


Mythic Case Study: Assessing Common Offensive Security Tools

 team-cymru.com/post/mythic-case-study-assessing-common-offensive-security-tools

S2 Research Team

September 6, 2022



- [S2 Research Team](#)
-
- - Sep 5
 -
 - 4 min read

Having covered the Sliver C2 framework in a previous post ([May 2022](#)), this blog will continue our examination of Cobalt Strike “alternatives”, focusing on the [Mythic](#) C2 framework.

The rationale for this write-up is based on conversations with red-team operators and our observations of internet-facing Mythic C2 servers over the past three months.

Like [Sliver](#), Mythic is a free-to-use, open-source tool. Written predominantly in Python, Mythic provides cross-platform payload creation options (Linux, MacOS, and Windows). With an active development community, and ‘plug-n-play’ functionality for its various (also open-source) agents, the technical entry barrier for users is comparatively low.

Mythic is therefore attractive to threat actors of varying skill sets; for the lower-skilled actor the ‘plug-n-play’ capabilities mean they can use the framework and additional agents ‘off-the-shelf’. In the case of higher-skilled actors, the framework’s flexibility for customization might be used to evade detection mechanisms based on ‘known’ fingerprints.

Key Findings

- Although dwarfed by Cobalt Strike, the number of online internet-facing Mythic servers outnumbers a number of other ‘common’ C2 frameworks, including Sliver.
- Mythic was observed being deployed alongside reNgine, a powerful reconnaissance tool.
- Connections to an operator identified previously utilizing Sliver, potentially in Pakistan-focused activities.
- Low confidence ties to e-crime operators have been identified within open source reporting.

Identification of Mythic Servers

Since the first quarter of 2021, the number of online Mythic servers has generally remained static; with 76 servers online at the time of writing - for ease of access we have used data from Shodan for this illustration.

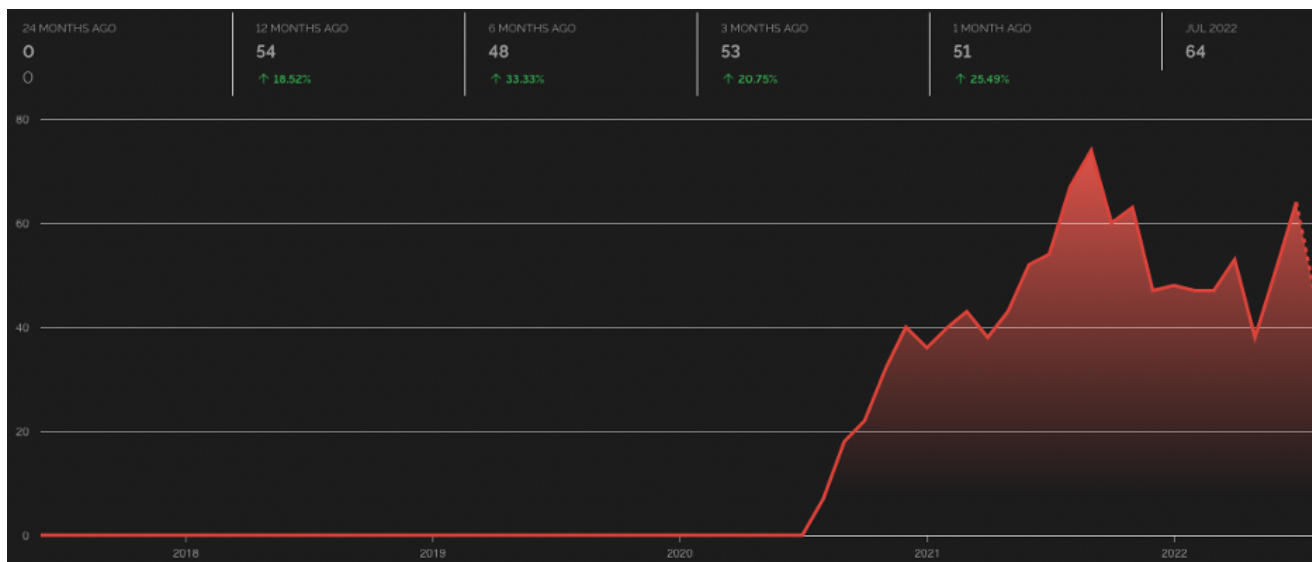


Figure 1: Online Mythic Servers

Comparing this to other C2 frameworks (including Cobalt Strike), Mythic accounts for about 2% of the current 'market share' – interestingly, about 8x more prevalent than Sliver at present.

