

Mar 15, 2026

Meta Hires the Duo Behind MoltBook

Why did they hire them? Probably because they want all of your money and all of your data. If they can see what your agents are doing, they can develop tools to get a bigger piece of your wallet. Kind of business as usual. No surprise. If you assume that you are using someone's API and they are NOT going to see what you are doing, you are fooling yourself and you need to implement it with that in mind. If that is a concern, please contact us. Credit: [Tech Crunch](#)

Please check out our blog at <https://www.cybercecurity.com/cyblog>

You can also find copies of the weekly newsletter at <https://cybercecurity-mitch-tanenbaum-blog.com/SNU>

We have a YouTube Channel with a lot of videos. Check it out at: [Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube](#)

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCecurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at <https://cybercecurity.us>. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

Security/Privacy Alerts

Senate Confirms Gen. Rudd to Head NSA and Cyber Command

The vote was 71-29 and it promotes him to a four star general. Rudd has no experience in either signals intelligence or cyber, but, apparently, the folks in Congress who also, for the most part, have no experience in those subjects either, thought it unimportant to have someone with domain expertise to head up those organizations. He is probably a very dedicated guy, but having no expertise in this very technical field is not a good thing. Credit: [Reuters](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#).

Anthropic Sues Pentagon Over Supply Chain Risk Label

I don't think this is much of a surprise, but they did file suit on Monday. Anthropic said in the lawsuit that blacklisting them was unlawful and violated its free speech and due process. Unless the Pentagon settles, this will play out in court. Anthropic is asking for an injunction while this plays out. Stay tuned. Credit: [Reuters](#)

Meta Hires the Duo Behind MoltBook

Why did they hire them? Probably because they want all of your money and all of your data. If they can see what your agents are doing, they can develop tools to get a bigger piece of your wallet. Kind of business as usual. No surprise. If you assume that you are using someone's API and they are NOT going to see what you are doing, you are fooling yourself and you need to implement it with that in mind. If that is a concern, please contact us. Credit: [Tech Crunch](#)

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

Q: If a client sends us CUI to our commercial environment and it gets synchronized with the Microsoft (or Google) cloud, what do we do?

A: The bad news is that you have a problem. First, this is reportable. Then you have to tell the feds that you may not be able to clean it up. That could put you at risk. If it gets reported in time, you can stop the synchronization, delete the spill and restart synchronization. Otherwise, you are going to have to work with your vendor to deal with it. The moral is, work with your customers and partners not to do this.

Reference

Nothing to report

Software and Hardware to Check Out

Google Releases Command Line Interface to Aid AI Agent Development

AI agents need a simple, deterministic interface to be able to interact with systems. There has been a third party command line interface (CLI) that some agent developers have used but since it didn't come from Google it wasn't always in sync. Now Google has released a command line interface that allows agents to interact with Google Drive, Gmail, Calendar, Docs, Chat and even Admin. If you are a Google Workspace company and interested in AI, this is good news for you. Unfortunately, Google is not "officially" supporting it. I hope this changes, but until then, you have to rely on the community for support. Still this is an important step forward. Credit: [Venture Beat](#)

Important Issues/Patches

Nothing to report

Legislative and Legal Activities

Meta Claims that Piracy is Legal - As Long as it is Used to Train Their AI

It is a bold argument; one that will ultimately make it to the Supremes. Basically, they are saying that since an AI LLM is a transformative use of the millions of copyrighted books they stole,

stealing them is not illegal. This is definitely one to watch because if they win, Copyright law is basically nuked out of existence and no creative work is protected. Credit: [My Privacy Blog](#)

Hackers “Department of Peace” Hack DHS Vendor Database and Makes it Public

The hacker’s name is obviously a play on the DoD’s unofficial name Department of War (only Congress can change the name of a government agency). They have released information on over 6,000 organizations that have either sold or tried to sell stuff to DHS, including employee names, business and personal addresses, phone numbers and emails, EINs and or SSNs, CAGE codes and internal DHS comments on the contractor. An example of what they are selling DHS is a microwave vehicle stopper (if it fries the vehicle’s electronics, will it also fry the occupants?). Credit: [My Privacy Blog](#)

Education

Government Uses Targeted Advertising to Track Your Location

For some people they don’t care. For others, it is a matter of principle. For still others, it is a matter of personal safety. If you are in one of the latter two categories, this article is important reading. If you are in the first category, just move on. And, Customs is finally admitting what we all suspected. They are buying commercial data to track you, with no controls on how long they keep it or what they do with it. Learn more at the link. Credit: [EFF](#)

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.

