

Information for companies

RANSOMWARE

Companies and institutions
as targets

www.g4c-ev.org



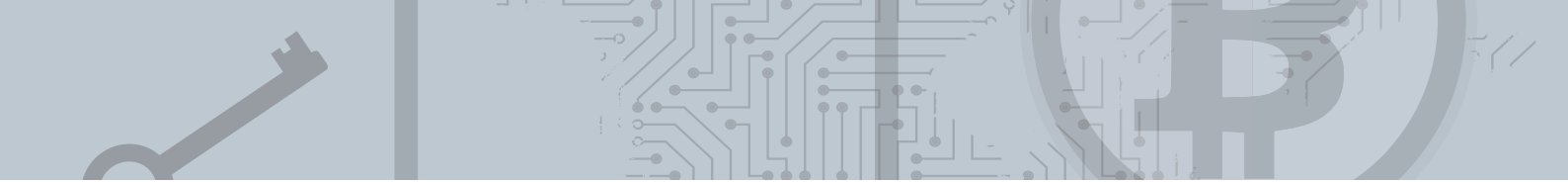
Our
Cooperation Partners



Bundeskriminalamt



Bundesamt
für Sicherheit in der
Informationstechnik



Ransomware

Malware, or harmful software that is used to encrypt data on other computers, denying access to the data by the actual owners. To obtain the key required for decryption, victims are expected to pay a ransom (generally payable in Bitcoin or the like).



How does ransomware get into the company?

Such malware is typically sent out by email in a broad, untargeted fashion. If these emails are not filtered out in advance by central security measures, such as spam filters or general virus scanners, there is a risk that recipients might open the emails and their harmful attachments. Should further system restrictions or workstation virus scanners fail to prevent the subsequent execution of the software, the automatic encryption of all accessible data begins. Mature variants of such software also attempt to spread over the internal network, allowing them to achieve a much greater extortion potential.

The consequences can be fatal

Data encryption can disrupt services and production for days or even bring them to a complete halt. In addition, the reputation of the company suffers heavily from negative headlines, as impacts of such infections can hardly be hidden from the public¹. Previously, extortionists demanded only a few Bitcoin as ransom, and the impacted companies generally did not concede to the demand. Instead, they continued their operations after restoring from backups.

Targeted attacks pose a new threat

As a new trend, attackers seek to encrypt nearly all data held by an organisation, including backups. If successful, they can demand significantly higher ransoms.

The impairment of services or production capacities can last for a considerable time, and in the worst case, all data could be permanently lost. For many companies, this effectively means an end to all business operations.

Information and assistance

This brochure is intended to assist companies and institutions in understanding the phenomenon of ransomware and the associated threats. It should help in the design of countermeasures for prevention and detection as well as provide advice in the case of an actual attack.

¹ Publicly known examples include the Lukaskrankenhaus Neuss (10 Feb. 2016), Deutsche Bahn (13 May 2017) and the Danish logistics group Maersk (26 Jan. 2018).

What do the attackers do?

Typically, the attacks come via email with corresponding malware attachments. The nature of these attacks can vary. In practice, however, it is very often Office documents (e.g. Word files) that load malware components after opening. Such emails can potentially reach any employee of a company. The oft-cited warning never to open attachments of emails from unknown senders is not practical if files are sent as unsolicited applications to the human resources department, to customer hotlines or to sales employees with outside contacts. Moreover: Current criminal groups also use or make reference to correspondence that they obtained from previous attacks on other companies, making it possible for them to impersonate known senders. When such methods are applied in bulk in a targeted way, this is called “dynamite phishing”.

The technical infection often progresses in several stages. First is the installation of a “downloader”, which downloads additional malware, such as the actual ransomware or remote access tools for further exploration of the company’s IT infrastructure².

