Malware Kronos

A British cybersecurity researcher has pleaded guilty for **developing a malware named Kronos** aimed at **stealing banking information.**

- It can be noted that the same researcher was earlier hailed as a hero for **finding a “kill switch” to the WannaCry virus.**
  - WannaCry virus was a **cryptoransomware, also known as WannaCrypt**, which affected thousands of computers spread over 150 countries, **including India in May, 2017.**
- Kronos is a **type of Trojan.** Trojans are commonly spread via email attachments, and once downloaded, can give attackers free reign to snoop and steal sensitive information like financial data, emails, and passwords.
  - Kronos first appeared online on a **Russian underground forum in 2014.**

Security Threats on the Web

- **Distributed Denial of Service (DDoS)**
  - A Distributed Denial of Service (DDoS) attack is an **attempt made to take down a website or online service** by flooding it with **more traffic than server/network can accommodate.**
  - In a DDoS attack, the traffic can come from **hundreds or thousands of sources**, which makes it near-impossible to stop the attack simply by blocking a single IP address.
  - Sites also **struggle to differentiate between a legitimate user and attack traffic.**
  - A DDoS attack differs from a **Denial of Service (DoS) attack, which typically uses a single computer** and connection to flood a system or site.
- **Viruses**
  - A computer virus is a **type of malicious code or program written** to alter the way a computer operates and is designed to **spread from one computer to another.**
  - It requires **some user interaction to be initiated.** Computer viruses cannot reproduce and spread without programming such as a file or document.
- **Malware and Trojans**
  - Malware is a more generic term that can be used to refer to nefarious software, which has been specifically designed to disrupt or damage a computer system, while **trojans are programs that pretend to be something they're not, and include malicious additions.**
  - Trojans are often **bundled with legitimate software** (eg, downloaded via P2P or file-download sites) but keep the original software intact to avoid suspicion and allow the trojan to spread further.
  - The term **'spyware' is a sub-division of malware** and refers to those programs dedicated to stealing personal details (logins, passwords, personal info, etc) once they've found a way onto computer or phone.
- **Phishing**
  - It is an effort by **scammers to trick users into giving up personal information** that they can then use to access your bank accounts or credit cards. Phishers can reach users through email, text or even by phone.
  - The **core of phishing attacks is deception**. Each attacker is attempting to convince users that they are a **familiar person or brand.**
- **Ransomware**

- Ransomware **prevents users from accessing their devices** and data until a certain ransom is paid to its creator or risk losing access forever.
- Ransomware usually locks computers, encrypts the data on it and prevents software and apps from running.

- **Worms**
  - A computer worm is a **type of malware that spreads copies of itself from computer to computer.** A worm can **replicate itself without any human interaction,** and it does not need to attach itself to a software program in order to cause damage.
  - This makes **worms potentially more dangerous than viruses**, trojans or other malware, as **they're harder to contain.**
  - While traditional anti-virus software will take care of a lot of the better-known viruses and trojans, the **ability to replicate itself to networked resources without any interaction makes containing a worm a much harder task.**