Microsoft Links Raspberry Robin USB Worm to Russian Evil Corp Hackers

thehackernews.com/2022/07/microsoft-links-raspberry-robin-usb.html

July 30, 2022

Microsoft on Friday disclosed a potential connection between the Raspberry Robin USB-based worm and an infamous Russian cybercrime group tracked as Evil Corp.

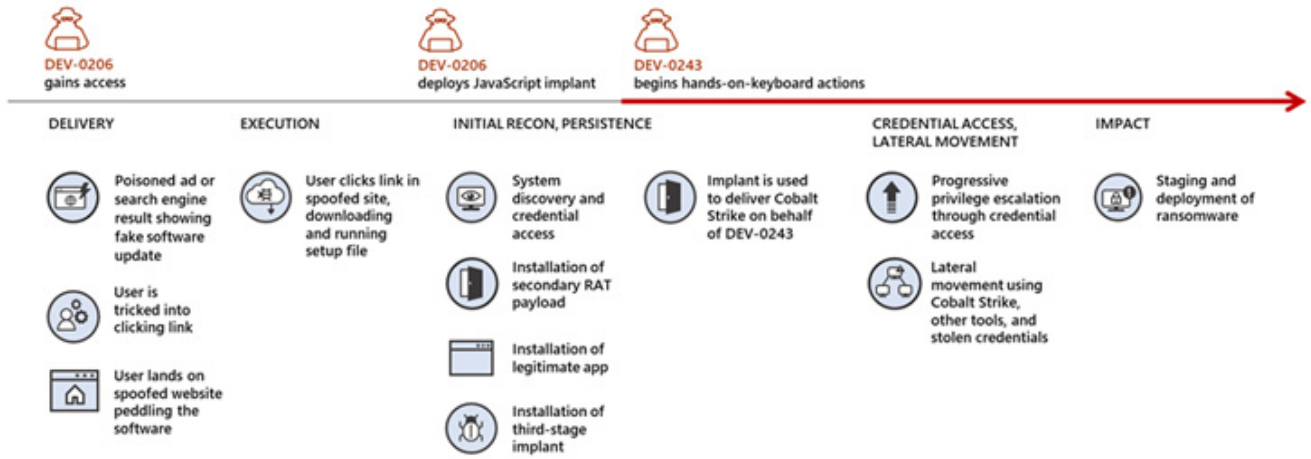
The tech giant said it observed the FakeUpdates (aka SocGholish) malware being delivered via existing Raspberry Robin infections on July 26, 2022.

Raspberry Robin, also called QNAP Worm, is known to spread from a compromised system via infected USB devices containing malicious a .LNK files to other devices in the target network.

The campaign, which was first spotted by Red Canary in September 2021, has been elusive in that no later-stage activity has been documented nor has there been any concrete link tying it to a known threat actor or group.

The disclosure, therefore, marks the first evidence of post-exploitation actions carried out by the threat actor upon leveraging the malware to gain initial access to a Windows machine.

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



DEV-0206 is Redmond's moniker for an initial access broker that deploys a malicious JavaScript framework called FakeUpdates by enticing targets into downloading fake browser updates in the form of ZIP archives.

The malware, at its core, acts as a conduit for other campaigns that make use of this access purchased from DEV-0206 to distribute other payloads, primarily Cobalt Strike loaders attributed to DEV-0243, which is also known as Evil Corp.

Referred to as Gold Drake and Indrik Spider, the financially motivated hacking group has historically operated the Dridex malware and has since switched to deploying a string of ransomware families over the years, including most recently LockBit.

"The use of a RaaS payload by the 'Evil Corp' activity group is likely an attempt by DEV-0243 to avoid attribution to their group, which could discourage payment due to their sanctioned status," Microsoft said.

It's not immediately clear what exact connections Evil Corp, DEV-0206, and DEV-0243 may have with one another.

Katie Nickels, director of intelligence at Red Canary, said in a statement shared with The Hacker News that the findings, if proven to be correct, fill a "major gap" with Raspberry Robin's modus operandi.

"We continue to see Raspberry Robin activity, but we have not been able to associate it with any specific person, company, entity, or country," Nickels said.

"Ultimately, it's too early to say if Evil Corp is responsible for, or associated with, Raspberry Robin. The Ransomware-as-a-Service (RaaS) ecosystem is a complex one, where different criminal groups partner with one another to achieve a variety of objectives. As a result, it can

be difficult to untangle the relationships between malware families and observed activity."

SHARE
SHARE