Upstream

Q1 2019 SEES RAPID GROWTH OF AUTOMOTIVE CYBER INCIDENTS

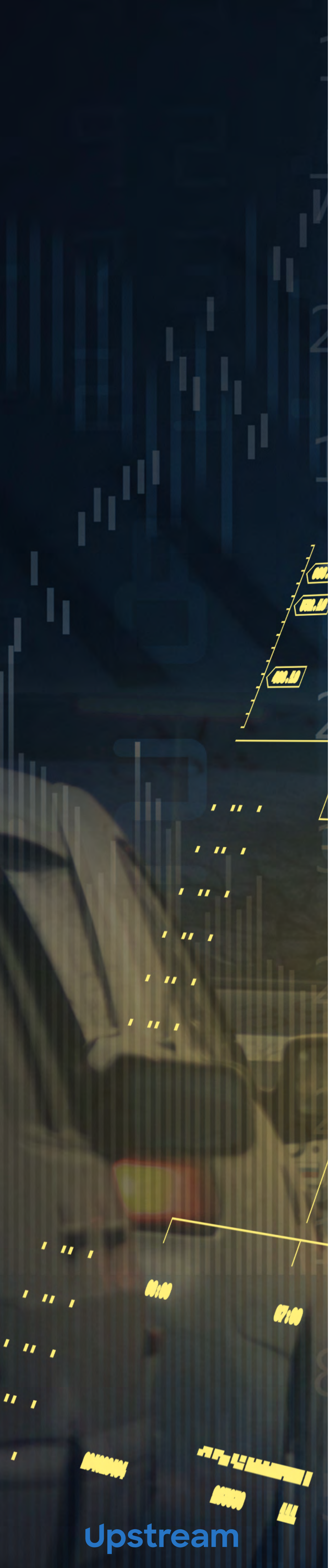


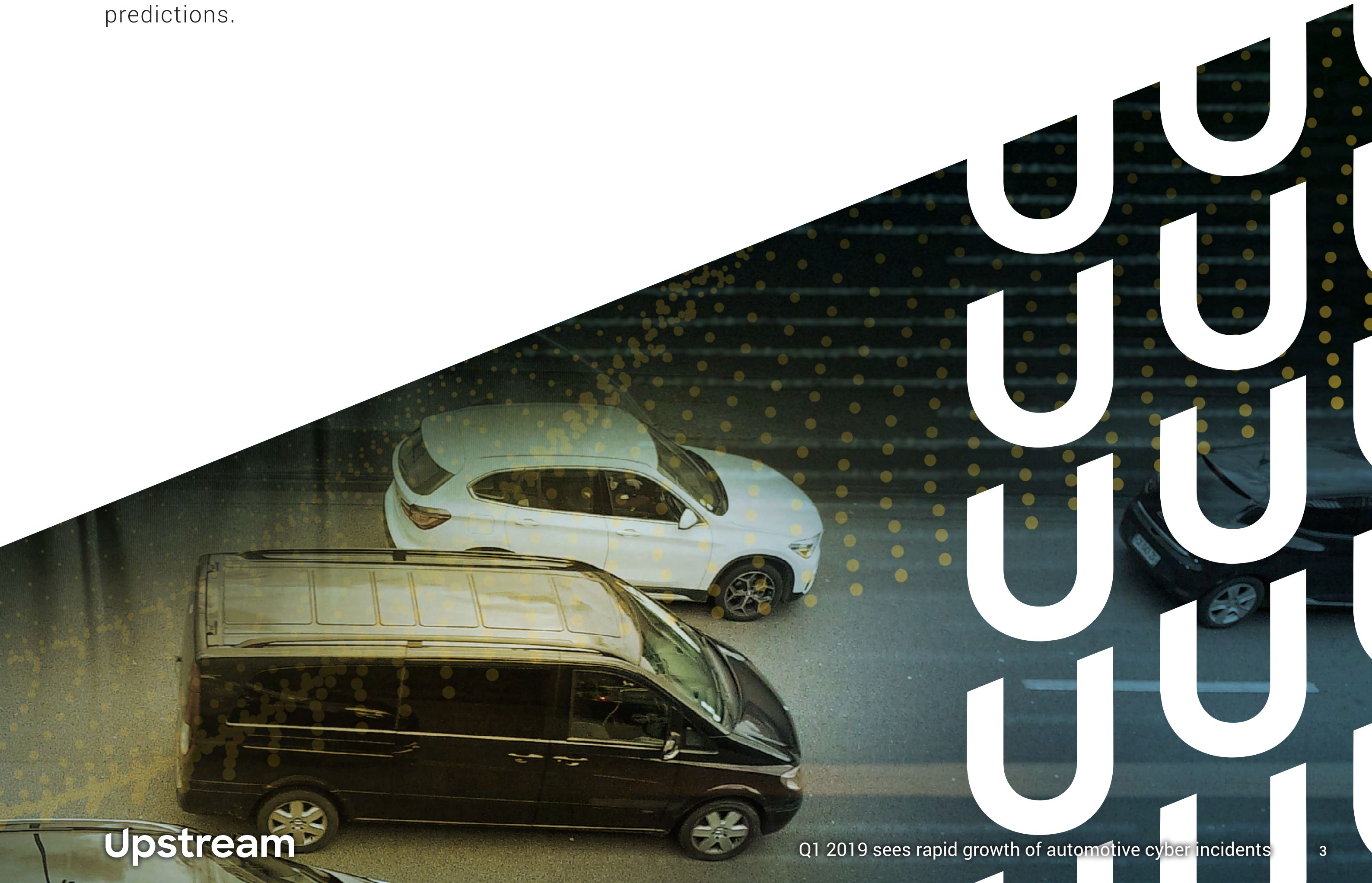
TABLE OF CONTENTS

Introduction

The cyber threats targeting the automotive landscape have been gaining predominant attention for the past few years - and for a noteworthy reason. Unlike cyber threats in general, which are perceived to be detrimental but are limited to the "online" domain, cyber threats against cars and mobility services in general are seen to have a direct and physical impact on us as individuals.

The Upstream Research and Intelligence Team has been examining this fundamental topic from the very beginning. By quantifying and analyzing real data in the field, based on published incidents, the central goal is to decipher this rapidly growing sector of cybersecurity, by classifying and analyzing multi-year data as well as summarizing the facts and figures into a first-of-its-kind report. This comprehensive report covers the entire "attack continuum", the core vectors ripe for attack, and the discernable impact upon various stakeholders.

With Q1 of 2019 now in the past, The Upstream Research and Intelligence Team is committed to examining the latest findings, discerning the trends that emerge from the data, and witnessing the truthful probability of our predictions.



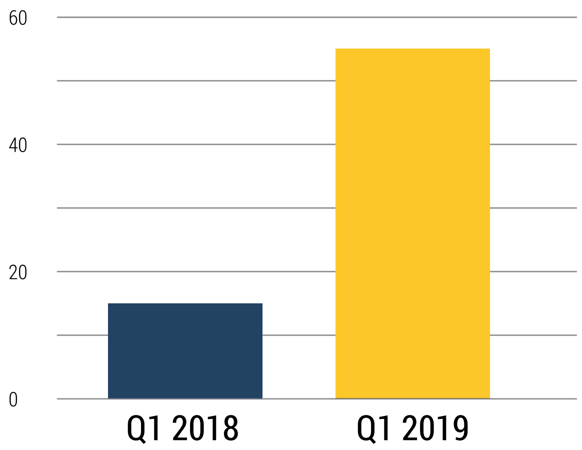
Chapter 1

THE TOTAL NUMBER OF INCIDENTS IS ON A SHARP RISE

Our research has identified 51 incidents in Q1 2019, compared to 15 incidents occurring in the same period of last year. This figure alone is alarming. It exemplifies an increase of more than 300% in reported incidents. Given that the total number of incidents for 2018 was 66, it is probable that things may continue to evolve in the same manner, where 2019 will see an overall increase of comparable proportions.

This growth is similar to another prominent phenomena in cybersecurity - ransomware, which was growing at a 350 percent annual rate, as cited in a recent study by Cisco. However, the core distinction is that ransomware uses established attack vectors such as email, and utilizes well-known exploits, whereas the automotive cyber threat is fairly new, and hackers have to establish novel ways to hack vehicles, making this increase even more substantial. To complete this analogy, ransomware attacks have also targeted the automotive sector in several high profile incidents, which reveals that this sector now endures the same setbacks as the rest of the industry.

