Business Intelligence

Some of the information being offered by the CMarket is geared more specifically toward industrial espionage and economic competition. Data such as this would allow a company or a state industry to monitor competitors, get information on pricing and contract negotiations, and steal intellectual property.

One of the private offerings was for “all company United states [sic],” as one of the cybercriminals described it to the undercover investigator in a chat log. The cybercriminal added, “All this information is detailed information, researched each part.”

The data was allegedly stolen by them from a contact information database of a major U.S. news outlet. The cybercriminal said it included 350,000 records with personal information on individuals who could be targeted through cyberespionage operations, so as to gain deeper access to the companies.

An entry in the marketplace offered information on employees of a large gas and oil company in Yemen, advertising the data for use in targeted attacks, and noted the breach maintained zero detection.

A separate entry offered a database containing personal and structural information on a chemical company in Egypt, noting it was “one of the main sources of production.” The entry was advertised at 35 to 40 bitcoins ($80,790 to $92,332).

Another entry for sale was one advertising “vulnerability system lists” airlines, which listed several major airlines by name, including United Airlines and Japan Airlines, as well as cargo airlines such as UPS and FedEx.

In one of the chat logs, the seller offered undercover investigator data from breaches of a major Indian bank and an Indian stock exchange. The seller offered access to the bank for $50,000, stating the group had breached the bank’s “central computer” and were in the process of “unlocking all user access [sic] and we can get more computers.” The seller also noted the breach of the stock market was “a work in progress but 90% [sic] done.”

Terrorists’ Devices Hacked

In 2016, hackers hired by a Russian group were able to breach the electronic devices of members of a terror cell. A chat log between a seller and an undercover investigator reveals that the terrorists were being trained to be sent to Europe to carry out attacks.

The Russian group was planning to sell access to the breached devices to authorities only after the cell had started carrying out attacks, which would increase the value of the information.

The seller said the hackers used skid of remote access Trojan (RAT) capable of taking full control of a device. The advanced RAT was developed by a researcher at a university.

Hospitals Held for Ransom

Hackers are actively breaking the systems of hospitals, then selling the access to other criminals. The criminals can then use the access to take control of and lock the hospital’s systems, holding them for ransom.

In one such case in 2016, the Hollywood Presbyterian Medical Center had to pay hackers $17,000 in bitcoin to regain control over its systems.

Sanctuary Cities Sessions Puts Squeeze on Sanctuary Cities With New Funding Criteria

Charlotte Cuthbertson

The Byrne JAG Program

The Byrne JAG funding allocations are calculated by the Bureau of Justice Statistics and are based on the state's population and violent crime statistics.

Once the state funding is calculated, 60 percent of the allocation is awarded to the state and 40 percent to eligible units of local government. State and local authorities often rely on the funding for law enforcement purposes.

In fiscal 2016, Byrne JAG handed out $147 million in grants to around 1,000 cities. Many cities reported that the grant would go toward training or new equipment like body cameras and radar.

New York City topped the list, receiving $8.3 million. Houston and Chicago were second and third, respectively, with $3.5 million apiece. Los Angeles was fourth with $1.8 million. All four cities are known for their sanctuary laws.

In New York, in fiscal 2016, Immigration and Customs Enforcement (ICE) submitted 80 inmate detainers to the NYPD, according to the mayor’s office. Two of the criminals were transferred to ICE.

Despite threats of funding cuts, cities such as Denver are furthering their sanctuary policies.

Just last week, the Denver City Council voted to essentially prohibit city officials from voluntarily cooperating with federal immigration authorities, according to a Denver Post report.

The city, which received more than $400,000 in Byrne JAG funding in fiscal 2016, is unlikely to qualify for any this round.

Sessions’s announcement comes after a Californian judge upheld an injunction on Trump’s original executive order, which sought to halt all federal funding to cities that limit cooperation with immigration officials.

Trump’s hard line on immigration appealed to many voters during his campaign.

“We will end the sanctuary cities that have resulted in so many needless deaths,” he said in Phoenix, Arizona, on Aug. 31, 2016. “Cities that refuse to cooperate with federal authorities will not receive taxpayer dollars, and we will work with Congress to pass legislation to protect those jurisdictions that do assist federal authorities.”

Congress is also moving forward on legislation regarding sanctuary cities.

In a June 29 vote, the House voted to cut federal funding to jurisdictions that fail to hand over illegal immigrants to immigration authorities when a detainee is lodged.

The bill, called the No Sanctuary for Criminals Act, will now go to the Senate.

“This is what the American people should be able to expect from their cities and states, and these long overdue reforms will help us take down MS-13 and other violent transnational gangs, and make our country safe,” Sessions said.