8.t Dropper (Malware Family)

By Fraunhofer FKIE

8T_Dropper has been used by Chinese threat actor TA428 in order to install Cotx RAT onto victim's machines during Operation LagTime IT. According to Proofpoint the attack was developed against a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. The dropper was delivered through an RTF document exploiting CVE-2018-0798.

▶ [TLP:WHITE] win_8t_dropper_auto (20251219 | Detects win.8t_dropper.)
