It’s becoming clear why the US’ response to COVID-19 is terrible



reader comments

506 with 216 posters participating

Share this story

Covid-19 Coverage

View more stories

The United States, already in possession of the largest number of infections in the COVID-19 pandemic, seems strangely committed to making things worse. As new infections have shot up to record levels, a major retailer made basic protective steps optional before reversing its decision, while the governor of Georgia is moving to block any local authorities

from acting to protect their citizens. This is despite the fact that the head of the US Centers for Disease Control (CDC) has said: “If we could get everybody to wear a mask right now, I really think in the next four, six, eight weeks, we could bring this epidemic under control.”

And it’s not just masks. Health experts are nearly unanimous in indicating that reopening schools should only take place in the context of having a low infection rate in the community, classrooms redesigned to allow greater social distancing, and distance learning used where needed. But the Trump administration is threatening to withhold funding from any schools that do not fully reopen for in-person education. Meanwhile, the administration is attempting to downplay the value of one thing—more testing—that could help us understand the virus’s progression through our population.

What in the world is going on?

This weekend delivered a few explanations for how the US went so badly wrong. One was in the form of a detailed account of how key decisions were made as the US approached its initial peak in infections. The second is an interview with President Trump himself, who comes across as living in a world of misinformation and conspiracy theories.

Problems at the top

Over the weekend, President Trump sat down for an extended interview with Fox News’ Chris Wallace. The interview touched on the pandemic multiple times and provides a window into Trump’s ideas about what’s going on. And it is revelatory, in that it revealed that he’s got a lot of ideas but very few of them have a basis in reality—and the interview brings out several of the reasons for the problems.

One of the most striking cases came when Wallace challenged Trump about the United States being one of the worst countries

in terms of its mortality rate due to COVID-19. Trump responded by getting his press secretary, Kayleigh McEnany, to hand Wallace a graph that supposedly contests this fact. The graph, however, only showed data from a handful of countries, with the US appearing better than some but worse than others. This suggests that part of the problem is that Trump isn't getting the full picture from his advisers and isn't engaged enough in the issue to realize the picture he's gotten is incomplete.

Trump's tendency to make things up in order to make himself look good also kicked in. Within the span of a few sentences, he went from "I think we have one of the lowest mortality rates in the world" to claiming the graph showed we had the "Number one low mortality fatality rates," even though the graph showed a couple of countries with better rates.

Trump's loose grasp of the issues also came up when Wallace asked about the huge surge in SARS-CoV-2 infections revealed by testing. Here, Trump repeated a theme he's returned to since cases started growing: it's all because of our testing capacity. "If we didn't test, you wouldn't be able to show that chart," he told Wallace at one point. "If we tested half as much, those numbers would be down."

But, as Ars' Tim Lee described, there's a way to track how much increased testing is influencing the total number of cases detected: the fraction of tests that return a positive result. And that measure shows that the growth in new cases in the US is being driven by the spread of the virus, rather than expanded testing. Trump *should* know this; the fact that he repeatedly says he doesn't indicates a failure of briefers to get him up to speed or a failure of his ability to process information.

Conspiratorial thinking and policy

But something else seems to be going on, as Wallace followed up with a comparison to the relatively small number of cases in Europe. “Is it possible that they don’t have the virus as badly as we do?” Wallace asked. Trump dismisses this with a conspiracy theory: “It’s possible that they don’t test, that’s what’s possible.”

This sort of conspiracy theorizing is also present in Trump’s response to public health policy within the United States. California has re-instituted restrictions on its citizens in response to the resurgence in cases it’s now experiencing. But, since Trump apparently doesn’t believe there is a resurgence, he suspects it’s a plot against him. “There’s no reason for California to do… to be doing what they’re doing except for November 3rd [election day],” he told Wallace. He later went on to say: “the Democrats want to keep it closed as long as possible because they think that’s good for election. But I think the economy is doing very well.”

And, having constructed an alternate reality in which the number of infections isn’t growing rapidly, Trump is setting policy accordingly. That includes pushing schools to reopen fully for in-person classes this fall or face the threat of a cutoff of federal funding. (To his credit, Wallace points out that this will hit the poorest communities the hardest.)

Huh?

There are, however, some nonsensical policy decisions that don’t fit neatly into any category. Wallace also brought up the CDC director’s argument that recent evidence suggests that population-wide mask use would allow us to get the pandemic under control in a matter of a couple of months or less. But Trump indicates he’s not willing accept expert opinion, much less base policy on it, saying, “I want people to have a

certain freedom, and I don’t believe in that. No, and I don’t agree with the statement that if everybody wears a mask everything disappears.”

The general lack of a grip on reality also seems to be driving other policy decisions that didn’t come up in the interview. On Saturday, The Washington Post revealed the administration is trying to keep Congress from inserting pandemic-focused funding into its next relief bill. Some of the funding at issue would be directed to the CDC—the ones whose advice Trump is dismissing. The rest would be for testing and contact tracing, which Trump blames for making the pandemic look worse than he thinks it is. So it’s clear that Trump’s beliefs, however he came about them, are influencing policy.

Not much help

Also on Saturday, The New York Times published a deeply researched story that describes how the government shifted into a default stance of ignoring the pandemic back when cases were approaching their first peak. The report indicates that, in addition to Trump having a view of matters not based on reality, his administration’s response was largely driven by a small group of senior leadership in the White House, all but one of whom had no medical expertise (naturally, the group included Jared Kushner and Hope Hicks).

Perhaps because of the commitment of some members to a small federal government, the group focused on shifting responsibilities to the states. This, despite some problems with this approach that became obvious early—such as the indications that competition between states for resources like testing kits and protective gear ended up raising prices for them. There are also some issues, like contact tracing, that can’t be handled by individual states, given the ease with which US citizens cross state lines.

The other thing that became clear is that, with only a single

public health expert consistently involved, the group didn't have a good perspective on what was happening with the pandemic. That expert, Dr. Deborah Birx, told the group that, by mid-April, modeling was showing that the United States was nearing a peak. This turned out to be true. But the peak and decline were largely driven by New York and nearby states, which instituted strict social-distancing and isolation rules. According to the Times, the models Birx relied on assumed that all states would take a New York-like approach—a caveat that others in the administration didn't fully register.

Ideology

In fact, the belief that no further restrictions were needed in order for the US to see cases drop to manageable levels fit in with President Trump's belief that it was critical for the economy to restart as quickly as possible. As a result, he started pushing states to reopen before the crest in cases was even reached. Nobody in the administration appears to have re-evaluated the approach despite the fact that, unlike European countries that had seen social-distancing rules followed, the US saw cases remain at a relatively high plateau. That turned out to be the product of the virus being established in the wider US population, setting the stage for its current growth.

A public health disaster of these proportions doesn't happen due to a single personality. Obviously, many officials in the Trump administration have failed the US by allowing their own ideology to drive decisions that went against well-established public health practices. But they've also failed in terms of allowing the president to not only maintain false beliefs but to set policies based on them.

As for Trump, Wallace was actually being understated when he suggested that "people say that you talk about the world as you'd like to see it rather than follow the science." The interview makes clear that Trump is likely to be incapable of

recognizing any science that runs counter to the world as he wishes it to be, much less follow it.

https://arstechnica.com/?p=1693045

Crooks have acquired proprietary Diebold software to “jackpot” ATMs



reader comments

88 with 69 posters participating

Share this story

Diebold Nixdorf, which made $3.3 billion from ATM sales and service last year, is warning stores, banks, and other customers of a new hardware-based form of “jackpotting,” the industry term for attacks that thieves use to quickly empty ATMs.

