F-Alert

Monthly threat updates from

F-Secure

August 2023

F-Secure

Discover the latest threat updates. Packed with insights from the experts at F-Secure. Delivered every month.

Discover an “uncensored” app that reveals the risks of malicious AI. See how Google is fighting stalking via Apple AirTags. Find out how Apple has sped up the delivery of security updates. And see how criminals can install malware on your Android device through your browser. All this and more in this month’s F-Alert.

WormGPT reveals AI risks

The power of a new AI chatbot that promises help with cyber crime seems to have scared even the creator of the service.

WormGPT declared itself an ”uncensored” version of ChatGPT when it appeared on a cyber crime marketplace earlier this summer, selling for 100 to 5000 Euros. Now the programmer behind the bot has admitted to adding some guardrails that prevent some malicious use.

Of course

A malicious AI chatbot was inevitable, according to Laura Kankaala, F-Secure Theat Intelligence Lead.

“Criminals take advantage of any technology that gives them anything that makes their crimes easier,” she said. “So, of course, they would take advantage of the most powerful new technologies ever.”

This bot appears to be powered by a large language model released in 2021, but not one of the far more powerful models that are behind ChatGPT and Google Bard. Yet, at launch it delivered “human-like” text that aids with the creation of advanced scams and computer code for powerful malware.

“The attacks WormGPT enables look just like ones we've been defending against for years, or even decades,” Kankaala said. “But there’s no doubt that the barriers to entry to cyber crime will keep getting lower, thanks to AI.”

Prohibiting “some subjects”

Legendary cyber security reporter Brian Krebs tracked down the creator of the malicious bot in August and found that the service has begun moderating some of its answers, just like ChatGPT and Bard.

“We have prohibited some subjects on WormGPT itself,” Rafael Morais told Krebs. “Anything related to murders, drug traffic, kidnapping, child porn, ransomwares, financial crime.”

He also bragged that the service is now “5 or 6 times better in terms of learning and answer accuracy.”

Kankaala noted that completely blocking the use of an AI bot for scams is almost impossible, whether the bot is designed to be malicious or not.

“Anything that produces articulate, grammatical text on-demand will be used by criminals in a wide variety of ways,” she added. “There are also active attempts to bypass the guardrails of legitimate AI by ‘jailbreaking’ the prompts in a way that produces otherwise prohibited text."

Laura Kankaala
Threat Intelligence Lead
Helsinki, Finland

expert tip

Criminals shamelessly employ tactics of manipulation and treachery. Listen to your intuition and remember that you can always back away from seemingly a great deal, or even a suspicious love interest.

“There’s no doubt that the barriers to entry to cyber crime will keep getting lower, thanks to AI.”

AirTag alerts coming to Android

Google rolls out "Unknown Tracker Alerts" for AirTags while working on industry-wide tracking protections with Apple.

Joel Latto
F-Secure Threat Advisor
Helsinki, Finland

expert tip

You don't have to wait to be alerted if you're worried you're being tracked. Google now offers a manual scan for unknown trackers in 'Settings' under 'Safety & Emergency'.

"Google and Apple will lead an initiative to create an industry-wide spec to address unwanted tracking"

Android updates this summer include a new feature that will let users know if there's an AirTag nearby that may be tracking them.

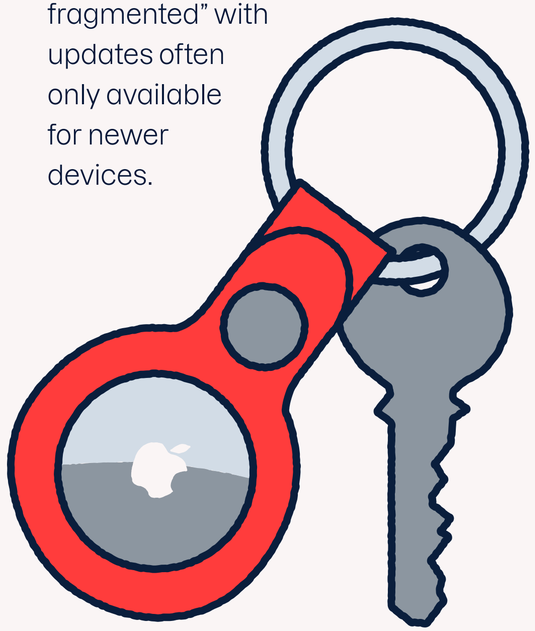
Just AirTags, for now

Joel Latto, F-Secure Threat Advisor, noted that the new notifications work with AirTag tracking devices, but not other popular trackers that utilize Bluetooth, including Chipolo, SmartTag, or Tile. At least, not yet.

