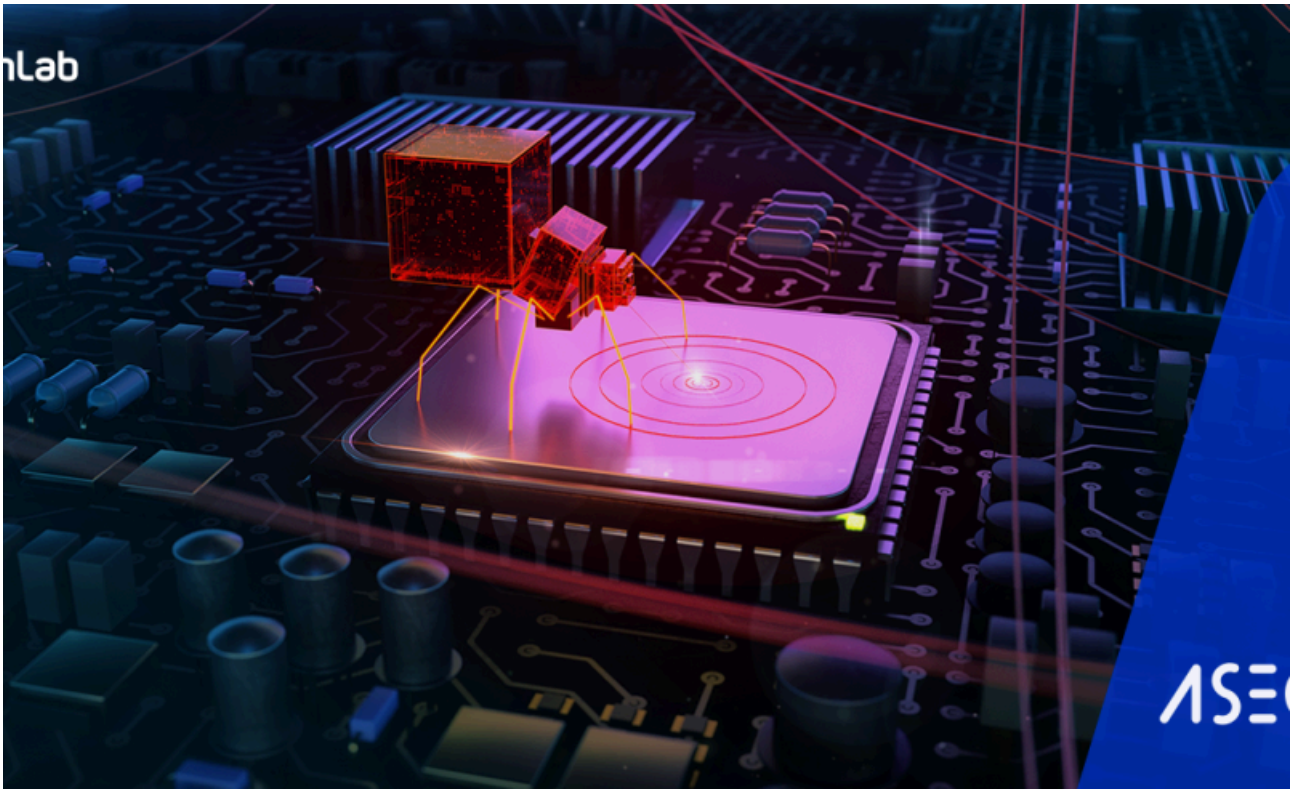
Bondnet Using Miner Bots as C2 - ASEC

By ATCP

Published: 2024-05-27 · Archived: 2026-04-05 16:24:59 UTC



Bondnet first became known to the public in an analysis report published by GuardiCore in 2017[1] and Bondnet's backdoor was covered in an analysis report on XMRig miner targeting SQL servers released by DFIR Report in 2022[2]. There has not been any information on the Bondnet threat actor's activities thereon, but it was confirmed that they had continued their attacks until recent times.

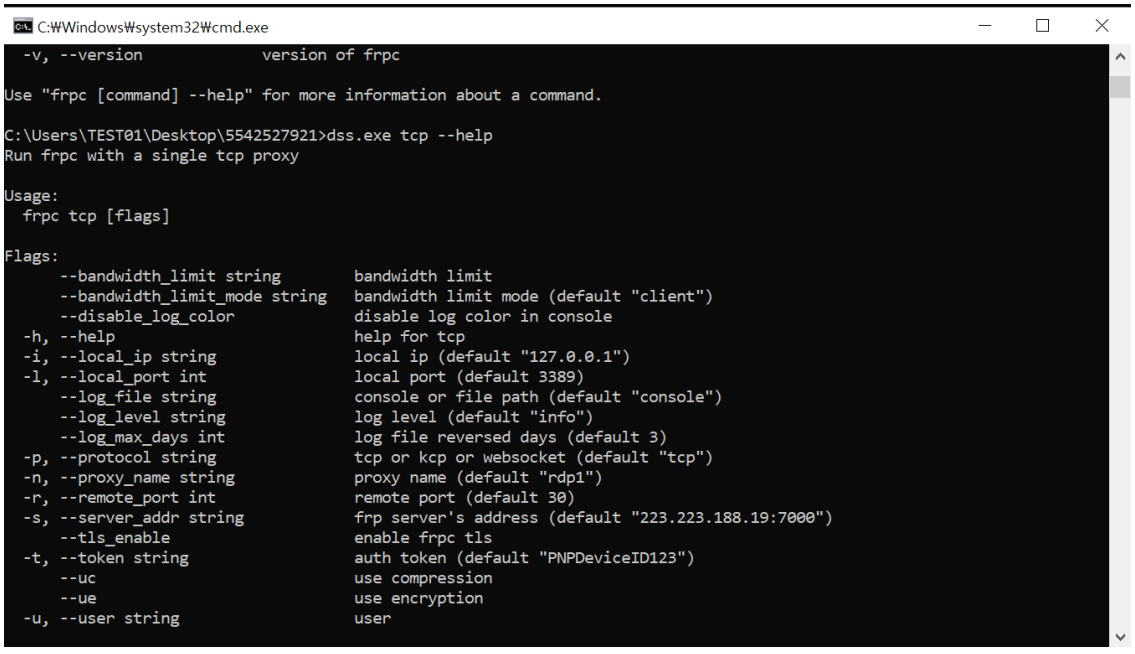
AhnLab SEcurity Intelligence Center (ASEC) found through analyzing systems infected with Bondnet miners that the **Bondnet threat actor is still active** and discovered circumstances of them **configuring a reverse RDP environment on high-performance bots and using them as C2 servers** since 2023. The reverse RDP environment was established on high-performance bots that fulfilled certain conditions.

Behavior	**Behavior Condition**
Add an adminxy account	is_pc (CPU condition check) • If the CPU manufacturer is Intel • If the model number is i3, i5, i7, or i9 is_pc2 (network interface condition check)

	• If the network interface manufacturer is Red Hat arr_find_str • If the system's language setting is one of the following: ◦ Russian, Korean, English, or Japanese ◦ The footnoted Dead Code includes a syntax
Download a reverse RDP program	Conditions for adding an adminxy account are met If the CPU core count exceeds 10

Table 1. Conditions for establishing a reverse RDP environment in the backdoor

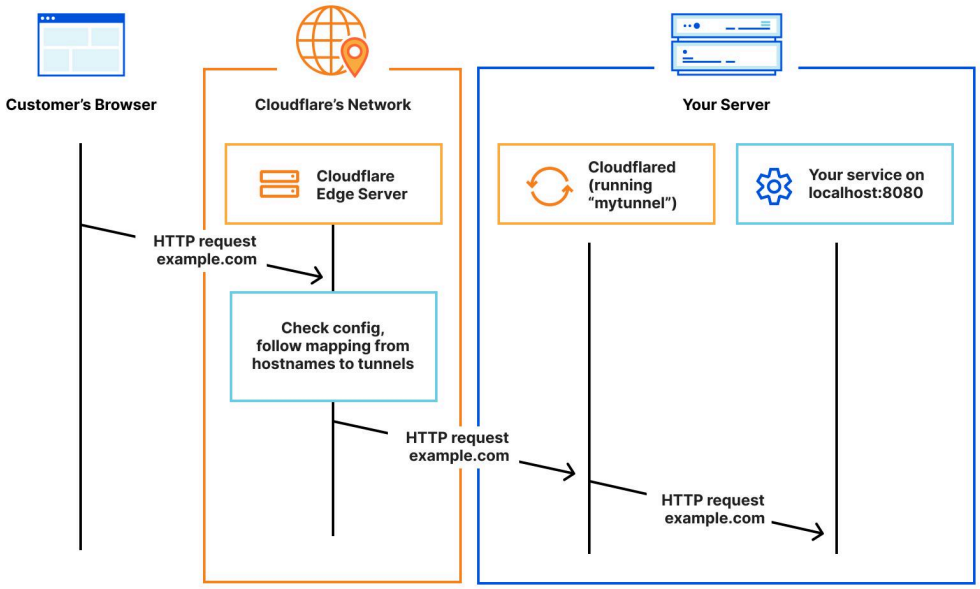
The Bondnet threat actor used proxy servers and a fast reverse proxy (hereinafter "FRP") tool to configure the reverse RDP environment. FRP is an open-source proxy program published on GitHub and the Bondnet threat actor modified the FRP program code before using it. The FRP program file modified by the threat actor included information necessary for connection including the threat actor's proxy server address, protocol, port, and token name.



After configuring the reverse RDP environment using the modified FRP program, the threat actor accessed the target system via RDP and executed two programs.

First, they executed the Cloudflare tunneling client.

The Cloudflare tunneling client allows tunneling between a certain port in the system it is executed in and a domain mapped to the Cloudflare network.

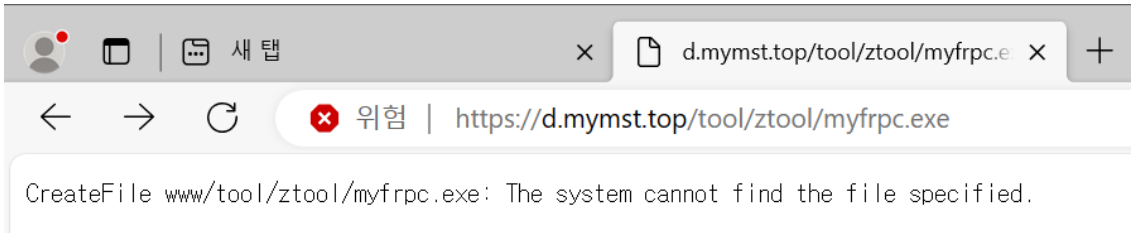


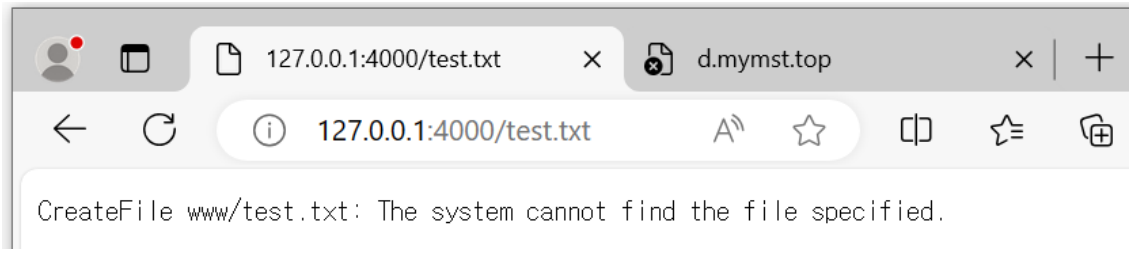
The Bondnet threat actor's C2 domain is registered on Cloudflare and the threat actor was able to use the Cloudflare tunneling client to link a certain service in the target system with the C2 domain registered in Cloudflare.

