# Group-IB presented latest cybercrime trends in Asia


**Hong Kong, Nov 19, 2018 (**Issuewire.com**)** - **Group-IB,** an international company that specializes in preventing cyber attacks, presented the findings of its latest Hi-Tech Crime Trends 2018 report at the FinTech Security Conference in Hong Kong organized by Binary Solutions Limited in partnership with Group-IB.

According to Group-IB's report findings, Asia is one of the most actively attacked regions in the world. Over the past year, 21 state-sponsored Groups were detected in the area, which is more than in Europe and the US combined. Hong Kong, Singapore, Seoul, and Shanghai, and many other financial powerhouses in Asia are likely to become primary targets of financially motivated hacker groups in the near future.

"Cyber trends and threats that we identified in the world are likely to occur in Asia. Asia's rapid economic growth has ramped up the interest of financially motivated hackers and state-sponsored hacker groups. Local banks have already been attacked by advanced hacker groups several times; we expect this trend to increase," – **comments Dmitry Volkov, Group-IB CTO**. The threats that are notable for the Asian region are represented by a significant number of attacks aimed at manufacturing

of chips, microprocessors and system control boards of different IT vendors, whose principal manufacturing operations are located in Asia. The attackers' research vector is now shifting from software vulnerabilities to those located at the hardware and firmware level. To exploit certain hardware vulnerabilities, hackers can simply run a JavaScript code, as in the case of Glitch vulnerability. It is very difficult, if not impossible to eliminate these vulnerabilities with software updates and as such, they create new opportunities for cybercriminals. It is likely that in the space of a few years they will seriously affect the cyber security market."

Since the beginning of 2018, Group-IB experts detected that cybercriminals were seeking to get access to the user databases of Hong Kong state Internet portals responsible for taxes, trade, procurement, logistics, innovations, and hi-tech infrastructure.

**Espionage and as one of the main APT groups' goals**

The threat landscape for critical infrastructures is growing more complex, provoked by the activity of state-sponsored threat actors, who are seeking to establish a sustained presence within critical infrastructure networks for long-term espionage or sabotage. These groups target companies in the energy, financial, aviation, water sectors etc. Banks are considered to be an integral part of critical infrastructure. Which is why the availability of tools and experience in disrupting bank systems are now priorities for attackers. Such tools are actively used by two groups in particular: BlackEnergy and Lazarus.

To infiltrate critical infrastructure networks hackers will continue to use phishing as one of their main tools, but the focus of attacks may shift to vulnerable network equipment connecting the network to the Internet. APT groups will keep investing heavily in the development and acquisition of zero-day exploits, according to Group-IB's forecasts.  Another trend Group-IB experts identified is networked compromise through key personnel's home networks and personal devices. Increasingly often, state-sponsored hackers are focusing on vulnerabilities in home routers. This allows them to not only spy on users without infecting their devices, but also maintain a more extensive and dynamic infrastructure and remain unnoticed.

Group-IB's new report features the activity of roughly **40 state-sponsored groups** around the world, **21** one of which were most active in Asia-Pacific, including the Infamous North-Korean Lazarus group. For some of the hacker groups detected, the country of origin is yet to be established. The attribution is sometimes complicated by the fact that some groups may imitate other groups' unique features to throw researchers off track.

**Attacks on Crypto**

In 2017-2018 hackers' interest in cryptocurrency exchanges ramped up. Thirteen exchanges were hacked in 2017 and in the first three quarters of 2018, amounting to a total loss of $877 million. Thus, 60% of the total amount was stolen from Coincheck, a Japanese cryptocurrency exchange. Silence, MoneyTaker and Cobalt are likely to conduct new attacks on crypto exchanges.

A relatively new method of fraud on the ICO market was stealing a White Paper of ICO project and presenting an identical idea under a new brand name. Spear phishing remains the major vector of attack: approximately 56% of all money siphoned off from ICO were stolen using phishing.

In 2018 Group-IB detected five successful “51% attacks” when attackers take control over at least 51% of mining power. Having 51% of computing power, the attackers create a stealthy alternative blockchain to confirm their own transactions. In 2018 the direct financial losses from these attacks amounted to almost $20 million.

