APT 40 in Malaysia

medium.com/@Sebdraven/apt-40-in-malaysia-61ed9c9642e9

Sebdraven February 7, 2020

Sebdraven

Feb 7, 2020

.

1 min read

The cert of Malaysia made an advisory the 5th february.

It's published many TTPs and IOCs on this group:

Advisories

MyCERT observed an increase in number of artifacts and victims involving a campaign against Malaysian Government…

www.mycert.org.my

There is many links interessisting:

the first are this IP 195.12.50.168 and 167.99.72.82. In my yeti, I found many relative observables on it:

hxxp://195.12.50.168/D2_de2o@sp0/ and hxxp://167.99.72.82/main.dotm

this Urls were used by a campaign discovered by ClearSky

targeting Malaysia. The victimology is interesting because it's concerning transport industry.

Another link interesting with this advisories is the link wit another campaign in November

https://app.any.run/tasks/ed03d492-688e-4182-9a06-6f65d8cb18fc/

found by

Malware used here is Dadjoke.

APT40 is an active Chinese group in South Asia, near of the MSS (Intelligence Service of China) according Intrusion Truth https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/

--

More from Sebdraven

Malwarist,Threat Huntist and pythonist / core dev of #yeti/ member of @ProjectHoneynet / co-organizer #BotConf / researcher