**BNP PARIBAS**

> **MALWARE ALERT: PROTECT YOUR BUSINESS AND RAISE AWARENESS AMONG YOUR EMPLOYEES.**
>
> In 2015, and more recently in 2018, tens of thousands of companies became the victims of malware, sometimes without even realising it. The head of BNP Paribas Cash Management interactive services tells us how this malicious software spreads, the damage it can do to companies and how to guard against it.

## HELLO, CAN YOU TELL OUR READERS WHAT MALICIOUS SOFTWARE IS?

As the name suggests, malicious software, or malware, is a program that is developed for the purpose of infecting a computer without the user's consent, to damage it or take advantage of its content.
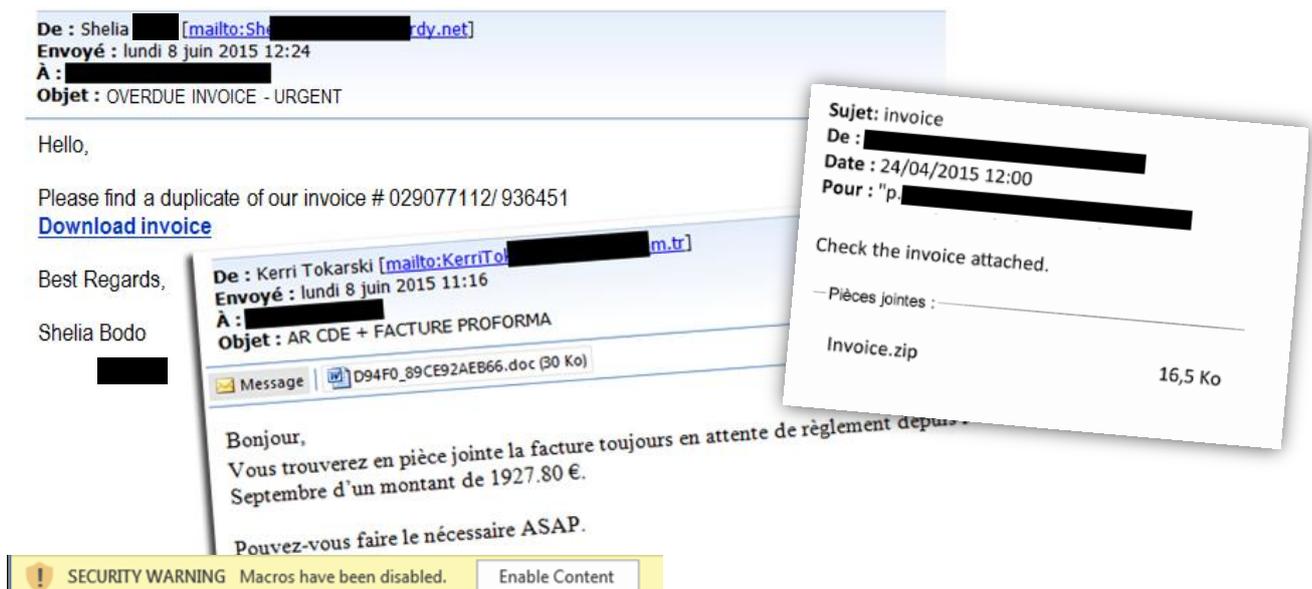
## SO IS THAT WHAT IS KNOWN AS A VIRUS?

Viruses are indeed malware. Depending on how it is spread, malware can be known as a virus, worm or Trojan horse.

## BUT HOW CAN MY PC BE INFECTED WITHOUT MY KNOWLEDGE?

Nowadays, most malware is spread by e-mails that contain an attachment, or a link to a file, and they are sent out in massive spam campaigns. For example, an accountant can receive a fraudulent e-mail containing an invoice in a Word or Excel format. Opening the attachment triggers the execution of a Visual Basic macro that allows the malware to be installed without their knowledge.
See below examples of fraudulent e-mails:

De : Shelia ███ [mailto:She████████rdy.net]
Envoyé : lundi 8 juin 2015 12:24
À :
Objet : OVERDUE INVOICE - URGENT

Hello,

Please find a duplicate of our invoice # 029077112/ 936451
**Download invoice**

Best Regards,

Shelia Bodo

De : Kerri Tokarski [mailto:KerriTok████████m.tr]
Envoyé : lundi 8 juin 2015 11:16
À :
Objet : AR CDE + FACTURE PROFORMA

Message | D94F0_89CE92AEB66.doc (30 Ko)

Bonjour,
Vous trouverez en pièce jointe la facture toujours en attente de règlement depuis
Septembre d'un montant de 1927.80 €.

Pouvez-vous faire le nécessaire ASAP.

