Cyber Alert ! Malicious Binary Malware on the Prowl

- Researchers identified a malicious binary, named inetinfo.sys, installed on a system at an organisation within the **transport and shipping sector of Kuwait**
- The criminal developer used character names from the anime series Hunter x Hunter.

Recent research findings show that hackers are targeting transport and shipping companies with a new trojan malware campaign, reports The Loadstar.

Cyber security compromised

The news comes as the logistics sector is undergoing a digital transformation, potentially increasing its vulnerability to cyber attacks. Paloalto Networks revealed this week it had identified a "*malicious binary, named inetinfo.sys, installed on a system at an organization within the transport and shipping sector of Kuwait*".

Through comparative analysis, they have identified related activity also has targeted Kuwait between July and December 2018. It added, *"While there are no direct infrastructure overlaps between the two campaigns, historical analysis shows that the 2018 and 2019 activities are likely related*."

Vulnerability concerns in Transport and Shipping

The cyber tools were previously unknown and have raised concerns about vulnerabilities in the transport sector. "*This report is indicative of recent trends we're observing with transport and shipping*," said Dave Weinstein, chief security officer at cyber security company Claroty. He added, "*Both the transport and shipping industries are undergoing a great deal of digital transformation to drive efficiencies, thus opening-up new attack vectors for malicious actors*." "*It's critical for organizations in these sectors to gain visibility into the intersection of their corporate and operational networks, as hackers are exploiting the former to target the latter*," he said.

Kuwait based company – First victim

The malware was discovered between May and June by Paloalto's Unit 42. It explained: "*The first known attack in this campaign targeted a **Kuwait transport and shipping company** in which the actors installed a backdoor tool named Hisoka*." "*Several custom tools were later downloaded to the system in order to carry out post-exploitation activities. All of these tools appear to have been created by the same developer. We were able to collect several variations of these tools, including one dating back to July 2018*."

NotPetya attack

The risk of cyber crime to shipping and logistics was amply demonstrated by last year's NotPetya **attack on Maersk, which cost the shipping group some $300m.**

FedEx's subsidiary TNT was also hit and is now facing legal action by a shareholder who claimed FedEx was not transparent about the costs and effects of the attack, and it "*permanently*" lost business as a result.