Modern Ransomware Shakes Up Banking, Government, Transportation Sectors in 1H 2021

This ransomware report collates detections from the different static and dynamic layers from over 20 industries. Based on detections from the last six months, ransomware operators have turned their attention to critical industries — namely the banking, government, and transportation (BGT) sectors.

Key highlights:

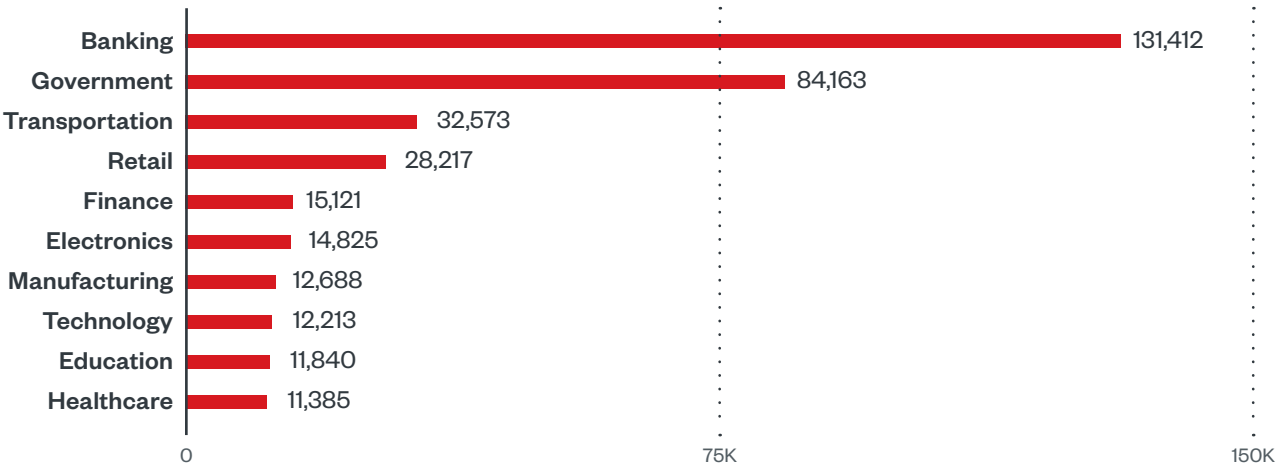
- Trend Micro data showed the banking, government, and transportation industries with the most ransomware detections across over 20 industries in 1H 2021. Modern ransomware, particularly REvil, was consistently present in the list of top ransomware detections in the top three industries.
- Ransomware detections in banking: over 131,000 detections were recorded, with the Americas having the most at over 122,000. REvil and Crysis, which have been used in modern ransomware attacks, have been highly detected in this industry in the first half of the year.
- Ransomware detections in government: over 84,000 ransomware detections were recorded, with Africa having the most at over 30,000. REvil, and Crysis are modern ransomware families that have been highly detected in this industry in the first half of the year.
- Ransomware detections in transportation: over 32,000 ransomware detections were recorded, with Africa having the most at over 27,000. REvil, Conti, Ryuk, and DarkSide are modern ransomware families that have been highly detected in this industry in the first half of the year.
- Being the common threat that plagues the banking, government, and transportation industries, organizations should be aware of how REvil typically gains a foothold into networks. REvil's common attack vectors include spear-phishing emails, unpatched vulnerabilities, compromised websites, and valid credentials that are either stolen or sold in the underground.
- In addition to the costs of paying the ransom without the assurance of data and systems being restored, the real costs of an attack continue to pile up even after the compromise. Companies' operations downtime (which averages $300,000 per hour for enterprises), regulatory fines, litigation settlements, and customer attrition are just some of the losses that add to recovery expenses

