
SHARPSHOOTER
AXIAL

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

-NERDS OF AX1AL

I. ABOUT

Operation Sharpshooter targeted nuclear, defence, energy and financial companies globally. This campaign leveraged an in-memory backdoor to download and retrieve a second-stage backdoor for further exploitation. According to McAfee Advanced Threat Research, the second-stage backdoor, dubbed Rising Sun used source code from Lazarus Group's 2015 Backdoor.Duuzer in a new framework.

II. TARGET SECTORS

Major targets were Defence and government related organizations.

III. METHODS USED

This campaign, while masquerading as legitimate industry job recruitment activity, gathers information to monitor for potential exploitation. It leverages an in-memory Backdoor to download and retrieve a second-stage Backdoor called Rising Sun for further exploitation. Also in this campaign's arsenal was extensive Social Engineering.

IV. ATTRIBUTION

McAfee researchers found similarities between the code of Backdoor.RisingSun and that of Backdoor.Duuzer, a previous cyber espionage backdoor that has been attributed to the Lazarus APT group. They also found indicators potentially pointing toward Lazarus. However, they make no determination of attribution, as they state it is also potentially an attempted false flag operation aimed at placing the blame on Lazarus.

AX1AL

V. OPERATIONS

- According to McAfee's Report, in October 2018 the Rising Sun backdoor had appeared in 87 organizations across the globe. Lazarus Group used recruiting as a lure to collect information about targeted individuals of interest and organizations that manage data related to the industries of interest.
- Targeted Users would be sent a link to a dropbox that contained the weaponized document. Once the user enables content, the malware executes a shellcode through macros, which would then download a decoy document and Rising Sun backdoor from their C2 server. The Backdoor gave them user information as well as allowed them to Encrypt and Exfiltrate the data off the user's system.
- Backdoor had the capabilities of Executing commands, Launching processes as well as getting info and termination, Read, Write, and execute files as well as delete them.
- It was later noted that the Campaign was more widespread than previously evaluated. Newer C2 servers were found and the campaign had begun as early as Sept. 2017, in which they had targeted a broader set of organizations in more industries and countries.

IV. IOC

MD5

- 8106a30bd35526bded384627d8eebce15da35d17
- 66776c50bcc79bbcecdbe99960e6ee39c8a31181
- 668b0df94c6d12ae86711ce24ce79dbe0ee2d463
- 9b0f22e129c73ce4c21be4122182f6dcbc351c95
- 31e79093d452426247a56ca0eff860b0ecc86009

C2

1. 34.214.99.20/view_style.php
2. 137.74.41.56/board.php
3. kingkoil.com.sg/board.php

DOCUMENT URLS

1. hxxp://208.117.44.112/document/Strategic Planning Manager.doc
2. hxxp://208.117.44.112/document/Business Intelligence Administrator.doc
3. hxxp://www.dropbox.com/s/2shp23ogs113hnd/Customer Service Representative.doc?dl=1

VIII. REFERENCES

- https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf
- https://threatpost.com/sharpshooter-complexity-scope/142359/

AXIAL