SNOW GLOBE

AXIAL

SNOW GLOBE

FRANCE

ALGERIA, AUSTRIA, CHINA
CONGO, COTE D'IVOIRE,IRAN, IRAQ, ISRAEL,

BABAR, CASPER,
DINO, EVILBUNNY

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SNOW GLOBE ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Snow Globe is a threat group based out of France which focuses on information theft and is a state sponsored threat group.

II. TARGETS

The target/s of this threat group mainly focuses on Defense, Government, Media and private sectors onto multiple countries.

III. METHODS USED

The exact methods used by this threat group include usage of tools like Babar, Casper, Dino, EvilBunny, Tafacalou, Nbot, Chocopop. which include RATs and spying malwares.

IV. CAMPAIGNS

This threat group has been linked to SNOWGLOBE campaign, also multiple campaigns involving espionage around various parts of the globe.

ATTRIBUTION

This threat group is attributed to be based out of France and is potentially nation-state driven spyware occurred in March 2014. SNOWGLOBE to be a state-sponsored CNO [Cyber Network Operation] effort, put forth by a French intelligence agency." The information given dates back to 2011 and nothing else has been published since. Now that specific Babar samples have been identified and analyzed, there might be new information, also with regards to similarities or differences between the two Remote Administration Tools (RATs) EvilBunny and Babar. [Cited from GData]

AX1AL

V. IOCS

EvilBunny-Samples (SHA256)
c6a182f410b4cda0665cd792f00177c56338018fbc31bb34e41b72f8195c20cc
7d1e5c4afb1682087d86e793b3fc5a8371dc7c28e27e7196e3b258934f6bafb5
7bfc135194d3e5b85cbe46ed1c6f5e21dbe8f62c0a3ef56245b2d6500fc3a618
be14d781b85125a6074724964622ab05f89f41e6bacbda398bc7709d1d98a2ef

Babar-Samples (SHA256, Dropper and Payload)
c72a055b677cd9e5e2b2dcbba520425d023d906e6ee609b79c643d9034938ebf: Dropper
82e6f9c10c7ba737f8c79deae4132b9ff82090ccd220eb3d3739365b5276c3c8: Dropper

aa73634ca325022dd6daff2df30484ec9031939044cf4c2a004cbdb66108281d: Payload (perf_585.dll)
57437a675cae8e71ac33cd2e001ca7ef1b206b028f3c810e884223a0369d2f8a: Payload: (dump21cb.dll)

VI. REFRENCES

https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope