Security Leftovers

By Roy Schestowitz
Created 14/08/2022 - 7:03am
Submitted by Roy Schestowitz on Sunday 14th of August 2022 07:03:09 AM Filed under Security [1]

- **SentinelOne discusses the rise of data-wiping malware [2]**

  During a Black Hat 2022 session, researchers showed how expectations of cyber war may differ from the reality.

- **Researchers reveal Kubernetes security holes, prevention [3]**

  Researchers with Palo Alto Networks took the stage at Black Hat to explain how configurations and system privileges in Kubernetes clusters can allow container escape and takeover.

- **Google researchers dissect Android spyware, zero days [4]**

  Researchers with Google's Threat Analysis Group say the ecosystem of surveillance vendors is far larger than just NSO Group, and some vendors are sharing or trading exploits.

- **Docker's rootless mode a welcome security update [5]**

  Docker containers have root privileges by default -- a known security issue for several years. Now Docker's rootless mode separates containers from underlying infrastructure.
New GwisinLocker ransomware encrypts Windows and Linux ESXi servers[6]

This site generally doesn’t cover or announce new types of ransomware, but this one targets the healthcare sector, so?.

Zero-Day Vulnerability Exploited to Hack Over 1,000 Zimbra Email Servers | SecurityWeek.Com[7]

A new zero-day vulnerability tracked as CVE-2022-37042 has been exploited since at least June to hack over 1,000 Zimbra email servers.

Source URL: http://www.tuxmachines.org/node/168319

Links: