Fodcha DDoS botnet reaches 1Tbps in power, injects ransoms in packets

By
Bill Toulas

- October 27, 2022
- 10:12 AM
- 0

A new version of the Fodcha DDoS botnet has emerged, featuring ransom demands injected into packets and new features to evade detection of its infrastructure.

360Netlab researchers discovered Fodcha in April 2022, and since then, it has been silently receiving development and upgrades, steadily improving and becoming a more potent threat.

According to a new report published by the same researchers, the latest Fodcha version 4 has grown to an unprecedented scale, with its developers taking measures to prevent analysis after Netlab's last report.

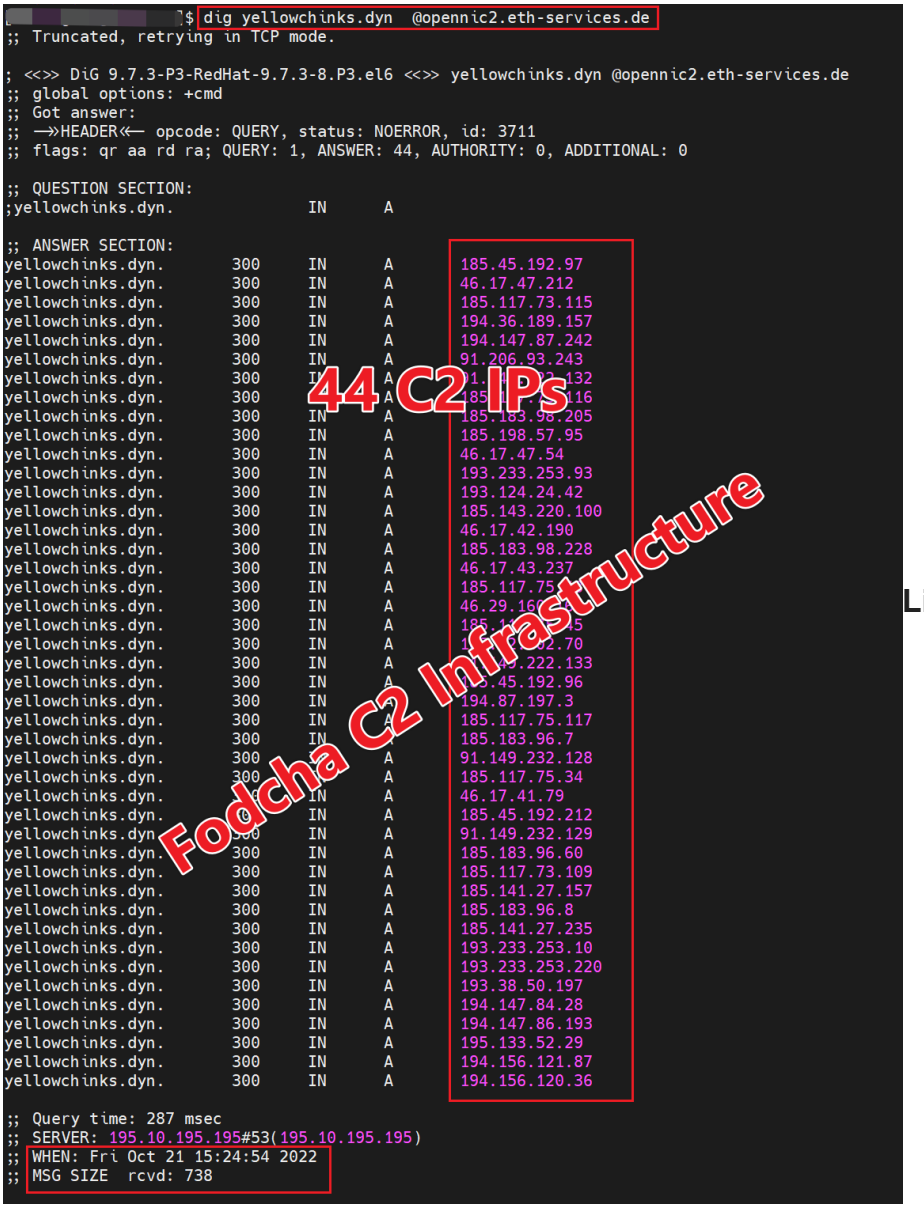
The most notable improvement in this botnet version is the delivery of ransom demands directly within DDoS packets used against victims' networks.

