Aus dem Blickwinkel der Sicherheitsexperten:

MÄCHTIGE HACKERWERKZEUGE

HACKING 4.0 PER USB-STICK „BASH BUNNY“

From the security expert viewpoint:

POWERFUL HACKING TOOLS

HACKING 4.0 BY “BASH BUNNY” USB FLASH DRIVE

Unsere Geräte werden immer kleiner, Mobiltelefone passen schon lange in die Hosentasche, PCs kommen im Taschenbuchformat, auch Computerchips sind bereits kleiner als ein Reiskorn. Die Miniaturisierung von technischen Komponenten schreitet schnell und stetig voran.

Ganze Computersysteme passen mittlerweile auch auf einen praktischen USB-Stick. Vor Kurzem wurde testweise ein winziger Computer entwickelt, der gerade mal 0.3mm misst. Auch Roboter werden immer winziger und sind mitunter kaum noch größer als Geldmünzen.

Miniaturgeräte sind nicht nur praktisch, bequem und vor allem portabel, sondern können am Ende auch ganz schön gefährlich sein. Das Zusammenspiel mit Plug&Play-Systemen verschärft die Bedrohungslage weiter. Einfach die neue Hardware über den USB-Port anstecken und schon sind die Geräte einsatzbereit oder die Daten können via USB-Stick abgerufen werden. Das ist für Anwender ein großer Vorteil, da eine komplexe Installation entfällt. Für die Sicherheit birgt es enorme Risiken. Denn mithilfe eines USB-Sticks können viele Sicherheitsvorkehrungen umgangen oder gar komplett ausgeschaltet werden.

Täuschen und tarnen

Die Bedrohung heißt „Bash Bunny“: Hinter dem IT-Gerät in Form eines USB-Sticks steckt ein kleiner, portabler und vor allem leistungsfähiger Linuxcomputer mit einem USB-Interface. Mit ihm können Angriffe auf Windows-, Mac-, Linux-, Unix- und Android-systeme durchgeführt werden.

Von außen sieht der Minicomputer wie ein gewöhnlicher USB-Stick aus. Bei näherer Betrachtung können damit sehr effiziente, schädliche Attacken erfolgen, um Zugang zu sensiblen Unternehmensdaten zu erhalten. Bash Bunny ist dank Quad-Core-CPU sehr leistungsfähig. Der kleine USB-Stick kann all das, was auch reguläre Linuxcomputer können, wie Python Scripts oder gängige Linuxbefehle ausführen. Beim Anstecken des unscheinbaren USB-Sticks gibt Bash Bunny vor, ein vertrauenswürdiges Medien- oder Netzwerkgerät zu sein, wie zum Beispiel ein Keyboard. Dafür imitiert es sogar Tastenanschläge. Die Absicht hinter einem Angriff mit Bash Bunny ist, möglichst viele Daten zu sammeln und vor allem Passwörter und Zugangsdaten zu stehlen und auf dem integrierten Flashspeicher zu sichern. So kann dann aus der Ferne der Zugriff auf den PC stattfinden, um Backdoors zu öffnen, Daten herunterzuladen und Programme auszuführen.

FAZIT:

Es bedarf nicht immer großer Rechenleistungen oder Botnetze, um Attacken auf Unternehmen durchzuführen. Die Bedrohung kann auch in Form eines kleinen, unscheinbaren USB-Sticks daherkommen.

Our devices are getting ever smaller, mobile phones have fitted in our pockets for ages, PCs come pocket-sized and even computer chips are already smaller than a grain of rice. The miniaturisation of technical components is rapid and relentless.

Entire computer systems now also fit comfortably onto a practical USB flash drive. Recently, a minute computer measuring just 0.3 mm was developed for test purposes. Robots also keep getting tinier and are now barely larger than coins.

Miniature devices are not only practical, convenient and, most of all, portable, they can also be really rather dangerous in the end. The threat level is further intensified by the interaction of plug-and-play systems. You simply plug new hardware into the USB port and the devices are ready to use, or you can retrieve data via a USB flash drive. This is a big advantage for users as they do not have to worry about complex installation, but the process is fraught with security risks. This is because a USB flash drive can be used to bypass many security measures or even completely disable them.

Deceive and disguise

The threat is called “Bash Bunny”: hidden behind the IT device in the form of a USB flash drive is a small, portable and most importantly powerful Linux computer with a USB interface. It can be used to carry out attacks on Windows, Mac, Linux, Unix and Android systems.

The minicomputer looks like a conventional USB flash drive from the outside. On closer examination, you can see that it can be used to carry out extremely efficient and damaging attacks, to gain access to sensitive corporate data. Thanks to its quad-core CPU, Bash Bunny is extremely powerful. The small USB flash drive can do everything that normal Linux computers can, such as Python scripts or common Linux commands. When the inconspicuous USB flash drive is plugged in, Bash Bunny pretends to be a trustworthy media or network device, such as a keyboard. It even imitates keystrokes. The purpose of a Bash Bunny attack is to collect as much data as possible, and most importantly, to steal passwords and access data and save them to the integrated flash memory. The PC can then be accessed remotely, to open backdoors, download data and run programs.

SUMMARY:

You do not always need processing power or botnets to launch attacks on a company. The threat can also come from a small and inconspicuous USB flash drive.

written by Nicole Jungmann