Inside the SystemBC Malware-As-A-Service

By Jason Reaves

Published: 2021-06-07 · Archived: 2026-04-05 22:06:08 UTC

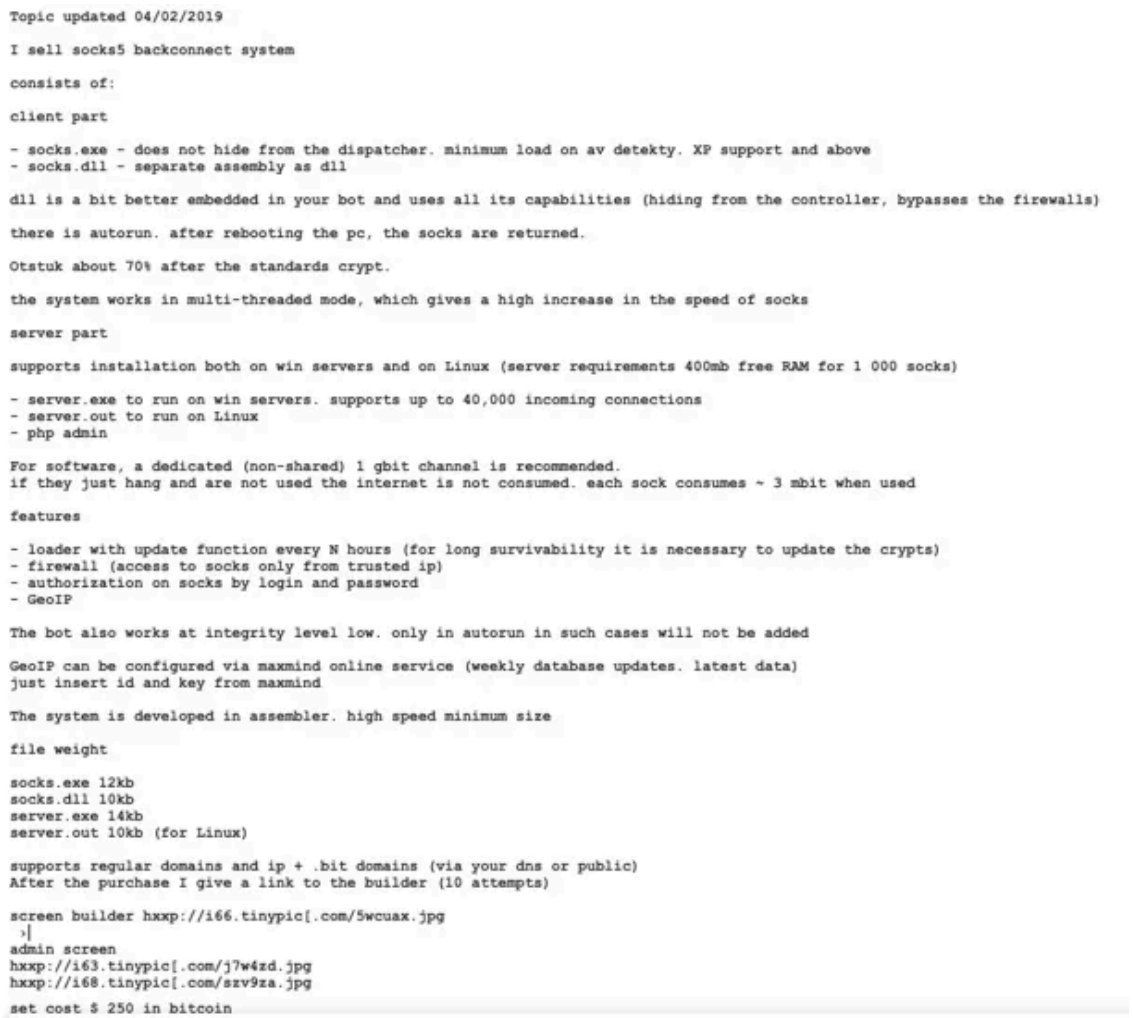
4 min read

Jun 7, 2021

By: Joshua Platt and Jason Reaves

Press enter or click to view image in full size

SystemBC has historically been a proxy bot that has been around for sale since at least April 2019[1].



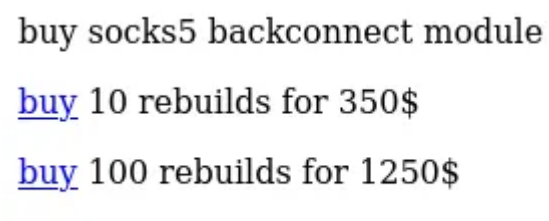
```
Topic updated 04/02/2019

I sell socks5 backconnect system

consists of:

client part

- socks.exe - does not hide from the dispatcher. minimum load on av detekty. XP support and above
- socks.dll - separate assembly as dll

dll is a bit better embedded in your bot and uses all its capabilities (hiding from the controller, bypasses the firewalls)

there is autorun. after rebooting the pc, the socks are returned.

Otstuk about 70% after the standards crypt.

the system works in multi-threaded mode, which gives a high increase in the speed of socks

server part

supports installation both on win servers and on Linux (server requirements 400mb free RAM for 1 000 socks)

- server.exe to run on win servers. supports up to 40,000 incoming connections
- server.out to run on Linux
- php admin

For software, a dedicated (non-shared) 1 gbit channel is recommended.
if they just hang and are not used the internet is not consumed. each sock consumes ~ 3 mbit when used

features

- loader with update function every N hours (for long survivability it is necessary to update the crypts)
- firewall (access to socks only from trusted ip)
- authorization on socks by login and password
- GeoIP

The bot also works at integrity level low. only in autorun in such cases will not be added

GeoIP can be configured via maxmind online service (weekly database updates. latest data)
just insert id and key from maxmind

The system is developed in assembler. high speed minimum size

file weight

socks.exe 12kb
socks.dll 10kb
server.exe 14kb
server.out 10kb (for Linux)

supports regular domains and ip + .bit domains (via your dns or public)
After the purchase I give a link to the builder (10 attempts)

screen builder hxxp://i66.tinypic[.com/5wcuax.jpg
admin screen
hxxp://i63.tinypic[.com/j7w4zd.jpg
hxxp://i68.tinypic[.com/szv9za.jpg

set cost $ 250 in bitcoin
```

From: https://www.proofpoint.com/us/threat-insight/post/systembc-christmas-july-socks5-malware-and-exploit-kits

SystemBC has also been leveraged by the TrickBot crew, specifically the high profile Ryuk subgroup involved in extortion and ransomware activities[2,3].

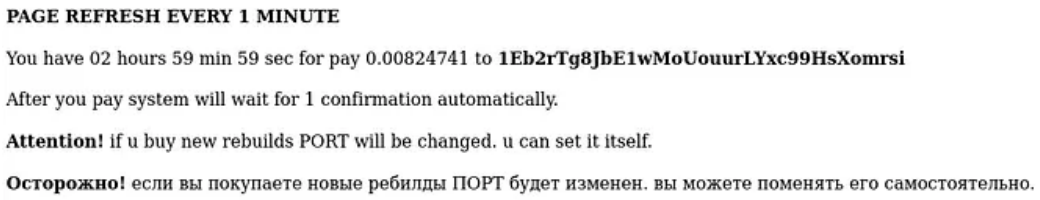
```
2020-02-25:
Ryuk Sample MD5:6a3b792208bd433a2ceff4f8321561a0
Cert: [Digital Leadership Solutions Limited]
Crypter as Emotet & TrickBot w/ Political/CoronaVirus Word Gen Meta 2020-03-03:
MD5: dceece60dcee5fd4d47755d6b3a85a75
Private Crypter - TrickBot Group
Cert: [Digital Leadership Solutions Limited]
C2: 149.248.34[.]200
```

The malware itself is pretty simplistic, although effective, but has mostly evolved into both a backdoor and proxy bot since it was first released. Customers now access a payment system over TOR(socks5v7v2snlwr7[.]onion) which presents a screen for building builds, the amount of builds you can buy along with the price has changed over time with the current option of buying involving 10 or 100 rebuilds.



After selecting which package you want you are given a screen with a timer and a wallet to send the payment to.

Press enter or click to view image in full size



After building you get a compressed archive containing your bot, server and PHP component:

```
Name
------------------------
install.txt
dll
www
www/systembc
www/systembc/geoip
server.exe
server.out
socks.exe
dll/socks32.dll
dll/socks64.dll
www/systembc/index.html
www/systembc/password.php
www/systembc/geoip/geoip2.phar
www/systembc/geoip/GeoLite2-City.mmdb
------------------------
```

The server that actors buy the package from actually contains the builder and database which is a collective of build IDs associated with each actors purchase and build. The stubs needed for building are also present. This method of building is also commonly used for crypters where you create a stub which is an already compiled executable file designed to have certain pieces of it overwritten by using either tag based identifiers or offsets in the binary. In this case it overwrites the needed configuration data in the stub files by finding the ‘BEGIN DATA’ marker and then packages them all up into a compressed archive for delivery to the buyer.

```
BEGINDATA
HOST1:192.168.1.149
HOST2:192.168.1.149
PORT1:4001
TOR:
```

The server just needs which ports to listen on for communicating with the PHP panel as well as with the incoming bots.

```
PORT0:4000
PORT1:4001
```

Hiding behind TOR is becoming an increasingly common tactic for CyberCrime actors but it does not make them invulnerable to being found, in this case the server after TOR is 107.175.150[.]179. From there we can recover most of the information needed for tracking the actor selling the malware and their customers, including the stub files for building:

```
socks-null.exe
server-null.out
```

Along with the database of customers and their builds which makes finding the actors and their panels relatively easy. Using the current pricing structure against the database we can estimate that the actor has made over ~100k USD from just selling malware builds via this server with just the current listing in the database. We also discovered that some of the actors clients are high profile criminals in the CyberCrime domain.

