Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.188 **23-05-2023**

Name: Windows-based LOBSHOT Trojan distributed through Rogue Google Ads

Threat Classification: Malware, Trojan

Affected Software / Services:

- Windows OS

Summary:

A financially motivated e-crime syndicate called TA505 is distributing a new Windows-based financial Trojan and information stealer called LOBSHOT. The malware is being distributed via rogue Google ads for legitimate tools like AnyDesk. It incorporates dynamic import resolution, anti-emulation checks, and string obfuscation to evade detection.

Severity	**High**
Attack Vector	**Social Engineering, Rogue Google Ads**

Once installed, LOBSHOT makes Windows Registry changes to set up persistence and siphons data from over 50 cryptocurrency wallet extensions present in web browsers. The malware's hVNC module allows for unobserved access to the compromised host, enabling threat actors to move quickly during the initial access stages with fully interactive remote control capabilities.

Recommendations:

- Monitor systems for any suspicious activity and ensure that all systems and software are up to date with the latest patches.

- Block rogue Google ads and prevent users from accessing the associated websites.
- Avoid clicking on suspicious links or downloading any unknown software or attachments.
- Regularly conduct awareness trainings for employees on cybersecurity best practices to help prevent successful attacks.
- Deploy a defense-in-depth strategy, including firewalls, intrusion detection and prevention systems, and anti-malware software. Implement IP blocking to prevent further infections.
- In case of any incident, please report to this office, through PTA CERT Portal and email.