Total incidents Q1 18 vs Q1 19

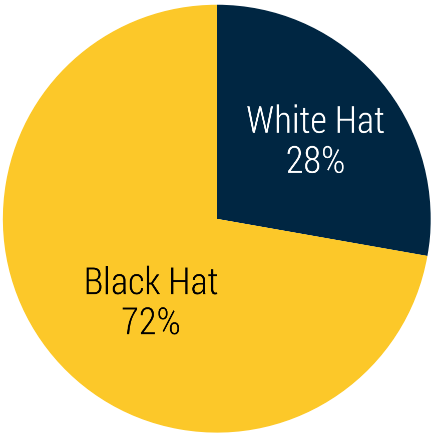


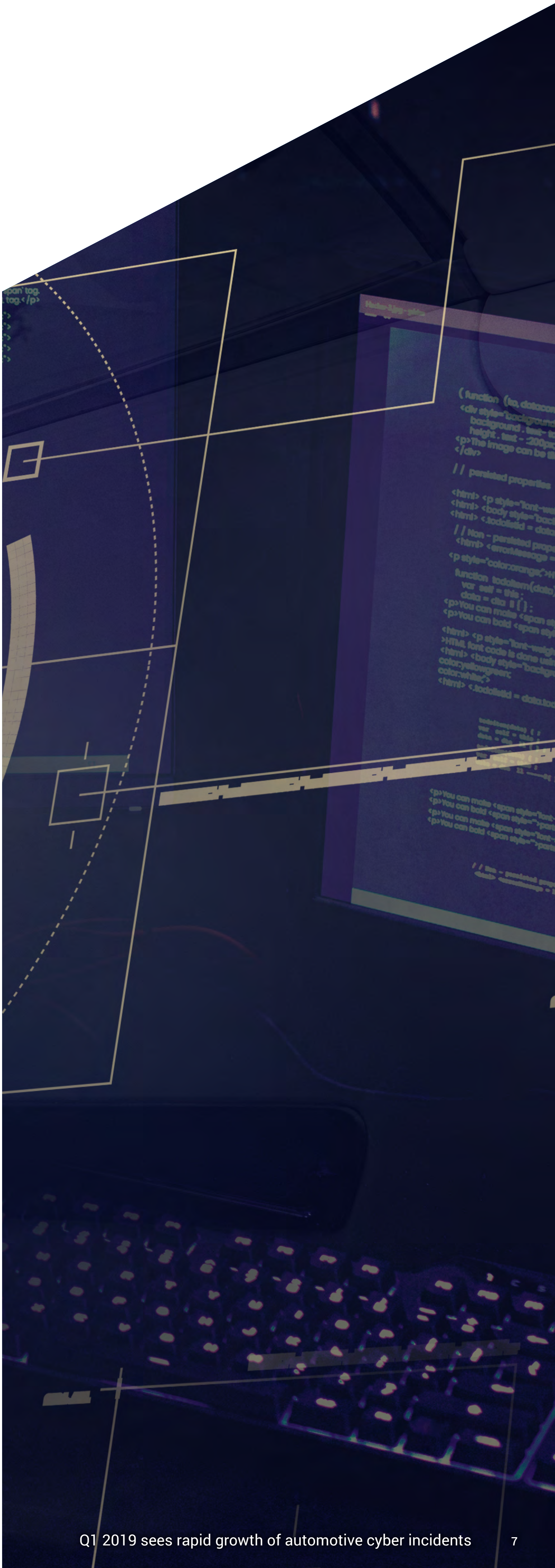
Chapter 2

BLACK HAT HACKERS ARE TIPPING THE SCALES

Incidents involving Black Hat (malicious) hackers have risen to 72% in Q1. Last year, the percentage of Black Hat and White Hat were nearly identical, at 55/45 percent, respectively. This is a clear indication that perpetrators are now well cognizant of the potential gains in automotive hacking via a variety of methods. Auto manufacturers as well as buyers need to be aware of the risks in order to safeguard themselves.

