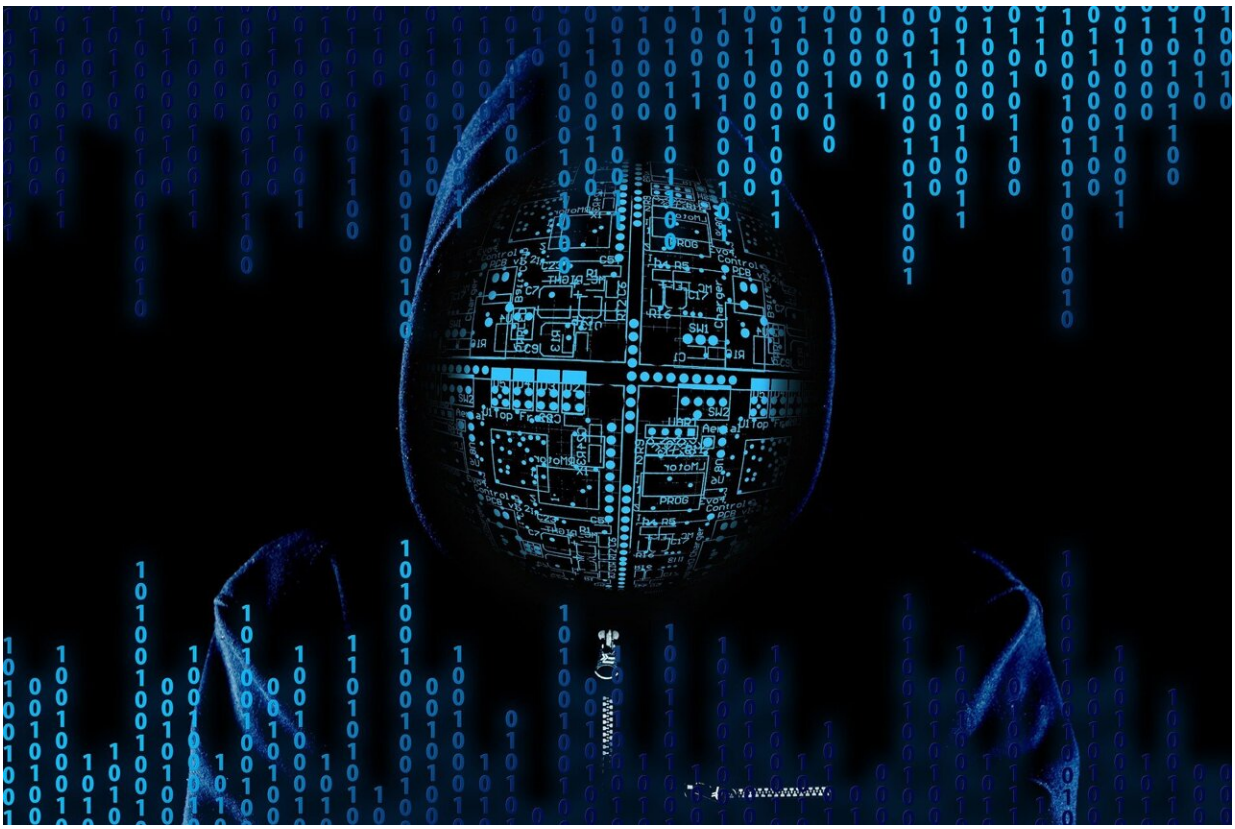
Hackers scored data center logins for big corporations more than a year ago. Now they're selling that information

February 21 2023, by Jordan Robertson



Credit: Pixabay/CC0 Public Domain

In an episode that underscores the vulnerability of global computer networks, hackers got ahold of login credentials for data centers in Asia

used by some of the world's biggest businesses, a potential bonanza for spying or sabotage, according to a cybersecurity research firm.

The previously unreported data caches involve emails and passwords for customer-support websites for two of the largest data center operators in Asia: Shanghai-based GDS Holdings Ltd. and Singapore-based ST Telemedia Global Data Centres, according to Resecurity Inc., which provides cybersecurity services and investigates hackers.

About 2,000 customers of GDS and STT GDC were affected. Hackers have logged into the accounts of at least five of them, including China's main foreign exchange and debt trading platform and four others from India, according to Resecurity, which said it infiltrated the hacking group.

It's not clear what—if anything—the hackers did with the other logins. The information included credentials in varying numbers for some of the world's biggest companies, including Alibaba Group Holding Ltd., Amazon.com Inc., Apple Inc., BMW AG, Goldman Sachs Group Inc., Huawei Technologies Co., Microsoft Corp. , and Walmart Inc., according to the security firm and hundreds of pages of documents that Bloomberg reviewed.

Responding to questions about Resecurity's findings, GDS said in a statement that a customer support website was breached in 2021. It's not clear how the hackers obtained the STT GDC data. That company said it found no evidence that its customer service portal was compromised that year. Both companies said the rogue credentials didn't pose a risk to clients' IT systems or data.

However, Resecurity and executives at four major U.S.-based companies that were affected said the stolen credentials represented an unusual and serious danger, primarily because the customer-support websites control

who is allowed to physically access the IT equipment housed in the data centers. Those executives, who learned about the incidents from Bloomberg News and corroborated the information with their security teams, who asked not to be identified because they weren't authorized to speak publicly about the matter.

The magnitude of the data loss reported by Resecurity highlights the growing risk companies face because of their dependency on third parties to house data and IT equipment and help their networks reach global markets. Security experts say the issue is particularly acute in China, which requires corporations to partner with local data service providers.

"This is a nightmare waiting to happen," said Michael Henry, former chief information officer for Digital Realty Trust Inc., one of the biggest U.S. data center operators, when told about the incidents by Bloomberg. (Digital Realty Trust wasn't affected by the incidents). The worst-case scenario for any data center operator is that attackers somehow get physical access to clients' servers and install malicious code or additional equipment, Henry said. "If they can achieve that, they can potentially disrupt communications and commerce on a massive scale."

GDS and STT GDC said they had no indication that anything like that happened, and that their core services weren't impacted.

The hackers had access to the login credentials for more than a year before posting it for sale on the dark web last month, for $175,000, saying they were overwhelmed by the volume of it, according to Resecurity and a screenshot of the posting reviewed by Bloomberg.

"I used some targets," the hackers said in the post. "But unable to handle as total number of companies is over 2,000."

The email addresses and passwords could have allowed hackers to masquerade as authorized users on the customer service websites, according to Resecurity. The security firm discovered the data caches in September 2021 and said it also found evidence the hackers were using it to access accounts of GDS and STT GDC customers as recently as January, when both data center operators forced customer password resets, according to Resecurity.

Even without valid passwords, the data would still be valuable—allowing hackers to craft targeted phishing emails against people with high-level access to their companies' networks, according to Resecurity.

Most of the affected companies that Bloomberg News contacted, including Alibaba, Amazon, Huawei and Walmart, declined to comment. Apple didn't respond to messages seeking comment.

In a statement, Microsoft said, "We regularly monitor for threats that could impact Microsoft and when potential threats are identified we take appropriate action to protect Microsoft and our customers." A spokesperson for Goldman Sachs said, "We have in place additional controls to protect against this type of breach and we are satisfied that our data was not at risk."

The automaker BMW said it was aware of the issue. But a company spokesperson said, "After assessment, the issue has a very limited impact on BMW businesses and has caused no damage to BMW customers and product related information." The spokesperson added, "BMW has urged GDS to improve the information security level."

GDS and STT GDC are two of Asia's biggest providers of "colocation" services. They act as landlords, renting space in their data centers to clients that install and manage their own IT equipment there, typically to be closer to customers and business operations in Asia. GDS is among

the top three colocation providers in China, the second-biggest market for the service in the world after the U.S., according to Synergy Research Group Inc. Singapore ranks sixth.

The companies are also intertwined: a corporate filing shows that in 2014, Singapore Technologies Telemedia Pte, the parent of the STT GDC, acquired a 40% stake in GDS.

Resecurity Chief Executive Officer Gene Yoo said his firm uncovered the incidents in 2021 after one of its operatives went undercover to infiltrate a hacking group in China that had attacked government targets in Taiwan.

Soon after, it alerted GDS and STT GDC and a small number of Resecurity clients that were impacted, according to Yoo and the documents.

Resecurity notified GDS and STT GDC again in January after discovered the hackers accessing accounts, and the security firm also alerted authorities in China and Singapore at that time, according to Yoo and the documents.

Both data center operators said they responded promptly when notified about the security issues and started internal investigations.

Cheryl Lee, a spokesperson for the Cyber Security Agency of Singapore, said the agency "is aware of the incident and is assisting ST Telemedia on this matter." The National Computer Network Emergency Response Technical Team/Coordination Center of China, a non-governmental organization that handles cyber emergency response, didn't respond to messages seeking comment.

GDS acknowledged that a customer-support website was breached and

said that it investigated and fixed a vulnerability in the site in 2021.

"The application which was targeted by hackers is limited in scope and information to non-critical service functions, such as making ticketing requests, scheduling physical delivery of equipment and reviewing maintenance reports," according to a company statement. "Requests made through the application typically require offline follow up and confirmation. Given the basic nature of the application, the breach did not result in any threat to our customers' IT operations."

STT GDC said it brought in external cybersecurity experts when it learned about the incident in 2021. "The IT system in question is a customer service ticketing tool" and "has no connection to other corporate systems nor any critical data infrastructure," the company said.

The company said its customer service portal wasn't breached in 2021 and that the credentials obtained by Resecurity are "a partial and outdated list of user credentials for our customer ticketing applications. Any such data is now invalid and does not pose a security risk going forward."

"No unauthorized access or data loss was observed," according to STT GDC's statement.

