Microsoft links Raspberry Robin malware to Evil Corp attacks

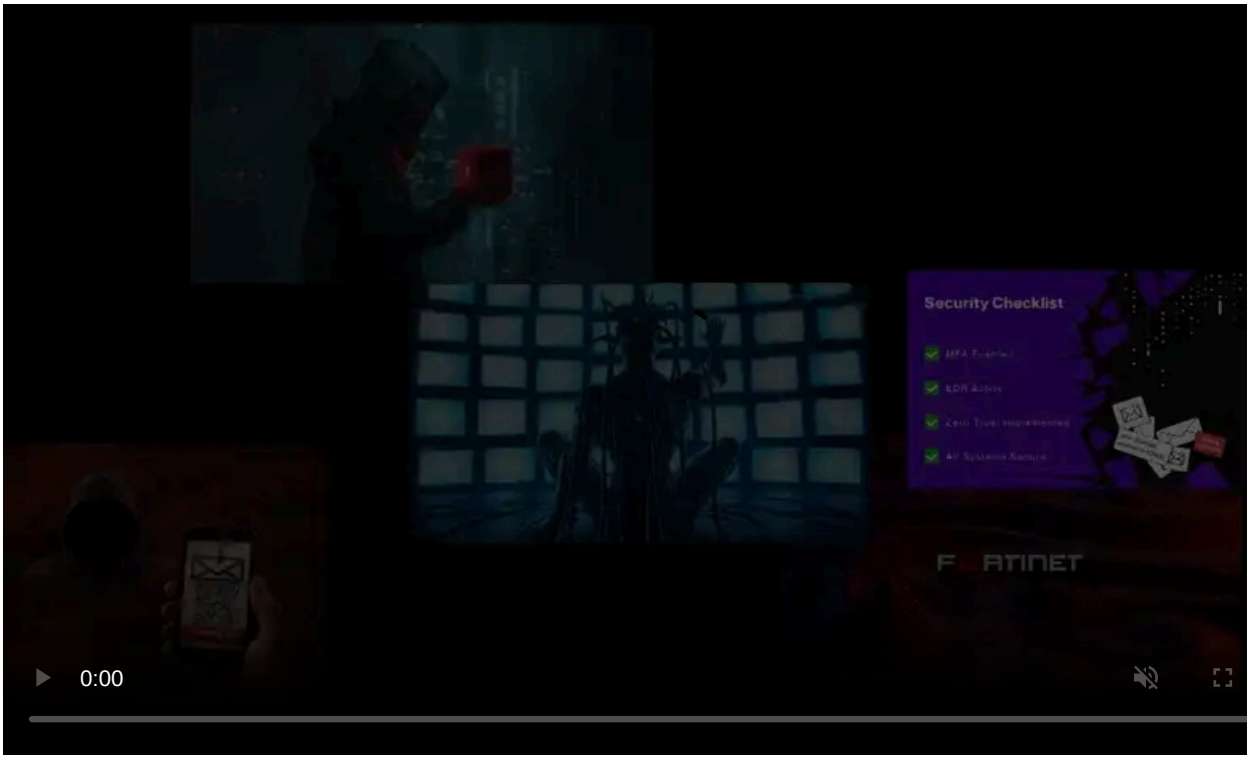
By Sergiu Gatlan

Published: 2022-07-29 · Archived: 2026-04-06 15:46:39 UTC

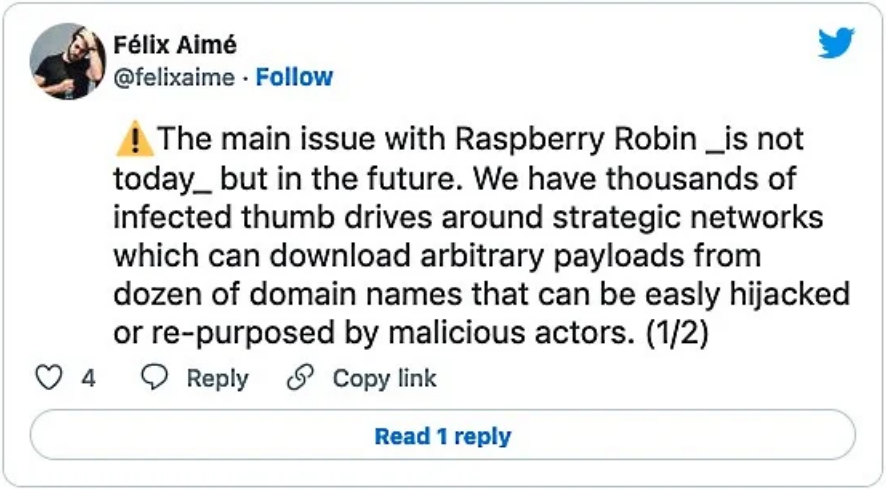
Microsoft has discovered that an access broker it tracks as DEV-0206 uses the Raspberry Robin Windows worm to deploy a malware downloader on networks where it also found evidence of malicious activity matching Evil Corp tactics.

