Gozi (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:13:12 UTC

2000 Ursnif aka Snifula
2006 Gozi v1.0, Gozi CRM, CRM, Papras
2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)
-> 2010 Gozi Prinimalka -> Vawtrak/Neverquest

In 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.
It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.

In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.

▶ [TLP:WHITE] win_gozi_auto (20251219 | Detects win.gozi.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi