TASK 5

1) Auto-Color (Linux Malware) — Found in February 2025

What happened:
Researchers found a new type of malware called *Auto-Color* that was attacking universities and government systems. It was a backdoor made for Linux computers. This malware was very sneaky — it changed its file names, used secret communication, and even made it hard to remove. It first started spreading around November–December 2024, and experts revealed it to the public in February 2025.

How it was handled:

- Security teams shared info: A cybersecurity group called Unit42 shared details like file names, domains, and how the malware behaved. This helped others look for it in their systems.
- Security software got updated: Companies updated their antivirus and monitoring tools so they could detect and block the malware.
- Cleanup steps were given: Affected organizations were told to isolate infected machines, collect evidence, reset accounts, fix the entry points, and sometimes completely reinstall the systems since the malware was very hard to remove.

Main lesson:
When dealing with advanced Linux malware, it's safer to wipe and reinstall machines rather than trying to clean them. Also, sharing threat information quickly helps stop the spread.

2) QakBot (Qbot) — Major Banking Trojan Taken Down in May 2025

What happened:
QakBot is a malware that has been around for years. It mainly infects Windows computers and usually spreads through fake email attachments. Once it gets in, it can steal data, spread to other machines, and even install ransomware. In May 2025, the U.S. Department of Justice (DOJ) reported that they charged one of the main operators behind it.

How it was handled:

- Law enforcement took action: Authorities from different countries shut down servers, seized money, and blocked the botnet's traffic.
- Cleanup on infected machines: In past operations, law enforcement even sent uninstall commands to infected computers to remove QakBot. They also gave tools and instructions to help victims clean their systems.
- Warnings and rules shared: Public alerts helped security teams learn how QakBot works so they could block it and prevent new infections.

Main lesson:
Government action can break big malware networks, but computers still need to be protected at the user level — people should avoid suspicious files, systems should be updated, and organizations should have a response plan.

3) DetourDog & Strela Stealer — DNS-Based Attack on 30,000+ Websites (Late 2025)

What happened:
Researchers discovered a large attack called *DetourDog*. The hackers didn't attack users directly — they hacked websites and tampered with their DNS settings (which control where a website points). When people visited these sites, they were silently redirected to pages that installed *Strela Stealer*, a malware that steals login details. This was hard to detect because the redirects happened in the server's DNS, not on the user's device.

How it was handled:

- Owners were alerted: Infoblox (the group that discovered this) contacted website owners and domain providers so they could fix their DNS settings and remove bad entries.
- Security fixes were suggested: They told people to secure DNS accounts, watch for strange DNS activity, apply DNSSEC, patch websites, and use filters to block bad traffic.
- Security companies reacted: Antivirus and hosting services updated their tools to detect and block the malware. Once DNS settings were cleaned, users stopped getting redirected.

Main lesson:
Hackers are now targeting DNS systems more often. Protecting and monitoring DNS is just as important as securing servers or passwords.