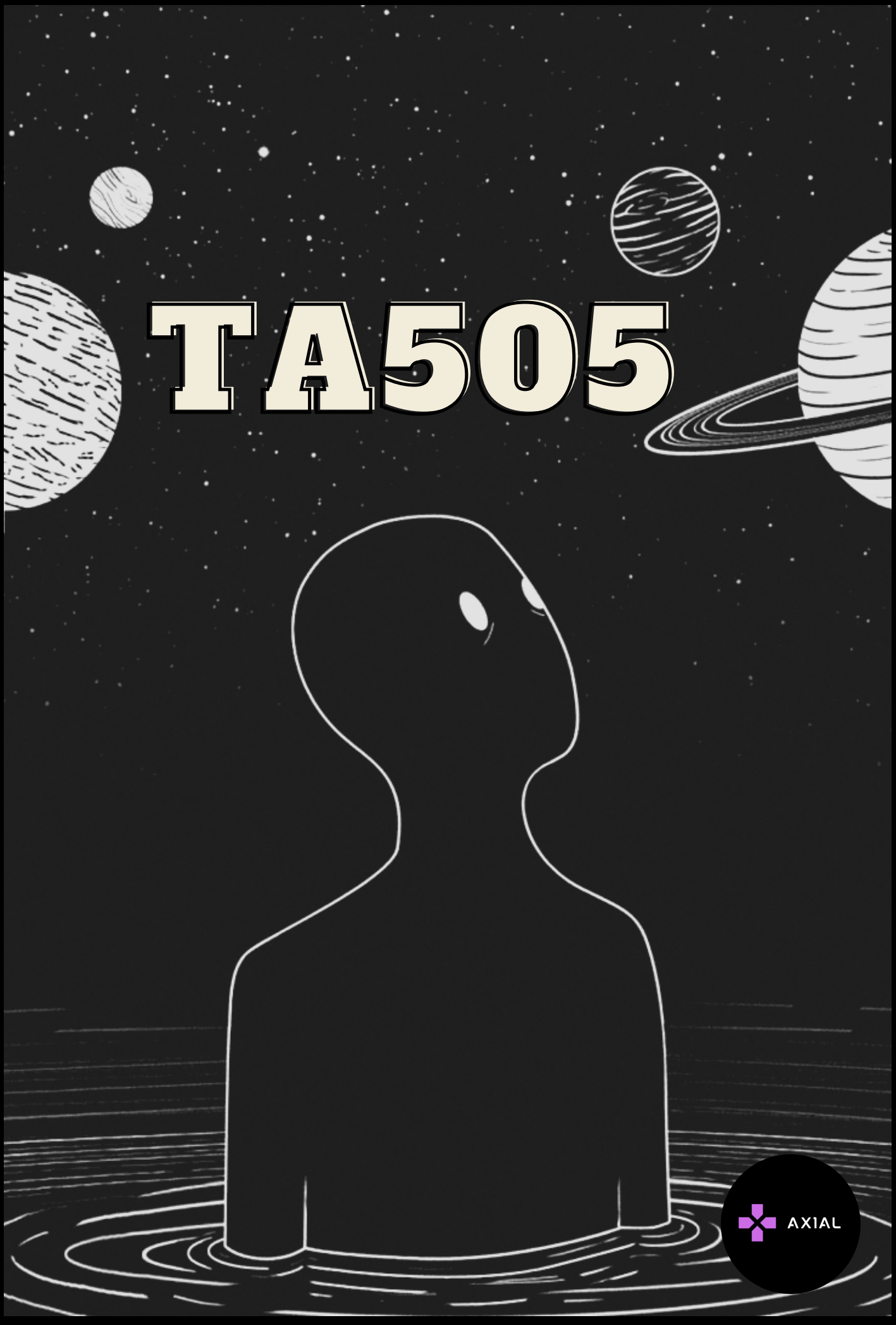
TA505
AXIAL

A SURVEY ON TA505: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

TA505 also known as Hive0065, SectorJ04 Group, GRACEFUL SPIDER, GOLD TAHOE is a financially motivated threat group that has been active since at least 2014. The group is known for frequently changing malware and driving global trends in criminal malware distribution. They use malicious email campaigns to distribute various banking trojans, ransomware, RATs, and backdoors.