"On July 26, 2022, Microsoft researchers discovered the FakeUpdates malware being delivered via existing Raspberry Robin infections," Microsoft revealed Thursday.

"The DEV-0206-associated FakeUpdates activity on affected systems has since led to follow-on actions resembling DEV-0243 pre-ransomware behavior."


Security Checklist
0:00

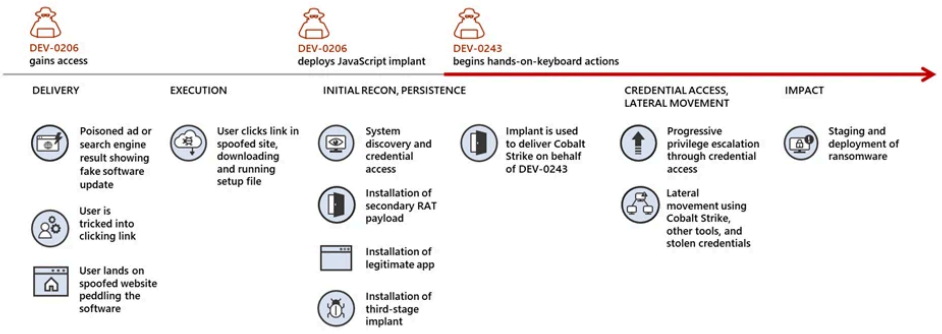
According to a threat intelligence advisory shared with enterprise customers, Microsoft has found Raspberry Robin malware on the networks of hundreds of organizations from a wide range of industry sectors.



First spotted in September 2021 by Red Canary intelligence analysts, it spreads via infected USB devices to other devices on a target's network once deployed on a compromised system.

Redmond's findings match those of Red Canary's Detection Engineering team, which also detected it on the networks of customers in the technology and manufacturing sectors.

This is the first time security researchers have found evidence of how the threat actors behind Raspberry Robin plan to exploit the access they gained to their victims' networks using this worm.



DEV-0206 to Evil Corp handover (Microsoft)

Evil Corp, ransomware, and sanctions evasion

Evil Corp, the cybercrime group that seems to take advantage of Raspberry Robin's access to enterprise networks (tracked by Microsoft as DEV-0243), has been active since 2007 and is known for pushing the Dridex malware and for switching to deploying ransomware.

From Locky ransomware and its own BitPaymer ransomware strain, the threat group has moved to install its new WastedLocker ransomware starting in June 2019.

From March 2021, Evil Corp moved to other strains known as Hades ransomware, Macaw Locker, and Phoenix CryptoLocker, finally being observed by Mandiant deploying ransomware as a LockBit affiliate since mid-2022.

Switching between ransomware payloads and adopting a Ransomware as a Service (RaaS) affiliate role are part of Evil Corp's efforts to evade sanctions imposed by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) for using Dridex to cause over $100 million in financial damages.

After being sanctioned by the U.S. government in 2019, ransomware negotiation firms refused to facilitate ransom payments for organizations hit by Evil Corp ransomware attacks to avoid facing legal action or fines from the U.S. Treasury Department.

Using other groups' malware also allows Evil Corp to distance themselves from known tooling to allow their victims to pay ransoms without facing risks associated with violating OFAC regulations.

Assuming a RaaS affiliate role would also likely allow its operators to expand the gang's ransomware deployment operations and its malware developers with enough free time and resources to develop new ransomware, which is harder to link to Evil Corp's previous operations.

Source: https://www.bleepingcomputer.com/news/security/microsoft-links-raspberry-robin-malware-to-evil-corp-attacks/