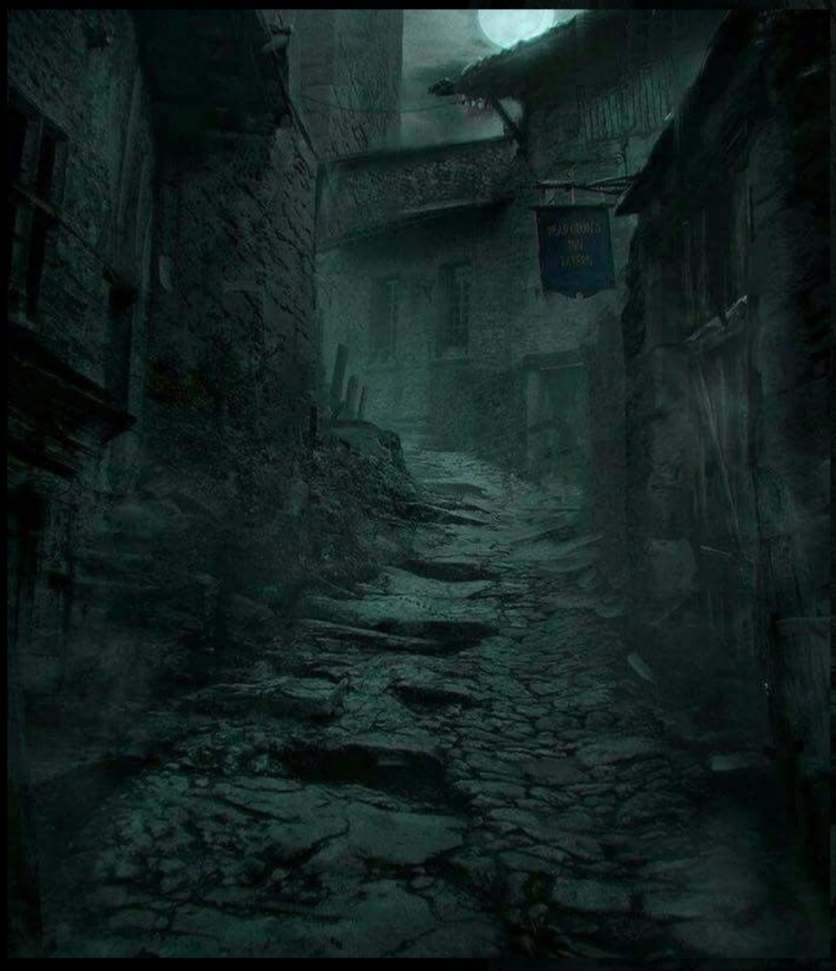
ITG18



AXIAL

ITG18

IRAN

USA

-

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON ITG18 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

IG18 is a threat group based out of Iran whose main motivation are Information theft and espionage.

II. TARGETS

The target/s of this threat group mainly focuses on Defense, Government, Pharmaceutical based out of the USA.

.

III. METHODS USED

The exact methods used by this threat group has not been uncovered yet but according to the operations performed by IBM X-Force IRIS lead to uncover of the information that, they used phishing techniques and many other information theft techniques.

IV. CAMPAIGNS

This threat group has been linked to campaigns related to compromise of multiple accounts of its targets hosted on its domains uncovered by IBM X Force.

ATTRIBUTION

This threat group is attributed to be based out of Iran and it's TTPs are overlapping with the other threat actors/groups based out of Iran.
[Cited from ThaiCERT]

AX1AL

V. IOCS

IOCs are currently not updates, if found will be updated soon.

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=ITG18