TREND MICRO | research

Cyclops Blink Sets Sights on Asus Routers

By Feike Hacquebord, Stephen Hilt, Fernando Merces

APPENDIX

Appendix A: Indicators of Compromise (IOCs)

SHA-256	ccae8f66ef880ac02b9affdeaca07a7ddb9428b4f683fd55b35ea3ec20ead5ca
ID	0xA08F078B
RSA-2560 Public Key	-----BEGIN PUBLIC KEY----- MIIBYjANBgkqhkiG9w0BAQEFAAOCAU8AMIIBSgKCAUEArDTQ3wSSUvkK/BdV7rQV jjmo0tRcvuSz6uQWOzNW2jdV5ngHfJA2JD+4nKuygMH5u1Rw0oL0bPpTtheV3Fhk SEaQ4E9o19bpLq/NRhsLblBD8yXOHnKMhvu+kkmSFSFkI5uBci15Uz746ret4lcF L1hSE3pIVPbOr7JWXMlBToXnQmOq9ZiZwfi16YCwSoX7hGPG1egm+RAYAzPm9WgO BrFqUMara2thAietFyGVqN6fO1DvJoXh4AzTznsYwa8sBRJy5YrhziMcWw8zK/k2 vLMHqD+tc8sp4bt4bCaI/SwHFzKctP7YBbfhyX4P08/6leZ4jNgcbDYrhzxuAmXv hwfI93WAQ76IWyt994nWLOMs1RCDGrFOno6Q9z14QRQ8U8xEc4ZNEyBlTvLnH3JS kHmC5zQMhYYzSUY4HPMepasCAwEAAQ== -----END PUBLIC KEY-----
Telfhash	t1f06196ca4c3bce13c522d62c7ce53f1a41465406b463ed005ef8f2684e5356aa18eb79

SHA-256	7923585e8e6117eb6b3fb4a12871bc31b81d54a7ed297927bf72715c45c41da6
ID	0xBD0A5B36

RSA-2560 Public Key	-----BEGIN PUBLIC KEY----- MIIBYjANBgkqhkiG9w0BAQEFAAOCAU8AMIIBSgKCAUEA2rhl3vp5nrf1oHP+FIKq whdLKkCO8bBjmZ6t56jw4k2NU4hA/9lExmfT6dZrkmAPltr3DZ2cBmRK6iYaUBHI foOum16m9Q9fMtcKnsbMDCJ1NyeBB7XcA7hLiPU6Kccw1i+XqNgb/bZl21Cr2bSE DLSKXxEGGwlX5sUPxM5gPh86DaEdOkgsm74ALEUfmclF6xHRhNeKOehFdZ4ZUf17 r0kM8kyNBZyq56mxWNed0bvzhlwG9/AE2QU8n43q+jAldenhbFS/WapF/sNLPNRs euRdG8JT13axJnbKnFifRRJkiT4L1L8Nau7L8f1SQ4NUQL1m/uHShM9J4ssIcMWG Zl+IT+cyGKO9COE60NrgoW3X0DCVfT3lvpiNnP5/rxB2LKddh7qR7mU8JUaWNmDQ nXFAguFHiCOqq/YAFr3peO0CAwEAAQ== -----END PUBLIC KEY-----
Telfhash	t1f06196ca4c3bce13c522d62c7ce53f1a41465406b463ed005ef8f2684e5356aa18eb79

Appendix A: Cyclops Blink Command-and-Control (C&C) Servers

C&C IP Address	Country
1.9.85.247	**MY**
1.9.85.248	**MY**
1.9.85.249	**MY**
1.9.85.252	**MY**
1.9.85.253	**MY**
1.9.85.254	**MY**

2.192.0.94	IT
2.192.1.120	IT
2.192.6.144	IT
2.192.67.0	IT
2.192.7.244	IT
2.192.71.115	IT
2.192.74.124	IT
2.229.24.16	IT
2.229.32.106	IT
2.230.110.137	IT
12.34.226.34	US
12.172.90.242	US
12.191.39.162	US
12.191.39.163	US
12.191.39.164	US
12.191.39.165	US

