Cybersecurity & Military Justice System

A Navy prosecutor during the week of 6 MAY 2019 sent an email to the editor of Navy Times that was embedded with a secret digital tracking device. The tracking device came at a time when the Naval Criminal Investigative Service is mounting an investigation into media leaks surrounding the high-profile court-martial of a Navy SEAL accused of war crimes.

That email, from Navy prosecutor Cmdr. Christopher Czaplak to Navy Times editor Carl Prine, came after several months of Navy Times reporting that raised serious questions about the Navy lawyers' handling of the prosecution in the war crimes case. When asked about the email Czaplak sent to Prine, NCIS spokesman Jeff Houston said 16 MAY that "during the course of the leak investigation, NCIS used an audit capability that ensures the integrity of protected documents. It is not malware, not a virus, and does not reside on computer systems. There is no risk that systems are corrupted or compromised." The Navy's top spokesman, Capt. Greg Hicks, declined to comment on the email device targeting Navy Times but acknowledged that the Navy is conducting "an ongoing investigation into the unauthorized disclosure of information covered by a judge's protective order." Hicks said the investigation is being conducted by the NCIS.

Czaplak is the lead prosecutor in two related war crimes cases involving Navy special warfare personnel. Special Operations Chief Edward Gallagher, has pleaded not guilty to a murder count in the death of an injured teenage militant he allegedly stabbed to death in 2017 in Iraq. Gallagher's platoon's commanding officer, Lt. Jacob Portier, is fighting charges of conduct unbecoming an officer for allegedly conducting Gallagher's re-enlistment ceremony next to the corpse. The case has become so high-profile that it has even drawn the attention of President Donald Trump, who ordered Gallagher moved from the brig to a hospital complex.Top of FormBottom of Form

And now the case has raised questions about how far the Navy will go in pursuing leaks and whether the government is illegally spying on journalists and defense attorneys in the case. The Navy email to Navy Times contained hidden computer coding designed to extract the IP address of the Navy Times computer network and to send that information back to a server located in San Diego. Under U.S. criminal law, authorities normally have to obtain a subpoena or court order to acquire IP addresses or other metadata. Not

using one could be a violation of existing privacy laws, including the Electronic Communications Privacy Act.

Defense attorneys involved in the SEALs' war crimes cases have said that 13 lawyers and paralegals on their team also received emails with a similar tracking device, according to court documents filed by the defense attorneys. In response to the receipt of the emails with tracking devices, defense attorneys have filed motions accusing prosecutors of misconduct for sending the emails. They demanded that no more be sent, and are seeking a halt in proceedings until after an investigation can be completed. Defense attorneys also want a public hearing before a military judge to address the question of how and why prosecutors deployed emails with tracking devices.

Tim Parlatore, attorney for Gallagher, whose case is covered by the gag order imposed by Navy Judge Capt. Aaron Rugh, told Military Times he has filed a motion calling for, among other things, the case to be dismissed and a full investigation into the emails by neutral parties. "It is illegal for the government to use [the emails] in the way they did without a warrant," he said. "What this constitutes is a warrantless surveillance of private citizens, including the media, by the military. We should all be terrified," Parlatore said. "Every Navy sailor should be terrified of whether they can get a fair trial in the Navy justice system," Parlatore said. "The only way they can ever have confidence in their own system is by full disclosure of what is going on."

Parlatore said that Czaplak admitted in court on 10 MAY that he sent the emails containing tracking devices. Czaplak, through a spokesman, declined comment. Gallagher's court-martial trial is scheduled to begin on 28 MAY. Hicks told Military Times that Navy Secretary Richard V. Spencer "is monitoring what's going on" with the NCIS investigation and the resulting concerns of spying on attorneys and a journalist, which was raised in defense motions and first reported by the Associated Press. "Ultimately, this is about Senior Chief Gallagher receiving a fair trial with due process in the military justice system," Hicks said, adding that Rugh, presiding over the Gallagher case, was concerned about leaks in a case covered by a gag order. "Following continuing and ongoing violations of the federal protective order, NCIS initiated a separate investigation into violations of that protective order," Hicks said. "That investigation is ongoing.