Variants with full encryption, including backups

■ Spreading throughout the entire network

The initial ransomware attempts to take over administrative accounts such as domain admins and backup accounts, for instance via network drives. A typical procedure is to guess passwords or make automated login attempts (brute force). Due to frequently used standard passwords and with the help of cleverly created password lists, attackers are often more successful with such tactics than generally

assumed. They also make use of unpatched weaknesses, such as in the intranet. If one of these methods is successful, the malware actively informs the perpetrators that a potentially lucrative victim can be expected here (more so than the typical case). The perpetrators then attempt – often still manually – to gain significant control over the company’s IT infrastructure with remote access tools or other methods, striving in particular to make all backup options entirely unusable.

■ Planned and targeted attacks

Attackers collect extensive information about the companies or institutions in advance by means of social engineering. They use social networks, telephone calls from false identities and phishing emails to get the lay of the land. These efforts reveal whether a lucrative situation exists and allow subsequent ransomware infections to be carefully targeted. In the course of such probing, criminal groups can move widely within the network and collect additional information about the company. Based on these insights, some perpetrators even adjust the amount of the ransom and issue demands which they think the company can afford without entirely threatening its economic existence.

² To look up in a web search: Names of historically prominent ransomware from 2016/2017 include “Locky” or “WannaCry”, while the relevant malware families as of 2018/19 have names like “Emotet/Trickbot”, “Ryuk”, “GandCrab”.

Typical scenario

It is typical for perpetrators to begin with efforts to fully encrypt the target IT infrastructure on Friday evening since the process can proceed undisturbed while the employees are away for the weekend. The IT disruptions usually go unnoticed until Monday morning when computers do not start, telephone systems, email servers, websites and the electronic banking system fail or backups are encrypted. It is also typical for a letter in English to appear demanding a large ransom – payable in a crypto currency – which can be in the five- to seven-digit euro range for targeted attacks.

What measures provide the most effective protection against infections with ransomware?

■ Basic protection against incoming malware

The basic components for defending against incoming malware are measures such as spam and malware filters on the central email server, possibly also on the web proxy and at other external interfaces, as well as on user desktops, servers, file shares, etc. The German Federal Office for Information Security (BSI) has appropriate information and advice available³.

■ Fostering awareness amongst employees and business partners

First and foremost, employees should be informed of the threat. Raising awareness among business partners and suppliers is another important and indispensable basic measure. Advice on handling these aspects can be found in a very informative report produced by the Heise Mediengruppe about a trojan attack on their own company⁴.

■ Thinking one step ahead

It must always be expected that malware arriving by email will pass through the first line of defence undiscovered. Clear internal rules for handling suspicious emails, such as emails with suspicious attachments, must be in place. As the employees receiving these emails may not have extensive IT skills, the corresponding action recommendations must be easy to find, simple and, above all, useful. Employees should be instructed to check sender addresses letter by letter, and direct assistance should be available if they are faced with the dilemma of whether or not to open a suspicious email and possibly trigger an infection or to delete it and possibly destroy an important email.

It can be useful to create an internal mailbox where employees can send suspicious emails, including attachments, to be checked before they are opened. Ideally, this mailbox should be protected by sandboxing measures⁵ and/or subject to detailed inspections by security experts, and the result of the check must be reported back to the employee promptly. A few organisations have already put this into practice, but (too) many other companies and institutions have not. Sometimes the option exists, but the employees are not sufficiently aware of it.

³ „BSI warns against targeted ransomware attacks on companies“ (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/BSI_warnt_vor_Ransomware-Angriffen-240419.html) and „Measures for protection from Emotet and dangerous emails in general“ (<https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html>).

⁴ „Trojan attack: Emotet at Heise“ (<https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html>).

⁵ A sandbox refers to an environment isolated from the company's IT infrastructure that simulates a real IT environment. Suspicious documents and emails can be opened here to check their effects on computer systems.

Which measures can prevent intentional data destruction?

■ Inspection of the backup and recovery measures

A backup concept designed primarily to ensure business continuity in the event of a storage media failure can sometimes be entirely ineffective against attacks with encryption trojans. To protect companies and institutions from such attacks, offline backups or storage media are required which cannot be reached and overwritten at any times via the network or file shares. A good backup concept must include regular, practical testing of the recovery capabilities to verify that a flawless operation system can be restored from the existing backups.

