TRUST IN
GERMAN
SICHERHEIT

G DATA
WHITEPAPER

G DATA USB KEYBOARD GUARD

CONTENTS

TRUST IN GERMAN SICHERHEIT

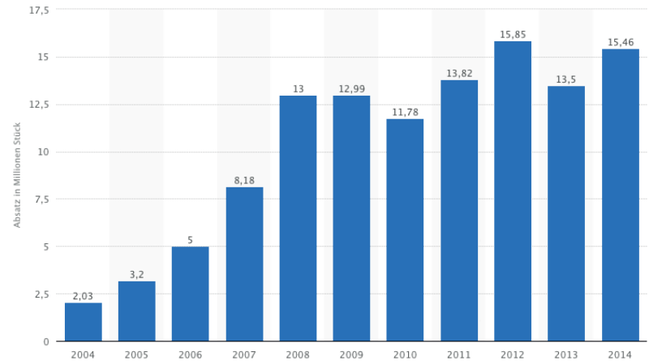
MOTIVATION

These days threats on the Internet originate from highly professional, interlinked, organized cyber criminals. Their aim is no longer to gain kudos among groups of hackers, but to acquire as much financial profit as possible. For this reason, almost every attack method is aimed at acquiring marketable information: access and credit card data, company data that is confidential or critical to security, state secrets, and botnet capacities. As a result, a black market has arisen, with an annual turnover in the millions. Hence it is no wonder that every potentially lucrative attack vector is being tried out and sooner or later will feature as a gateway for threats. The results for the second half of 2014 have shown that USB devices are the next major source of threats.

Security researchers at Berlin-based Security Research Labs impressively demonstrated at the BlackHat security conference in August 2014 that USB sticks, being universally popular, offer the biggest threat potential. Manipulating the firmware on these devices gives hackers open access to safety-critical system functions. But because the target of the manipulation is not the data stored on the stick but the USB controller and its firmware, conventional security solutions are not enough. As soon as a manipulated "BadUSB" stick is connected to a computer, it is too late: the effect is the same as if a hacker had sat down at the keyboard of the computer himself and quickly been able to take control of it.[1]

The size of the potential of this threat is clear from the sales figures for USB sticks in Germany. In recent years sales have increased to 15.85 million units per year (2012), with 7.39 million units sold in the first half of 2014 alone. Around 100 million USB sticks are in use in Germany in total,[2] and this is ignoring the numerous mobile phones, webcams and keyboards that also have a USB interface and controller. Not least, the general perception of USB devices as "safe" and the correspondingly carefree way they are used to exchange data is contributing to the threat.

Consequently, hacker kits are now circulating on the Internet containing a "BadUSB" module that can be used to manipulate USB sticks. Alternatively, primed USB sticks such as "Rubber Ducky" can be ordered individually or in large quantities for a price discount. The hacker scene has long been involved in making the new attack vector highly exploitable for their purposes.[3]



The number of USB sticks sold in Germany has stabilized at a high level (source: Statista).

[1] https://blog.gdata.de/artikel/usb-viren-im-anmarsch
[2] http://de.statista.com/statistik/daten/studie/151613/umfrage/absatz-von-usb-sticks-seit-2004-in-deutschland/
[3] http://www.heise.de/security/meldung/BadUSB-Tools-kursieren-im-Netz-Angriffs-Stick-im-Eigenbau-2411135.html

HOW A "BADUSB" STICK ATTACK WORKS

The principle behind the attack method using a "BadUSB" stick is easy to explain: the controller's firmware – part of every USB device – is manipulated so that the stick identifies itself as not just a storage medium when connected to a computer but also as a keyboard on the system. Any input from this supposed keyboard is accepted and implemented without being checked, just as if the user was typing on a genuine keyboard. Every type of computer that supports USB keyboards is susceptible to this deception.[4]

Once the identification is complete, the programmed script sends keyboard commands to the system. In the case of a Windows PC, the keyboard shortcut Windows + R could be used to open the Window for entering commands, for example. Another text command can then be transferred to start the Windows PowerShell environment. This is followed by another text command from the USB stick to download and launch a backdoor program from the Internet.[5]

If the initiated process can be completed by the script, the attacker can remotely take over complete control of the system via the backdoor program. Karsten Nohl, Jakob Lell and Henryk Plötz from Security Research Labs in Berlin demonstrated that this attack method works to WDR journalists in a sequence shown on the programme "Monitor".[6] In the example described, a conventional security solution could only intervene if the program downloaded had a known malware signature. If the attack consists of a sequence of individually innocuous keyboard commands, no form of defence would be effective.[5]

```
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
```

Example of a simple "BadUSB" script for launching the Windows Notepad program and publishing the text "Hello World" [5]

[4]http://www.zeit.de/digital/datenschutz/2014-07/usb-controller-chip-angriff-srlabs
[5]https://entwickler.de/online/security/sicherheitsrisiko-usb-angriffe-ueber-den-serial-bus-114998.html
[6]http://www1.wdr.de/daserste/monitor/extras/monitorpresse-usb100.html

TRUST IN GERMAN SICHERHEIT

The underlying script language is so easy to learn that even inexperienced programmers could develop their own attack methods in a short time.

Besides a straightforward attack on an individual computer, complex distribution mechanisms can be imagined. Once resident on the compromised system, the downloaded malware could manipulate any other USB stick connected to the computer and thus enable fast distribution.

The carefreeness with which data is currently exchanged between colleagues, friends and family by USB stick triggers unimaginable security issues.[4]

The question of how the "BadUSB" stick comes to be connected to the compromised computer is answered with the term "social engineering". Generally, it is sufficient for the user to "find" the manipulated USB stick. The majority of users will insert the stick into the port on their computer sooner or later out of curiosity and in doing so will rely on their – in this case useless – security solution to protect them against malware. Where there is physical access, the attacker can attach his USB stick to an unprotected PC when nobody is looking: a customer advisor in a bank who leaves his workstation briefly during a consultation will forget to lock the computer in all probability. And of course business travellers' laptops on the train or at trade shows are an ideal target for this attack method.[5]

In the autumn, Nohl and his team demonstrated at the PacSec security conference that other attack methods are conceivable but harder to carry out and hence less likely. For example, it was possible to set up a smartphone as a USB network adapter for a laptop and redirect its network traffic via the telephone using DHCP. According to the Security Research Labs research results, around half of all USB devices purchased are susceptible to this type of manipulation. The determining factors for the ability to manipulate the stick are the type of controller chip installed, the ability to program externally via the USB port and the presence of a Flash memory for storing the modified code.[7]

[7]http://www.heise.de/security/meldung/Viele-USB-Geraete-verwundbar-fuer-BadUSB-Angriffe-2454715.html

HOW G DATA USB KEYBOARD GUARD OFFERS PROTECTION AGAINST "BADUSB" STICKS

There is one key difficulty when it comes to detecting manipulated USB devices: as there is no signing or certification standard for USB firmware, there is no possibility of distinguishing genuine from fake firmware. This means that manipulations can only be determined by means of intensive analysis.

Instead, G DATA USB KEYBOARD GUARD detects a "BadUSB" stick by means of its distinctive characteristic – identifying itself to the system as a keyboard. The program informs the user when a new keyboard has been connected to the computer and enables this keyboard to be approved or blocked.

This is a natural way of bringing the detection of a manipulated USB stick to the attention of the user, who will know whether or not a keyboard has actually been connected to the computer. A mouse click is all it takes to approve a genuine keyboard for input or block a manipulated USB stick from making fake keyboard entries and identifying it as an attack tool. This even functions when the script on the "BadUSB" stick has a delay and is not activated for another hour. In this case, it is all the more apparent to the user that something must be wrong and that he needs to block the potential keyboard. Once a USB keyboard has been approved by the user, it is saved to a whitelist so the device does not need to be confirmed each time it is connected.

In this way G DATA USB KEYBOARD GUARD protects the user against the most critical and widespread attack method via manipulated USB sticks.

This message informs the user that a new keyboard has been logged on the system.

TRUST IN GERMAN SICHERHEIT

REFERENCES

1. USB viruses on the increase? (German)
https://blog.gdata.de/artikel/usb-viren-im-anmarsch

2. Sales of USB sticks on the consumer market in Germany from 2004 to the first half of 2014 (German)
http://de.statista.com/statistik/daten/studie/151613/umfrage/absatz-von-usb-sticks-seit-2004-in-deutschland/

3. "BadUSB" tools circulating on the net, self-made attack stick (German)
http://www.heise.de/security/meldung/BadUSB-Tools-kursieren-im-Netz-Angriffs-Stick-im-Eigenbau-2411135.html

4. Patrick Beuth: Any USB stick can become a weapon (German)
http://www.zeit.de/digital/datenschutz/2014-07/usb-controller-chip-angriff-srlabs

5. Carsten Eilers: USB security risk: attacks via the serial bus (German)
https://entwickler.de/online/security/sicherheitsrisiko-usb-angriffe-ueber-den-serial-bus-114998.html

6. MONITOR press release: Uncontrollable security hole via USB sticks – experts talk of a "disaster for data protection" (German)
http://www1.wdr.de/daserste/monitor/extras/monitorpresse-usb100.html

7. Many USB sticks vulnerable to "BadUSB" attacks (German)
http://www.heise.de/security/meldung/Viele-USB-Geraete-verwundbar-fuer-BadUSB-Angriffe-2454715.html

TRUST IN GERMAN SICHERHEIT