DigiKnow
CYBER SECURITY DEPENDS ON YOU

RANSOMWARE AND ROUTERS - SCORE TWO FOR THE DEPARTMENT OF JUSTICE

February 2024| Issue 2024:2

DEPARTMENT OF JUSTICE TAKES DOWN FANCY BEAR ROUTER ATTACKS

In an ongoing battle against cyber threats, the United States Department of Justice (DOJ) has carried out a covert operation resulting in the removal of malware from over a thousand routers across U.S. homes and businesses. This malware was linked to the Russian hacking group, Fancy Bear, known for coordinating botnets to commit cybercrimes and conduct espionage. The operation, dubbed "Operation Dying Ember," involved routers that were vulnerable due to unchanged default administrative passwords, and were running Ubiquiti's EdgeOS.

This sophisticated cyber takedown by the DOJ utilized the malware itself, Moobot. The malware's creator, Fancy Bear, hijacked this initial infection, installing additional scripts to repurpose the routers into their espionage network. The DOJ's strategic counter-operation not only involved the deletion of the botnet files but also altered the routers' firewall rules to block further remote management access. This decisive action ensured a temporary disconnection of the routers from Fancy Bear's reach.

Fancy Bear's activities have been a significant concern, especially considering their focus on Ukraine amidst the ongoing conflict. The botnet's presence within US routers presented a complex challenge, as it could have made it appear as if American individuals or entities were the ones carrying out cyberattacks against Ukrainian targets. The DOJ's action to neutralize the botnet was critical not only for the security of American networks but also for maintaining international cyber peace.

FBI PUTS A LOCK ON LOCKBIT

Cybercriminal gangs have adopted ransomware as a get-rich-quick scheme. Now, in the era of "ransomware as a service", this has become a prolific and highly profitable tactic. Providing ransomware as a service means groups benefit from affiliate schemes where commission is paid for successful ransom demands.

The Department of Justice joined the United Kingdom and international law enforcement partners in London on February 20, 2024, to announce the disruption of the LockBit ransomware group.

The FBI reports that The LockBit ransomware variant first appeared around January 2020 and had grown into one of the most active and destructive variants in the world. LockBit members have executed attacks against more than 2,000 victims in the United States and around the world, making at least hundreds of millions of U.S. dollars in ransom demands and receiving over $120 million in ransom payments. The LockBit ransomware variant, like other major ransomware variants, operates in the "ransomware-as-a-service" (RaaS) model, in which administrators, also called developers, design the ransomware, recruit other members — called affiliates — to deploy it, and maintain an online software dashboard called a "control panel" to provide the affiliates with the tools necessary to deploy LockBit.

Affiliates, in turn, identify and unlawfully access vulnerable computer systems, sometimes through their own hacking or at other times by purchasing stolen access credentials from others. Using the control panel operated by the developers, affiliates then deploy LockBit within the victim computer system, allowing them to encrypt and steal data for which a ransom is demanded to decrypt or avoid publication on a public website maintained by the developers, often called a data leak site.

The U.K. National Crime Agency's (NCA) Cyber Division, working in cooperation with the Justice Department, Federal Bureau of Investigation (FBI), and other international law enforcement partners disrupted LockBit's operations by seizing numerous public-facing websites used by the group to connect to the organization's infrastructure and seizing control of servers used by administrators, thereby disrupting the ability of LockBit actors to attack and encrypt networks and extort victims by threatening to publish stolen data.

For most homes, the Wi-Fi router is an all-in-one network device that handles both the Wi-Fi access point side of things and the security and routing of the entire network. If your router is seriously out-of-date with unpatched vulnerabilities, it's not just the neighbors' kid stealing your Wi-Fi you have to worry about, it's the security of your internet too.

Now is a good time to check the age of your router at home. You should upgrade your router every 3-5 years to ensure access to new Wi-Fi technology, improved hardware, and consistent security updates.

Solomon Adote
Chief Security Officer

“For years, LockBit associates have deployed these kinds of attacks again and again across the United States and around the world. Today, U.S. and U.K. law enforcement are taking away the keys to their criminal operation,” said Attorney General Merrick B. Garland. “And we are going a step further — we have also obtained keys from the seized LockBit infrastructure to help victims decrypt their captured systems and regain access to their data. LockBit is not the first ransomware variant the Justice Department and its international partners have dismantled. It will not be the last.”

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**