HungerRush Point of Sale Software for Restaurants Hacked

HungerRush is a cloud based restaurant management system for pizza restaurants and fast-casual brands. Hackers are claiming that they have 28 million records of both customers and restaurants themselves. The company says they are investigating. Credit: [Daily Dark Web](#)

Handala Attack Hits Israeli Weather Stations and Cameras

While Trump’s war is definitely kinetic, it is also cyber. The Handala group claims to have successfully breached and disrupted Jerusalem’s security camera network and Israel’s government and military weather network. Credit: [DailyDarkWeb](#)

MedTech Giant Stryker Hit by Iran-Linked Hacker Attack

Stryker is a Fortune 500 company that manufactures medical devices like surgical equipment, orthopedia implants and other products. With revenue of around \$25 billion and with 56,000 employees, they definitely are “critical infrastructure” to hospitals and doctors. Iran-linked hacker group, Handala, claimed to have wiped more than 200,000 servers, mobile devices and other systems. They also claim to have stolen 50 terabytes of data. The company told employees not to turn on their devices and disconnect from all networks immediately. The company said they are having a “global network disruption” and “we have no indication of ransomware or malware” and they think they have contained the incident. Reports are coming out of employees seeing the Handala logo on their screens. Iran may be flipping the script on Washington, choosing a cyber war, which can be fought from anywhere on the planet, including from inside the United States, vs. a kinetic war, in which they are vastly overpowered by the United States. By going after private companies which may or may not have great cybersecurity

practices, they are putting the Department of Defense on the defensive. Protecting 50 million independent networks is a lot harder for the DoD than fighting one war on Washington's terms. And, for Stryker and its customers, recovering 200,000 devices from a factory reset (which may or may not remove all malware), is not a simple task. Only time will tell what the truth is. Credit: [Security Week](#)

Hebrew University of Jerusalem Suffers Destructive Data Breach

The hackers, who claim to be Handala, attacked HUJI, what they call "one of the scientific and research symbols of the Zionist regime". You can guess where they are from. They claim that all servers of the university were destructively wiped and in addition they wiped 48 terabytes of vital and infrastructural data. Hopefully this can be recovered from backups. But they also claim to have stolen an additional 23 terabytes of educational, research, administrative, financial and communications data including personal and confidential information of thousands of students and faculty, all emails, official documents and other files. "You bomb, we hack" they said. Credit: [Daily Dark Web](#)

AI Assistants - The Good and Not so Good

So you want your AI assistant to order you some housewares online - that is good (unless of course you want to order it from Amazon; they have convinced a judge to give them a restraining order to stop your AI from doing that). If your AI has access to your email (it probably would) and it decides to delete all of your email - that is, maybe, not so good. Ultimately, it is up to you to manage the risk. Learn more [here](#).

AI Hacked AI Agent - Easily

Following on the AI theme here, Security must be front and center when it comes to AI agents. One AI was used recently to hack another AI. It masqueraded as Donald John Trump. Learn more [here](#).

1 BILLION Identity Records Exposed - Who is Responsible?

Banks and others are legally required to confirm your identity. While conceptually this may be good, it does expose an attack surface. In this case, it exposed a billion identity records, which is, to be polite, not good. Worse yet, the vendor in question says they don't own the data involved. Learn more [here](#).

Security News for the week ending March 13, 2026

This week's news: RI lawmakers consider making private encryption keys private, Microsoft takes Anthropic's side in fight with DoD, Iran says US tech companies are legitimate targets, Instagram to discontinue end to end encrypted messages; TrikTok too and DOGE engineer stole hundreds of millions of taxpayers' data. Details [here](#).

Are you thinking about implementing AI in your company but are not sure about the security and privacy implications? The time to address this is before you start implementing AI. Contact us for assistance.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663

