SOWBUG

AXIAL

SOWBUG

SOUTH AMERICA
SOUTHEAST ASIA

CUSTOM
MALWARE

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Sowbug is a threat group which has been focusing on information theft and espionage.

II. TARGETS

The targets of this threat group has been focused onto South America and South East Asia and have targeted foreign policy institutions and it's diplomatic targets.

III. METHODS USED

Sowbug has been using tools like Backdoor.Felimus & Trojan.Starloader
.

IV. CAMPAIGNS

This threat group has been involved in infiltrating organization in South East Asia in September 2016.
This threat group has also been seen targeting multiple government entities across U.S., Europe and Asia also some parts of South America.

ATTRIBUTION

This threat group is not attributed to any nation rather it has been found attacking government entities across the globe. The attributions is received will be updated onto this report .

V. IOCS

514f85ebb05cad9e004eee89dde2ed07
Backdoor.Felismus

00d356a7cf9f67dd5bb8b2a88e289bc8
Backdoor.Felismus

c1f65ddabcc1f23d9ba1600789eb581b
Backdoor.Felismus

967d60c417d70a02030938a2ee8a0b74
Backdoor.Felismus

Trojan.Starloader samples

MD5
Detection
4984e9e1a5d595c079cc490a22d67490
Trojan.Starloader

Hacktools

MD5
Detection
e4e1c98feac9356dbfcac1d8c362ab22
Hacktool.Mimikatz

VI. REFRENCES

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=d544bd14-1dd2-4ab6-a5a0-181788b7d73b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

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