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

Amsterdam, 02/12/2021 — 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.

For the 10th 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: European 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 **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.

This segment of the cybercriminal underground has a relatively low entry barrier. Poor corporate cyber risk management combined with the fact that tools for conducting attacks against corporate networks are widely available both contributed to a record-breaking rise in the number of initial access brokers. In H2 2019–H1 2020, the Group-IB Threat Intelligence team detected only **86** active brokers. In H2 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.

The geography of initial access brokers' operations has also expanded. In H2 2020–H1 2021, the number of countries where cybercriminals broke into corporate networks increased from **42** to **68**. **US-based companies** are the most popular among sellers of access to compromised networks — they account for **30%** of all victim-companies in H2 2020–H1 2021, followed by **France (5%)**, and **the UK (4%).**

In Europe alone, the total cost of all the accesses to the region's companies offered for sale in the underground totaled **$590,095** in the review period, which is nearly a **22%** decrease year-on-year.Over the review period, initial access brokers offered access to **261 European companies**, which is a 3-fold increase compared to H2 2019 — H1 2020 (**76** companies). **French companies** were the most popular lot for sellers of access to compromised networks – they accounted for **20%** of all victim-companies in H2 2020 — H1 2021 in Europe, followed by **the UK (18%)**, **Italy (13%)**, **Spain (10%)**, **Germany (9%)**, and **the Netherlands (5%).**

One of the main driving forces for initial access market growth is the steep increase in the number of ransomware attacks. Initial access brokers remove the need for ransomware operators to break into corporate networks on their own.

Lock, Lock Who's There? Corporansom

The unholy alliance of initial access brokers and ransomware operators as part of Ransomware-as-as-a-Service (RaaS) affiliate programs has led to the rise of the ransomware empire. In total, data relating to **2,371** companies were released on DLSs (Data Leak Sites) over H2 2020–H1 2021. This is an increase of an unprecedented **935%** compared to the previous review period, when data relating to **229** victims was made public.

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 ransom, and the most aggressive ransomware strains.

Over the review period, Group-IB analysts identified **21** new Ransomware-as-a-Service (RaaS) affiliate 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 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 victim-companies 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), and Pysa (123).

Country-wise, most companies whose data was posted on DLSs by ransomware operators in 2021 were based in the United States (**968**), Canada (**110**), and France (**103**), while most organizations affected belonged to the manufacturing (**9.6%**), real estate (**9.5%**), and transportation industries (**8.2%**).

In 2021, **Europe** became the second most frequently region targeted by ransomware with data on **598** local companies published only DLS after North America (1,213). This year's "leaders" in Europe are **France (data on 103 companies on DLS)**, **the UK (92)**, **Italy (76)**, **Germany (72),** and **Spain (42).**

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 started their online migration to Europe, America, Asia, and the Middle East. This is exemplified by Classiscam: an automated scam-as-a-service designed to steal 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 create by affiliate program members most often mimic marketplaces **(69.5%),** delivery services (**17.2%)**, and carpooling services **(12.8%)**.

Carding: The Joker's Last Laugh

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 price surged from **$500** to **$750**.

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**.

In **Europe** specifically, the carding market dropped by **46%** from **$219.1 million** to **$118.6 million** in the review period. The total number of compromised payments cards issued by European banks traded in the underground also decreased from **7,605,022** in H2 2019 – H1 2020 to **5,911,921** over the

review period. This was accompanied by the increase in the average price of text card data from **$15.16** to **$18.94** and a dramatic drop in the price of a card dump from **$77.29** to **$27.22**.

About Group-IB

Group-IB is one of the leading solutions providers dedicated to detecting and preventing cyberattacks, identifying online fraud, investigating high-tech crimes and intellectual property protection, headquartered in Singapore. The company's threat intelligence and research centers are located in the Middle East (Dubai), the Asia-Pacific (Singapore), Europe (Amsterdam), and Russia (Moscow).

Group-IB's Threat Intelligence & Attribution system has been named one of the best in class by Gartner, Forrester, and IDC. Group-IB's Threat Hunting Framework intended for the proactive search and the protection against complex and 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, an Al-driven platform for identifying and mitigating digital risks and counteracting brand impersonation attacks with the company's patented technologies at its core.

Group-IB's technological leadership and R&D capabilities are built on the company's 18 years of hands-on experience in cybercrime investigations worldwide and 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory, high-tech crime investigations department, and round-the-clock CERT-GIB. Group-IB is an active collaborator in global investigations led by international law enforcement organizations, such as Europol and INTERPOL. Group-IB is also a member of the Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security created in order to foster closer cooperation between Europol and its leading non-law enforcement partners.

Group-IB's experience in threat hunting and cyber intelligence has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyberattacks. Group-IB's mission is to fight high-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.