Regardless of how the hackers may have used the information, cybersecurity experts said the thefts shows that attackers are exploring novel ways to infiltrate hard targets.

The physical security of IT equipment in third-party data centers and the systems for controlling access to it represent vulnerabilities that are often overlooked by corporate security departments, said Malcolm Harkins, former chief security and privacy offer of Intel Corp. Any tampering of data center equipment "could have devastating consequences," Harkins

said.

The hackers obtained email addresses and passwords for more than 3,000 people at GDS—including its own employees and those of its customers—and more than 1,000 from STT GDC, according to the documents reviewed by Bloomberg News.

The hackers also stole credentials for GDS's network of more than 30,000 surveillance cameras, most of which relied on simple passwords such as "admin" or "admin12345," the documents show. GDS didn't address a question about the alleged theft of credentials to the camera network, or about the passwords.

The number of login credentials for the customer-support websites varied for different customers. For instance, there were 201 accounts at Alibaba, 99 at Amazon, 32 at Microsoft, 16 at Baidu Inc., 15 at Bank of America Corp., seven at Bank of China Ltd., four at Apple and three at Goldman, according to the documents. Resecurity's Yoo said the hackers only need one valid email address and password to access a company's account on the customer service portal.

Among the other companies whose workers' login details were obtained, according to Resecurity and the documents, were: Bharti Airtel Ltd. in India, Bloomberg LP (the owner of Bloomberg News), ByteDance Ltd., Ford Motor Co., Globe Telecom Inc. in the Philippines, Mastercard Inc., Morgan Stanley, Paypal Holdings Inc., Porsche AG, SoftBank Corp., Telstra Group Ltd. in Australia, Tencent Holdings Ltd., Verizon Communications Inc. and Wells Fargo & Co.

In a statement, Baidu said, "We do not believe that any data was compromised. Baidu pays great attention to ensure the data security of our customers. We will keep a close eye on matters such as this and remain on alert to any emerging threats to data security in any part of our

operations."

A representative for Porsche said, "In this specific case we have no indication that there was any risk." A SoftBank representative said a Chinese subsidiary stopped using GDS last year. "No customer information data leakage from the local China company has been confirmed, nor has there been any impact on its business and services," the representative said.

A spokesperson for Telstra said, "We are not aware of any impact to the business following this breach," while a Mastercard representative said, "While we continue to monitor this situation, we are not aware of any risks to our business or impact to our transaction network or systems."

A representative for Tencent said, "We are not aware of any impact to the business following this breach. We manage our servers inside data centers directly, with data center facility operators having no access to any data stored on Tencent servers. We have not discovered any unauthorized access of our IT systems and servers after investigation, which remain safe and secure."

A spokesperson for Wells Fargo said it used GDS for backup IT infrastructure until December 2022. "GDS did not have access to Wells Fargo data, systems, or the Wells Fargo network," the company said. The other companies all declined to comment or didn't respond.

Resecurity's Yoo said that in January, his firm's undercover operative pressed the hackers for a demonstration of whether they still had access to accounts. The hackers provided screenshots showing them logging into accounts for five companies and navigating to different pages in the GDS and STT GDC online portals, he said. Resecurity allowed Bloomberg News to review those screenshots.

At GDS, the hackers accessed an account for the China Foreign Exchange Trade System, an arm of China's central bank that plays a key role in that country's economy, operating the government's main foreign exchange and debt trading platform, according to the screenshots and Resecurity. The organization didn't respond to messages.

At STT GDC, the hackers accessed accounts for the National Internet Exchange of India, an organization that connects internet providers across the country, and three others based in India: MyLink Services Pvt., Skymax Broadband Services Pvt., and Logix InfoSecurity Pvt., the screenshots show.

Reached by Bloomberg, the National Internet Exchange of India said it wasn't aware of the incident and declined further comment. None of the other organizations in India responded to requests for comment.

Asked about the claim that hackers were still accessing accounts in January using the stolen credentials, a GDS representative said, "Recently, we detected multiple new attacks from hackers using the old account access information. We have used various technical tools to block these attacks. So far, we haven't found any new successful break-in from hackers which is due to our system vulnerability."

The GDS representative added, "As we are aware, one single customer didn't reset one of their account passwords to this application which belonged to an ex-employee of theirs. That is the reason why we recently forced a password reset for all the users. We believe this is an isolated event. It is not a result of hackers breaking through our security system."

STT GDC said it received notification in January of further threats to customer service portals in "our India and Thailand regions." "Our investigations to date indicate that there has been no data loss or impact to any of these customer service portals," the company said.

In late January, after GDS and STT GDC changed customers' passwords, Resecurity spotted the hackers posting the databases for sale on a dark web forum, in English and Chinese, according to Yoo.

"DBs contain customer information, can be used for phishing, access of cabinets, monitoring of orders and equipment, remote hands orders," the post stated. "Who can assist with targeted phishing?"