



## PRESS RELEASE

# Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers

Wednesday, September 18, 2024

### For Immediate Release

U.S. Attorney's Office, Western District of Pennsylvania

## ***Actors Unsuccessfully Sought to Prevent FBI's Disruption of Botnet***

WASHINGTON – The Department of Justice today announced a court-authorized law enforcement operation that disrupted a botnet consisting of more than 200,000 consumer devices in the United States and worldwide. As described in court documents unsealed in the Western District of Pennsylvania, the botnet devices were infected by People's Republic of China (PRC) state-sponsored hackers working for Integrity Technology Group, a company based in Beijing, China, and known to the private sector as "Flax Typhoon."

The botnet malware infected numerous types of consumer devices, including small-office/home-office (SOHO) routers, internet protocol (IP) cameras, digital video recorders (DVRs), and network-attached storage (NAS) devices. The malware connected these thousands of infected devices into a botnet, controlled by Integrity Technology Group, which was used to conduct malicious cyber activity disguised as routine internet traffic from the infected consumer devices. The court-authorized operation took control of the hackers' computer infrastructure and, among other steps, sent disabling commands through that infrastructure to

the malware on the infected devices. During the course of the operation, there was an attempt to interfere with the FBI's remediation efforts through a distributed denial-of-service (DDoS) attack targeting the operational infrastructure that the FBI was utilizing to effectuate the court's orders. That attack was ultimately unsuccessful in preventing the FBI's disruption of the botnet.

"The Justice Department is zeroing in on the Chinese government backed hacking groups that target the devices of innocent Americans and pose a serious threat to our national security," said Attorney General Merrick B. Garland. "As we did earlier this year, the Justice Department has again destroyed a botnet used by PRC-backed hackers to infiltrate consumer devices here in the United States and around the world. We will continue to aggressively counter the threat that China's state-sponsored hacking groups pose to the American people."

"The targeted hacking of hundreds of thousands of innocent victims in the United States and around the world shows the breadth and aggressiveness of PRC state-sponsored hackers," said Eric G. Olshan, the United States Attorney for the Western District of Pennsylvania. "This court-authorized operation disrupted a sophisticated botnet designed to steal sensitive information and launch disruptive cyber attacks. We will continue to work with our partners inside and outside government, using every tool at our disposal, to defend and maintain global cybersecurity."

"This dynamic operation demonstrates, once again, the Justice Department's resolve in countering the threats posed by PRC state-sponsored hackers," said Assistant Attorney General Matthew G. Olsen of the National Security Division. "[For the second time this year](#), we have disrupted a botnet used by PRC proxies to conceal their efforts to hack into networks in the U.S. and around the world to steal information and hold our infrastructure at risk. Our message to these hackers is clear: if you build it, we will bust it."

"The disruption of this worldwide botnet is part of the FBI's commitment to using technical operations to help protect victims, expose publicly the scope of these criminal hacking campaigns, and to use the adversary's tools against them to remove malicious infrastructure from the virtual battlefield," said FBI Deputy Director Paul Abbate. "The FBI's unique legal authorities allowed it to lead an international operation with partners that collectively disconnected this botnet from its China-based hackers at Integrity Technology Group."

According to the court documents, the botnet was developed and controlled by Integrity Technology Group, a publicly traded company headquartered in Beijing, China. The company built an online application allowing its customers to log in and control specified infected victim devices, including with a menu of malicious cyber commands using a tool called "vulnerability-arsenal." The online application was prominently labelled "KRLab," one of the main public brands used by Integrity Technology Group.

The FBI assesses that Integrity Technology Group, in addition to developing and controlling the botnet, is responsible for computer intrusion activities attributed to China-based hackers known by the private sector as “Flax Typhoon.” Microsoft Threat Intelligence described [Flax Typhoon](#) as nation-state actors based out of China, active since 2021, who have targeted government agencies and education, critical manufacturing, and information technology organizations in Taiwan, and elsewhere. The FBI’s investigation has corroborated Microsoft’s conclusions, finding that Flax Typhoon has successfully attacked multiple U.S. and foreign corporations, universities, government agencies, telecommunications providers, and media organizations.

A cybersecurity advisory describing Integrity Technology Group tactics, techniques and procedures was also published today by the FBI, the National Security Agency, U.S. Cyber Command’s Cyber National Mission Force, and partner agencies in Australia, Canada, New Zealand and the United Kingdom. [JCSA: People’s Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations](#)

The government’s malware disabling commands, which interacted with the malware’s native functionality, were extensively tested prior to the operation. As expected, the operation did not affect the legitimate functions of, or collect content information from, the infected devices. The FBI is providing notice to U.S. owners of devices that were affected by this court-authorized operation. The FBI is contacting those victims through their internet service provider, who will provide notice to their customers.

The U.S. Attorney’s Office for the Western District of Pennsylvania, FBI’s San Diego Office and Cyber Division, and the National Security Cyber Section of the Justice Department’s National Security Division led the domestic disruption effort. Assistance was also provided by the Criminal Division’s Computer Crime and Intellectual Property Section. These efforts would not have been successful without the collaboration of partners, including French authorities, and Lumen Technologies’ threat intelligence group, Black Lotus Labs, which first identified and described this botnet, which it named Raptor Train, in July 2023.

If you believe you have a compromised computer or device, please visit the FBI’s [Internet Crime Complaint Center \(IC3\)](#) or [report online to CISA](#). You may also contact your local FBI field office directly.

The FBI continues to investigate Integrity Technology Group’s and Flax Typhoon’s computer intrusion activities.

*Updated September 18, 2024*

## Topic

**CYBERCRIME**

## Component

[USAO - Pennsylvania, Western](#)

# Related Content

### PRESS RELEASE

## **Rydox Cybercrime Marketplace Shut Down and Three Administrators Arrested**

December 12, 2024

### PRESS RELEASE

## **Justice Department Seizes Four Web Domains Used to Create Over 40,000 Spoofed Websites and Store the Personal Information of More Than a Million Victims**

April 18, 2024

### PRESS RELEASE

## **Moldovan Botnet Operator Indicted for Role in Conspiracy to Unlawfully Access Thousands of Infected Computers Throughout the United States**

April 16, 2024

---



700 Grant Street, Suite 4000  
Pittsburgh, PA 15219

17 South Park Row, Room A330  
Erie, PA 16501

319 Washington Street, Suite 200  
Johnstown, PA 15901

Email USAO-WDPA



Pittsburgh: 412-644-3500  
Fax: 412-644-4549

Erie: 814-452-2906  
Fax: 814-455-6951

Johnstown: 814-533-4547  
Fax: 814-533-4545