II. ENGAGEMENTS

- Oct 2017, On October 10, TA505 introduced their first geo-targeted campaign dropping either Locky or The Trick banking Trojan. In this campaign, HTML files were attached to emails inquiring about the status of an invoice.
- Jun 2018, We first observed an actor embedding SettingContent-ms inside a PDF on June 18. However, on July 16 we observed a particularly large campaign with hundreds of thousands of messages attempting to deliver PDF attachments with an embedded SettingContent-ms file.
- Nov 2018, Since November 15, 2018, Proofpoint began observing email campaigns from a specific actor targeting large retail chains, restaurant chains, and grocery chains, as well as other organizations in the food and beverage industries.
- Nov 2018, ServHelper and FlawedGrace – New malware introduced by TA505.
- Dec 2018, In mid-December 2018 a spear-phishing campaign was detected as targeting large US-based retailers along with organizations in the food and beverage industry. Masquerading as a legitimate communication sent from a Ricoh printer, the initial email lured victims into opening an attached malicious Microsoft Word document.
- Dec 2018, 360 Threat Intelligence Center captured multiple phishing emails sent by TA505 Group to target financial institutions. These phishing emails contain Excel attachments with Excel 4.0 Macro embedded and download Backdoor at last.
- Apr 2019, LOLBins and a New Backdoor Malware.
- May 2019, Yoroi CERT noticed a suspicious attack against an Italian organization. The malicious email contains a highly suspicious sample which triggered the ZLAB team to investigate its capabilities and its possible attribution, discovering a potential expansion of the TA505 operation.
- 2019, In this newly discovered campaign from TA505, threat actors targeted German companies with trojanized emails disguised as job applicants. While this activity appeared to be geographically based in Germany, these same techniques could easily be applied to any organization. Once the email attachment was activated, a company's security credentials and credit card data could be transmitted covertly to the threat actors. In the 2019 iterations of this attack, TA505 used commercial tools to encrypt all the user's files, which suggests this recent activity could also lay the groundwork for an infection vector into the company's network to encrypt files.
- Jan 2020, Microsoft says that an ongoing TA505 phishing campaign is using attachments featuring HTML redirectors for delivering malicious Excel documents, this being the first time the threat actors have been seen adopting this technique.
- Apr 2020, TA505 Continues to Infect Networks With SDBbot RAT
- Jun 2020, To evade detection, hackers are requiring targets to complete CAPTCHAs
- Oct 2020, Microsoft is warning that cybercriminals have started to incorporate exploit code for the ZeroLogon vulnerability in their attacks.

AX1AL

III. TARGET SECTORS

Their main targets are Education, Financial, Healthcare, Hospitality, Retail.

IV. METHODS USED

This group uses malicious email campaigns to distribute various banking trojans, ransomware, RATs, and backdoors.

V. ATTRIBUTIONS

- The attack group, which is believed to be based in Russia, has been implicated in large-scale spam campaigns and has distributed Trojans such as Dridex and The Trick as well as Locky and Jaff ransomware, according to Proofpoint, which published a detailed analysis of the group in 2017.

VI. IOC

C&C IP Addresses

1. **91[.]214[.]124[.]25**
2. **91[.]214[.]124[.]20**
3. **185[.]176[.]221[.]45**

&C Domains

1. **drm-server-booking[.]com**
2. **microsoft-live-us[.]com**
3. **dl1.sync-share[.]com**

VII. REFERENCES

- https://attack.mitre.org/groups/G0092/
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi g=TA505%2C%20Graceful%20Spider%2C%20Gold%20Evergreen
- https://malpedia.caad.fkie.fraunhofer.de/actor/ta505
- https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
- https://www.trendmicro.com/en_us/research/19/f/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns.html
- https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
- https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times
- https://threatpost.com/ta505-servhelper-malware/140792/
- https://www.bankinfosecurity.com/ta505-apt-group-returns-new-techniques-report-a-13678

AXIAL