911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation

Published: 2024-05-29 · Archived: 2026-04-05 19:17:35 UTC

A court-authorized international law enforcement operation led by the U.S. Justice Department disrupted a botnet used to commit cyber attacks, large-scale fraud, child exploitation, harassment, bomb threats, and export violations.

As part of this operation, YunHe Wang, 35, a People's Republic of China national and St. Kitts and Nevis citizen-by-investment, was arrested on May 24 on criminal charges arising from his deployment of malware and the creation and operation of a residential proxy service known as "911 S5."

According to an indictment unsealed on May 24, from 2014 through July 2022, Wang and others are alleged to have created and disseminated malware to compromise and amass a network of millions of residential Windows computers worldwide. These devices were associated with more than 19 million unique IP addresses, including 613,841 IP addresses located in the United States. Wang then generated millions of dollars by offering cybercriminals access to these infected IP addresses for a fee.

"This Justice Department-led operation brought together law enforcement partners from around the globe to disrupt 911 S5, a botnet that facilitated cyber-attacks, large-scale fraud, child exploitation, harassment, bomb threats, and export violations," said Attorney General Merrick B. Garland. "As a result of this operation, YunHe Wang was arrested on charges that he created and operated the botnet and deployed malware. This case makes clear that the long arm of the law stretches across borders and into the deepest shadows of the dark web, and the Justice Department will never stop fighting to hold cybercriminals to account."

"Working with our international partners, the FBI conducted a joint, sequenced cyber operation to dismantle the 911 S5 Botnet—likely the world's largest botnet ever," said FBI Director Christopher Wray. "We arrested its administrator, Yunhe Wang, seized infrastructure and assets, and levied sanctions against Wang and his co-conspirators. The 911 S5 Botnet infected computers in nearly 200 countries and facilitated a whole host of computer-enabled crimes, including financial frauds, identity theft, and child exploitation. This operation demonstrates the FBI's commitment to working shoulder-to-shoulder with our partners to protect American businesses and the American people, and we will work tirelessly to unmask and arrest the cybercriminals who profit from this illegal activity."

According to court documents, Wang allegedly propagated his malware through Virtual Private Network (VPN) programs, such as MaskVPN and DewVPN (torrent distribution models that he operated) and pay-per-install services that bundled his malware with other program files, including pirated versions of licensed software or copyrighted materials. Wang then managed and controlled approximately 150 dedicated servers worldwide, approximately 76 of which he leased from U.S. based online service providers. Using the dedicated servers, Wang

deployed and managed applications, commanded and controlled the infected devices, operated his 911 S5 service, and provided paying customers with access to proxied IP addresses associated with the infected devices.

“As alleged in the indictment, Wang created malware that compromised millions of residential computers around the world and then sold access to the infected computers to cybercriminals,” said Principal Deputy Assistant Attorney General Nicole M. Argentieri, head of the Justice Department’s Criminal Division. “These criminals used the hijacked computers to conceal their identities and commit a host of crimes, from fraud to cyberstalking. Cybercriminals should take note. Today’s announcement sends a clear message that the Criminal Division and its law enforcement partners are firm in their resolve to disrupt the most technologically sophisticated criminal tools and hold wrongdoers to account.”

“YunHe Wang created and administered a residential proxy service—a botnet known as 911 S5—that affected millions of computers all over the world,” said U.S. Attorney Damien M. Diggs for the Eastern District of Texas. “He will now be held accountable. Proxy services like 911 S5 are pervasive threats that shield criminals behind the compromised IP addresses of residential computers worldwide. Successfully tackling a problem of this scale is only possible with strong collaboration and exceptional investigative work between our law enforcement partners at home and abroad, and we stand ready to hold accountable anyone—no matter where they are located—who exploits our telecommunications infrastructure for their own criminal purpose.”

Cybercriminals then used proxied IP addresses purchased from 911 S5 to conceal their true originating IP addresses and locations, and anonymously commit a wide array of offenses. These offenses including financial crimes, stalking, transmitting bomb threats and threats of harm, illegal exportation of goods, and receiving and sending child exploitation materials. Since 2014, 911 S5 allegedly enabled cybercriminals to bypass financial fraud detection systems and steal billions of dollars from financial institutions, credit card issuers, and federal lending programs.

911 S5 customers allegedly targeted certain pandemic relief programs. For example, the United States estimates that 560,000 fraudulent unemployment insurance claims originated from compromised IP addresses, resulting in a confirmed fraudulent loss exceeding $5.9 billion. Additionally, in evaluating suspected fraud loss to the Economic Injury Disaster Loan (EIDL) program, the United States estimates that more than 47,000 EIDL applications originated from IP addresses compromised by 911 S5. Millions of dollars more were similarly identified by financial institutions in the United States as loss originating from IP addresses compromised by 911 S5.

The 911 S5 client interface software, which was hosted on U.S.-based servers, enabled cybercriminals located outside of the United States to purchase goods with stolen credit cards or criminally derived proceeds, and illegally export them outside of the United States contrary to U.S. export laws, such as the Export Administration Regulations (EAR). The 911 S5 client interface may also contain encryption or other features which subject it to export controls detailed in the EAR. Accordingly, downloads of the 911 S5 client interface software by certain foreign nationals without a license may constitute violations of the EAR.

“The disruption, seizure, and arrest of the perpetrator(s) responsible for the 911 S5 cybercriminal enterprise demonstrates the forward leaning posture of the Department of Defense Office of Inspector General Defense Criminal Investigative Service (DCIS) Cyber Field Office,” said DCIS Director Kelly P. Mayo. “This investigation showcases the critical import of identifying and pursuing emerging threats and technologies targeting

our warfighters, and the industrial base that supports them. Today's announcement illustrates the magnitude of cooperation within federal law enforcement and our foreign partners pursuing criminals in the rapidly evolving cybercrime arena."

The indictment further alleges that from 2018 until July 2022, Wang received approximately $99 million from his sales of the hijacked proxied IP addresses through his 911 S5 operation, either in cryptocurrency or fiat currency. Wang used the illicitly gained proceeds to purchase real property in the United States, St. Kitts and Nevis, China, Singapore, Thailand, and the United Arab Emirates. The indictment identifies dozens of assets and properties subject to forfeiture, including a 2022 Ferrari F8 Spider S-A, a BMW i8, a BMW X7 M50d, a Rolls Royce, more than a dozen domestic and international bank accounts, over two dozen cryptocurrency wallets, several luxury wristwatches, 21 residential or investment properties (across Thailand, Singapore, the U.A.E., St. Kitts and Nevis, and the United States), and 20 domains.

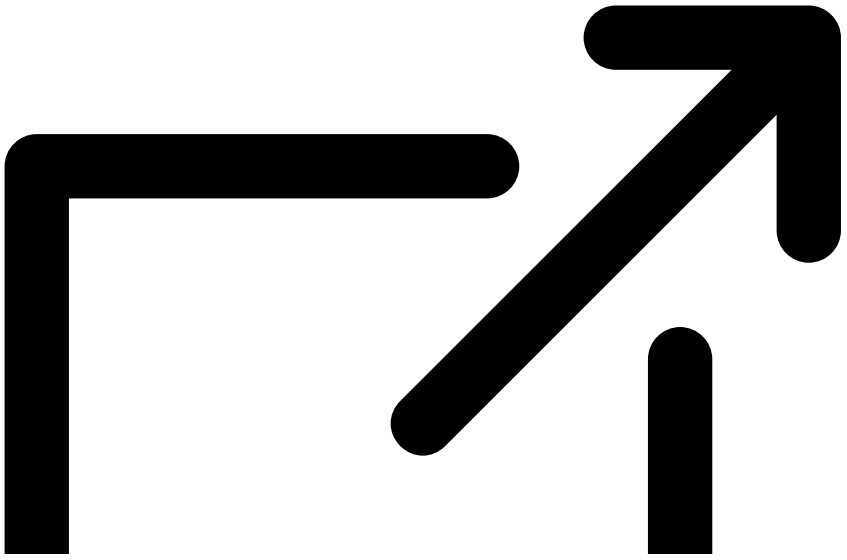
Law enforcement initially focused on 911 S5 during an investigation of a money laundering and smuggling scheme, where criminal actors in Ghana and the United States used hijacked IP addresses purchased from 911 S5 to place fraudulent orders using stolen credit cards on the Army and Air Force Exchange Service (AAFES) online e-commerce platform known as ShopMyExchange. Although approximately 2,525 fraudulent orders valued at $5.5 million were submitted, credit card fraud detection systems and federal investigators were able to thwart the bulk of the attempted purchases, reducing the actual loss to approximately $254,000.

"The conduct alleged here reads like it's ripped from a screenplay: A scheme to sell access to millions of malware-infected computers worldwide, enabling criminals over the world to steal billions of dollars, transmit bomb threats, and exchange child exploitation materials—then using the scheme's nearly $100 million in profits to buy luxury cars, watches, and real estate," said Assistant Secretary for Export Enforcement Matthew S. Axelrod of the U.S. Department of Commerce's Bureau of Industry and Security (BIS). "What they don't show in the movies though is the painstaking work it takes by domestic and international law enforcement, working closely with industry partners, to take down such a brazen scheme and make an arrest like this happen."

Wang is charged with conspiracy to commit computer fraud, substantive computer fraud, conspiracy to commit wire fraud, and conspiracy to commit money laundering. If convicted on all counts, Wang faces a maximum penalty of 65 years in prison.

This operation was a coordinated multiagency effort led by law enforcement in the United States, Singapore, Thailand, and Germany. Agents and officers searched residences, seized assets valued at approximately $30 million, and identified additional forfeitable property valued at approximately $30 million. The operation also seized 23 domains and over 70 servers constituting the backbone of Wang's prior residential proxy service and the recent incarnation of the service. By seizing multiple domains tied to the historical 911 S5, as well as several new domains and services directly linked to an effort to reconstitute the service, the government has successfully terminated Wang's efforts to further victimize individuals through his newly formed service Clourouter.io and closed the existing malicious backdoors.

On May 28, the Treasury Department's Office of Foreign Assets Control (OFAC) issued financial sanctions



against Wang, Jingping Liu, and Yanni Zheng, for their activities associated with 911 S5, and three entities for being owned or controlled by Wang.

The FBI Dallas and Denver Field Offices, DCIS Cyber Field Office, and BIS Office of Export Enforcement's Dallas field office are investigating the case.

Trial Attorneys Candy Heath and Lydia Lichlyter of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Camelia Lopez and William Tatum for the Eastern District of Texas are prosecuting the case.

The Department appreciates the significant assistance provided by the Attorney-General's Chambers of Singapore, Singapore Police Force (SPF), Royal Thai Police, and the Office of the Attorney General and the Anti-Money Laundering Office of the Kingdom of Thailand. The Justice Department's Office of International Affairs and Money Laundering and Asset Recovery Section provided crucial support to this operation. The Treasury Department's OFAC also provided support to this operation. Additionally, the Department offers its thanks to Chainalysis, the Shadowserver Foundation, and Microsoft for the assistance provided by each during the investigation and the operation.

For more information or to determine if you are a victim of 911 S5 malware, please visit www.fbi.gov/911S5.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Source: https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation