Government of India
National Critical Information Infrastructure Protection Centre
(A Unit of NTRO)

Date: 22 Nov 2019

Cyber Security Advisory: **Ransom.Win32.GOSPORT.C(DNP)**

This data is to be considered as **TLP:AMBER**

A ransomware has been observed which arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. It encrypts files which can be found on the following drives: Fixed Drives, Removable Drives, Network Drives. This Ransomware avoids encrypting files found in the following folders : windows , microsoft , trend , office , google ,netlogon, sysvol. It appends .hdmr extension to the file name of the encrypted files. It avoids encrypting files with the following file extensions: .hdmr, .exe, .dll, .sys, .vxd, .ini, .lnk, .msi, .cab.

Analyst's Notes:
It drops the following file(s) as ransom note: {all encrypted path}\ReadMeAndContact.txt.

MD5: 9370aae3f440fcb951aff17a27ddef70
SHA1: b753e87fabd097e287a5380d480f5076fe208561

IOCs:

Hashes
36bb5c74854f7353b5b0532927f9b4cf6f53240c - Ransom.Win32.GOSPORT.A
5173a6b453cf1ef902274dfc41caecb291edac4a - Ransom.Win32.GOSPORT.B
1d6d827ac3bfe555d1885ae8b641db69b030dc9c - Ransom.Win32.GOSPORT.B

CnC
239.255.255.250

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430