All NCIS investigations are conducted in accordance with applicable laws, properly coordinated and executed with appropriate oversight. The government is acting appropriately as part of a lawful, authorized and legitimate investigation into the unauthorized disclosure of information associated with the Gallagher case." Hicks would not state for the record whether the Navy obtained a search warrant or subpoena in connection with the emails with tracking devices. Though Navy Times received one of the emails with a tracking device, Hicks emphasized that the media is not being targeted. "The media was not it and is not the focus of the investigation," he said. "The focus of the investigation is squarely on identifying unauthorized disclosures that violate the judge's protective order."

But the issue is raising concerns with press freedom groups. "By using this tool, if the prosecutor was able to intercept email content, that could potentially be a direct Fourth Amendment violation, even if what the prosecutors got was just the metadata, namely the IP address," said Gabe Rottman, the director of the Technology and Press Freedom Project at the Reporters Committee for Freedom of the Press, a not-for-

profit legal services group. Rottman said his level of concern depends on the nature of the tool used in the emails.

Hicks, however, offered few details about the email received by Prine, what kind of technology was used, how long the investigation has been ongoing, whether the U.S. Attorneys Office or any other civilian court was involved in approving the use of the tracking device or whether any other journalists have received emails with similar tracking devices. Hicks declined to say whether there is any Navy policy regulating the sending of such emails. Nor would he rule out the Navy sending out emails with tracking devices in the future. “I am not speculating on the future,” he said. “I don’t know what will arise. If I did I would buy a lottery ticket.”

What was it?

Emails with tracking devices have been the subject of legal proceedings in the civilian world. That’s where Parlatore first encountered them. A few months back, while investigating a client who was being stalked, Parlatore said he learned the suspected stalker knew the victim’s whereabouts because he had sent the victim an email containing a tracking device that gathered up the location and other information from the victim’s phone. As a result, when Parlatore received the first of three emails from Czaplak containing an unusual logo of an American flag with a bald eagle perched on the scales of justice beneath the prosecutor’s signature on 8 MAY, Parlatore said it immediately raised red flags.

The next day, Parlatore responded to Czaplak with an email of his own. “I am writing regarding your emails from yesterday, which contained an embedded image that was not contained in any of your previous emails,” Parlatore wrote. “At the risk of sounding paranoid, this image is not an attachment, but rather a link to an unsecured server which, if downloaded, can be used to track emails, including forwards. I would hope that you aren’t looking to track emails of defense counsel, so I wanted to make sure there wasn’t a security breach on your end. Given the leaks in this case, I am sure you can understand.”

A few hours later, Czaplak responded to Parlatore, telling him he would get back to him “ASAP.” On May 10, Air Force Lt. Col. Nicholas McCue, an attorney for Portier, received an email on his military computer system from Czaplak, also containing the unusual logo beneath the prosecutor’s signature. Finding that suspicious, McCue contacted his Air Force communications squadron, according to court documents filed by the defense. “He was instructed that the embedded image contained a cyber-tool known as a **‘splunk**’ tool,’ which can allow the originator full access to his computer, and all the files on the computer,” according to a Portier defense motion filed 14 OCT.

“The Air Force Information Systems Security Manger advised McCue to stop using the NIPR network for communications pertaining to the Portier case.” The NIPR network is the military’s network for unclassified material.

In an email on that same day, Daniel Harrison, Information Systems Security Manager for the Cybersecurity Office with the 60th Communications Squadron at Travis Air Force Base told McCue that the email from Czaplak could contain one of several types of cyber tools. Harrison was so concerned about the email received by McCue that he urged him to use the military’s Secret Internet Protocol Router

Network, known as the SIPR, which is far more secure than the Non-classified Internet Protocol Router, or NIPR. “I would strongly recommend using SIPR or a system that is not on the NIPR network for communications that pertain to this case,” Harrison urged McCue.

