“LokiBot,” the malware that steals your most sensitive data, is on the rise

reader comments

18 with 18 posters participating

Share this story

Federal and state officials are seeing a big uptick in infections coming from LokiBot, an open source DIY malware package for Windows that’s openly sold or traded for free in underground forums. It steals passwords and cryptocurrency wallets, and it can also download and install new malware.

In an alert published on Tuesday, the Department of Homeland Security’s Cybersecurity and Infrastructure Agency and the Multi-State Information Sharing & Analysis Center said LokiBot activity has scaled up dramatically in the past two months. The increase was measured by “EINSTEIN,” an automated intrusion-detection system for collecting, correlating, analyzing, and sharing computer security information across the federal civilian departments and agencies.

“CISA has observed a notable increase in the use of LokiBot malware by malicious cyber actors since July 2020,” Tuesday’s alert stated. “Throughout this period, CISA’s EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected persistent malicious LokiBot activity.”

While not quite as prevalent or noxious as the Emotet malware,

LokiBot remains a serious and widespread menace. The infostealer spreads through a variety of methods, including malicious email attachments, exploitation of software vulnerabilities, and trojans sneaked into pirated or free apps. Its simple interface and reliable codebase make it attractive to a wide range of crooks, including those who are new to cybercrime and have few technical skills.

EINSTEIN isn't the only source that's measuring an increase in LokiBot activity of late. Sherrod DeGrippo, senior director of threat research and detection at security firm ProofPoint, said Emotet typically dwarfs LokiBot by an order of magnitude, with volume on Monday being about 300,000 for the former versus 1,000 for the latter. More recently, there have been exceptions. Last Thursday, for instance, DeGrippo counted a LokiBot run of more than 1 million messages.

Full-featured

The malware includes a keylogger that records passwords and other sensitive keystrokes, code that harvests passwords stored in browsers, administrative tools, and cryptocurrency wallets, and can steal information from more than 100 different applications, according to security firm Gigamon.

According to the MITRE ATT&CK knowledge base of adversary tactics and techniques, a fuller list of capabilities and features includes:

- Discover the domain name of the infected host.
- Use obfuscated strings with base64 encoding.
- Several packing methods for obfuscation of binary files.
- Ability to discover the username on the infected host.
- Ability to initiate contact with command and control to exfiltrate stolen data.
- Process hollowing to inject into legitimate Windows process vbc.exe.
- The ability to capture input on the compromised host via

keylogging.

- Use of HTTP for command and control.
- The ability to discover the computer name and Windows product name/version.
- Can be executed through malicious documents contained in spear-phishing emails.
- Can steal credentials from multiple applications and data sources including Windows operating system credentials, email clients, FTP, and Secure File Transfer Protocol clients.
- The ability to steal credentials from multiple applications and data sources including Safari and Chromium and Mozilla Firefox-based Web browsers.
- The ability to copy itself to a hidden file and directory.

The graphic below, also from the MITRE ATT&CK, lays out some of its capabilities in targeting enterprises.

MITRE ATT&CK

Researchers at Palo Alto Networks said that the LokiBot is the most popular tool used by SilverTerrier, a Nigerian crime group known for performing business-email compromises that

scam high-ranking employees into wiring company funds overseas.

Protecting against LokiBot involves the usual advice about being highly judicious before opening email attachments, not enabling Microsoft Office macros without ample experience and a good reason, steering clear of software that’s pirated or comes from unknown sources, and remaining skeptical online.

https://arstechnica.com/?p=1708765

Blogger who trashed Fauci online “retires” after being ID’d as NIH staffer

Enlarge / Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, wears a Washington Nationals protective mask after a House Energy and Commerce Committee hearing in Washington, DC, on Tuesday, June 23, 2020.

reader comments

170 with 103 posters participating

Share this story

A public affairs officer at the National Institute of Allergy and Infectious Diseases is out of a day job after a report found he was moonlighting pseudonymously as an editor for a

conservative website, where he regularly trashed his agency and its director, Dr. Anthony Fauci.

The RedState managing editor known as “streiff” is actually William Crews, The Daily Beast reported yesterday. Crews was, until this week, a public affairs specialist at NIAID, which is one of the 27 institutes and centers that comprise the National Institute of Health.

As streiff, Crews “derided his own colleagues as part of a left-wing anti-Trump conspiracy and vehemently criticized the man who leads his agency,” according to The Daily Beast. Additionally, he described his boss as “attention-grubbing and media-whoring Anthony Fauci” and “a mask nazi.”

Crews also described the entire pandemic as a “massive fraud,” writing:

> *I think we’re at the point where it is safe to say that the entire Wuhan virus scare was nothing more or less than a massive fraud perpetrated upon the American people by ‘experts’ who were determined to fundamentally change the way the country lives and is organized and governed.*

The Daily Beast diplomatically calls these pseudonymous posts “a remarkable break” from NIAID’s public position—a position that Crews, as a public affairs official, would spend his working hours promoting.

