



FXMSP



FXMSP

 KAZAKHSTAN

 Around the globe

 RDP AND EXPOSED AD



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

- NERDS OF AXIAL

I. INTRODUCTION

FXMSP also known as ATK-317 is a threat group based out of Kazakhstan whose main motive is financial gain.

This threat group has been linked to campaigns related to breaches of three major anti-virus companies, on July 2020 this threat group has been linked to million-dollar hacking operation.

IV. CAMPAIGNS

II. TARGETS

The target/s of this threat group mainly focuses on Aviation, Education, Energy, Financial, Food and Agriculture, Government, Manufacturing, Retail, Transportation around multiple countries.

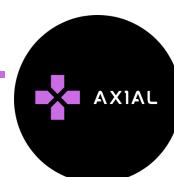
ATTRIBUTION

This threat group is attributed to be based out of Kazakhstan, but according to advanced intel the heads of this group belong from Moscow.

III. METHODS USED

[Cited from Advanced Intel and ThaiCERT]

The actor claimed to have developed a credential-stealing botnet capable of infecting high-profile targets in order to exfiltrate sensitive usernames and passwords. Fxmsp has claimed that developing this botnet and improving its capabilities for stealing information from secured systems is their main goal.



V. IOCS

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

VI. REFERENCES

<https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Fxmsp>

