New wave of malicious emails associated with the Hive0117 group

Data: 2025-09-27 14:18:42

Autor: Inteligência Against Invaders

Redazione RHC**:27 September 2025 16:17**

F6 has reported a new wave of malicious emails associated with the **Hive0117** group.

Hive0117 has been active since February 2022 and uses the **DarkWatchman RAT Trojan** . The group disguises its campaigns as *messages from legitimate organizations, records email infrastructure and control domains, and sometimes repurposes them* .

According to F6, DarkWatchman activity was detected on September 24, after several months of silence.

The attacks were carried out under the guise of the *Federal Bailiff Service from the address mail@fssp[.]buzz.* Similar mailings were observed in June and July. Analysis revealed the domains *4ad74aab[.]cfd and 4ad74aab[.]xyz.*

The attacks targeted companies in Russia and Kazakhstan. The list of 51 targets included *banks, telecommunications operators, marketplaces, logistics and manufacturing companies, car dealerships, construction companies, retailers, insurance and investment firms, fuel and energy companies, pharmaceutical companies, research institutes, a technology park, a municipal solid waste management operator, as well as services in the tourism, fitness, and IT sectors.*

DarkWatchman was also distributed via mailings disguised as supposedly Department of Defense archives and fake subpoenas .

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli