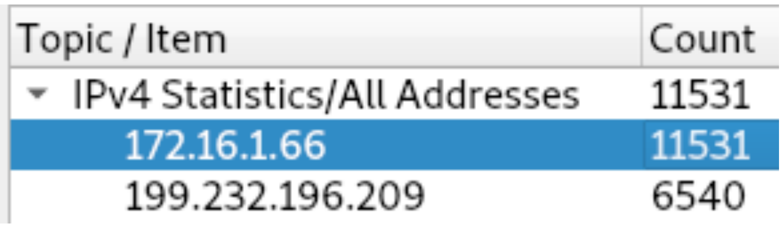
2024-07-30 (RETRY LATER)

1. check statistics

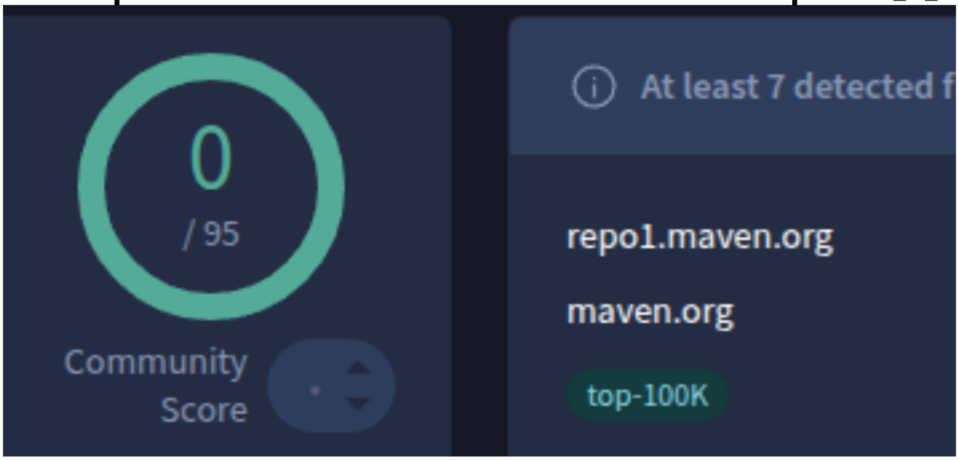


Topic / Item	Count
IPv4 Statistics/All Addresses	11531
172.16.1.66	11531
199.232.196.209	6540

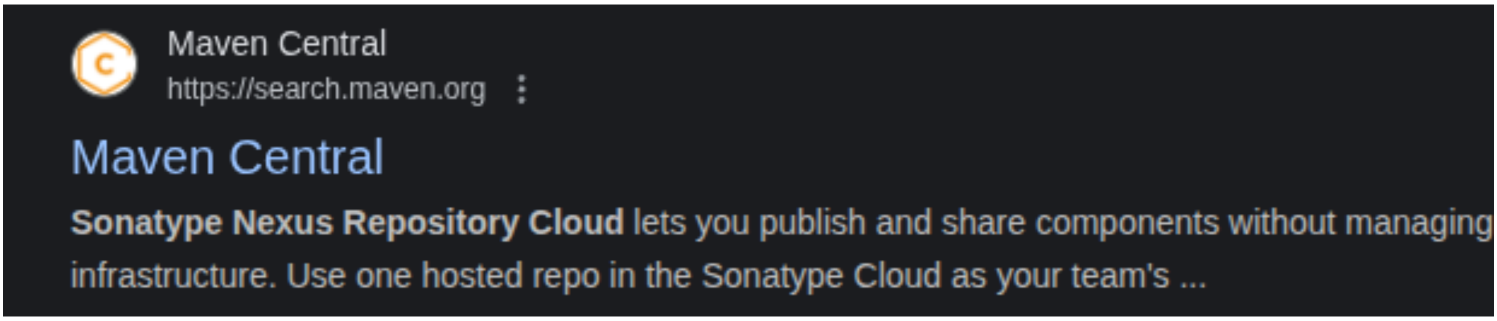
all IPv4 packets are related to 172[.]16[.]1[.]66 - I1

199[.]232[.]196[.]209 - E1 seems to be the external malicious IP
185[.]199[.]110[.]133 - E2
141[.]98[.]10[.]79 - E3

2. investigate E1
TLS packet shows SNI to be repo1[.]maven[.]org



no results on VT



Maven Central
https://search.maven.org

Maven Central

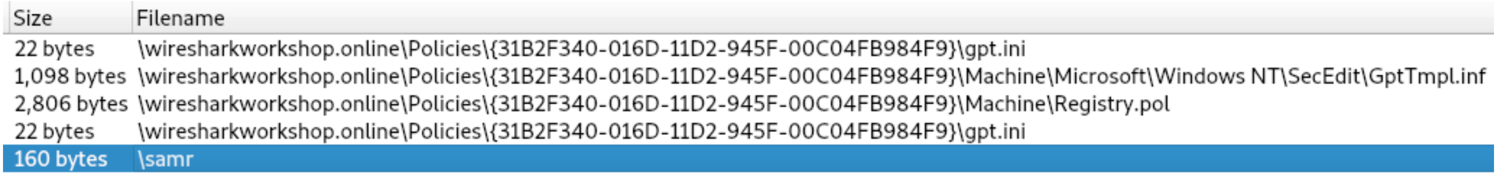
Sonatype Nexus Repository Cloud lets you publish and share components without managing infrastructure. Use one hosted repo in the Sonatype Cloud as your team's ...

seems to be some repository for code

3. investigate E2
SNI is objects[.]githubusercontent[.]com

4. investigate connections to I2
a lot of traffic between I1 and I2 before and after traffic with E1 and E2

5. investigate smb traffic

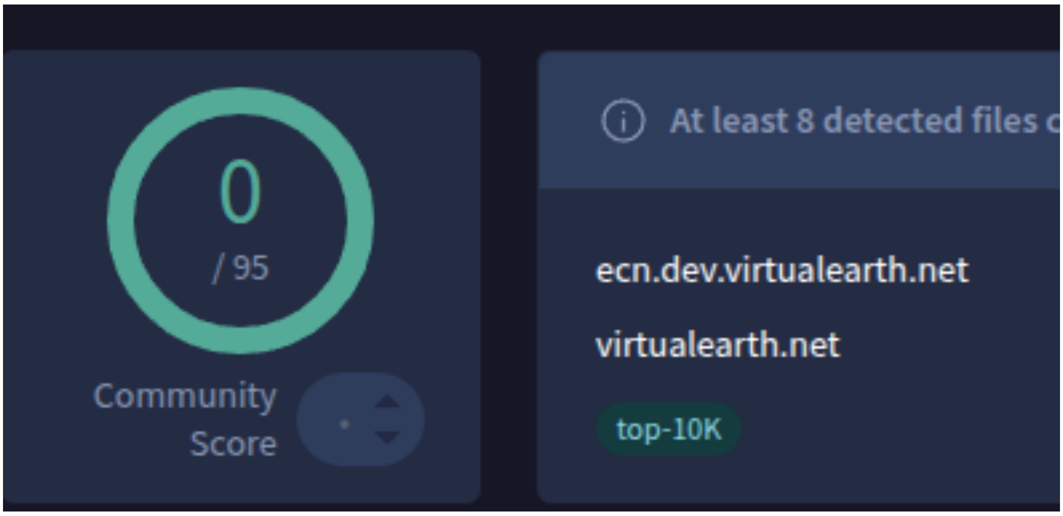


Size	Filename
22 bytes	\wiresharkworkshop.online\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
1,098 bytes	\wiresharkworkshop.online\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
2,806 bytes	\wiresharkworkshop.online\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Registry.pol
22 bytes	\wiresharkworkshop.online\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
160 bytes	\samr

can't find anything suspicious

6. investigate dns traffic
request for ecn[.]dev[.]virtualearth[.]net => ip: 23[.]46[.]192[.]165 - E4

