Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:34:29 UTC

Description(Trend Micro) In 2012, the source code of BlackPOS was leaked, enabling other cybercriminals and attackers to enhance its code.

Even though BlackPOS ver2 has an entirely different code compared to the BlackPOS which compromised Target, it duplicates the data exfiltration technique used by the Target BlackPOS. It is an improved clone of the original, which is why we decided to call this BlackPOS ver2.

It is also being reported in the press that some security vendors called this malware as “FrameworkPOS.”
