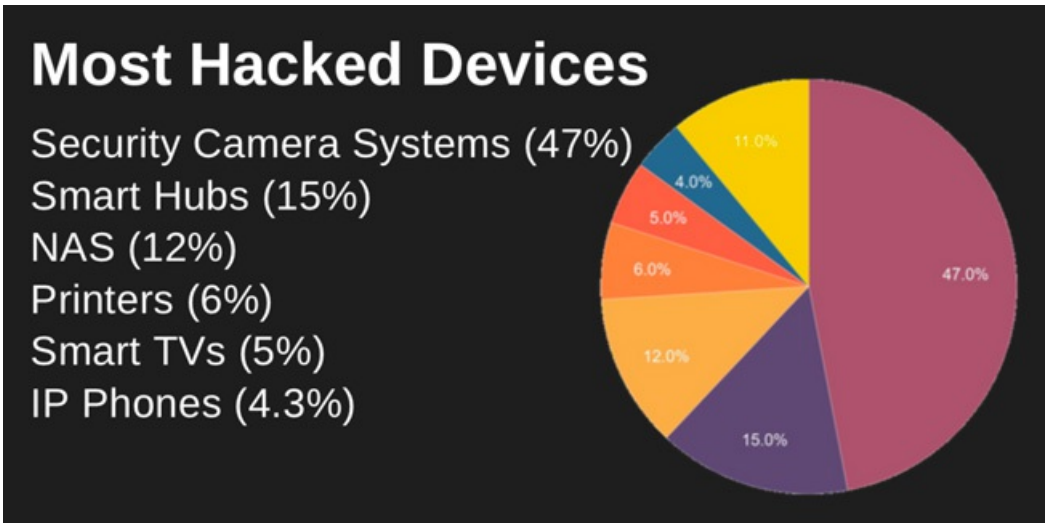
IP-камеры - самые атакуемые IoT-устройства

Интернет вещей (IoT) уже стал частью повседневной жизни людей. По некоторым данным, в домохозяйствах Европы насчитывается в среднем четырнадцать устройств, подключенных к Глобальной сети, а в США аналогичный показатель достигает семнадцати. Хотя перечень техники с сетевыми возможностями очень широк и включает в себя самые разнообразные девайсы - от смартфонов и компьютеров до смарт-телевизоров, "умных" счетчиков и кухонных приборов, некоторые устройства чаще других подвергаются взломам. Исследование ИБ-компании SAM Seamless Network показало, что почти половина всех атак на IoT-устройства (если точнее - 47 процентов) приходится на домашние камеры и системы видеонаблюдения.



Производители дешевых IP-камер, как правило, не особенно заботятся об их защите. Нередко в этих недорогих устройствах, имеющих схожие спецификации, встречаются аналогичные уязвимости, что еще больше облегчает задачу хакеров.

> "Самым серьезным атакам подвергаются IP-камеры. Такое ощущение, что люди не хотят тратить деньги на лучшие современные модели, цена которых может достигать нескольких сотен долларов, предпочитая им недорогие камеры наблюдения. Это очень уязвимые устройства", - заявил порталу ZDNet специалист SAM Seamless Network Омри Маллис (Omri Mallis), комментируя результаты исследования.

Также в тройке самых популярных у хакеров целей - системы управления "умным домом" типа Google Home и Amazon Alexa, и сетевые накопители (NAS). По данным экспертов, на них приходится примерно 15 и 12 процентов атак. Также в список шести наиболее часто взламываемых IoT-устройств попали принтеры (6%), смарт-телевизоры (5%) и IP-телефоны (4,3%).

Кроме того, собранная специалистами статистика показала, что больше всего атак инициируется в Китае и США. Характерно, что в этих же странах IoT-устройства и чаще подвергаются взломам. В среднем подключенное к интернету устройство атакуют пять раз в сутки, чаще всего, в полночь. Скорее всего, хакеры предпочитают это время, поскольку ночью пользователи обычно спят и не могут заметить, если с их устройствами происходит что-то необычное.

В начале мая 2019 года исследователи SAM Seamless Network зарегистрировали всплеск хакерской активности. Преимущественно попытки получить удаленный доступ к IoT-устройствам предпринимались из трех стран - Китая, США и Ирана. 50 процентов из них были атаками бот-сетей. Также исследователи недавно обнаружили новые подвиды опасного вредоносного ПО Mylobot, отключающего антивирусную защиту Windows Defender. По данным SAM Seamless Network, от него пострадали компьютеры под управлением Windows более чем в 170 странах мира.