rewterz

2022

THREAT INTEL INSIGHTS

FEBRUARY 2022

1

CYBERATTACKS ON GOVERNMENT ENTITIES

Finnish Diplomats were attacked using Pegasus Spyware, Turkish organizations were attacked by MuddyWater, and German Oiltanking was also the victim of a cyberattack.

2

THE RUSSIAN-UKRAINIAN CYBERWAR

February saw the acceleration to the Russian-Ukrainian CyberWar with multiple DDoS, hacktivism, and ransomware attacks on both sides. With threat various threat groups such as ransomware groups also taking sides and partaking motivated by nationalism.

3

LINUX BASED MULTI-CLOUD ENVIRONMENTS UNDER ATTACK

Even though Linux environments are considered safer and more secure than windows environments, attacks on linux based environments have increased drastically.

4

MUSTANG PANDA

Mustang Panda, which although is a Chinese group, has also been taking advantage of the Russian-Ukrainian cyber warfare and used the situation to deploy a malware Ukraine.exe

5

SQUIRRELWAFFLE

Not only is the malspam loader sophisticated, it also implements multi-layer phishing to increase “legitimacy”

6

DONOT APT

Donot APT group has been actively dropping malicious samples and targeting Government officials to exfiltrate data.

7

ANONYMOUS COLLECTIVE

Anonymous, a hacktivist and activist collective, has declared their support for Ukraine in this ongoing cyber war.