rewterz

2022

# THREAT INTEL INSIGHTS

**JANUARY** 2022

1

# CYBERATTACKS ON GOVERNMENT ENTITIES

Ukraine, Germany, China, Canada, and North Korea have been appealing targets for APT groups in this first month of 2022.

rewterz

2

# LOCKBIT RANSOMWARE

LockBit 2.0, a Ransomware-as-a-Service, has taken the world by storm.

3

# BRAZILIAN RAT ANDROID (BRATA)

BRATA android malware, with the ability to perform a factory reset on devices and run GPS tracking on them, is a deadly threat.


# PWNKIT

A memory corruption vulnerability in a SUID-root Program (polkit’s pkexec) allows any unprivileged user to gain full root privileges.

5

# CONTI RANSOMWARE

Tech Giant Delta Electronics and Indonesian Financial sector were both victims of the Conti Ransomware group.

6

# WIN32K VULNERABILITY

The January 2022 patches in the patch Tuesdays by Microsoft fixed this win32k vulnerability. However, the vulnerability is being exploited in the wild by threat actors after PoC of the vulnerability was published online.

rewterz

7

# MOLERATS

Molerats is a politically motivated nation-state actor that is conducting cyber espionage against targeted nations including Palestine, U.S., and also the UK.