Following The Daily Beast’s reporting, NIAID told media, “Mr. Crews has informed us of his intention to retire,” adding only that it would not comment further on “a personnel matter.”

Murky messages

Unfortunately, Crews is not the administration’s only health communications official who has been simultaneously sabotaging federal efforts at public health messaging.

Michael Caputo, who at the time was the assistant secretary of public affairs for the Department of Health and Human Services, earlier this month released a podcast calling the closure of schools and other efforts to mitigate the COVID-19 pandemic “nonsense.” He also posted a live video to Facebook in which he claimed that the Centers for Disease Control and Prevention harbor a “resistance unit” determined to undermine President Donald Trump, up to and including committing “sedition.” He went on to claim, with absolutely no evidence, that left-wing “hit squads” are preparing for armed insurrection after the election.

Caputo, who is by background a political operative rather than a health expert, announced he would take a leave of absence for 60 days after his remarks in the video and podcast were widely reported. His science advisor, Paul Alexander, also left the agency after emails obtained by Politico showed he had repeatedly tried to prevent Fauci from saying children can spread COVID-19 or advocating they wear masks, among other scientifically false claims.

https://arstechnica.com/?p=1708665

T-Mobile amassed “unprecedented concentration of spectrum,” AT&T complains

Enlarge / A pigeon rests on a T-Mobile logo outside a mobile phone store, operated by Deutsche Telekom AG, in Munich,

Germany, on Monday, Feb. 6, 2017.

reader comments

105 with 74 posters participating

Share this story

AT&T and Verizon are worried about T-Mobile’s vast spectrum holdings and have asked the Federal Communications Commission to impose limits on the carrier’s ability to obtain more spectrum licenses. Verizon kicked things off in August when it petitioned the FCC to reconsider its acceptance of a new lease that would give T-Mobile another 10MHz to 30MHz of spectrum in the 600MHz band in 204 counties. AT&T followed that up on Friday with a filing that supports many of the points made in Verizon’s petition.

T-Mobile was once the smallest of four national carriers and complained that it didn’t have enough low-band spectrum to match AT&T and Verizon’s superior coverage. But T-Mobile surged past Sprint in recent years and then bought the company, making T-Mobile one of three big nationwide carriers along with AT&T and Verizon. T-Mobile also bolstered its low-band spectrum holdings by dominating a 600MHz auction in 2017.

“The combination of Sprint and T-Mobile has resulted in an unprecedented concentration of spectrum in the hands of one carrier,” AT&T wrote in its filing to the FCC on Friday. “In fact, the combined company exceeds the Commission’s spectrum screen, often by a wide margin, in Cellular Market Areas representing 82 percent of the US population, including all major markets.”

T-Mobile’s large spectrum holdings demand “changes in how the Commission addresses additional acquisitions of spectrum by that carrier,” AT&T said in another part of the filing. AT&T also posted a blog on the topic, saying that “Additional spectrum leases with Dish will cause T-Mobile to exceed the

250MHz screen by as much as 136MHz.”

FCC must explain itself, AT&T says

The FCC’s spectrum screen is not a hard-and-fast limit but, rather, one data point the FCC uses in its public-interest analyses. T-Mobile’s new leases in the 600MHz band are with entities called Channel 51 License Company and LB License Co, which do not provide any service over the spectrum.

Even without the pending transactions, Verizon told the FCC that “T-Mobile already holds licenses for 311MHz of low- and mid-band spectrum nationwide. That is more than the low- and mid-band spectrum licensed to Verizon and AT&T *combined*.” Verizon said there is “a high likelihood” of competitive harms being caused by T-Mobile acquiring more spectrum, and it urged the FCC to “reject the arrangements or require T-Mobile to take action to mitigate those harms, including requiring spectrum divestitures.”

Officially, AT&T said it “takes no position on whether T-Mobile’s lease applications were properly accepted by the FCC,” but the company said that the FCC “should provide an explanation of why it permitted T-Mobile to further exceed the spectrum screen.”

“The Commission’s failure to issue a written order in a transaction allowing spectrum aggregation in excess of the screen to this degree is highly unusual… Moreover, without a written order explaining its analysis, there is no evidence that the Commission has carefully attempted to evaluate the potential for competitive harm,” AT&T wrote.

T-Mobile says Verizon is

“disingenuous”

T-Mobile opposed Verizon’s position in an August filing. “Verizon does not even try to demonstrate any harm to itself from the 600MHz spectrum leases—a requirement for petitioners who did not participate in an earlier stage of the proceeding,” T-Mobile wrote. “As a company that elected not to participate in the Commission’s 600MHz auction and currently touts its massive millimeter-wave spectrum holdings as support for 5G superiority, it is simply disingenuous for Verizon to now complain that T-Mobile’s addition of 600MHz spectrum to its portfolio is somehow anticompetitive.”

