Alleged Members of Egregor Ransomware Cartel Arrested

trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html

March 26, 2021

Ransomware

Trend Micro served as one of the cybersecurity partners of law enforcement authorities involved in the investigation.

By: Trend Micro March 26, 2021 Read time: (words)

Content added to Folio

Three alleged members of the Egregor ransomware cartel were apprehended in Ukraine in a crackdown conducted by the French and Ukrainian authorities last month. The arrests were also made possible with the help of private-public sector partnerships, which include Trend Micro.

About Egregor ransomware

Since its first appearance in September 2020, Egregor ransomware has been involved in high-profile attacks against retailers, human resource service companies, and other organizations. It operated under the ransomware-as-a-service (RaaS) model where groups sell or lease ransomware variants to affiliates, making it relatively easier even for inexperienced cybercriminals to launch attacks. Like some prominent ransomware variants, Egregor employs a “double extortion” technique where the operators threaten affected users with both the loss and public exposure of the encrypted data.

The ransomware is typically distributed as a secondary payload to remote access trojans such as QAKBOT. It also spreads through phishing emails with malicious attachments or via remote desktop protocol (RDP) or VPN exploits.

Further details on the arrests

French law enforcement initiated the investigation on the Egregor operators after the latter launched attacks on several France-based companies for logistics, newspaper publication, and video game development. The three suspects were arrested after French authorities tracked them down with the help of Ukrainian authorities. The names and the exact designations of the arrestees have not been released.

In an email interview with The Record about the incident, François B., the Head of the Computer Security Incident Response Team for the French Judicial Police (CSIRT-PJ), cited partnerships with cybersecurity and incident response companies including Trend Micro. He noted that these organizations help in active investigations as they “provide us with the most accurate information on an ongoing case, tools, or threat intelligence data.”

Protecting systems against ransomware

Ransomware is a persistent security problem that unceasingly and rapidly evolves into an even more destructive threat. To protect systems from ransomware, users are advised to follow these best practices:

- Avoid downloading attachments and clicking on links in emails from unverified sources.
- Regularly patch and update operating systems, programs, and software.
- Periodically back-up files by observing the 3-2-1 rule: Create at least three copies of the data, store it in two different formats, and keep at least one duplicate offsite.

Security solutions such as Trend Micro XDR^{TM} also offer protection across different components of the system, including email, endpoints, servers, cloud workloads, and networks. By collecting and correlating data in all these layers, security and IT teams gain a better context of attacks that otherwise may seem insignificant on their own. This allows faster and more accurate detections.