The CMarket seller said that the Russian group had provided them with a unique cyberweapon to carry out the breach. The seller described the tool as “basically RAT but way more advanced … capable of infecting other malware and to find other hackers” who had sold similar tools or had similar criminal interests.

The seller wrote, “They’re all active supporters and combatants [sic],” the seller wrote, noting that the terrorists were being trained at the time and “will be sent in other parts of Europe. … Not all, but some.”

“For once, we have a real cyberterrorist cell that was allegedly being trained to infiltrate Western Europe,” the seller wrote.

Data for sale on the CMarket is geared specifically toward government and military interests.

A tab on the site’s marketplace for “Government Attacks” listed data and access for sale, including “Personal identity data for Mexico’s National Public Security System and its federal police force,” available for between 100 to 120 bitcoins ($16,465 to $23,628). The cybercriminal also stated his group had begun infiltrating Qatar University, and noted, “The university is the only government university in the country.” University breaches are typically valuable for accessing research projects and for targeting professors for influence campaigns.

Data on government employees can be used as a starting point for government-level espionage, hackers will typically try to breach computers of government employees to gain access to the agency’s networks. Another entry offered access to SCADA systems, which are used to control moving parts in infrastructure systems such as power plants. The cybercriminals listed access to 5 to 100 bitcoins ($8,815 to $11,425) each, noting they had multiple targets available.

Data on law enforcement agencies was also available. According to BlackOps, the CMarket cybercriminals were trying to market the breach to smugglers who could use it to trace and avoid Coast Guard ships.

Other data is marketed to cybercriminals, including access to hospitals, which are typically used for ransomware attacks.

According to BlackOps, the CMarket cybercriminals listed access to hospitals, which are typically used for ransomware attacks. The data included “radio location for advance [sic] cyberespionage,” available for between 7 to 10 bitcoins ($11,465 to $23,628). A larger post offered access to a major telecommunications project across Mexico and Pacific time zone, which included access to 32 states and 26 municipalities in the west coast of Mexico. According to BlackOps, the CMarket cybercriminals listed access to hospitals, which are typically used for ransomware attacks. The data included “radio location for advance [sic] cyberespionage,” available for between 7 to 10 bitcoins ($11,465 to $23,628). A larger post offered access to a major telecommunications project across Mexico and Pacific time zone, which included access to 32 states and 26 municipalities in the west coast of Mexico.

Law Enforcement Data for Sale

Hackers on a darknet criminal marketplace were selling data bases from Mexico’s national public security system and its federal police force.

The hackers were asking for between 100 to 120 bitcoins ($16,465 to $23,628) for the data. Sensitive information like this, in many cases, marketed directly to drug cartels and other organized crime groups, who can then use it to identify law enforcement agents.

Criminal Networks

Several items on the marketplace area were marketed specifically to cartels and organized crime rings. One item was for access to the U.S. Coast Guard’s Vessel Identification System, which can monitor automatic tracking systems used to identify and track ships, including those used by law enforcement. The files were being sold for 5 to 7 bitcoins ($81.24 to $116.48).

Other data is marketed to cybercriminals, including access to hotels, which are typically used for ransomware attacks.