ROHDE&SCHWARZ

Make ideas real

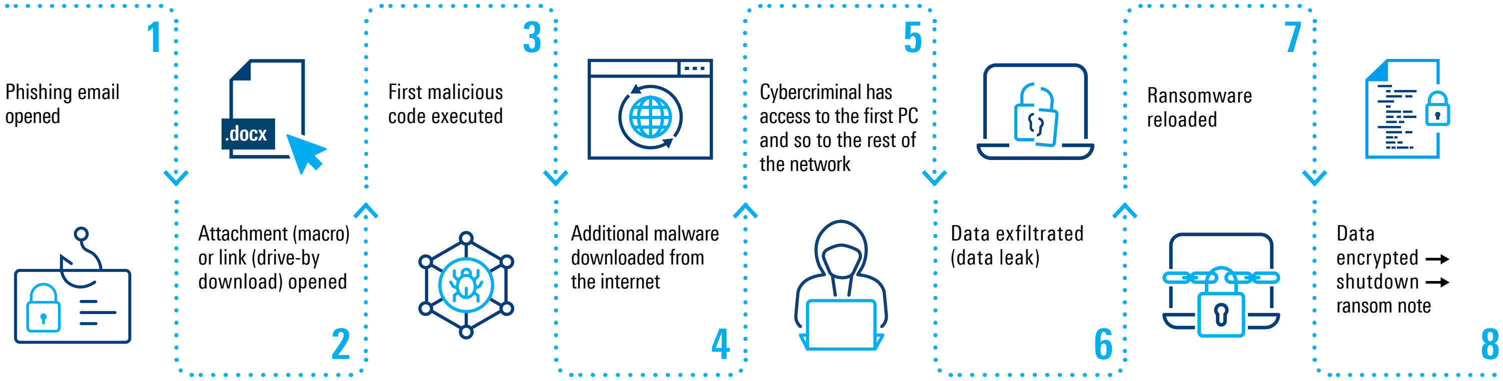
# PROACTIVE PROTECTION AGAINST RANSOMWARE

## WHAT IS RANSOMWARE?

The number of cyberattacks is constantly rising. One of the most common types of attack is the use of malware: malicious software that infiltrates networks. Malware has developed into a kind of toolbox for cybercriminals and the most frequently used malware tool is undoubtedly ransomware — malicious programs that can restrict or prevent access to data and networks, exfiltrate data, and only release these resources again if a ransom is paid. Ransomware encrypts files and even entire computers.

Ransomware has evolved from a fake antivirus product to malware with advanced encryption capabilities, increasingly **targeting enterprises**, but also **critical infrastructures** and the **public sector**. It is often spread via phishing emails, hidden in images or as executable files attached to emails.

## HOW DO RANSOMWARE ATTACKS TYPICALLY UNFOLD?



1 Phishing email opened

2 Attachment (macro) or link (drive-by download) opened

3 First malicious code executed

4 Additional malware downloaded from the internet

5 Cybercriminal has access to the first PC and so to the rest of the network

6 Data exfiltrated (data leak)

7 Ransomware reloaded

8 Data encrypted → shutdown → ransom note

The entry points loaded via macro (e.g. from a Microsoft Office document) or phishing link are just a sort of basic malware. Their main purpose is simply to look different for each attack to ensure they remain undetected by traditional antivirus software. The real threat is downloaded by the malware loader over an encrypted channel: programs that exfiltrate data and passwords before encrypting them.

## HOW DID RANSOMWARE DEVELOP?

Ransomware is becoming a bigger talking point in cybercrime not only on account of the enormous amount of damage it can cause but also because cases of ransomware attacks continue to rise. When compared globally, Germany is victim to more ransomware attacks than most countries. Once again, the **threat posed** by ransomware attacks grew dramatically in 2021. Ransomware also poses the biggest threat in terms of cybercrime tactics according to the German Federal Criminal Police Office. For example, the **Bitkom industry association** determined that losses attributable to ransomware attacks increased by 358 percent between 2019 and the end of 2021. And this trend is expected to continue in the future.

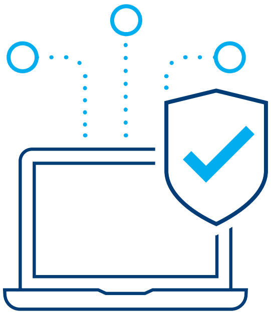
Whereas some time ago attackers encrypted individual computers and demanded a ransom per encrypted PC, today they spy on the affected authority or corporate networks in a targeted manner. During this first phase, the attackers often exfiltrate data (**data leak**) and evaluate each victim. They then adjust their ransom demands for each organization. So-called **double extortion** is now standard practice with ransomware attacks, which involves attackers threatening to expose compromised, sensitive data in addition to encrypting it. This therefore also makes a good backup strategy redundant.

Another alarming trend is **ransomware as a service** (**RaaS**), which means cybercriminals no longer need to have the technical skills to program their own malware. Instead, they can simply pay for a whole range of malicious software. Thus, attackers are finding it increasingly easy to perform complex attacks.

## WHY IS IT IMPORTANT TO ACT NOW?

- Cybercriminals are getting smarter and demanding more money
- Downtime costs are often underestimated
- Data leaks also cause reputational damage, which invariably leads to enormous losses for affected companies
- A backup strategy alone is no longer a sufficient safeguard
- Even if you pay the ransom, there is no guarantee that the cybercriminals will not access the system again or will actually delete/release the stolen data

# WHAT CAN YOU DO?



1. Install security patches on a regular and timely basis, and regularly implement security updates.
2. Device lifecycle management is an integral part of network security. You should not run old and outdated systems with operating systems that are no longer supported, e.g. Windows XP, on networks connected to the internet under any circumstances.
3. Do not open any email attachments or links that come from unknown or suspicious sources.
4. Only download programs from the internet that come from verified sources.
5. Back up your data regularly to external data storage devices.

Nearly all companies and public authorities have a basic level of security. However, this is not enoughto protect them from highly specialized methods of cyberattack. **If you want to ensure full and proactive protection against ransomware attacks, you have to take additional measures.**

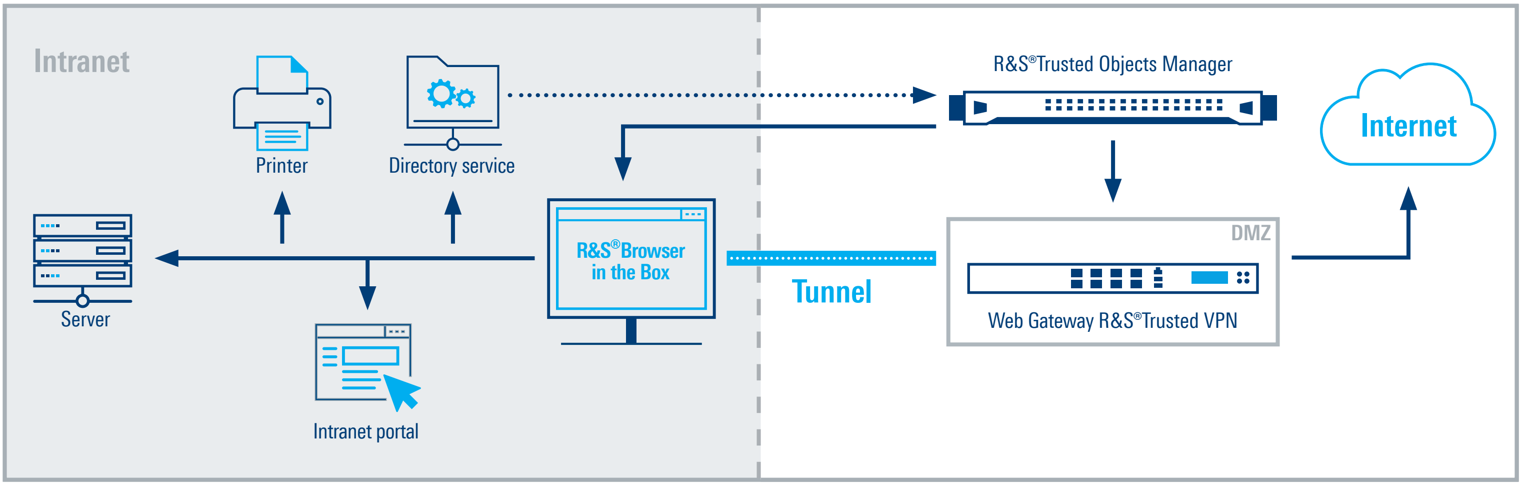
# HOW DO YOU PROACTIVELY PROTECT YOURSELF?