T-Mobile also said its expanded spectrum holdings will boost competition for home-Internet service, “as T-Mobile plans to use the leased spectrum to offer sorely needed in-home wireless broadband in competition with Verizon—particularly in rural areas.”

Verizon had complained about T-Mobile’s large holdings of low- and mid-band spectrum in big cities including Los Angeles, Chicago, San Francisco, Baltimore, Philadelphia, Boston, Dallas, Houston, and Atlanta. T-Mobile countered that Verizon actually has more spectrum overall in each of those cities when counting the high-band (millimeter-wave) spectrum Verizon uses in its 5G network. But as we’ve covered in numerous articles, millimeter-wave signals don’t travel far and are easily blocked by walls and other obstacles, resulting in Verizon having a sparse 5G footprint. Recent tests by OpenSignal found that T-Mobile has significantly more 5G coverage than its rivals.

https://arstechnica.com/?p=1708362

Everything we know so far about Oracle not actually buying TikTok

Enlarge / ¯_(□)_/¯

reader comments

193 with 107 posters participating

Share this story

It was a weird weekend to end a weird summer for one of the country’s most poular social media apps, TikTok. First, in August, the Trump administration threatened to ban TikTok unless it found a US buyer. Then last weekend, one-time dark horse Oracle emerged victorious in a federally mandated contest to acquire TikTok. Except, it turns out, Oracle isn’t actually acquiring TikTok at all—and Oracle and TikTok’s current parent company, ByteDance, disagree on who is going to be in charge.

If you’re confused, you’re in good company. Here’s our attempt to lay out everything we know about TikTok, Oracle, and their mysterious deal so far.

What is TikTok? Who owns it?

TikTok is an extremely popular short-form video app used worldwide. The app appeared in its current incarnation after its parent company, Beijing-based ByteDance, acquired US startup Musical.ly in 2017 and integrated it with its existing TikTok product under the TikTok name.

Why is TikTok being banned?

President Donald Trump on August 6 issued an executive order determining TikTok to be a national security threat, writing:

> *TikTok, a video-sharing mobile application owned by the Chinese company ByteDance Ltd., has reportedly been downloaded over 175 million times in the United States and over one billion times globally. TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.*
>
> *TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities. This mobile application may also be used for disinformation campaigns that benefit the Chinese Communist Party, such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus.*

TikTok, for its part, has vigorously and repeatedly denied that it passes US user data through China or gives the Chinese government access to US users' personal information.

The ban on TikTok was initially scheduled to go into effect on September 20.

Is that legal?

The White House obviously thinks so. TikTok disagrees. The company filed a lawsuit against the federal government on August 24, arguing that the administration's efforts to ban TikTok or force a sale are part of "an anti-China political campaign" and are "not rooted in bona fide national security concerns."

So TikTok is banned?

Not yet. The Department of Commerce late Saturday issued a one-week extension bumping TikTok's theoretical ban from September 20 to Sunday, September 27. You can still download, update, and use TikTok however you want inside the US today.

They will likely issue another extension before next Sunday's new deadline, unless something else unpredictable happens.

Why is TikTok *not* banned now?

Before issuing the executive order, Trump in early August issued a personal ultimatum to TikTok requiring it to find a US buyer or else face a ban. A second executive order (PDF), issued August 14, determined retroactively that ByteDance should never have been able to acquire Musical.ly in the first place and demanded TikTok be spun back off to a US owner.

Microsoft had since early August been in talks to acquire part or all of TikTok's operations. Oracle and Walmart both entered the race later that month. Late on September 13, The Wall Street Journal was first to announce that Oracle, headed by Trump supporter Larry Ellison, won out in the end.

Did Oracle buy TikTok?

Oracle did not buy and is not buying TikTok—but it is investing in the company.

The transaction, as we currently understand it, has ByteDance spinning off TikTok operations in the United States and most other nations to a new company, TikTok Global.

Oracle will hold a 12.5 percent stake in TikTok Global at its inception and will also serve as the cloud hosting provider for the new entity. Walmart will hold another 7.5 percent stake. The remaining 80 percent will be held by ByteDance. The new company also plans to launch an initial public offering of stock before the end of 2021. That much, we know for certain.

What other conditions are there on the deal?

Oracle and Walmart promised the TikTok Global investment would bring 25,000 jobs to the United States, which Trump now seems to be saying will be based in Texas. The president also first said in August he wanted the Treasury to get a big cut of the deal.

