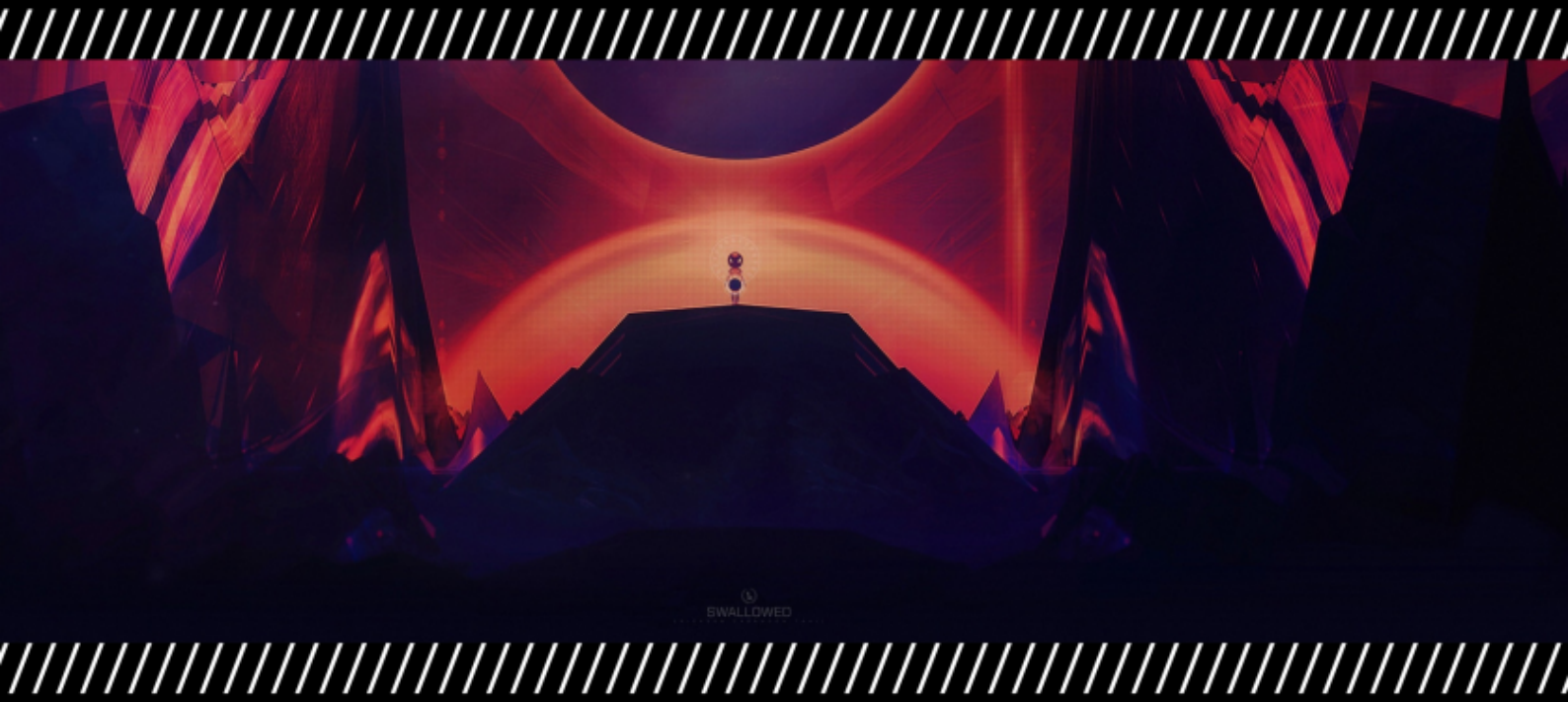
SOFT CELL

AXIAL



SOFT CELL

CHINA

TECH , EDUCATION
MANUFACTURING

WEB SHELL

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SOFT CELL ABOUT , WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Soft Cell is a threat group which is attributed to China and is likely state-sponsored.

II. TARGETS

The targets of this threat group has been focused onto tech, education and manufacturing and telecommunications networks.

III. METHODS USED

SoftCell has been using WinRAR to compress and enctypt stolen data prior to exfiltration.
SoftCell used Powershell for execution to assist in lateral movement as well as for dumping credentials stored on compromised machines.
SoftCell used Web Shells and HTRAN for C2 as well as to exfiltrate data.
SoftCell established DLL side -loading to covertly load Poisonlvy into memory on the victim machine.
SoftCell used softwares like China Chopper and PlugX.

IV. CAMPAIGNS

This threat group has been involved in targeting global telecommunications providers or Operation Soft Cell over worldwide .

ATTRIBUTION

This threat group is attributed to China and probably is a stat sponsored also has been attributed to other Chinese affiliated groups like APT-10 .

[cited from Cyberason]

AX1AL

V. IOCS

To be added

VI. REFRENCES

https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

https://attack.mitre.org/groups/G0093/