BadUSB: Wenn USB-Geräte böse werden

Wer die Firmware eines USB-Sticks kontrolliert, kann den zu einem perfekten Trojaner umfunktionieren. Deutsche Forscher zeigen, dass das komplett via Software möglich ist und sich damit ganz neue Infektions-Szenarien eröffnen.

Ein infizierter Rechner genügt, um all Ihre USB-Sticks zu infizieren – oder den USB-Drucker und die Web-Cam. Und das auf eine Art und Weise, die weder zu entdecken noch rückgängig zu machen ist. Das klingt nicht nur unheimlich – es ist es auch und erinnert ein wenig an den angeblichen Super-Trojaner BadBIOS, der letztes Jahr Aufsehen erregte. Die konkreten Details will Karsten Nohl von den SRLabs in seinem Vortrag BadUSB - On accessories that turn evil auf der Black Hat präsentieren; gegenüber heise Security erklärte er jedoch vorab schon den technischen Hintergrund.
USB-Trojaner sind eigentlich ein alter Hut: Sie sehen aus wie Speicher-Sticks, enthalten aber in Wirklichkeit einen kleinen Computer, der sich als Tastatur am System anmeldet und es dann durch passende Eingaben kapert. Bereits 2011 warnte Adrian Crenshaw vor Malicious USB Devices; der Rubber Ducky macht sowas zum Kinderspiel. Doch die Forscher rund um Karsten Nohl präsentieren jetzt etwas ganz anderes: Sie können einen ganz normalen USB-Speicher-Stick in ein Trojanisches Pferd verwandeln – und zwar ganz ohne Lötkolben ganz allein via Software.

Firmware-Hacking

Die Kommunikation zwischen PC und USB-Sticks setzt auf das altbewährte SCSI-Protokoll auf. Dabei implementieren die Controller-Chips der Sticks mehr oder weniger SCSI-konform zusätzliche Hersteller-spezifische Erweiterungen. Über die kann Software auf dem PC dann etwa die Firmware des Sticks auslesen und auch einen neue, etwas modifizierte Firmware schreiben. Sicherheitsfunktionen, die dies irgendwie absichern würden, gibt es in der Regel nicht.
Laut Nohl kommen bei USB-Speicher-Sticks fast nur Controller von drei Herstellern zum Einsatz; sehr weit verbreitet sind die von Phison. Wie Nohl im Rahmen seiner Forschung herausfand, hatten bereits andere deren proprietäre SCSI-Befehle analysiert. Nohls Team gelang es, nach einer Analyse der Firmware auf diesem Weg einen ganz normalen USB-Speicherstick umzuprogrammieren. Danach meldet der sich als USB-Tastatur an und infiziert dann jedes Windows-System, mit dem er zukünftig in Kontakt kommt – das dann wiederum weitere Sticks infizieren könnte – ein USB-Virus ist geboren.

Der USB-Virus

Wobei dessen Verbreitung keineswegs auf Windows beschränkt ist, sondern mit Linux analog funktionieren würde. Der USB-Stick könnte sogar sein Host-System anhand der Eigenheiten der USB-Kommunikation erkennen und die passende Infektions-Routine auswählen. Um dann wiederum weitere Sticks zu infizieren, benötigt der Schadcode zwar Systemrechte, doch die lassen sich in der Regel ohne allzu großen Aufwand beschaffen – insbesondere, wenn man bereits "an der Tastatur sitzt". Auch andere USB-Gerätschaften können zum Ziel werden; Nohl nennt etwa Webcams oder Festplatten als mögliche BadUSB-Angriffsziele.
Sich gegen solche BadUSB-Geräte zu schützen, dürfte sich als sehr schwer erweisen. Denn das System, das auf den Stick zugreift, bekommt nur noch das zu sehen, was ihm die manipulierte Firmware zeigen will. Antiviren-Software ist damit quasi komplett außen vor. Auch ein Whitelisting-Ansatz dürfte sich als schwierig erweisen. Es kann gut sein, dass Netzwerk-Admins in Hochsicherheitsbereichen nach Nohls Vortrag wieder zur Heißklebe-Pistole greifen werden, um USB-Zugänge nachhaltig zu sichern.
(ju)

Erschienen am 31.07.2014 um 19:09 Uhr auf heise.de

Permalink: http://heise.de/-2281098