(i)

About Group-IB → Media Center → Press Releases

2 December 2021

Ransomware, carding, and initial access brokers: Group-IB presents report on trending crimes

CYBERCRIMECON THREAT RESEARCH

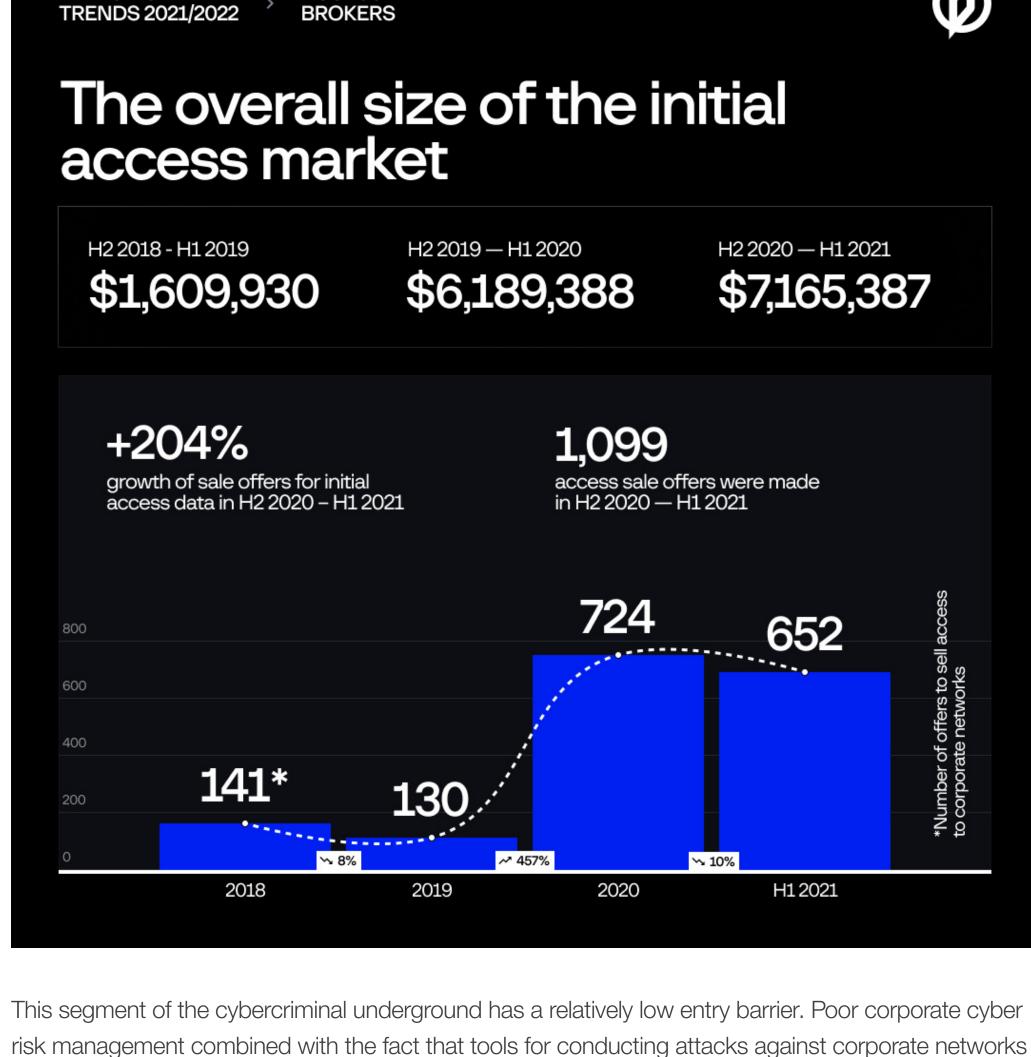
Group-IB, one of the global cybersecurity leaders, has presented its research into global cyberthreats in the report Hi-Tech Crime Trends 2021/2022 at its annual threat hunting and intelligence conference, CyberCrimeCon'21. In the report, which explores cybercrime developments in H2 2020—H1 2021, Group-IB 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.

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

For the 10th consecutive year, the Hi-Tech Crime Trends report analyzes the various aspects of the

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 Fxmsp, who was charged by the US Department of Justice in 2020, the market of corporate initial access grew

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. HI-TECH CRIME ACCESS

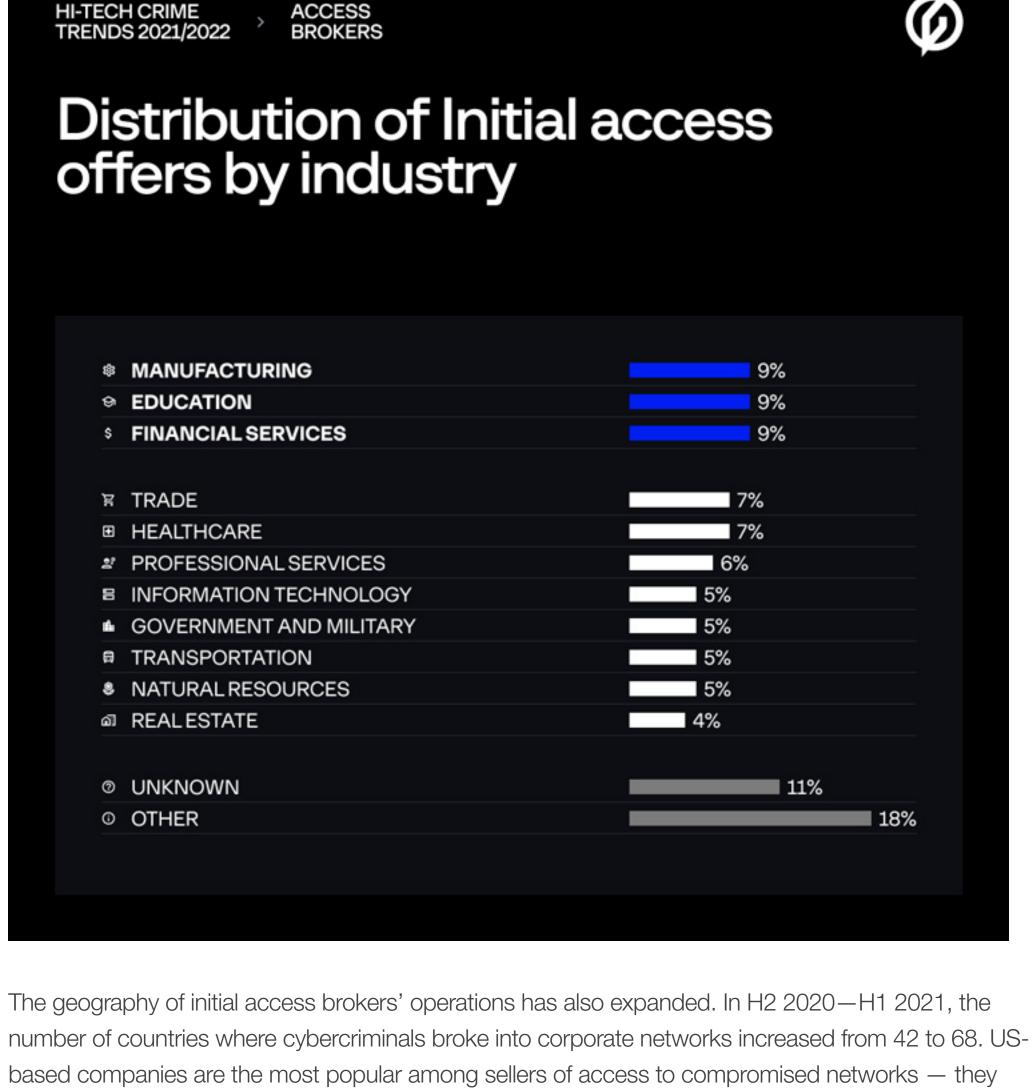


2020—H1 2021, however, this number skyrocketed to 262, with 229 new players joining the roster. Most companies affected belonged to the manufacturing (9% of all companies), education (9%), financial services (9%), healthcare (7%), and commerce (7%). In the review period, the number of industries exploited by initial access brokers surged from 20 to 35, which indicates that cybercriminals are becoming aware of the variety of potential victims.

are widely available both contributed to a record-breaking rise in the number of initial access brokers.

In H2 2019—H12020, the Group-IB Threat Intelligence team detected only 86 active brokers. In H2

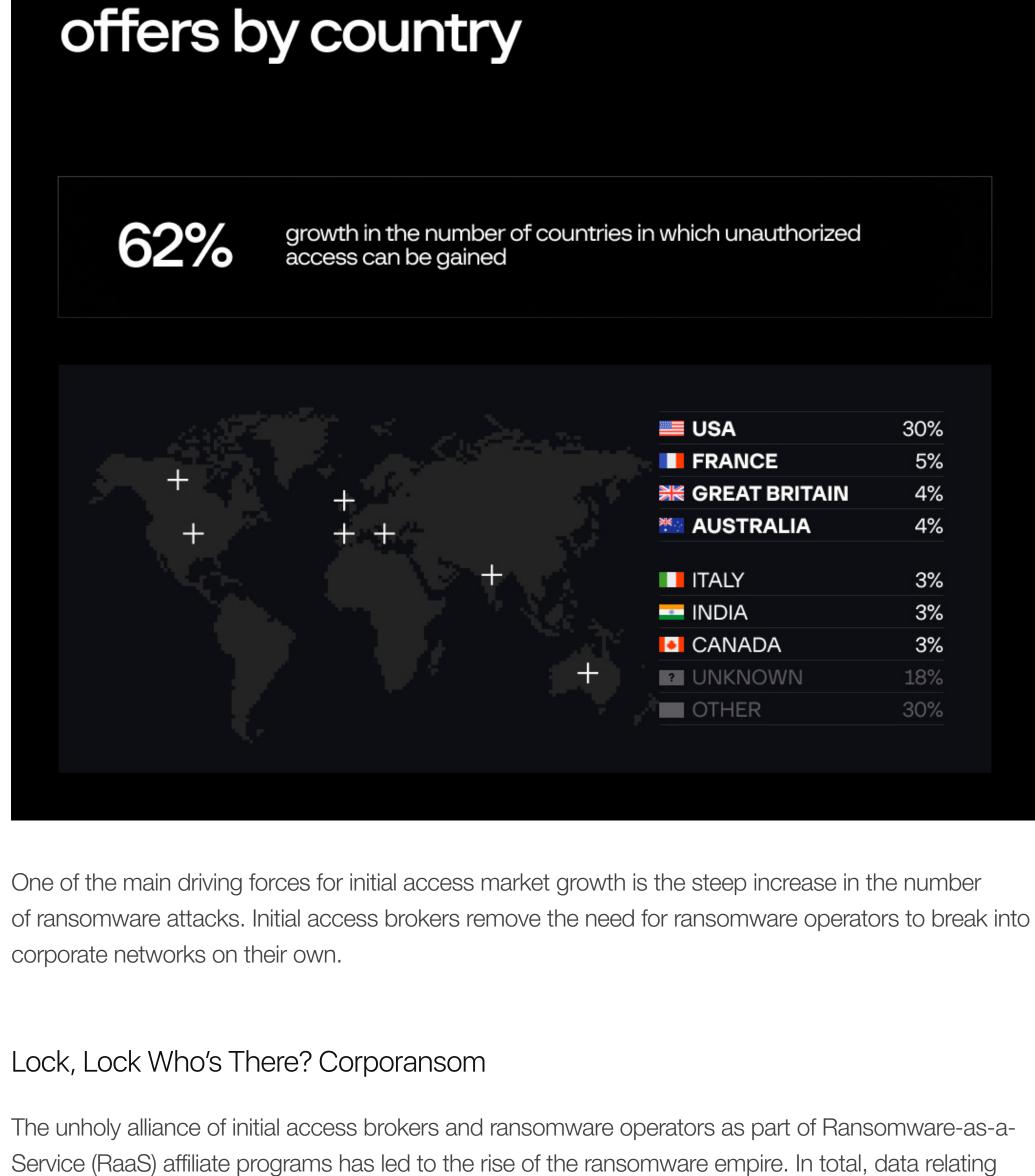
HI-TECH CRIME ACCESS BROKERS TRENDS 2021/2022



HI-TECH CRIME ACCESS BROKERS TRENDS 2021/2022 Distribution of initial access

account for 30% of all victim-companies in H2 2020—H1 2021, followed by France (5%), and the UK

(4%).



Thanks to the Threat Intelligence & Attribution system, Group-IB researchers were able to trace how the ransomware empire has evolved since it appeared. Group-IB's team analyzed private Ransomware affiliate programs, DLSs where they post exfiltrated data belonging to victims who refused to pay the

is an increase of an unprecedented 935% compared to the previous review period, when data relating

to 2,371 companies were released on DLSs (Data Leak Sites) over H2 2020-H1 2021. This

to 229 victims was made public.

and Pysa (123).

ransom, and the most aggressive ransomware strains.

programs, which is a 19% increase compared to the previous period. During the review period, the cybercriminals mastered the use of DLSs, which are used as an additional source of pressure on their victims to make them pay the ransom by threatening to leak their data. In practice, however, victims can still find their data on the DLS even if the ransom is paid. The number of new DLSs more than doubled during the review period and reached 28, compared to 13 in H2 2019—H1 2020.

It is noteworthy that in the first three quarters of 2021, ransomware operators released 47% more data

on attacked companies than in the whole of 2020. Taking into account that cybercriminals release data

relating to only about 10% of their victims, the actual number of ransomware attack victims is likely

Over the review period, Group-IB analysts identified 21 new Ransomware-as-a-Service (RaaS) affiliate

to be dozens more. The share of companies that pay the ransom is estimated at 30%. Having analyzed ransomware DLSs in 2021, Group-IB analysts concluded that Conti was the most aggressive ransomware group: it disclosed information about 361 victims (16.5% of all victimcompanies whose data was released on DLSs), followed by Lockbit (251), Avaddon (164), REvil (155), and Pysa (118). Last year's top 5 was as follows: Maze (259), Egregor (204), Conti (173), REvil (141),

Country-wise, most companies whose data was posted on DLSs by ransomware operators in 2021

affected belonged to the manufacturing (9.6%), real estate (9.5%), and transportation industries (8.2%).

were based in the United States (968), Canada (110), and France (103), while most organizations

Over the review period, the carding market dropped by 26%, from \$1.9 billion to \$1.4 billion compared to the previous period. The decrease can be explained by the lower number of dumps (data stored on the magnetic stripe on bank cards) offered for sale: the number of offers shrank by 17%, from

70 million records to 58 million, due to the infamous card shop Joker's Stash shutting down.

Meanwhile, the average price of a bank card dump fell from \$21.88 to \$13.84, while the maximum

An opposite trend was recorded on the market for the sale of bank card text data (bank card numbers,

expiration dates, names of owners, addresses, CVVs): their number soared by 36%, from 28 million

records to 38 million, which amongst others can be explained by the higher number of phishing web resources mimicking famous brands during the pandemic. The average price for text data climbed from \$12.78 to \$15.2, while the maximum price skyrocketed 7-fold: from \$150 to an unprecedented \$1,000.

price surged from \$500 to \$750.

Carding: The Joker's Last Laugh

The Scamdemic Another cohort of cybercriminals actively forging partnerships over the review period were scammers. In recent years, phishing and scam affiliate programs have become highly popular. The research conducted by Group-IB revealed that there are more than 70 phishing and scam affiliate programs.

Participants aim to steal money as well as personal and payment data. In the reporting period, the

threat actors who took part in such schemes pocketed at least \$10 million in total. The average

amount stolen by a scam affiliate program member is estimated at \$83. Affiliate programs involve large numbers of participants, have a strict hierarchy, and use complex technical infrastructures to automate fraudulent activities. Phishing and scam affiliate programs actively use Telegram bots that provide participants with ready-to-use scam and phishing pages. This helps scale phishing campaigns and tailor them to banks, popular email services, and other organizations.

Phishing and scam affiliate programs, initially focused on Russia and other CIS countries, recently

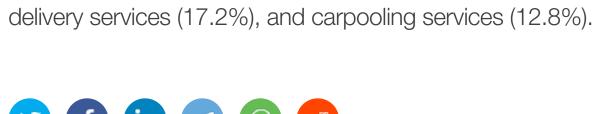
by Classiscam: an automated scam-as-a-service designed tosteal money and payment data. Group-IB

is aware of at least 71 brands from 36 countries impersonated by affiliate program members. Phishing

and scam websites created by affiliate program members most often mimic marketplaces (69.5%),

started their online migration to Europe, America, Asia, and the Middle East. This is exemplified