■ Restrictive use of privileged and administrative accounts

The more extensively and the more often user accounts with expanded access rights are used for daily work, the greater the risk of an accidental infection. Accounts such as the domain administrator should only be used as actually intended. Whenever possible, local administrators should be prevented from logging in over the network or the local administrator accounts themselves should be disabled via group policy. If such accounts are in fact needed, a specific local administrator password is recommended. For example, Microsoft offers the free tool "Local Administrator Password Solution" (LAPS), which automatically manages passwords and saves them in a separate directory.

■ Create passwords for administrative accounts very carefully

It is critical that sensitive accounts have secure, hard-to-guess passwords. Default or standard passwords definitely do not offer sufficient pro-

tection, but even a unique password should be selected with careful thought. Secure passwords should contain a combination of upper and lower case letters, numbers and special characters. Strings that appear in dictionaries and references to personal information must be avoided.

■ Security patches also in the intranet

In practical terms, the root problem that makes ransomware infections possible is that emails with harmful attachments have passed undetected through the first hurdle of virus protection on the central mail server. If malware is subsequently activated by opening the attachment, it is already on the internal network. It is therefore recommended that security patches be installed as promptly as possible, even in the intranet, which is supposed to be protected from outside attacks. If the installation of security patches is not possible or is significantly delayed (such as on older industrial systems, production lines or medical devices), these machines should be isolated from the rest of the network as far as possible.

■ Inspection of connections to service providers and business partners, especially for outsourced IT and cloud solutions

Advanced ransomware attempts to spread across all existing network connections, including connections to service providers and business partners. To prevent infections spreading over these connections, the associated access options and network authorisations should be evaluated. Business partners must take these security precautions as well to prevent being a source of infections themselves.

Creation of a system for emergency planning and crisis preparedness

■ Emergency planning and evaluation of the existing measures

Many companies have already taken measures to prepare for serious security incidents and crisis scenarios and have created emergency plans. But do these also cover a full encryption of the company's entire IT systems and data? A detailed evaluation of the emergency planning is highly recommended to identify necessary improvements. An external assessment by a recognised and qualified IT security company can be a good investment in the future and can offer a valuable direct contact should an actual incident occur later. Certified IT security service providers that meet specific, verified quality standards are listed on the BSI website⁶.

■ Ensure communication capability in an emergency

If an incident occurs, a company's entire IT infrastructure could be encrypted and therefore non-functional. This also applies to email software, fax and telephone systems, including contact data. However, it is essential in such a situation to be able to communicate internally with employees and the press department as well as externally with law enforcement agencies, IT security companies, business partners, media, lawyers, banks, etc. Company mobile phones could serve as a functional communication tool, but these may only offer limited access to internal information. For this reason, emergency documents, such as contact lists for the most important internal and external contact persons, should always be available as a paper printout or at least on a separate USB stick or CD. This allows companies to access the infor-



mation even independently of potentially compromised or disabled systems.

■ Ensure the ability to make payments

Even if companies suffer from crippled IT infrastructure for a prolonged period, they must still meet their payment obligations. With compromised systems, however, this may no longer be possible. In the course of building a backup system, the company main bank should be consulted. The bank may be able to offer online access to the company accounts that function outside of the company's technical infrastructure for use in an emergency.

⁶ „Certified IT security service providers“ (https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/Stellen_node.html).

■ **Preparatory contacts and networking**

Contacts with industry associations and other companies of the same industry or supply chain as well as with institutions such as G4C and, in particular, law enforcement agencies are useful for defending against cyber attacks. Law enforcement agencies have established “Central police cyber crime contacts for businesses” (ZAC)⁷ for this purpose. It can also be useful to consult with the company main bank on this topic. Many banks know the topic well from daily business with corporate customers and may already have diverse measures in place. These range from preventive raising of awareness and alternative options for payment transactions to – for extreme emergencies – active support in contacting law enforcement agencies or in procuring Bitcoins.

■ **Cybersecurity insurance or fidelity bonds**

In principle, it is possible to insure oneself against potential damages from cyber attacks. The risks and losses that this insurance should actually cover must be evaluated on a case-by-case basis. It is generally very important to insurers that suitable preventive measures are in place. Whether and to what extent it is useful to insure against total losses or ransom payments must be evaluated by each individual company on its own and then discussed with the respective insurer.

How can companies ensure early detection?

■ **Stay up to date**

In the process of forging preparatory contacts and networking, companies can learn early how current attack scenarios unfold. In addition, the Twitter account of the CERT-Bund (BSI)⁸ is a very good source of up-to-date information.

■ **Join “information sharing” initiatives**

With information sharing, participating companies can learn about attack characteristics that they can address in their own security mechanisms. Such indicators of compromise (IOCs) include typical features of incoming attack emails and their attachments or server names and IP addresses to which active malware connects for command and control purposes.

■ **Independently collect and share additional information**

Among other measures, the use of a central contact point in the company for suspicious emails can provide the company with more information about the real threat situation, which can then also be shared with other companies. Voluntary information sharing between companies is a mutual consultation to the benefit of all participants.

⁷ https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

⁸ <https://twitter.com/certbund>

What is to be done in the event of an attack?

■ Time is now money!

Responsibilities and expected actions should be as clear as possible to everyone involved at the company. Communication chaos is not only unprofessional, it wastes valuable time and may have long-lasting consequences on the working climate at the company and with management.

■ Reach out to previously established contacts

In the course of creating an emergency and crisis preparedness system, contact with the ZAC and certified security service providers should already have been established. These contacts should be consulted for assistance as quickly as possible.

■ Hands off the technology, and bring in external expertise

This extremely pragmatic initial tip can be more effective than half-hearted restoration attempts. Such attempts can cause even more damage and make decryption impossible even after paying the ransom and obtaining the key. It is better to bring in the respective police's ZAC at an early stage and to rely on specially qualified IT forensics companies. If you have not already established good, trustworthy contacts in advance during the emergency planning, you can find a source below for corresponding "emergency IT security service providers" that have been vetted and checked by BSI⁹.

If a ransomware infection is detected, fast action is called for. Extensive preparations by everyone involved play an important role. After all, only when procedures and responsibilities are defined and known can companies minimise long-term financial and communicative risks.

First and foremost, one important piece of advice is: If you do not have considerable expertise in fighting cyber crime yourself, consult an external expert promptly (see below).

■ When in doubt: Switch it off for now!

If a company has discovered an attack early and qualified IT security expertise is available in-house or external expertise can be quickly organised, the criminal activities can be observed. This opportunity should be used to monitor and limit the impacts. If this is not possible, a complete network disconnection or shutdown of as many components as possible should be considered until it is clear which systems are impacted and which are not.

■ Stay on the safe side

The downloaded malware is often not detected by standard antivirus software in the initial time after its dissemination. Such malware sometimes makes far-reaching changes to infected systems that cannot be easily undone. The basic recommendation is therefore to consider such infected systems as entirely compromised.

⁹ Qualified service providers in the event of cyber attacks (https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html), especially the section for "APT response", in other words, responses to a targeted attack (advanced persistent threat).

Access data saved on such systems or entered after an infection should be treated as compromised, and the passwords should be changed.

■ **Focus on administrative accounts, network segmentation and security patches**

If the attackers have succeeded in accessing administrative accounts, a restoration without changing the associated accounts and passwords will generally be fruitless. Even a restoration of an outdated security patch level from the backup may go up in smoke.

■ **Adhere to reporting deadlines**

Companies should also adhere to any reporting deadlines. In general: Where malware has been installed, data has presumably been stolen. In the case of personal data, companies may sometimes face severe penalties if reporting deadlines, such as those based on GDPR, are not complied with.

Let's talk ransom: What should the company do?

BSI, law enforcement agencies, security experts and G4C all urgently advise against paying ransoms. This avoids providing further support for criminal business models, especially since there may be alternatives for decrypting the infected company data. In the case of a ransom payment, it is not guaranteed that companies or institutions will receive the necessary keys or that they will actually work. If it is possible to restore business capability on their own, companies should therefore never give in to the demands of the extortionists.

However, such general recommendations are of little help if a company is unable to operate due to a full encryption, including backups, or a non-functioning recovery. If a company or institution is facing the choice of fully ceasing business operations or paying a ransom, a payment can be considered in the individual case. Before this decision is made, however, external expertise should always be consulted:

- There may actually be other ways to obtain any decryption codes or to reconstruct the data. With the advanced ransomware currently on



the market, this is now relatively unlikely, but an initial expert assessment – assuming the malware family has been identified – is generally quick and worth a try.

■ It is in no way simple to convert large amounts of euros into crypto currency quickly and without preparation. However, it is not rare for attackers to put time pressure on companies by threatening increasing ransom demands¹⁰. Victims need quick access to experts who can assist them in this situation. A company will generally also have to inquire about putting off the payment anyway. Here as well, professional support is recommended.

■ Advanced ransomware attackers who directly target companies normally have a “reputation interest” in their decryption methods also functioning properly. Under some circumstances, this approach may offer a chance of restoration as a final lifeline. However, only experts familiar with the material and the situation can assess how good this chance is.

Affected companies should never use the emergency option of paying the ransom as an excuse for neglecting preventive action. Even in the best case, the odds of being saved by paying the demanded amount may be no better than 80 to 20.

Instead, companies should be aware that a “post mortem” restoration of the system, whether from the recovery data or with a decryption code after paying the ransom, is only half the journey. The attackers now have extensive knowledge of the respective company and its IT infrastructure. To prevent renewed attacks or infections, victims must go the rest of the way with a more or less complete reconstitution of their IT landscape.



This makes it all the more critical to secure the company’s IT structures, engage in extensive internal and external information management and build up a useful network of relevant agencies and companies in the same industry. Because when it comes to ransomware, the old saying still applies: An ounce of prevention is worth a pound of cure.

¹⁰ Sample excerpt of the messages of one of the ransomware gangs: “Countdown to double price: 2 days”, along with a backwards-running clock.



As a non-profit association, the German Competence Centre against Cyber Crime (G4C) is dedicated to preventing, investigating and responding to attacks in cyberspace. G4C shares expertise, issues early warnings and initiates regular exchanges of information about threats on the internet. The operational cooperation partners are the Federal Criminal Police Office (BKA) and the Federal Office for Information Security (BSI). At the international level, the association also exchanges information with relevant agencies for fighting cyber attacks (in the USA: National Cyber-Forensics and Training Alliance – NCFTA; in Great Britain: Cyber Defence Alliance – CDA).

The association's work is based on four pillars: G4C is building an up-to-date data platform as an early warning system to supplement direct personal contacts. The association also performs data extraction for the BKA and other investigative authorities, engages in training and education and participates in background checks to improve the competence of cyber security professionals.

The founders and initial members of G4C are banks and insurance companies, but the association has consistently expanded its competence to include other industries.

All contents of this brochure, in particular texts, images and graphics, are protected by copyright. Distribution and utilization is permitted as long as it is non-commercial. Any duplication or processing of such material beyond the scope of the copyright law shall require the prior written consent of G4C. The use of extracts from the brochure is only permitted with reference to the source.

CONTACT

Entry in register of
associations
Wiesbaden VR 6806

www.g4c-ev.org

Version: November 2019

German Competence Centre
against Cyber Crime e. V. (G4C e. V.)

Borsigstraße 36
65205 Wiesbaden

Telephone: +49 6122 178 4800

Fax: +49 6122 178 4803

Email: info@g4c-ev.org