New online menaces: from spamming fridges to hijackers

February 27 2014, by David Williams

A visitor speaks on his phone in Barcelona on February 25, 2014, on the second day of the 2013 Mobile World Congress

It has to be annoying when your fridge sends spam without your knowledge, but how would you feel if a hacker with a smartphone disabled your car brakes or even remotely hijacked your plane?

Those security-risk scenarios may not be as far-fetched as you think.

Indeed, a fridge has already been caught sending spam.

Security provider Thinkpoint Inc. said last month it had uncovered more than 750,000 malicious emails from more than 100,000 everyday consumer gadgets such as home-networking routers, multi-media centres, televisions and at least one refrigerator.

Just as hackers can take over personal computers, creating robot-like "botnets" to send spam or other emails, now they are compromising Internet-connected objects, or "thingbots' for the same ends.

"Many of these devices are poorly protected at best and consumers have virtually no way to detect or fix infections when they do occur," said David Knight, general manager of Proofpoint's information security division.

Rik Ferguson, vice president in charge of security research for Japan-headquartered Trend Micro, said the most common mobile security threats now were viruses designed to make your smartphone send a premium-cost text message or even make a premium-cost call without your knowledge.

Next on the list is spyware, which collects personal information like an address book for malicious ends such as fraud or spam, extending in rare cases to taking video images or sound from an infected device.

But a new, potentially more ominous threat is emerging as more and more everyday objects are connected online and to smartphones, a phenomenon known as the "Internet of Things".

"Things like connected cars bring the risk of physical damage to persons and property in an attack," Ferguson said in the run-up to the February 24-27 World Mobile Congress in Barcelona, Spain.

Hacking a car by SMS

"If you can get in through the entertainment system for example, and work your way through the rest of the car if it has not been adequately secured and disable the brakes, then you are going to cause all kinds of damage."

It has to be annoying when your fridge sends spam without your knowledge, but how would you feel if a hacker with a smartphone disabled your car brakes or even remotely hijacked your plane?

Equally, a hacker could target a traffic control system, he said.

Last year, a security consultant claimed he could even hijack a passenger plane using a smartphone Android application, Ferguson noted.

The US Federal Aviation Administration manufacturer quickly denied such a vulnerability actually existed.

Even if such spectacular attacks are not an immediate threat, our vulnerability is growing as the Internet spreads its reach yet deeper into our lives, said Vicente Diaz, senior malware analyst at online security group Kaspersky Lab.

More devices mean more opportunities for infiltration, he said.

"That could lead to cross-device infections, but more worrisome is the potential lack of security software and security updates in such devices," he said.

Security researchers had already demonstrated, for example, that a car could be hacked and used remotely just by sending an SMS text message, he said.

Consumers were sometimes responsible for unwittingly increasing their risks, Diaz warned.

Many people seemed to be happy to trade their privacy for free services, for example allowing free email or messaging applications access to personal data, he said.

Just using a smartphone application can leak reams of personal information if the device has already been compromised, Diaz said.

The Guardian newspaper last month published documents it said were from US intelligence leaker Edward Snowden indicating that US and

British spies had been developing ways to use data from smartphone apps such as the smash-hit game Angry Birds.

"Apps such as Angry Birds ask for many permissions, geolocation being an example for some versions. This data is transmitted back home, and is undoubtably juicy for any mass-surveillance operation," Diaz said.

It has to be annoying when your fridge sends spam without your knowledge, but how would you feel if a hacker with a smartphone disabled your car brakes or even remotely hijacked your plane?

Finland-based Rovio, the developer of Angry Birds, has stressed that it does not share data, collaborate or collude with any government spy agencies.

"When talking about privacy, having more devices connected to the Internet sending information of ourselves does not sound like great

news," Diaz warned.

"So if you are a user worried about your privacy, be careful in what you consciously share, what permissions your apps are requesting and what technologies better fit your needs."