Overview of ransomware detections in 1H 2021

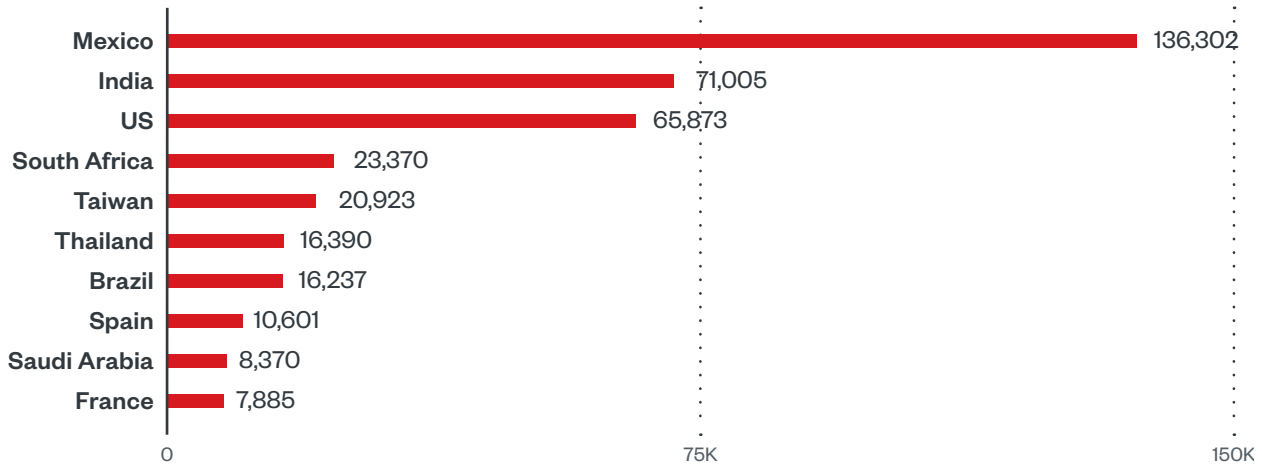
Total ransomware detections:

3,600,439

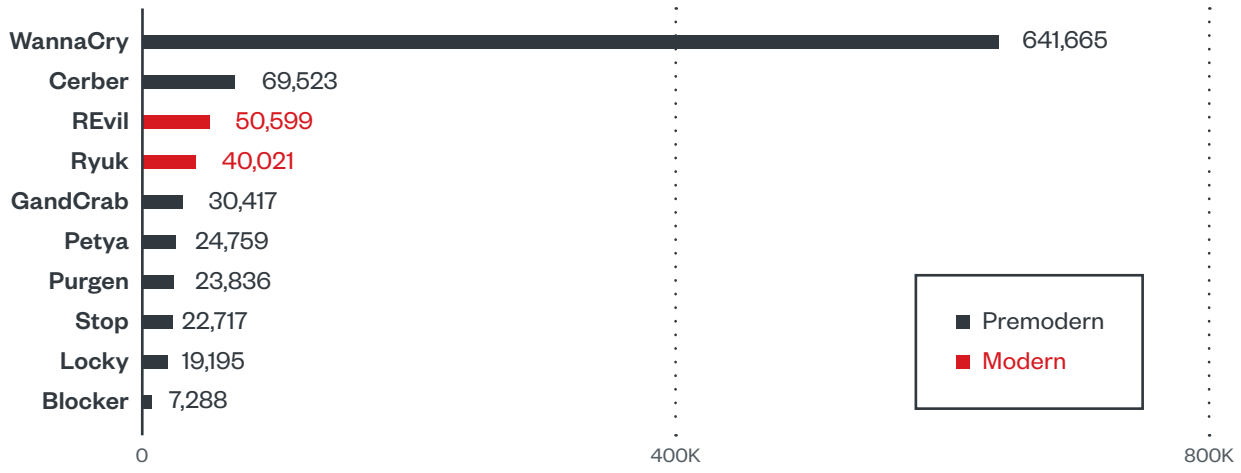
Modern Ransomware Shakes Up Banking, Government, Transportation Sectors in 1H 2021



Top 10 industries with the most ransomware detections in 1H 2021



Top 10 countries with the most ransomware detections



Top ransomware families in 1H 2021

Trend Micro Vision One™ and **Trend Micro Apex One™** offer next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, and provides multilayered protection and behavior detection. **Trend Micro Cloud One™ Workload Security** protects systems against both known and unknown threats that exploit vulnerabilities, providing up-to-date, real-time protection. **Trend Micro™ Deep Discovery™ Email Inspector** employs custom sandboxing and advanced analysis techniques to effectively block ransomware before it gets into the system.

TREND MICRO™ | research