“We set a date, I set a date, of around September 15th, at which point it’s going to be out of business in the United States. But if somebody, whether it’s Microsoft or somebody else, buys it, that’ll be interesting,” Trump told reporters at the time, adding:

> *More than anything else, I said a very substantial portion of that price is going to have to come into the Treasury of the United States. Because we’re making it possible for this deal to happen. Right now, they don’t have any rights, unless we give it to them. So if we’re going to give them the rights, then it has to come into, it has to come into this country…*

> *So it’ll close down on September 15th, unless Microsoft or somebody else is able to buy it, and work out a deal, an appropriate deal, so the Treasury of the— really the Treasury, I suppose you would say, of the United States, gets a lot of money. A lot of money.*

Can he demand that?

Nobody ever has before, and there is no known legal mechanism for it, but the absence of precedents or mechanisms has not previously been a guardrail on the actions of the current administration. The US government can impose certain divestiture and behavioral conditions on mergers and acquisitions to assure antitrust compliance, and of course it can charge taxes on transactions when required. But commissions or kickbacks are not typically part of the process.

Trump on Saturday said the companies would be meeting his terms by “setting up a very large fund” for educational initiatives in Texas. “That’s their contribution that I’ve been asking for,” he added.

Walmart and Oracle said in their joint statement that TikTok Global would contribute more than $5 billion in taxes to the Treasury. The companies also confirmed part of Trump’s “educational fund” comments but did not put a value on that particular contribution, instead saying: “TikTok Global, together with Oracle, SIG, General Atlantic, Sequoia, Walmart, and Coatue will create an educational initiative to develop and deliver an AI-driven online video curriculum to teach children from inner cities to the suburbs, a variety of courses from basic reading and math to science, history, and computer engineering.”

So will TikTok be owned by China or the US?

Whether this proposed transaction puts the company in US hands appears to be wildly up for debate.

About 40 percent of ByteDance itself is held by US investors. Supporters of the deal claim that ownership would therefore translate to about 53 percent of TikTok Global being held by US investors, thus giving the US majority control.

Oracle executive Ken Glueck said today, “Upon creation of TikTok Global, Oracle/Walmart will make their investment and the TikTok Global shares will be distributed to their owners, Americans will be the majority, and ByteDance will have no ownership in TikTok Global.”

ByteDance, however, does *not* see it that way. In a statement today, translated and reported by CNBC and The Wall Street Journal, the company made clear that not only is Oracle not getting its core assets, but Oracle is also not gaining control of the company.

Instead, ByteDance said, TikTok Global will be created as a wholly owned subsidiary. That subsidiary will then do a round of funding (with Walmart and Oracle evidently providing those funds) that will reduce ByteDance’s stake to 80 percent. “The current plan does not involve the transfer of any algorithms and technologies. Oracle has the authority to check the source code of TikTok USA” for security reasons, ByteDance added.

“Eighty percent ownership” and “no ownership” are pretty far apart, as these things go, and it is unclear at best how that difference will be reconciled in the end.

So Trump approved the deal, right?

Yes… until he maybe doesn't anymore.

Trump on Saturday evening gave the deal his "blessing," telling reporters he "approved the deal in concept."

A short time after the president's remarks, TikTok issued a statement confirming the transaction's approval. Around the same time, Oracle and Walmart also issued a joint statement confirming the president's "tentative approval" of the transaction.

Trump touted the deal in an interview with Fox & Friends on Monday but hedged on a full-throated approval.

"It's going to bring 25,000 jobs, and it's going to be located in Texas, and they look forward to doing it," Trump said. "So they're moving it into our country. I like it. But we'll see how it comes out. There can be zero security risk."

"It's going to be totally controlled by Oracle," Trump added. "If we find that they don't have total control, then we're not going to approve the deal."

Is China approving the deal?

That's another giant shrug. The answer, as far as anyone can tell, is: probably. China's export ban prevents the sale of TikTok's proprietary assets to the United States but seems to permit an investment such as the Oracle proposal.

Chinese state-affiliated paper the Global Times this morning described the deal as "unfair" but "reasonable," CNBC reports, finding that the plan would be better than a ban or a full sale to US interests.

However, a few hours later, Global Times editor-in-chief Hu Xijin said on Twitter that, based on his knowledge, "Beijing

won’t approve the current agreement between ByteDance, TikTok’s parent company, and Oracle, Walmart, because the agreement would endanger China’s national security, interests, and dignity.”

The Wall Street Journal reports that experts on China are mixed, finding both that the deal is “daylight robbery” but also describing it as a win for both China and ByteDance.

Does anyone else have to sign off?

Yes. Here in the states, the Committee on Foreign Investment in the United States (CFIUS) also has to approve the planned deal.

CFIUS reviews transactions in which a foreign entity acquires a stake in a US company for any potential national security concerns that may arise. Trump’s second TikTok executive order, the August 14 one, requires CFIUS to oversee ByteDance’s divestment of its US operations. The order puts a 90-day deadline on that divestment, which works out to November 12.