The new variation uses a device that runs parts of the company’s proprietary software stack. Attackers then connect the device to the ATM internals and issue commands. Successful attacks can result in a stream of cash, sometimes dispensed as fast as 40 bills every 23 seconds. The devices are attached either by gaining access to a key that unlocks the ATM chassis or by drilling holes or otherwise breaking the physical locks to gain access to the machine internals.

In previous jackpotting attacks, the attached devices, known in the industry as black boxes, usually invoked programming interfaces contained in the ATM operating system to funnel commands that ultimately reached the hardware component that dispenses cash. More recently, Diebold Nixdorf has observed a spate of black box attacks that incorporated parts of the company’s proprietary software.

“Some of the successful attacks show a new adapted Modus Operandi on how the attack is performed,” Diebold Nixdorf warned in an active security alert that was issued last week and provided to Ars by a company representative. “Although the fraudster is still connecting an external device, at this stage of our investigations it appears that this device also contains parts of the software stack of the attacked ATM.”

The advisory said elsewhere:

> *In general, jackpotting refers to a category of attacks aiming to dispense cash from an ATM illegitimately. The black box variant of jackpotting does not utilize the software stack of the ATM to dispense money from the terminal.*

> *Instead, the fraudster connects his own device, the "black box," to the dispenser and targets the communication to the cash-handling device directly.*
>
> *In the recent incidents, attackers are focusing on outdoor systems and are destroying parts of the fascia in order to gain physical access to the head compartment. Next, the USB cable between the CMD-V4 dispenser and the special electronics, or the cable between special electronics and the ATM PC, was unplugged. This cable is connected to the black box of the attacker in order to send illegitimate dispense commands.*
>
> *Some incidents indicate that the black box contains individual parts of the software stack of the attacked ATM. The investigation into how these parts were obtained by the fraudster is ongoing. One possibility could be via an offline attack against an unencrypted hard disc.*

Mimicking the ATM computer

The growing number of attacks target the company's ProCash line terminals, particularly the ProCash 2050xs USB model. The ongoing attacks are occurring in "certain European countries," the advisory said.

Bruno Oliveira, an expert in ATM security, said he had heard of the earlier form of black-box attack. The connected device manipulates the APIs included in OS extensions such as XFS or CFS, which communicate with remote servers operated by financial institutions. Black boxes, which mimic an ATM's internal PC, can either be laptops or Raspberry or Arduino hardware that's fairly easy to build, Oliveira said. Black boxes are one of four jackpotting techniques that Diebold Nixdorf describes here.

In some cases, the attached devices connect directly to the

cash dispenser and issue commands for it to spit out cash. The other form of black-box attack plugs into network cables and records cardholder information as it’s relayed back and forth between the ATM and the transaction center that processes the session. The attached device then changes authorized maximum withdrawal amounts or masquerades as the host system to allow the ATM to dispense large sums of money.

The above-linked jackpotting brochure describes two other types of attacks. The first swaps out the legitimate hard drive with one created by the attackers. The other uses phishing attacks against bank employees. Once attackers obtain access inside the network of a financial institution, they issue commands that infect ATMs with malware that can be used to clean out the machines.

Good news and bad news

The new attack variation described by Diebold is both good and bad news for consumers. On the one hand, there’s no indication thieves are using their recently acquired software stack to steal card data. The bad news is that attackers appear to have their hands on proprietary software that makes attacks more effective. The recent increase in successful jackpotting ultimately results in higher fees, as financial institutions pass on the costs caused by the losses. Diebold has issued a variety of defenses that ATM owners can take to protect against the attacks.

There’s little ATM users can do to prevent jackpotting. Still, it’s important to use only ATMs belonging to major banks and eschew those from mom-and-pop businesses. It’s also a good idea to shield the keyboard while entering PINs and to check bank statements each month in search of any unauthorized transactions.

https://arstechnica.com/?p=1692972

Facebook overrides fact-checks when climate science is “opinion”



Enlarge / Facebook’s election “War Room” on Wednesday, Oct. 17, 2018.

reader comments

103 with 71 posters participating

Share this story

Facebook has touted its fact-checking process as one of the ways it intends to fight rampant disinformation heading into the 2020 US presidential election. New reports about the way

the site handles the fact-checking of climate science stories, though, make clear that fact-checking can only work as well as Facebook allows it to—and that the months from now to November are going to be a slog.

Facebook does not employ fact-checkers directly but rather works with a range of third-party organizations to rate how true or false content shared in categories is. The efforts are not universal, however. While Facebook has heavily invested in efforts to stem the overwhelming tide of false and misleading COVID-19 information, for example, it does not heavily fact-check information related to climate change.

The New York Times recently explained the platform's reasoning behind how it handles climate change. Facebook considers opinion content largely exempt from review—and climate change can, as far as Facebook's rules are concerned, be a matter of opinion.

Rarely reviewed, however, is different from never. "When someone posts content based on false facts—even if it's an op-ed or editorial—it is still eligible for fact-checking," Facebook Communications Director Andy Stone told the NYT. "We're working to make this clearer in our guidelines so our fact checkers can use their judgment to determine whether it is an attempt to mask false information under the guise of opinion."

The line has been clear as mud, so far, and Facebook has at least twice overturned the rulings of climate scientists who determine content to be partly or fully false. The first time, a group that partners with Facebook as one of its fact-checkers—Climate Feedback—marked a 2019 Washington Examiner op-ed as false. A climate-change denial organization, the CO2 Coalition, complained to Facebook about the fact-check, and the content warning was then removed.

More recently, an article about climate change published by

The Daily Wire, a right-leaning site that generates very high traffic on Facebook, also earned a “partly false” rating from Climate Feedback. The author of the Daily Wire article publicly complained about being “censored,” and Facebook staff reviewed the fact-check. Popular Information obtained internal Facebook documents showing that the Facebook staff agreed with the “partly false” rating. An email thread that alerted high-ranking company executives to the kerfuffle showed that the fact-checking and communications teams apparently wanted to leave it alone, but the policy team said its “stakeholders” thought the fact-check was “biased.” The notice no longer appears on Facebook shares of the Daily Wire story.

Factually intermittent

Facebook and fact-checking have long had a rocky relationship.

The company first established its system of third-party fact-checking in late 2016 in the wake of the half-dozen privacy and misinformation scandals surrounding the lead-up to that year’s presidential election. Late last year, Facebook unveiled a slew of “election integrity” efforts aimed at avoiding the same pitfalls as we head into the 2020 election.

That election is now just over 100 days away, and those efforts appear to have a mixed success rate at best. One of the few categories of political speech where Facebook does promise a bright line is any attempt at voter suppression. That includes advertisements that contain deliberate misinformation about voting, such as including the wrong date (the big day this year is November 3), as well as any ad that suggests “voting is useless or meaningless, or advises people not to vote.” The policy also prohibits ads that “exclude people from political participation on the basis of things like race, ethnicity, or religion.” Ads that say to vote or not to vote for a candidate because of their race or that threaten violence or intimidation fall under that guideline.

Last week, however, ProPublica reported that explicit misinformation about voting remains rampant on the platform. The problem is particularly pronounced with claims about voting by mail, which have increased as the COVID-19 pandemic has made remote voting seem the safer option for tens of millions of Americans.

“Many of these falsehoods appear to violate Facebook’s standards yet have not been taken down or labeled as inaccurate,” ProPublica notes. “Some of them, generalizing from one or two cases, portrayed people of color as the face of voter fraud.”

False claims about voter fraud that come from politicians and candidates for office, including President Donald Trump, have proved particularly thorny for Facebook. While the platform did pull down ads from the Trump campaign that included misleading claims about the census, Facebook has been highly reticent to touch statements from Trump or the Trump campaign, even when they violate Facebook’s published standards.

A group of senators led by Sen. Elizabeth Warren (D-Mass.) last week demanded Facebook explain its inconsistent position on fact-checking.

“Notably, since Facebook issued a blog post on its efforts to combat misinformation on Facebook in April 2017, disinformation campaigns on the platform have continued and expanded, often with state-sponsored support,” the senators wrote. “If Facebook is truly ‘committed to fighting the spread of false news on Facebook and Instagram,’ the company must immediately acknowledge in its fact-checking process that the climate crisis is not a matter of opinion and act to close loopholes that allow climate disinformation to spread on its platform.”

https://arstechnica.com/?p=1692862

There’s a reason your inbox has more malicious spam—Emotet is back



reader comments

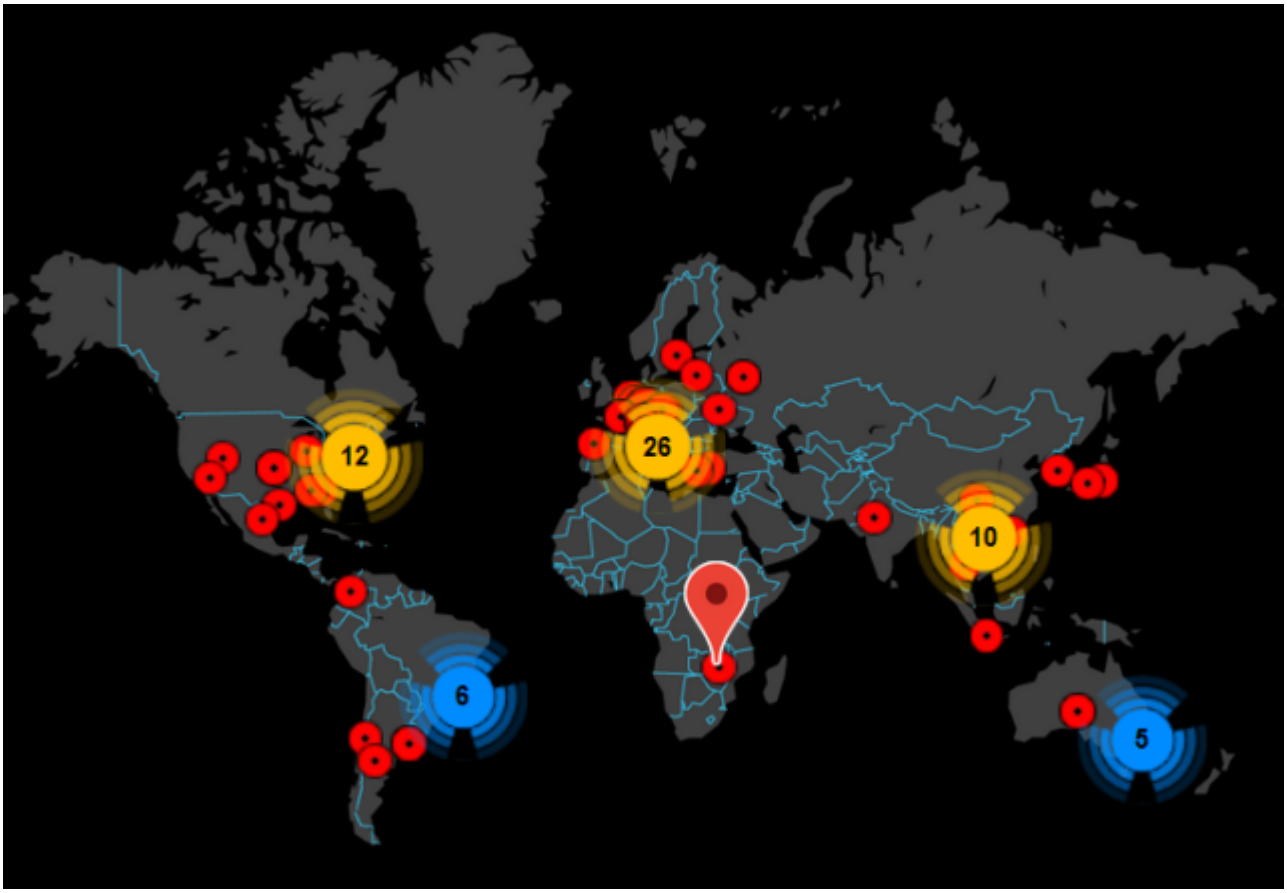
69 with 40 posters participating

Share this story

Emotet, the world’s most costly and destructive botnet, returned from a five-month hiatus on Friday with a blast of malicious spam aimed at spreading a backdoor that installs ransomware, bank-fraud trojans, and other nasty malware.

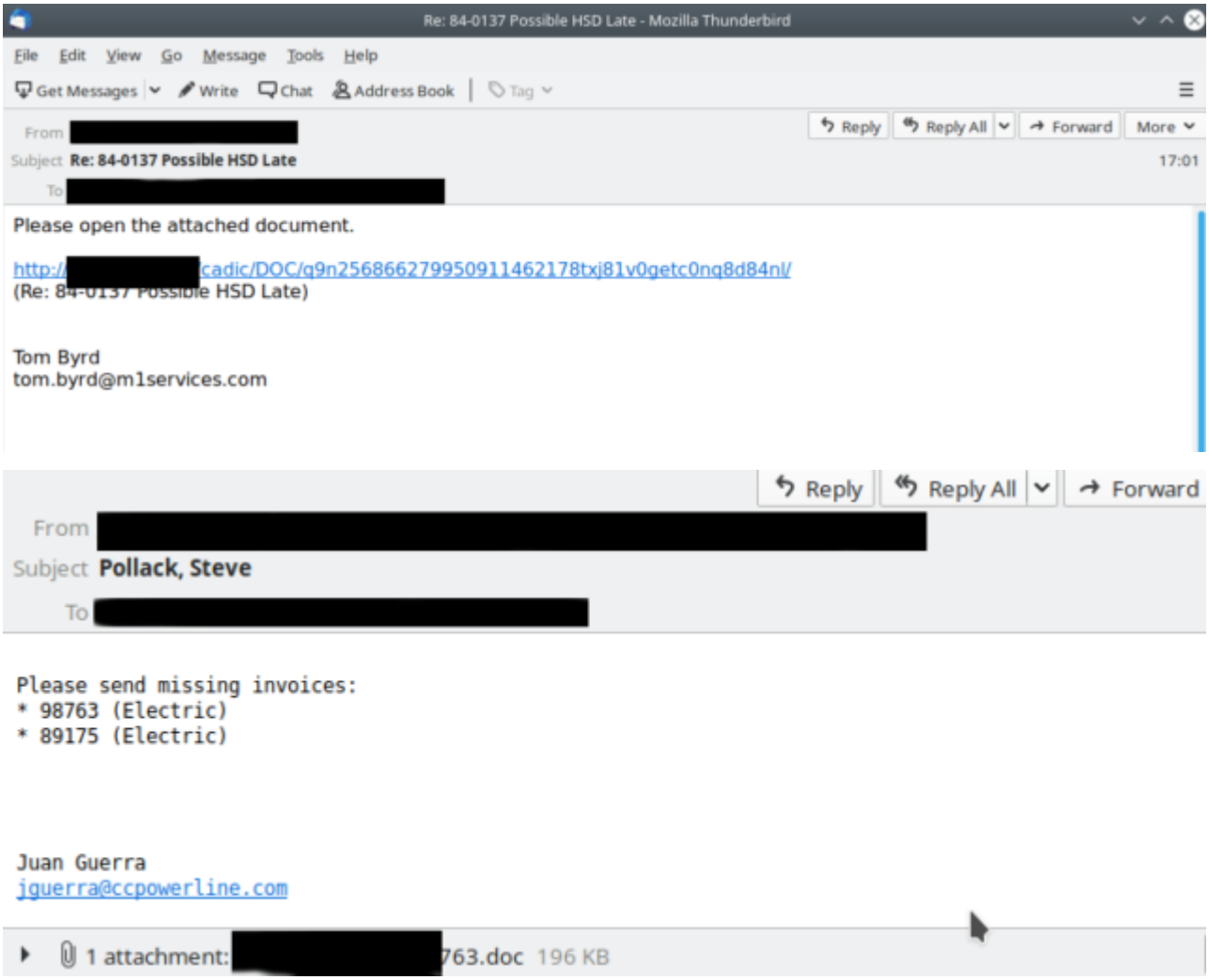
The botnet sent a hefty 250,000 messages during the day, mostly to people in the United States and the United Kingdom, Sherrod DeGrippo, senior director of threat research and

