222 | 1,1 | 86.96.72.139:2222 | 0,1 |  
74.214.61.68:443 | 1,1 | 74.33.196.114:443 | 1'} }
```

IOCs:

richtools.info  
216.120.201.170

JS:  
44221d33eb4f6c9f7067cd7ddb1d8feb43ded30a  
5ea8d40ca22df82aa4512bb359748dbbe1844ec8

MSI: 72cef301ca25db6f1aa42f9380ab12ae2e99a725

## References

---

1:

<https://isc.sans.edu/diary/Google+ad+traffic+leads+to+stealer+packages+based+on+free+software/29376>

2: <https://gist.github.com/sysopfb/8c71915b065a54e458b188fec8333c22>

3: <https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me>