Several Republican senators, including John Cornyn (R-Texas), Josh Hawley (R-Mo.), Marco Rubio (R-Fla.), Rick Scott (R-Fla.), Thom Tillis (R-N.C.), and Roger Wicker (R-Miss.), have all publicly objected to the proposed deal. The Senators all urge CFIUS to reject the proposal, arguing that it is insufficient to prevent the national security threat for which a ban or sale was being required in the first place.

US Treasury Secretary Steven Mnuchin remains confident that CFIUS will greenlight the proposal, Bloomberg reported today, but officials are also reportedly preparing for Trump to change his mind and reject the deal.

https://arstechnica.com/?p=1708267

Proposal would give EU power to boot tech giants out of European market

Enlarge / Belgien, Brussel, Europaische Kommission, Berlaymont-Gebaude, Europa-Flaggen.
Westend61 | Getty Images

reader comments

137 with 86 posters participating

Share this story

The EU wants to arm itself with new powers to take on big technology companies, including the ability to force them to break up or sell some of their European operations if their market dominance is deemed to threaten the interests of customers and smaller rivals.

EU Commissioner Thierry Breton told the Financial Times that the proposed remedies, which he said would only be used in extreme circumstances, also include the ability to exclude large tech groups from the single market altogether.

In addition, Brussels is considering a rating system that would allow the public and stakeholders to assess companies' behavior in areas such as tax compliance and the speed with which they take down illegal content.

"There is a feeling from end users of these platforms that

they are too big to care," said Mr. Breton, who is leading the overhaul of digital rules in the bloc. "[Under] certain conditions we may also have the power to impose structural separation."

His comments followed a public consultation on the EU's forthcoming Digital Services Act, which will set new rules on platforms' responsibilities in dealing with illegal content and disinformation online.

The DSA will update the e-commerce directive, adopted in 2000 when most of the dominant players in the sector were either in their infancy or did not yet exist.

Large technology companies are under pressure from regulators elsewhere. In the UK a new watchdog will have the ability to impose fines without having to go through the courts, as is currently the case. And in the US, tech founders, including Amazon's Jeff Bezos and Mark Zuckerberg of Facebook, struggled to convince members of Congress that they had been driven by more than self-interest when building their digital empires.

The new EU legislation would increase Brussels' powers to scrutinize the way technology companies gather information on users, following concerns raised by independent researchers that the voluntary disclosures groups make are often misleading or partial.

Mr. Breton confirmed that the EU would not remove the limited liability that companies have for the content published on their platforms. "The safe harbor of the liability exemption will stay," he said. "That's something that's accepted by everyone."

However, regulators in Brussels are drawing up a blacklist of activities that technology companies would be required to stamp out. They are proposing a sliding scale of penalties for non-compliance, up to and including the separation of some operations. Mr. Breton said draft legislation will be ready by

the end of the year.

Activities that could lead to tougher sanctions include companies preventing users from switching platforms or forcing customers to use only one service, he added.

Mr. Breton compared the power of the big platforms with that of the banks before the financial crisis, saying regulators need to take similar steps today to rein them in.

“It’s like for small banks and big banks you don’t have the same rules—you have more flexibility for the smaller players and of course when you become a systemic [bank] you have a [different] set of rules,” he said.

Mr. Breton said the new system of oversight will be based on a collective effort between national governments and the EU.

“We need better supervision for these big platforms, as we had again in the banking system [after the financial crisis],” he said.

Proposals are being finalized, and once they are agreed they will go through the European Parliament and the European Council.

One EU official warned that Brussels will need to strike the right balance. “Going overboard can also backfire and you score an own goal,” the official said. “On the other hand, too low an ambition will not address the concerns [about Big Tech].”

© 2020 The Financial Times Ltd. All rights reserved Not to be redistributed, copied, or modified in any way.

https://arstechnica.com/?p=1708269

Court blocks Trump’s WeChat ban from taking effect today

Enlarge / There both is and is not a ban in effect on WeChat.

reader comments

206 with 87 posters participating, including story author

Share this story

A federal judge in California put a temporary halt on the White House’s efforts to ban WeChat inside the United States, preventing that ban from going into effect at midnight tonight.

“The plaintiffs have shown serious questions going to the merits of their First Amendment Claim,” US Magistrate Judge Laurel Beeler wrote in her ruling (PDF) early this morning.

The ruling came in response to a lawsuit filed by a group of WeChat users inside the US. The group, organized as the US WeChat Users Alliance, argued in their complaint that the ban violated their First and Fifth Amendment rights as well as the Religious Freedom Restoration Act and the Administrative Procedures Act. The group also argues that the law cited in the executive order banning WeChat does not in fact give President Donald Trump the authority claimed in the order.

The Alliance established “that there are no viable substitute platforms or apps for the Chinese-speaking and Chinese-American community,” Beeler added. Their evidence shows that

“WeChat is effectively the only means of communication for many in the community, not only because China bans other apps, but also because Chinese speakers with limited English proficiency have no options other than WeChat.”

The government does have a compelling national security interest, Beeler’s ruling concludes, but the administration “has put in scant little evidence that its effective ban of WeChat for all US users addresses those concerns.”

Trump declared WeChat and another China-owned app, TikTok, to be national security threats in August, and the bans on both were slated to go into effect at midnight tonight.

Neither of those bans will now go into effect this weekend, however. WeChat is saved thanks to the preliminary injunction on enforcing the order, and the Department of Commerce announced late last night that it would delay the enforcement on TikTok for at least a week following Trump’s personal approval of a deal between TikTok and Oracle.

https://arstechnica.com/?p=1708153

Trump approves Oracle, TikTok deal “in concept”

Enlarge / It’s official… kind of.

reader comments

135 with 79 posters participating

Share this story

President Donald Trump has reportedly granted his personal approval of Oracle's proposal to invest in TikTok, moving the entire saga one step closer to an end.

The president told reporters this afternoon he approved the deal "in concept," according to Bloomberg News.

"I have given the deal my blessing," Trump said. "I approved the deal in concept."

Late last Sunday one-time dark horse Oracle emerged as the victor in a complex and deeply unusual bidding process for TikTok that kicked off when the White House declared the popular video-sharing app to be a national security threat.

Bloomberg reports that the transaction will leave the majority of TikTok's assets and proprietary algorithms in the hands of parent company ByteDance, with Oracle and other US investors taking minority stakes in the newly-formed TikTok Global.

Trump first said in August that he wanted the US Treasury to receive a cut of the transaction.

"We set a date, I set a date, of around September 15th, at which point it's going to be out of business in the United States. But if somebody, whether it's Microsoft or somebody else, buys it, that'll be interesting," Trump told reporters at the time, adding:

> *More than anything else, I said a very substantial portion of that price is going to have to come into the Treasury of the United States. Because we're making it possible for this deal to happen. Right now, they don't have any rights, unless we give it to them. So if we're going to give them the rights, then it has to come into, it has to come into this country. … "So it'll close down on September 15th, unless Microsoft or somebody else is able to buy it, and work out a deal, an*

> *appropriate deal, so the Treasury of the— really the Treasury, I suppose you would say, of the United States, gets a lot of money. A lot of money/*

The federal government does not generally receive a commission or cut of any merger or acquisition, other than any taxes that may be due, which are paid to the Treasury as required.

According to Bloomberg, the companies have agreed to donate $5 billion to an educational fund based in Texas to meet this particular term. “They’re going to be setting up a very large fund,” Trump said. “That’s their contribution that I’ve been asking for.”

The deal still requires approval from the Treasury department and from Chinese authorities before it can move forward. It is as yet unclear whether Trump’s “blessing” is sufficient to prevent TikTok from being kicked out of Apple and Google’s mobile app stores tomorrow night.

Update, 7:42pm: After Ars first published our story, TikTok issued a statement confirming a few high-level details about the deal.

“We are pleased that the proposal by TikTok, Oracle, and Walmart will reserve the security concerns of the US Administration and settle questions around TikTok’s future in the US,” the company wrote.

Oracle will “become our trusted technology provider, responsible for hosting all US user data and securing associated computer systems,” TikTok added. “Both companies will take part in a TikTok Global pre-IPO financing round in which they can take up to a 20% cumulative stake in the company.”

https://arstechnica.com/?p=1708137

Telegram messages are a focus in newly uncovered hack campaign from Iran

Enlarge / Rampant Kitty has been targeting Telegram like a feline to twine.
Check Point

reader comments

26 with 22 posters participating, including story author

Share this story

Researchers said they have uncovered an ongoing surveillance campaign that for years has been stealing a wide range of data on Windows and Android devices used by Iranian expatriates and dissidents.

The campaign, which security firm Check Point has named Rampant Kitten, comprises two main components, one for Windows and the other for Android. Rampant Kitten's objective is to steal Telegram messages, passwords, and two-factor authentication codes sent by SMS and then also take screenshots and record sounds within earshot of an infected phone, the researchers said in a post published on Friday.

The Windows infostealer is installed through a Microsoft Office document with a title that roughly translates to "The Regime Fears the Spread of the Revolutionary Cannons.docx." Once opened, it urges readers to enable macros. If a user

complies, a malicious macro downloads and installs the malware. The Android infostealer is installed through an app that masquerades as a service to help Persian-language speakers in Sweden get their driver's license.

"According to the evidence we gathered, the threat actors, who appear to be operating from Iran, take advantage of multiple attack vectors to spy on their victims, attacking victims' personal computers and mobile devices," Check Point researchers wrote in a longer report also published on Friday. "Since most of the targets we identified are Iranians, it appears that similarly to other attacks attributed to the Islamic Republic, this might be yet another case in which Iranian threat actors are collecting intelligence on potential opponents to the regiment."

The Windows infostealer takes a particular interest in Telegram. Fake Telegram service accounts push phishing pages that purport to be official Telegram login sites. The malware also seeks out messages stored in Telegram for Windows when it's installed on infected computers. To survive reboots, Check Point said, the infostealer hijacks the Telegram for Windows update process by replacing the official Updater.exe file with a malicious one. (I attempted to ask Telegram officials if the service uses code signing to prevent such tampering but didn't succeed in reaching anyone.)

Passwords, messages, and conversations are all ours

Check Point said other features of the Windows malware included:

- Uploads relevant Telegram files from victim's computer. These files allow the attackers to make full usage of the victim's Telegram account
- Steals information from KeePass password manager

application
- Uploads any file it can find which ends with pre-defined extensions
- Logs clipboard data and takes desktop screenshots

As noted earlier, the Android backdoor targets SMS-sent one-time passwords and records nearby conversations. Check Point said evidence from passive DNS records—which log other domains that have used the same IP address used in Rampant Kitten—suggested that the attackers have been active since at least 2014.

A separate report published by the Miaan Group, a human rights organization that focuses on digital security in the Middle East, echoed the research and added details, including the exfiltration of the malware of data from the WhatsApp messenger.

"Since early 2018, Miaan researchers have been tracking malware used in a series of cyberattacks on Iranian dissidents and activists," organization researchers wrote. "The research has uncovered hundreds of victims of malware and phishing attacks that stole data, passwords, personal information, and more." It wasn't clear if that malware included the infostealers detailed by Check Point.

Readers should remember that the ability to extract Telegram, KeePass, or WhatsApp data from an infected computer isn't automatically an indication of especially sophisticated malware or a flaw in the targeted applications. To be useful, all three applications have to decrypt contents when a user needs it. That moment presents an opportunity for malware already installed to obtain the information. People should remember there are rarely good reasons to enable macros in Office documents and that messages to allow them is a red flag.

Both reports provide extensive indicators of compromise that

people can use to determine if they’ve been targeted.

https://arstechnica.com/?p=1707906

$100,000 in bribes helped fraudulent Amazon sellers earn $100 million, DOJ says

Enlarge / Amazon boxes.

reader comments

62 with 51 posters participating

Share this story

Six people were indicted on allegations of paying over $100,000 in bribes to Amazon employees and contractors as part of a scheme to give third-party sellers unfair advantages on the Amazon marketplace. Among other things, the indictment says that Amazon workers who accepted bribes reinstated sellers whose accounts had been suspended for offering dangerous products, and these workers suspended the seller accounts of fraudulent sellers’ competitors.

The US Department of Justice today announced the indictment handed down by a grand jury in the Western District of Washington. The “defendants paid bribes to at least ten different Amazon employees and contractors,” the DOJ said. In one case, a 31-year-old defendant named Nishad Kunju “accepted

bribes as a seller-support associate in Hyderabad, India, before becoming an outside consultant who recruited and paid bribes to his former colleagues," the DOJ said.

In exchange for bribes, Amazon workers "baselessly and fraudulently conferred tens of millions of dollars of competitive benefits upon hundreds of [third-party] seller accounts that the Defendants purported to represent," the indictment said. The DOJ said that workers "helped reinstate products and merchant accounts that Amazon had suspended or blocked entirely from doing business on the Amazon Marketplace" and that "the fraudulently reinstated products included dietary supplements that had been suspended because of customer-safety complaints, household electronics that had been flagged as flammable, consumer goods that had been flagged for intellectual-property violations, and other goods." These fraudulently reinstated seller accounts included ones Amazon had "suspended for manipulating product reviews to deceive consumers, making improper contact with consumers, and other violations of Amazon's seller policies and codes of conduct," the DOJ said.

The previously suspended merchants made over $100 million from Amazon sales after their "baseless and fraudulent reinstatement," the indictment said. The scheme started no later than July 2017 and continued until September 2020, the indictment said.

Besides Kunju, the indicted people were Ephraim Rosenberg, 45, of Brooklyn, New York; Joseph Nilsen, 31, and Kristen Leccese, 32, of New York City; Hadis Nuhanovic, 30, of Acworth, Georgia; and Rohit Kadimisetty, 27, of Northridge, California. The defendants who bribed Amazon workers acted as consultants to third-party sellers, the DOJ said. Three of the defendants—Nilsen, Leccese, and Nuhanovic—also allegedly "made their own sales on the Amazon Marketplace through [third-party] accounts they operated."

Attacks on competitors alleged

To give sellers further advantage over rivals, the bribed employees and contractors "facilitated attacks against competitors' [third-party] accounts and product listings, by (a) sharing competitive intelligence about competitors' revenues, customers, advertising campaigns, and suppliers; (b) using their inside access to Amazon's network to suspend competitors' [third-party] accounts; and (c) providing consultants with information about Amazon's internal algorithms, which allowed the consultants to flood competitors' product listings with fictitious negative product reviews," the DOJ said.

