Microsoft links Raspberry Robin worm to Clop ransomware attacks

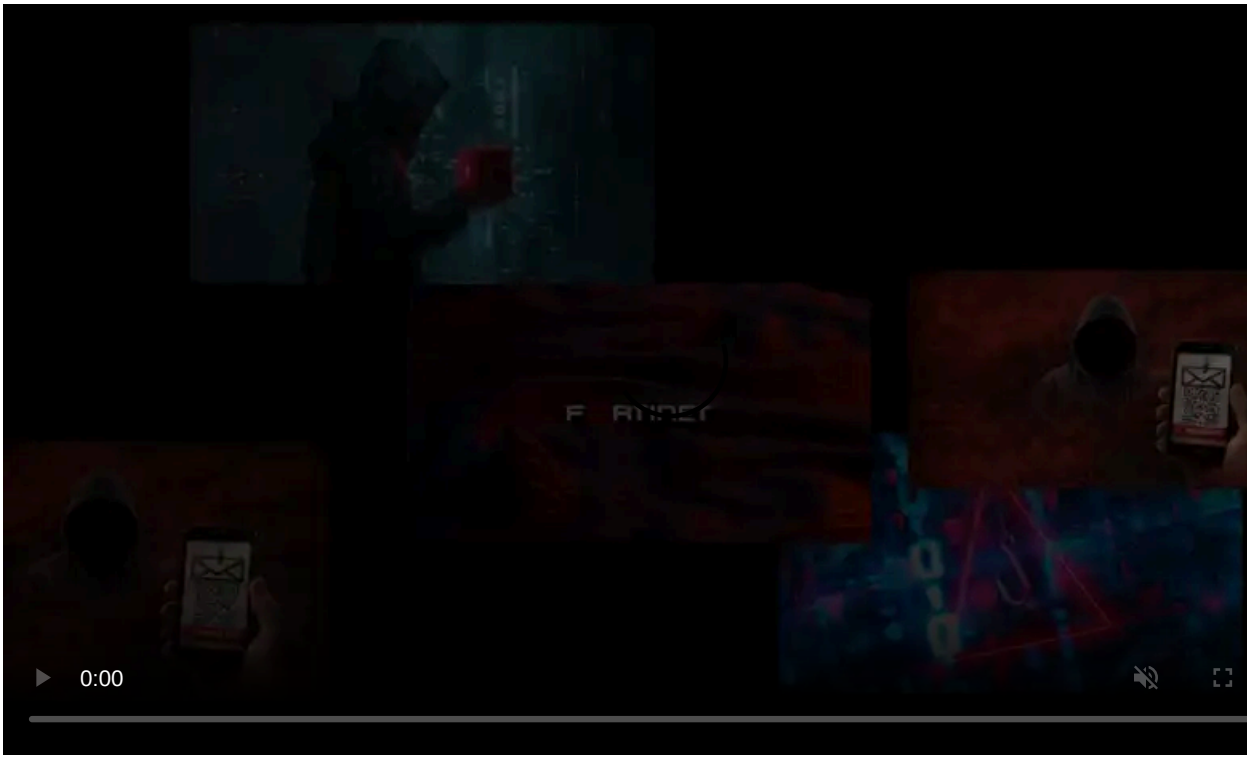
By Sergiu Gatlan

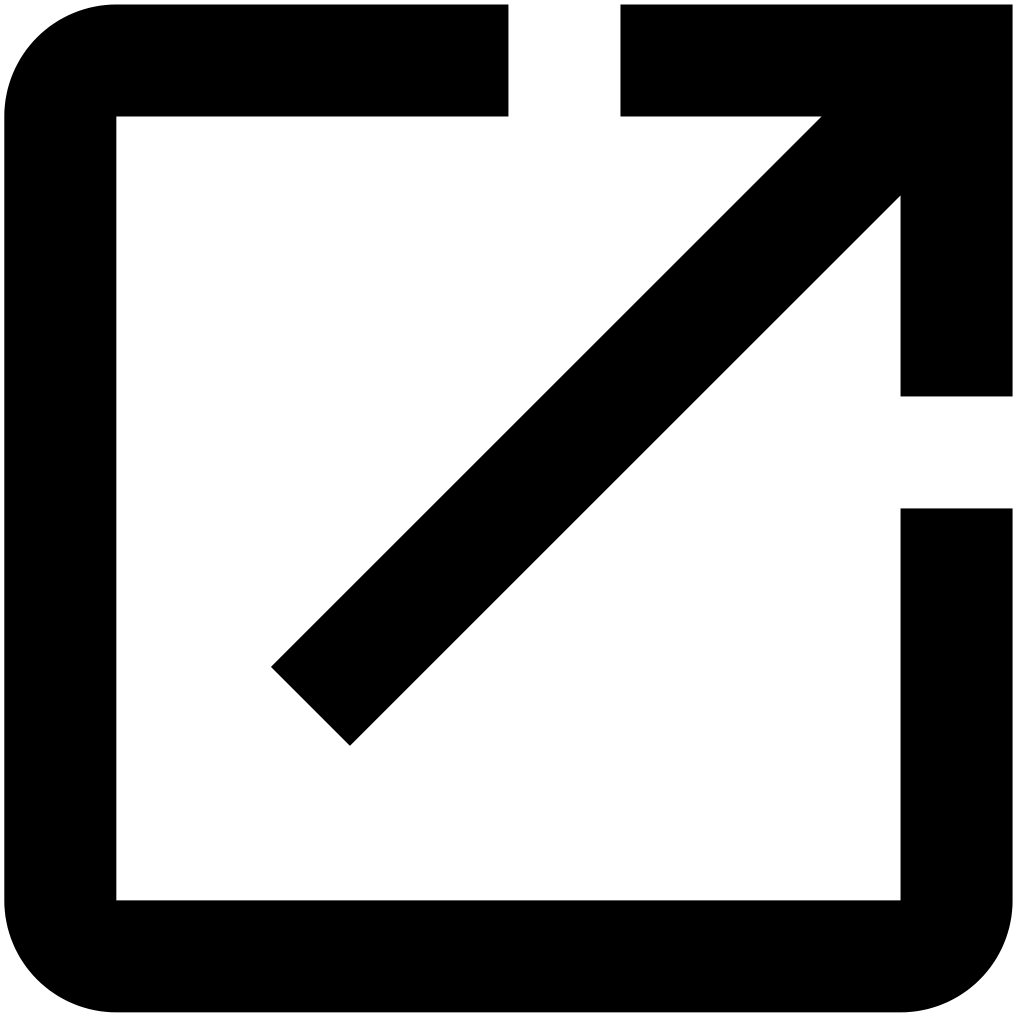
Published: 2022-10-27 · Archived: 2026-04-05 23:04:48 UTC

