

September 20, 2026

Threat Groups (AKA Hackers) are Using AI Better than Defenders

Criminals and state hackers are using automation and agentic AI much better than defenders are. In many cases this allows them to bypass traditional defenses. Hackers are using AI to triage targets, launch brute force attacks and even figure out how to move laterally once they are inside. Can you say the same with regard to your defenses? Are you coming to a fork fight with a spoon? That might not work out so well in the long run. Credit: [Cybersecurity Dive](#)

Please check out our blog at [HTTPS://TCPS-BLOG.COM](https://TCPS-BLOG.COM)

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

Hackers Stole a Flock Camera; Decrypted the Software and Thousands of Images

Hackers say that physical security comes first. Without it, you don't have much security at all. One group stole a Flock camera and, instead of destroying it, extracted the software, found an on-device encryption key and with it were able to decrypt at least some of the software and thousands of images. They shared what they found with Wired and 404 Media, who each wrote stories about it. Since privacy is a key issue here, Wired found that records from Alpharetta, Georgia's Flock cameras were accessible to more than 2,000 agencies, including police, colleges, airports and the Office of the Inspector General for the General Services Administration. Credit: [404 Media](#) and [Wired](#).

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#). If you are a government employee, check out our AI Governance for Govies at the same site.

Want to stay on top of the news about AI - Check out our news feed on the AIGIP web site at <https://aigip.ai/news/latest-ai-news>

Microsoft Releases Draft AI Code of Conduct for Public Comment

As AI evolves - rapidly - companies need to figure out how to use AI and what is off limits. While companies like Anthropic are asking for government intervention (as a cover for why they are not doing things), Microsoft has released its own code of conduct that it plans to use to guide how it trains its own models. No reason why you can't use it too. You can find the draft [here](#) and it is open for comment. Credit: [Redmond Magazine](#)

Nvidia, Palantir, Others Demand AI Providers Prove Data Protection

This should not surprise you. Big players who have clout are demanding that companies like OpenAI and Anthropic prove they are protecting their intellectual property. While you can often get a claim that they don't use your data to train their models, that does not mean that they are not collecting and reviewing your data and metadata. Zero data retention and air-gapped servers are part of it. If you are a small player you don't have that clout, but there are things that you can do. Credit: [Tom's Hardware](#)

OpenAI has Hundreds Of Humans Reading Transcripts of your Chats

They say it is to improve the responses from their LLM and we all know that some of the responses could use improvement, but if you thought that your conversation about whatever - diseases, love life, mental health, CORPORATE INTELLECTUAL PROPERTY - was between you and a computer, apparently you are wrong. Credit: [Tom's Hardware](#)

Litigation Management in the Age of AI

AI and the law sometimes collide. If you get into a situation where you may have to deal with a lawsuit and you use AI in your business, are you prepared? Check out this [blog post](#) on the subject.

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.*

Did You Mark Something as N/A? That Might Not be The Best Idea

Here is the problem with that. If you mark it as N/A and later need to do something that MAY be considered a "significant change" under the DoD's guidance and trigger the requirement for a reassessment. For example, if you say removable storage is N/A and then the CEO needs to use a flash drive, that may be enough to trigger the reassessment requirement. On the other hand, if you, in your policies, procedures and SSP say "we don't do this right now, but if we did, here is the process we would follow", then that is just a change consistent with your documentation. The issue with N/A is that it was not assessed during your assessment.

BAE Settles With the Feds for \$38 Million

The BAE settlement was for violating ITAR laws. ITAR and CUI are different, but very similar. Not all CUI is ITAR and not all ITAR is CUI, but there is a lot of overlap. Violate CUI rules and you get fined. Violate ITAR rules and you can go to prison. Learn more on our FCA page at <https://www.tcps-blog.com/fca>

**** REMINDER** NEW SPRS/PIEE System Access Requirements**

This is not a change to CMMC, but PIEE is now requiring that you log in at least every 34 days to keep your account active, so make sure you put this on your recurring task list.

Reference

Threat Groups (AKA Hackers) are Using AI Better than Defenders

Criminals and state hackers are using automation and agentic AI much better than defenders are. In many cases this allows them to bypass traditional defenses. Hackers are using AI to triage targets, launch brute force attacks and even figure out how to move laterally once they are inside. Can you say the same with regard to your defenses? Are you coming to a fork fight with a spoon? That might not work out so well in the long run. Credit: [Cybersecurity Dive](#)

Software and Hardware to Check Out

China Moves its Next AI Chip Forward as White House Can Only Watch

Huawei is moving its Ascend 960DT AI chip to early 2027 as US chip sanctions block buying US chips. This is 9 months earlier than previously announced. They also plan to release their Ascend 960PR in third quarter 2027. Performance, they say, will be double from the previous generation. They are also working on beating Nvidia by making thousands of less capable chips work together in unison. A supernode will cluster up to 4,096 processors and a supercluster able to connect up to a million AI processors. You don't need the fastest chips if you can do this. Credit: [Tech Republic](#)

Important Issues/Patches

Microsoft Releases EMERGENCY Patches to Fix RDS Failures Caused by This Month's Updates

Given they patched close to a thousand bugs, some failures are to be expected. The patch to the patches fix RDS failures and Hyper-V and USB audio problems on some Windows versions. There are multiple other collateral damage fixes as well. Credit: [Bleeping Computer](#)

Apparently Apple Has Heard of AI, Too - Patches More Than 260 Bugs

Apple released the single largest bug fest in its history, patching more than 260 CVEs. While this is a lot less than Microsoft (974+), they also sell way fewer products. None of the bugs were reported to be under active exploitation - possibly until the announcement. Credit: [The Register](#)

Legislative and Legal Activities

Senator Asks Rubio and Blanche to Oppose Canadian Surveillance Legislation

Canada is working on a bill that would require cloud providers in other countries (like the US) to provide the Canadian government with data on users, including Americans. While the American government spies on people (all governments do), this bill is a bit too far. Would a company like Apple leave Canada? Probably not, but they could do what they did in England and, for example, disable encryption instead of providing a back door and then claiming the government won't let us provide you with secure apps. Stay tuned; I hope this will either be significantly modified in the Upper Chamber or die a death on the floor of Parliament. Credit: [The Record](#)

Education

Why Musk is Fighting Multiple Lawsuits on Being Accountable

A college girl has gone public about the challenges she has faced after she was videoed at a college frat party and the videos of her nudified and having sex went viral on an underground network of men who seem to get their thrills from ruining the lives of unsuspecting victims. Her parents have spent tens of thousands of dollars to help her recover and get those responsible charged. It was a long battle and it is still not over. Most of the online part happened on Twitter and if Musk were to be liable for every time this happens, he would not be rich any more. The article discusses the challenges in getting the school, the feds and local police to do anything about it. In her case her parents had the resources to force the issue, but most of the time that is not the case. Credit: [Wired](#) (note: you may need to be a subscriber to access this article)

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.**

Nutex Health Breached by Shiny Hunters

They were hacked by *The Gentlemen* and have not disclosed the details. Apparently the hackers posted the data for download and Nutex is trying to figure out the scale of the damage. Given what everyone is saying, this is likely to be a big one. The company admits that “several proposed class action complaints were filed against the company”. Credit: [The HIPAA Journal](#)

Regulation of AI - yes or no?

AI CEOs issued a call to ‘slow the pace’ of AI. This is a worldwide concern. Every country is doing it differently, but many of them are ‘concerned’. Beijing says it is just fearmongering. Sure, I will go with that. Not. The president is not a big fan of AI regulation. He said that all that is required is his high IQ. But Congress is less convinced. It is not clear what is going to happen. Learn more [here](#).

Even critical infrastructure is on its own for defending against cyber threats

CISA fired a third of its staff and more left on their own. Now CISA is trying to hire new people. The president came up with a half baked strategy to assist critical infrastructure that he is testing in Texas, but it will only last 6 months. This is a huge problem with no inexpensive solution. Learn more [here](#).

Litigation readiness in the era of AI

Dealing with litigation is never fun. From an IT standpoint, up until now, at least we have had a handle on how to do it. With AI in the mix, that all goes out the window. Learn more [here](#).

Security News for the week ending September 18, 2026

This week’s news: AT&T store worker gets 16 months for side hustle, cops say Flock camera search reason is ‘LMAO’, Texas data centers have been giving the gov the middle finger and another cop caught abusing Flock camera data and well, more than one. Details [here](#).

AI is making the world of patch management “interesting”. With Microsoft releasing a thousand patches a month, Apple releasing hundreds of patches, everyone else in between and the time

to exploit decreasing rapidly, your old patch strategy is not going to work any more - ever again.
Need help? Contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663