HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

ALERT

Issued 6/8/17

Unprotected Database Exposes VINs, Owner Info of 10 Million Cars

A database containing information on 10 million cars sold in the US and personal information about their owners has been found exposed online. The unprotected database was discovered by researchers from the Kromtech Security Research Center, and contains three sets of data:

1. Vehicle details: Vehicle Identification Number (VIN), make, model, model year, vehicle color, mileage, etc.

2. Sales details: VIN, mileage odometer, sales gross, pay type, monthly payment amount, purchase price, payment type, etc.

3. Customer details: Full name, address, mobile / home / work phones, email, birth date, gender, occupation, etc.

Kromtech's Chief Communication Officer Bob Diachenko says that the database appears to be a collection of marketing data from big and small US-based auto dealerships. "The database has been online for more than 137 days now. Security Researchers have yet to identify the owner of the database and asking for anyone from the exposed dealerships or the potential owner to contact us," he added. "Sophisticated criminals have now created a way to combine traditional offline crimes like stealing cars and technology. Criminals are now using leaked or hacked data to obtain unique identifiers for a vehicle and then 'cloning' a VIN to make a stolen car appear to be perfectly legal," Diachenko explained. "The criminals chose the make, model of the car they want to steal, then they use the database of VIN numbers to make a new VIN plate and obtain a fake title.

Once the criminals have the stolen car and the real VIN number from the database they can then sell the car to an unsuspecting buyer. The victim may not realize right away that the car is stolen until the criminals are long gone with the money and there is no chance to get it back." Knowing a car's VIN might also allow criminals to create duplicate keys for it, and steal it without having to break into the car. This particular approach was used by members of a Tijuana-based motorcycle club to steal a considerable number of Jeep Wranglers in the last three years. The criminals did not steal the VINs from a database, but obtained them by simply reading them from the vehicle's dashboard. "Scouts would send the VIN to leaders, who in turn, would send the VIN to key cutters.

Key cutters would, without authorization, access a proprietary database containing codes used to create and program duplicate keys for Jeep Wranglers. Key cutters would use one of the codes to create a duplicate key for the targeted Jepp Wrangler. Key cutters would provide the duplicate key to leaders along with the second code, which thieves would need in order to program the microchip within the key at the time of the theft," it is explained in the recently unsealed indictment. Last year, security researcher Troy Hunt demonstrated how a vulnerability in the mobile app used to interact with Nissan LEAF, a popular electric car, can be exploited by remote, unauthenticated attackers to switch the car's AC and heating system on and off. The only thing that an attacker would need to know in order to do this is the car's VIN.