rewterz

2022

THREAT INTEL INSIGHTS

MAY 2022

1

DOCKER ENGINE HONEYPOTS

Docker Engine honeypots were compromised by Ukraine supporters, most likely the Ukraine IT Army, in attacks against Belarusian and Russian websites. DOS attacks were conducted on Russian websites by compromising exposed Docker Engine API.

2

COSTA RICA ANNOUNCES STATE OF EMERGENCY

Costa Rican President Rodrigo Chaves declared a national cybersecurity emergency following the crippling of the country’s government and economy by the Conti ransomware attack.

3

MASSIVE HACKING CAMPAIGN

The campaign targeting WordPress sites begin on May 9th, 2022. In order to hack the website and insert malicious scripts, attackers are exploiting multiple different vulnerabilities in WordPress plugins and themes.

4

GITHUB OAUTH BREACH

GitHub announced that attackers used stolen OAuth app tokens supplied to Heroku and Travis-CI to steal the login data of around 100,000 npm accounts during a mid-April security compromise.

5

ANONYMOUS COLLECTIVE ACTIVITIES

The group claimed to have hacked various corporations and government entities. The stolen data was leaked by hacktivists on DDoSecrets (forum).

6

POWERSHELL RAT

An unknown threat actor targets German users interested in the Ukraine issue and infect them with a custom PowerShell RAT. The malware campaign employs a decoy site to entice users into false news bulletins regarding the Ukraine crisis.

7

MICROSOFT WARNS OF WEB SKIMMING CAMPAIGN

Researchers detected an online skimming campaign that employed numerous obfuscation techniques to escape detection. The threat actors disguised the skimming script by encoding it in PHP.