Ransomware criminals look to other hackers to provide them with network access

By Rene Millman

Published: 2021-06-17 · Archived: 2026-04-05 15:25:59 UTC

According to a new report, cyber criminals distributing ransomware are increasingly turning to other hackers to buy access into corporate networks.

Researchers at Proofpoint said a “robust and lucrative criminal ecosystem” exists where criminals work together to carry out ransomware attacks. In this ecosystem, ransomware operators buy access from independent cyber criminal groups who infiltrate major targets for part of the ransom proceeds.

“Cyber criminal threat groups already distributing banking malware or other trojans may also become part of a ransomware affiliate network,” said researchers.

The researchers tracked ten threat actors acting as initial access facilitators or likely ransomware affiliates. They also found there is not a one-to-one relationship between malware loaders and ransomware attacks. Instead, multiple threat actors use the same malware payloads for ransomware distribution.

Latest Videos From IT Pro

“Ransomware is rarely distributed directly via email,” the report said. “Just one ransomware strain accounts for 95 percent of ransomware as a first-stage email payload between 2020 and 2021.”

The hackers who offer access compromise organizations via first-stage malware like The Trick, Dridex, or Buer Loader. They will then sell their access to ransomware operators to deploy data theft and encryption operations.

Researchers said banking trojans – often used as ransomware loaders – represented 20% of malware seen in named campaigns in the first half of 2021, making it the most widespread malware type the company sees in the landscape.

Researchers also saw evidence of ransomware deployed via SocGholish, which uses fake updates and website redirects to infect users, and via the Keitaro traffic distribution system (TDS) and follow-on exploit kits that operators use to evade detection.

In the course of investigations into this ecosystem, researchers tracked several hackers operating as initial access facilitators.

TA800 is a large cyber crime actor Proofpoint has tracked since mid-2019. This threat actor attempts to deliver and install banking malware or malware loaders including The Trick, BazaLoader, Buer Loader, and Ostap.

TA577 is a prolific cyber crime threat actor Proofpoint has tracked since mid-2020. This actor conducts broad targeting across various industries and geographies. Proofpoint has observed TA577 deliver payloads including Qbot, IcedID, SystemBC, SmokeLoader, Ursnif, and Cobalt Strike. Researchers said that TA577 is associated with the March 2021 Sodinokibi ransomware infection.

According to researchers, with the US government proposing new efforts to combat ransomware, “it is possible with new disruptive efforts focused on the threat and growing investments in cyber defense across supply chains, ransomware attacks will decrease in frequency and efficacy.”

Source: https://www.itpro.com/security/ransomware/359919/ransomware-criminals-look-to-other-hackers-to-provide-them-with-network