The bribes also helped third-party sellers and consultants gain "unauthorized access to Amazon's highly confidential standard operating procedures and algorithms," providing "coveted insight into the systems that power Amazon's search engine, Amazon's product reviews, and Amazon's enforcement processes," the DOJ said.

Bribed workers provided contact information for Amazon employees and consumers, "which the members of the conspiracy misused and shared widely," the DOJ said. Bribed workers also circumvented Amazon rules when they "increased [third-party] sellers' storage limits in Amazon's warehouses, facilitated [third-party] sellers' otherwise meritless requests to sell products in restricted categories, and provided [third-party] sellers with inside knowledge about the most successful advertising campaigns and most profitable product listings," the DOJ said.

The six defendants were charged with conspiracy to use a communication facility to commit commercial bribery, conspiracy to access a protected computer without authorization, conspiracy to commit wire fraud, and wire fraud. The wire-fraud charges alone "are punishable by up to

20 years in prison and a $250,000 fine," while the other charges are "punishable by up to five years in prison and a $250,000 fine," the DOJ said.

Amazon said it has fired the workers who accepted bribes and that it assisted federal investigators in the case. "Amazon has systems in place to detect suspicious behavior by sellers or employees, and teams in place to investigate and stop prohibited activity," the company said when contacted by Ars today. "We are especially disappointed by the actions of this limited group of now-former employees, and appreciate the collaboration and support from law enforcement to bring them and the bad actors they were entwined with to justice. There is no place for fraud at Amazon and we will continue to pursue all measures to protect our store and hold bad actors accountable."

https://arstechnica.com/?p=1707893

Comcast shut off Internet to hundreds, saying they were illegally connected

reader comments

232 with 109 posters participating

Share this story

Comcast says that a broadband reseller illegally sold Comcast Internet service in residential buildings in the Denver area and has terminated the connections to those buildings.

As reported by Denver7 this week, the shutoff affected hundreds of people who live in buildings serviced by AlphaWiFi, "which installs and services Internet in approximately 90 apartment buildings across Denver." The shutoff came as a surprise to residents, including Kaley Warren, who has been working at home during the pandemic.

"It is my entire lifeline," said Warren, who said that without warning last Friday, her Internet service disappeared. "I felt lost. It was truly the first time during the pandemic that I… had the feeling of 'What am I supposed to do?'"

When contacted by Ars, a Comcast spokesperson said that "AlphaWiFi is under a standard commercial agreement which expressly prohibits the resale of Comcast services." Comcast did not answer questions about how many people were affected and when they will get service restored, but it did provide us with the same statement it previously gave to Denver7, which says:

> *Comcast learned that AlphaWiFi has been improperly reselling Comcast's Internet services to individual residential customers throughout the Denver area. We take the unauthorized resale of our services very seriously as it violates our contracts and the law, and can negatively affect services provided to customers across our network. We notified AlphaWiFi well in advance that its service would be terminated and asked that they notify impacted users of the need to transition their services. We also provided multiple advance notices to the residents we believed would be affected and have been working to transition those who are interested to our residential services. We're committed to*

> *delivering the best experience and remain available to assist those impacted.*

AlphaWiFi blames Comcast

AlphaWiFi President Keith Lawton told Denver7 that "we absolutely dispute Comcast's take on this matter. Comcast knew our business plan, and we made it clear to Comcast that despite our disagreement, we wanted to work with them in order to transition these accounts with no disruption. Unfortunately for these customers, Comcast opted to cancel their service instead of working with us and unnecessarily impacted these consumers. AlphaWiFi continues to work diligently to support our customers and get their Internet access reinstated."

The statement doesn't explain AlphaWiFi's theory on why it can resell Comcast service. We contacted AlphaWiFi yesterday, asking for details on the resale question, for details on how many buildings and residents lost service, and for an update on when people will be reconnected. We'll update this article if we get a response.

Like hundreds of other ISPs, Comcast signed a Federal Communications Commission pledge to keep Internet users connected during the pandemic. But the pledge expired at the end of June, and it covered individual users who were unable to pay bills rather than cases of illegal resales, so it may not have applied to the Denver situation anyway.

The shutoff apparently also caught a building management company by surprise. RIO Properties, which manages dozens of buildings, including the one where Warren lives, told residents in an email, "We apologize and did not know in advance this was going to happen," according to Denver7. We contacted RIO yesterday and will update this article if we get a response.

Heidi Chapman, who also lost service, called the shutoff during a pandemic “heartless,” saying people could lose their jobs when they don’t have Internet access. “[S]he knew nothing about the impending Internet shutdown until she lost Internet service, and it could be up to a month before a deal with another Internet provider,” Denver7 wrote. “She was left scrambling to add a hotspot to her phone.”

https://arstechnica.com/?p=1707732