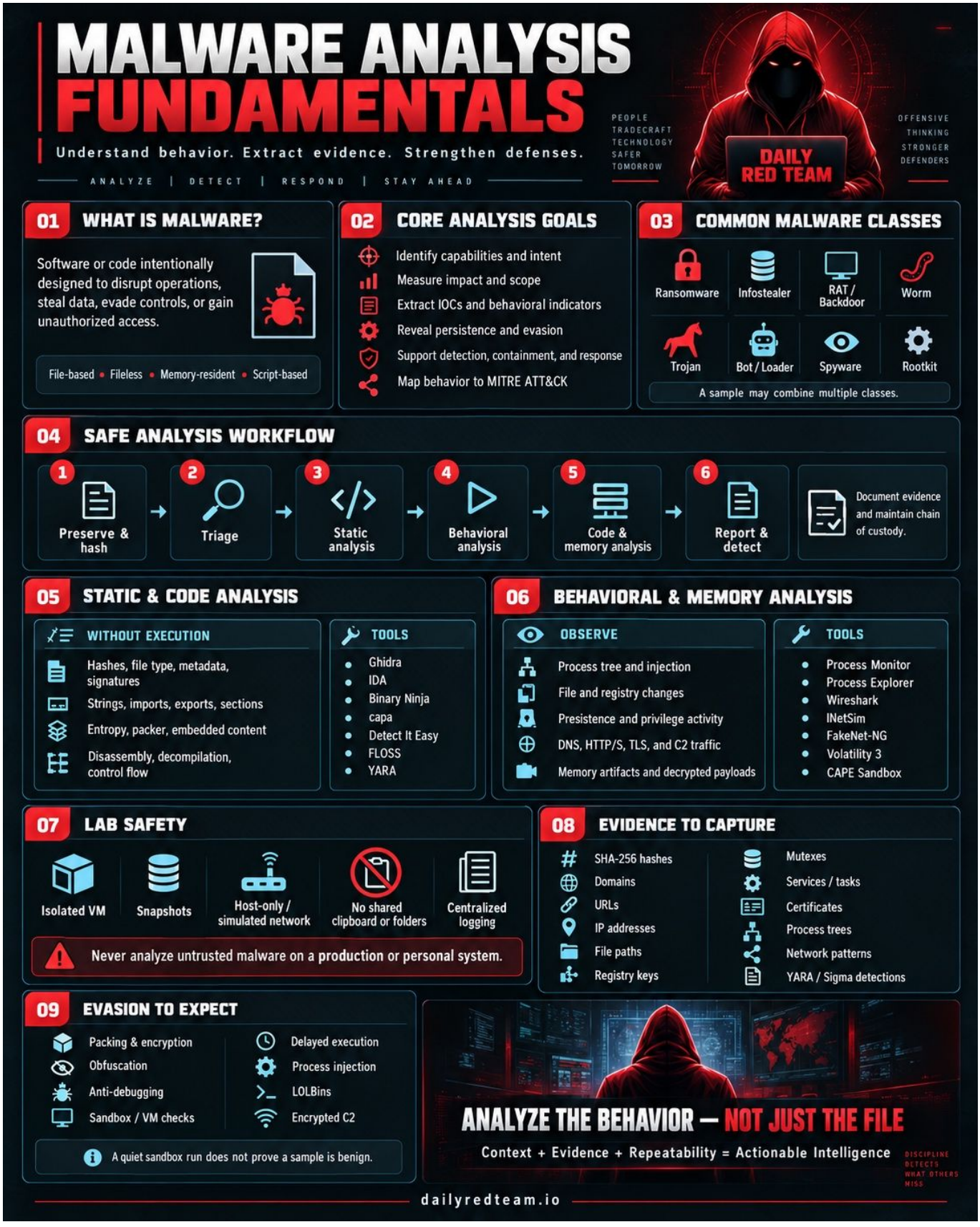
Malware

- Malware Bible (Github)

Analysis



Sandboxes

If you’re serious about malware analysis, start using these: Cuckoo Sandbox: An open-source sandbox that provides automated analysis of suspicious files and behaviors. https://github.com/cuckoosandbox/cuckoo

 Any.Run: A web-based interactive sandbox that allows users to run and analyze malware in real-time. https://any.run/

 Joe Sandbox: Community Edition of Joe Sandbox offers a free version for malware analysis. https://www.joesandbox.com/#windows

 IRMA (Incident Response & Malware Analysis): An open-source platform for analyzing malware and performing incident response https://github.com/quarkslab/irma

 Viper: A framework for analyzing malware samples. It provides a user-friendly web interface and supports multiple analysis tools. https://github.com/viper-framework/viper

 Limon Sandbox: An open-source sandbox developed to automate the analysis of Linux malware. https://github.com/monnappa22/Limon

 BinaruGuard: Automated malware analysis on a revolutionary bare-metal platform in the cloud. https://www.crunchbase.com/organization/binary-guard

 Hybrid Analysis: A cloud-based platform that combines sandbox analysis with threat intelligence feeds. https://hybrid-analysis.com/

 Filescan: operating at 10x speed compared to traditional sandboxes with 90% less resource usage https://www.filescan.io/scan

 Sandblast: Its a malware analysis system by Checkpoint https://threatpoint.checkpoint.com/ThreatPortal/emulation

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/malware

Last update: **2026/09/22 11:51**