


GCHQ

 AXIAL



GCHQ



UK



BELGIUM, UK



REGIN



 AXIAL

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

-NERDS OF AXIAL

I. INTRODUCTION

GCHQ is a threat group based out of the United Kingdom and is a state sponsored threat group focuses on information theft and espionage.

This threat group has been linked to various campaigns which includes intercepting foreign communications at G20 summits and operation socialist which includes breach of the infrastructure of the Belgian telecommunications company Belgacom.

IV. CAMPAIGNS

II. TARGETS

The target/s of this threat group mainly focuses on Belgium and UK mainly on government and telecommunications.

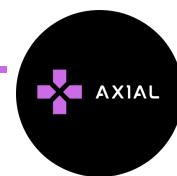
ATTRIBUTION

This threat group is attributed to be based out of United Kingdom.

[Cited from ThaiCERT]

III. METHODS USED

The methods used by this group is Regin a malware which has the capability which falls into the category of backdoor, and info stealers



V. IOCS

MD5 Hashes

06665b96e293b23acc80451abb413e50
187044596bc1328efa0ed636d8aa4a5c
1c024e599ac055312a4ab75b3950040a
2c8b9d2885543d7ade3cae98225e263b
4b6b86c7fec1c574706cecedf44abded
6662c390b2bbbd291ec7987388fc75d7
b269894f434657db2b15949641a67532
b29ca4f22ae7b7b25f79c1d4a421139d
b505d65721bb2453d5039a389113b566
26297dc3cd0b688de3b846983c5385e5
ba7bb65634ce1e30c1e5415be3d1db1d
bfbe8c3ee78750c3a520480700e440f8
d240f06e98c8d3e647cbf4d442d79475
ffb0b9b5b610191051a7bdf0806e1e47

VI. REFERENCES

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

<https://us-cert.cisa.gov/ncas/alerts/TA14-329A>

