Busy North Korean hackers have new malware to target ATMs

Enlarge / ATM in the Indian city of Jaipur.

reader comments

10 with 9 posters participating

Share this story

Hackers widely believed to work for North Korea’s hermit government have developed a new strain of malware that steals data used at automatic teller machines in India, researchers from Kaspersky Lab said on Monday.

One piece of malware, dubbed ATMDtrack by researchers with the Moscow-based security firm, has been targeting Indian ATMs since last summer. It allows its operators to read and store data associated with cards that are inserted into infected ATMs. As researchers with the Moscow-based security firm investigated further, they found that the ATM malware was part of a larger remote-access trojan that carries out traditional espionage activities. Dubbed “Dtrack,” it was used as recently as this month to target financial institutions and research centers.

Dtrack payloads were carefully encrypted with utilities known as packers, which made it hard for researchers to forensically analyze the malware. As the researchers analyzed the memory of infected devices, they found that both ATMDtrack and Dtrack shared unique code sequences. When company researchers peeled

away the layers of encryption and began analyzing the final payload, they saw pieces of code that were first used in a 2013 attack that wiped the hard drives of South Korean banks and broadcasters. The campaign, known as DarkSeoul, was eventually tied to Lazarus Group, the main hacking arm of the North Korean government.

Not your father's ATM malware

"When we first discovered ATMDtrack, we thought we were just looking at another ATM malware family, because we see new ATM malware families appearing on a regular base [sic]," Kaspersky Lab researcher Konstantin Zykov wrote in a post published Monday. The reused code made clear that Dtrack and ATMDtrack were actually the work of the same group of hackers behind the 2013 attack that wreaked havoc on South Korea.

Lazarus first landed on the radar of many security researchers following the destructive hack on Sony Pictures in late 2014. Once considered a ragtag ensemble of hackers, the group has risen to prominence over the years with a series of lucrative hacks on the SWIFT payment network used by banks.

A wide variety of researchers and analysts say Lazarus was also behind the WannaCry ransom worm that shut down computers around the world in 2017. News agencies including Reuters have cited a United Nations report from last month that estimated North Korean hacking has generated $2 billion for the country's weapons of mass destruction programs. The Trump administration sanctioned people associated with Lazarus and the two of its subgroups 10 days ago.

The more than 180 samples of Dtrack Kaspersky Lab has found circulating in the wild demonstrate yet another campaign of this now-prolific hacking group. The discovery of the malware in 2018 and the use of it as recently as this month suggest that Dtrack is a new addition to the growing Lazarus toolset. Samples analyzed by Kaspersky Lab include the following

capabilities:

- keylogging
- retrieving browser history
- gathering host IP addresses, information about available networks and active connections
- listing all running processes
- listing all files on all available disk volumes

Monday's post demonstrates a previously unknown capability of this already prolific group.

"The vast amount of Dtrack samples that we were able to find shows that the Lazarus group is one of the most active APT groups in terms of malware development," Zykov wrote. "They continue to develop malware at a fast pace and expand their operations."

https://arstechnica.com/?p=1573283

Snapchat reportedly has "Project Voldemort" dossier on Facebook's bad behavior

Enlarge / Mark Zuckerberg testifying before Congress in April, 2018.

reader comments

66 with 43 posters participating

Share this story

Facebook is only 15 years old, yet in that time it has become the world's dominant social media platform, boasting more than 2.4 billion users. It has also become the world's second-largest digital advertising platform, effectively the runner-up in a worldwide duopoly dominated by Google. Now, it is under a baker's dozen of investigations alleging that it rose to the top by using unfair, anticompetitive tactics—and at least one competitor kept records.

Snap, parent company of Snapchat, kept a dossier "for years" detailing Facebook's attempts to thwart it, sources told The Wall Street Journal. The file, dubbed "Project Voldemort" after the just-doesn't-know-when-to-stay-dead villain of *Harry Potter* fame, "chronicled Facebook's moves that threatened to undermine Snap's business."

According to the WSJ, Snap's legal team recorded instances where Facebook discouraged prominent social media influencers with a presence on multiple platforms from mentioning Snap on their Instagram accounts. Snap executives also suspected Facebook was suppressing content that originated on Snap from trending on Instagram, when such content was shared there.

Facebook twice tried to acquire Snapchat and was twice rejected. In 2013, Snap turned down a $3 billion takeover offer. In 2016, Facebook reportedly once again made overtures to the firm, which instead went forward with an IPO early in 2017.

After the snubs, Facebook started cloning many of Snapchat's most popular features, The Economist reported in 2018. Instagram Stories launched in August 2016, and Facebook Stories followed suit in March 2017.

Quashing the competition?

Facebook's behavior toward competitors is at the heart of the many antitrust probes against it. Being the dominant player in a sector is not against the law, even if you're the only real player in a sector—as long as you play fair. Abusing that market power, or actively working to squash, suppress, or buy out competitors, is called anticompetitive behavior. That *is* illegal.

Startups are now harder to, well, start up, The Economist reported last year, thanks to the overwhelming influence the largest tech players—Facebook, Google, and Amazon—have in the sector. "Big tech firms have been known to intimidate startups into agreeing to a sale, saying that they will launch a competing service and put the startup out of business unless they agree to a deal," one source who used to conduct such negotiations on behalf of a big tech firm told The Economist.

The more acquisitions a firm like Facebook makes, the more it's well-positioned to make future acquisitions. The WSJ reports that Onavo, an Israeli startup that Facebook acquired in 2013, is also on regulators' radar. Onavo's free app advertised itself as a VPN… and redirected traffic it carried through Facebook servers, where it could then be logged and analyzed. Data gathered through Onavo gave Facebook a heads up into Snapchat's growing popularity—and also let Facebook see when its Stories features succeeded in siphoning off Snapchat users. Onavo data also helped drive Facebook's 2014 acquisition of WhatsApp.

(Onavo was pulled from Apple's App Store in 2018 and from Google Play a few months later; Facebook finally discontinued it in May.)

Facebook CEO Mark Zuckerberg's actions are also part of the many antitrust probes, the WSJ notes:

> *In some cases, after Facebook's overtures were spurned, the social-media giant copied features of the former targets.*
>
> *For example, when Mr. Zuckerberg met with the founders of startups, including Evan Spiegel, chief executive of Snap, and Dennis Crowley, co-founder of Foursquare Inc., he presented them with two scenarios: either they accept the price he was offering for their companies, or face Facebook's efforts to copy their products and make operating more difficult, according to people familiar with the matter. In both cases, after the companies rejected the overtures, Facebook soon after released features that mimicked the products from Snap and Foursquare.*
>
> *Foursquare in 2014 started shifting from a consumer-focused app to providing location-based tech and data to businesses.*

Widening investigation

At this stage, a list of regulators who aren't investigating Facebook might be easier to compile than a list of regulators who are.

In June, Congress launched an antitrust probe looking at "competition in digital markets." Several hearings related to the issue took place in June and July, and more are scheduled for this fall. The House Judiciary Committee also recently sent a massive request for information to the four companies, seeking a decade's worth of relevant data.

By July, the traditional antitrust regulators were all on board. The Department of Justice publicly confirmed that its antitrust division was actively investigating widespread "concerns that consumers, businesses, and entrepreneurs have expressed" about "market-leading online platforms." The agency didn't name names, but that list of "market-leading" platforms is generally considered to include Amazon, Apple, Facebook,

and Google.

Facebook also told investors that month that it was the target of an open antitrust investigation by the Federal Trade Commission.

Attorneys general for several states also launched an antitrust probe into Facebook earlier this month. New York Attorney General Letitia James, leading the coalition, said the probe would determine “whether their actions endangered consumer data, reduced the quality of consumers’ choices, or increased the price of advertising.”

Meanwhile, Facebook might be an American company, but its global footprint means regulators worldwide have a vested interest in its behavior. The European Union is also actively probing Facebook for antitrust reasons, according to media reports, and member states such as Germany are also taking action. Australian regulators also think they should maybe have a closer look.

https://arstechnica.com/?p=1572957

Yahoo data-breach settlement: You’ll get $100, if you’re lucky

Enlarge / A Yahoo logo on a smartphone.
Getty Images | SOPA Images

reader comments

60 with 44 posters participating

Share this story

People who had Yahoo accounts between 2012 and 2016 can now apply for a cash payment of $100, but the final amount you receive could be more or less than $100 depending on how many people file claims.

It’s also possible to file claims for up to $25,000 if you can document actual out-of-pocket losses and lost time due to the breach. However, actual payouts for all claims could be much lower if the total amount claimed exceeds what’s available from the $117.5 million settlement. The settlement class potentially includes up to 194 million people, so these amounts would be paid in full only if the vast majority of eligible people don’t ask for money.

The settlement website lets all class members choose from at least two years of free credit monitoring services or the $100 cash payment. While that amount isn’t guaranteed, just like in the Equifax settlement, at least the Yahoo settlement website makes that clear up front.

To apply for cash in the Yahoo settlement, you have to check boxes certifying that you already have credit monitoring and provide the name of the company you get the credit monitoring from.

“If you can verify that you already have credit monitoring or identity protection services that you will keep for at least 12 months, you may instead make a claim for a cash payment in an amount of $100, although that amount may be less or more up to $358.80, depending on how many claims are submitted,” the claim form says.

The credit-monitoring-or-cash option is available to US or

Israeli residents who had a free Yahoo account at any time between January 1, 2012 and December 31, 2016. People who paid for premium Yahoo accounts can also receive up to 25% of the amount they paid Yahoo from 2012 to 2016. The 25% option is also available to small businesses that paid for Yahoo service.

If the amount required to fund all requests for money exceeds the amount available in the settlement fund, the cash payments will be distributed on a *pro rata* basis. The possibility of $100 payments ballooning to $358.80 would come into play if the amount requested is lower than what's available.

Huge data breaches led to settlement

The Yahoo settlement stems from a class action lawsuit over data breaches in 2013, 2014, and 2016. The 2013 breach affected all 3 billion Yahoo accounts worldwide. Yahoo has been owned by Verizon since June 2017.

Yahoo agreed to pay for a settlement fund of $117.5 million, including attorneys fees of up to $30 million. The settlement class includes all US and Israeli residents and small businesses with Yahoo accounts, which is at most 896 million accounts and 194 million people.

While it's possible to ask for up to $25,000, this will require documentation of out-of-pocket losses and hours lost to the breach. The settlement website says:

> *You may additionally provide documentation or proof to receive reimbursement of up to $25,000.00 in out-of-pocket losses, including lost time, that you believe you suffered or are suffering because of the Data Breaches. As to documented lost time, you can receive payment for up to fifteen hours of time at an hourly rate of $25.00 per hour or unpaid time off*

> *work at your actual hourly rate, whichever is greater. If your lost time is not documented, you can receive payment for up to five hours at that same rate.*

Claims for credit monitoring or money must be made by July 20, 2020, while objections to and comments on the settlement must be filed by March 6, 2020. Opting out of the settlement must also be done by March 6, 2020.

The sides in the class action lawsuit originally agreed to a settlement of $50 million plus attorneys' fees and other expenses, but it was rejected by US District Judge Lucy Koh in January. They came up with the $117.5 million settlement in April and obtained Koh's preliminary approval.

The settlement is still pending final court approval. The court scheduled a final approval hearing for April 2, 2020.

https://arstechnica.com/?p=1573155

Facebook suspends tens of thousands of apps in ongoing privacy investigation

reader comments

54 with 45 posters participating

Share this story

Facebook—the social media company that has been under intense public criticism for not adequately safeguarding the personal information of its 2 billion users—has suspended tens of thousands of apps for a variety of violations, including improperly sharing private data.

In a post published on Friday, Facebook VP of Product Partnerships Ime Archibong said the move was part of an ongoing review that began in March 2018, following revelations that, two years earlier, Cambridge Analytica used the personal information of as many as 87 million Facebook users to build voter profiles for President Donald Trump's presidential campaign. Facebook has been embroiled in several other privacy controversies since then.

The tens of thousands of apps were associated with about 400 developers. While some of the apps were suspended, in a few cases others were banned completely. Offenses that led to banning included inappropriately sharing data obtained from the Facebook platform, making data available without protecting user's identities, or clear violations of the social network's terms of service.

One of the few apps Facebook identified was called myPersonality. According to Archibong, it "shared information with researchers and companies with only limited protections in place, and then refused our request to participate in an audit."

Friday's post said Facebook took legal action against some groups associated with the apps. Companies LionMobi and JediMobi, Archibong said, used their apps to infect users' phones with malware in a profit-generating scheme. Facebook has already stopped the alleged fraud and refunded advertisers. Facebook has also sued Ukrainian men Gleb Sluchevsky and Andrey Gorbachov for allegedly using quiz apps

to scrape users' Facebook data. Facebook has also sued South Korean data-analytics company Rankwave for allegedly failing to cooperate with the investigation.

Archibong wrote:

> *And we are far from finished. As each month goes by, we have incorporated what we learned and reexamined the ways that developers can build using our platforms. We've also improved the ways we investigate and enforce against potential policy violations that we find.*
>
> *Beyond this investigation, we've made widespread improvements to how we evaluate and set policies for all developers that build on our platforms. We've removed a number of APIs, the channels that developers use to access various types of data. We've grown our teams dedicated to investigating and enforcing against bad actors. This will allow us to, on an annual basis, review every active app with access to more than basic user information. And when we find violators, we'll take a range of enforcement actions.*

According to The New York Times, court documents filed in state court in Boston as part of an investigation by the Massachusetts attorney general into Facebook show that the company has suspended 69,000 apps. Of those, 10,000 were removed from Facebook for potentially misappropriating Facebook users' data, the NYT reported.

Over the past 12 months, Facebook has faced scathing criticism for practices that have revealed personal information of its users. In July, the company agreed to pay the Federal Trade Commission $5 billion to settle charges it "subverted users' privacy choices to serve its own business interests."

