**From:** eims@ic.fbi.gov <eims@ic.fbi.gov>
**Date:** Saturday, November 13, 2021 at 2:06 AM
**To:** abuse alias
**Subject:** Urgent: Threat actor in systems

Delivered From External Sender

---

Our intelligence monitoring indicates exfiltration of several of your virtualized clusters in a sophisticated chain attack. We tried to blackhole the transit nodes used by this advanced persistent threat actor, however there is a huge chance he will modify his attack with fastflux technologies, which he proxies trough multiple global accelerators. We identified the threat actor to be Vinny Troia, whom is believed to be affiliated with the extortion gang TheDarkOverlord, We highly recommend you to check your systems and IDS monitoring. Beware this threat actor is currently working under inspection of the NCCIC, as we are dependent on some of his intelligence research we can not interfere physically within 4 hours, which could be enough time to cause severe damage to your infrastructure.
Stay safe,
U.S. Department of Homeland Security | Cyber Threat Detection and Analysis | Network Analysis Group