SILENCE

AXIAL

SILENCE

RUSSIA

EUROPE, AFRICA
ASIA

SPEAR
PHISHING

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Group-IB experts discovered that Silence have significantly expanded their geography and increased the frequency of their attacks. Additionally, the total confirmed amount of funds stolen by Silence has increased fivefold since the publication of Group-IB's original report, and is now estimated at USD 4.2 million.

II.TARGETS

Countries:
Europe, Latin America, Africa, and Asia.

III. ATTRIBUTION

Group-IB researchers believe that there might also be a connection between Silence and TA505, another presumably Russian-speaking threat actor first named by researchers from Proofpoint.

IV. TOOLS USED

Notably, at the initial infection stage, in addition to their infamous primary loader Silence.Downloader (aka TrueBot), the cybercriminals started using Ivoke, a fileless loader, written in PowerShell.

V. METHODS USED

- Silence uses phishing emails to infect their victims. In October 2018, however, Silence implemented new tactics: the gang began sending out reconnaissance emails as part of a preparatory stage for their attacks. Silence's "recon" looks like a "mail delivery failed" message that usually contains a link without a malicious payload.

-Such "recon" emails allow cybercriminals to obtain a list of valid emails for future attacks and get information about the cybersecurity solutions used by a targeted company all the while remaining undetected.

- Another new tool in Silence's arsenal is a previously unknown PowerShell agent based on Empire and dnscat2 projects, dubbed EmpireDNSAgent.

- he Trojan is used during the lateral movement stage and is designed to control compromised systems by performing tasks through the command shell and tunneling traffic using the DNS protocol.

VI. IOCS

1. 2250174b8998a787332c198fc94db4615504d771
2. 1b8c71131891dc1c728349405409a687caeefdbc
3. d1dd819dc64c26913d2d9ec8dd4ad9c4e26512a9
4. d0dcfbeeb9f81af8bad758d5e255a412ad5a7004
5. 3A8E362F8183BC9D33320F03285CEEA07FD19250
6. 8D37648A1AD242F8EAB2016AAEE7A5B314757764
7. E4B7DBDAD70443C565673DC46D8EEA05DD5C2B69
8. d044bc7fb58792a6bf612116662df892a306a931
9. 4d0d5ecaea133dbcc603119a5271796bfe371036
10. f88d4e44d85ef3acc24c8b459c68915c76e792ed

C&C

1. 5.39.221[.]46
2. mobilecommerzbank[.]com
3. 5.39.218[.]205
4. 5.8.88[.]254
5. fpbank[.]ru
6. 91.243.80[.]200
7. itablex[.]com
8. 91.243.80[.]84
9. 146.0.72[.]188
10. 146.0.77[.]104

VII. REFERENCES

1. https://www.group-ib.com/media/silence-attacks/
2. https://www.darkreading.com/attacks-breaches/silence-apt-group-broadens-attacks-on-banks-gets-more-dangerous/d/d-id/1335596
3. https://www.computerweekly.com/news/252468853/Silence-APT-group-eyes-APAC-banks
4. https://thehackernews.com/2019/08/silence-apt-russian-hackers.html
5. https://www.securityweek.com/russian-apt-silence-steals-35-million-one-year
6. https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf
7. https://www.computing.co.uk/news/3080737/russia-hacking-silence-apt