Title: Exclusive: Bitdefender Discovers Ring Doorbell Vulnerability

Author: Neil Rudenking

Reference:

Rudenking, N. (8 Nov 2019) Exclusive: Bitdefender Discovers Ring Doorbell Vulnerability. *PC Mag Australia*, Retrieved from: https://au.pcmag.com/bitdefender-box-2/64310/exclusive-bitdefender-discovers-ring-doorbell-vulnerability on 1 April, 2024.

Brief Summary: The article discusses an issue associated with the Ring Doorbell. This product aims to replace conventional doorbells with a "smart" equivalent that contains several additional features, including the ability to see who is at the door from a remote smart device, such as a user's phone. For the Ring Doorbell to function, it needs to be connected to the local WiFi network, so during the initial setup of the doorbell it needs to get the credentials to the home WiFi. To enable the user to input those credentials, an initial WIFI connection from a user device to the Doorbell is made, but this connection is not encrypted. As a result, anyone within a reasonable physical distance of the device and with hardware capable of capturing WiFi signals is able to observe these credentials.

Information Asset: The information asset involved is the credentials to the user's WiFi network which the Ring Doorbell is being connected to. This asset is in the state of transmission when it is vulnerable. Notably, multiple other information assets could be compromised in subsequent chain of events. For example, access to these credentials could facilitate access to other devices on the home network.

Threat: Exposure of the credentials for access to the user's network via network sniffing (i.e., listening to the data exchanged between two devices by an external threat actor). This action would compromise the confidentiality of these credentials.

Vulnerability: The use of an unencrypted connection between the Ring Doorbell and the user's device to facilitate the exchange of the home WIFI credentials in the set-up phase is a vulnerability. This vulnerability is associated with property - as it is an implementation oversight by the developer of the Ring Doorbell product.

Security Incident / Attack: In the unlikely case where the WiFi credentials happen to be captured by a threat actor when the Ring doorbell is initially being setup, this would be considered a passive attack. It is a passive attack, as the threat actor does not need to directly interact with the Ring Doorbell/Home WiFi system. However, the article also describes a specific process that the threat actor can use after the Ring doorbell is in use, to trigger the vulnerable condition and subsequently sniff the users' credentials. In this case, the threat actor uses a common de-authentication method to remove the Ring Doorbell from the network. This forces the users to connect the device again, while the threat actor is waiting to sniff the users' credentials. If this occurred, the actions to remove the Ring doorbell from the network form an active attack, as deliberate action involving direct interaction with the system is required. Importantly, the research described in this article was demonstrated in the real world, meaning this is not purely theoretical. As the organisation uses this Doorbell in the workplace, this is a relevant risk.