POLITICOPRO
Morning Cybersecurity

BY JOHN SAKELLARIADIS

With help from Maggie Miller and Dana Nickel

DRIVING THE DAY

— The White House's latest effort to unearth evidence that the Obama administration lied about Russian meddling in the 2016 election is revealing in ways they likely didn't intend.

HAPPY TUESDAY, and welcome to MORNING CYBERSECURITY! Thank you to John for handling today's MC top for me while I head to Las Vegas. Any matcha recs near the convention center? (I know there's a shortage, but when in Rome.) Drop me a line at dnickel@politico.com.

Follow POLITICO's cybersecurity team on X at @RosiePerper, @johnnysaks130, @delizanickel and @magmill95, or reach out via email or text for tips. You can also follow @POLITICOPro on X.

AT THE WHITE HOUSE

ACTIVE MEASURES — Newly released files from the Trump administration don't prove Russian meddling in the 2016 election was a treasonous Democratic conspiracy, as the Trump administration has alleged — rather, they seem to expose fresh holes in that argument.

— What's new: Documents declassified last week from Special Counsel John Durham's 2023 probe into the FBI investigation of the Trump campaign in 2016 detail Durham's failure to fully corroborate explosive Russian intelligence memoranda U.S. spy agencies obtained between January and July of that year.

between January and July of that year.

After his roughly four-year-long investigation, Durham was also unable to prove the veracity of several English-language emails appended to those memos, which were purportedly stolen from a slew of left-leaning think tanks and non-profits that had been hacked prior to 2016.

— The politics behind it: The Durham annex has long been the subject of intense speculation among the GOP because the memoranda contain explosive allegations about Democrats in 2016, chief among them that former Democratic presidential nominee Hillary Clinton approved a "plan" in the summer of 2016 to knowingly mislead the FBI about Trump's ties to Russia.

— On the flip side: The Durham annex includes findings suggesting some of the emails in the Russian memoranda were — while not invented whole-cloth — the work of subtle Russian fabrication.

U.S. intelligence officials at one point acquired two slightly different versions of the same hacked email, the Durham report reads. In another case, Durham's office found content from a legitimate email in a Russian document — but presented as if the sender were someone else.

— What that may mean: It's unclear if the Russians were intentionally looking to stir up disinformation or merely trying to impress their bosses in the spy services back home, said Michael van Landingham, a former CIA analyst.

Either way, van Landingham said, the declassified Durham report suggested two things: that the Russians were obsessed with taking down Clinton, and that the so-called Clinton plan was made up. "The material absolutely appears fake," said van Landingham, who was the principal author on the intelligence community's report into Russia's

principal author on the intelligence community's report into Russia's actions in the 2016 election.

— Charging ahead: Senior Trump administration officials bristled against the allegation the memoranda contained Russia disinformation over the weekend, after The New York Times reported on similar concerns Friday.

Asked about the possibility the administration is relying on unverified information from a Russian intelligence service, an ODNI official referred MC to the fact that Durham declined to rule out the veracity of Clinton's plan (though he didn't bring any charges for it); that FBI agents he interviewed considered some of the material authentic; and the fact that the CIA issued an assessment in which in it stated it did not judge the memoranda to be Russian fakes.

— Yes, but: In 2020, then-Director of National Intelligence John Ratcliffe said the U.S. spy community "does not know" if the Russian memoranda were real. Van Landingham also pointed out the CIA lacks the authority to vet the documents as Durham did.

"As CIA analysts, we don't have the badge and subpoena power to get answers from victims," he said.

THE CONFERENCE CIRCUIT

CISA SHAKEUP — CISA acting Director Madhu Gottumukkala is no longer coming to Las Vegas for this week's Black Hat conference. Marci McCarthy, CISA's director of public affairs, confirmed to your host late Monday night that Gottumukkala pulled out of the conference due to a "personal matter."

The announcement — which was first reported Monday night by Nextgov — marks the removal of one of the few government officials originally set to headline the conference. Gottumukkala was on the

originally set to headline the conference. Gottumukkala was on the docket to give a keynote talk on Thursday about the top cyber agency's posture to protect U.S. critical infrastructure in cyberspace.

