FROM THE CITIES TO THE GAMERS, EVERYONE'S NOW A TARGET

DDoS and other security attacks are spreading. Even online gamers are hiring hackers to give them advantages, Michael Wheeler of NTT tells Alan Burkitt-Gray. And the internet of things will just expand the threat

Michael Wheeler, head of global IP network business, NTT

Big cities being hit by ransomware attacks has become almost routine. In May, the city of Baltimore was hit, leaving citizens unable to pay utility bills, taxes and fines. Criminals had demanded $114,000 in bitcoin.

Last week the city council in Riviera Beach, Florida, agreed to pay even more, $592,000 – again in untraceable bitcoin –to whoever had locked down its computer systems.

It's not a game – it's serious and could have life-threatening consequences – but, according to Michael Wheeler, head of NTT's global IP network business, fanatical computer gamers are now arming themselves with such weapons.

They are, says Wheeler, ordering distributed denial of service (DDoS) attacks online in order to block their opponents' IP addresses during particularly furious competitions.

"Generally speaking they will leverage DDoS for hire, paying by bitcoin for 20 minutes," he tells me. "Gamers aren't scary, but there are still costs involved. They are paying someone else to do it." It's a sign of how the idea of computer attacks is spreading, and even apparently harmless gamers are funding this shadowy industry.

Who is generally responsible for attacks such as that in Baltimore in May? Wheeler can't say: "Organised crime or nation-state actors," he suggests.

Wheeler is a member of the ITW Global Leaders' Forum (GLF), and its working group on network security "has been identifying how we can collaborate more than we were already. Security does not have a one-size-fits-all solution. Last year we launched a platform so that carriers can share experiences both post-mortem and in real time. Anything like that can give us a critical mass of work to do."

"The industry sees value in the discussions," says Wheeler. "Companies apply the resources that they have available, and security is a challenge to all of the industry. We need as much coordination and collaboration as we can. The hacker community and such people come up with new tactics."

But what is their motivation? "Generally there are two reasons," says Wheeler. One is to extract money – as we saw in Baltimore and Riviera Beach. The other is "claims of social injustice: the Arab spring and what's going on in Hong Kong at the moment tend to create motives for people to be zealous. And there's always an element of social engineering."

> *"The platform from the GLF is an additional solution. Companies can share what they learn and this is helpful for the industry"*

Gamers seem to be a fairly recent arrival on the scene, paying for someone to mount DDoS attacks against certain IP addresses to give them advantages in an online game. "These are small-scale DDoS attacks, much less significant," he notes. "But the point is there are tools and different approaches all over the place," and they are important for "anyone running a network".

That's why "the platform from the GLF is an additional solution", he adds. "Companies can share what they learn and this is helpful for the industry. The network operators are trying to keep the network available for everyone."

Network attacks are global, says Wheeler, but the level of infrastructure means they are commonest in Asia, Europe and North America. "In certain parts of the world it's not as big a problem yet. It does happen in countries such as Brazil and South Africa, and for the rest it's a question of when, not if."

Meanwhile the internet of things (IoT) is spreading what he calls "dumb devices" around the networks "and those devices can get marshalled" to be used for DDoS attacks. "This affects not just the telecoms industry but the whole tech industry. I don't think IoT is going to slow down or stop. It's going to make it a bigger challenge for us all over time."

The threat extends from industrial IoT devices to thermostats and doorbells in your home. "These devices have IP addresses and they don't recognise software upgrades. They can be forgotten at the business level and the home level." Attackers can ping them to see if they're online – not necessarily for an immediate attack, "as it doesn't change in two months or even two years".

Attacks have already taken place: a device is taken control of and then used to attack another target, such as a bank, via a DDoS attack. There are billions of devices and the internet is now a tool for whoever's controlling them – that makes it difficult to contend with." But Wheeler and his colleagues in the GLF are working hard on it.