## Severity

High

## 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

- 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

## Impact

- Credential Theft
- Financial Loss

## Indicators of Compromise

#### MD5

- 074333816e82613e878ba704e5905c81

#### SHA-256

- e44a1c3c7069e3b2a2f3cbbd6e414f1c4fc1331e0ef96ea80780b958ced9bf57

#### SHA-1

- 9808d9b42c8053128f6507a9f6ae571b94a4e74c

## Remediation

- Block the threat indicators at their respective controls.
- Do not respond to unexpected emails from untrusted email addresses.