Mirai Botnet Update

October 24, 2016

To Our Valued Customers,

On Oct. 21st, 2016, the Mirai botnet, a malware, used vulnerable technology to launch a DDoS attack, overwhelming the web service DYN with traffic, resulting in slow Internet speeds and offline sites. Amazon, Spotify and Twitter were among sites affected by the attack. The Mirai botnet malware used default admin passwords to exploit Telnet vulnerabilities.

We have not received any reports of Hikvision products being affected by the Mirai botnet malware.

Hikvision is committed to combating cybersecurity risks and as part of these efforts the company has established the industry-leading security lab and engaged third-party security professionals. At Hikvision, we believe it is our duty to be vigilant about cybersecurity, and it is our responsibility to protect and be a resource for our valued customers and the security industry as a whole.

As part of the Security Activation Procedure, Hikvision products no longer have a default admin passcode; instead, a user-defined passcode must be created during device initialization. Telnet access was disabled by default, and is no longer available. Hikvision is committed to staying ahead of evolving cybersecurity threats. The Security Center has detailed instructions on how to change passwords and upgrade firmware on Hikvision IP cameras and recorders – two procedures that are crucial for cybersecurity.

By setting high standards for product security and following the strict guidelines of reputable outside sources, Hikvision is committed to the utmost quality and safety of its products. We encourage our partners to take advantage of the many cybersecurity resources Hikvision offers, and to contact us via the Hikvision Security Center, Tech Support or your Hikvision representative at anytime with any concerns or questions.

Hikvision USA and Canada

+1 909-895-0400 Main
+1 866-200-6690 Toll-Free (US & Canada only)

Hikvision USA Inc.
18639 Railroad Street
City of Industry, CA 91748
www.hikvision.com