LevelBlue - Open Threat Exchange

By milind

- Created 10 years ago by milind
- Public
- TLP: Green

MVS Research team has detected multiple attacks on its PoS customers from Gorynich malware. Gorynich was used to download a repurposed BlackPOS malware with RAM scraping functionality and upload all the dumped credit card numbers in memory. As the original BlackPOS used a text file to store pilfered credit card data, Gorynych now grabs that text file and does an HTTP POST to complete the data exfiltration.