Friday's revelations suggest that the scope of the privacy controversies may be bigger than company officials have previously acknowledged. Now would be a good time for readers

who use Facebook to review the apps they've installed and delete any that request large amounts of data or don't provide a meaningful benefit.

https://arstechnica.com/?p=1572585

"Grassroots" anti-Amazon nonprofit turns out to be retailer astroturfing

Enlarge / The Amazon logo at the entrance of a logistics center in France, July 2019.

reader comments

31 with 31 posters participating

Share this story

It's no secret that retailers who compete with Amazon for consumer dollars want regulators to take a closer look at the way their titanic, globe-spanning rival works. They've openly said so, many times. And yet, three major firms reportedly spent a great deal of time and effort obscuring their ties to a nonprofit that exists to rally support against Amazon.

The nonprofit, called the Free and Fair Markets Initiative, describes itself as "a nonprofit watchdog committed to scrutinizing Amazon's harmful practices and promoting a fair, modern marketplace that works for all Americans." According to

a new report today from The Wall Street Journal, however, the group is funded by rivals, including Walmart, Oracle, and mall-owner Simon, who all have a strong financial interest in dethroning Amazon.

All three are competing fiercely with Amazon in their own market sectors. Walmart, the nation's biggest big-box store, competes in retail, selling goods and groceries. Oracle competes in Internet services and has been fighting against Amazon, for example, to secure a $10 billion government contract. And Simon, the country's largest mall owner, is at the front and center of the retail apocalypse and all the dead malls that retail bankruptcies leave in their wake.

FFMI declined to answer questions from the WSJ about its funders, backing, or structure, instead providing the newspaper with a statement saying that it is, "focusing on the substantive issues and putting a spotlight on the way companies like Amazon undermine the public good—something that media outlets, activists, and politicians in both parties are also doing with increasing frequency."

Astroturf, covering up real concerns

Alliances and coalitions form all the time to agitate against something like a major merger, but the Journal notes that it is "rare" for an entire nonprofit group "to be created for the sole purpose of going after a single firm," calling the formation of FFMI, "an indication of the degree to which competing companies have coalesced to counter the growing and accumulated power of Amazon and how far competitors are increasingly willing to go to counter-strike."

But while FFMI might be as fake a "grassroots" organization as ever there was, the growing opposition to Amazon is very real. Genuine nonprofits, such as the Institute for Local Self-

Reliance, have a years-long history of opposition to Amazon's tactics. Community activism in New York City led Amazon to scrap its plans to open a secondary headquarters office location in Queens. And retail trade groups have openly pushed for federal regulators to launch antitrust investigations against the company. Dozens of media reports in recent months have also highlighted privacy and competition issues with Amazon's Alexa voice assistant, Ring home surveillance business, and in-house logistics and delivery business.

The pressure, it seems, is working. The Department of Justice and Federal Trade Commission are both working on big tech antitrust investigations, focusing on Amazon, Apple, Facebook, and Google. Congress is also digging into the way all four companies use their market power and recently asked for a massive trove of documentation from the company about its business practices.

Amazon also faces several antitrust investigations overseas: Germany, Austria, Italy, and the European Union all have separate probes in progress.

https://arstechnica.com/?p=1572197

AT&T tells court: Customers can't sue over sale of phone location data

Getty Images | SOPA Images

reader comments

34 with 27 posters participating

Share this story

AT&T is trying to force customers into arbitration in order to avoid a class-action complaint over the telecom's former practice of selling users' real-time location data.

In a motion to compel arbitration filed last week, AT&T said that plaintiffs agreed to arbitrate disputes with AT&T when they entered into wireless service contracts. The plaintiffs, who are represented by Electronic Frontier Foundation (EFF) attorneys, will likely argue that the arbitration clause is invalid.

The case is pending in US District Court for the Northern District of California. In March 2018, a judge in the same court ruled that AT&T could not use its arbitration clause to avoid a class-action lawsuit over the company's throttling of unlimited mobile data plans. That's because the California Supreme Court had ruled in *McGill v. Citibank* "that an arbitration agreement that waives the right to seek the statutory remedy of public injunctive relief in any forum is contrary to California public policy and therefore unenforceable," the District Court judge wrote at the time.

In the new case, AT&T argues that the *McGill* decision does not apply "because the injunctive relief Plaintiffs seek is directed at a subgroup of AT&T customers, not the general public as a whole."

"Indeed, numerous district courts in this Circuit have held McGill inapplicable when—as here—plaintiffs seek what amounts to private injunctive relief on behalf of a class rather than an injunction benefiting the public in general," AT&T wrote in its motion to compel arbitration.