"However, perhaps the bigger and more positive news here is that Google and Apple will lead an initiative together to create an industry-wide specification to address unwanted tracking," he said.

WIRED has called AirTags a "gift to stalkers", and concerns about the possible misuse of these devices led to a class-action lawsuit in the US.

Latto added that Google's decision to roll out this feature to all Android versions from 6.0 to 13 is "surprising but good," as it shows how seriously the company is taking stalking. The Android landscape can be "very fragmented" with updates often only available for newer devices.



For loss, not theft

AirTags have been used in a wide variety of ways since they were first announced in 2021. They've been used to track everything from dogs to drug trafficking suspects.

But Latto conceded that these alerts could be exploited by criminals.

"If, let's say, a car gets stolen with an AirTag in it, it's possible that the thief now gets an alert to their phone about the tracker, and then proceeds to dig for it and dispose of it," he said.

However, there are other ways to prevent theft. And these alerts seem to be the best way to prevent device-enabled stalking.

Trending Scam

Instagram
Sugar Daddies and Mommies

WHAT:
Using stolen images and, occasionally, stolen accounts, sugar daddies and mommies approach potential victims via direct messages on Instagram, dating apps, or any social media platform. These big talkers start lengthy conversations, promising a life of luxury. But what they want, obviously, is your money.

HOW:
These scams develop in two ways. Either the daddy or mommy will quickly ask for money. Or the scammer will offer some sort of payment to gain the victim's trust. That transaction will be quickly canceled, or the sugar parent will just ask for the money back.

PREPARE:
Any unexpected request for information related to money or services that enable monetary transactions, including PayPal, Venmo or MobilePay, should make your internal alarm bells blare. To verify if you're dealing with an actual person, try a video chat. Also, use Google to assess a stranger's legitimacy.

Breach that matters

University of Missouri System

WHY IT MATTERS:
Over 100,000 individuals involved with Missouri's public university system had their private data published on the site of the ransomware gang cl0p. That makes the system one of hundreds of organizations impacted by a vulnerability in MOVEit, a software used for secure file transfers.

BREACHED DATA:
The personal information shared seems to include details of student records including names, addresses, email addresses, birthdates, phone numbers, student IDs, and social security numbers.

WHAT SHOULD YOU DO:
Victims in any organization affected by the MOVEit vulnerability should expect to face targeted phishing attacks utilizing the leaked data, including attacks that pretend to be from the University system itself. There's also a possibility that criminals could use this data to apply for loans or new credit. Consider putting a freeze on your credit report to prevent any new accounts being opened in your name.

Is your data being exposed online?
Check with our **F-Secure Identity Theft Checker!**

Infostealers in the wild

Shedding light on a growing cyber security issue – the rise of the infostealer

An infostealer is malware designed to steal important information from your browsers and more. Here, we've ranked infostealers by most stolen records discovered through the 1st of June until the 21st of August :

Raccoon	12,610,436	**Unidentified Cronos**	48,807
Redline	7,365,889	**Titan**	17,417
LummaC2	4,345,819	**Rhadamanthys**	10123
Vidar	4,267,622	**Atlantida**	7,721
stealc	3,163,366	**Darth**	6252
MetaStealer	2,994,085	**Taurus**	549
Russian	1,523,166	**Vikro**	121
Aurora	474,393	**Ebrium**	5
Dark Crystal	66,475	**Predator**	2

A closer look at

Why it matters:

Public and private data of 2.6 million users of the language acquisition site Duolingo appeared on a hacking forum in mid-August. The same data, which seems to have been gathered from user profiles using the site's exposed application programming interface (API), first appeared on an illicit forum early in 2023.