In addition, the botnet now uses encryption to establish communication with the C2 server, making it harder for security researchers to analyze the malware and potentially take down its infrastructure.

More DDoS power

As a DDoS operation, Fodcha had grown significantly since April, when it targeted an average of 100 victims daily. The average number of targets has increased by ten times, reaching 1,000 daily.

The botnet now relies on 42 C2 domains to operate 60,000 active bot nodes daily, generating up to 1Tbps of destructive traffic.




```
[redacted]$ dig yellowchinks.dyn  @opennic2.eth-services.de
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6 <<>> yellowchinks.dyn @opennic2.eth-services.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3711
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 44, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;yellowchinks.dyn.              IN      A

;; ANSWER SECTION:
yellowchinks.dyn.       300     IN      A       185.45.192.97
yellowchinks.dyn.       300     IN      A       46.17.47.212
yellowchinks.dyn.       300     IN      A       185.117.73.115
yellowchinks.dyn.       300     IN      A       194.36.189.157
yellowchinks.dyn.       300     IN      A       194.147.87.242
yellowchinks.dyn.       300     IN      A       91.206.93.243
yellowchinks.dyn.       300     IN      A       91.[redacted].132
yellowchinks.dyn.       300     IN      A       185.[redacted].16
yellowchinks.dyn.       300     IN      A       185.183.98.205
yellowchinks.dyn.       300     IN      A       185.198.57.95
yellowchinks.dyn.       300     IN      A       46.17.47.54
yellowchinks.dyn.       300     IN      A       193.233.253.93
yellowchinks.dyn.       300     IN      A       193.124.24.42
yellowchinks.dyn.       300     IN      A       185.143.220.100
yellowchinks.dyn.       300     IN      A       46.17.42.190
yellowchinks.dyn.       300     IN      A       185.183.98.228
yellowchinks.dyn.       300     IN      A       46.17.43.237
yellowchinks.dyn.       300     IN      A       185.117.75.[redacted]
yellowchinks.dyn.       300     IN      A       46.29.160.[redacted]
yellowchinks.dyn.       300     IN      A       185.[redacted].25
yellowchinks.dyn.       300     IN      A       1[redacted].2.70
yellowchinks.dyn.       300     IN      A       [redacted].222.133
yellowchinks.dyn.       300     IN      A       [redacted].45.192.96
yellowchinks.dyn.       300     IN      A       194.87.197.3
yellowchinks.dyn.       300     IN      A       185.117.75.117
yellowchinks.dyn.       300     IN      A       185.183.96.7
yellowchinks.dyn.       300     IN      A       91.149.232.128
yellowchinks.dyn.       300     IN      A       185.117.75.34
yellowchinks.dyn.       300     IN      A       46.17.41.79
yellowchinks.dyn.       300     IN      A       185.45.192.212
yellowchinks.dyn.       300     IN      A       91.149.232.129
yellowchinks.dyn.       300     IN      A       185.183.96.60
yellowchinks.dyn.       300     IN      A       185.117.73.109
yellowchinks.dyn.       300     IN      A       185.141.27.157
yellowchinks.dyn.       300     IN      A       185.183.96.8
yellowchinks.dyn.       300     IN      A       185.141.27.235
yellowchinks.dyn.       300     IN      A       193.233.253.10
yellowchinks.dyn.       300     IN      A       193.233.253.220
yellowchinks.dyn.       300     IN      A       193.38.50.197
yellowchinks.dyn.       300     IN      A       194.147.84.28
yellowchinks.dyn.       300     IN      A       194.147.86.193
yellowchinks.dyn.       300     IN      A       195.133.52.29
yellowchinks.dyn.       300     IN      A       194.156.121.87
yellowchinks.dyn.       300     IN      A       194.156.120.36

;; Query time: 287 msec
;; SERVER: 195.10.195.195#53(195.10.195.195)
;; WHEN: Fri Oct 21 15:24:54 2022
;; MSG SIZE  rcvd: 738
```

