Last month, we found out that hackers took down a county government in California. Around the same time, a city in Maine lost control of all its data. These followed New York state’s capital, Albany, admitting that hackers had crippled the city’s technology operations, which means just about everything important in the city was taken down. And just last week, Baltimore was hit by a successful ransomware attack that demanded 13 bitcoin to decrypt city files that were being held hostage.
The world is supposed to be launching into a dazzling smart city future where governments are always connected and, therefore, move quicker and more efficiently than before. But if that’s where we’re going, we have to deal with the fact that many cities fall victim to profit-driven hackers.

The weapon often used against cities is ransomware, a type of malware designed to gain access, take control of important data and then demand money to end the ensuing crisis. It’s a popular extortion-hacking scheme that’s now seeing a new source of success.

American governments, particularly cities, states, law enforcement agencies, and schools, are being increasingly targeted by ransomware, according to a new report from the cybersecurity firm Recorded Future. At least 170 government systems have been attacked since 2013, according to public reports. And there have been 21 attacks so far this year, Recorded Future found, and 2019 is on pace to tally the highest ever number of ransomware attacks against cities. But due to the lack of transparency and accountability, there are likely more attacks unknown to both the public and many defenders.

Is this due to an overall rise in ransomware attacks, or is it a result of more cities bringing their systems online? No one knows the full answer because, thanks to a lack of transparency and information sharing rules, no one knows fully what’s happening.

In a time when American cities are struggling to deal with crumbling infrastructure—bad roads, collapsing bridges, old hospitals—it’s becoming increasingly clear that vulnerable networks ought to be added to the list of decaying necessities in dire need of an upgrade. With the emergence of the so-called smart city, in which everything is connecting to the internet—including those very same roads, bridges, and hospitals—the challenges facing cities loom even larger.

“We see with cities coming online in every respect so that when ransomware takes them offline, how much it affects constituents,” Recorded Future’s Allan Liska told Gizmodo. “Atlanta had everything in the ‘smart city,’ so even
court systems were taken offline, no one could pay anything through the city because the systems were taken offline.”

Cities around the country are racing to become “smart.” Tech and federal money along with an undeniable popular sentiment to modernize government is driving the push to connect. But it’s one thing to let an algorithm direct road crews or build a facial recognition system to identify drivers—it’s an entirely different issue to have cities prepared to deal with the inevitable security problems that will pop up. That’s to say nothing of the looming privacy concerns of smart cities.

The 2018 Atlanta ransomware attack stands as one of the most high-profile demonstrations of the stakes here. It cost millions to recover from an attack that initially demanded about $50,000 in ransom. When Albany was hit, the city’s police were crippled for a full day. An attack against San Francisco, a city at the heart of the American technology industry, ended up losing millions of dollars on lost revenue when the Municipal Transportation Agency couldn’t accept money from riders. Baltimore’s computers systems, phone, and email remain offline a week after the ransomware was discovered.

 Alone, cities are often unable to deal with the enormity of the task. In the U.S., big infrastructure questions have historically been answered by the federal government, and Liska argues that’s the level of assistance needed here.

“This is a national security problem,” Liska said. “We made clear this isn’t a nation-state actors but if your city is shut down it doesn’t matter if its a nation-state or cybercriminal, the effect is the same.”

Liska says he hopes to see the Department of Homeland Security, the agency tasked with defending critical infrastructure, pouring more money into the mission of defending cities.

“As the cities become smarter, more and more people expect this and it becomes an extension of what we consider infrastructure,” Liska said. “These online methods will become the only way to accomplish certain tasks, which
means these attacks will have more impact. From what we’re seeing, the attacks are only going to increase.”

RELATED STORIES

Privacy Expert Resigns From Alphabet-Backed Smart City Project Over Surveillance Concerns

The Dark Side of the "Smart City"

Report: Google's Parent Company Has 100 People Working on Its City of the Future

Baltimore's Government Held Hostage by Ransomware Attack

One of the World's Largest Crypto Exchanges, Binance, Hacked to the Tune of $40 Million

Reports: Police Bust Deep Dot Web, Saying It Made Millions Off Referral Links to Dark Web Markets

ABOUT THE AUTHOR

Patrick Howell O’Neill

Reporter in Silicon Valley. Contact me: Email poneill@gizmodo.com, Signal +1-650-488-7247
New Feature Lets Uber Black Car Riders Tell Their Filthy Pleb Drivers to Shut the Fuck Up

Matt Novak
32 minutes ago

Uber CEO Dara Khosrowshahi walks outside of the New York Stock Exchange on May 10, 2019
Photo: Getty Images

Uber has announced a new feature that will allow some riders to properly express their disgust for their filthy, lower class drivers—all with the simple touch of a button.

Starting today, Uber Black and Uber Black SUV riders will be able to select “Quiet Mode” from the app, which will inform their driver that they should shut the fuck up and not talk unless it’s absolutely necessary.

The change is one of many being rolled out today for Uber’s Black Car service, which differentiates itself from regular Uber trips by using premium cars with leather seats and “professional drivers” which must maintain a rating of
4.85 or higher. The Uber serial killer who murdered six people, for instance, only had a rating of 4.73 and would not have been allowed to drive for the Uber Black service.

But Uber Black isn’t just about fancy cars and high ratings anymore. Now there are a multitude of new features that can be selected on the app for Black Car rides, including preferences for temperature control, help with luggage, and, again, telling your driver to shut the fuck up because they’re of a lower social class and it’s not civilized when members of different classes communicate beyond what is absolutely necessary. At least that seems to be the idea.

“We know that when riders choose Uber Black and Uber Black SUV, they want a consistent, high quality experience every time they ride,” Uber’s senior product manager Aydin Ghajar said in a statement, presumably while wearing a monocle or some shit. “With these new features and more to come, we’re excited to ensure that our riders can arrive relaxed and refreshed, wherever they’re headed.”

Making riders feel like they have their own personalized driver has been Uber’s promise from the start. Founder Travis Kalanick first heard the idea for the app from StumbleUpon founder Garrett Camp in 2008 while on a trip to Paris, and Camp was upset that he’d recently spent $800 on black car service in New York, despite being a very rich man. Camp imagined splitting the cost among a number of people to bring the price down, and the company