Sophisticated malware could target your smart home in 2019

By Darren Allan November 29, 2018 Internet

McAfee’s threat predictions for next year make for worrying reading

Malware will become far more sophisticated in 2019, with cybercriminals using AI to drive attacks, according to McAfee’s latest threat predictions for the coming year, which also underline the dangers likely to be posed to the smart home.

McAfee believes that new strains of malware will be equipped with increasingly sophisticated evasion techniques. So, for example, we will see cryptocurrency mining malware with built-in measures to prevent detection.
The security firm notes that the WaterMiner malware is capable of stopping its mining process whenever the victim runs an antivirus scan, or indeed opens up the Task Manager to try and see if any running processes are consuming a lot of CPU usage – effectively hiding itself. Botnets will also use cleverer obfuscation techniques.

And not only will cybercriminals be better able to deal with AI-powered anti-malware measures, but they will begin to employ AI themselves. McAfee notes: “We expect evasion techniques to begin leveraging artificial intelligence to automate target selection, or to check infected environments before deploying later stages and avoiding detection.”

Malware using AI to such ends will soon be found in the wild, according to the security company.

As for the smart home, the often wobbly security associated with the many internet-connected gadgets therein is always a worry, and McAfee believes that these will be a focus for attacks in 2019.

More specifically, McAfee thinks cybercriminals will target two main vectors to compromise smart home security: smartphones/tablets, and routers.

More than Mirai…

We’ve already seen the security problems that many routers suffer from – just witness the havoc the Mirai botnet caused when it popped up a couple years ago, compromising routers and other IoT devices – but McAfee is now stressing the threat from smartphones.

The company wrote: “Malware authors will take advantage of phones and tablets, those already trusted controllers, to try to take over IoT devices by password cracking and exploiting vulnerabilities.

“These attacks will not appear suspicious because the network traffic comes from a trusted device. The success rate of attacks will increase, and the attack routes will be difficult to identify.”

Vulnerabilities in smartphone apps and cloud services are also likely to be weak points, as cybercriminals attempt to build up botnets capable of launching the likes of huge DDoS attacks (as seen with Mirai).

And these DDoS (Distributed Denial of Service) attacks could potentially be accompanied with demands for ransoms and the threat of “destruction of property” in some cases. Or at least serious messing with the IoT gadgets in your house…

“These attacks will not appear suspicious because the network traffic comes from a trusted device. The success rate of attacks will increase, and the attack routes will be difficult to identify.”

McAfee Threat Predictions

Threats to your property certainly sounds extreme, but as McAfee notes, digital assistants are another element of the smart home under threat from exploitation. The danger here is more sophisticated IoT malware will find its way onto your network and be able to exploit voice-controlled assistants, with eventual scenarios envisaged such as cybercriminals opening your smart locks and doors.

As McAfee puts it: “Soon we may hear infected IoT devices themselves exclaiming: ‘Assistant! Open the back door!’”

The firm has some advice for helping to secure your smart home, and that includes making sure you use some form of security software on your smartphone.

It’s also a good idea to keep your IoT gadgets on a separate network away from your main home network which hooks up all your PCs, tablets and phones. You can create a guest network to this end, which is something we discuss in our article on six ways to secure your home Wi-Fi.

Also do make sure that any routers or IoT devices you own don’t use the factory default username and password.