Severity

Medium

Analysis Summary

In the past few years Orcus was known as Schnorchel, is a Remote Access Trojan with some odd activity. This RAT enables attackers to create plugins using a custom development library and offers a robust core feature set that makes it one of the most dangerous malicious programs in its class. The ability of Orcus RAT include:

- Keylogging and remote administration
- Stealing system information and credentials
- Taking screenshots, recording video from Webcams, recording audio from microphones, and disabling webcam light
- Executing remote code execution and Denial-of-Service
- Exploring/editing registry
- Detecting VMs
- Reverse Proxying
- Real-Time Scripting
- Advanced Plugin System

Government entities, financial services organizations, information technology service providers, and consultancies are the main target sectors of Orcus RAT.

Impact

- Credential Theft
- Financial Loss

Indicators of Compromise

MD5

- 45f4ce7314bc120c5d76e818b901a6f3
- cdf0cecf651a9182fb4c91f0e21f857d

SHA-256

- b31a34a6ab47907b5fe10f8f30a7bfac9a30e352906d7de3551fc5d946d19b12
- e7bc4f31a489a6ea5a5785364ab377bb2a0cc597bbd0765657c670d431c2e1fd

SHA-1

- a09f084fe5095358231e5ea8b4b2d3567bcef5d7
- 3ca4b01108d7417388733566d2d3d3e4c79d7ec6

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.