The US Is Building a One-Stop Shop for Buying Your Data

Plus: A mysterious hacking group's secret client is exposed, Signal takes a swipe at Microsoft Recall, Russian hackers target security cameras to spy on aid to Ukraine, and more.

IN THE FOURTH WEEK OF MAY 2025, WIRED launched our Rogues issue–which included going a bit rogue ourselves. WIRED senior correspondent Andy Greenberg flew to Louisiana to see how easy it would be to recreate the 3D-printed gun authorities say they found on Luigi Mangione when they arrested him for the murder of UnitedHealthcare›s CEO. The result? It was both easy and legal.

In May 2025, US, European, and Japanese authorities announced the disruption of one of the world›s most widely used infostealer malware. Known as Lumma, the malware was used to steal sensitive information from victims around the world, including passwords, banking information, and cryptocurrency wallets details, according to authorities. Microsoft›s Digital Crime Unit aided in the operation, taking down some 2,300 URLs that served as the Lumma infrastructure.

A mysterious database containing more than 184 million records was taken down this week following its discovery by security researcher Jeremiah Fowler.

The database contained 47 GB of data, which included information related to Amazon, Apple, Discord, Facebook, Google, Instagram, Microsoft, Netflix, Nintendo, PayPal, Snapchat, Spotify, Twitter, WordPress, Yahoo, and more.

In other news, the US charged 16 Russian nationals for allegedly operating the DanaBot malware, which authorities say was used in a wide variety of attacks, from ransomware to espionage

The US Is Building a One-Stop Shop for Buying Your Data

The US intelligence community is looking to create a marketplace where private information gathered by data brokers under the guise of marketing can be purchased by American spies, The Intercept reports. Contracting data shows the US spy agencies intend to create a "Intelligence Community Data Consortium" that uses AI tools to sift through people's personal data; information that the Office of the Director of National Intelligence has previously acknowledged "could facilitate blackmail, stalking, harassment, and public shaming." In addition to providing insight into Americans' behaviors and religious and political beliefs, commercial data frequently includes precise location information, offering the US government the ability to surveil people's movements without acquiring a warrant–exploiting a widely recognized loophole in US privacy law.

Federal lawmakers attempted to ban the US government from buying what it calls "commercially accessible information" last year, with the Republican-controlled House passing a version of a law known as the "Fourth Amendment Is Not For Sale Act." However, the US Senate, then controlled by the Democratic Party, rejected the legislation.

Reporting by WIRED has repeatedly demonstrated how such data can offer US adversaries the ability to monitor the movements of US military and intelligence personnel, including in and around sensitive facilities that house nuclear arms.

A Mysterious Hacking Group Is Revealed to Work for the Spanish Government

Back in 2014, Russian security firm Kaspersky announced it had discovered a sophisticated hacking group it called Careto, Spanish for "Ugly Face" or "Mask," that had targeted victims across Europe and Cuba. Now, more than a decade later, former employees of the company have finally confirmed what Kaspersky wouldn't spell out at the time: That they believe Careto was a rare sighting of hackers working on behalf of the Spanish government. Careto's targets included energy companies, research institutions, and activists, but it particularly focused on Cuba, likely due to the island nation's giving refuge to members of a Spanish separatist group designated as terrorists by several European countries. Kaspersky's researchers found a Spanish phrase in the hackers' malware code that translates to "I shit in the sea," an expletive phrase typically used by Spaniards but not other Spanish speakers. Given the sophistication of Careto's hacking, the public confirmation of Kaspersky's attribution to Spain adds another known player to the game of high-level state-sponsored hacking.

Signal Introduces New Feature to Block Screenshots by Microsoft Recall

Microsoft's Recall feature, which constantly takes

and archives screenshots of Windows users' activity, still represents a serious privacy problem–even after Microsoft significantly walked back its rollout in response to criticism. So the encrypted messaging app Signal has gone so far as to exploit a digital rights management feature of Windows typically used to protect copyrighted materials to block Recall from taking screenshots of the app by default on Windows machines. After all, the Recall feature–which will likely be required for some corporate or government users–will essentially remove any privacy promise from Signal's disappearing messages feature for both Recall users and anyone communicating with them. The screenshot-prevention feature can be turned off in Signal's settings, but it will be turned on by default in Windows. "Microsoft has simply given us no other option," Signal wrote in a blog post.

Russia's Fancy Bear Hackers Targeted Security Cameras to Spy on Ukraine Aid

The hacker group within Russia's GRU military intelligence agency known as APT28 or Fancy Bear first rose to infamy for its targeting of the 2016 US election, but it's no surprise that the group has more recently focused on Ukraine. According to a new assessment from no fewer than 11 countries' intelligence agencies, the hacker group has been targeting a broad array of technology and logistics firms involved in providing aid to Ukraine. "Dozens of entities, including government organizations and private/commercial entities across virtually all transportation modes: air, sea, and rail" have been targeted in the campaign, the advisory reads. Perhaps most notable about the agencies' accusations is that the hackers targeted 10,000 security cameras in countries bordering Ukraine, including at border crossings, military facilities, and train stations. According to the agencies, the GRU hackers also carried out reconnaissance of the network of at least one producer of industrial control system components for railway systems–suggesting a possible intention to attempt sabotage–but didn't actually succeed in breaching the company.

US Indicts Russian National Over Qakbot Malware

The US Department of Justice indicted a Russian national, Rustam Gallyamov, on allegations that he designed software that was widely used by ransomware gangs and is known to have infected hundreds of thousands of computers, netting the gangs roughly $8.6 million in profit, according to DOJ figures. Prosecutors say more than $24 million was seized from Gallyamov, 48, over the course of its investigation. Federal charges unsealed this week allege that Gallyamov himself gained access to victims' computers and provided it to an array of cybercriminal organizations, including Dopplepaymer, REvil, Black Basta, and Cactus, among others.

The investigation into the now disrupted malware, known as Qakbot, was announced in August 2023 under former US attorney general Merrick Garland, who credited a multinational operation that included Europol and prosecutors and law enforcement agencies in France, Germany, the Netherlands, Romania, Latvia, and the United Kingdom. Agencies of Canada and Denmark have also been credited in the investigation that targeted Gallyamov.