कर्मचारी भविष्य निधि संगठन
EMPLOYEES' PROVIDENT FUND ORGANISATION
(श्रम एवं रोजगार **मंत्रालय**, भारत सरकार)
(MINISTRY OF LABOUR & EMPLOYMENT, GOVT. OF INDIA)
राष्ट्रीय **डाटा केंद्र** /NATIONAL DATA CENTRE
1ST Floor, Bhavishya Nidhi Bhawan, Plot No.23, Sector-23, Dwarka,New Delhi-110075
www.epfindia.gov.in

सत्यमेव जयते

CISO/Security/2022/ 1184 Date: 18.05.2022

CYBER SECURITY ADVISORY No 2022/02 : DATA WIPER MALWARE

1. A surge in use of data wiper malware by nation sponsored threat actors is being reported. The Primary motive of the attacker for using these malware is the destruction of the victim machine/ data. A brief overview of different data wiper active in cyber landscape is provided below:-

(a) **AwfulShred**: AwfulShred is data-wiping bash script targeting LINUX based system.

(b) **DoubleZero**: Doublezero is a data wiper attributed as a .NET-based implant, which destroys files, registry keys, and trees on the Victim Windows machine. It aims to overwrite all files in all drives by destroying all files in all drives except for a specific list of the locations hardcoded in the wiper. It wipe files either by overwriting their content with zero blocks of 4096 bytes or using API-calls.

(c) **CaddyWiper**: CaddyWiper is wiper malware targeting non primary domain controller window machines. Upon execution, malware overwrites each file with zero to ensure that data is destroyed and not recoverable.

(d) **ACIDRAIN**: AcidRain is wiper malware target modems and routers used for internet access. AcidRain performs an initial recursive overwrite and delete non-standard files in the filesystem.

(e) **DesertBlade**: DesertBlade malware is deployed via Active directory Group Policy Object [GPO] indicating that attacker has first gained control of the Active directory for the network. It overwrites files on victim machine and then deletes them.

2. **Recommendations**: As Data wiper malware wipes the victim machine data, having proper periodic backups of all critical information and data would limit the impact of data or system loss and help in expediting the recovery process. It is also advised that data backup should be kept on a separate device and in offline mode.

3. For information and necessary action please.

(Rahul Modgil)
Chief Information Security Officer

To,

1. Website Admin
2. Field Office Application Admin
3. Network Admin
4. Storage Admin
5. OS Admin
6. Active Directory (AD) Admin
7. Database Admin
8. Team Leader, RailTel Team

Copy to:

1. OSD to CPFC
2. Sh. Radha Krishan Singh, ACC HQ (IS)
3. FA & CAO, CVO
4. Sh. Pankaj Raman, ACC (IS)
5. Director, PDUNASS
6. CTO
7. ALL RPFCs Incharge of Regional Offices & NDC

} for information please