U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

Press Release

Wednesday, January 31, 2024

For Immediate Release
Office of Public Affairs

Court-Authorized Operation Removed Malware from U.S.-Based Victim Routers and Took Steps to Prevent Reinfection

A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers.

The hackers, known to the private sector as "Volt Typhoon," used privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities directed against U.S. and other foreign victims. These further hacking activities included a campaign targeting critical infrastructure organizations in the United States and elsewhere that was the subject of a May 2023 FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and foreign partner advisory. The same activity has been the subject of private sector partner advisories in May and December 2023, as well as an additional secure by design alert released today by CISA.

The vast majority of routers that comprised the KV Botnet were Cisco and NetGear routers that were vulnerable because they had reached "end of life" status; that is, they were no longer supported through their manufacturer's security patches or other software updates. The court-authorized operation deleted the KV Botnet malware from the routers and took additional steps to sever their connection to the botnet, such as blocking communications with other devices used to control the botnet.

“The Justice Department has disrupted a PRC-backed hacking group that attempted to target America’s critical infrastructure utilizing a botnet,” said Attorney General Merrick B. Garland. “The United States will continue to dismantle malicious cyber operations – including those sponsored by foreign governments – that undermine the security of the American people.”

“In wiping out the KV Botnet from hundreds of routers nationwide, the Department of Justice is using all its tools to disrupt national security threats – in real time,” said Deputy Attorney General Lisa O. Monaco. “Today’s announcement also highlights our critical partnership with the private sector – victim reporting is key to fighting cybercrime, from home offices to our most critical infrastructure.”

“China’s hackers are targeting American civilian critical infrastructure, pre-positioning to cause real-world harmto American citizens and communities in the event of conflict,” said FBI Director Christopher Wray. “Volt Typhoon malware enabled China to hide as they targeted our communications, energy, transportation, and water sectors. Their pre-positioning constitutes a potential real-world threat to our physical safety that the FBI is not going to tolerate. We are going to continue to work with our partners to hit the PRC hard and early whenever we see them threaten Americans.”

“Today, the FBI and our partners continue to stand firmly against People's Republic of China cyber actors that threaten our nation's cyber security,” said FBI Deputy Director Paul Abbate. “We remain committed to thwarting malicious activities of this type and will continue to disrupt and dismantle cyber threats, safeguarding the fabric of our cyber infrastructure.”

“This operation disrupted the efforts of PRC state-sponsored hackers to gain access to U.S. critical infrastructure that the PRC would be able to leverage during a future crisis,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “The operation, together with the release of valuable network defense guidance by the U.S. government and private sector partners, demonstrates the Department of Justice’s commitment to enhance cybersecurity and disrupt efforts to hold our critical infrastructure at risk.”

“Using traditional law enforcement tools to disrupt state-of-the-art technologies, the U.S. Attorney’s Office for the Southern District of Texas protected Americans from PRC government-sponsored cyber-criminals who used U.S. based routers to hack into American targets,” said U.S. Attorney Alamdar S. Hamdani for the Southern District of Texas. “This case demonstrates my office’s ongoing commitment to defending our critical infrastructure from PRC initiated cyber-attacks. We thank the FBI and the Justice Department’s National Security Division for its work, and we will continue to work shoulder to shoulder with them to shield our country from state-sponsored hackers.”

“The FBI’s dismantling of the KV Botnet sends a clear message that the FBI will take decisive action to protect our nation’s critical infrastructure from cyber-attacks,” said Special Agent in Charge Douglas Williams of the FBI Houston Field Office. “By ensuring home and small-business routers are replaced after their end-of-life expiration, everyday citizens can protect both their personal cyber security and the digital safety of the United States. We need the American public’s vigilance and support to continue our fight against malicious PRC-sponsored cyber actors.”

As described in court documents, the government extensively tested the operation on the relevant Cisco and NetGear routers. The operation did not impact the legitimate functions of, or collect content information from, hacked routers. Additionally, the court-authorized steps to disconnect the routers from the KV Botnet and prevent reinfection are temporary in nature. A router's owner can reverse these mitigation steps by restarting the router. However, a restart that is not accompanied by mitigation steps similar to those the court order authorized will make the router vulnerable to reinfection.

The FBI is providing notice of the court-authorized operation to all owners or operators of SOHO routers that were infected with the KV Botnet malware and remotely accessed pursuant to the operation. For those victims whose contact information was not publicly available, the FBI has contacted providers (such as a victim's internet service provider) and has asked those providers to provide notice to the victims.

FBI Houston Field Office and Cyber Division, U.S. Attorney's Office for the Southern District of Texas, and National Security Cyber Section of the Justice Department's National Security Division led the disruption effort. The Justice Department's Criminal Division's Computer Crime and Intellectual Property Section and Office of International Affairs provided valuable assistance. These efforts would not have been successful without the partnership of numerous private-sector entities.

If you believe you have a compromised router, please visit the FBI's Internet Crime Complaint Center or report online to CISA. The remediated routers remain vulnerable to future exploitation by Volt Typhoon and other hackers, and the FBI strongly encourages router owners to remove and replace any end-of-life SOHO router currently in their networks.

The FBI continues to investigate Volt Typhoon's computer intrusion activity.

5018 search warrant
5530 search warrant
5451 search warrant
5432 search warrant
Updated January 31, 2024

Topics

Cybercrime

National Security

Press Release Number: 24-122