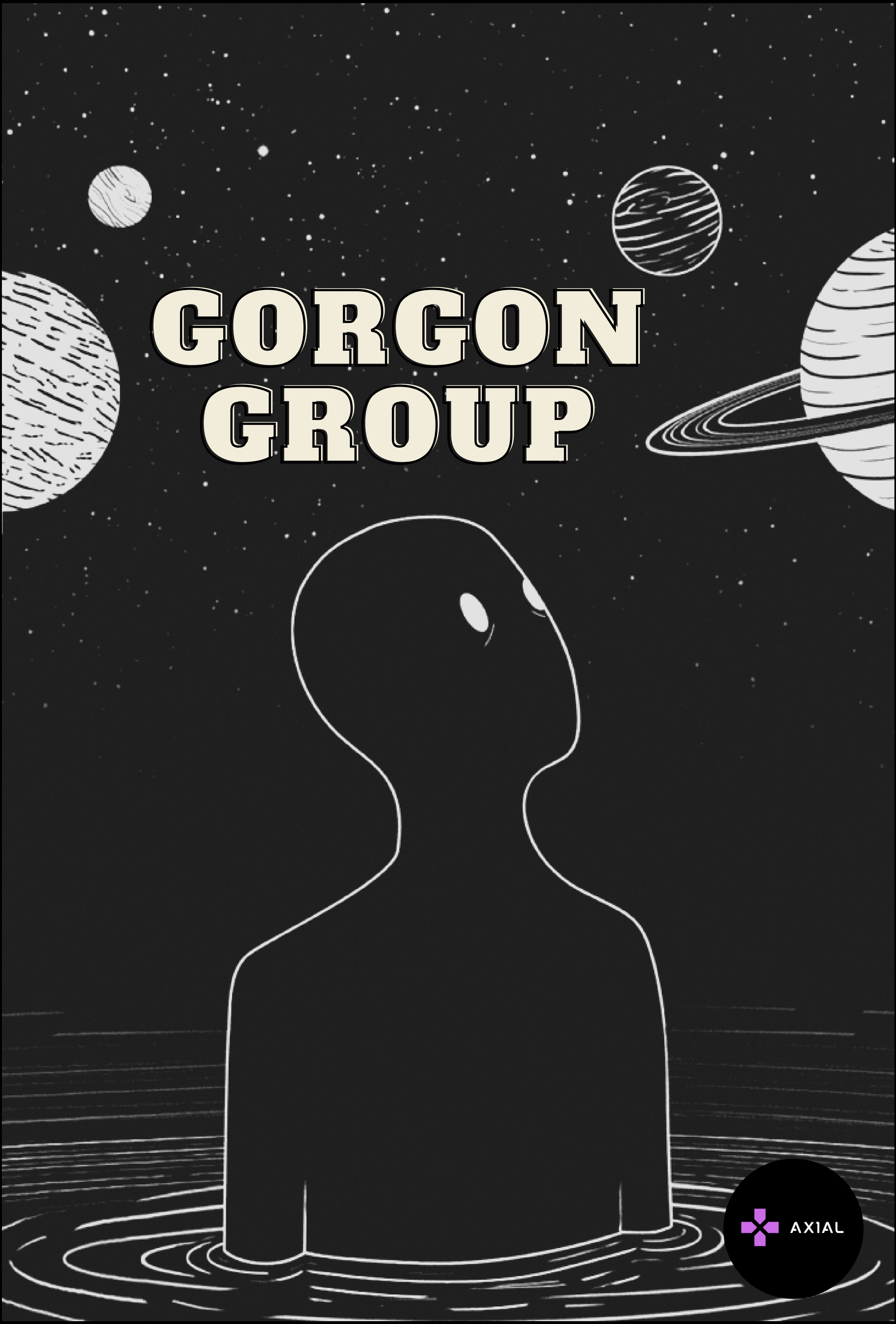
GORGON GROUP



AXIAL

A SURVEY ON GORGON GROUP: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Gorgon Group also known as Subaat, ATK 92, TAG-CR5 is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States.

II. TARGET SECTORS

Governmental organizations.

III. ENGAGEMENTS

- Jul 2017, a small wave of phishing emails targeting a US-based government organization. Within the 43 emails we observed, we found that three unique files were delivered, which consisted of two RTFs and a Microsoft Excel file. Both RTFs exploited CVE-2012-0158 and acted as downloaders to ultimately deliver the QuasarRAT malware family. The downloaders made use of the same shellcode, with minor variances witnessed between them. Additionally, the RTFs made use of heavy obfuscation within the documents themselves, making it more difficult to extract the embedded shellcode.
- Feb 2018In addition to the numerous targeted attacks, Unit 42 discovered that the group also performed a litany of attacks and operations around the globe, involving both criminals as well as targeted attacks. Starting in February 2018, Palo Alto Networks Unit 42 identified a campaign of attacks performed by members of Gorgon Group targeting governmental organizations in the United Kingdom, Spain, Russia, and the United States. Additionally, during that time, members of the Gorgon Group were also performing criminal operations against targets across the globe, often using shared infrastructure with their targeted attack operations.
- Apr 2020, Gorgon APT targeting MSME sector in India.
- Jul 2020, Advance Campaign Targeting Manufacturing and Export Sectors in India.

IV. METHODS USED

Generally, they do phishing attacks and the phishing attempts are kept very simple and lightweight by using OLE2Link objects that will usually make use of URL shortening services such as Bitly and t2m[.]io.

V. COMMON ATTRIBUTIONS

- Microsoft Office attachments delivered via spearphishing emails that contain a macro.
- The delivery document contains a macro that downloads an executable from a remote server.
- Attempt to disable security features in Microsoft Office and Windows Defender using the taskkill command.

VI. IOC

Domains

1. **t2m.io**
2. **acorn-paper.com**
3. **xyz-storez.xyz**
4. **securebotnetpanel.tk**
5. **diamondfoxpanel.ml**

Hashes

1. **c8f457649a33e2c828a70bef48546c7d7a33619dd16ac50207dc744fa4a72260**
2. **137e72e83b4cd50bb880378eb1cd5bfd2e6a6b1c42da9dbb49595a23b5f7a56d**
3. **907d3ce8d28a602ce9cdfbb5d1ffb73ed4addbfffb6c8ad66881ee96b8627888**
4. **8cdbebdd4f05304622623273903ebca5849515ba31a5be499f117eae08671200**
5. **71ea8894d4656933a13476da57b1c31e1192fb8bb7d487a8260a09344b6ed553**

VII. REFERENCES

- https://attack.mitre.org/groups/G0078/
- https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state
- https://malpedia.caad.fkie.fraunhofer.de/actor/the_gorgon_group
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Gorgon%20Group&n=1