detection at security firm Proofpoint, told Ars. Other researchers said targets were also located in the Middle East, South America, and Africa. The botnet followed its characteristic pattern of sending either a malicious document or link to a malicious file that, when activated, installs the Emotet backdoor.



Enlarge / A map showing where Emotet hit on Friday.

The botnet gave its first indications of a return on Tuesday, with small message volumes being sent out. Email samples that appeared on Twitter accounts from threat monitors abuse.ch and Spamhaus looked like this:



Emotet's resurgence on Friday was also spotted by antivirus provider Malwarebytes and Microsoft.

Box of tricks

Emotet has proven to be one of the more resourceful threats to face people in recent years. Emails often appear to arrive from a person the target has corresponded with in the past. The malicious messages often use the subject lines and the bodies of previous email threads the two have participated in. Emotet gets this information by collecting the contact lists and inboxes of infected computers.

The technique has a dual benefit. It tricks the target into thinking the message can be trusted because it comes from a known friend, acquaintance, or business associate who is following up on a previously discussed matter. The inclusion

of authentic content also makes it harder for spam filters to detect the emails as malicious.

Another of Emotet's clever tricks: it steals usernames and passwords for outgoing email servers. The botnet then uses the credentials to send mail from those servers rather than relying on its own infrastructure. Because the trusted servers send the malicious messages, they're harder for security products to detect and block.

Hit and run

DeGrippo said that the last time Emotet had shown itself was during a five-day run in early February, that delivered about 1.8 million messages. The botnet is known for making big blasts for short periods of time and then going silent for weeks or months at a time. Last September, it woke from a four-month slumber.

The group is known for taking long breaks and regularly taking time off during weekends and major holiday seasons. True to its normal pattern, the latest Emotet activity had completely stopped on Saturday morning, as this post went live. Besides allowing its workers to maintain a healthy work-life balance, the schedule makes campaigns more successful.

"The key for most threat actors is to minimize the time between when [malicious mail] hits the inbox and when it gets opened by the target." DeGrippo explained. "The longer that time elapses, the bigger the risk to the threat actor that their payload won't get delivered because of mitigating controls."

Emotet messages include malicious Microsoft Word documents or PDF files or URLs that link to malicious Word files. The Word documents contain macros that, when activated, install the Emotet backdoor. The backdoor typically waits a period of days before installing follow-on malware, such as the banking

trojan TrickBot or the Ryuk ransomware.

Researchers have published indicators of compromise from Friday's message blast here, here, and here.

Emotet is yet another reminder that people should be highly suspicious of files and links sent in email, particularly if they seems out of context, such as when a friend sends an invoice. People should be doubly suspicious of any Word document that requires macros be enabled before content can be viewed. There is rarely any reason for consumers to use macros, so a good household rule is to never enable them for any reason. A better policy still is to open Word documents in Google Docs, which prevents any malware from getting installed on the local computer.

https://arstechnica.com/?p=1692725

CBP does end run around warrants, simply buys license plate-reader data



Enlarge / A worker for repo firm Relentless Recovery in Cleveland, Ohio, backs a car equipped with automated license plate recognition cameras out of the garage before going out to scan for cars that need to be repossessed on April 30, 2018.

reader comments

161 with 86 posters participating

Share this story

US Customs and Border Protection can track everyone’s cars all over the country thanks to massive troves of automated license plate scanner data, a new report reveals—and CBP didn’t need to get a single warrant to do it. Instead, the agency did just what hundreds of other businesses and investigators do: straight-up purchase access to commercial databases.

CBP has been buying access to commercial automated license plate-reader (ALPR) databases since 2017, TechCrunch reports, and the agency says bluntly that there’s no real way for any

American to avoid having their movements tracked.

“CBP cannot provide timely notice of license plate reads obtained from various sources outside of its control,” the agency wrote in its most recent privacy assessment (PDF). “The only way to opt out of such surveillance is to avoid the impacted area, which may pose significant hardships and be generally unrealistic.”

When reached by TechCrunch for comment, CBP spokesperson Matthew Dyman told the site, “How would you be able to opt out of a license plate reader? Can I opt out of speed cameras here in DC?”

A different spokesperson told Vice Motherboard that the agency uses commercial ALPR databases for tasks such as “locating and apprehending the subjects of criminal investigations, illicit activity, or aliens who illegally entered the United States.”

Previous reporting by Vice led the site to conclude that CBP is likely contracting with a company called Vigilant Solutions, but the agency would neither confirm nor deny Vice’s questions, and the company did not return Vice’s requests for comment.

Get a warrant

Thanks to the US Constitution and decades of case law, there are rules about what data law enforcement agencies can collect directly. For example, the Supreme Court in 2018 ruled that police and other investigators need a search warrant in order to obtain an individual’s mobile phone location data.

The warrant process also allows courts to push back on overbroad requests for information from law enforcement. A judge pushed back on the Department of Justice’s 2017 attempt to get records of more than 1.3 million IP addresses that visited a website organizing a protest against President

Donald Trump, for example.

Massive, privately owned databases, however, so far seem to provide a convenient end run around the warrant process. CBP already buys cell phone location data, even though it would not legally be able to hoover it up on a wide scale directly. Police also purchase hacked and breached data from third-party vendors that they can then use to track and identify individuals in ways that otherwise might have required a warrant.

Although hundreds of jurisdictions nationwide use automated plate-scanning technology, fewer than 20 states have laws of any kind on their books governing the collection, use, and storage of ALPR data. Even fewer of those laws specify what private entities can collect ALPR data and what can be done with that information. The software also seems to become more granular almost by the day.

Theoretically, CBP only has authority to operate within 100 miles of the US border. The data it purchases, however, may allow it to track any given license plate basically anywhere in the country.

Public-private muddy waters

CBP writes in the privacy assessment that the ALPR data to which it has access comes from "both public and private sources," including but not limited to "private businesses (e.g., parking garages), local governments (e.g., toll booth cameras), law enforcement agencies, and financial institutions."

The technology itself continues to spread—not just to businesses and private investigators, but also to individual consumers. A company called Rekor began marketing ALPR technology, adapted for home-surveillance use, to consumers in January of this year. In April, Ars reported on a leaked

survey that showed Amazon floating the idea of ALPR integration into Ring security cameras to some of its customers.