Breched data:

The personal information leaked includes emails, users' real names, and phone numbers along with a wide variety of details from the users' profile and interactions on the site.

What you should do:

Affected users should expect targeted phishing attacks, including ones that pretend to be from Duolingo itself. Avoid clicking any links or attachments in any unexpected messages and contact the site, or any financial institution you deal with, directly rather than through unsolicited emails or SMS messages.

Apple’s agile security updates

New update system deals with hiccups as tech giants get behind the movement to offer smaller, faster fixes.

Apple is delivering on the promise to offer “a new type of software release for iPhone, iPad, and Mac” that fixes vulnerabilities actively exploited by criminals. But a recent update showed how challenging it can be to balance timely fixes with the need to test new software releases.

Like any new technology

Traditionally, users have to wait for major system updates to fix security holes. Rapid Security Response, which was announced by Apple in December of 2022 and rolled out in May of this year, offers a fresh approach.

“This system is designed to swiftly deliver crucial security improvements between major software updates, keeping your devices safeguarded against emerging threats,” said Ash Shatrieh, F-Secure Threat Intelligence Researcher. “However, like any technology, there can be occasional hiccups.”

A Rapid Security Response released in July had an unintended consequence on some websites, causing display issues. “Apple promptly acknowledged the problem and provided a solution by introducing updated versions or the possibility to rollback/remove the update,” he said.

It’s that “agility” that makes the system so promising, even if it requires speeding up the testing process, Shatrieh noted.

Recognition across the industry

Rapid Security Response targets key components like the Safari web browser, the WebKit framework stack, and critical system libraries, which Shatrieh says are crucial for maintaining a secure online experience.

“Apple’s efforts show that the importance of quick security updates is gaining recognition across the tech industry,” he said. “Google recently announced a similar approach with their Google Chrome app, delivering security updates once a week to tackle security issues promptly,”

Meanwhile, Microsoft is sticking with “Patch Tuesdays” which offer software fixes once a month.

At least for now.

Ash Shatrieh
Threat Intelligence Researcher
Helsinki, Finland

expert tip

Rapid Security Response is available on all Apple devices that use iOS 16.2, iPadOS 16.2, and macOS 13.2 or later. Check your settings under General > Software Update to make sure it’s enabled.

“The importance of quick security updates is gaining recognition across the tech industry.”

Amit Tambe
Researcher
Helsinki, Finland

expert tip

Ignore notifications about app updates that come from SMS messages. Instead, rely on the app itself for update information.

“Just as developers can install APKs directly on user’s phones, so can attackers.”

WebAPK enables fake app install

New attack exploits a shortcut that allows users to skip the Play Store to put apps on home screens.

Android’s WebAPK offers convenient access to new apps. Now, criminals are taking advantage of the very same convenience to push fake banking apps that steal valuable credentials.

The only step

Installing an Android app generally involves the Google Play Store or directly installing an APK (Android Package Kit) a user finds in some other, less safe destination.

“WebAPK allows APKs to be generated and installed automatically from the web browser, without the need of Google Play Store,” said Amit Tambe, a researcher at F-Secure. “Just as developers can install APKs directly on user’s phones, so can attackers.”

A recent attack discovered by the Polish Financial Supervision Authority’s Computer Security Incident Response Team involved a phishing attack delivered via SMS. The message urged the victim to install an update for a banking app.

“The only step that the threat actor needs to take is to somehow convince the user to click on a malicious link to make this attack a reality,” Tambe said.

Especially concerning

The researchers note that this attack is especially effective because it doesn’t trigger any alerts on the victim’s device.

Tambe added that once executed, this attack invites users to offer their banking credentials. This is only possible due to a technology called Progressive Web App, which produces the WebAPK that installs the app.

He wonders if these apps are too progressive for their own good.

“An innocuous URL could be replaced with a malicious URL that leads to installation of malware by completely bypassing the checks of Google Play Store.”

As the user interacts with the app, believing everything is fine, the stolen data is sent directly to the attacker’s server.

About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 180 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit f-secure.com today!

F-Secure