METMOX

Delivering values innovatively

Malware

A ‘Living’ Virus discovered in years

Ever since the birth of digitalization, people were fighting against the threats of malware. But what exactly is malware? It is malicious software that is harmful to computers, PCs, mobile devices, servers and more. Malware authors use a variety of physical and virtual means to spread it to infect devices and networks. Once the malware has been installed, it infects the digital device and begins working towards the hackers’ goals.

Techniques employed by KBOT:

Once a system is infected, KBOT gains Persistence by writing itself to start-up and the task scheduler, infecting all .exe files on logical drives and shared network folders.

- It performs web Injection in order to steal the victim's data.
- It uses the RC6 Algorithm to encrypt its files and stolen data in a virtual file system.
- It uses DLL Hijacking to operate directly into the memory allocated to legitimate running DLL processes. It also scans for DLLs related to antivirus software in order to suspend them.

How organizations can defend against KBOT:

KBOT virus takes out system files with no hope of recovery but the following recommendations will reduce the damage.

- Check for traces of this Malware in your environment using the IoCs mentioned below.
- Keep applications/software and OS at the latest released patch level.
- Make sure antivirus and the files associated with it are updated.
- Advise users to not click on unknown/unsolicited links.
- Always check for suspicious emails from unknown senders. Verify the legitimacy of email attachments before opening them.
- Always be cautious of an unverified/unknown page and website connections labelled as ‘not secure’.

‘KBOT’ the new malware

Including illicit cryptocurrency miners, Trojans, ransomware, and highly complex surveillance software designed to infiltrate the devices and networks. Like the tough get tougher, researchers have recently discovered a new malware, dubbed as KBOT, being delivered via Internet-facing systems, local networks, and removable drives.

- It is a virus that spreads by injecting malicious polymorphic code into Windows executable files.
- It attempts to steal the victim's personal and banking data stored in browsers.
- The malware-related files are stored in a virtual file system, along with the stolen data that is sent to the Command & Control server.
- It also sends the bot ID of the infected system and detailed information such as computer name, operating system, and lists of files, local users and installed security software.
- It can receive commands such as deleting and updating files, updating bot modules or performing self-destruction.
- It is also capable of controlling the infected system through Remote Desktop Sessions and downloading additional Info Stealer modules.
- The reason why this malware is being called a ‘Living Virus’ is that it can spread quickly in the system, local network, and removable drives.
- It slows down the system as it injects into running processes. Additionally, it overwrites the code of the exe files, rendering them unrecoverable

Companies should also implement a multifaceted security strategy that controls access to enterprise resources and continuously monitors business-critical endpoints for malicious activities and work towards the demolition of such malware in their devices or networks.

CERTIFIED ISO 27001 CERTIFIED