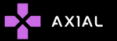


SEA TURTLE



SEA TURTLE



TURKEY



ALBANIA, ARMENIA,
CYPRUS, EGYPT,
GREECE, IRAQ,
JORDAN, LEBANON,
LIBYA



DRUPALGEDDON
AND DNS
HIJACKING



A SURVEY ON SEA TURTLE ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

- NERDS OF AXIAL

I. INTRODUCTION

Sea Turtle is a threat group based out of Turkey and is more likely not to be a state sponsored threat group.

This threat group has been linked to DNS hijacking techniques, and on April 2019 Institute of Computer Science breach has also been linked to Sea Turtle threat group.

IV. CAMPAIGNS

II. TARGETS

The target/s of this threat group mainly focuses on Aerospace, Defense, Energy, Government, NGOs, Think Tanks and Intelligence agencies onto countries like Cyprus, Syria, USA, UAE and multiple countries.

ATTRIBUTION

This threat group is attributed to be based out of Turkey

[Cited from ThaiCERT]

III. METHODS USED

The methods used by this group are Drupalgeddon and DNS hijacking .This new technique is similar in that the threat actors compromise the name server records and respond to DNS requests with falsified A records. This new technique has only been observed in a few highly targeted operations. This threat group has been actively using exploits of type 0-day of which the mainly affected was Drupal.



V. IOCS

| Hostnames | IP addresses | Operational Status |
|---------------------------|----------------------|--------------------|
| ns1[.]rootdnserver[.]com. | 45[.]32[.]100[.]62 | Active |
| ns2[.]rootdnserver[.]com. | 45[.]32[.]100[.]62 | Active |
| ns1[.]intersecdns[.]com | 95[.]179[.]150[.]101 | Inactive |
| ns2[.]intersecdns[.]com | 95[.]179[.]150[.]101 | Inactive |

| Date | IP address |
|----------------|----------------------|
| April 13, 2019 | 95[.]179[.]131[.]225 |
| April 16, 2019 | 95[.]179[.]131[.]225 |
| April 11, 2019 | 95[.]179[.]131[.]225 |
| April 11, 2019 | 140[.]82[.]58[.]253 |
| April 10, 2019 | 95[.]179[.]156[.]61 |

Cited from CISCO Talos

VI. REFERENCES

<https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html>

<https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Sea%20Turtle>