Microsoft says a threat group tracked as DEV-0950 used Clop ransomware to encrypt the network of a victim previously infected with the Raspberry Robin worm.

DEV-0950 malicious activity overlaps with financially motivated cybercrime groups tracked as FIN11 and TA505, known for deploying Clop payloads ransomware on targets' systems.

Besides ransomware, Raspberry Robin has also been used to drop other second-stage payloads onto compromised devices, including IcedID, Bumblebee, and Truebot.


0:00

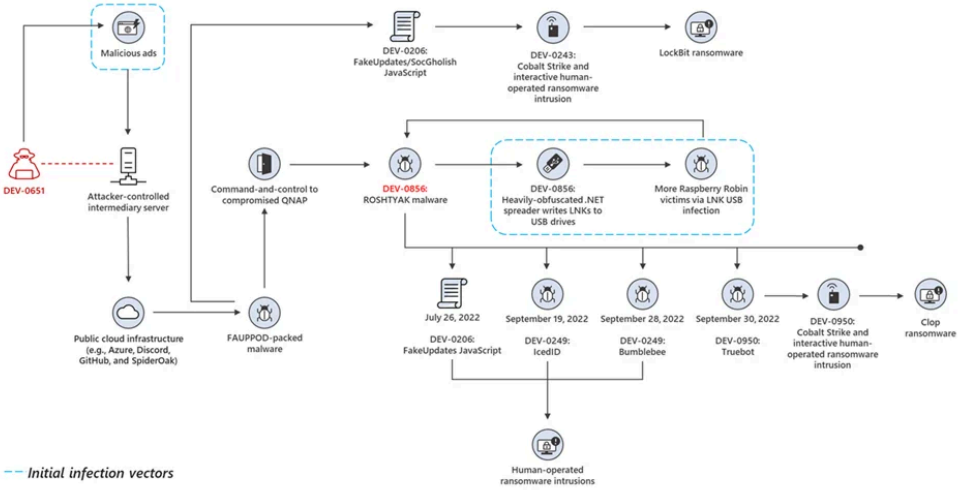


"Beginning on September 19, 2022, Microsoft identified Raspberry Robin worm infections deploying IcedID and—later at other victims—Bumblebee and TrueBot payloads," Microsoft Security Threat Intelligence analysts said.

"In October 2022, Microsoft researchers observed Raspberry Robin infections followed by Cobalt Strike activity from DEV-0950. This activity, which in some cases included a Truebot infection, eventually deployed the Clop ransomware."

This hints at Raspberry Robin's operators selling initial access to compromised enterprise systems to ransomware gangs and affiliates who now have an additional way to get into their targets' networks besides phishing emails and malicious ads.

In late July, Microsoft also said it detected Evil Corp pre-ransomware behavior on networks where an access broker tracked as DEV-0206 dropped the FakeUpdates (aka SocGholish) backdoor on Raspberry Robin-infected devices.



Raspberry Robin cybercriminal ecosystem (Microsoft)

Nearly 1,000 orgs compromised within 30 days

Spotted in September 2021 by Red Canary intelligence analysts, Raspberry Robin spreads to other devices via infected USB devices containing a malicious .LNK file.

After the USB device is attached and the user clicks the link, the worm will spawn a msiexec process using cmd.exe to launch a second malicious file stored on the infected drive.

On compromised Windows devices, it communicates with its command and control servers (C2). It also delivers and executes additional payloads after bypassing User Account Control (UAC) on infected systems using several legitimate Windows utilities (fodhelper, msiexec, and odbcconf).

Microsoft said in early July that it detected Raspberry Robin malware infection on the networks of hundreds of organizations from a wide range of industry sectors.

Today, the company revealed that the worm has spread to systems belonging to nearly 1,000 organizations within the past month.

"Microsoft Defender for Endpoint data indicates that nearly 3,000 devices in almost 1,000 organizations have seen at least one Raspberry Robin payload-related alert in the last 30 days," Microsoft added.