The same day McCue and the other defense attorneys and staff received the email from Czaplak, Prine, the Navy Times editor, got one too. Will Alexander, vice president for technology and engineering for Sightline Media, the parent company for Navy Times and Military Times, examined that email and said it contained a tracking beacon pointing to an IP address assigned to Cox Cable Modem customers in the San Diego area, where the cases against Gallagher and Portier are being tried. “We suspect the sender likely intended to correlate an IP address with Carl's email account,” he said. “This correlation can be used to then track Carl's past and future access to other systems within the tracker's control.” Beyond that, Alexander said that Sightline Media has no evidence of any attempt to take additional data from Prine’s computer or the company’s internal systems.

So how bad is this?

The prosecution’s attempt to track the emails of defense attorneys and media has several chilling effects. The tracking devices and their underlying technology originated as a marketing tool allowing companies to gather information from customers. By clicking on a box to see a photograph, for instance, the recipients are sending metadata to a server for collection.’ But when used for law enforcement, the tracking takes on a more nefarious connotation. In the judicial part of this equation, tracking devices give the user an unfair advantage in court proceedings. If you know who your opposing counsel is contacting, you can divine how they are building their case and find ways to counter it.

Last year, the Illinois Bar Association became the fourth such organization to rule that emails like the one received by the defense attorneys and Prine are unethical for a variety of reasons, according to Mark C. Palmer, Professionalism Counsel under the Illinois Supreme Court Commission on Professionalism. Bar associations in Alaska, Pennsylvania and New York, where Czaplak was admitted to the bar in 2009 according to state records, have previously reached the same conclusion.

The Illinois State Bar Association opinion concludes that, “at a minimum, the use of such tools by counsel in communications with other lawyers constitutes dishonesty or deceit under Illinois Rule of Professional Conduct,” Palmer wrote in a blog entry on attorneyatwork.com, a discussion site for the legal profession. “Such deception can penetrate the attorney-client relationship of the receiving lawyer and that lawyer’s client to potentially, and likely, divulge protected, extraordinary insight that might not only be protected, but might be quite relevant to the matter.”

As for journalists, the email received by Prine may be unchartered territory, said Rottman of the Reporters Committee. “This is the first case I am aware of that something like this has happened," Rottman said. “If a prosecutor sent an email to a reporter with a tracking device intending to identify a leak, that is certainly concerning." Rottman said the emails in question raise two main concerns.

- The first is the chilling effect on the news gathering process and the free flow of information. “Reporters rely on confidential sources and confidential disclosures of information to do their

jobs," he said. "Any law enforcement scrutiny of unauthorized disclosure has a potentially chilling effect on news gathering." In addition to gaining information about Prine's communications on this case, Rottman said emails with tracking software could affect sources in cases having nothing to do with this. "If it is true that a government official included tracking software in an email to a reporter surreptitiously to find out who the reporter is talking to," he said, "that potentially exposes that reporter's other sources in totally unrelated cases to government scrutiny."

- The other line of concern, said Rottman, is cybersecurity. "It is interesting that the information assurance personnel suggest that the defense counsel bump their communications to a more secure network," said Rottman after being shown an email, contained in court filings, from the Air Force cyber expert offering advice to a defense lawyer on what to do about the email received from Czaplak. Whether any of this is illegal depends on the device used, said Rottman.

"There are all kinds of questions that come into play here," said Rottman, "with respect to the Fourth Amendment," which protects against unlawful search and seizure. "If the Department of Justice were seeking to do this in a criminal leak investigation, it would likely have to get a court order or use a subpoena even to get the metadata under the Electronic Communications Privacy Act," Rottman said.

Kelly Thornton, spokeswoman for the U.S Attorneys Office for the Southern District of California said her office is not handling the Gallagher court-martial proceedings "and is not involved in the production or dissemination of discovery in that case." Sri Sridharan, managing director and chief operating officer for the Florida Center for Cybersecurity at the University of South Florida, said the tracking emails sent out by Czaplak seem to be breaking new ground that cries out for legislative action. "Lawyers will have a field day with this," he said. "Congress needs to pay attention and bring about some serious legislation in cybersecurity."

[Source: MilitaryTimes | Howard Altman | May 16, 2019 ++]