## Pakistan Telecom Authority Headquarters, Islamabad

**PTA Cyber Security Advisory No. 238** **05-03-2024**

**Name:** RansomHouse Operation Deploys 'MrAgent' for Automated VMware ESXi Attacks

**Threat Classification:** Ransomware / Cyber Threat

**Affected Software / Services:**

- VMware ESXi hypervisors
- Windows and Linux Operating Systems

**Summary:**

A recent surge in RansomHouse ransomware attacks introduces a new level of sophistication with the deployment of 'MrAgent.' This specialized tool streamlines and automates attacks on VMware ESXi hypervisors, posing a significant threat to organizations relying on virtual environments. The automation capabilities of MrAgent underscore the evolving strategies of ransomware-as-a-service (RaaS) operations, demanding heightened vigilance from targeted entities.

| | |
|---|---|
| **Severity** | **High** |
| **Attack Vector** | Automated ESXi Exploitation |

**Recommendations:**

- Ensure prompt updating of software to mitigate potential vulnerabilities.
- Implement comprehensive network monitoring to detect and respond to suspicious activities promptly.
- Fortify access controls to limit unauthorized entry and movement within networks.
- Conduct regular employee training programs to enhance security awareness and vigilance.
- Deploy advanced endpoint protection solutions capable of detecting and neutralizing evolving threats.
- Implement regular and secure data backup practices to minimize the impact of potential ransomware attacks.
- In case of any incident, please report to this office, through PTA CERT Portal and email.