


NSA asks Congress to let it get on with that warrantless data harvesting, again

Also: That Pokemon is actually a RAT, Uncle Sam fails a password audit

 [Brandon Vigliarolo](#)

Sat 14 Jan 2023 // 20:57 UTC

IN BRIEF A US intelligence boss has asked Congress to reauthorize a controversial set of powers that give snoops warrantless authorization to surveil electronic communications in the name of fighting terrorism and so forth.

NSA director General Paul Nakasone told the Privacy and Civil Liberties Oversight Board yesterday that the loss of Section 702 of the Foreign Intelligence Surveillance Act (FISA) would mean American spies would "lose critical insights into the most significant threats to our nation" if allowed to lapse on December 31.

In his speech, Nakasone said Section 702 is "irreplaceable," and he provided several stories of the FBI and NSA cooperating using the law to stop terrorist plots and online attacks to justify his claim.

Section 702 was added to the Foreign Intelligence Surveillance Act in 2008, and has long been a bone of contention between civil liberties groups arguing it's a gross privacy violation, and those who say that, if you're not a terrorist, surely a little harmless observation by Uncle Sam is okay.

The NSA has long held that Section 702 saved American lives and protected the nation and its allies, though documents declassified in 2019 showed that it was frequently used against US persons, despite the law specifically being designed to only apply to foreign targets.

Despite those restrictions, the FBI was found to have used the database of electronic communications gathered from US telecom and tech companies under S.702 to search for records of US persons who were caught up in data gathering sweeps.

When asked about the use of Section 702-gathered data to surveil US persons during hearings over its previous renewal in 2017, the NSA refused to provide figures. "Seems like baloney to me ... It's the greatest intelligence service on the planet. You'd think they'd be able to know that," House Representative Jim Jordan (R-OH) said during the hearings.

"Section 702 cannot be used to target Americans anywhere in the world or any person inside the United States regardless of nationality. No exceptions," Nakasone said.

The records beg to differ, and this time they're known about before reauthorization hearings. Whether that'll change the outcome is another thing altogether.

Avoid this Pokémon

South Korean security firm Ahnlab says it has discovered a malware-spreading campaign that tries to trick netizens into downloading a remote access trojan – a backdoor for remote control in other words – disguised as a beta version of a new Pokémon card game.

This Pokemon-themed malware is hiding in the tall grass, having been subtly tweaked to bypass security tools, the researchers warned. We're told that the trojan uses various legit tools, such as NetSupport Manager, AnyDesk, TeamViewer and others, to provide the backdoor access. These programs include config files with hard-coded command-and-control server IP addresses, as well as the ability to gain persistence by adding a shortcut to the Windows startup folder and adding a hidden appdata path.

Once installed, Ahnlab said, the attacker can make use of any of the features the remote control software includes, giving them potential total control over an infected system.

While nothing in this malware campaign is particularly innovative or exceptionally dangerous, its Pokemon-themed delivery method is, even though the idea of using a children's game to trick kids into downloading malware isn't new.

Federal parks agency fails password security audit ... badly

The US Department of the Interior's mission is to protect America's natural resources, but it might have a hard time doing so if its systems remain as unsecured as a recent Office of the Inspector General report uncovered.

There's no better way to relay the conclusions than the report itself: "We found that the Department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data," the OIG said [PDF].

Several of the bad practices found in DOI systems were the same that allowed the Colonial Pipeline ransomware attack to occur in 2021, the OIG said.

Inspectors were able to crack 21 percent of the agency's passwords (totaling 18,174) - 16 percent of which they figured out within the first 90 minutes of investigating. Of the accounts it managed to break into, 288 had elevated privileges, and 362 belonged to senior US Government employees.

In addition, the OIG said multifactor authentication wasn't consistently implemented at the DOI and password complexity requirements were "outdated and ineffective ... allow[ing] unrelated staff to use the same inherently weak passwords—meaning there was not a rule in place to prevent this practice."

The DOI also wasn't deactivating unused accounts or enforcing password age limits, leaving more than 6,000 additional accounts vulnerable to attack, inspectors found.

The Inspector General had eight recommendations for the DOI, including not implementing MFA methods that can be bypassed, as is currently the case, and enhancing password complexity requirements.

More broadly, the OIG seems to want the DOI to develop a security posture that's less fly-by-night crypto space fintech startup, and more federal government agency with an \$18.1 billion dollar budget. ®

Sponsored: It's time to fill those cloud security gaps

SIMILAR TOPICS

18  COMMENTS

[Foreign Intelligence Surveillance Act](#) [NSA](#) [Password](#) [More like these](#)

Long data privacy notices aren't foolproof, Euro watchdog tells Meta

As Meta reels from €390 million EU fine, the 'personalized ads' case might not be over, Max Schrem's legal group says

SECURITY

3 days | 3 

Wiretap lawsuit accuses Apple of tracking iPhone users who opted out

This is the company that claims: 'Privacy. That's iPhone'

SECURITY

6 days | 9 

CES Worst in Show slams gummi gouging, money-wasting mugs, and other dubious kit

Technology has the potential to make life better. This isn't it.

PERSONAL TECH

10 days | 116 

Bringing the best of all technology worlds to next-gen laptops


Memory is the key to enabling lightweight, power efficient, high-performance portability

SPONSORED FEATURE

No more holidays for US telcos, FCC is cracking down

IN BRIEF Also, LastPass faces class action, and Louisiana says that, while the internet may be for porn, ID is still required


SECURITY

8 days | 41 

Canadian owes bosses for 'time theft' after work-tracking app sinks tribunal bid

She hoped to score thousands but laptop app had other ideas

SECURITY

3 days | 29 

Palantir's Covid-era UK health contract extended without competition

US spy-tech firm's controversial work with patient data pushed out 6 months due to delayed data platform procurement

DATABASES

12 days | 39 

Google gets off easy in location tracking lawsuits

\$29.5 million and we don't have to admit wrongdoing? Where do we sign?

SECURITY

13 days | 4 

LastPass admits attackers have a copy of customers' password vaults

Thankfully a well encrypted copy that could take an eon to crack, unless users practiced bad password hygiene

SECURITY

24 days | 121 

TikTok confirms it tracked journalists' locations as part of leak investigation

As if you needed another reason to delete the app right now

NETWORKS

24 days | 32 

Lawyer mom barred from Rockettes show by facial recognition tech

No Girl Scout cookies for you

AI + ML

25 days | 90 

Parental control apps prove easy to beat by kids and crims

20m downloads can't be wrong? Or can they?

SECURITY

26 days | 19 

The Register Biting the hand that feeds IT

[About Us](#)

[Our Websites](#)

[Your Privacy](#)

