The Attack Surface of the Japanese Auto Industry

Japan is the third largest economy in the world, a distinction that makes it a natural target for cyber attackers. As a global hub for many industries including financial services, telecommunications & media, and manufacturing, Japan's attack landscape far exceeds just companies and organizations within the geographic boundaries of Japan. Global Japanese brands have many overseas subsidiaries that represent significant risks for cyber security experts.

The Japanese automotive industry is just such an example as it is a major player on the world stage with brands consisting of subsidiaries all around the globe. In our latest report we take a look at the entire Japanese attack landscape and analyze the automotive industry specifically. Below are a few of the key trends and findings our researchers uncovered.

Product Security Threats:

Japanese vehicles are built and bought in locations all over the world making product security and the protection of intellectual property and vehicle information a critical component of strong security.

Our research identifies many examples of breaches — particularly stemming from overseas subsidiaries — that resulted in vehicle information and technology intellectual property being stolen by attackers and sold for exploitation.

In one such example, the attacker, "Oleg-Maslov," offered to sell stolen copies of Toyota Techstream, a dealership diagnostic tool that would have allowed threat actors to conduct reconnaissance on targeted vehicles and collect critical information. In another instance, Rapid7 researchers observed an "AgentGrabber" car theft tool available for sale on criminal forums that would enable abuse of Keyless Entry systems for several major auto manufacturers, many Japanese brands.

Compromised Customer Data:

Personally identifiable information, or PII, is a very common and sought after class of data by cyber attackers. Automotive customer data can include information regarding addresses, names, email addresses, and even VIN numbers for vehicles sold to individuals. This data can be used to create fraudulent lines of credit and other outcomes of identity theft.

Breaches among the automotive industry over the last few years include that of major Japanese brand dealerships and sales subsidiaries which resulted in millions of customers having some or all of the PII held by those dealerships compromised and collected by attackers. In one instance, a breach at a third-party vendor exposed more than 4.9 million Honda customers to having some or all of their names, email addresses, and VINs to attackers.

Business Email Compromise:

Automotive companies can be high-valued targets for business email attacks as they are a major component of the Japanese economy with values as high as some of the globes largest companies. Often attackers pose as senior executives or external partners through legitimate email accounts compromised through social engineering scams. The attackers will then seek to have money sent to them under the guise of legitimate business practices.

These are just a few of the impacts attackers have had on the Japanese auto industry in just the last few years. For more on this sector and several others, read the report.