Ring now boasts more than 1,400 active partnerships with local law enforcement agencies all over the country. Police in those towns, cities, and counties are able to request footage from homeowners who use Ring surveillance products. The addition of plate-scanning software to something as widespread as Ring doorbell cameras would then give thousands of police departments potential access to that kind of data as well—regardless of what laws states have on the books about law enforcement use of ALPR.

https://arstechnica.com/?p=1692626

FCC: Phone carriers that profit from robocalls could have all calls blocked



Getty Images | Bill Oxford

reader comments

99 with 62 posters participating

Share this story

“Bad-actor” phone companies that profit from robocalls could be blocked by more legitimate carriers under rules approved unanimously yesterday by the Federal Communications Commission.

Under the change, the FCC said carriers can block calls “from bad-actor upstream voice service providers that pass illegal or unwanted calls along to other providers, when those upstream providers have been notified but fail to take action to stop these calls.” Carriers that impose this type of blocking will get a safe harbor from liability “for the unintended or inadvertent blocking of wanted calls, thus eliminating a concern that kept some companies from

implementing robust robocall blocking efforts."

This expanded level of blocking—spurred by a new law in which Congress directed the FCC to expand safe harbors—could be implemented by companies that sell phone service directly to consumers. That includes mobile carriers Verizon, AT&T, and T-Mobile, traditional landline companies, and VoIP providers.

Carriers won't be able to block calls from just any provider. As Chairman Ajit Pai explained, the safe harbor will be available in cases when the "bad-actor" telecom has been notified by the FCC that it is carrying illegal traffic and "fails either to effectively mitigate such traffic or to implement effective measures to prevent customers from using its network to originate illegal calls."

Allowing carriers to block virtually all calls from a particular provider is a significant change in policy, the FCC said in a draft of yesterday's order:

> *Until very recently, we have only authorized call blocking for particular calls, not based on the provider. In April of this year, the Commission's Enforcement Bureau and the FTC jointly issued letters making clear that, in some instances, provider-based blocking is appropriate. Today, we clarify that voice service providers are permitted to block calls from "bad-actor" upstream voice service providers… The safe harbor thus provides protection to a voice service provider that blocks all calls from a bad-actor voice service provider.*

Accused phone providers would be given 48 hours to "take effective mitigation measures" before other carriers can block their call traffic. The FCC identifies these bad-actor providers using traceback technology, in collaboration with the telecom industry. The new rules are scheduled to take effect 30 days after the FCC order is published in the Federal Register.

Despite the safe harbor, carriers will still have to “make all reasonable efforts to avoid blocking emergency public safety calls,” the FCC said.

FCC threats have been effective

Yesterday’s vote follows other US government efforts to cut robocalls off closer to the source. The FCC sent letters in April and May to six gateway phone companies, telling them to cut off scam robocalls or have all their calls blocked by other phone providers. “Within 48 hours of receiving the letters, each of the gateway providers confirmed they had terminated the robocall traffic,” the FCC said in the draft of yesterday’s order. The Department of Justice also sued two small companies that allegedly connected hundreds of millions of fraudulent robocalls from Indian call centers to US residents.

The new safe harbor is one of several measures adopted in yesterday’s FCC order. Another new safe harbor “protects phone companies that use reasonable analytics, including caller ID authentication information, to identify and block illegal or unwanted calls.” The FCC also laid the groundwork for future rulings by voting to seek public comment “on whether to obligate phone companies to better police their networks against illegal calls, and whether to require them to provide information about blocked calls to consumers for free.”

https://arstechnica.com/?p=1692606

Iranian state hackers caught with their pants down in intercepted videos



Enlarge / The flag of the Islamic Republic of Iran.

reader comments

104 with 58 posters participating

Share this story

Iranian state hackers got caught with their pants down recently when researchers uncovered more than 40GB of data, including training videos showing how operatives hack adversaries' online accounts and then cover their tracks.

The operatives belonged to ITG18, a hacking group that overlaps with another outfit alternatively known as Charming Kitten and Phosphorous, which researchers believe also works on behalf of the Iranian government. The affiliation has long

targeted US presidential campaigns and US government officials. In recent weeks, ITG18 has also targeted pharmaceutical companies. Researchers generally consider it a determined and persistent group that invests heavily in new tools and infrastructure.

In May, IBM's X-Force IRIS security team obtained the 40GB cache of data as it was being uploaded to a server that hosted multiple domains known to be used earlier this year by ITG18. The most telling contents were training videos that captured the group's tactics, techniques, and procedures as group members performed real hacks on email and social media accounts belonging to adversaries.

Included in the footage was:

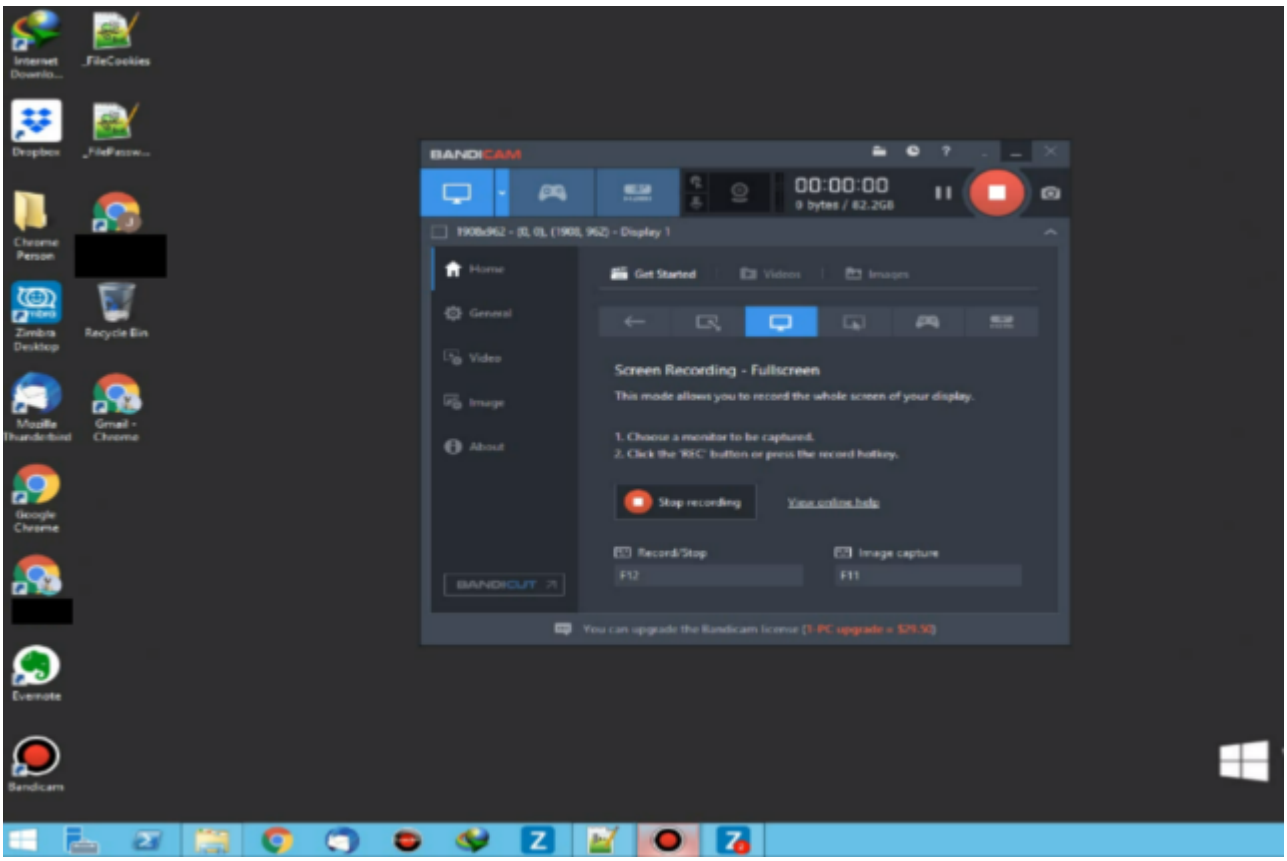
- Almost five hours of video showing operators searching through and exfiltrating data from multiple compromised accounts belonging to two people, one a member of the US Navy and the other a seasoned personnel officer in the Hellenic Navy.
- Failed phishing attempts that targeted US State Department officials and an Iranian American philanthropist. The failures were the result of emails bouncing because they appeared suspicious.
- Online personas and Iranian phone numbers used by group members.