Using the internet has become an indispensable part of daily work. However, the browser needed to access the internet also acts as a gateway for ransomware and other common malware.

Developed in cooperation with the German Federal Office for Information Security (BSI), the fully virtualized surfing environment R&S®Browser in the Box offers an innovative, multilevel concept for secure and convenient internet surfing and optimum protection against malware for public authorities and companies. R&S®Browser in the Box has two protection goals: Isolation at the computer level and isolation at the network level.

With **computer-level isolation**, the virtual browser closes the internet security gap by providing digital quarantine for attacks: malware is isolated before it can even be executed. Instead of detecting malicious code - as in anti-virus programs - execution is prevented from the outset. Any potentially dangerous activity is isolated in a closed virtual browser. The operating system and browser are completely separated from one another. This helps prevent all kinds of malware attacks, including malvertising which injects malicious code into seemingly innocuous digital ads. As soon as a user clicks on one of these ads, malicious software is downloaded to the server. The malware then deactivates various security mechanisms and is able to spread effectively throughout the system and network. Following this, ransomware is used to encrypt personal and business data, making it inaccessible.

When it comes to ransomware attacks (and malware attacks in general), the second protection goal is crucial - **network-level** isolation. Thanks to unlimited internet access in the encapsulated browser, the actual end user's operating system only needs access to a few carefully selected web servers. This provides much more detailed control over internet access and thus makes it possible to limit access exclusively to trusted internet servers, which naturally excludes all internet servers and services hosted by cybercriminals. And if the cybercriminal's server cannot be accessed, malware cannot cause any damage to your computer system — effectively preventing any attack.



## R&S®Browser in the Box benefits:

- Security thanks to a **fully virtual environment and complete separation of internet and intranet**
  - Maximum protection against malware by blocking malware downloads
  - Data leak prevention
  - Proactive blocking of all telemetry services
- **Two-browser strategy**
  - Intranet browser for intranet portals
  - R&S®Browser in the Box for the internet (Firefox, Chrome, Tor browser for special use cases)
- For **workstation PCs** and **terminal server environments**
- Developed in cooperation **with the German Federal Office for Information Security (BSI)**

