Group-IB: hackers hit hard SEA and Singapore in 2018

Singapore, 19.03.2019 – **Group-IB**, an international company that specializes in preventing cyberattacks, on Money2020 Asia presented the analysis of hi-tech crime landscape in Asia in 2018 and concluded that cybercriminals show an increased interest in Asia in general and Singapore in particular. Group-IB team discovered new tool used by the Lazarus gang and analyzed North Korean threat actor's recent attacks in Asia. Group-IB specialists discovered **19 928** of Singaporean banks' cards that have shown up for sale in the dark web in 2018 and found hundreds of compromised government portals' credentials stolen by hackers throughout past 2 years. The number of leaked cards increased in 2018 by **56%.** The total underground market value of Singaporean banks' cards compromised in 2018 is estimated at nearly **$640 000.**

Lazarus go rogue in Asia. New malware in gang's arsenal

According to Group-IB Hi-Tech Crime Trends 2018 report, Southeast Asia, and Singapore in particular, is one of the most actively attacked regions in the world. In just one year, 21 state-sponsored groups, which is more than in the United States and Europe combined, were detected in this area, among which Lazarus – a notorious North-Korean state-sponsored threat actor.

Group-IB established that Lazarus is responsible for a number of latest targeted attacks on financial organizations in Asia. Group-IB Threat Intelligence team detected and analyzed the gang's most recent attack, detected by the company experts, on one of the Asian banks. In January 2019, Group-IB specialists obtained information about previously unknown malware sample used in this attack, dubbed by Group-IB **RATv3.ps** (RAT - remote administration tool). The new Trojan was presumably downloaded to a victim's computer as part of the second phase of a so-called watering hole attack, which, according to Group-IB report on Lazarus, the group has been actively using since 2016. During the first stage, cybercriminals supposedly infected a website, visited by a victim, with a Trojan Ratankba, a unique tool used by Lazarus. Group-IB specialists note that the new **RATv3.ps** might have been used by North Korean hackers in other recent attacks at the end of 2018. At least one of RATs was available via a legitimate Vietnamese resource, which might have been involved in other attacks.

"The newly discovered Lazarus' malware is multifunctional: it is capable of data exfiltration from the victim's computer, downloading and executing programs and commands via shell, acting as a keylogger to retrieve victim's passwords, moving, creating and deleting files, injecting code into other processes and screencasting," – comments **Dmitry Volkov, Group-IB CTO and Head of Threat Intelligence.** "So in case of Lazarus a stitch in time saves nine. It is very hard to contain their attacks as they happen. You have to be well prepared and know their tactics and tools. In particular, it is extremely important to have most up-to date indicators of compromise, unavailable publicly, that can only be gathered through automated machine learning-powered threat hunting solutions. Given the group's increased activity in the region in 2018, we believe that Lazarus group will continue further to attack banks and steal funds via SWIFT and will likely experiment with attacks on card processing, primarily focusing on Asia and the Pacific."

Several cybersecurity researchers note that also in 2018 Lazarus carried out global campaign known as "Rising sun". The malicious campaign affected close to 100 organizations around the world, including Singapore. The gang's new endeavor took its name from the implant downloaded to victims' computers. It was found that Rising Sun was created on the basis of the Trojan Duuzer family, which also belongs to cybercriminals from the Lazarus group. The malware spreader as part of this campaign was primarily aimed at collecting information from the victim's computer according to various commands

According to Group-IB Hi-Tech Crime Trends report 2018, Lazarus, unlike most of other state-sponsored threat actors, does not shy away from attacking crypto. "Singapore, being one of the most crypto-friendly countries in the world, attracts not only thousands of crypto and blockchain entrepreneurs every year, but also threat actors willing to grab a piece of the pie. We expect that that other APTs like Silence, MoneyTaker, and Cobalt will stage multiple attacks on cryptocurrency exchanges in the near future," – says **Dmitry Volkov.**

Have you been pwned?

Group-IB **Threat Intelligence** team identified **hundreds** of compromised credentials from Singaporean government agencies and educational institutions over the course of 2017 and 2018. Users' logins and passwords from **the Government Technology Agency (https://www.tech.gov.sg/), Ministry of Education (https://www.moe.gov.sg/), Ministry of Health (https://www.moh.gov.sg/), Singapore Police Force website (https://polwel.org.sg/about/), National University of Singapore learning management system (ivle.nus.edu.sg) and many other resources were stolen by cybercriminals**. **CERT-GIB** (Computer Emergency Response Team) reached out to Singaporean CERT upon identification of this information. "Users' accounts from government resources are either sold on underground forums or used in targeted attacks on government agencies for the purpose of espionage or sabotage. Even one compromised account, unless detected at the right time, can lead to the disruption of internal operations or leak of government secrets," – **comments Dmitry Volkov**. Cybercriminals steal user accounts' data using special spyware aimed at obtaining users' authentication data. According to Group-IB data, **PONY FORMGRABBER, QBot and AZORult** became the **TOP 3 most popular Trojan-stealers** among cybercriminals.

Pony Formgrabber retrieves login credentials from configuration files, databases, secret storages of more than 70 programs on the victim's computer and then sends stolen information to cyber criminals' C&C server. Another Trojan-stealer — AZORult, aside from stealing passwords from popular browsers, is capable of stealing crypto wallets data. Qbot worm gathers login credentials through use of keylogger, steals cookie files and certificates, active internet sessions, and forwards users to fake websites. All these Trojans are capable of compromising the credentials of crypto wallets and crypto exchanges users. More information on the most actively used Trojans and their targets can be accessed through Group-IB Threat Intelligence.

Public data leaks is another huge source of compromised user credentials from government websites. Group-IB team analyzed recent massive public data breaches and discovered **3689 unique** records (email & passwords) related to Singaporean government websites accounts.

Underground market economy. Number of compromised cards of Singaporean banks on sale increases

In 2018, Group-IB detected the total of **19,928** compromised payment cards related to Singaporean banks on darknet cardshops. Singapore, as one of the major financial hubs in Southeast Asia is drawing more and more attention of finically motivated hackers every year. According to Group-IB data, compared to 2017, the number of leaked cards increased in 2018 by **56%.** The total underground market value of Singaporean banks' cards compromised in 2018 is estimated at nearly **$640,000.**

Group-IB Threat Intelligence team observed two abnormal spikes in Singaporean banks' dumps, unauthorized digital copies of the information contained in magnetic stripe of a payment card, offered for sale on the dark web in 2018. The first one occurred on July 20th, when almost 500 dumps related to top Singaporean banks surfaced on one of the most popular underground hubs of stole card data, Joker's Stash. On overage, the price per dump in this leak was relatively high and kept at 45$. The high price is due to the fact that most of the cards were premiums (e.g. Platinum, Signature etc.).

Another significant breach happened on November 23rd when the details of 1147 Singaporean banks dumps were set up for sale on cardshops. The seller wanted 50$ per item– 50% of stolen cards in batch were also marked as Premium.

Group-IB Threat Intelligence continuously detects and analyses data uploaded to cardshops all over the world. According to Group-IB's annual Hi-Tech Crime Trends 2018 report, on average, from June 2017 to August 2018, the details of 1.8 million payment cards were uploaded to card shops monthly.

About Group-IB

Group-IB is a leading provider of solutions aimed at detection and prevention of cyberattacks, 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 sixteen 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 OSCE. Group-IB is a member of the World Economic Forum.

For more information, please contact:

Sergei Turner

Communications Manager

turner@group-ib.com

https://www.group-ib.com

https://www.group-ib.com/blog

Twitter | Linkedin