Ransomware Attackers Partnering With Cybercrime Groups to Hack High-Profile Targets

By The Hacker News

Published: 2021-06-16 · Archived: 2026-04-05 12:49:24 UTC

As ransomware attacks against critical infrastructure skyrocket, new research shows that threat actors behind such disruptions are increasingly shifting from using email messages as an intrusion route to purchasing access from cybercriminal enterprises that have already infiltrated major targets.

"Ransomware operators often buy access from independent cybercriminal groups who infiltrate major targets and then sell access to the ransomware actors for a slice of the ill-gotten gains," researchers from Proofpoint said in a write-up shared with The Hacker News.

"Cybercriminal threat groups already distributing banking malware or other trojans may also become part of a ransomware affiliate network."

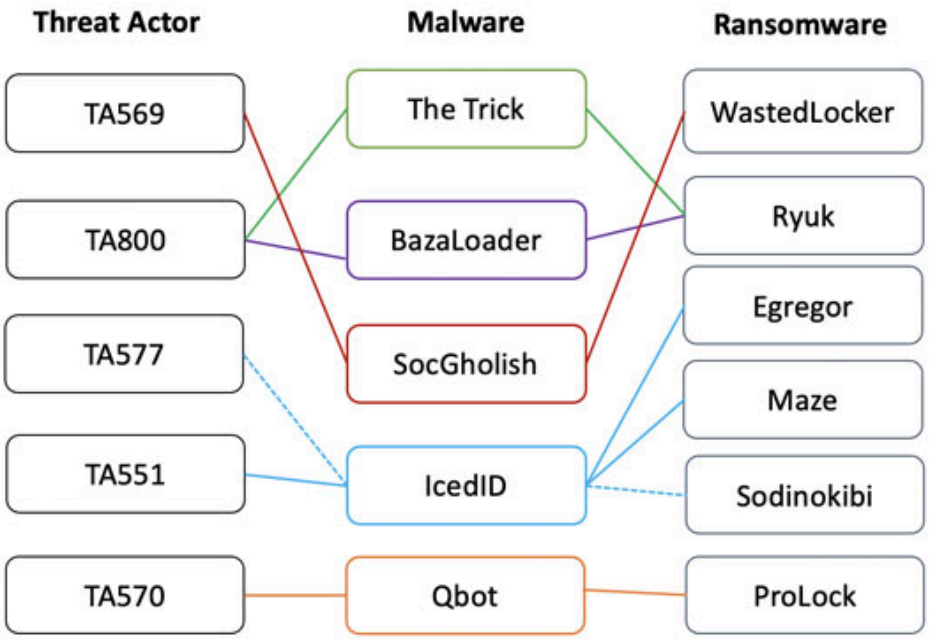
Besides angling for a piece of the illegal profits, the email and cloud security firm said it is currently tracking at least 10 different threat actors who play the role of "initial access facilitators" to supply affiliates and other cybercrime groups with an entry point to deploy data theft and encryption operations.

Initial access brokers are known to infiltrate the networks via first-stage malware payloads such as The Trick, Dridex, Qbot, IcedID, BazaLoader, or Buer Loader, with most campaigns detected in the first half of 2021 leveraging banking trojans as ransomware loaders.

The brokers — which were identified by tracking the backdoor access advertised on hacking forums — include TA800, TA577, TA569, TA551 (Shathak), TA570, TA547, TA544 (Bamboo Spider), TA571, TA574, and TA575, with overlaps observed between various threat actors, malware, and ransomware deployments.

For example, both TA577 and TA551 have been found to use IcedID as an initial access payload to deliver Egregor, Maze, and REvil ransomware, while TA800 has employed BazaLoader to deploy Ryuk on targeted systems.

In a hypothetical attack chain, a threat actor could send an email with a malware-infected Office document, which, when opened, drops the first-stage payload to maintain persistent backdoor access. This access can then be sold to a second threat actor, who exploits it to deploy a Cobalt Strike beacon to pivot laterally across the broader network and deploy the ransomware.



That said, attacks that rely on email messages to directly distribute ransomware in the form of malicious attachments or embedded hyperlinks continue to remain a threat, albeit at lower volumes. Proofpoint noted that it identified 54 ransomware campaigns distributing a little over one million messages over the past year.

"Short dwell times, high payouts, and collaboration across cybercriminal ecosystems have led to a perfect storm of cybercrime that the world's governments are taking seriously," the researchers concluded. "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."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
