Cyber Threats – Bad Rabbit

Malware is everywhere and often sits within an organisations' network undetected but gives its perpetrators the means to access your organisations' data causing security professionals a serious challenge due to its "lay low" nature. We have already seen two large-scale ransomware attacks this year; we are talking about the infamous WannaCry and ExPetr (also known as Petya and NotPetya). It seems that a third attack is on the rise: The new malware is called Bad Rabbit — at least, that's the name indicated by the darknet website linked in the ransom note.

What is known now is that Bad Rabbit ransomware has infected several big Russian media outlets, with Interfax news agency and Fontanka.ru among the confirmed victims of the malware. Odessa International Airport has reported on a cyber-attack on its information system, though whether it's the same attack is not yet clear.

Tips to Raise Your Defences

The Bad Rabbit outbreak appears to have got its start via files on hacked Russian media websites, using the popular guise of pretending to be an Adobe Flash installer. It is a drive-by attack: Victims download a fake Adobe Flash installer from infected websites and manually launch the .exe file, thus infecting themselves.

- Ditch Flash altogether. Fake flash installers and updates only work as a social engineering tactic if you use or want Flash. By removing Flash entirely, you not only protect yourself from Flash zero-day holes, but also eliminate the temptation to download fake updates

- Patch promptly. Outbreaks such as NotPetya and WannaCry exploited a vulnerability for which patches were already available. Don't lag once patches are available for known security holes – the crooks will be only too happy to take advantage

- Remember your backups. Make them regularly, and keep a recent backup both offline and offsite, so you can access it even if your workplace ends up off limits due to fire, flood or some other cause not related to malware

- Don't make users into administrators. When you want to perform administrative tasks, promote yourself to an administrator account, and relinquish those privileges as soon as you can. Network-aware malware like Bad Rabbit can spread without even needing to guess passwords if you already have administrator-level access to other computers on the network

Get in touch to find out how the HR Solutions Team can help your business.

HR Solutions Team
info@hrsolutionsteam.co.uk
Telephone: 01284 848230
www.hrsolutionsteam.co.uk

Sources: Meena Martin, Naked Security, Kaspersky