

APT 40 in Malaysia

By Sebdraven

Published: 2020-02-07 · Archived: 2026-04-05 15:39:06 UTC



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

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

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:

Press enter or click to view image in full size

Value	Tags	Context	Creation date
http://195.12.50.168/D2_de2o@sp0/ (167.99.72.82 (2 context) - hostname)	network_activity reported url	malware	2019-11-29 06:44
http://167.99.72.82/main.dotm (167.99.72.82 (2 context) - hostname)	network_activity reported url	malware	2019-11-29 06:44

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

Get Sebdraven's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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/>

Source: <https://medium.com/@Sebdraven/apt-40-in-malaysia-61ed9c9642e9>