y f in √ (S) ⊕

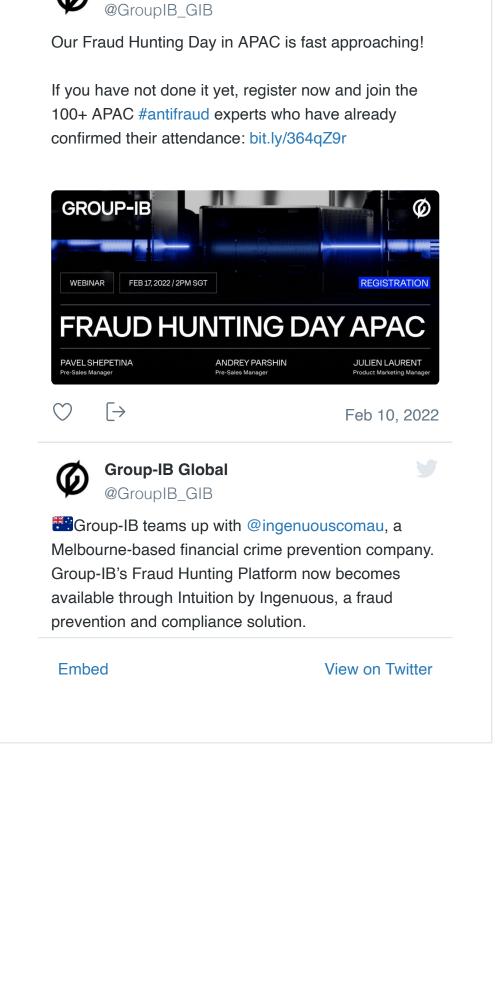


Group-IB is one of the leading providers of solutions dedicated to detecting and Group-IB's technological leadership and R&D capabilities are built on the company's preventing cyberattacks, identifying online fraud, investigation of high-tech crimes and 18 years of hands-on experience in cybercrime investigations worldwide and intellectual property protection, headquartered in Singapore. The company's threat 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory, high-tech crime investigations department, and round-the-clock intelligence and research centers are located in the Middle East (Dubai), the Asia-Pacific (Singapore), Europe (Amsterdam), and Russia (Moscow). CERT-GIB. Group-IB is a partner of Europol.

Group-IB's Threat Intelligence & Attribution system has been named one of the best Group-IB's experience in threat hunting and cyber intelligence has been fused into in class by Gartner, Forrester, and IDC. Group-IB's Threat Hunting Framework (earlier an ecosystem of highly sophisticated software and hardware solutions designed known as TDS) intended for the proactive search and the protection against complex to monitor, identify, and prevent cyberattacks. Group-IB's mission is to fight highand previously unknown cyberthreats has been recognized as one of the leaders in Network Detection and Response by the leading European analyst agency KuppingerCole Analysts AG, while Group-IB itself has been recognized as a Product Leader and Innovation Leader. Gartner identified Group-IB as a Representative Vendor in Online Fraud Detection for its Fraud Hunting Platform. In addition, Group-IB was granted Frost & Sullivan's Innovation Excellence award for its Digital Risk Protection (DRP), an Al-driven platform for identifying and mitigating digital risks and

tech crime while protecting our clients in cyberspace and helping them achieve their goals. To do so, we analyze cyber threats, develop our infrastructure to monitor them, respond to incidents, investigate complex high-tech crimes, and design unique technologies, solutions, and services to counteract adversaries.

Response



Tweets by @GroupIB_GIB

Group-IB Global





counteracting brand impersonation attacks with the company's patented technologies at its core. Company Products Services overview Resources About Group-IB Threat Research Threat Intelligence & Prevention Attribution Leadership

Protection

CERT-GIB Security Assessment Red Teaming Incident Response Incident Response Compliance Audit Retainer Pre-IR Assessment Compromise Assessment Cyber Education

GIB Crypto

Investigation

Investigations

Digital Forensics

eDiscovery

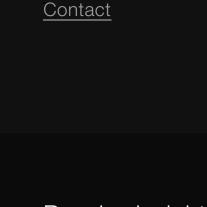
Amsterdam

+31 20 226-90-90

Kuala Lumpur

Financial Forensics

Investigation Subscription



Business Email

Terms of Use

Partners

<u>Program</u>

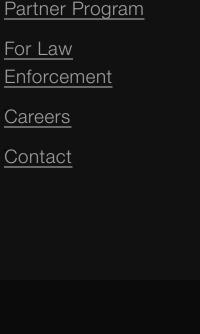
For Law

Careers

Enforcement

Reseller Partner

MSSP & MDR

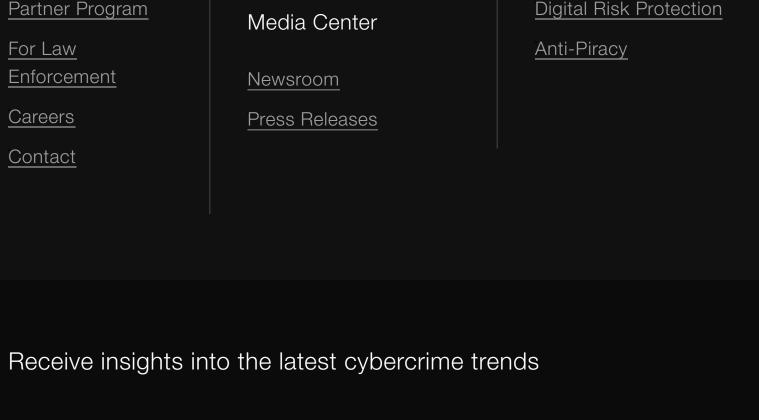




I understand and agree that my personal data will be

collected and processed according to the Privacy and

Cookies Policy and unconditionally agree and accept the



Threat Hunting Framework

Atmosphere: Cloud Email

Fraud Hunting Platform



© 2003 – 2021 Group-IB is a global leader in attribution-based threat intelligence, best-in-class threat hunting, fraud prevention, and cybercrime investigations.

SUBSCRIBE