AT&T also claims that the Federal Arbitration Act (FAA) preempts the *McGill* standard but acknowledged that a panel of judges on a federal appeals court "recently held that the FAA does *not* preempt the McGill rule." AT&T claims that federal appeals court ruling "contravene[s] Supreme Court precedent" and noted that "*En banc* review is being sought" in the case.

AT&T also told the court that AT&T itself shouldn't be a defendant in the case because AT&T Inc. is just "a holding company organized in Delaware and headquartered in Texas" that does no business in California. This motion wouldn't end the case, because two AT&T Inc. subsidiaries, AT&T Mobility and AT&T Services, would still be defendants.

When contacted by Ars, EFF staff attorney Aaron Mackey said the EFF "look[s] forward to responding to the motions" but declined comment on how the group will respond.

Data sales were "dangerous breach of… privacy"

The class-action complaint was filed in July against AT&T and two location data aggregators called LocationSmart and Zumigo. "AT&T used LocationSmart and Zumigo to manage the buying and selling of its customers' real-time location data," the lawsuit said. The lawsuit seeks monetary damages for customers, an injunction preventing AT&T from selling location data, and certification of a class including all AT&T wireless subscribers between 2011 and the present "whose carrier-level location data AT&T permitted or caused to be used or accessed by any third party without proper authorization."

The lawsuit says:

> *Despite vowing to its customers that it does not "sell [their] Personal Information to anyone for any purpose," AT&T has been selling its customers' real-time location data to*

> *credit agencies, bail bondsmen, and countless other third parties without the required customer consent and without any legal authority. AT&T's practice is an egregious and dangerous breach of Plaintiffs' and all AT&T customers' privacy, as well as a violation of state and federal law.*

AT&T previously denied that selling phone location data was illegal, even though Section 222 of the Communications Act says phone companies may not use or disclose customer location information "without the express prior authorization of the customer." The lawsuit alleges that AT&T violated the Communications Act, the California Unfair Competition Law, the California Constitution's right to privacy, and the California Consumers Legal Remedies Act.

A series of reports by Motherboard beginning in January 2019 showed that T-Mobile, Sprint, and AT&T continued selling customers' real-time location data after all the major cellular carriers promised to stop doing so. The data "end[ed] up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country," Motherboard reported at the time. The news site also wrote about AT&T's motion to compel arbitration yesterday.

Wireless carriers now say they've really stopped the controversial data sales. In addition to the case against AT&T in California, more class action suits seeking refunds for customers were filed in May against AT&T, Verizon, T-Mobile, and Sprint in US District Court for the District of Maryland.

https://arstechnica.com/?p=1572295

Comcast promised not to raise prices—guess what happened next

Enlarge / A Comcast sign at the Comcast offices in Philadelphia.

reader comments

47 with 40 posters participating

Share this story

Comcast offered customers in Utah a “lifetime” price guarantee in order to compete against Google Fiber, then later violated the lifetime promise by raising those customers’ prices, according to a lawsuit pending in a federal court.

“In 2016, Comcast was under intense competitive pressure from Google’s high speed fiber-optic data service,” the lawsuit says. In Salt Lake City, “Comcast engaged extra sales staff to try to effectively beat the Google Fiber sales staff as they made their way up and down the streets of each neighborhood. To compete, Comcast sales staff began to offer ‘lifetime’ contracts to some of its customers and sold Comcast’s broadband services by using door to door salespeople, especially in cities and neighborhoods where Google was aggressively offering its fiber-optic service.”

Customer Brian Baker, the plaintiff in the proposed class-action suit, says that in July 2016 he took up Comcast’s offer for a $120-per-month plan including TV, Internet, and phone service. Baker’s lawsuit says he received a mailing from Comcast that said the $120 price would be locked in for as

long as he wanted.

The mailing included a price list, on which a Comcast salesperson had written that “this is a lifetime price” and that “these are not promotional prices—no yearly increases,” the lawsuit said. A copy of this mailing is exhibit B toward the end of this court document.

When Baker contacted Comcast to accept the offer, the salesperson again “emphasized that the Triple Play price was no mere short-term promotion, but was a ‘lifetime price,'” the lawsuit said. Baker and Comcast then “entered into a contract providing that Plaintiff would pay $120 per month for Defendant’s ‘Extreme Triple Play’ services for life,” the lawsuit said. (Another exhibit in the lawsuit shows the service order, but it doesn’t mention a lifetime guarantee.)

The lawsuit claims that “as many as 20% of Comcast’s over 200,000 contracts in Utah may be ‘lifetime’ contracts.” But in June 2019, Comcast increased Baker’s bill by $10 a month, and “Other customers have had their bill unilaterally increased as much as $50 per month over the specified ‘lifetime’ rate,” the lawsuit says.

The complaint continues:

> *Many customers, upon seeing the substantial increase in monthly billing, contacted Comcast and were told by Comcast employees or representatives that Comcast’s “lifetime” plan does not exist in spite of the previous representations by its sales staff and in spite of the numerous written contracts with the “lifetime” language prominently displayed.*

Seeking class-action certification

The lawsuit was originally filed in a Utah state court on August 14 and was transferred last week at Comcast’s request to US District Court for the District of Utah. We contacted

Comcast about the lawsuit today and will update this story if we get a response. Comcast has until October 18 to file an answer to the complaint in court.

The lawsuit seeks certification of a class including all people who “entered into a ‘lifetime’ contract with Comcast on which Comcast reneged.” It further seeks financial damages and an “order enjoining Comcast from increasing the price on other lifetime contracts and restoring the price to original levels for contracts it has breached.”

Comcast’s alleged reneging on the lifetime prices came after Google Fiber pulled back from its ambitious fiber broadband plans. In October 2016, Google announced layoffs and that it was “pausing” or ending fiber operations in 10 cities where it hadn’t yet fully committed to building.

Google Fiber continued offering service in most areas where it was already available, including Salt Lake City. But construction slowed down, leaving many Salt Lake City residents without the option to purchase Google Fiber and making it easier for Comcast to hold onto customers.

https://arstechnica.com/?p=1571273

Musk spent $50,000 digging into critic’s personal life

Enlarge / Elon Musk in 2015.

reader comments

352 with 173 posters participating

Share this story

Elon Musk spent more than $50,000 digging into the personal life of British expat and Thai caver Vern Unsworth in summer 2018 in an effort to substantiate the claim that he was a "pedo guy." Musk revealed the spending in his latest response to a defamation lawsuit Unsworth filed against him last year.

Initially, Musk's investigator turned up some seemingly damning information about Unsworth, including a claim that Unsworth began dating his wife when she was around 12 years old. However, further investigation failed to confirm this claim, with the investigator finding she was actually around 18 years old when the couple met. (The wife, Woranan Ratrawiphukkunand, later told UK newspapers she was 33 when they met.)

But Musk argues that it doesn't matter, legally speaking, if his claims about Unsworth were actually true. What matters is that Musk believed the claims were true at the time he repeated them to BuzzFeed reporter Ryan Mac.

Musk also blames Mac for publishing the email even though Musk had marked it as "off the record." Ultimately, Musk argues, he shouldn't be held legally responsible for false claims about Unsworth winding up in the media.

At the same time, Musk argues that his initial statement about Unsworth—that he was a "pedo guy"—wasn't intended to be a factual claim at all. Instead, he says, it was intended to be taken as a generic insult.

“Sorry, pedo guy, you really did ask for it”

The bizarre legal battle began last July when Musk had a team of SpaceX engineers construct a miniature submarine to help rescue kids stranded in a cave in Thailand. Musk thought two divers could carry the craft between them as they exited the cave.

Ultimately, Thai officials rescued the boys without Musk’s help. Unsworth, a cave expert who helped plan the rescue effort, went on CNN to talk about the effort. Asked about Musk’s project, he described it as a publicity stunt that had “absolutely no chance of working.” He encouraged Musk to “stick his submarine where it hurts.”

On Twitter, Musk vowed to prove Unsworth wrong by demonstrating that the submarine could be squeezed through the cave’s narrowest passages. “Sorry pedo guy, you really did ask for it,” he tweeted. When pressed on the “pedo” charge, Musk added “Bet ya a signed dollar it’s true.”

Musk apologized a few days later and deleted his tweets. But he didn’t seem all that sorry. “You don’t think it’s strange he hasn’t sued me?” he asked on Twitter in late August.

In July, Musk asked the head of his family office, Jared Birchall, to retain a private investigator to dig into Unsworth’s personal life. Birchall says that, in a series of phone calls, investigator James Howard told him that Unsworth’s wife was 11 or 12 at the time the couple started dating. In a subsequent written report, Howard stated that Unsworth’s wife was actually around 18 at the time they met.

Musk says his claims about Unsworth living in Pattaya Beach also came from Howard. In a report, Howard wrote that he was trying to verify that Unsworth had moved to a part of Thailand renowned for sex trafficking—which would bolster the view that

he was a “sexpat.” Howard explained that a sexpat is someone who “whore-mongers his way through the go-go bars of Thailand.” He reported that Unsworth was an “unpopular loner” and that some other expats found Unsworth “creepy.”

Around the same time, Buzzfeed reporter Ryan Mac asked Musk for comment about his dispute with Unsworth. Musk responded with accusations that were apparently drawn from Howard’s findings:

> *He’s an old, single white guy from England who has been traveling to or living in Thailand for 30 or 40 years, mostly Pattaya Beach, until moving to Chiang Rai for a child bride who was about 12 years old at the time. There’s only one reason people go to Pattaya Beach. It isn’t where you go for caves, but it is where you’d go for something else. Chiang Rai is renowned for child sex-trafficking.*

Musk wrote “Off the record” at the top of the email, apparently expecting that would obligate Mac not to publish his comments. But Mac hadn’t promised Musk to keep his email confidential, so he published it in full.

Musk blames Mac for publishing the emails

The Buzzfeed email probably represents Unsworth’s strongest chance of winning the lawsuit, since it contains specific, factual claims about Unsworth—especially the claim that he moved to Chiang Rai for a 12-year-old bride. But Musk argues that there are two reasons he shouldn’t be held responsible for that apparently false claim.

Musk “believed the investigator to be credible” and didn’t entertain serious doubts about his findings, Musk says. Musk argues that paying $50,000 for Howard’s work is a sign that Musk believed he was getting high-quality information—even if

the information ultimately turned out to be faulty.

Second, Musk didn't expect Mac to publish the emails. Musk says he believed that journalistic ethics required Mac not to publish emails that were marked as off the record (many journalists disagree). He also believed that Mac would verify the salacious information before disseminating it to a broad audience.

Finally, Musk argues that he is on solid legal ground because Unsworth was a public figure in the context of the Thai cave rescue debate. American courts have set a high bar in defamation cases involving public figure: a plaintiff must show that a defendant showed "actual malice" in the publication of defamatory information. Mere sloppiness isn't enough—under this standard, if Unsworth is held to be a public figure he would have to show that Musk either deliberately printed false information or showed reckless disregard for the truth.

Musk has sought to depose Mac for the case, but Buzzfeed has objected, arguing that Mac has already supplied both parties all relevant information about the case. Buzzfeed argues that Musk is trying to harass Mac and punish him for publishing Musk's emails.

Musk: "Bet ya a signed dollar" was actually an expression of uncertainty

Musk claims that he didn't mean for people to take his "pedo guy" insult literally. He claims that this was a schoolyard taunt he heard growing up in South Africa and that it was a generic insult rather than a factual claim about the subject engaging in pedophilia.

A tricky thing about this claim, however, is that Musk

followed it up by tweeting “bet ya a signed dollar it’s true”—which seems like confirmation that he meant it to be taken literally.

But Musk argues that’s wrong. Rather, Musk’s lawyers write, it was a “flippant comment” that Musk didn’t intend to be taken seriously.

“By proposing such an insubstantial wager, Musk was not taking a strong position as to whether his statements were true, or even capable of being proven true,” his lawyers write. Rather, they claim Musk meant to covey “obviously I’m not certain about this.”

Hence, Musk’s lawyers conclude, “there is no evidence that Musk intended or believed that his July 15 tweets, that Unsworth was “pedo guy'” would be interpreted as fact.

There’s an obvious tension between the two halves of Musk’s argument. On the one hand, he argues that his early tweets—that Unsworth was a “pedo guy” and Musk would “bet ya a signed dollar” it was true—was meant to be merely generic insults, not factual claims. But if that’s true then why would Musk spend $50,000 to substantiate claims that weren’t intended to be taken literally?

On the flip side, the fact that Musk first tweeted about Unsworth being a “pedo guy” before launching his investigation of Unsworth could make it easier for Unsworth to argue that Musk had shown reckless disregard for the truth.

Ken White, a First Amendment lawyer who runs the Popehat blog, argues that Musk’s arguments could ultimately prevail, but it won’t be a quick victory. His argument “isn’t the best fit for a summary judgment motion, which requires that there be no material disputed facts,” White wrote in an email to Ars. There are plenty of disputed facts here. So we can expect this case to drag on for some time to come.

https://arstechnica.com/?p=1569951

Trump to eliminate California's car emission standards waiver

reader comments

302 with 149 posters participating

Share this story

The New York Times reports that the Trump administration will use a meeting at the Environmental Protection Agency on Wednesday to announce the revocation of California's ability to set its own air pollution standards. The state's authority was granted by a waiver that allows it to set pollution limits that are stricter than the federal government's, which is now threatening the administration's ability to roll back Obama-era standards for automobile fuel economy. This move has been rumored to be under consideration for months and sets up a legal showdown that will pit the federal government against California and the 13 states that plan to follow its lead.

As part of the Obama administration's push to limit greenhouse gas emissions, the Obama-era EPA negotiated a deal with automakers that would significantly improve the efficiency of future vehicles. As with many Obama-era environmental accomplishments, that agreement has been targeted by the Trump

administration. In its analysis, the Trump EPA claimed that fuel-efficient vehicles would increase the fatalities from automobile accidents and proposed freezing fuel efficiency at 2020 levels while preparing new standards. But that analysis was hammered by scientists, who suggested that its cost/benefit analysis was flawed and that it failed to take into account negative consequences.

Meanwhile, various news reports indicated that automakers were uneasy about the degree to which the Trump administration was intending to cut back on automotive efficiency. Part of that unease was likely due to the fact that the automakers are already building far more efficient vehicles for markets that do have stricter standards. But a major factor for automakers was California's likely unwillingness to go along with the changes.

During the initial implementation of the Clean Air Act, the Golden State was suffering from extensive smog problems and was granted a waiver that allowed it to set stricter pollution standards than those under the Clean Air Act. The waiver has since given the state significant leverage in negotiations regarding national automotive pollution controls, a position enhanced by the decision of a number of states to adopt whatever standards California sets. Due to the vast size of these states' collective economies, car companies are compelled to meet its pollution standards or generate two different products: one for California and one for the rest of the country. Most have found it easier to simply involve California in negotiations from the start.

Thus, the automakers were worried that the Trump administration was preparing standards that California would never agree to and therefore would likely produce a bifurcation in the US market. Indications are that the Trump EPA is now caught in the middle of balking automakers, decisions that are difficult to justify scientifically (and thus in court), and the hard-line deregulatory stance of

administration officials.

A secret plan

That’s where things stood in July, when California sprung a surprise: it had secretly negotiated a deal with Honda, Ford, Volkswagen, and BMW that would see the automakers meet standards that were substantially higher than those being considered by the EPA. That did not sit well with the administration, which reportedly launched an antitrust probe focused on the automakers, a move that drew Congress into the disagreement.

All of which would explain why the Trump administration would be interested in revoking the state’s waiver and why it’s already laid out arguments to justify doing so. The Times reports that this isn’t an indication that the EPA has decided what the new standards should be yet, simply that the agency is clearing the way to impose the standards when they’re ready.

But the Clean Air Act waiver mechanics are set up so that the EPA administrator must grant a waiver to any state wanting stricter standards unless the state is acting in an “arbitrary and capricious” manner or its standards don’t address “compelling and extraordinary conditions.” California would certainly have compelling arguments that climate change represents a compelling and extraordinary condition. And it’s near certain that the state would be willing to test those arguments in court.

https://arstechnica.com/?p=1570159

Video: DOD pulls plug on Boeing/Raytheon missile interceptor program

reader comments

13 with 12 posters participating

Share this story

SITREP: The RKV has been cancelled, meaning multi-target ballistic missile interceptors are even further off.
With North Korea throwing missiles around again and Iran continuing to depart from the nuclear framework after President Donald Trump exited the deal and re-imposed sanctions, there is as much reason as ever to be concerned about the United States' nascent anti-ballistic missile defenses. While the Missile Defense Agency's Ground-based Midcourse Defense System (GMD) and the Navy's Aegis Ballistic Missile Defense system have shown some promise in testing, there are still some weaknesses in those systems that could be exploited by an attacker—including the use of multiple decoys to soak up attempted intercepts.

That was the rationale behind the Redesigned Kill Vehicle (RKV), a $1 billion program intended to create the US military's next ballistic missile interceptor. A joint effort by Boeing and Raytheon, RKV was supposed to give GMD the capability of engaging multiple targets with a single interceptor. The RKV was intended to build on the Exo-Atmospheric Kill Vehicle, or EKV, currently deployed as part of the Missile Defense Agency's Ground-based Midcourse Defense

System. But the RKV program has been cancelled, and the Department of Defense has put the whole program back into competitive bidding after having been placed on hold for evaluation in May by Undersecretary of Defense for Research and Engineering Michael Griffin.

There are currently 44 interceptors equipped with the EKV deployed at Fort Greely in Alaska and Vandenberg Air Force Base in California. The Defense Department plans to add 20 more silos at Fort Greely for additional interceptors. But the EKV has had some problems even hitting a single simple target, scoring 11 hits on ICBM-like targets out of 19 tries.

Meanwhile, the US Navy will deploy a new Aegis Ashore missile defense system in Poland by the end of the year, and it’s looking at potential deployments in Guam and Hawaii. Japan is buying its own Aegis Ashore system to defend against potential North Korean missile threats. But the latest missile for the Aegis ballistic defense system, the SM-3 Block IIA, is also not trouble-free—a test firing from an Aegis Ashore test site in Hawaii last year missed its target, but it succeeded in a ship-based test last November.

Listing image by Missile Defense Agency

https://arstechnica.com/?p=1569711