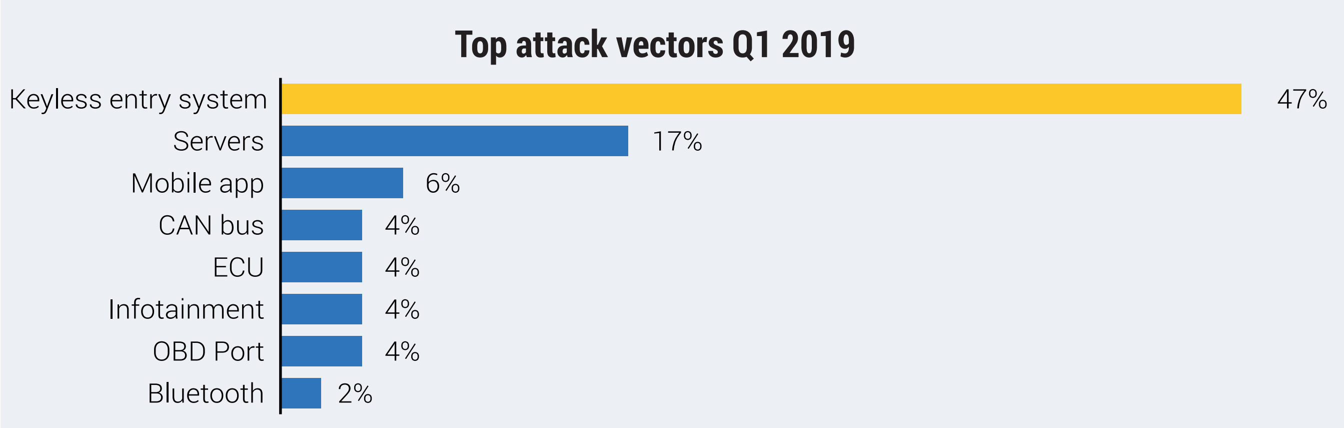
Black Hat vs White Hat





Chapter 3

POPULAR ATTACK VECTORS



Automotive security has made many inroads since automotive crime peaked in the latter part of the 20th century. However, all these security layers amount to nothing, when you see how today, systems are being circumvented by hackers utilizing widely available digital devices.

Keyless Entry systems are an additional feature to the overcrowded space of automotive security concerns. The popular news site, SUN, dispatched a team to steal cars using a cheap electronic gadget. Keyless vehicles were discovered to be an easy target to steal. Fords, Skodas and Jaguars were targeted, ranging from driveways to parking lots. Using this inexpensive device, cars were compromised within seconds. The investigation demonstrated how easy it is to employ this legal scanner in order to steal a car, leaving no detectible evidence. Car thieves have been quick to capitalize on such vulnerabilities and exploit novel ones.

A gang in San Antonio used a different technique where they amplified the signal from a key inside a home and used it to open the vehicle and steal it. The situation reached new heights, that a new safety rating has been suggested, designed to warn car buyers of the theft risk posed by models with insecure keyless entry systems. Security expert, Thatcham Research, announced the new ratings, which will label each car as either 'superior', 'good', 'basic', 'poor' or 'unacceptable' based on their vulnerability to thieves. However, the scheme has been questioned by car industry figures for obscuring the issue, rather than simplifying it.

Servers - The backend of mobility is also vulnerable

Attacks against servers are the second most common attack vector in Q1, and now account for about 17% of reported incidents. Servers are the "Backend" of the mobility revolution and the potential consequences of a hacked server are far more extensive than hacking a single vehicle.

One significant example is a major vulnerability in two popular smart alarm systems, that allowed potential hackers to track the vehicles, unlock their doors and, in some cases, cut off the engine. A security research team uncovered authentication issues in the alarm systems made by Viper and Pandora Car Alarm System, two of the largest smart car alarm makers in the world. The two brands have as many as 3 million customers between them. The researchers showed that both applications' API didn't properly authenticate for update requests, including requests to change the password or email address. This reveals that cyber criminals could potentially have unrestricted access to vehicles through the vehicle's onboard telematics component.

All the researchers needed to do was send the request to a specific host URL and they were able to change an account's password and email address without notifying the victim that anything had happened. Once they had gained access to the account, the researchers had full control over the smart car alarm. This allowed them to learn where a car was and unlock it, but more crucially, to take control over its motor functions.

However, attacks against servers are not always targeting vehicles. For instance, a large parking garage in Canada was a target for Ransomware that decrypted the accessed files on the server and demanded ransom. This had resulted in disabling the attendant system, meaning that all drivers in the 1,000-space lot did not require ID and therefore they could park for free.

Mobility-related apps are ever so popular, but many leak information or cause mishaps.

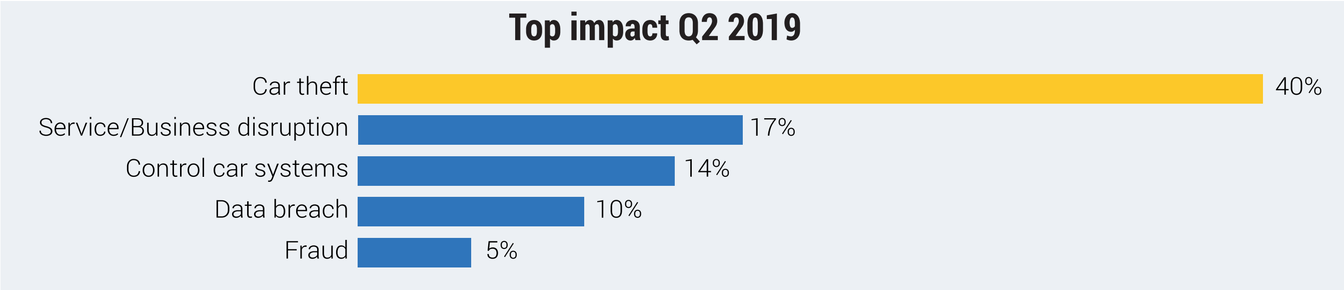
Incidents involving mobility related apps are now the third most frequent, and account for 6% of the total number of incidents. Generally, mobile apps are not considered to have robust security. Numerous apps have been found to leak information or enable 3rd parties to access sensitive data. But just like any other facet, when it comes to mobility, the impacts of such mishaps are graver since it involves very personal information such as owner and vehicle whereabouts.

