

# THREAT INTEL INSIGHTS

MARCH 2022



# 1

## **NEW DATA WIPERS EMERGED THAT WERE TARGETING UKRAINE**

HermeticWiper, IsaacWiper, and DoubleZero Wipers emerged as a new threat for Ukrainian government officials and organizations.



2

# **RUSSIAN NUCLEAR INSTITUTE HIT BY ANONYMOUS COLLECTIVE**

Anonymous Collective not only breached the Russian Nuclear Institute, but also leaked thousands of emails and files.



**3****PHISHING EMAILS  
TARGETING PAKISTAN'S  
FINANCIAL SECTOR**

Our security analysts have discovered a new phishing campaign targeting banks in Pakistan. These phishing emails are invoice themed and contain malicious links/files.



# 4

## SERPENT BACKDOOR

French entities have become a target for a new backdoor called "Serpent." The backdoor uses the Chocolatey package installer to deliver the backdoor.



**5**

# MUSTANG PANDA'S HODUR


New Mustang Panda activity has been observed that involves the use of DLL side-loading to deliver PlugX. A new korplug variant has been discovered by researchers named "Hodur."



# 6

## GRAPHSTEEL AND GRIMPLANT MALWARE

GraphSteel and GrimPlant Backdoors have been used in conducting cyberattacks on Ukrainian authorities. The backdoors allow threat actors to gain unauthorized access and control of the victim's system.



7

# LAPSUS\$ CYBERATTACKS

LAPSUS\$ group (or DEV-0537) is a new and emerging Data Extortion group that has successfully attacked major conglomerates including Samsung, Microsoft, NVIDIA, Vodafone, Mercado Libre, Ubisof, and Okta to name a few.