The haul of data is a potential intelligence coup because it allows researchers (and presumably US officials) to identify the strengths and weaknesses of an adversary that is steadily improving its hacking talent. Defenders can then improve protections designed to keep the attackers out. The bird's-eye view may also have signaled plans for future ITG18 operations.

A rare opportunity

“Rarely are there opportunities to understand how the operator behaves behind the keyboard, and even rarer still are there recordings the operator self-produced showing their operations,” IBM researchers Allison Wikoff and Richard Emerson wrote in a post published Thursday. “But that is exactly what X-Force IRIS uncovered on an ITG18 operator whose OPSEC failures provide a unique behind-the-scenes look into their methods, and potentially, their legwork for a broader operation that is likely underway.”

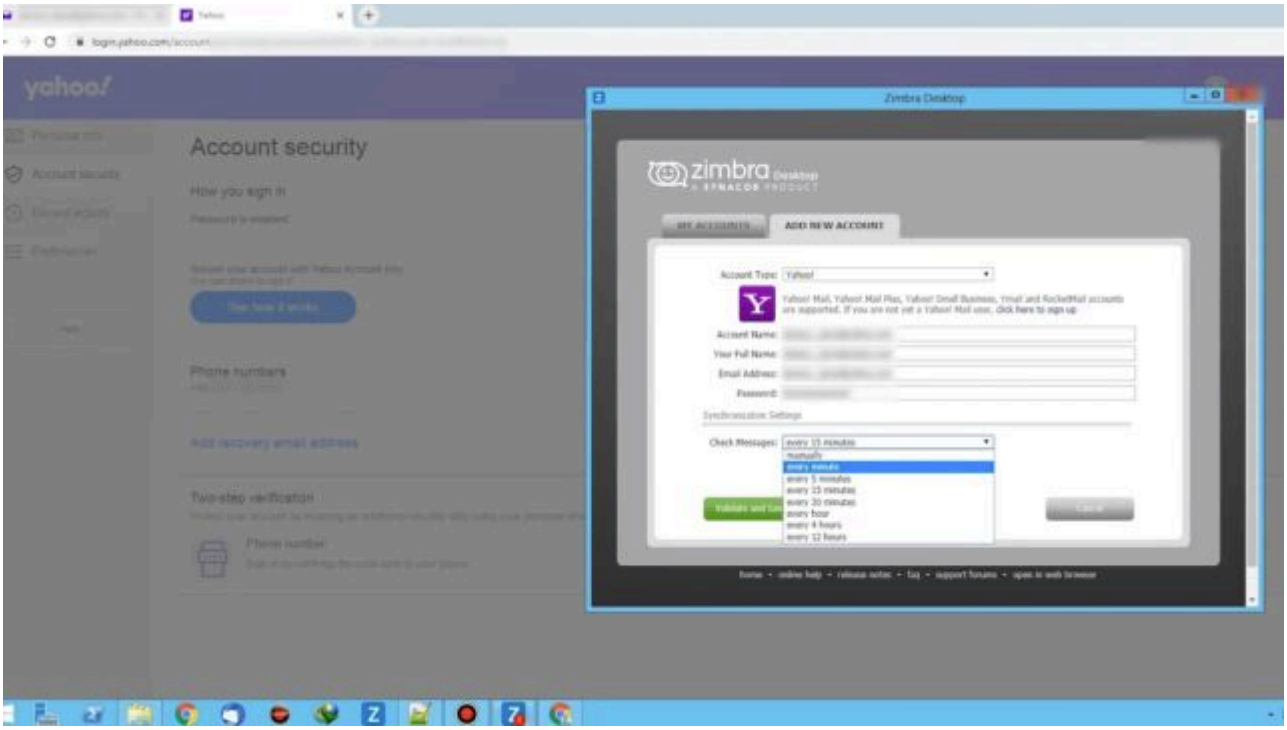
The videos were shot using a desktop recording tool called Bandicam and ranged from two minutes to two hours. Timestamps indicated the videos were recorded a day or so before they were uploaded. Five of the videos showed operators pasting passwords into compromised accounts and then demonstrating how to efficiently exfiltrate contacts, photos, and other data stored there and in associated cloud storage.



Enlarge / An ITG18 operator desktop from a Bandicam recording.

IBM X-Force IRIS

The footage also showed the settings that group members changed in the security configurations of each compromised account. The changes allowed the hackers to connect some of the accounts to Zimbra, an email collaboration program that can aggregate multiple accounts into a single interface. Using Zimbra made it possible to manage hacked email accounts simultaneously.



Enlarge / An image capture of an ITG18 operator syncing a persona account to Zimbra.

BM X-Force IRIS

Three other videos revealed that the operators had compromised several accounts associated with an enlisted member of the US Navy and an officer in the Hellenic Navy. ITG18 members had credentials for what appear to be their personal email and social media accounts. In many cases, the hackers deleted emails notifying the targets that there had been suspicious logins to their accounts.

Painstaking detail

The attackers also accessed files showing the military units the Navy personnel were in, their naval base, residence,

personal photos and videos, and tax records. The operators methodically combed through targets' other accounts, including those on video-streaming sites, pizza-delivery services, credit-reporting agencies, mobile carriers, and more.

"The operators appear to have been meticulously gathering trivial social information about the individuals," the IBM researchers wrote. "In total, the operator attempted to validate credentials for at least 75 different websites across the two individuals.

Other videos displayed the Iran-based phone number and other profile details for a fake persona ITG18 members used in their operations. The video also revealed attempts to send phishing emails to the Iranian American philanthropist and two possible State Department officials.

Another potentially useful discovery: when operators used a password to successfully gain initial access to an account that was protected by multifactor authentication, they would proceed no further. That suggests that Charming Kitten's previously revealed ability to bypass multifactor authentication is limited.

The behind-the-scenes account IBM obtained demonstrates the double-edged sword that's wielded by espionage hackers. While their operations often yield useful information on their targets, the targets can also turn that around in *Spy vs. Spy* fashion.

https://arstechnica.com/?p=1692490

US-EU Privacy Shield data sharing agreement struck down by court



Enlarge / EU Commissioner for Values and Transparency – Vice President Vera Jourova (L) and the EU Commissioner for Justice Didier Reynders (R) are talking to media during the EU Commission press conference on data protection at International Level on July 16, 2020 in Brussels, Belgium.

reader comments

59 with 29 posters participating

Share this story

Europe’s highest court today struck down the agreement by which companies operating in the EU are allowed to transfer data to the United States. The court ruled that the agreement

leaves European customers' data too exposed to US government surveillance.

