Severity

Medium

Analysis Summary

Anonymous, a hacktivist and activist collective, has declared their support for Ukraine in this ongoing cyberwar. The group recently claimed to have hacked various corporations and government entities. The stolen data was leaked by hacktivists using DDoSecrets.

Here are the top headlines by Collective for the previous week:

1. Anonymous collective has released a 130 GB archive including over 116,500 emails via DDoSecrets of SOCAR Energoresource. SOCAR Energoresource works with major Russian energy and oil firms such as Gazprom, Rosneft, and Lukoil. It is primarily owned by the Azerbaijan Republic's State Oil Company (SOCAR).
2. The Polar Branch of the Russian Federal Research Institute of Fisheries and Oceanography has been hacked. The hackers leaked 466 GB of emails from the organization also, B00daMooda and @DepaixPorteur are the sources of this leak.
3. Collective has made to the Russian local government email database, according to data provided on the DDoSecrets website. Over 7,000 emails from the Achinsk city administration have been stolen, and an 8.5GB collection was exposed by the collective.
4. The Port and Railway Projects Service of JSC UMMC runs Russia's two main coal-shipping ports. These ports transport coal to over 30 countries, including South Korea, Japan, China, the United Kingdom, Germany, Spain, Italy, Finland, Brazil, Israel, and Turkey. They've also become the victim of a collective attack, with a 106 GB archive containing nearly 77,500 emails leaked by DDoSecrets last week.

From the beginning of the war, Anonymous has been wreaking havoc on a number of Russian government websites. The collective has already declared that they will continue to return for more until Russia backs down.

Impact

- Cyber Espionage
- Cyber Warfare

Remediation

- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner.
- 2FA — Enable two-factor authentication.
- Patch — Patch and upgrade any platforms and software timely. Prioritize patching known exploited vulnerabilities.
- WAF — Set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- Passwords — Implement strong passwords.
- Logging — Log your eCommerce environment's network activity and web server activity.