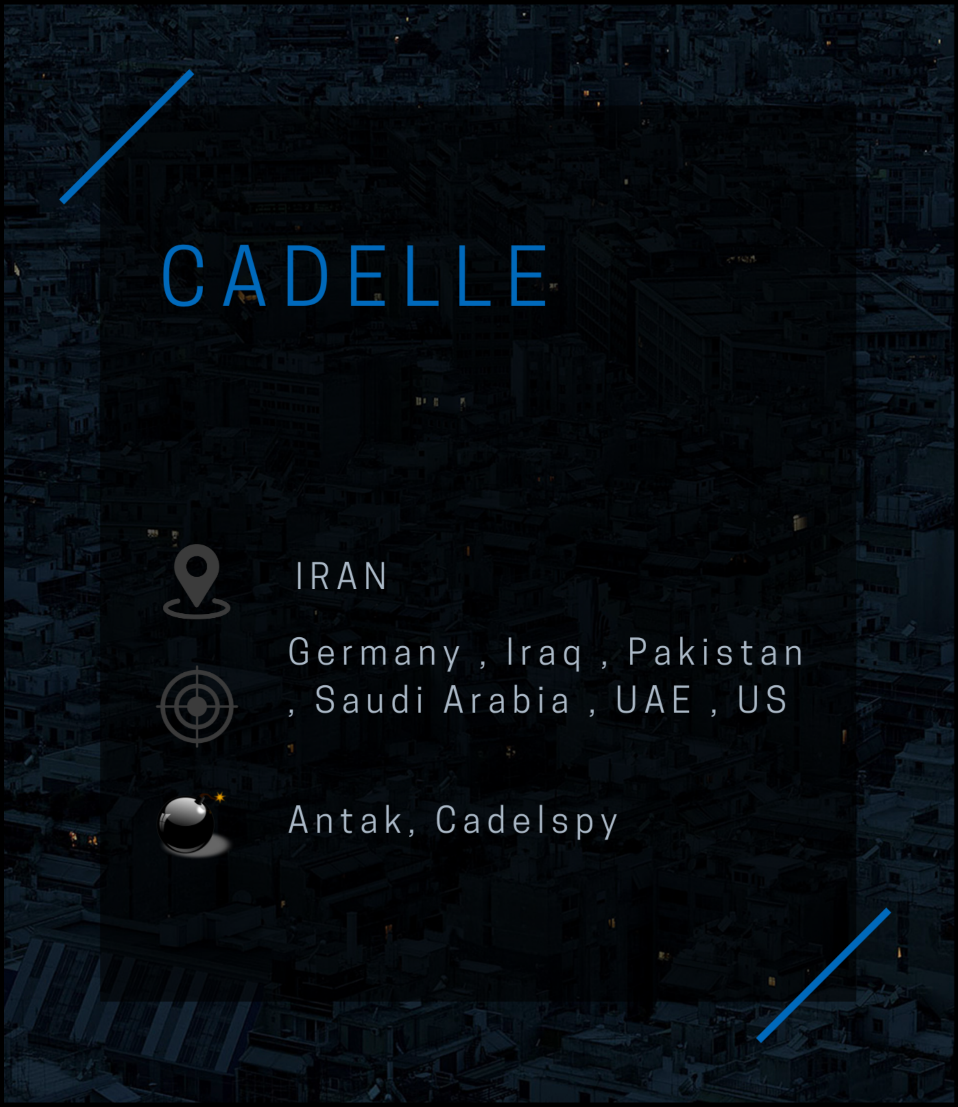
CADELLE

AXIAL



CADELLE

IRAN

Germany , Iraq , Pakistan , Saudi Arabia , UAE , US

Antak, Cadelspy

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT CADELLE ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Symantec telemetry identified Cadelle and Chafer, APT 39 activity dating from as far back as July 2014, however, it's likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.There is evidence to suggest that the two teams may be connected in some way, though we cannot confirm this. A number of computers experienced both Cadelspy and Remexi infections within a small time window. In one instance, a computer was compromised with Backdoor.Cadelspy just minutes after being infected with Backdoor.Remexi. The Cadelle and Chafer groups also keep the same working hours and focus on similar targets. However, no sharing of C&C infrastructure between the teams has been observed.If Cadelle and Chafer are not directly linked, then they may be separately working for a single entity. Their victim profile may be of interest to a nation state.

II. TARGETS

Germany, Iran, Iraq, Netherlands, Pakistan, Saudi Arabia, Singapore, Sudan, Tajikistan, Thailand, Turkey, UAE, UK, USA.

III. TOOLS USED

Antak, Cadelspy.

IV. ATTRIBUTION

There are a number of factors in these groups' campaigns that suggests that the attackers may be based in Iran. Cadelle and Chafer are most active during the day time within Iran's time zone and primarily operate during Iran's business week (Saturday through Thursday).

Additionally, Symantec observed that Backdoor.Cadelspy's file strings seem to include dates written in the Solar Hijri calendar, which is used in Iran and Afghanistan. While the Gregorian calendar marks the current year as 2015, the Solar Hijri calendar states that it is 1394. When we converted the dates in the file strings from the Solar Hijri calendar to the Gregorian one, we found that they were close to the compilation times of the executables and also close to when Cadelle's targets were initially compromised.

V. REFERENCES

1. https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets
2. https://securityaffairs.co/wordpress/42641/breaking-news/cadelle-and-chafer-iranian-hackers.html
3. https://securityboulevard.com/2020/01/iranian-apt-group-overview/
4. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=4eccc5e0-b5f3-44fe-bc5c-81eaf95f2118&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
5. https://malpedia.caad.fkie.fraunhofer.de/actor/apt39