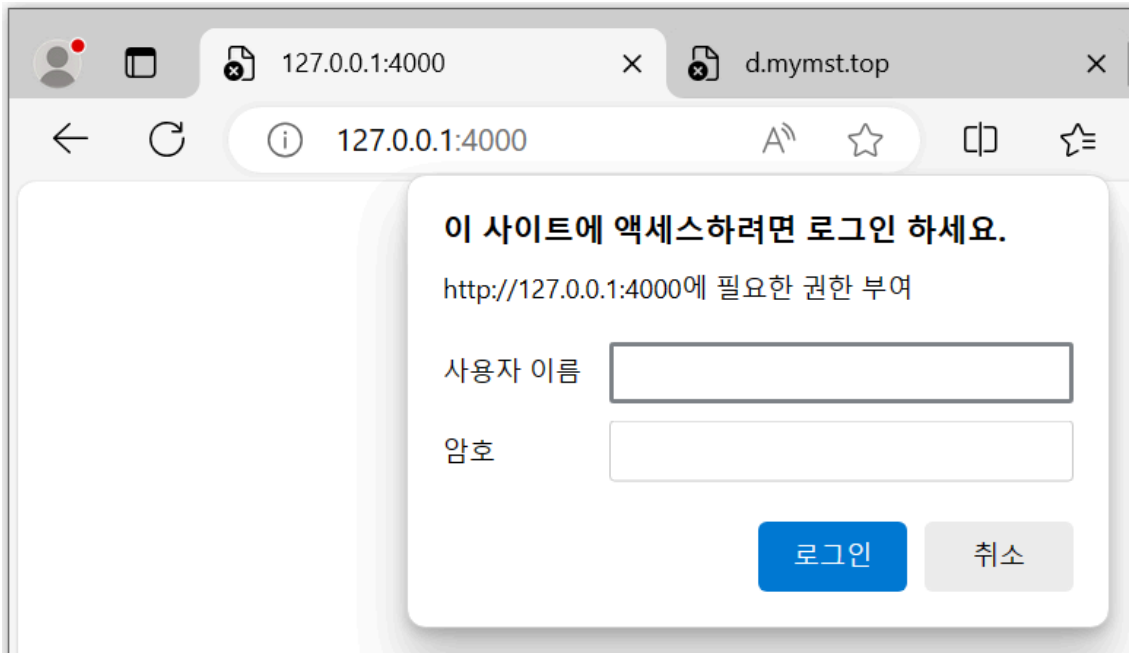
```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2021-05-26
Comment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0
```

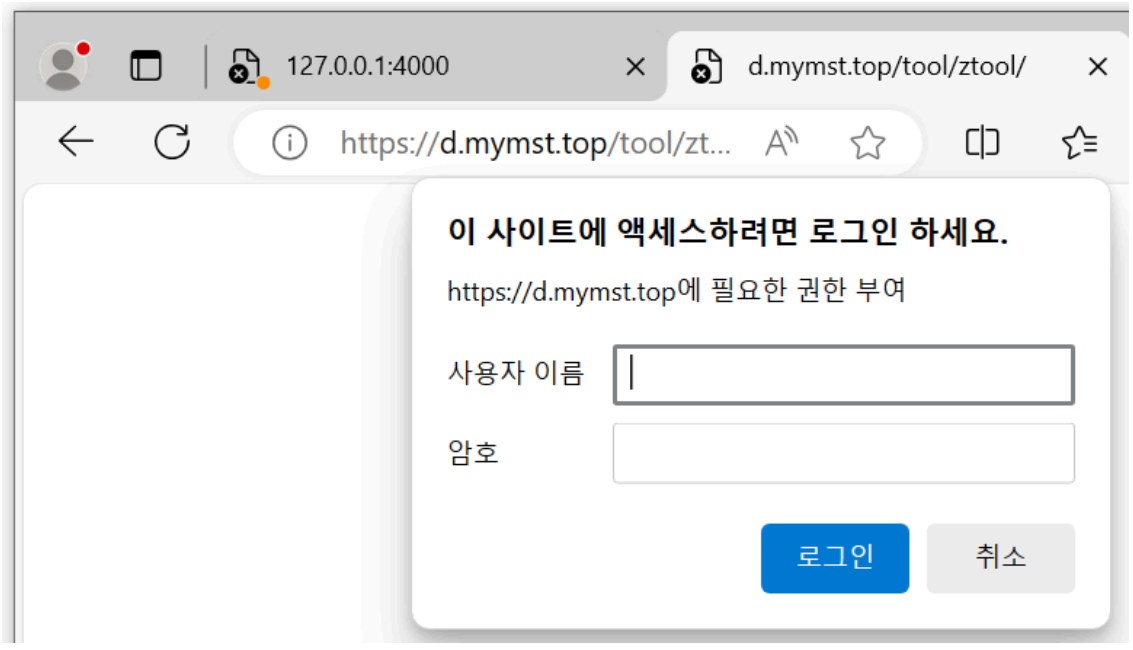
Next, they executed an HTTP File Server (HFS) program.

Upon execution, the HFS program provides a file server service to the TCP 4000 port. For the HFS program, similarities could be found with the threat actor's C2 environment. It was confirmed that the reply message for requesting a path that does not exist and the login pop-up that appears when approaching the directory path were the same. It is believed that the same HFS program would have been running in the C2 at the time of analysis.









The Bondnet threat actor used two programs in the affected system to create the HFS service in the target system and tried to connect the service with the Cloudflare domain via tunneling to use as a C2.

However, the HFS program written in Golang failed to run due to environmental issues of the affected system, and the ASEC team could not confirm the behavior of the system being converted to a C2. Although the actual

conversion process could not be observed, the following circumstances lead to the conclusion that the threat actor intended to utilize a botnet system as a C2.

- After the reverse RDP connection, there were no observed behaviors in the affected system of information leakage or internal movement
- The threat actor executed the Cloudflare tunneling client and the HFS program in the target system
- The threat actor's C2 domain is linked to Cloudflare
- The UI of the HFS program and that of the threat actor's C2 are the same
- Some malicious files could not be downloaded from the threat actor's C2 at the time of analysis
- About one month later, the UI of the threat actor's C2 changed, new malicious files appeared, and deleted malicious files were restored

After failing to convert the affected system to a C2, the Bondnet threat actor changed the C2 UI about a month later. It seems as if after facing failure in the target system, the threat actor used another bot to replace the C2, likely employing another program instead of the HFS program which caused an issue in the target system.

[File Detection]

- CoinMiner/Win.XMRig.C5449500(2023.07.05.00)
- Downloader/FOMB.Agent(2024.02.27.00)
- Downloader/Win64.Agent.C2426880(2018.03.29.04)
- HackTool/Win.Agent(2024.03.15.00)
- HackTool/Win.Frpc.C5473755(2023.08.20.03)
- HackTool/Win.PassViewer.C5353351(2023.01.09.03)
- HackTool/Win.PassViewer.C5353353(2023.04.26.02)
- HackTool/Win.PstPass.C5135577(2022.08.31.02)
- HackTool/Win.PSWTool.R345815(2023.06.02.01)
- HackTool/Win32.Mailpassview.R165244(2016.07.12.09)
- Ransomware/Win.Phobos.R363595(2023.08.28.04)
- Trojan/BAT.RUNNER.SC198137(2024.03.15.00)
- Trojan/BAT.RUNNER.SC198138(2024.03.15.00)
- Trojan/BAT.Runner.SC198226(2024.03.18.02)
- Trojan/RL.Mimikatz.R248084(2018.12.10.01)
- Trojan/Win.Lazardoor.R496534(2022.05.14.01)
- Trojan/Win32.Infostealer.C1259157(2015.11.16.06)
- Trojan/Win32.Infostealer.C1259157(2015.11.16.06)
- Trojan/Win32.Infostealer.C1259157(2020.07.17.00)
- Trojan/Win32.Miner.C2462674(2018.04.13.09)
- Trojan/Win32.Neshta.X2117(2018.03.16.06)
- Unwanted/Win.PassView.C5359535(2023.01.16.03)
- Unwanted/Win32.HackTool.C613821(2014.11.02.03)
- Unwanted/Win32.Masscan.C3122810(2019.12.06.00)
- Unwanted/Win32.Passview.C568442(2014.09.23.00)
- Unwanted/Win32.PassView.R333746(2020.04.22.08)

Reference Links

1 The Bondnet Army: https://www.akamai.com/blog/security/the-bondnet-army
2 SELECT XMRig FROM SQLServer: https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver
3 Cloudflare Docs: https://developers.cloudflare.com/cloudflare-one/connections/connect-networks

MD5

00fa7f88c54e4a7abf4863734a8f2017

057d5c5e6b3f3d366e72195b0954283b

0753cab27f143e009012053208b7f63e

0fc84b8b2bd57e1cf90d8d972a147503

15069da45e5358578105f729ec1c2d0b

Additional IOCs are available on AhnLab TIP.

URL

http[:]//185[.]141[.]26[.]116/hotfixl[.]ico

http[:]//185[.]141[.]26[.]116/stats[.]php

http[:]//185[.]141[.]26[.]116/winupdate[.]css

http[:]//46[.]59[.]210[.]69[:]7000/

http[:]//46[.]59[.]214[.]14[:]7000/

Additional IOCs are available on AhnLab TIP.

FQDN

d[.]mymst[.]top

frp[.]mymst007[.]top

m[.]mymst[.]top

Additional IOCs are available on AhnLab TIP.

IP

223[.]223[.]188[.]19

47[.]99[.]155[.]111

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/66662/