rewterz

2022

THREAT INTEL INSIGHTS

APRIL 2022

1

T-MOBILE CONFIRMS LAPSUS$ HACK

In March, it was reported that LAPSUS$ had breached T-Mobile and Okta, which provides services to big names like Hitachi, T-Mobile, HP, and Siemens. T-Mobile confirmed the LAPSUS$ breach in April.

2

INDUSTRIAL SPY

A new Leaked Data Marketplace has emerged named "Industrial Spy”. The gang behind this marketplace uses adware and cracks to spread further.

3

RUSSIA'S CONTINUOUS CYBER ATTACKS AGAINST UKRAINE.

Russia's cyber attacks against Ukraine have opened up doors for Russian cybercriminals to attack what they deem "Enemies" of Russia.

4

ICS/SCADA DEVICES UNDER ATTACK

APT groups have created custom-made tools to attack and infiltrate ICS/SCADA devices. These tools have been observed in control specific devices and attacks.

5

SANCTIONS OF HYDRA DARK WEB MARKETPLACE

Germany’s Federal Criminal Police Office announced sanctions against Russia-based darknet market Hydra. ZIT, along with the U.S. law enforcement authorities conducted the investigation that led to the seizure of Hydra.

6

ANONYMOUS COLLECTIVE'S ACTIVITY ROUND-UP

Anonymous collective leaked the names, ranks, and other personal information of Russian military officers stationed at Bucha. They also leaked 900,000 emails from the All-Russia State Television and Radio Broadcasting Company (VGTRK).

7

HIVE RANSOMWARE

Hive ransomware operates as an affiliate-based ransomware, employs a wide variety of tactics, techniques, and procedures (TTPs), uses phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP).