STRIDER

AXIAL

STRIDER

USA

RUSSIA , CHINA , SWEDEN, BELGIUM IRAN,RWANDA

REMSEC BACKDOORS

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

The Strider crew has been active since at least 2011, its abilities and the type of targets lead the experts into believing that it is nation-state group. The Strider group uses a sophisticated strain of malware dubbed Remsec, that set up a backdoor in the infected host.
Strider is capable of creating custom malware tools and has operated below the radar for at least five years, Remsec is a stealthy tool that appears to be primarily designed for spying purposes.

II.TARGETS

Countries:
Russia, Belgium, China, Iran, Sweden, and Rwanda.

III. ATTRIBUTION

Based on the espionage capabilities of its malware and the nature of its known targets, it is possible that the group is a nation-state level attacker.

IV. TOOLS USED

Backdoor.Remsec

V. METHODS USED

- The group uses an advanced piece of malware known as Remsec (Backdoor.Remsec) to conduct its attacks. Remsec is a stealthy tool that appears to be primarily designed for spying purposes. Its code contains a reference to Sauron, the all-seeing antagonist in Lord of the Rings.

- Loader: Named MSAOSSPC.DLL, this module is responsible for loading files from disk and executing them. The files on disk contain the payload in an executable blob format. The loader also logs data. Executable blobs and data are encrypted and decrypted with a repeating key of 0xBAADF00D. The loader maintains persistence by being implemented as a fake Security Support Provider.

-Lua modules: Several examples of Remsec use modules written in the Lua programming language. Remsec uses a Lua interpreter to run Lua modules which perform various functions. These Lua modules are stored in the same executable blob format as the loader.

AX1AL

VI. IOCS

1. 46a676ab7f179e511e30dd2dc41bd388
2. 9f81f59bc58452127884ce513865ed20
3. e710f28d59aa529d6792ca6ff0ca1b34
4. 1F7DDB6752461615EBF0D76BDCC6AB1A
5. 227EA8F8281B75C5CD5F10370997D801
6. 2F704CB6C080024624FC3267F9FDF30E
7. 34284B62456995CA0001BC3BA6709A8A
8. 181c84e45abf1b03af0322f571848c2d
9. F3B9C454B799E2FE6F09B6170C81FF5C
10. 5D41719EB355FDF06277140DA14AF03E
11. 71EB97FF9BF70EA8BB1157D54608F8BB
12. 5DDD5294655E9EB3B9B2071DC2E503B1
13. 5DDD5294655E9EB3B9B2071DC2E503B1
14. 951EBE1EE17F61CD2398D8BC0E00B099

C&C

1. 185.78.64[.]121
2. rapidcomments[.]com
3. bikessport[.]com
4. 178.211.40[.]117
5. 176.9.242[.]188
6. flowershop22[.]110mb[.]com
7. wildhorses[.]awardspace[.]info
8. sx4-ws42*.yi[.]org_(mask)
9. 217.160.176[.]157
10. asrgd-uz%d.weedns[.]com (mask)

VII. REFERENCES

1. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
2. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190157/The-ProjectSauron-APT_IOCs_KL.pdf
3. https://securityaffairs.co/wordpress/50119/intelligence/projectsauron-apt-stride.html
4. https://securelist.com/faq-the-projectsauron-apt/75533/
5. https://informationsecuritybuzz.com/expert-comments/symantec-discovers-strider-new-cyberespionage-group/