12.191.39.166	US
24.39.220.218	US
24.96.94.11	US
24.199.247.222	US
24.227.240.210	US
24.227.240.211	US
37.26.183.94	FR
37.71.147.186	**FR**
37.99.163.162	SA
37.99.163.163	SA
37.99.163.164	SA
37.99.163.165	SA
37.99.163.166	SA
41.142.240.197	MA
50.192.49.210	**US**
50.196.104.201	**US**

50.243.3.153	**US**
50.243.3.154	**US**
50.243.3.155	**US**
50.243.3.156	US
50.243.3.157	**US**
50.255.126.65	US
65.183.166.218	US
65.183.166.219	US
65.183.166.220	US
65.183.166.222	US
69.54.25.34	US
70.62.153.174	US
70.89.246.33	US
70.89.246.34	US
70.89.246.35	US
70.89.246.36	US

70.89.246.37	US
70.91.93.133	US
72.68.69.63	**US**
78.134.89.167	IT
79.11.46.30	**IT**
80.15.113.188	FR
80.118.6.90	FR
80.153.75.103	DE
80.155.38.210	DE
80.155.38.211	DE
80.155.38.212	DE
80.155.38.213	DE
80.155.38.214	DE
81.4.177.114	CY
81.4.177.115	CY
81.4.177.116	CY

81.4.177.117	CY
81.4.177.118	CY
82.198.72.201	DE
82.62.143.41	IT
87.139.213.76	DE
87.193.135.123	DE
90.63.245.175	FR
90.85.224.121	FR
90.85.224.122	FR
90.85.224.123	FR
90.85.224.124	FR
90.85.224.125	FR
93.51.177.66	IT
93.51.177.67	IT
93.51.177.68	IT
93.51.177.69	IT

93.51.177.70	IT
96.67.145.115	US
96.80.68.193	**US**
96.80.68.194	**US**
96.80.68.195	**US**
96.80.68.196	**US**
96.80.68.197	**US**
97.87.91.211	US
97.87.91.212	US
97.87.91.213	US
97.87.91.214	US
97.87.91.215	US
97.87.91.216	US
97.87.91.217	US
97.87.91.218	US
97.87.91.219	US

100.42.249.124	CA
100.43.220.234	US
100.43.220.235	US
100.43.220.236	US
100.43.220.237	US
100.43.220.238	US
102.50.244.205	**MA**
105.157.69.243	MA
105.159.248.137	MA
109.192.30.125	DE
137.103.44.146	US
148.76.89.2	**US**
148.76.89.3	**US**
148.76.89.4	**US**
148.76.89.5	**US**
148.76.89.6	**US**

151.0.169.240	IT
151.0.169.241	IT
151.0.169.242	IT
151.0.169.243	IT
151.0.169.244	IT
151.0.169.245	IT
151.0.169.246	IT
151.0.169.247	IT
151.0.169.250	IT
151.0.185.146	**IT**
151.0.185.147	**IT**
151.0.185.148	**IT**
151.0.185.149	**IT**
151.0.185.150	**IT**
151.84.220.205	IT
156.67.22.130	IT

162.17.254.17	**US**
162.226.120.185	US
162.226.120.186	US
162.226.120.187	US
162.226.120.188	US
162.226.120.189	US
178.251.78.84	IT
178.251.78.85	IT
178.251.78.86	IT
182.73.50.114	**IN**
182.73.50.115	**IN**
183.171.8.8	MY
184.185.80.174	US
185.82.169.99	IT
185.82.169.99	IT
185.198.198.254	**TR**

188.125.98.34	IT
188.125.98.42	IT
188.125.98.43	IT
188.125.98.45	IT
188.152.254.170	IT
190.5.142.154	SV
190.5.142.155	SV
194.219.4.77	GR
194.243.24.214	IT
198.0.120.242	US
198.0.120.243	US
205.237.46.215	CA
208.81.37.50	**US**
208.81.37.55	**US**
208.81.37.56	**US**
208.81.37.57	**US**

208.81.37.58	**US**
208.81.37.59	**US**
208.81.37.60	**US**
208.81.37.61	**US**
209.33.154.42	US
209.33.154.43	US
209.33.154.44	US
209.33.154.45	US
209.33.154.46	US
209.162.240.245	CA
209.181.47.54	US
212.31.113.18	CY
212.103.208.182	**IT**
212.103.222.218	IT
212.202.147.10	DE
212.234.179.113	FR

213.166.202.194	FR
216.211.37.59	**CA**
217.57.78.18	IT
217.57.80.18	**IT**
217.141.177.210	IT
218.161.2.56	TW

Note: The IP addresses in bold were live C&Cs at the time of authoring this report.

Appendix A: Observed TCP Ports of Cyclops Blink C&Cs

TCP Ports
636
989
990
992
994
995
3269

8443

Appendix A: SSL Certificates of Cyclops Blink C&Cs

SHA-1 Fingerprint SSL Certificates	Date Issued	Expiration Date
032b81932632de35c638fb3a162e61a859ec96a7	6/13/19	6/10/29
1d78109c682633a692d97e3a0e445ac346204eb4	6/13/19	6/10/29
3438ba29aa7326c06e2d0d1fdf4677fc3f890579	6/13/19	6/10/29
3a938bf9cdb34a50b10227e1452b3a2382f1cfbf	6/13/19	6/10/29
5dde5b3c50e897fa98daff8fe6bb90d0bccf7410	6/13/19	6/10/29
645b4017bb86b3cd9adf87d78b6c2cf32257332a	6/13/19	6/10/29
9749568682af219c4a7edc3f1f5e077fea3b3199	6/13/19	6/10/29
9ae317167849c02294b1d1f5cc42a26d1e112a0a	6/13/19	6/10/29
a2850e272e78d4ec72c3997593696a9201e6ea3a	6/13/19	6/10/29
fc6f3f7343bd028f7e9aefd5fc239a4456e08a24	6/13/19	6/10/29
341fba1927b3367bb562e2561047cca1b6e10355	11/6/19	11/3/29
97e07c31ae997c73d0bd5b989c4d457ec43222fe	11/6/19	11/3/29
c37c2e56aff660b1445105de510506c3a648b679	11/6/19	11/3/29
fe4aaacdf2d36691ca4065f59ea4103d73797830	11/6/19	11/3/29
78c911793dcd9011f99ffacd145fc31a4b8aed47	11/7/19	11/4/29
3781d0b7084bb8491b1c05f325252aebd0f41c86	11/20/19	11/17/29
3a243509406a802a25cb54b8c91f760a7818b053	11/20/19	11/17/29
561ba51b42834e4117caa2ccacc316f8842fdf2d	11/20/19	11/17/29
59d414fda0be25c2cc62c23f0cf73e992699e3d2	11/20/19	11/17/29
6a862edfafe169621fd0205ac4cdfb75e8d0237b	11/20/19	11/17/29

a10eeeb0e26224d330668ec0c17d71f0e45330df	11/20/19	11/17/29
2dbeb423407a5e465b3150c5cdc5037fe08f918c	1/10/20	1/7/30
dbea1a0ac979df94f04431e9a8b10a63d7881b6c	1/10/20	1/7/30
ed30a5645350a75de6ac80699a068444f6426929	1/10/20	1/7/30
5fdd710e8f514a30bd73ba466f5f36caa0e0b591	6/8/20	6/6/30
6df2b3368f17ac97060986ae83c1753af087e152	6/8/20	6/6/30
80b899d4ad0d0062357aa1fc64568602aed4a650	6/8/20	6/6/30
8689ec491dec95a72a56d5c61fbe396fc38f89c4	6/8/20	6/6/30
8f2d4b671412f4f110625374e379bd698bda5160	6/8/20	6/6/30
9ca27e887b6809ff2d41a936b1453e4da7ab1092	6/8/20	6/6/30
e0febc8fe7ff14bdb5d070f7510964b88473576f	6/8/20	6/6/30
f349504661e647fb7b431fa4934a8623cc1661d2	6/8/20	6/6/30
f7922b3b9bca298b41260100f45e93974e6f1eba	6/8/20	6/6/30
b842552d6f19fb05fc2283e015122878d459c60a	7/15/20	7/13/30
47bf0f22402bb85c33720ec1a9a5ed85412a69be	1/15/21	1/13/31
57efcc6b354bfb23e0dc4f6e828e0dd50905be4b	1/15/21	1/13/31
821c012e736a45ffca188f8f77d9e6a34c177bbf	1/15/21	1/13/31
9b85aed5497d7b63619494fe5780e10cd564db15	1/15/21	1/13/31
a1930fef8f879fadf218661967d7ec97f048d1c0	1/15/21	1/13/31
c008fda4b34dfcdf35faf0ad7850ccece13fdd10	1/15/21	1/13/31
d5a7f453a577b2d38b0adf26612e6a4197dea064	1/15/21	1/13/31
fde64cec72d21dbfad2d29aed997bea562912245	1/15/21	1/13/31
14cfe6615b4198d7c948ad32b9a16a73e00a42b3	1/18/21	1/16/31
1db4a62936f13aa12d56bbf48811ba0d12cb43e1	1/18/21	1/16/31
713a6024f483b6669798a1666962ca9b842f0d30	1/18/21	1/16/31