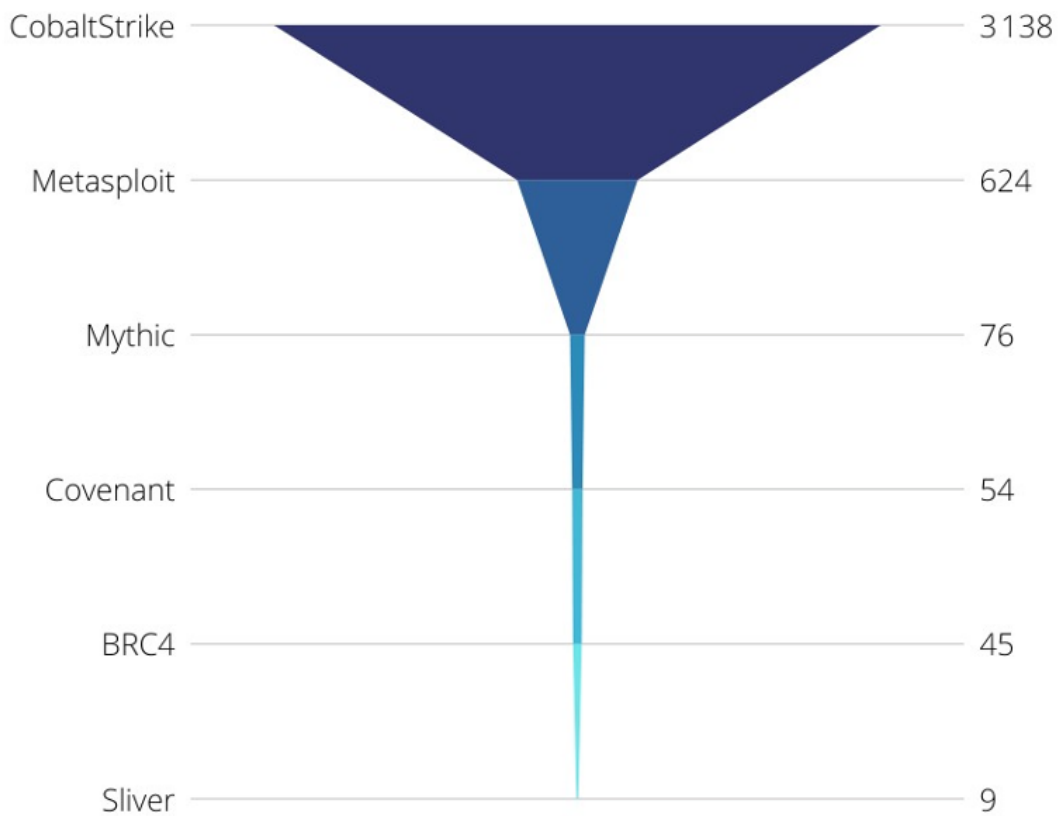


Figure 2: C2 Framework Market Share

Whilst 76 servers may seem like a low number, this only accounts for internet-facing infrastructure and likely doesn't include many of the Mythic instances being used for red team operations within closed / controlled environments.

With that being said, Cobalt Strike remains the most prevalent framework in use today. Therefore, the purpose of this blog series is not to suggest defenders divert resources away from the detection of Cobalt Strike as a threat vector, but merely to heighten awareness of emerging and plausible alternatives.

Mythic in the Wild?

Reviewing the currently online Mythic servers, most of them (90%) fit a 'default' profile, with details for the web portal port, SSL certificate, etc. having not been altered from the 'out-of-the-box' settings.

Default settings:

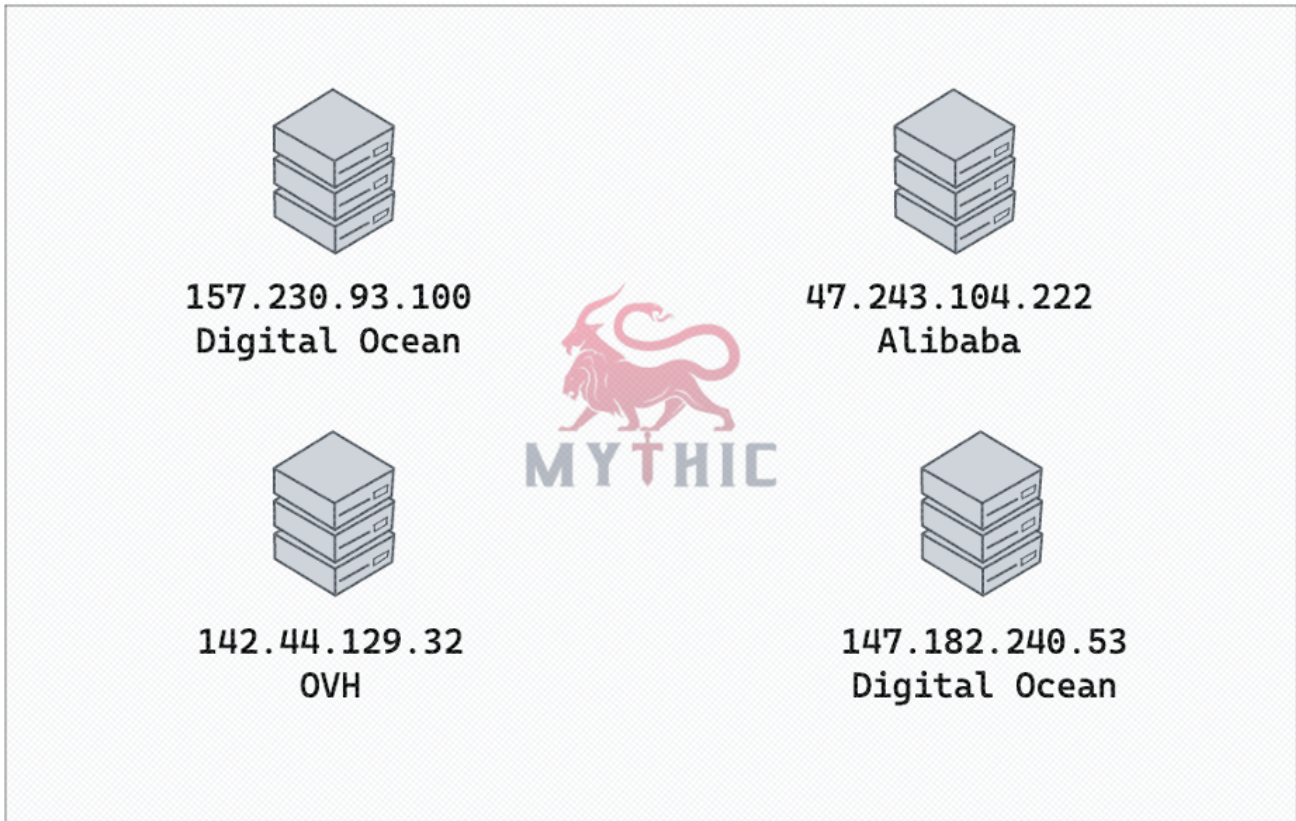
- Port - 7443
- SSL certificate - Issuer: O=Mythic

In cases where these settings were modified, we have observed cases of re-use, where modified configurations were seemingly copied from box to box over time. In doing this, actors leave behind an attributable trail which makes tracking from C2 server to C2 server possible.

For example, by following E-Tag information (present in HTTP headers), we were able to tie multiple Mythic servers together. From this starting point we start to 'zoom in' on activities utilizing the Mythic framework, shedding light on some of the use cases.

Mythic + reNgin

We were able to follow this particular operator for a number of months, based on a recurring E-Tag value. In addition to Mythic, this operator was also observed using a reconnaissance framework called 'reNgin'.