SECURITY WARNING   Macros have been disabled.   Enable Content

Sujet: invoice
De :
Date : 24/04/2015 12:00
Pour : "p.

Check the invoice attached.

Pièces jointes :

Invoice.zip

16,5 Ko

### IN THIS EXAMPLE, THE HACKER TAKES ADVANTAGE OF A USER'S LACK OF CAUTION TO INSTALL THE MALWARE. IS THAT ALWAYS THE CASE?

Generally, yes. Hackers usually seek the path of least resistance: they almost always exploit human failure. E-mails containing a malware attachment are the most frequent method nowadays, but hackers use a variety of means.

For example:

- If you install a free or hacked software package, it may contain a Trojan horse.
- You can also visit a booby-trapped internet site that exploits a vulnerability in your system, or you can run a fake software update.
- Also be wary of fake technicians who can take control of your PC remotely, with your authorisation.

### ONCE MY PC HAS BEEN INFECTED, WHAT CAN I EXPECT?

The threats are many and varied. For instance, hackers can use your PC to launch network cyberattacks, or they can spy on your firm. But to get straight to the point, I'll mention the three main threats that are likely to strike businesses today: **transfer fraud**, **extortion of funds** and **data theft.**
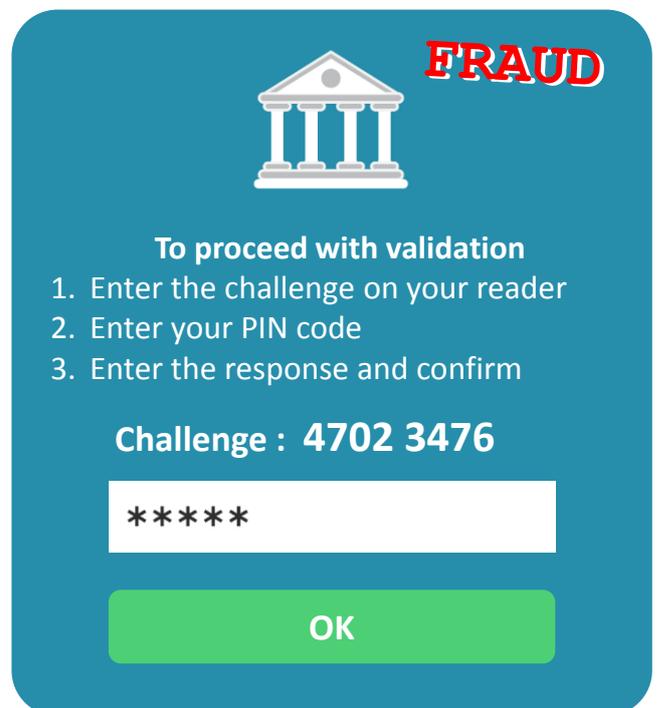
#### Transfer fraud

In this case, the malware creates a beneficiary account on your online banking tool and then enters a fraudulent transfer debited from your firm's bank account. If need be, it will display a fake page prompting the accountant to enter a code that is required to execute the transfer (such as an SMS code or a validation code).
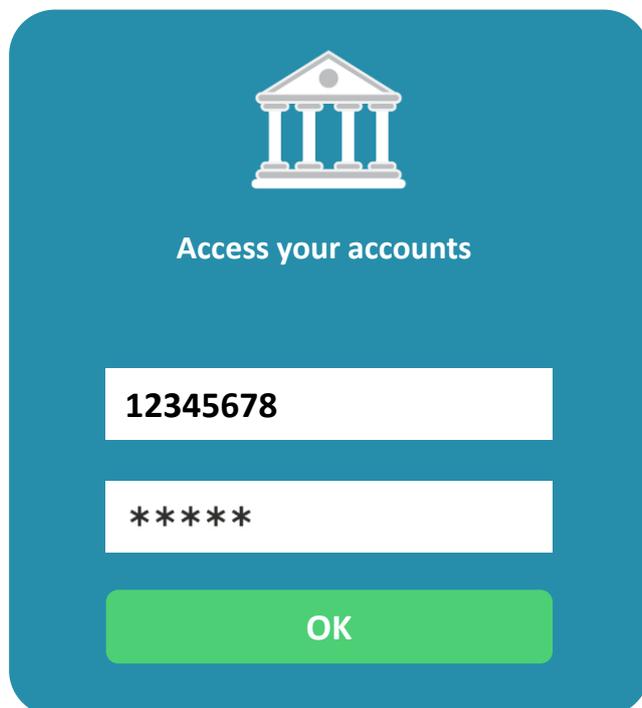
| **Regular login page** | **Bogus page : signature request** at login |
|---|---|
| **Access your accounts** | **FRAUD** |
| | **To proceed with validation** |
| | 1. Enter the challenge on your reader |
| | 2. Enter your PIN code |
| | 3. Enter the response and confirm |
| **12345678** | **Challenge : 4702 3476** |
| ***** | ***** |
| OK | OK |

#### Extortion of funds

Some types of malware, known as ransomware, can encrypt the files that are stored on the victim's hard drive or network drive, and then demand a ransom for the delivery of a decryption key with which the company can retrieve its data. A hospital in California recently admitted to paying a ransom of $17,000 to retrieve its data.

### Data theft and the resulting damage

Malware can also steal all kinds of data. For example, DRIDEX, one of the most widespread strains of malware, does more than just execute fraudulent transfers: it steals your internet browsing history, your identifiers and passwords (for online banking sites, webmail accounts, commercial sites, etc.), bank card numbers, your partners' contact details and account numbers, and more.

All of this data is extremely valuable to hackers: they can sell it to other fraudsters in the deep web[1], or use it for other types of scams – bank card fraud, identity theft and so on.

## DOES THE ANTI-VIRUS SOFTWARE ON MY PC PROTECT ME AGAINST MALWARE?

Yes, partially. It is **crucial to have a good anti-virus program**, updated daily, on every computer. More generally, it is important to **use only trustworthy, non-pirated operating systems and software that are updated every day**.  We also advise you to protect your e-mail gateways using screening systems. You should be aware, however, that hackers constantly change the files that spread malware to prevent anti-virus software from detecting them. Therefore, **anti-virus software is not enough!**

## SO WHAT CAN BE DONE TO PROTECT ONE'S SYSTEM?

**Raising employee awareness is essential**
Let's be perfectly clear: in most cases, it is an employee who allows the malware to be installed without even realising it. And, many small and medium-sized companies tend to neglect raising awareness amongst their employees.

Any company, whatever its size, **should regularly train its employees in cyber risks and apply common sense rules for computer security.**

| A FEW EXAMPLES OF COMMON SENSE RULES | COMMENTS |
|---|---|
| Never open an attachment from an unknown sender. | Disable automatic opening of attachments in e-mail software. |
| Never authorise the execution of a macro on an attachment. | Disable automatic execution of macros in Microsoft Office. |
| Check links contained in e-mails before clicking on them (by hovering over them with the mouse), and only visit trustworthy sites. | The use of a black list, or even better a white list of websites, can be helpful. |
| Never install software or an update from an uncertain source. | Software installation rights should be restricted to system administrators. |

## TO SUM UP: RAISE AWARENESS REGULARLY AMONG MY EMPLOYEES, A GOOD ANTI-VIRUS PROGRAM AND SOUND MANAGEMENT OF MY INFORMATION SYSTEM...

Yes, those are the basic steps that every company should take. But let's be humble. No one is completely safe. That's why I'd like to give three more pieces of advice to businesses, with the aim of protecting them if they fall victim to malware: the **correct use of your payment applications**, **data back-up** and **encryption**.

### The correct use of your payment applications

To steer clear of transfer fraud, I advise you to establish a segregation of duties or dual validation in your banking tools. Keeping track of your accounts on a daily basis is also a simple and effective way to detect out-of-the-ordinary transactions and to react quickly in the event of fraud.

---

[1]*The deep web, also known as **the invisible web** or the hidden **web**, refers to the part of the internet that is available online but it is not indexed by standard search engines.*

### Regular data back-up

To prevent damage from **ransomware**, it is vital to perform **daily back-ups** of the company's data.

### Encrypt the most sensitive data

To prevent the theft of very sensitive data or industrial espionage, I recommend that you assess the critical nature of your data and protect the most sensitive elements with **strong authentication** and **encryption**.

### TO CONCLUDE, WHAT WOULD YOU TELL A COMPANY MANAGER WHO IS HESITANT TO TAKE THESE STEPS DUE TO A LACK OF TIME OR BECAUSE THEY DO NOT THINK THEIR COMPANY WILL BE A VICTIM?

The malware phenomenon has become massive. It is increasingly profitable to the organised criminals behind these scams. The problem is not likely to disappear soon. You have to be prepared for an attack. Of course, it's legitimate for any firm to adapt its protection measures to its risks.

- In large companies, this is the work of the Chief Information Officer or the Chief Security Officer.
- For certain SMEs, raising awareness regularly among employees and sound management of the company's IT system (anti-virus, regular back-ups, etc.) will often be enough.

For the most reluctant, who think they're already protected, I would say **at the very least, you should provide regular employee training in cyber risks and IT security best practices; this is absolutely indispensable.**

Feel free to contact your relationship manager to carry out a risk analysis and set up solutions that are suited to your organisation.