Justice Department Disrupts Russian Intelligence Spear-Phishing Efforts

Published: 2024-10-02 · Archived: 2026-04-06 15:26:19 UTC

The Justice Department announced today the unsealing of a warrant authorizing the seizure of 41 internet domains used by Russian intelligence agents and their proxies to commit computer fraud and abuse in the United States. As an example of the Department's commitment to public-private operational collaboration to disrupt such adversaries' malicious cyber activities, as set forth in the National Cybersecurity Strategy, the Department acted concurrently with a Microsoft civil action to restrain 66 internet domains used by the same actors.

"Today's seizure of 41 internet domains reflects the Justice Department's cyber strategy in action – using all tools to disrupt and deter malicious, state-sponsored cyber actors," said Deputy Attorney General Lisa Monaco. "The Russian government ran this scheme to steal Americans' sensitive information, using seemingly legitimate email accounts to trick victims into revealing account credentials. With the continued support of our private sector partners, we will be relentless in exposing Russian actors and cybercriminals and depriving them of the tools of their illicit trade."

"This disruption exemplifies our ongoing efforts to expel Russian intelligence agents from the online infrastructure they have used to target individuals, businesses, and governments around the world," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "Working closely with private-sector partners such as Microsoft, the National Security Division uses the full reach of our authorities to confront the cyber-enabled threats of tomorrow from Russia and other adversaries."

"Working in close collaboration with public and private sector partners—in this case through the execution of domain seizures — we remain in prime position to counter and defeat a broad range of cyber threats posed by adversaries," said FBI Deputy Director Paul Abbate. "Our efforts to prevent the theft of information by state-sponsored criminal actors are relentless, and we will continue our work in this arena with partners who share our common goals."

"This seizure is part of a coordinated response with our private sector partners to dismantle the infrastructure that cyber espionage actors use to attack U.S. and international targets," said U.S. Attorney Ismail J. Ramsey for the Northern District of California. "We thank all of our private-sector partners for their diligence in analyzing, publicizing, and combating the threat posed by these illicit state-coordinated actions in the Northern District of California, across the United States, and around the world."

The domain names are identified below:

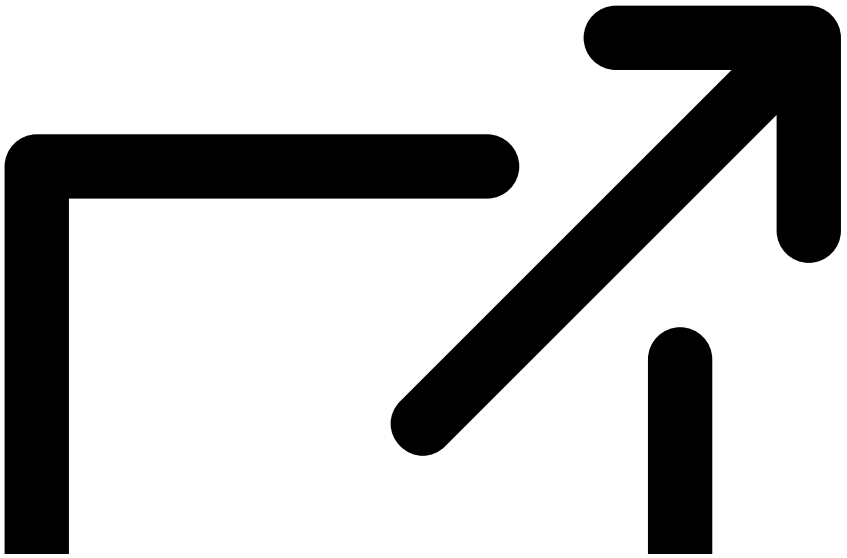
accutanebb[.]com	SUBJECT DOMAIN NAME 1
albuteroltab[.]com	SUBJECT DOMAIN NAME 2
allowdoorinto[.]com	SUBJECT DOMAIN NAME 3

baijiapaintbrush[.]com	SUBJECT DOMAIN NAME 4
baricitinc[.]com	SUBJECT DOMAIN NAME 5
cbdhempoilww[.]com	SUBJECT DOMAIN NAME 6
cbdonlineww[.]com	SUBJECT DOMAIN NAME 7
cenforcep[.]com	SUBJECT DOMAIN NAME 8
cialismgz[.]com	SUBJECT DOMAIN NAME 9
delitky[.]com	SUBJECT DOMAIN NAME 10
divisionintro[.]com	SUBJECT DOMAIN NAME 11
dompurifycheerio[.]com	SUBJECT DOMAIN NAME 12
fastloginway[.]com	SUBJECT DOMAIN NAME 13
fasttruncatedoor[.]com	SUBJECT DOMAIN NAME 14
finduscore[.]com	SUBJECT DOMAIN NAME 15
gateallowsearch[.]com	SUBJECT DOMAIN NAME 16
ghxsjyk[.]com	SUBJECT DOMAIN NAME 17
gnfamotidine[.]com	SUBJECT DOMAIN NAME 18
gnibuprofen[.]com	SUBJECT DOMAIN NAME 19
govdoorsec[.]com	SUBJECT DOMAIN NAME 20
hempcbdww[.]com	SUBJECT DOMAIN NAME 21
inthetrustview[.]com	SUBJECT DOMAIN NAME 22
ithostprotocol[.]com	SUBJECT DOMAIN NAME 23
ivermectint[.]com	SUBJECT DOMAIN NAME 24
londonshowcorp[.]com	SUBJECT DOMAIN NAME 25
maxlliance[.]com	SUBJECT DOMAIN NAME 26
myavtsim[.]com	SUBJECT DOMAIN NAME 27
newtransfersearch[.]com	SUBJECT DOMAIN NAME 28
outviewmachine[.]com	SUBJECT DOMAIN NAME 29
setitcloud[.]com	SUBJECT DOMAIN NAME 30

smartloginbreak[.]com	SUBJECT DOMAIN NAME 31
smartscontract[.]com	SUBJECT DOMAIN NAME 32
tipstoway[.]com	SUBJECT DOMAIN NAME 33
toolpointtrim[.]com	SUBJECT DOMAIN NAME 34
trustvaluespath[.]com	SUBJECT DOMAIN NAME 35
verificationtrim[.]com	SUBJECT DOMAIN NAME 36
viewwaypath[.]com	SUBJECT DOMAIN NAME 37
waylogintexas[.]com	SUBJECT DOMAIN NAME 38
webgovview[.]com	SUBJECT DOMAIN NAME 39
wingscamein[.]com	SUBJECT DOMAIN NAME 40
incomcorporate[.]com	SUBJECT DOMAIN NAME 41

According to the partially unsealed affidavit filed in support of the government's seizure warrant, the seized domains were used by hackers belonging to, or criminal proxies working for, the "Callisto Group," an operational unit within Center 18 of the Russian Federal Security Service (the FSB), to commit violations of unauthorized access to a computer to obtain information from a department or agency of the United States, unauthorized access to a computer to obtain information from a protected computer, and causing damage to a protected computer. Callisto Group hackers used the seized domains in an ongoing and sophisticated spear-phishing campaign with the goal of gaining unauthorized access to, and steal valuable information from, the computers and email accounts of U.S. government and other victims.

In conjunction, Microsoft announced



the filing of a civil action to seize 66 internet domains also used by Callisto Group actors. Microsoft Threat Intelligence tracks this group as “Star Blizzard” (formerly SEABORGIUM, also known as COLDRIVER). Between January 2023 and August 2024, Microsoft observed Star Blizzard target over 30 civil society entities and organizations – journalists, think tanks, and nongovernmental organizations (NGOs) – by deploying spear-phishing campaigns to exfiltrate sensitive information and interfere in their activities.

The government’s affidavit alleges the Callisto Group actors targeted, among others, U.S.-based companies, former employees of the U.S. Intelligence Community, former and current Department of Defense and Department of State employees, U.S. military defense contractors, and staff at the Department of Energy. In December 2023, the Department announced charges against two Callisto-affiliated actors, Ruslan Aleksandrovich Peretyatko (Перетятько Руслан Александрович), an officer in FSB Center 18, and Andrey Stanislavovich Korinets (Коринец Андрей Станиславович). The indictment charged the defendants with a campaign to hack into computer networks in the United States, the United Kingdom, other North Atlantic Treaty Organization member countries, and Ukraine, all on behalf of the Russian government.

The FBI San Francisco Field Office is investigating the case.

The U.S. Attorney’s Office for the Northern District of California and the Justice Department’s National Security Cyber Section of the National Security Division are prosecuting the case.

The case is docketed at *Application by the United States for a Seizure Warrant for 41 Domain Names For Investigation of 18 U.S.C. § 1956(a)(2)(A) and Other Offenses*, No. 4-24-71375 (N.D. Cal. Sept. 16, 2024).

An affidavit in support of a seizure warrant and an indictment are merely allegations. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.