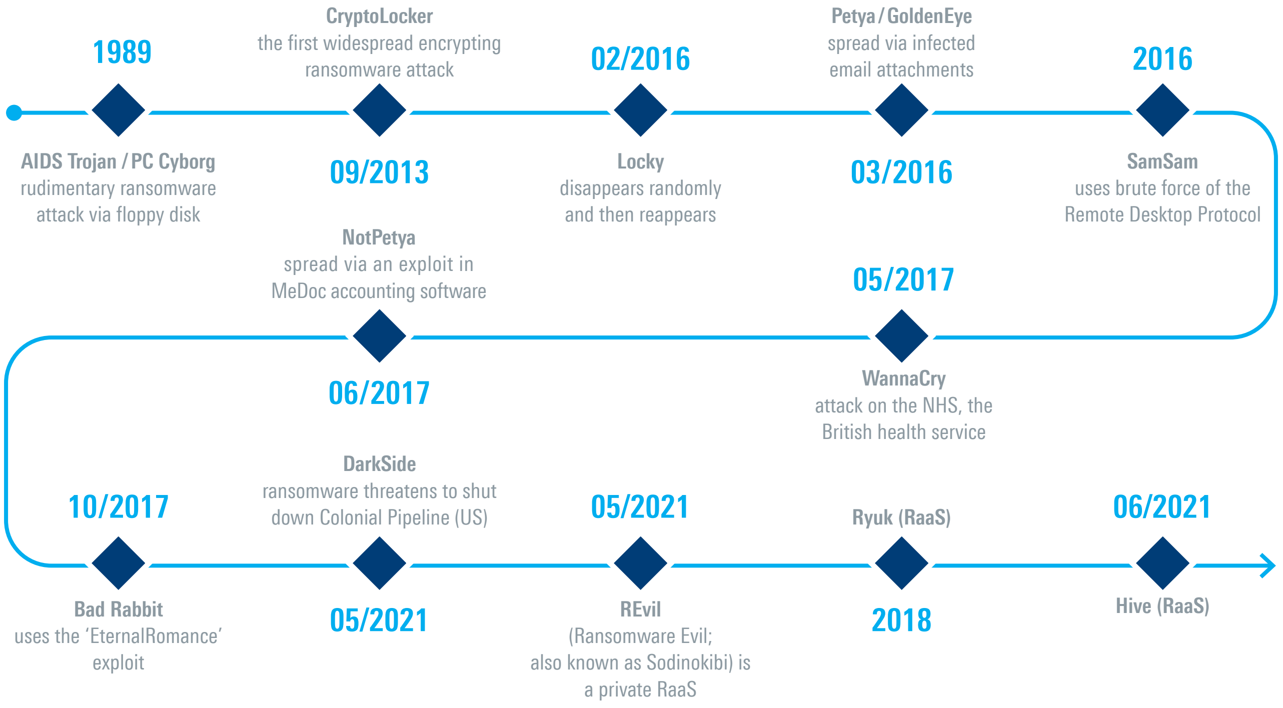
## Frequently asked questions about R&S®Browser in the Box

**How does R&S®Browser in the Box prevent malware attacks (e.g. Emotet)?**
Modern malware attacks are typically controlled via a command and control (C&C) server: the malware loader communicates with the servers and downloads the desired programs as instructed. Using R&S®Browser in the Box prevents this communication entirely. The solution allows you to completely neutralize malware like Emotet because instructions cannot be executed without communication.

**Does R&S®Browser in the Box replace antivirus software/firewalls?**
No. Our solution provides additional protection on top of basic security measures like firewalls and virus software. Businesses and organizations can only protect themselves effectively against cyberattacks by separating their intranet and internet networks.

**Does it restrict internet use in any way?**
Our solution does not limit internet use in any way. However, administrators can set up restrictions, e.g. defining which file types can be downloaded or imposing a complete upload ban.

**Can you use it for video chats and video conferences?**
Yes. You can host and join video chats and conferences in all established video conference solutions with no problem at all when using R&S®Browser in the Box.



1989
AIDS Trojan / PC Cyborg
rudimentary ransomware attack via floppy disk

09/2013
CryptoLocker
the first widespread encrypting ransomware attack

02/2016
Locky
disappears randomly and then reappears

03/2016
Petya / GoldenEye
spread via infected email attachments

2016
SamSam
uses brute force of the Remote Desktop Protocol

05/2017
WannaCry
attack on the NHS, the British health service

06/2017
NotPetya
spread via an exploit in MeDoc accounting software

10/2017
Bad Rabbit
uses the ‘EternalRomance’ exploit

05/2021
DarkSide
ransomware threatens to shut down Colonial Pipeline (US)

05/2021
REvil
(Ransomware Evil; also known as Sodinokibi) is a private RaaS

2018
Ryuk (RaaS)

06/2021
Hive (RaaS)

**Rohde & Schwarz Cybersecurity GmbH**
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

**Rohde & Schwarz GmbH & Co. KG**
www.rohde-schwarz.com

PD 3683.3842.32 | Version 02.00 | Januar 2023 (NP)

3683384232