— Other agency personnel: McCarthy added that Chris Butera, the agency's executive assistant director for cybersecurity and Bob Costello, CISA's chief information officer, will "be participating in a number of conversations throughout the week discussing CISA's technical leadership and collaborative efforts to defend the Nation's critical infrastructure."

HACKED

DO WE EVER REALLY KNOW OUR COWORKERS? —The prolific North Korean scheme to infiltrate Western companies by posing as remote IT workers continues to grow more common, according to a new report from cybersecurity giant CrowdStrike.

CrowdStrike's latest threat-hunting report, out on Monday, identified more than 320 incidents over the last year — a more than 200 percent increase from the year before — in which North Korean operatives infiltrated western companies by posing as remote IT workers to funnel their high-paying salaries back to Pyongyang.

— Old scheme, new tricks: While this scheme isn't new, North Korean operatives are using new technology to strengthen it.

The North Korean operatives, which CrowdStrike dubbed "Famous Chollima" in the report, are relying more on continuously improving AI-powered tools to generate convincing resumes and deepfake videos during remote interviews.

AT THE AGENCIES

SLIMMING DOWN — The Pentagon's Defense Technical Information

SLIMMING DOWN — The Pentagon's Defense Technical Information Center will soon cut its personnel down to 40 as part of the larger effort by the Defense Department to slash its workforce, as Maggie writes in.

The change was announced Monday in a memo signed by Emil Michael, DOD under secretary for research and engineering, noting that the DTIC "will be reduced in size through a targeted, deliberate, and expeditious civilian reduction-in-force."

According to the memo, the Pentagon aims to save around $25 million annually through the RIFs, which will be sent to employees at the DTIC by Aug. 25.

It claims that the DTIC has an "unfocused organizational model and legacy information platform," which makes the agency unable to keep up with technological changes by artificial intelligence and other emerging tech. The DTIC is the main repository at the Pentagon for information on government-funded technological and scientific work.

— Uncertain outlook: It's not clear how many personnel currently work at DTIC, and spokespersons for the group did not respond to a request for comment on the specific number.

INDUSTRY INTEL

OPEN [SOURCE] SEASON — Google's AI-powered vulnerability hunter reported its first round of cybersecurity vulnerabilities.

On Monday, Heather Adkins, Google's vice president of security, announced on X that Big Sleep, the tech giant's LLM-based bug researcher, found and reported 20 flaws in popular open-source software.

Big Sleep — which was developed by Google's AI department and

Big Sleep — which was developed by Google's AI department and Project Zero, a team of hackers — identified the vulnerabilities mostly in software like photo editor ImageMagick and video and audio library FFmpeg.

VULNERABILITIES

SHADOW AI — A new report from Menlo Security is recommending companies crack down on employees using shadow AI — the unsanctioned use of AI tools in the workplace.

The report, out today, found that 68 percent of employees use their personal accounts to access free AI tools at work, such as ChatGPT. More than 50 percent of employees input company data into the chatbot, inadvertently exposing potentially sensitive information.

Menlo's report recommends that companies set and enforce rules on AI usage and ban shadow AI in the workplace.

QUICK BYTES

SPILLING TEA — The recent breach of the women's safety dating app Tea is a warning sign for new apps, Business Insider's Sydney Bradley and Henry Chandonnet write.

TICK TOCK — The Information Technology Industry Council is urging lawmakers not to let the 2015 Cybersecurity Information Sharing Act lapse as the September deadline is now less than four weeks away.

BLACKSUIT — CyberScoop's Matt Kapko has new details on the multi-national law enforcement effort to bring down the Russian BlackSuit ransomware group.

DEPARTMENT OF CORRECTIONS

DEPARTMENT OF CORRECTIONS

An item written by Maggie in an earlier version of Monday's Morning Cybersecurity newsletter inaccurately characterized the types of coding repositories targeted by nation-state hackers, as detailed in a report from Strider.

Chat soon.

Stay in touch with the whole team: Rosie Perper (rperper@politico.com); John Sakellariadis (jsakellariadis@politico.com); Maggie Miller (mmiller@politico.com), and Dana Nickel (dnickel@politico.com).

Follow us on X

Rosie Perper @RosiePerper

Maggie Miller @magmill95

Dana Nickel @delizanickel

John Sakellariadis @johnnysaks130

FOLLOW US