The agreement, known as Privacy Shield, has been in place since 2016, and more than 5,000 companies operate under its terms. Boiled down, the Court of Justice of the European Union (CJEU) basically ruled that US law is too weak to protect EU citizens' data to the extent EU law demands. As the court put it in a press release (PDF):

> *The limitations on the protection of personal data arising from the domestic law of the United States, on the access and use by US public authorities of such data transferred from the European Union… are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law.*

As a result of the case, US companies doing business in Europe or handling data from European clients will either have to negotiate new individual data-handling arrangements, called Standard Contract Clauses (SCC), with the EU or stop porting data from European operations into the US. The ruling applies to data that companies such as Facebook move around to US servers for internal reasons, but it does not affect "necessary" data transfers, such as take place when someone in Europe sends an email to a recipient in the US, books a flight or a hotel on a US website, or does something equally mundane.

Privacy Shield?

From 2000 to 2015, the agreement governing the sharing of EU customer data between Europe and the United States was called Safe Harbor. The CJEU invalidated Safe Harbor in 2015, following a legal challenge from Maximillian Schrems, a privacy advocate from Austria. In the wake of the Snowden revelations, Schrems alleged the Safe Harbor agreement (which permitted NSA access to EU citizens' personal data) stood in

conflict with EU law. The court agreed and invalidated the Safe Harbor framework in October 2013.

EU lawmakers, together with the US Department of Commerce, rapidly pulled together the Privacy Shield framework after Safe Harbor was tossed, and the European Commission adopted it in 2016. The framework, however, faced deep skepticism before lawmakers even voted to adopt it. EU regulators warned before the deal was even formally signed that "Privacy Shield, as it stands, is not robust enough to withstand future legal scrutiny before the court."

Regulators also warned at the time that Privacy Shield might be in conflict with Europe's sweeping privacy law, the General Data Protection Regulation (GDPR). EU lawmakers adopted that law in 2016, and it has been in effect since 2018.

Schrems in 2016 joked to Ars that although he wanted someone to file suit, he personally wasn't necessarily interested in being the one to do so. As it turns out, however, he did—the case on which the CJEU ruled today is commonly called *Schrems II*—and once again won.

"It is clear that the US will have to seriously change their surveillance laws, if US companies want to continue to play a major role on the EU market," Schrems said in a statement after the CJEU ruling. "This judgment is not the cause of a limit to data transfers, but the consequence of US surveillance laws."

Slow change

Major US tech companies were quick to deliver assurance that the ruling will not substantially change their operations in Europe for the time being, with many confirming they already use SCCs in addition to Privacy Shield agreements.

"If you are a commercial customer, you can continue to use

Microsoft services in compliance with European law," Microsoft wrote in a corporate blog post. "The court ruling does not change your ability to transfer data today between the EU and US using the Microsoft cloud."

Microsoft also plans to "work proactively with the European Commission and the US government to address the issues raised by the ruling," the company added.

Facebook representative Eve Nagle issued a statement saying, "We welcome the decision of the Court of Justice of the European Union to confirm the validity of Standard Contractual Clauses for transfers of data to non-EU countries." The statement added that Facebook, "like many businesses," is now "carefully considering the findings and implications of the decision" and "looks forward to regulatory guidance in this regard."

Replacement?

Tech trade groups wasted no time calling on US and EU regulators to quickly develop a firm regulatory framework to replace the now-defunct Privacy Shield.

"The collapse of the Privacy Shield will disproportionately affect small- to medium-sized businesses that make up 70 percent of the companies using the Privacy Shield," said Morgan Reed, president of the App Association, which represents more than 5,000 app developers globally. "This decision leaves thousands of US and EU companies without a much-needed data sharing mechanism and will significantly disrupt the transatlantic data market, worth hundreds of billions of dollars. We urge the European Union and the US government to negotiate a replacement as quickly as possible to guarantee legal certainty for all businesses who use cross-border data transfers and to ensure the continued growth of the transatlantic data economy."

The Computer & Communications Industry Association—which represents many of the large tech companies you've heard of including Amazon, Facebook, and Google—echoed the sentiment. "This decision creates legal uncertainty for the thousands of large and small companies on both sides of the Atlantic that rely on Privacy Shield for their daily commercial data transfers," CCIA Senior Manager of Public Policy Alexandre Roure said. "We trust that EU and US decision-makers will swiftly develop a sustainable solution, in line with EU law, to ensure the continuation of data flows which underpins the trans-Atlantic economy."

https://arstechnica.com/?p=1692235

Georgia's Republican governor orders cities to stop requiring masks



Enlarge / Georgia Gov. Brian Kemp during a “Wear A Mask” tour stop in Dalton, Georgia, on Thursday, July 2, 2020.

reader comments

382 with 189 posters participating

Share this story

Georgia Governor Brian Kemp yesterday issued an executive order that overturns local mask-wearing requirements.

Kemp’s executive order says that “any state, county, or municipal law, order, ordinance, rule, or regulation that requires persons to wear face coverings, masks, face shields, or any other Personal Protective Equipment while in places of public accommodation or on public property are suspended to the extent that they are more restrictive than this Executive Order.”

Kemp, a Republican, issued the order despite evidence that masks are an effective tool in fighting the COVID-19 pandemic.

Wearing masks is one of several important steps people can take to limit the spread of coronavirus, among others, such as hand-washing and social distancing. Kemp acknowledges that, as his executive order says, “all residents and visitors of the State of Georgia are strongly encouraged to wear face coverings as practicable while outside their homes or place of residence, except when eating, drinking, or exercising outdoors.” Kemp also went on a tour of various cities to encourage mask wearing, but he has said, “we don’t need a government mandate to do the right thing.”

Kemp’s executive order attempts to void rules that “at least 15 local governments across the state had adopted even though Kemp had earlier said cities and counties had no power to order masks,” the Associated Press wrote. Kemp has declined to impose a statewide mandate for Georgia, but 26 US states and the District of Columbia are enforcing mask requirements, according to Axios.

Kemp’s ban on mask mandates puts him at odds with Atlanta, the state capital and most populous city in Georgia with over 500,000 people. Atlanta Mayor Keisha Lance Bottoms, a Democrat, last week issued an executive order requiring masks in commercial spaces and public areas when social distancing is not feasible “in response to the rising number of COVID-19 infections.”

Atlanta will reportedly continue enforcing the mandate despite Kemp’s order. “The Mayor’s Order remains in effect, as science and data will continue to drive the City’s decisions. Masks save lives,” the mayor’s office told Newsweek today.

Other localities may also continue to enforce their rules. “I have been in regular communication with mayors in several other Georgia cities with mask requirements, and we wish for our local requirements to remain in place,” Athens-Clarke County Mayor Kelly Girtz told the Associated Press. “We strongly believe this is within our authority.”

[Update at 7:50pm ET: To enforce his executive order, Kemp today sued Mayor Bottoms and members of the Atlanta City Council in Superior Court of Fulton County. Bottoms criticized the lawsuit on Twitter, writing that "a better use of taxpayer money would be to expand testing and contact tracing."**]**

"Local mask mandates are unenforceable"

Kemp spokesperson Candice Broce wrote on Twitter that "Previous executive orders—and now this order—state no local action can be more or less restrictive than ours. We have explained that local mask mandates are unenforceable. The Governor continues to strongly encourage Georgians to wear masks in public."

Mayor Bottoms said on CNN yesterday that President Trump violated city law by not wearing a mask in Atlanta. "I am somehow not surprised that he disregarded our rules and regulations in this city," she said.

Under the Atlanta rule, "penalties for violations could include a citation, or, in strict enforcement, an arrest," 11Alive reported last week. "If convicted, the sentence could include up to six months in jail or a $1,000 fine." While the Atlanta mask mandate can technically be punished with prison time, Bottoms said that "won't happen to anyone," leaving citations and fines as the enforcement mechanisms. Bottoms said, jokingly, that Trump would only get a "citation that sends him back to Washington, DC."

