FBI Warning: HelloKitty Ransomware Add DDoS to Extortion Arsenal

speartip.com/resources/fbi-hellokitty-ransomware-adds-ddos-to-extortion-arsenal/

November 2, 2021

Chris Swagler | November 2nd, 2021

The United States Federal Bureau of Investigation (FBI) issued a warning to private company partners that the HelloKitty ransomware group (aka FiveHands) has added distributed denial-of-service (DDoS) attacks to their extortion methods. Coordinating with the Cybersecurity and Infrastructure Security Agency (CISA), the FBI explained that the ransomware group will shut down their victims' websites in DDoS attacks if they refuse the ransom demands. The HelloKitty ransomware group is known for extracting sensitive data from the victims' compromised servers before encrypting them. By using the exfiltrated files as leverage, the threat actors pressure victims into paying the ransom by threatening to release the stolen data on their data leak website.

According to the FBI, the threat actors implement a DDoS attack on a company's public website if they refuse to pay the ransom or do not respond quickly. HelloKitty (FiveHands) actors demand customized Bitcoin (BTC) ransom payments equivalent to each victim's ability to pay. The threat actors either post the stolen data on their Babuk site "payload.bin" or sell it to a third-party data broker if the victim does not pay the ransom. The HelloKitty operators utilize several tactics and techniques to breach the targeted networks, including compromised credentials and security flaws in recently patched SonicWall products, including CVE-2021-20016, CVE-2021-20021, CVE-2021-20022, and CVE-2021-2002.

In November 2020, HelloKitty began as a human-operated ransomware group and quickly attracted the FBI's attention in January 2021. In February, the group was responsible for breaching and encrypting the CD Projekt Red systems and stealing source codes from Cyberpunk 2077, Witcher 3, Gwent, and other games. Although it was never confirmed, HelloKitty claimed that the stolen CD Projekt Red files were purchased by a third party. The ransomware group has been using a Linux variant targeting VMware's ESXi virtual machine platform since July 2021. HelloKitty is one of many ransomware groups targeting Linux servers after companies switch to virtual machines for more efficient resource use and easier device management. Ransomware operators can simultaneously encrypt multiple servers with a single command by targeting a company's virtual machines, saving the group time and effort. HelloKitty was increasingly active in July and August since they started using the Linux variant in their attacks, according to victim submissions on the ID Ransomware platform.

To assist cybersecurity professionals and system administrators in guarding their networks against coordinated HelloKitty ransomware attacks, the FBI added an extensive collection of indicators of compromise (IOCs) in their alert. With ransomware groups like HelloKitty adding more complex extortion techniques, including DDoS, to their attack arsenal, it's crucial that companies view paying threat actors the ransom as a "last resort". Groups like HelloKitty will deploy different extortion tactics, like DDoS, to squeeze payments out of victims.

At SpearTip, our certified engineers have the experience in handling these situations and negotiating with threat actors, so your company won't have to. In any situation, threat actors are never to be trusted because they will try to implement a DDoS attack on your company's website even after payment has been made

With our certified engineers working 24/7 at our three Security Operations Center locations, we continuously monitor your networks for potential threats, including HelloKitty. The most effective route in protecting your company's network is always being proactive. A great proactive tool we offer clients of any size is our ShadowSpear Platform, our endpoint detection and response system, because it prevents ransomware, like HelloKitty, from infiltrating your company's servers and provides a direct communication line to our engineers should you have any questions. Our engineers can be reached through email at .

If your company is experiencing a breach, call our Security Operations Centers at 833.997.7327 to speak directly with an engineer.

Total Economic Impact™ Of SpearTip ShadowSpear