8d374b3e19afa0321f7dfef64990d0940f77ae86	1/18/21	1/16/31
9a7bc345225dfc8ef4c06ab6741345f44cc3eede	1/18/21	1/16/31
223ef00e4c351831ab12f986b8b205f8d845ecee	1/20/21	1/18/31
4005125d4d437b91e9531e7397233d5e1cbfbee3	1/20/21	1/18/31
4510ef44b806ed718f7c87d6993a4cb22e93000d	1/20/21	1/18/31
49d89c7f1b304d7f12ccf0a7d6cbea830e44c4f9	1/20/21	1/18/31
5ea1e512c0d3708cafef682fffc84d193ec36add	1/20/21	1/18/31
7350e6fa073c65ac8e7f26aead5e84792e358910	1/20/21	1/18/31
a397af8074cc1a19d57cbaf0230b1b7c9880ddbf	1/20/21	1/18/31
7339f3584a2d8d63e3b78136d530dda6ab3b6749	2/10/21	2/8/31
408da97d8e4911b2461b44792dc7c2c253efc91f	12/20/21	12/18/31
88ca87a3b38080d85690538f3dfe7843eefbce19	12/20/21	12/18/31

Appendix B: C&C Server Validation Script

To validate a host suspected of being a Cyclops Blink C&C server, we wrote a script that would perform the TLS handshake, send a 4-byte packet, and wait for the 4-byte response from the server. The source code for the script is as follows:

```
#!/usr/bin/env python3


import socket

import ssl

import sys

import requests

from pathlib import Path


def usage():

    print("Usage:\n\t{0} HOST[:]PORT\n\nExamples:\n\t{0} 8.8.8.8 443\n\t{0}
9.9.9.9:666\n".format(Path(__file__).name))

    sys.exit(1)
```

```
def myip():
    r = requests.get('https://api.ipify.org?format=json')
    return r.json()['ip']

def check_cyclops_blink_c2(hostname, port, extaddr):
    ctx = ssl.create_default_context()
    ctx.check_hostname = False # Disables hostname checking
    ctx.verify_mode = ssl.CERT_NONE # Do not verify the certificate

    veredict = 'NOT DETECTED'
    response = ''

    try:
        with socket.create_connection((hostname, port), timeout=5) as sock:
            with ctx.wrap_socket(sock, server_hostname=hostname) as ssock:
                ssock.settimeout(10)
                ssock.send(b'\x00\x00\x00\x08')
                response = ssock.read(2048)
                if len(response) == 4:
                    veredict = 'POSSIBLE'
                    if socket.inet_ntoa(response) == extaddr:
                        veredict = 'ACTIVE'
                ssock.close()
    except:
        veredict = 'UNREACHABLE'

    print(hostname,
    port,
    len(response),
    response,
```

```
    veredict)


def main(argv):
    if len(argv) < 2:
        usage()

    # Accepts both host:port or host<space>port
    pos = sys.argv[1].find(':')
    if pos != -1:
        hostname = sys.argv[1][:pos]
        port = sys.argv[1][pos+1:]
    else:
        if len(argv) < 3:
            usage()
        hostname = sys.argv[1]
        port = sys.argv[2]

    check_cyclops_blink_c2(hostname, port, myip())


if __name__ == "__main__":
    main(sys.argv)
```

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

©2022 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.