**Attacks on banks and their clients**

Advanced hacker groups that Group-IB identifies as most dangerous to the banking sector all over the world are Lazarus, MoneyTaker, Cobalt, and Silence. The three latter are led by Russian-speaking hackers. All these groups are able to not only penetrate a bank’s network and access isolated financial systems, but also withdraw money via SWIFT, card processing systems, and ATMs. The Lazarus group will continue to attack banks and steal funds via SWIFT. They will likely experiment with attacks on card processing, primarily focusing on Asia and the Pacific. New cybercrime is also expected to start operations in Asia and Latin America.

The number of attacks via SWIFT increased dramatically over the reviewed period. In the previous period, three such attacks were tracked – in Hong Kong, Ukraine, and Turkey. In this period, however, 9 successful attacks have already taken place in Nepal, Taiwan, Russia, Mexico, India, Bulgaria, and Chile. Only two hacker groups target the SWIFT interbank transfer system: Lazarus and Cobalt. The average volume of theft attempt via SWIFT is estimated **at $26 million**.

Group-IB marked the six new PC Trojans that appeared internationally: IcedID, BackSwap, DanaBot, MnuBot, Osiris и Xbot. Web phishing, which is another popular attack vector, has grown globally. The financial phishing is, predictably, mainly targeting US-based companies. The corresponding share of financial phishing webpages is 26%. France and Germany are second and third, respectively, in this ranking. Among all phishing resources, 73% can be divided into the following categories: cloud storages (28%), financial platforms (26%), and online services (19%).

During the last year, Group-IB Threat Intelligence detected 27 million cards uploaded to card shop. The company’s records indicate that dumps account for 62% of data sold, which means that POS Trojans are the main method of compromising plastic cards. Unlike dumps, text data is sold much cheaper in card shops: its total value amounted to $95,6 million, accounting for only 17% of the overall market value, compared to 19,9 million dumps, which cost as much as $567,8 million.

**Group-IB in Asia**

Group-IB is not a stranger to the region. It has recently announced the opening of the Global HQ in Singapore by the end of 2018, where Group-IB will manage and keep developing its global threat-hunting infrastructure aimed at adversary-centric detection and proactive threat hunting. Group-IB’s portfolio of clients in Asia includes banks, financial and government organizations in Singapore, Thailand and other countries. Southeast Asia accounts for more than 30% of the company’s international revenue.

**About Group-IB**

Group-IB is a leading provider of solutions aimed at detection and prevention of cyber attacks, online fraud, and IP protection. GIB Threat Intelligence system was named one of the best in class by Gartner, Forrester, and IDC. Group-IB’s technological leadership is built on company’s fifteen years of hands-on

experience in cybercrime investigations all over the world and 55 000 hours of cyber security incident response accumulated in the largest forensic laboratory in Eastern Europe and a round-the-clock center providing a rapid response to cyber incidents—CERT-GIB. Group-IB is a partner of INTERPOL, Europol, and a cybersecurity solutions provider, recommended by SWIFT and OSCE.

**About Dragon Advance Tech**

Dragon Advance Tech has been protecting our customers from the most advanced and sophisticated attacks in the world, attacks that are usually not detected by anti-virus software nor stopped by firewalls. Our capabilities in malware analysis and reverse engineering, augmented by industry-leading threat intelligence, have enabled us to become one of the most preferred cybersecurity and incident response service providers in the Asia Pacific region.

**About Binary Solutions**

Binary Solutions helps clients ensure that their entire business information system is trusted and secure, from the physical space to the digital space. In the event that a company's security is compromised, such as a cyber attack or a data leak, we provide instant and effective solutions to contain and tackle the problem.

Our trusted consultants come from a variety of professional backgrounds and have decades of experience in different industries. We provide clients with comprehensive and up-to-date technical and investigative expertise, with proven track records of protecting our clients' businesses. In short, we help protects our customers' secret, and we find out the bad guys if bad things happened.

**Media Contact**

Group-IB

yarmak@group-ib.com

Source : Group-IB