

2 December 2021

Ransomware, carding, and initial access brokers:

Group-IB presents report on trending crimes

CYBERCRIMECON

THREAT RESEARCH

Group-IB, one of the global cybersecurity leaders, has presented its research into global cyberthreats in the report [Hi-Tech Crime Trends 2021/2022](#) at its annual threat hunting and intelligence conference, [CyberCrimeCon](#)<sup>21</sup>. In the report, which explores cybercrime developments in H2 2020—H1 2021, Group-IB researchers analyze the increasing complexity of the global threat landscape and highlight the ever-growing role of alliances between threat actors. The trend manifests itself in partnerships between ransomware operators and initial access brokers under the Ransomware-as-a-Service model. Scammers also band together in clans to automate and streamline fraudulent operations. Conversely, individual cybercrimes such as carding are in decline for the first time in a while.

For the 10<sup>th</sup> consecutive year, the Hi-Tech Crime Trends report analyzes the various aspects of the cybercriminal industry's operations, examines attacks, and provides forecasts for the threat landscape for various sectors. For the first time, the report was divided into five major volumes, all with a different focus: ransomware, the sale of access to corporate networks, cyberwarfare, threats to the financial sector, and phishing and scams. The forecasts and recommendations outlined in Hi-Tech Crime Trends 2020-2021 seek to prevent damage and downtime for companies worldwide.

Initial access brokers: US companies among the most frequent targets

One of the underlying trends on the cybercrime arena is a sharp increase in the number of offers to sell access to compromised corporate networks. Pioneered by the infamous hacker [Fxnsp](#), who was charged by the US Department of Justice in 2020, the market of corporate initial access grow by almost 16% in H2 2020—H1 2021, from \$6,189,388 to \$7,165,387. The number of offers to sell access to companies almost tripled over the review period: from 362 to 1,099. This exclusive data was obtained by Group-IB's Threat Intelligence & Attribution system, which gathers even deleted information from cybercriminal underground forums.