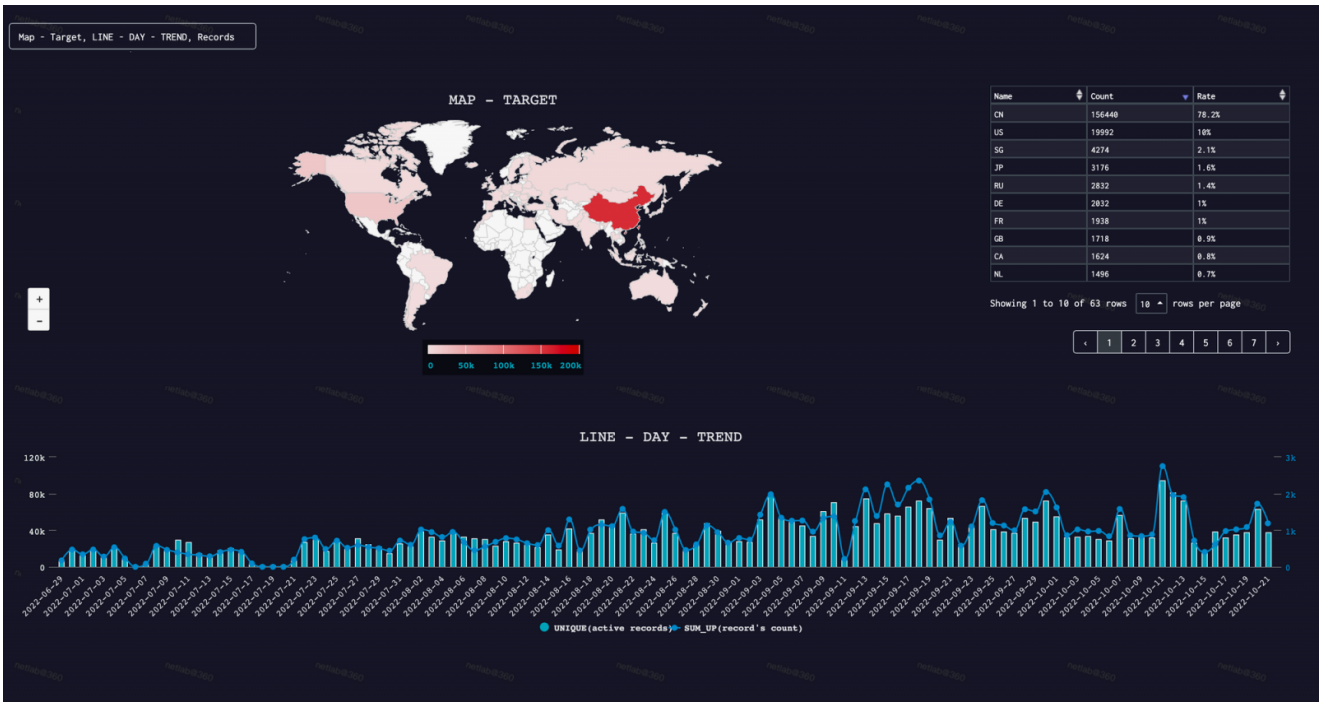
List of C2 addresses used by Fodcha *(360Netlab)*

According to Netlab, Fodcha reached a new peak on October 11, 2022, attacking 1,396 targets in a single day.

Some notable examples of confirmed attacks of Fodcha include:

- A DDoS attack against a healthcare organization on June 7 and 8, 2022.
- A DDoS attack against the communication infrastructure of a company in September 2022.
- A 1Tbps DDoS attack against a well-known cloud service provider on September 21, 2022.

