TRUST IN GERMAN SICHERHEIT

G DATA

Whitepaper

G DATA USB Keyboard Guard

G DATA CyberDefense AG | 02/2015

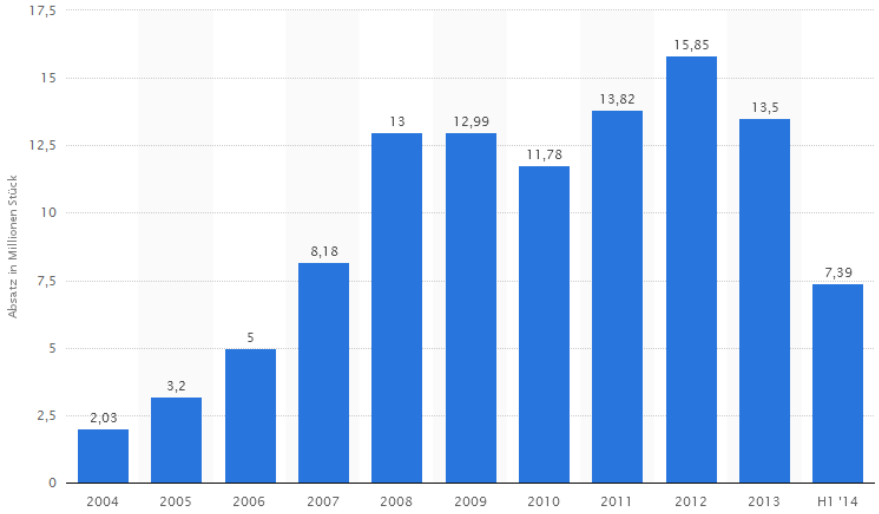
INHALT

MOTIVATION

Bedrohungen im Internet gehen heutzutage von hochprofessionellen, untereinander vernetzten und organisierten Cyberkriminellen aus. Deren Ziele liegen schon lange nicht mehr darin, Ruhm in Hackerkreisen zu erlangen, sondern in möglichst großem finanziellem Gewinn. Fast alle Angriffsmethoden zielen deshalb auf das Erlangen von verkäuflichen Informationen ab: Zugangs- und Kreditkartendaten, vertrauliche oder sicherheitskritische Unternehmensdaten, Staatsgeheimnisse, Botnet-Kapazitäten. Auf diese Weise ist ein Schwarzmarkt entstanden, der jedes Jahr Umsätze in Millionenhöhe tätigt. Kein Wunder also, dass jeder potenziell lukrative Angriffsvektor abgeklopft wird und früher oder später als Einfallstor für Gefährdungen in Erscheinung tritt. Ereignisse des zweiten Halbjahrs 2014 haben gezeigt: USB-Geräte sind die nächste große Bedrohungsquelle.

Sicherheitsforscher der Berliner Security Research Labs haben auf der „BlackHat“-Sicherheitskonferenz im August 2014 eindrucksvoll bewiesen, dass vor allem die allseits beliebten USB-Sticks ein massives Gefährdungspotenzial besitzen. Eine Manipulation von deren Firmware ermöglicht Hackern einen offenen Zugang zu sicherheitskritischen Systemfunktionen. Da aber nicht auf dem Stick gespeicherte Daten, sondern der USB-Controller und dessen Firmware Ziel der Manipulation sind, greifen herkömmliche Sicherheitslösungen nicht. Sobald ein manipulierter „BadUSB“-Stick mit einem PC verbunden wird, ist es zu spät: Der Effekt ist derselbe, als ob ein Hacker unmittelbar an der Tastatur des Computers Platz genommen hätte und kurze Zeit später die Kontrolle übernehmen kann. [1]

Wie groß das Potenzial dieser Bedrohung ist, verdeutlichen die Verkaufszahlen von USB-Sticks in Deutschland: In den vergangenen Jahren ist der Absatz auf bis zu 15,85 Millionen Stück im Jahr (2012) angewachsen, in der ersten Jahreshälfte 2014 waren es bereits 7,39 Millionen Stück. Insgesamt sind in Deutschland ca. 100 Millionen USB-Sticks im Umlauf [2], dazu kommen ungezählte Mobiltelefone, Webcams oder Tastaturen, die ebenfalls mit einer USB-Schnittstelle und Controller ausgestattet sind. Nicht zuletzt trägt die allgemeine Wahrnehmung von USB-Geräten als „sicher“ und ein dementsprechend sorgloser Umgang beim Austausch von Daten zur Gefährdung bei.



Die Zahl verkaufter USB-Sticks in Deutschland liegt stabil auf hohem Niveau (Quelle: Statista).

Folgerichtig kursieren bereits jetzt im Internet Hacker-Bausätze, mit dessen „BadUSB“-Modul USB-Sticks manipuliert werden können. Alternativ können fertige USB-Sticks wie „Rubber Ducky“ einzeln oder mit

Preisnachlass in größerer Stückzahl geordert werden. Die Hacker-Szene ist also längst dabei, den neuen Angriffsvektor in großem Stil für sich nutzbar zu machen. [3]

SO FUNKTIONIERT EIN ANGRIFF PER „BADUSB“-STICK

Das Prinzip hinter der Angriffsmethode durch einen „BadUSB“-Stick ist schnell erklärt: Die Firmware des Controllers - Teil jedes USB-Geräts -, wird dahingehend manipuliert, dass sich der Stick beim Anschließen an einen Computer nicht nur als Speicherlaufwerk, sondern ebenso als Tastatur beim System anmeldet. Jegliche Eingaben dieser vorgetäuschten Tastatur werden ohne Prüfung angenommen und umgesetzt, eben so, als ob der Anwender auf einer echten Tastatur tippen würde. Anfällig für diese Täuschung sind alle Arten von Computern mit Unterstützung von USB-Tastaturen. [4]

Ist die Anmeldung vollzogen, schickt ein programmiertes Script Tastaturbefehle an das System. Im Fall eines Windows-PCs könnte das zum Beispiel zunächst das Tastenkürzel Windows + R sein, um das Fenster für die Eingabe von Befehlen zu öffnen. Als nächstes erfolgt per Übertragung eines weiteren Textbefehls der Start der Windows-„Powershell“-Umgebung. Darin folgt ein weiterer Textbefehl des USB-Sticks zum Herunterladen und Starten eines Backdoor-Programms aus dem Internet. [5]

Kann der durch das Script angestoßene Prozess abgeschlossen werden, übernimmt der Angreifer per Fernsteuerung über das Backdoor-Programm die umfassende Kontrolle des Systems. Dass diese Angriffsmethode funktioniert, haben Karsten Nohl, Jakob Lell und Henryk Plötz von den Security Research Labs Berlin Journalisten des WDR im Rahmen eines Beitrags des Magazins „Monitor“ demonstriert. [6] Im beschriebenen Beispiel könnte eine herkömmliche Sicherheitslösung frühestens dann eingreifen, wenn das nachgeladene Programm eine bekannte Malware-Signatur hat. Besteht der Angriff aus einer Folge jeder für sich harmloser Tastaturbefehle, bleibt jede Abwehr wirkungslos. [5]

Die zugrundeliegende Scriptsprache ist so einfach zu erlernen, dass selbst ungeübte Programmierer in kurzer Zeit eigene Angriffsmethoden entwickeln können.

```
REM Kommentare werden wie zum Beispiel in BASIC durch REM gekennzeichnet
REM Zuerst gibt es eine kleine Pause, angegeben in Millisekunden * 10
DELAY 3000
REM GUI emuliert die Windows-Taste, hier wird also virtuell Windows-r gedrückt und damit das run-Menü
aufgerufen
GUI R
REM Jetzt braucht der Rechner etwas Zeit, um den Befehl auszuführen - gönnen wir ihm also eine Pause
DELAY 500
REM STRING gibt einen String aus, indem nacheinander die angegebenen Tasten virtuell gedrückt werden -
hier wird also notepad eingegeben
STRING notepad
REM Wieder etwas Zeit für den Rechner
DELAY 500
REM ENTER emuliert natürlich den Druck auf die ENTER-Taste
ENTER
REM Und wieder eine Pause, damit Notepad Zeit zum Starten hat
DELAY 750
REM Hier ist sie nun - die Ausgabe (oder besser Eingabe) von "Hello World!"
STRING Hello World!
REM Und zum Abschluss noch einmal ENTER drücken
ENTER
```

Beispiel für ein einfaches „BadUSB“-Script für den Start des Windows-Programms „Notepad“ und die Ausgabe des Textes „Hello World“ (Quelle: [5])

Neben einem einfachen Angriff auf einen einzelnen Rechner sind komplexe Verbreitungsmechanismen denkbar: Einmal auf dem angegriffenen System resident könnte eine nachgeladene Malware alle weiteren mit dem Computer verbundenen USB-Sticks manipulieren und damit für eine schnellen Verbreitung sorgen.

Die Sorglosigkeit, mit der Daten derzeit per USB-Stick unter Kollegen, Freunden oder in der Familie ausgetauscht werden, eröffnet hier ungeahnte Sicherheitsprobleme. [4]

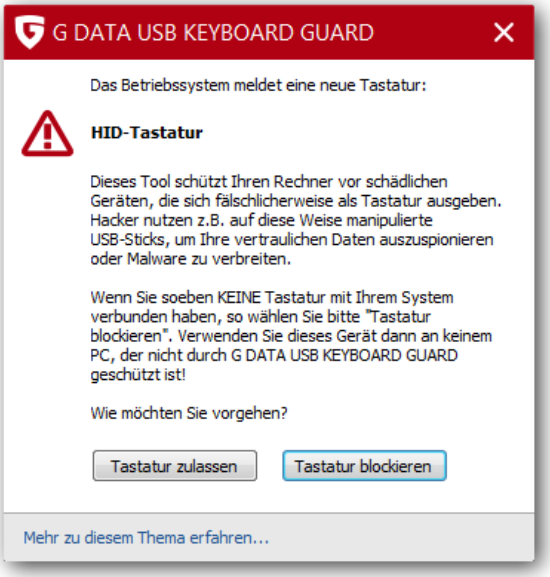
Die Frage danach, wie der „BadUSB“-Stick in den Anschluss des angegriffenen Computers gelangt, lässt sich mit dem Begriff „Social Engineering“ beantworten: In der Regel genügt es, dessen Nutzer den manipulierten USB-Stick „finden“ zu lassen. Aus Neugier werden die meisten Menschen den Stick früher oder später in den Anschluss Ihres Computers stecken und sich dabei auf ihre – in dem Fall wirkungslose - Sicherheitslösung zum Schutz vor Malware verlassen. Sofern physischer Zugang besteht, kann der Angreifer seinen USB-Stick in einem unbeobachteten Moment mit dem ungeschützten PC verbinden: Ein Kundenberater der Bank, der im Beratungsgespräch kurz seinen Arbeitsplatz verlässt, vergisst mit großer Wahrscheinlichkeit die Sperrung seines Computers. Und natürlich sind Laptops von Geschäftsreisenden im Zug oder auf Messen ein geeignetes Ziel für diese Angriffsmethode. [5]

Nohl und sein Team zeigten im Herbst während der Sicherheitskonferenz PacSec, dass weitere Angriffsmethoden denkbar, aber schwieriger zu realisieren und somit weniger wahrscheinlich sind. So gelang es zum Beispiel, ein Smartphone gegenüber einem Laptop als USB-Netzwerkadapter auszugeben und dessen Netzwerkverkehr per DHCP über das Telefon umzuleiten. Insgesamt sind nach den Forschungsergebnissen der Security Research Labs etwa die Hälfte aller verkauften USB-Geräte anfällig für derartige Manipulationen. Ausschlaggebend für die Manipulierbarkeit sind der Typ des verbauten Controllerchips, die Programmierbarkeit von außen über den USB-Anschluss und das Vorhandensein von Flash-Speicher zum Ablegen des veränderten Codes. [7]

SO SCHÜTZT G DATA USB KEYBOARD GUARD VOR „BADUSB“-STICKS

Bei der Erkennung von manipulierten USB-Geräten existiert eine prinzipielle Schwierigkeit: Da es keinen Signierungs- oder Zertifizierungsstandard für USB-Firmware gibt, existiert keine Möglichkeit, eine echte von einer gefälschten Firmware zu unterscheiden. Manipulationen lassen sich deshalb nicht ohne intensive Analyse feststellen.

G DATA USB KEYBOARD GUARD erkennt einen „BadUSB“-Stick stattdessen anhand seines unverwechselbaren Merkmals: der Anmeldung als Tastatur am System. Das Programm meldet dem Anwender, wenn eine neue Tastatur mit dem Computer verbunden wird und ermöglicht es, diese Tastatur freizugeben oder zu sperren.



Diese Meldung informiert den Anwender über die Anmeldung einer neuen Tastatur am System.

Die Erkennung eines manipulierten USB-Sticks fällt so auf natürliche Weise dem Anwender zu, der weiß, ob er gerade eine Tastatur an den Computer angeschlossen hat oder nicht. Ein Mausklick genügt daraufhin, um eine echte Tastatur für Eingaben zuzulassen oder einen manipulierten USB-Stick für gefälschte Tastatureingaben zu blockieren und als Angriffswerkzeug zu identifizieren. Das funktioniert sogar dann, wenn das Skript auf dem „BadUSB“-Stick eine Verzögerung vorsieht und erst nach einer Stunde aktiv wird. In dem Fall wird dem Anwender umso deutlicher bewusst, dass „etwas faul sein“ muss und er die vorgeblich erkannte Tastatur blockieren sollte. Einmal vom Anwender freigegebene USB-Tastaturen werden auf einer Whitelist gespeichert, sodass das Gerät nicht bei jedem Einsteckvorgang bestätigt werden muss.

Damit schützt G DATA USB KEYBOARD GUARD den Anwender vor der wichtigsten und am weitesten verbreiteten Angriffsmethode über manipulierte USB-Sticks.

LITERATURVERZEICHNIS

1. USB-Viren im Anmarsch?
   https://blog.gdata.de/artikel/usb-viren-im-anmarsch
2. Absatz von USB-Sticks auf dem Konsumentenmarkt in Deutschland von 2004 bis Halbjahr 2014
   http://de.statista.com/statistik/daten/studie/151613/umfrage/absatz-von-usb-sticks-seit-2004-in-deutschland/
3. BadUSB-Tools kursieren im Netz, Angriffs-Stick im Eigenbau
   http://www.heise.de/security/meldung/BadUSB-Tools-kursieren-im-Netz-Angriffs-Stick-im-Eigenbau-2411135.html
4. Patrick Beuth: Jedes USB-Gerät kann zur Waffe werden
   http://www.zeit.de/digital/datenschutz/2014-07/usb-controller-chip-angriff-srlabs
5. Carsten Eilers: Sicherheitsrisiko USB: Angriffe über den Serial Bus
   https://entwickler.de/online/security/sicherheitsrisiko-usb-angriffe-ueber-den-serial-bus-114998.html
6. MONITOR-Pressemeldung: Unkontrollierbare Sicherheitslücke durch USB-Sticks - Experten sprechen von einer „Katastrophe für den Datenschutz“
   http://www1.wdr.de/daserste/monitor/extras/monitorpresse-usb100.html
7. Viele USB-Geräte verwundbar für BadUSB-Angriffe
   http://www.heise.de/security/meldung/Viele-USB-Geraete-verwundbar-fuer-BadUSB-Angriffe-2454715.html