The vulnerability in apps have been used to break into parked vehicles. In rare security camera footage from Tulsa, Oklahoma, a man is shown to be standing next to a parked car, fiddling around with an app on his mobile phone until he is able to open the car door.

In Israel, the country's top parking app, Pango, has been sued for violation of privacy. Allegedly, the mobile app allowed anyone to insert any license plate number and learn the vehicle's location, without having to prove ownership or possession of the vehicle.

Chapter 4

THE IMPACT OF CYBER THREATS UPON VEHICLES



Car theft

40% of cyber activities against vehicles resulted in car theft, which makes it the category with the greatest impact on mobility. In some areas the situation became so dire, that local police had to advise local vehicle owners, notifying them about the rise in keyless car thefts in the area and suggested how to act in order to mitigate this threat.

Service/Business disruption

17% of incidents caused service or business disruptions, signaling that the rapid adoption of mobility without proper security could have catastrophic consequences.

In an accurate example of business disruption, we have Uber and a former employee. With the ride sharing app company entering the Australian ride-sharing scene a year after local company GoCatch, Uber developed spyware called "Surfcam" to track GoCatch' vehicles and scrape information on their drivers in a bid to lure them towards Uber. With the operation, GoCatch would lose clients with Uber stealing drivers. With the drop in drivers, customers went to Uber and eventually GoCatch was disrupted enough to shut down their operations.

Control car systems

14% of incidents involved manipulation of control car systems, such as a demonstration by researchers from Tencent that showed how they could manipulate a Tesla Model S' Autopilot system. They showed that they could control the steering system via the Tesla Autopilot system using a wireless gamepad, even when the Autopilot system wasn't driver-activated.

1 in 10 mobility-related cyber incidents are data breach related

In the last few weeks of Q1' 2019, details of over 3 million Toyota and Lexus car owners were breached. The company would not divulge what type of information was compromised. However, the investigation is ongoing to see if any of the data was exfiltrated.

Why steal the vehicle when you can simply use it for fraudulent means?

5% of incidents are related to fraudulent, illegal activities. Ride sharing services like Uber and Lyft serve millions of people and conduct numerous transactions, and as such, could be utilized for the purpose of money laundering.

With Uber, for example the transaction laundering process involved collusion between the active parties - the drivers and the money launderers. When more drivers are involved, more money can be laundered. When a driver agrees to a rate, Uber takes its percentage from a ride that never took place. The drivers in collusion share their earnings with the laundering kingpin and pass the laundered money to their client.

In another incident, data from over 1.5 million vehicle odometers was tampered with, 10 percent of them being in Texas. Manipulating odometers can change the value of a used vehicle prior to sale, and thus misleading potential buyers into paying much more for a run-down vehicle with high mileage.

Summary

As we learn from the data, there is an undeniable increase in both the quantity and severity of incidents. We witness more incidents involving Black Hat hackers, that are focusing their efforts on stealing not only the cars, but their data or manipulating and disturbing the mobility service providers via other means.

All the incidents are available online and are regularly updated on Upstream's website. Please subscribe to our mailing list to receive updates on the most updated incidents.

About Upstream Security

Upstream improves the safety and security of connected vehicles and services built for them. It does this by monitoring business critical events and identifying cyber threats in real-time via a centralized cloud-based analysis of multiple automotive data feeds, including telematics and mobile applications. The solution is 100% agent-less and does not require any hardware or software inside the vehicles. Upstream's solution is already used by millions of vehicles worldwide, providing an effective and innovative method of detecting threat anomalies and mission critical events using a combination of machine learning, cybersecurity engines, and service policy enforcement. The result enables Smart Mobility services to run safely and smoothly while providing the customer with real-time alerts tailored to their needs.

For More Information

Visit us at: www.upstream.auto
Contact: hello@upstream.auto
Find us: