RDM – Ransomware Detecting Machine

Version: 1.0
Author: Xylen LLC
Last Updated: June 15, 2025

Overview

RDM (Ransomware Detecting Machine) is an advanced, user-friendly security tool designed to help individuals and organizations detect ransomware infections on their systems. By leveraging behavioral analysis, known signature detection, and system monitoring, RDM actively searches for signs of ransomware activity to prevent data loss and minimize damage.

Key Features

- **Real-Time Monitoring**
  Constantly watches system processes and file behaviors to catch early signs of ransomware activity.
- **Threat Signature Database**
  Maintains an up-to-date database of known ransomware signatures and families.
- **Heuristic & Behavioral Detection**
  Detects suspicious actions like mass encryption, file renaming, or unauthorized registry changes.
- **Alert System**
  Notifies users immediately upon detecting threats with severity levels and recommendations.
- **Quarantine Mode**
  Automatically isolates suspicious files to prevent ransomware spread.
- **Scheduled & Manual Scans**
  Run system scans on demand or schedule them at regular intervals.
- **Cross-Platform Support**
  Works on Windows, Linux, and macOS.

🛠️ System Requirements

Component	Minimum Requirements
Operating System	Windows 10/11, Ubuntu 20.04+, macOS 12+
RAM	2 GB
Disk Space	100 MB
Permissions	Admin/root required for full scanning

⚙️ Installation

Windows

```
Clone RDM from https://github.com/cyberxylen/RDM.git

Run the installer `RDM_Setup.exe` and follow the wizard.
```

Linux (Debian/Ubuntu)

```
wget  https://github.com/cyberxylen/Linux/rdm-linux.git
sudo dpkg -i rdm-linux.deb
sudo rdm --start
```

macOS

```
brew install rdm-tool
rdm --start
```

🧪 How It Works

1. **Startup Scan** – RDM performs an optional quick scan at boot to detect dormant ransomware.
2. **Real-Time Monitoring** – Monitors system behavior and flags suspicious encryption-like activities.
3. **Behavioral Analysis** – Uses machine learning to detect ransomware based on actions, not just known signatures.

4. **Threat Containment** – Stops suspect processes and quarantines files before encryption spreads.
5. **Notifications** – Informs users of threats and provides recommended actions in a clean UI or terminal output.

🧭 Usage Examples

Quick Scan

```
rdm --scan quick
```

Full System Scan

```
rdm --scan full
```

Scan Specific Folder

```
rdm --scan /home/user/Documents
```

Check Quarantine

```
rdm --quarantine list
```

Update Definitions

```
rdm --update
```

🔧 Command Reference

Command	Description
`rdm --scan`	Runs a quick system scan
`rdm --scan full`	Full scan of all mounted drives
`rdm --monitor on`	Enables real-time ransomware watch
`rdm --quarantine`	Shows or manages quarantined files
`rdm --restore <file>`	Restores a quarantined file
`rdm --update`	Updates threat detection database

Command	Description
`rdm --status`	Shows current scan/monitor status

🔄 Threat Database Updates

RDM updates its threat database from a secure cloud repository daily. You can also manually trigger updates:

```
rdm --update
```

Offline update packages are also available for air-gapped environments.

🔐 Security and Privacy

- No sensitive data is transmitted without explicit user consent.
- RDM logs remain local unless shared manually.
- Quarantine files are encrypted and sandboxed.

📞 Support

Need help or want to report a bug?

- Website: N/A
- Support Email: xln.supplies@atomicmail.io
- GitHub Issues: https://github.com/cyberxylen/RDM/issues

🧠 Pro Tips

- Keep RDM updated daily for the best protection.
- Schedule full scans weekly.
- Use in combination with a strong backup strategy.
- Isolate suspected ransomware infections by disconnecting from the network.