Get Jason Reaves's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Historically proxy bots such as SystemBC have not been tracked as closely, as it hasn't thought to be leveraged in large scale attacks, but we discovered some of the clients panels contained a significant number of bots. Some of the groups this actor is selling to include TrickBot, QBot and IcedID.

In conjunction with the discovery of the large panels we also discovered that some of the panels the bots were being tasked with downloading CobaltStrike, for example one panel was pushing the following tasks:

```
hxxp://172.104.63[.]157/crypt_beacon.exe
hxxp://172.104.63[.]157/crypt_artifact.exe
```

Being leveraged by some large CyberCrime groups as more of a backdoor for delivering CobaltStrike makes SystemBC one more thing to look out for being installed in your environment and potentially left behind even after cleaning up the other related infections.

IOCs

```
backupboxsite.com
infodialsxbz.com
data.servicestatus.one
185.61.138.59
s.avluboy.xyz
fmk7kux2dsxowkks.onion
5.188.60.166
proxyshmoxy.xyz
brabulco.ac.ug
adobeupd.host
panamontana.bit
aitchchewcdn.online
microsoftmirror.ac.ug
213.227.155.220
149.28.145.240
cheakendinner.xyz
fastconnectionbit.xyz
zghiexdgwfzi44b5.onion
gigabitsolutions.pw
217.8.117.42
ordercouldhost.com
upteambuilding.com
37.49.229.138
jjj2.rop.dev
asdasd08.com
ncordercreatetest.com
hcwakentent.com
kvarttet.com
amendingnoum.xyz
h4yk5u554epyhhen.onion
138.124.187.15
rar-archiver.ru
3q5d4sgdxdxkkzhl.onion
tvtmhltd.org
23.249.163.103
vpnstart.chickenkiller.com
```

```
hcwakententx2.com
62.77.156.147
hfbplsny55xcsgbn.onion
sweetcloud.link
199.19.225.233
system.proredirector.com
scserv1.info
proxybro.top
139.60.161.58
tik-tak.club
bc.fgget.top
185.254.121.121
scserv2.info
fahrrados.de
45.145.65.32
prorequestops.com
arbetfroll.pw
asdasd08.xyz
r55q2zj8sb89b33k.bit
37.1.220.248
gosigoji.bit
dealsbestcoupons.com
dfhg72lymw7s3d7b.onion
213.159.213.225
fresher.at
cp.nod32clients.com
predatorhidden.xyz
92.53.90.70
tdsstats.mooo.com
176.123.6.150
s2.avluboy.xyz
whatimnot.sc.ug
s1.freesocksvpn.xyz
kunkflok4ochg2m5.onion
soks5.icu
e6rldxwjc4jeb72c.onion
tik-tak-super-puper.xyz
usmostik.com
t6xhk2j3iychxc2n.onion
91.241.19.10
176.123.8.226
45.146.165.247
217.8.117.18
fragrant.digital
manillarout.com
63bwf6zdrgsmagpt.onion
5.79.124.201
```

```
138.197.141.150
generalnetworking.net
coinupdater.bit
arbetfrolli.pw
35.246.195.35
5.206.224.199
arhi-lab.com
185.119.57.126
31.44.184.186
you.bit
xxxxxxtnuhffpbep.onion
217.8.117.65
cashnet-server.com
4renewdmn.biz
137.74.151.42
35.246.186.86
84.38.129.162
ssl.virtualpoolnet.com
websitetbox.com
bmwsocksmozg.top
92.63.197.143
coinsdoctor.bit
systemhomeupdate.com
dragonfire.ac.ug
185.33.84.190
2y0y.l.time4vps.cloud
socks5.in
92.53.90.84
socks5.eu
masonksmith.me
s1.freevpnsocks.xyz
www.wappallyzer.com
advertrex20.xyz
devstudiakomp.xyz
cleanerwors.com
188.212.22.165
5.188.60.95
maka.bit
194.61.24.117
shellcon.pro
dwuhpii.bit
dktigsgquxihyrik.onion
bitdesk.online
93.187.129.249
asdfghjkl.host
gentexman37.xyz
tbueguicsrwo64i7.onion
```

```
proxybum.xyz
217.8.117.24
core-networking.com
jlayxnzzin5y335h.onion
103.124.104.11
qtrader.club
185.125.230.131
protoukt.com
185.197.74.227
master-socks.cc
23hfdne.com
americalatina.club
jjj.rop.dev
45.77.65.71
45.77.65.72
149.28.201.253
efydniaemviuxkfo.onion
masonksmith.tech
194.5.250.151
devstudiakomp.com
23hfdne.xyz
93.187.129.252
mydomain47267.xyz
mydomain47294.xyz
huxere.xyz
dl-link.network
dl-link.club
88.198.147.80
78.47.64.46
```

References

1:https://www.proofpoint.com/us/threat-insight/post/systembc-christmas-july-socks5-malware-and-exploit-kits

2:https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

3:https://twitter.com/vk_intel/status/1234891766924484609?lang=en

---