144.91.122.255
Contabo GmbH

Login to reNgine
Current release: v1.1

[Learn how to create reNgine account.](#)

Username
@ username

Password
Password

Log In

Figure 3: Identified Operator Infrastructure

Based on observed certificate information (CN = redteamtools.msrfven0m[.]xyz), this infrastructure was likely used by a red team operator to target multiple customer organizations - although the potential for a false flag cannot be ruled out.

Leaf Certificate**973486342b80415cb7593e334a133ce05805487d10e2036652e6e68130432482**

CN=redteamtools.msfn0m.xyz

C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1

Figure 4: Certificate for 47.243.104.222

In this case the scenario was quite simple, reNgine was first used to scan port 443 on the victim server, seeking vulnerabilities which would allow initial compromise / exploitation. A Mythic beacon was then dropped on a victim machine for management of the exfiltration stage.

As a side note, reNgine is another powerful tool which blue team operators should become familiar with. At the time of writing, approximately 920 online reNgine servers were identifiable.

Mythic + Pakistani Focus

In our blog on [Sliver](#), we identified a campaign which appeared to target both Pakistan and Turkey, based on the domain names observed. Whilst hunting for Mythic servers, we identified a similar domain 'rd.mofa-pk[.]org' - which appears to target the Pakistani Ministry of Foreign Affairs.

The domain mofa-pk[.]org was most recently hosted on 3.239.29.103 (assigned to AMAZON-AES), amongst the other domains hosted on this IP are:

- nationalhelpdesk[.]pk
- sngpl.org[.]pk

Both of these domains were highlighted in our Sliver blog as being connected to the same activity, as outlined below:

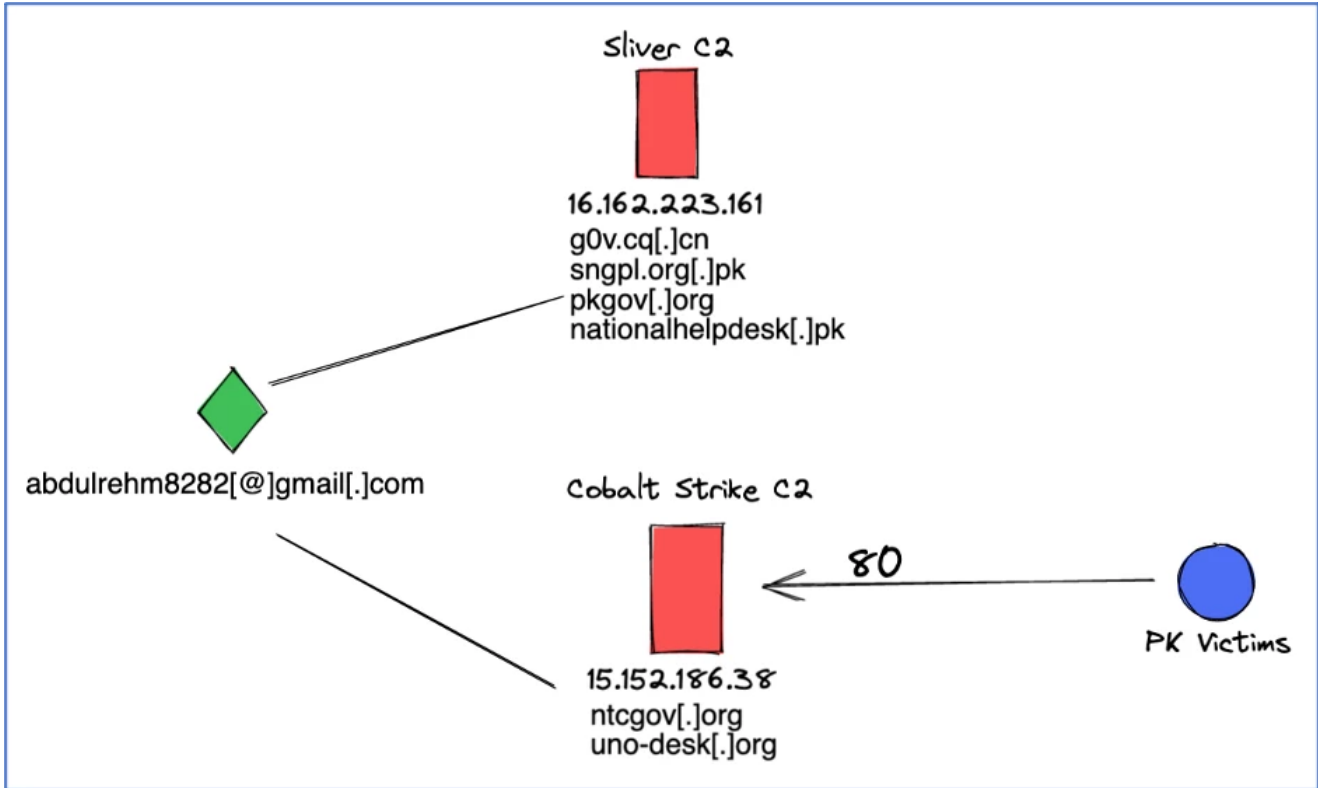


Figure 5: Excerpt from the Sliver Blog

It would appear that the operator behind this linked infrastructure makes use of a diverse range of C2 frameworks in their activities. Our investigations into this cluster continue.

Mythic + Bazarloader / Bazarbackdoor?

In June 2022, a researcher shared a new Mythic C2 framework on Twitter with a slightly different web login panel. The default login panel for a Mythic C2 contains the Mythic logo, but in this case, the page contained this “Botleggers Club” image:



Benkow moxueq

@benkow_

<https://cryptolvl-rsa-check.com/new/login>
Mythic C2 Framework

[Traduire le Tweet](#)

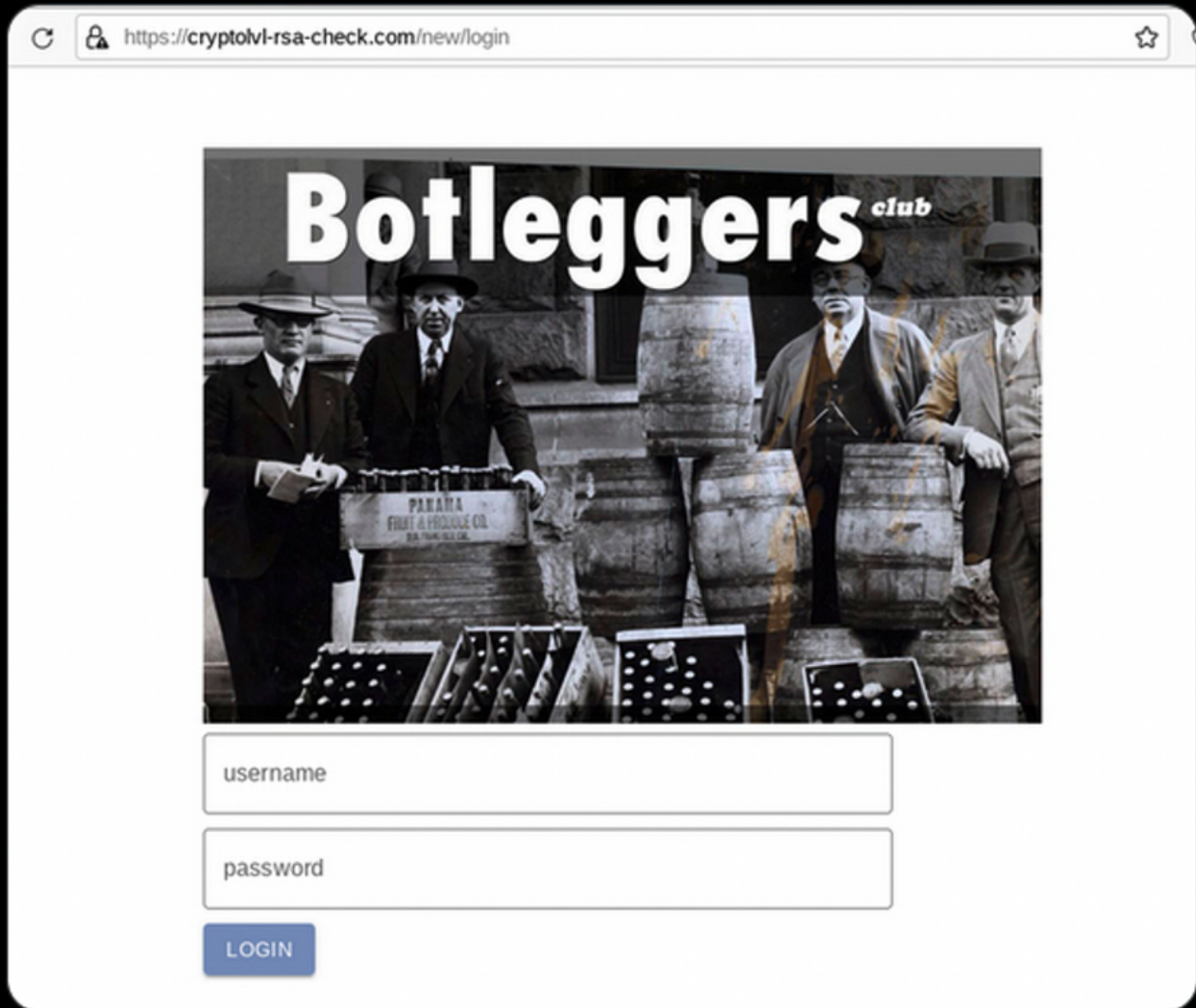


Figure 5: Source - https://twitter.com/benkow_/status/1542047469860683777

The “Botleggers Club” was mentioned in the [Conti Leaks](#) as a panel to manage / administrate and interact with clients (the bots), and also to deliver malware (BazarLoader / BazarBackdoor).

By pivoting on E-Tag values once again, a number of IP addresses were identified, sharing the same details as the Mythic C2 mentioned above (cryptolvl-rsa-check[.]com):

- 139.59.72.48
- 147.189.169.143
- 159.223.193.246
- 203.28.246.137
- 34.240.115.152
- 43.142.60.207

However, after this information (the Tweet) was publicly exposed, the server configurations were modified and now only one of these IPs is displaying the same E-Tag. It is likely that the other servers were either shut down, or moved elsewhere with updated configurations.

Conclusion

From a technical point of view, Mythic has all of the advantages of Cobalt Strike (or any of the most popular C2 frameworks). Based on the number of commits, issues, and pull requests on GitHub, the community is highly active in contributing to the development of the framework. In other forums, such as Twitter, we also observe researchers sharing their tips and tools for the improvement of Mythic functionality.

As noted already, Cobalt Strike remains the most popular C2 framework, but we wouldn't be surprised to see growth in the use of Mythic in the near future. Indeed for some red team operators, this trend is already occurring - we would expect that malicious actors have taken note and are either considering or have already adopted the use of Mythic into their TTPs.

Indicators of Compromise

Note - only the most recently active Mythic C2 servers are shared.

Domains

cisco-update.com

corpse.sh

idinfosystems.com

linux-sec.top

live-office365.com

mofa-pk.org

onerule.digital

v56119.php-friends.de

IP Addresses

101.35.90.253

103.134.19.126

139.162.8.112

139.59.144.58

139.59.249.255

142.93.166.252

142.93.246.237

159.223.234.22

3.212.113.251

3.96.54.147

46.243.186.22

47.96.177.12

5.2.79.164

54.173.67.191

Mitre Att&ck Matrix:

This Mitre Att&ck Matrix is a summary of the combined capabilities of every Mythic agent (Apollo, Athena, Tetanus, etc.):

Technique	Technique ID	Observable
Scheduled Task/Job	T1053	
Process Injection	T1055	Spawns Processes
Obfuscated Files or Information	T1027	
Software Packing	T1027.002	
Timestomp	T1070.006	Suspicious Timestamp
Virtualization/Sandbox Evasion	T1497	
Disable or Modify Tools	T1562.001	Guard pages creation
Remote System Discovery	T1018	Reads host file
Process Discovery	T1057	Query running processes

System Information Discovery	T1082	Read machine GUID, software policy, volume information
Security Software Discovery	T1518.001	
DLL Side-Loading	T1574.002	Load missing DLLs
Native API	T1016	
Application Wide Discovery	T1010	Monitors Window changes
System Time Discovery	T1124	
Application Layer Protocol	T1071	Perform DNS lookups
