Inside the SystemBC Malware-As-A-Service

medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6

Jason Reaves June 7, 2021

Jason Reaves

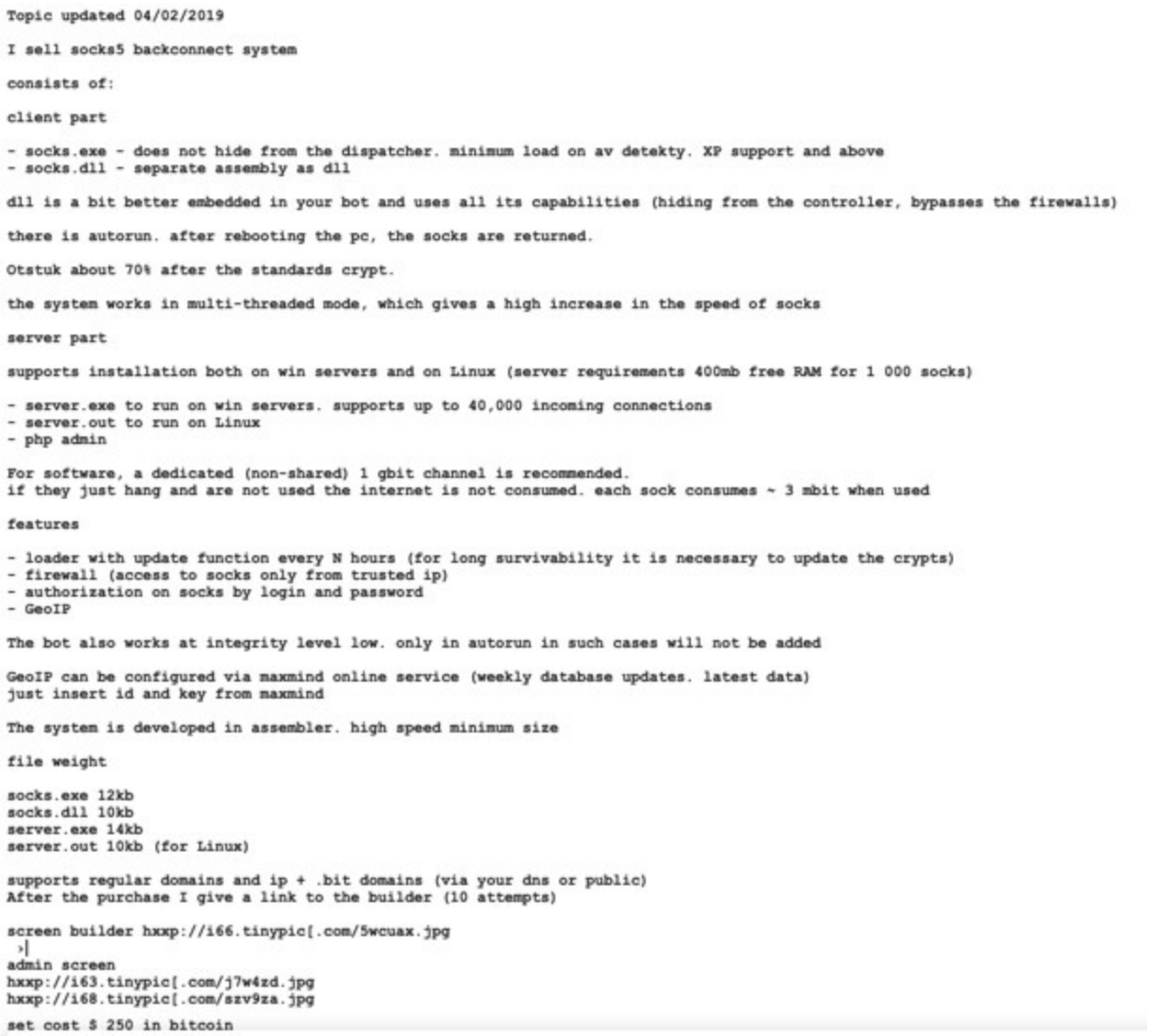
Jun 7, 2021

.

4 min read

By: Joshua Platt and Jason Reaves

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:

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.

buy socks5 backconnect module

buy 10 rebuilds for 350$

buy 100 rebuilds for 1250$

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

PAGE REFRESH EVERY 1 MINUTE

You have 02 hours 59 min 59 sec for pay 0.00824741 to **1Eb2rTg8JbE1wMoUouurLYxc99HsXomrsi**

After you pay system will wait for 1 confirmation automatically.

Attention! if u buy new rebuilds PORT will be changed. u can set it itself.

Осторожно! если вы покупаете новые ребилды ПОРТ будет изменен. вы можете поменять его самостоятельно.

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

```
Name-----------------------
install.txtdllwwwwww/systembcwww/systembc/geoipserver.exeserver.outsocks.exedll/socks3
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.

```
BEGINDATAHOST1:192.168.1.149HOST2:192.168.1.149PORT1:4001TOR:
```

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

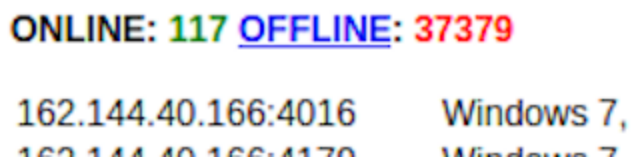
```
PORT0:4000PORT1:4001
```

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.exeserver-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.

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.cominfodialsxbz.comdata.servicestatus.one185.61.138.59s.avluboy.xyzfmk7k
archiver.ru3q5d4sgdxdxkkzhl.oniontvtmhltd.org23.249.163.103vpnstart.chickenkiller.comh
tak.clubbc.fgget.top185.254.121.121scserv2.infofahrrados.de45.145.65.32prorequestops.c
tak-super-
puper.xyzusmostik.comt6xhk2j3iychxc2n.onion91.241.19.10176.123.8.22645.146.165.247217.
lab.com185.119.57.12631.44.184.186you.bitxxxxxtnuhffpbep.onion217.8.117.65cashnet-
server.com4renewdmn.biz137.74.151.4235.246.186.8684.38.129.162ssl.virtualpoolnet.comwe
networking.comjlayxnzzin5y335h.onion103.124.104.11qtrader.club185.125.230.131protoukt.
socks.cc23hfdne.comamericalatina.clubjjj.rop.dev45.77.65.7145.77.65.72149.28.201.253ef
link.networkdl-link.club88.198.147.8078.47.64.46
```

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