7. investigate E4



At least 8 detected files c

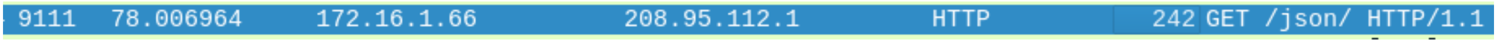
ecn.dev.virtualearth.net

virtualearth.net

top-10K

traffic is encrypted so I can't see

8. investigate http traffic



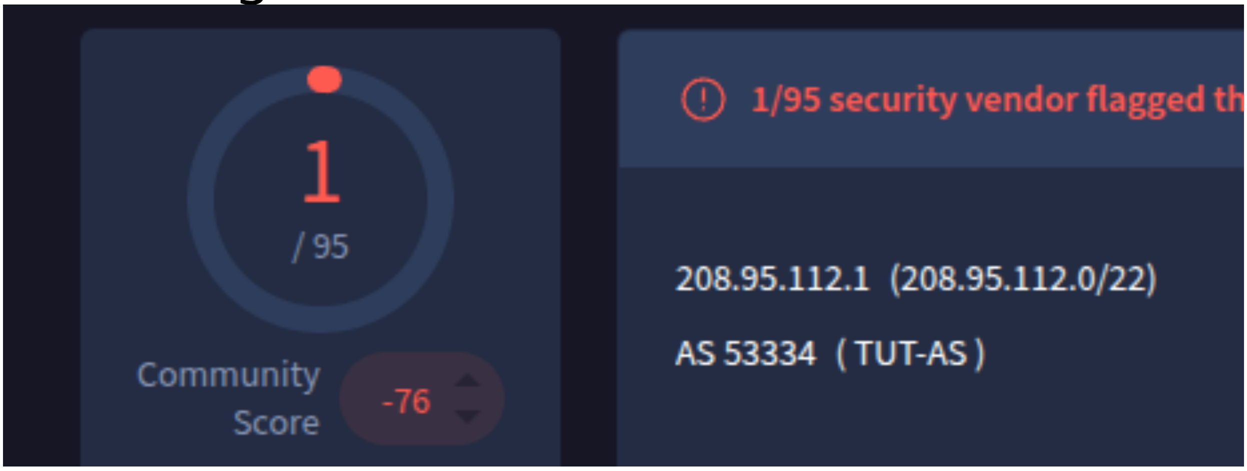
```
9111   78.006964      172.16.1.66           208.95.112.1         HTTP          242 GET /json/ HTTP/1.1
```

I1 requests json file from 208[.]95[.]112[.]1 - E5

{"status":"success","country":"United States","countryCode":"US","region":"TX","regionName":"Texas","city":"Austin","zip":"78752","lat"[:]30[.]2095,"lon":-97[.]7972,"timezone":"America/Chicago","isp":"Google Fiber, Inc[.]","org":"Google Fiber","as":"AS16591 Google Fiber, Inc[.]","query":"136[.]49[.]34[.]127"}

reply from contains an IP: 136[.]49[.]34[.]127 - E6

9. investigate E5

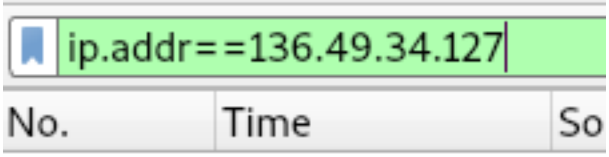


1/95 security vendor flagged th

208.95.112.1 (208.95.112.0/22)

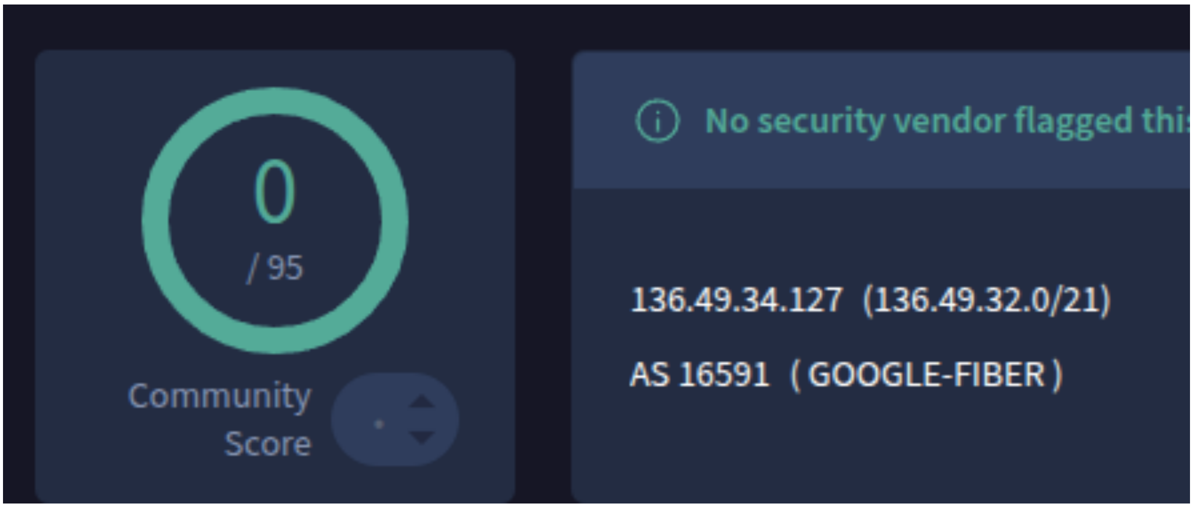
AS 53334 (TUT-AS)

10. investigate E6



ip.addr==136.49.34.127

no traffic with E6



No security vendor flagged thi

136.49.34.127 (136.49.32.0/21)

AS 16591 (GOOGLE-FIBER)