WhatsApp suit says Israeli spyware maker exploited its app to target 1,400 users

reader comments

59 with 46 posters participating

Share this story

Facebook and its WhatsApp messenger division on Tuesday sued Israel-based spyware maker NSO Group. This is an unprecedented legal action that takes aim at the unregulated industry that sells sophisticated malware services to governments around the world. NSO vigorously denied the allegations.

Over an 11-day span in late April and early May, the suit alleges, NSO targeted about 1,400 mobile phones that belonged to attorneys, journalists, human-rights activists, political dissidents, diplomats, and senior foreign government officials. To infect the targets with NSO's advanced and full-featured spyware, the company exploited a critical WhatsApp vulnerability that worked against both iOS and Android devices. The clickless exploit was delivered when attackers made a video call. Targets need not have answered the call or taken any other action to be infected.

Routing malware through WhatsApp servers

According to the complaint, NSO created WhatsApp accounts

starting in January 2018 that initiated calls through WhatsApp servers and injected malicious code into the memory of targeted devices. The targeted phones would then use WhatsApp servers to connect to malicious servers allegedly maintained by NSO. The complaint, filed in federal court for the Northern District of California, stated:

> *In order to compromise the Target Devices, Defendants routed and caused to be routed malicious code through Plaintiffs' servers—including Signaling Servers and Relay Servers—concealed within part of the normal network protocol. WhatsApp's Signaling Servers facilitated the initiation of calls between different devices using the WhatsApp Service. WhatsApp's Relay Servers facilitated certain data transmissions over the WhatsApp Service. Defendants were not authorized to use Plaintiffs' servers in this manner.*
>
> *Between approximately April and May 2019, Defendants used and caused to be used, without authorization, WhatsApp Signaling Servers, in an effort to compromise Target Devices. To avoid the technical restrictions built into WhatsApp Signaling Servers, Defendants formatted call initiation messages containing malicious code to appear like a legitimate call and concealed the code within call settings. Disguising the malicious code as call settings enabled Defendants to deliver it to the Target Device and made the malicious code appear as if it originated from WhatsApp Signaling Servers. Once Defendants' calls were delivered to the Target Device, they injected the malicious code into the memory of the Target Device—even when the Target User did not answer the call.*

100 civil society members from 20 countries

Critics of the spyware industry have long said that NSO and its competitors sell products and services to oppressive

governments that use them to target attorneys, journalists, human-rights advocates, and other groups that pose no legitimate threat. Citizen Lab, a University of Toronto research group that tracks hacking campaigns sponsored by governments, volunteered to help Facebook and WhatsApp investigate the attacks on its users. Citizen Lab said among those targeted in the campaign were 100 members of "civil society" from 20 countries.

Citizen Lab said the targets included:

- multiple prominent women who have been targeted by cyber violence
- prominent religious figures from multiple religions
- well-known journalists and television personalities
- human-rights defenders
- lawyers working on human rights
- officials at humanitarian organizations
- individuals who have faced assassination attempts and threats of violence, as well as their relatives

"The commercial spyware industry is one that has tried to carve out an unaccountable space for itself, cozying up to the governments that it sells stuff to while simultaneously denying any responsibility for abuses conducted with its tools," John Scott-Railton, a Citizen Lab senior researcher, told me. "WhatsApp's lawsuit, which is important and precedent-setting, shatters that false distinction and makes it clear that they are willing to hold NSO accountable for the Wild West that exists in the spyware industry generally and is reflected in the target set."

In an email, NSO representatives wrote:

> *In the strongest possible terms, we dispute today's allegations and will vigorously fight them. The sole purpose of NSO is to provide technology to licensed government intelligence and law enforcement agencies to help them fight*

> *terrorism and serious crime. Our technology is not designed or licensed for use against human-rights activists and journalists. It has helped to save thousands of lives over recent years.*
>
> *The truth is that strongly encrypted platforms are often used by pedophile rings, drug kingpins, and terrorists to shield their criminal activity. Without sophisticated technologies, the law enforcement agencies meant to keep us all safe face insurmountable hurdles. NSO's technologies provide proportionate, lawful solutions to this issue.*
>
> *We consider any other use of our products than to prevent serious crime and terrorism a misuse, which is contractually prohibited. We take action if we detect any misuse. This technology is rooted in the protection of human rights—including the right to life, security, and bodily integrity—and that's why we have sought alignment with the UN Guiding Principles on Business and Human Rights, to make sure our products are respecting all fundamental human rights.*

The suit said that targeted users had WhatsApp numbers with country codes from the Kingdom of Bahrain, the United Arab Emirates, and Mexico. Public reports—including those here, here, and here—have listed the governments of all three countries as NSO customers.

Facebook and WhatsApp shut down the attacks on May 13 with a software update that patched the critical vulnerability. According to the complaint, an NSO employee responded to the move by saying: "You just closed our biggest remote for cellular… It's on the news all over the world." According to a statement from WhatsApp, company officials sent a special message to the approximately 1,400 targeted users informing them of the attack.

In an op-ed published by The Washington Post, Will Cathcart, the head of WhatsApp, wrote:

> *This should serve as a wake-up call for technology companies, governments, and all Internet users. Tools that enable surveillance into our private lives are being abused, and the proliferation of this technology into the hands of irresponsible companies and governments puts us all at risk.*
>
> *NSO has previously denied any involvement in the attack, stating that "under no circumstances would NSO be involved in the operating… of its technology." But our investigation found otherwise. Now, we are seeking to hold NSO accountable under US state and federal laws, including the US Computer Fraud and Abuse Act.*

Cathcart added: ""While their attack was highly sophisticated, their attempts to cover their tracks were not entirely successful."

Tuesday's complaint alleges that NSO violated the Computer Fraud and Abuse Act, the California Comprehensive Computer Data Access and Fraud Act, and a California law governing breach of contract. The action seeks a permanent injunction barring NSO from accessing WhatsApp servers, creating or using WhatsApp or Facebook accounts, or further violating WhatsApp terms of service.

Besides Facebook and WhatsApp apps and servers, NSO allegedly used servers owned by Amazon Web Services and smaller hosts Choopa and Quadrant. The leased servers connected targeted devices to a network of remote servers that were designed to distribute malware and send commands to devices once they were infected. Tuesday's complaint said that an IP address assigned to one of the malicious servers was previously used by a subdomain operated by NSO.

Now that Facebook and WhatsApp have taken the unprecedented step of suing a spyware provider for using its servers to target its users, it will be interesting to see if Amazon and the other server hosts mentioned in the complaint follow suit.

So far, they haven’t responded to emails seeking comment.

https://arstechnica.com/?p=1593555

Russia’s Fancy Bear hackers conduct “significant cyberattacks” on anti-doping agencies

reader comments

3 with 3 posters participating

Share this story

Fancy Bear, the Russian-sponsored hacker group, recently conducted “significant cyberattacks” on 16 national and international sports and anti-doping organizations, and at least some of the offensives were successful, Microsoft said on Monday.

The attacks began on September 16, just days ahead of news reports that the World Anti-Doping Agency, often known as WADA, had opened proceedings against Russian athletes after finding inconsistencies in lab data. Those proceedings, which involve the manipulation of thousands of anti-doping tests, could lead to the ouster of the Russian athletes.

Olympics obsession

The attacks are only the latest brazen steps the group has taken to shield against or retaliate for allegations of cheating by Russian Olympic athletes. In 2016, WADA blamed Fancy Bear for a hack that stole confidential medical data. The hackers then published the data, which included the drug regimens of Simon Biles, Serena and Venus Williams, and other athletes, in an attempt to paint them as flouters of WADA regulations. Two years later, hackers WADA identified as Fancy Bear published private emails taken from the International Olympic Committee. The action came after Russia was banned from the Winter Olympics. That same year, Fancy Bear struck the Olympics again with a hack that disrupted ticket sales, Wi-Fi networks, and other functions at the opening of the Winter Olympics. In an attempt to fly a false flag that implicated other nations, Fancy Bear crafted the malware used in the attack with file names and other characteristics used by North Korean and Chinese hacking groups. Microsoft's report on Monday didn't identify any of the 16 sports and anti-doping organizations by name. The company did, however, say that the group behind the attacks was Strontium, Microsoft's internal name for Fancy Bear, which is also known as APT28, Pawn Storm, Sofacy, Sednit, and Tsar Team. The company had already singled out Strontium twice in the past three months, once in July, in a post detailing the most prolific nation-sponsored hacking groups and again in August in an advisory about IoT hacks used as beachheads to more deeply access sensitive networks.

"The methods used in the most recent attacks are similar to those routinely used by Strontium to target governments, militaries, think tanks, law firms, human rights organizations, financial firms and universities around the world," Tom Burt, Microsoft's corporate vice president of customer security & trust, wrote. "Strontium's methods include spear-phishing, password spray, exploiting internet-connected devices and the use of both open-source and custom malware."

According to an indictment US prosecutors filed in 2018, when those methods fail, Fancy Bear tactics also include traveling to targets' physical locations and hacking targets' computer networks or hotel Wi-Fi connections. Fancy Bear is also one of two Russia-sponsored hacker groups that researchers say hacked the Democratic National Committee in 2016.

While some of the most recent attacks were successful, the majority were not, Burt said. Microsoft has notified all customers who were targeted and has worked with those requesting help. The successful attacks raise the possibility of leaks in the coming weeks or months, airing private documents that cast doubt on the legitimacy of the organizations. It also wouldn't be surprising to see the 2020 Olympics itself targeted.

By far the most effective measure for warding off Fancy Bear attacks is to protect accounts with multi-factor authentication, ideally with physical security keys. Learning how to spot advanced phishing attacks, using services that detect malicious Web links, and keeping software and firmware up to date are also effective.

https://arstechnica.com/?p=1592949

Eagles fly to Iran, rack up huge roaming charges

reader comments

72 with 57 posters participating

Share this story

A group of Russian scientists was hit by crippling roaming charges after some of the eagles the researchers were studying flew to countries with high roaming charges, including Iran, Turkmenistan, and Pakistan. The birds were outfitted with electronic devices that tracked their locations and sent back status updates a few times a day.

The scientists have been tracking eagle migration patterns since 2015. This year, the scientists were tracking 13 endangered steppe eagles who spend summers in northern latitudes in Russia and Kazakhstan. In the fall, the birds fly south, passing through countries like Iran, Afghanistan, and Pakistan.

The BBC reports that one eagle, named Min, was particularly expensive for the scientists. He spent his summer in Kazakhstan out of range of cell phone towers. During this period, his tracking device queued up hundreds of messages to send later.

When he flew south into Iran in early October, the device connected to a cell phone tower and sent the queued messages. Each cost the researchers 49 rubles ($0.77)—more than five times the expected price, according to The New York Times. The researchers say that these charges pushed the researchers over their budget for cellular service.

The team launched a crowdfunding campaign to help cover the costs, raising over $5,000 by the weekend. The researchers also convinced their wireless provider, MegaFon, to write off some of the charges and give them better roaming rates going forward.

The roaming charges have generated so much attention that other wireless providers have started offering free wireless service, the researchers told the *Times*. So the scientists may not have to worry about roaming charges next year.

https://arstechnica.com/?p=1592575

Facebook’s new political-ad policy already showing cracks, loopholes

Enlarge / Thumbs down.

reader comments

78 with 61 posters participating, including story author

Share this story

If you create a system, someone will try to game it—that’s true of everything from *Candyland* to the tax code. And so we should not be terribly surprised that Facebook—which is desperately trying to create some kind of coherent system for political advertising and speech as the United States careens headlong into the 2020 election season—already has players pushing to exploit loopholes in its policy.

Facebook confirmed earlier this month that while it attempts to fact-check certain kinds of posts and articles, posts by politicians are exempt from review on that basis, as are ads

posted by campaigns. But while the social media giant doesn't care if politicians lie outright in their ads, the company does have *some* standards: nob—including politicians—is allowed to post ads that intentionally try to suppress voter turnout.

So when The Washington Post found a targeted ad campaign on Facebook seemingly designed to mislead voters, the paper had questions.

"Official records show that your voter registration is incomplete," an ad targeted to Arizona voters said. The ad exhorted those who saw it to "Follow the link below to complete your voter registration NOW!"

The Post found that the ad, along with about two dozen other similar messages in the past five months, was purchased and run by a pro-Trump super PAC. When the WaPo reached out to Facebook about the advertisements, which seem to violate Facebook's policies, Facebook said it would remove four of the messages and submit others to third-party fact-checkers for verification.

It all depends on the messenger

Facebook CEO Mark Zuckerberg faced intense questioning about the company's political-advertising policy during an appearance on Capitol Hill last week.

During the five-hour hearing, Rep. Alexandria Ocasio-Cortez (D-N.Y.) specifically challenged Zuckerberg: "So there is some threshold where you will fact-check political advertisements? Could I run ads targeting Republicans in primaries saying that they voted for the Green New Deal?" referencing her own progressive policy proposal package.

Zuckerberg was unsure of the answer. He responded, "I don't know the answer to that off the top of my head. I think probably."

So a left-leaning PAC, The Really Online Lefty League (TROLL), did exactly what its name suggests: it bought a stunt ad claiming Sen. Lindsay Graham, a staunch Republican from South Carolina, supports the Green New Deal.

Sen. Graham, of course, ardently opposes the proposal, and Facebook did indeed fact-check that ad and suspended its paid distribution.

A Facebook spokesman told Reuters that—since the ad came from a third-party political action group, rather than directly from a politician—it was eligible for review and removal. Had Rep. Ocasio-Cortez herself decided to run such a spot, however, it's not clear that Facebook would have taken any action.

Nobody's happy

The poor reception Facebook is receiving for its contorted policy isn't only coming from lawmakers and the general public. Dissent is coming from inside the big blue house, too.

The New York Times reports today that more than 250 employees so far have signed onto an open letter to Zuckerberg, posted to the whole company on its internal social network, that strongly objects to the political-ad policy.

"Free speech and paid speech are not the same thing," the employees wrote in the letter, continuing:

> *Misinformation affects us all. Our current policies on fact-checking people in political office, or those running for office, are a threat to what FB stands for. We strongly object to this policy as it stands. It doesn't protect voices but instead allows politicians to weaponize our platform by targeting people who believe that content posted by political figures is trustworthy.*

The employees suggest instead that political advertising should be held to the same standard as other advertising (which it used to be). Political ads should also be visually distinct and have their ability to narrowly target extremely granular populations limited, the letter suggests.

https://arstechnica.com/?p=1592399

The FTC fosters fake reviews, its own commissioners say

Morsa Images | Getty Images

reader comments

41 with 33 posters participating

Share this story

Like much of the Internet, online reviews are often fake. No matter the platform—Amazon, TripAdvisor, Yelp, or another—no matter the subject, where user reviews are public, fakery usually follows.

The practice has surged in popularity in recent years as retailers scramble to capitalize on consumers' love of ecommerce. Saoud Khalifah, CEO of the fraudulent-review tracking company FakeSpot, says the number of companies padding their online ratings using reviews generated by bots, ghostwriters, or other schemes has increased dramatically over the past four years.

“When I started [looking into] this in 2015, it wasn’t as big as it is today,” said Khalifah. “Today, it has reached epidemic proportions—whether you’re looking at Sephora, Walmart, Amazon—it’s like a plague right now.”

Commissioners Rohit Chopra and Rebecca Slaughter of the Federal Trade Commission say it’s about to get a lot worse, and they know who to blame: their own agency. The FTC this week brought its first case against a company for enlisting its employees in a coordinated fake-review campaign to boost sales. Chopra and Slaughter say the decision reached by their fellow commissioners could usher in even more review fraud. The settlement did not require the company to admit fault, notify customers of the fraud, or turn over any ill-gotten gains.

“Dishonest firms may come to conclude that posting fake reviews is a viable strategy, given the proposed outcome here,” Chopra said in a statement dissenting from the FTC’s decision, joined by Slaughter. “Honest firms, who are the biggest victims of this fraud, may be wondering if they are losing out by following the law. Consumers may come to lack confidence that reviews are truthful.”

A fraught fraud case

The case in question concerns skin-care brand Sunday Riley, which on Monday agreed to settle FTC charges that it posted faked reviews for its products on Sephora’s website for nearly two years. The FTC has the power to punish companies for engaging in online review fraud through fines, forfeitures, or notices, among other things. But the Sunday Riley decision amounted to little more than finger wagging, Chopra and Slaughter say.

The dissenting commissioners say the agency's investigation uncovered more than enough evidence to prove that Sunday Riley had engaged in online review fraud—including an Instagram comment posted by a brand representative that confirmed the company had posted fake reviews. But the FTC voted 3–2 to allow Sunday Riley to settle the charges by agreeing not to post future fake reviews, without admitting fault.

Chopra and Slaughter say the settlement will ultimately do more harm than good and that it tells companies there's little risk in engaging in online review fraud; even if regulators find the fake reviews, the company won't face a meaningful punishment, the dissenters say. Other agency staffers said they feared the decision could harm competition online, as the FTC's reluctance to crack down on fake reviews in such a high-profile case may also influence decisions by state and local courts.

It is extraordinarily rare for the FTC to get a fake-review case as straightforward, prosecutable, and evidence-rich as Sunday Riley, FTC staffers say. Normally, it's difficult for regulators to identify when companies engage in fake review schemes online, as the agency doesn't have the staff to investigate the millions of online reviews; staffers say they often rely on tips from the fraud teams at ecommerce platforms to begin an investigation. Even then, the FTC is often hamstrung because there's not enough evidence to build a strong case, or because many peddlers of fake reviews aren't located in the US.

Multiple agency staffers described the Sunday Riley case as an unusually good enforcement opportunity. It was brought to the FTC's attention after a <ahref="https://www.reddit.com/r/SkincareAddiction/comments/9ogete/psa_sunday_riley_employee_we_write_fake_sephora/">whistle-blower shared a company email to Reddit in which Sunday Riley employees were given step-by-step directions on how to post fake reviews to Sephora's website and avoid detection. A

subsequent investigation found more evidence implicating company executives.

“It is difficult to imagine more egregious facts, yet all the commission is imposing is an order that the company and its CEO not repeat their lawbreaking,” Chopra said. “This settlement sends the wrong message to the marketplace.”

The three commissioners who voted in favor of the settlement did not issue an opinion explaining their reasoning. Commissioners Noah Wilson and Christine Phillips declined to comment when asked about the case. Neither FTC Chair Joseph Simons nor Sunday Riley responded to multiple requests for comment.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1591385

Johannesburg’s network shut down after second attack in 3 months

Enlarge / Johannesburg City Hall

reader comments

20 with 19 posters participating

Share this story

Johannesburg, the biggest city in South Africa and the 26th largest city worldwide, has shut down its website, billing and electronic services after being hit by a serious network attack, the second one in three months, municipality officials said.

A group calling itself Shadow Kill Hackers took to Twitter to take credit for the attack, claiming it took Johannesburg's "sensitive finance data offline." The group is demanding 4 Bitcoins, valued at about $32,000 US, for the safe return of the data.

A Johannesburg spokesman said the city took down the site after it detected a breach and that so far no formal ransom demands had been made. He also played down the extent of the breach.

"It was picked up very early while it was at the user level, before it reached the applications level where critical information sits," he told a TV news reporter. "So for us it was important that we safeguard the information first, before we start with the remedial work."

All your servers have been hacked

Accounts on Twitter told a different story. This purported image of the ransom note, which was addressed to "Joberg city" claimed to have full control over the city's network. Rather than encrypting the data and demanding a ransom in return for the encryption key, the attackers appeared to threaten to publish the data unless the money was handed over.

"All of your servers have been hacked," the note stated. "We have dozens of backdoors inside your city." The note went on to demand the Bitcoin ransom by Monday. "If you don't pay on time, we will upload the whole data to anyone on the

Internet," the note continued. "If you pay on time, we will destroy all the data we have, and we will send you IT a full report about how we hacked your system and your security…."

Enlarge / A purported screenshot of the note left by attackers of Johannesburg.
@pule_madumo

The group's Twitter messages also said the site outages weren't the result of Johannesburg officials taking their systems offline as the officials claimed, but rather the hacking group turning off the city's domain name system, which is used to help translate domain names into IP addresses. Another Twitter message posted what purported to be screenshots showing DNS controls and an Active Directory set up for Johannesburg City network.

This is the second breach in the past three months to hit the city. In July, Johannesburg’s municipal power provider suffered a ransomware attack that left residents without electricity.

In the first nine months of this year, at least 621 government entities, healthcare service providers and school districts, colleges and universities have been hit by ransomware, according to security firm Emsisoft recently reported. At least 68 of those attacks were on state, county and municipal entities. An attack in June on Baltimore cost the city at

least $18 million. Three Florida cities were also infected this year.

Emsisoft spokesman Brett Callow told Ars that the Johannesburg attackers appeared to be new to the ransomware scene.

“The personalized login screen message is quite unusual and not one we’ve seen before,” he said. “Nor is the email address provided in the ransom note one that we’ve seen used in other attacks (it’s also never been used in any previous submission to ID Ransomware).”

The Johannesburg spokesman, meanwhile, said the city’s IT staff is working around the clock to get systems back online.

https://arstechnica.com/?p=1591849

Comcast fights Google’s encrypted-DNS plan but promises not to spy on users

Enlarge / A Comcast van in Sunnyvale, California, in November 2018.
Getty Images | Andrei Stanescu

reader comments

123 with 107 posters participating

Share this story

Comcast has gone on the record to say that it does not track its broadband users' Web browsing histories, even though the company is lobbying against a Google plan that could make it harder for ISPs to track their users.

Comcast yesterday released a statement titled "The Facts about Privacy with Comcast's Xfinity Internet Service." Comcast said:

> *Where you go on the Internet is your business, not ours. As your Internet Service Provider, we do not track the websites you visit or apps you use through your broadband connection. Because we don't track that information, we don't use it to build a profile about you and we have never sold that information to anyone.*

Comcast further said that it does not and has never sold "information that identifies who you are to anyone," and the company claims it has never sold location data gathered from Comcast's mobile service. Comcast also said it deletes DNS queries generated by its Internet customers every 24 hours "except in very specific cases where we need to research a security or network performance issue, protect against security threats, or comply with a valid legal request."

Comcast's statement came one day after Motherboard ran an article titled "Comcast Is Lobbying Against Encryption That Could Prevent it From Learning Your Browsing History."

In the article, Motherboard published a lobbying presentation that it says Comcast has been distributing to US lawmakers. The Comcast slide deck claims that a Google/Mozilla plan to send DNS queries over the encrypted HTTPS protocol would "centraliz[e] a majority of worldwide DNS data with Google" and "give one provider control of Internet traffic routing and vast amounts of new data about consumers and competitors."

When contacted by Ars, Comcast did not confirm or deny that it is distributing the slide deck to lawmakers.

The broadband industry's major lobby groups have also been complaining to Congress about Google's plan for DNS over HTTPS, or simply DoH. Google has said its plan for the Chrome browser is to "check if the user's current DNS provider is among a list of DoH-compatible providers, and upgrade to the equivalent DoH service from the same provider." Google's public DNS system is one of six providers on the list, which also includes Cleanbrowsing, Cloudflare, DNS.SB, OpenDNS, and Quad9.

If what Google says is accurate, the company will not switch any Chrome users to Google DNS. If a Chrome user relies on their ISP's DNS or uses another DNS provider that isn't on the list, Chrome would make no changes for that user. If a Chrome user is using one of the five non-Google options on the list, Chrome would switch the user to the encrypted version of that provider's DNS system, not to Google's.

Mozilla plans a more aggressive rollout of encrypted DNS for Firefox, but Comcast and other ISPs have primarily expressed concerns about Google. Google has said that it "has no plans to centralize or change people's DNS providers to Google by default" and that "any claim that we are trying to become the centralized encrypted DNS provider is inaccurate."

ISPs exaggerate scope of Google plan

That hasn't stopped ISPs from urging Congress to intervene and claiming (apparently falsely) that Google plans to automatically switch DNS requests on Chrome for desktops and Chrome for Android to its own DNS servers. A letter to Congress from lobby groups including NCTA, which represents Comcast, claims that Google is making its own DNS service "the

encrypted DNS lookup provider by default" on both Chrome and Android.

Comcast's presentation for lawmakers claims that Google's plan means that "ISPs and other enterprises will be precluded from seeing and resolving their users' DNS queries and will be bypassed in favor of Google's own DNS resolver, i.e., Google Public DNS."

"With close to 70 percent of the browser market and over 80 percent of the mobile operating system market globally, Google/Mozilla's unilateral move will profoundly remake the Internet to Google's liking by centralizing DNS data in Google's hands," Comcast said.

Comcast further said that "Google's unilateral imposition of default, *centralized* DNS encryption will harm key components of the Internet" and that "Congress should demand that Google pause and answer key questions." Here are some of the questions that Comcast says Congress should force Google to answer:

- *How will Google address security concerns that arise from having just a single DNS resolver for a large proportion of US Internet traffic?*
- *Is it good for Google to be the sole source of malware protection for the entire US Internet ecosystem?*
- *Given Google's market power in the browser and OS market, and because Google is attempting to seize control of DNS data, does this raise competitive concerns?*
- *Will consumer's [sic] be given a meaningful choice to avoid Google and Mozilla's DNS services—how will Google explain the risks to customers?*
- *How will Google support parental controls and content filtering? Will such services be provided exclusively by Google and/or those it does business with?*

Comcast’s opposition to Google’s plans could raise concerns that Comcast is tracking its broadband users’ browsing activity. Those same concerns were raised when Comcast and other ISPs lobbied Congress to kill broadband privacy rules in 2017. The federal government’s decision to eliminate privacy rules at the broadband industry’s request means that companies like Comcast are not prohibited from using customers’ browsing histories to sell targeted ads or from sharing customers’ browsing histories with third parties.

Comcast defended its privacy practices at the time, saying that it doesn’t sell its users’ Web browsing histories.

What is Comcast worried about?

But if Comcast isn’t tracking its users, why is it so concerned about Google’s DNS plans? Comcast’s presentation says that Google deploying encrypted DNS would “create challenges for content delivery, content protection, law enforcement, and ISP customer support/troubleshooting” and “undermine network service quality and performance—including 5G.”

In a statement to Ars, Comcast said it supports encrypted DNS but that it “want[s] to make sure that it is implemented in a careful, collaborative manner for the benefit of Internet customers to ensure that important parental controls, cybersecurity protections, and network security features are not broken in the process.” Comcast said it would support a “collaborative, industry-wide solution that protects everyone,” but not “unilateral action” by Google and Mozilla.

Comcast’s other statement about its privacy practices doesn’t name Google, but the cable company is clearly trying to draw a distinction between the privacy of its own service and the privacy of Google’s.

“We’ve never used [DNS query] data for any sort of marketing

or advertising—and we have never sold it to anyone," Comcast said.

Google makes most of its revenue from advertising and collects browsing data in order to target ads at users. But Google says that Google Public DNS is not used to serve ads and that it doesn't correlate IP addresses or location data with users' personal information.

Comcast runs an advertising business

While Comcast says it doesn't track its users' browsing history, Comcast does sell online ads for "multiple premium, high-traffic online destinations" through its advertising business.

Comcast's website says that it may target online ads based on users' information, though apparently not their browsing histories:

> *Comcast may sell graphical display, text, and other ads, and deliver promotional offers for its products and services, on the Comcast Web Services and other digital properties. These ads and promotional offers may be based on information that you have provided to Comcast or its affiliates (such as the ZIP code of your Xfinity Internet service address), information about your current subscription or use of Comcast's or its affiliates' products or services, or other generally available information about you.*

Comcast also sells targeted ads on its cable TV service.

Since Comcast already operates an advertising platform, it probably wouldn't be difficult for the company to track its broadband users' browsing histories in order to serve targeted ads. (AT&T used to do exactly that.) Comcast may not track

browsing activity today, but its lobbying against privacy rules and Google’s DNS plans could help Comcast keep its options open.

https://arstechnica.com/?p=1591629

Congress concerned teenagers’ favorite app is national security threat

Enlarge / Visitors visit the booth of Douyin (TikTok) at the 2019 smart expo in Hangzhou, China, Oct. 18, 2019.

reader comments

60 with 46 posters participating

Share this story

Trade War! USA v. China

View more stories

Two senators are pressing for an investigation into TikTok, a short-form video app that’s mostly popular with teenagers, for potential national security concerns.

Senators Tom Cotton (R-Ark.) and Chuck Schumer (D-N.Y.), who generally agree about very little, sent a letter yesterday to

Acting Director of National Intelligence Joseph Maguire formally requesting an investigation of TikTok "and other China-owned content platforms."

"TikTok's terms of service and privacy policies describe how it collects data from its users and their devices, including user content and communications, IP address, location-related data, device identifiers, cookies, metadata, and other sensitive personal information," the senators wrote. "While the company has stated that TikTok does not operate in China and stores US user data in the US, ByteDance is still required to adhere to the laws of China."

China, they continue, is a problem:

> *Security experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party. Without an independent judiciary to review requests made by the Chinese government for data or other actions, there is no legal mechanism for Chinese companies to appeal if they disagree with a request.*
>
> *Questions have also been raised regarding the potential for censorship or manipulation of certain content. TikTok reportedly censors materials deemed politically sensitive to the Chinese Communist Party, including content related to the recent Hong Kong protests, as well as references to Tiananmen Square, Tibetan and Taiwanese independence, and the treatment of Uighurs. The platform is also a potential target of foreign influence campaigns like those carried out during the 2016 election on U.S.-based social media platforms.*

TikTok?

The TikTok app is similar in its base concept to the late,

great Vine, the Twitter-owned six-second video service that shut down in 2016. With TikTok, users create videos up to 15 seconds long featuring themselves doing *something*—singing, dancing, comedy—and use the app's native tools to include music or other effects.

Beijing-based ByteDance launched its first version of the app, Douyin, in China in 2016. TikTok for the US market, which runs separately, followed in 2017. Since then it has soared in popularity, *especially* among younger users. TikTok is the second most-downloaded app worldwide, behind Facebook-owned WhatsApp, dominating the iOS and Google Play charts for several quarters running, surpassing Instagram, Facebook, Snapchat, and YouTube and amassing more than 110 million cumulative downloads in the US.

"We are committed to transparency and accountability in how we support our TikTok users in the US and around the world," TikTok responded in a corporate blog post. "We store all TikTok US user data in the United States, with backup redundancy in Singapore. Our data centers are located entirely outside of China, and none of our data is subject to Chinese law."

The company added:

> *TikTok does not remove content based on sensitivities related to China. We have never been asked by the Chinese government to remove any content and we would not do so if asked. Period. Our US moderation team, which is led out of California, reviews content for adherence to our US policies – just like other US companies in our space. We are not influenced by any foreign government, including the Chinese government; TikTok does not operate in China, nor do we have any intention of doing so in the future.*

Chinese investment

Investment by China in every US business sector is rampant, and there's an obvious surface-level reason: the United States, as a nation, is rich. We have an enormous economy and collectively spend quite a lot of money on goods and services. We also have a robust, highly developed business and investment infrastructure. In short: if you're in the business of making money, you want to be in the US market.

Over the months and years of the Trump administration, however, concern about China's investment in US businesses has continued to spiral. We're now several months deep into a trade war of increasing rhetoric and increasing tariffs on physical goods, with challenges in the digital market mounting right behind.

Chinese mobile phone maker Huawei is now the poster child for the effect international tensions are having on the tech market. A federal law from 2018 prohibited the federal government from buying Huawei tech, and earlier this year, the company was effectively barred from the US market by executive order, causing ongoing headaches for the Android-based devices.

The concern about TikTok, however, feels more akin to a challenge a very different app faced earlier this year.

Chinese gaming company Beijing Kunlun Tech Co. acquired a majority stake in Grindr, a matchmaking app for men seeking men, in 2016 and then acquired the company outright in 2018.

The Committee on Foreign Investment in the United States (CFIUS), a panel operating out of the Treasury Department that comprises representatives from about a dozen different departments and agencies, reviews mergers and other significant investments in which a foreign company takes a stake in a US firm for national security concerns. Kunlun was

allowed to acquire Grindr without incident, but in March of this year, media reports revealed that the CFIUS was pressuring the company to unwind the acquisition for national security reasons that were not publicly specified.

Reuters reported in May that the CFIUS probe followed a discovery that a database of US user activity was made accessible to company engineers based in Beijing.

Around the same time of the Reuters report, Kunlun publicly agreed to divest Grindr to another buyer by June, 2020. By July, however, CFIUS had dropped opposition to Kunlun's plan to take Grindr public and was once again working on an IPO.

https://arstechnica.com/?p=1591343

Man planted keyloggers in companies' networks and stole their data

reader comments

17 with 15 posters participating

Share this story

A New Jersey man has admitted he installed keyloggers and laptops on the networks of two companies and used them to steal data related to an emerging technology they were using.

According to documents filed in US District Court for New Jersey, Ankur Agarwal, 45, of Montville, New Jersey, physically trespassed on the properties of both companies. He then installed hardware-based keyloggers that recorded the usernames and passwords of the companies' employees. He also installed laptops in the companies' networks that he used to remotely access the compromised employee accounts. Agarwal also used his unauthorized access at one of the companies to create a fraudulent employee badge that allowed him continued access to the company's premises.

The New Jersey man created a programming script designed to exfiltrate data. He used it against multiple computers to steal more than 15,000 files relating to the companies' emerging data, human resources data, employees' personal information, and email. Among the multiple employees who were targeted were a chief network engineer officer and a network engineer. The crimes began in February 2017 and came to an end around April 2018, when network security employees for one of the companies detected the intrusion and began an investigation.

Agarwal pleaded guilty to two counts of obtaining information from computers and one count of aggravated identity theft. He faces up to 12 years in prison and $750,000 in fines or twice the gain or loss of his offenses. He will also be required to pay restitution and to surrender computer gear. Sentencing is scheduled for January 28. A court document is here and a federal prosecutor release is here.

https://arstechnica.com/?p=1591219

Man sues AT&T after fraudulent SIM swap led to $1.8M cryptocurrency theft

Enlarge / An AT&T sign outside a company office in New York City.

reader comments

63 with 53 posters participating

Share this story

A lawsuit against AT&T alleges that the carrier's employees helped hackers perform SIM-swap attacks on a customer and rob him of $1.8 million worth of cryptocurrency.

Plaintiff Seth Shapiro of Torrance, California, says that AT&T is liable for the acts of its employees and failed to implement systems and procedures to prevent them from pulling off the scheme. The complaint, filed on October 17 in US District Court for the Central District of California, says:

> *On at least four occasions between May 16, 2018 and May 18, 2019, AT&T employees obtained unauthorized access to Mr. Shapiro's AT&T wireless account, viewed his confidential and proprietary personal information, and transferred control over Mr. Shapiro's AT&T wireless number from Mr. Shapiro's phone to a phone controlled by third-party hackers in exchange for money. The hackers then utilized their control over Mr. Shapiro's AT&T wireless number—including control secured through cooperation with AT&T employees—to access his personal and digital finance accounts and steal more than $1.8 million from Mr. Shapiro.*

In a SIM-swap attack, “the SIM card associated with the victim’s wireless account is switched from the victim’s phone” to someone else’s, which “effectively moves the victim’s wireless phone—including any incoming data, texts, and phone calls associated with the victim’s phone—from their phone to a phone controlled by the third party,” the lawsuit notes.

“The hacker’s phone then becomes the phone associated with the victim’s carrier account, and the hacker receives all of the text messages and phone calls intended for the victim,” the complaint continues. “Meanwhile, the victim’s phone loses its connection to the carrier network.”

In Shapiro’s case, AT&T employees did not just unwittingly give hackers control over his phone, the lawsuit says. AT&T’s “employees *actively profited* from this unauthorized access by knowingly giving control over his phone number to hackers for the purposes of robbing him,” the lawsuit says.

Shapiro backs up his lawsuit with details from a criminal case filed by the US government against nine people, including former AT&T employees Robert Jack and Jarratt White.

“[C]riminal investigations reveal that a third-party (an individual identified by authorities as ‘JD’) paid Jack and White to change the SIM card associated with Mr. Shapiro’s AT&T account from the SIM card in Mr. Shapiro’s phone to a SIM card in a phone controlled by JD and others,” the lawsuit said. JD paid White $4,300 to conduct SIM swaps, including the swaps in May 2018 that targeted Shapiro, and paid $585.25 to White, the lawsuit said.

These employees were “prolific SIM swappers,” with White conducting 29 unauthorized SIM swaps in May 2018 and Jack conducting 12 unauthorized swaps that same month, the lawsuit said.

Shapiro’s complaint said:

> *AT&T also informed law enforcement that the hacker involved in Mr. Shapiro's SIM swap had requested that 40 different AT&T wireless accounts be moved onto his phone (identified by its IMEI number) in the months leading up to Mr. Shapiro's swap. AT&T therefore had the technology to track how many different accounts were being [moved] on to the same telephone, as demonstrated by its ability to pull this information for law enforcement. Despite its ability to track this highly suspicious behavior, AT&T failed to use this technology to protect Mr. Shapiro's account. If AT&T had proper security safeguards in place, it would have recognized this behavior, flagged it as suspicious, and prevented any further SIM swaps onto that phone—thereby protecting Mr. Shapiro.*

Shapiro is asking the court for financial damages, saying the company violated privacy requirements applied to common-carrier phone companies under the Communications Act. His lawsuit also accuses AT&T of violating the California Unfair Competition Law by failing to disclose its inadequate security practices and by making material misrepresentations "concerning its sale of access to and safeguarding of Mr. Shapiro's" private information. The suit also says AT&T is guilty of negligence and of violating the US Computer Fraud and Abuse Act.

Man put life savings in cryptocurrency

Shapiro's lawsuit describes him as "a two-time Emmy Award-winning media and technology expert" who regularly advises large companies. Shapiro, who has a wife and two children, said the $1.8 million worth of digital currency "constituted the entirety of the profits from the sale of Mr. Shapiro's family home and his life savings." That money also included funds for his business.

“The digital currency stolen during the SIM swap attacks also included cryptocurrency raised by Mr. Shapiro for a business venture. As a result of the theft, Mr. Shapiro had to end the venture and lay off all employees,” the lawsuit said.

This is not the first such lawsuit filed against AT&T. The company was also sued by a man named Michael Terpin, who says that AT&T allowed a SIM-swap hack that cost him nearly $24 million worth of cryptocurrency.

In July, a federal judge allowed Terpin’s suit against AT&T to move forward despite AT&T’s arguments that Terpin didn’t adequately explain how the phone hack led to the loss of his cryptocurrency and that AT&T shouldn’t be held responsible for the misconduct of hackers who stole the cryptocurrency. Terpin recently wrote an open letter to Federal Communications Commission Chairman Ajit Pai, urging him to issue new security requirements that carriers would have to follow to prevent SIM-swap attacks.

When contacted by Ars about the Shapiro case, AT&T said, “We dispute these allegations and look forward to presenting our case in court.” AT&T also noted that it provides customers with information about SIM-swap scams at this webpage but did not provide any specific information disputing Shapiro’s allegations.

Despite disputing Shapiro’s lawsuit, AT&T says on that webpage that it is improving its technology and training to reduce the likelihood of SIM-swap attacks.

SIM-swap nightmare

The lawsuit details four incidents of SIM swapping in which Shapiro was the victim.

On May 16, 2018, Shapiro was attending a conference in New York City and noticed that his phone was no longer connected

to the AT&T network. Shapiro suspected that he was being victimized by a SIM swap "and called AT&T in an attempt to secure his account," his lawsuit said. The call resulted in "lengthy holds" followed by an AT&T rep suspending Shapiro's service and telling Shapiro to visit an AT&T store.

At the store in Manhattan, Shapiro bought a new iPhone and a new SIM card as an AT&T rep advised, and AT&T employees "assured him that his SIM card would not be swapped again without his authorization," the lawsuit said.

But Shapiro says he was victimized by a second SIM attack "mere minutes later" while he was still in the store. He "immediately informed" AT&T employees of the second attack and they "informed him that he needed to wait until it was his turn to be assisted," the lawsuit said.

Shapiro ended up waiting 45 minutes for help in the AT&T store. The lawsuit said:

> *In that time, third-party individuals were able to use their control over Mr. Shapiro's AT&T cell phone number to access Mr. Shapiro's personal and financial accounts and rob him of approximately $1.8 million, all while Mr. Shapiro stood helplessly in the AT&T store asking for the company's help.*

The attack was apparently exacerbated by the fact that many services use mobile phone numbers as the second factor in login systems protected by two-factor authentication. Hackers also can take control of various accounts by "exploiting password reset links sent via text message," the lawsuit noted.

The third parties who gained control over Shapiro's wireless number "used that control to access and reset the passwords for Mr. Shapiro's accounts on cryptocurrency exchange platforms, including KuCoin, Bittrex, Wax, Coinbase, Huobi, Crytopia, LiveCoin, HitBTC, Coss.io, Liqui, and Bitfinex," the

lawsuit said. Hackers also changed the passwords "for approximately 15 of Mr. Shapiro's online accounts, including four email addresses, his Evernote account… and his PayPal account," the lawsuit said.

After taking control of his cryptocurrency accounts, "hackers then transferred Mr. Shapiro's currency from Mr. Shapiro's accounts into accounts that they controlled. In all, they stole more than $1.8 million from Mr. Shapiro in the two consecutive SIM swap attacks on May 16, 2018," the lawsuit said.

14 hours later…

Shapiro says he regained access to his email and other personal accounts within 14 hours, but he never regained access to several cryptocurrency accounts and had already lost the money. As we noted in a previous article, thefts of cryptocurrency are likely permanent "since no one has the authority to cancel transactions once they're committed to the blockchain."

Shapiro says that he remained an AT&T customer after the hack based on the company's assurances that it would protect his data going forward. He changed his AT&T account passcode on the company's advice, which was supposed to prevent further SIM swaps from happening without his consent. But "Mr. Shapiro's trust in AT&T was misplaced," as he ended up being victimized by SIM swaps twice more, in November 2018 and May 2019, the lawsuit said.

Shapiro says he received a letter from AT&T in May 2019 informing him that "an employee of one of [AT&T's] service providers accessed [Mr. Shapiro's] Customer Proprietary Network Information [CPNI] without authorization." The letter also said that AT&T "notified federal law enforcement concerning the unauthorized access of your CPNI as required by Federal Communications Commission regulations."

In the lawsuit, Shapiro blames AT&T for making it possible to perform SIM swaps without his consent. AT&T's failure to establish a proper level of security means that its promises to consumers were misleading, the lawsuit said:

> *AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Shapiro's account and the data therein was used without his authorization or consent, and disclosed to third parties. Mr. Shapiro's privacy and personal information was not safe, as demonstrated by the repeated breaches of his AT&T account. AT&T's statement that it would protect customers' privacy and keep their personal information safe is therefore a material misrepresentation.*

AT&T's promise to users that it doesn't sell personal information was also false, the lawsuit says.

"As alleged fully above, AT&T employees sold access to Mr. Shapiro's AT&T account to third parties," the lawsuit said. "AT&T's statement that it would not sell customers' personal information is therefore a material misrepresentation."

https://arstechnica.com/?p=1591047