Most of Fodcha's targets are located in China and the United States, but the botnet's reach is already global, having infected systems in Europe, Australia, Japan, Russia, Brazil, and Canada.



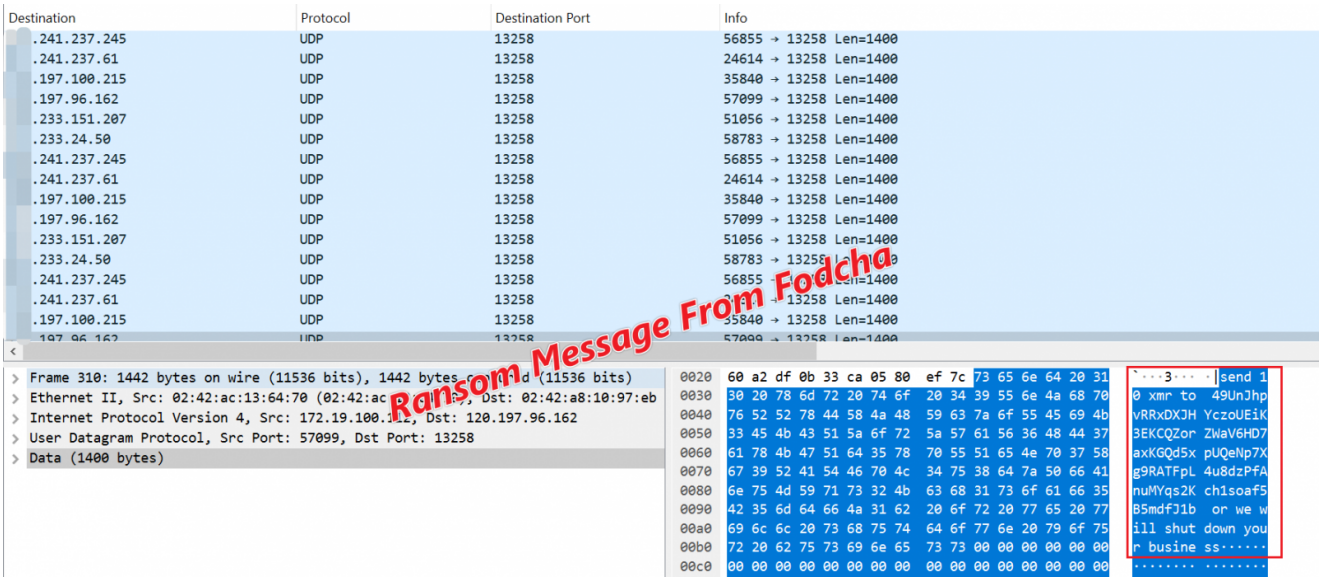
Fodcha's victim heatmap and activity volume diagram *(360Netlab)*

Embedding ransom demands

Netlab's analysts believe Fodcha is making money by renting its firepower to other threat actors who wish to launch DDoS attacks. However, the latest version also includes extortion by demanding a Monero ransom to stop the attacks.

Based on DDoS packets deciphered by Netlab, Fodcha now demands the payment of 10 XMR (Monero) from victims, worth approximately $1,500.

These demands are embedded in the 'Data' portion of the botnet's DDoS packets and warn that the attacks will continue unless a payment is made.



Fodcha's ransom message *(360Netlab)*

However, as Monero is a privacy coin, it is much harder to trace. Therefore, it is not offered for sale by almost all US crypto exchanges due to the legal requirements to prevent money laundering or other illicit activity.

Therefore, while ransomware gangs and other threat actors commonly request XMR as a payment option, almost all companies choose to pay in bitcoin, which will likely be a similar situation with DDoS attacks.

Related Articles:

Updated RapperBot malware targets game servers in DDoS attacks

Malicious extension lets attackers control Google Chrome remotely

New Chaos malware infects Windows, Linux devices for DDoS attacks

Pro-Russian hacktivists take down EU Parliament site in DDoS attack

FBI: Hacktivist DDoS attacks had minor impact on critical orgs

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.