Georgia, which has 10.6 million residents, has reported 127,834 COVID-19 cases, 3,091 deaths, 14,102 hospitalizations, and 2,702 ICU admissions.

“Kemp does not give a damn about us”

Kemp’s ban on local mask mandates angered Savannah Mayor Van Johnson, a Democrat. “It is officially official. Governor Kemp does not give a damn about us,” Johnson wrote on Twitter yesterday. “Every man and woman for himself/herself. Ignore the science and survive the best you can. In Savannah, we will continue to keep the faith and follow the science. Masks will continue to be available!”

Savannah, which has about 144,000 residents, became the first major city in Georgia to impose a mask mandate on July 1. “The Savannah Police Department has been out enforcing and handing out masks to people who are seen not wearing one,” WTOC reported at the time. Under the rule, people who refuse an offer of a mask can be fined $500.

There are also mask mandates in Athens-Clarke County, Avondale Estates, Brookhaven, College Park, Decatur, DeKalb County, Doraville, Dunwoody, East Point, Fairburn, South Fulton, and Union City.

Oklahoma Gov. Kevin Stitt, a Republican, this week became the first governor of a US state to test positive for COVID-19. Stitt said on June 30 that he “will not consider or reconsider mandating masks. We believe in freedoms.”

https://arstechnica.com/?p=1692276

Musk, Obama, Biden, Bezos, Gates—bitcoin scam hits Twitter in coordinated blitz



reader comments

196 with 140 posters participating, including story author

Share this story

Twitter accounts of the rich and famous—including Elon Musk, Bill Gates, Jeff Bezos, and Joe Biden—were simultaneously hijacked on Wednesday and used to push cryptocurrency scams.

As of 3:58 PM California time, one wallet address used to receive victim's digital coin had received more than $118,000, though it wasn't clear all of it came from people who fell for the scam. The bitcoin came from 356 transactions that all occurred over about a four-hour span on Tuesday. The wallet address appeared in tweets from at least 15 accounts—some with

tens of millions of followers—that promoted fraudulent incentives to transfer money. At least one other Bitcoin wallet was used in the mass scam.

“I’m giving back to all my followers,” one now-deleted tweet from Musk’s account said. “I am doubling all payments sent to the Bitcoin address below. You send 0.1 BTC, I send 0.2 BTC back!” A tweet from the Bezos account said the same thing. “Everyone is asking me to give back, and now is the time,” a Gates tweet said. “I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

Another variation of the scam promoted a partnered initiative that pledged to donate 5000 BTC to the community and included a domain link to send money. The domain was quickly suspended. This variation came early in the hijacking spree and appeared to affect only cryptocurrency-related businesses, including Binance and Gemini.

Other hijacked accounts belonged to Barack Obama, Mike Bloomberg, Apple, Kanye West, Kim Kardashian West, Wiz Khalifa, Warren Buffett, YouTube personality MrBeast, Wendy’s, Uber, CashApp, and a raft of cryptocurrency entrepreneurs. Here’s a sampling of some of the scammy tweets:

At 2:58 PM California time, Musk’s account continued to pump out fraudulent tweets, despite the mass account hijackings being two hours old. What’s more, a screenshot tweeted by a security researcher showed that attackers have changed associated email addresses of some of the hijacked accounts.

That so many social media accounts were taken over in such a short time and remained hijacked for so long is extraordinary if not unprecedented. Previous hijackings that happened to one or two high-profile accounts to promote scams were the result of phishing attacks or the accounts being protected by weak passwords. And in almost all cases, the rightful account

holders quickly regained control.

The ability of the attackers to regain control of accounts was also highly unusual. The compromise of so many accounts—many belonging to people who are seasoned in the importance of having good security hygiene—raised serious questions that the compromises were the result of a breach of Twitter's infrastructure.

A Twitter spokeswoman said company personnel are looking into the cause and would respond soon.

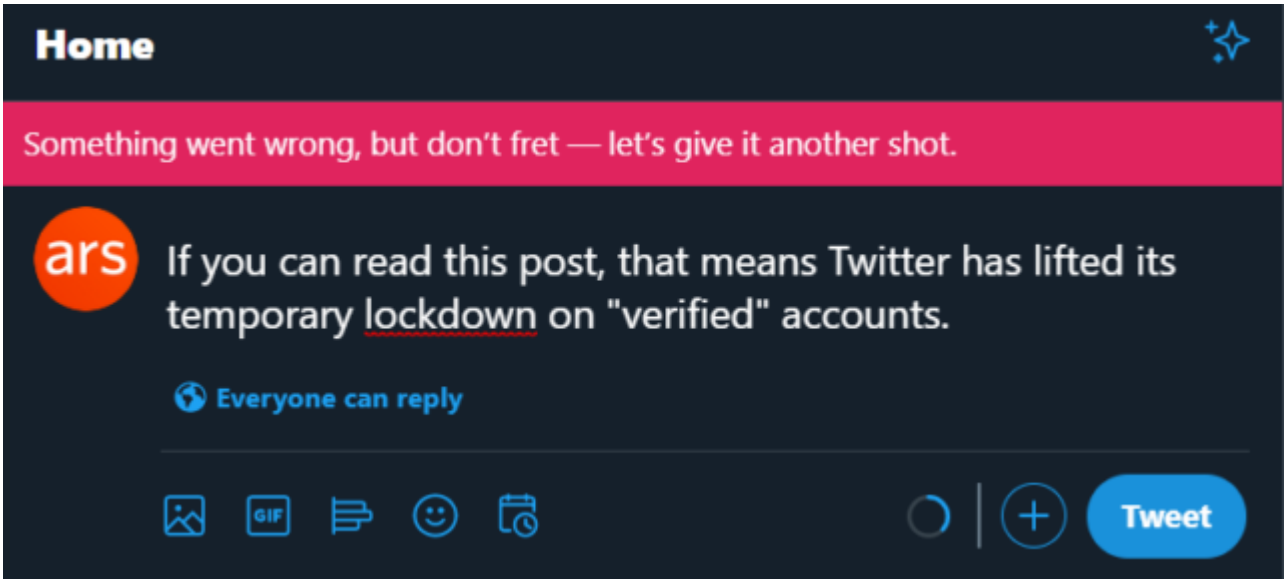
A statement Binance issued said its personnel "confirmed that this Twitter breach was not caused by a vulnerability of Binance's platform or team members." The statement didn't provide any other details about the cause of the hijacking. Binance went on to say: "Our security team has verified that there are zero Binance accounts/users who have sent funds to the hacker's wallet addresses. The hacker's wallets are not associated with Binance, and we have prevented all Binance wallet addresses from depositing assets into the hacker's addresses."

Emails to some of the other affected account holders weren't immediately returned.

A spokeswoman for security firm RiskIQ said company researchers were able to track of the infrastructure belonging to the party behind Wednesday's large-scale hack. So far, they have compiled a list of more than 400 associated domains that included cryptoforhealth.com. the site included in the fraudulent tweet from Binance and other cryptocurrency businesses. Many of the domains didn't respond, while others led to browser warnings like the one below.

As the hijackings continued, Twitter said that while it investigated, it was suspending the ability of many but not all Twitter users to tweet or respond to tweets. Accounts belonging to verified users were unable to tweet or reply to

other tweets. Instead they got a message that said: “This request looks like it might be automated. To protect our users from spam and other malicious activity, we can’t complete this action right now. Please try again later.” The suspension didn’t apply to retweets or direct messages. Unverified accounts worked normally.



This is a developing story. This post will be updated as more details become available.

https://arstechnica.com/?p=1692068