

zix™



Rise of Ransomware: How To Protect Your Organization



Graham Cluley
Independent security analyst
Host “Smashing Security” podcast



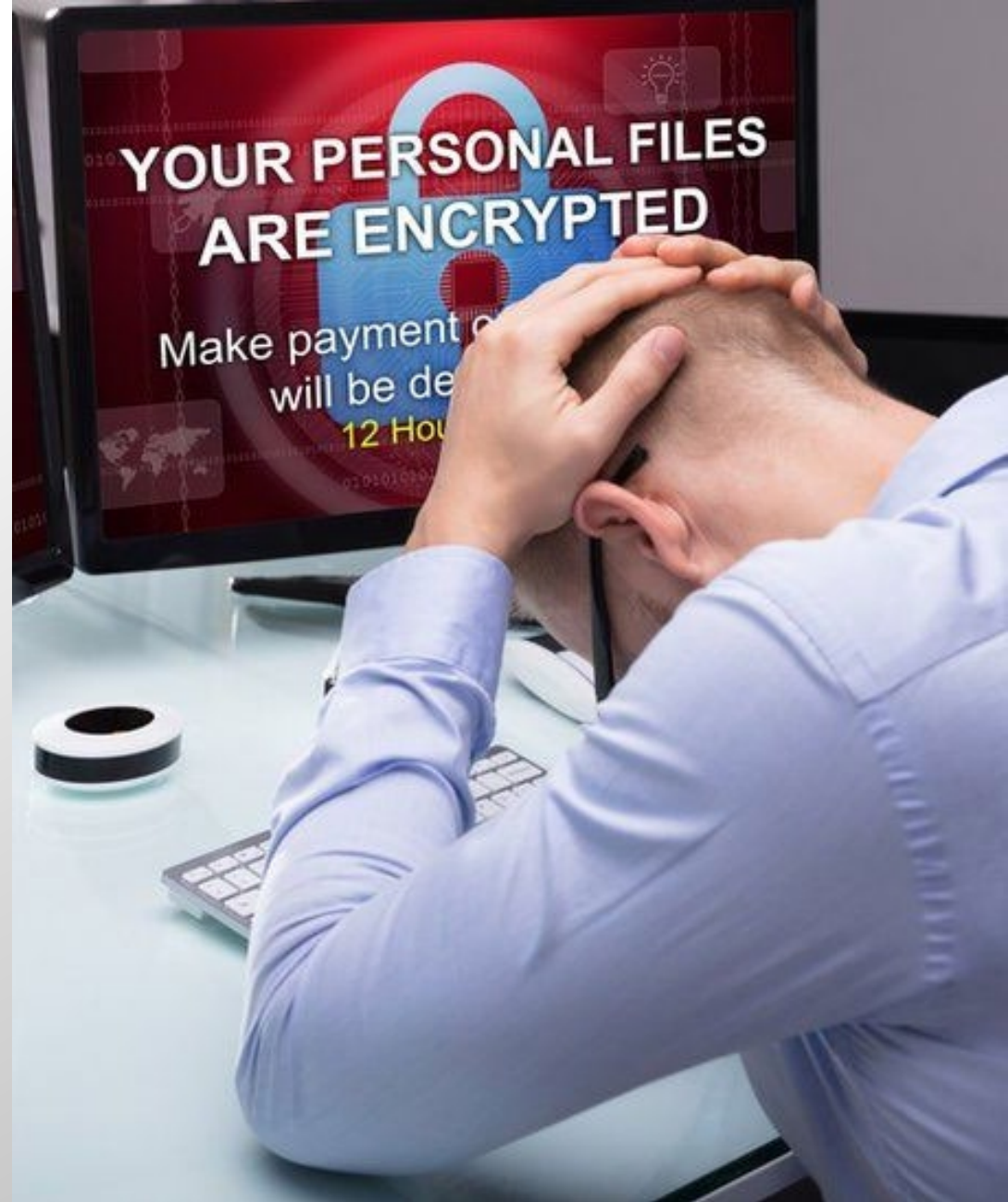
Andrew Murphy
Director of Product Marketing

Ransomware on the rise: How to protect your organization

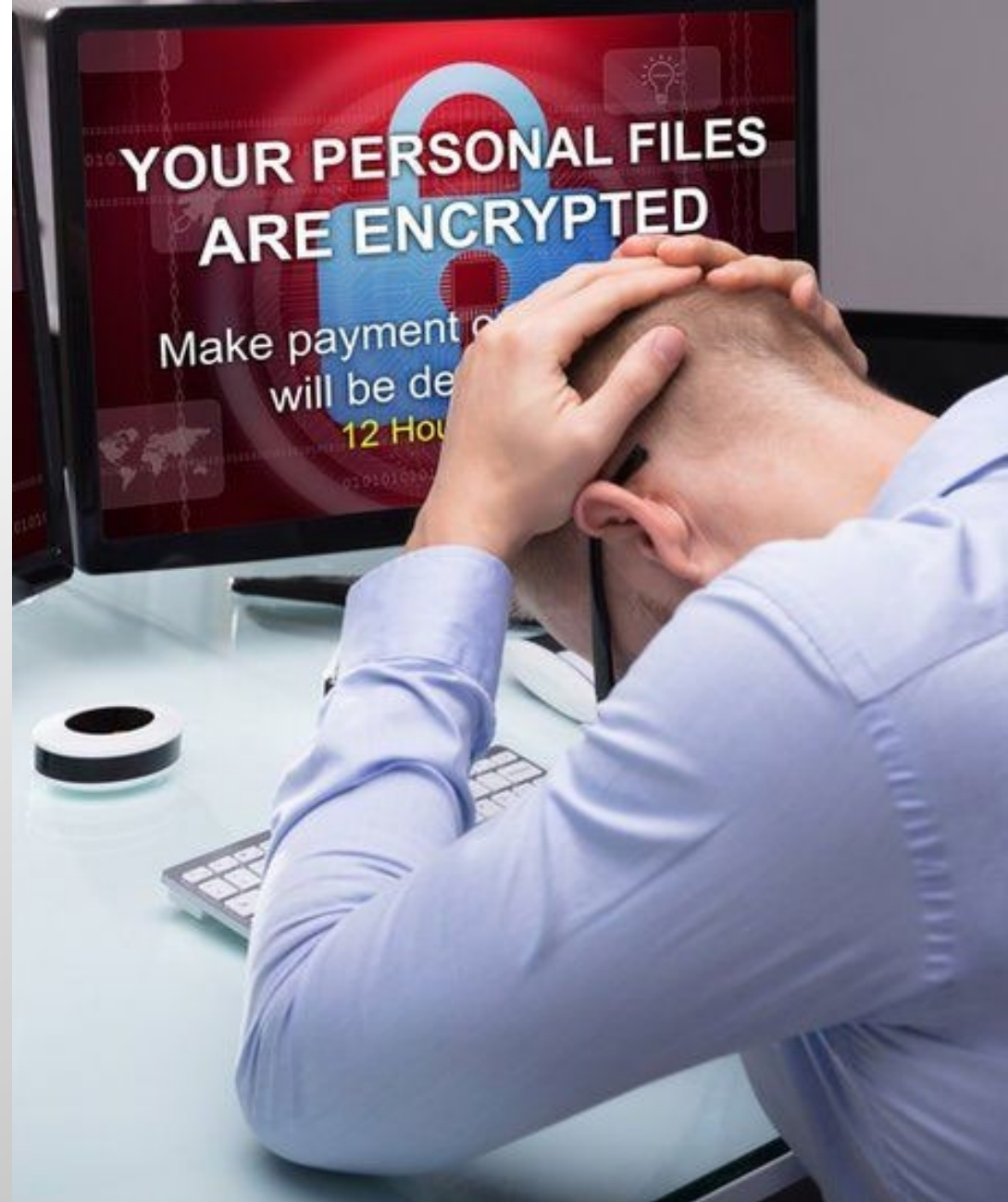
Graham Cluley

Independent security analyst

Host “Smashing Security” podcast



Ransomware: What is it?

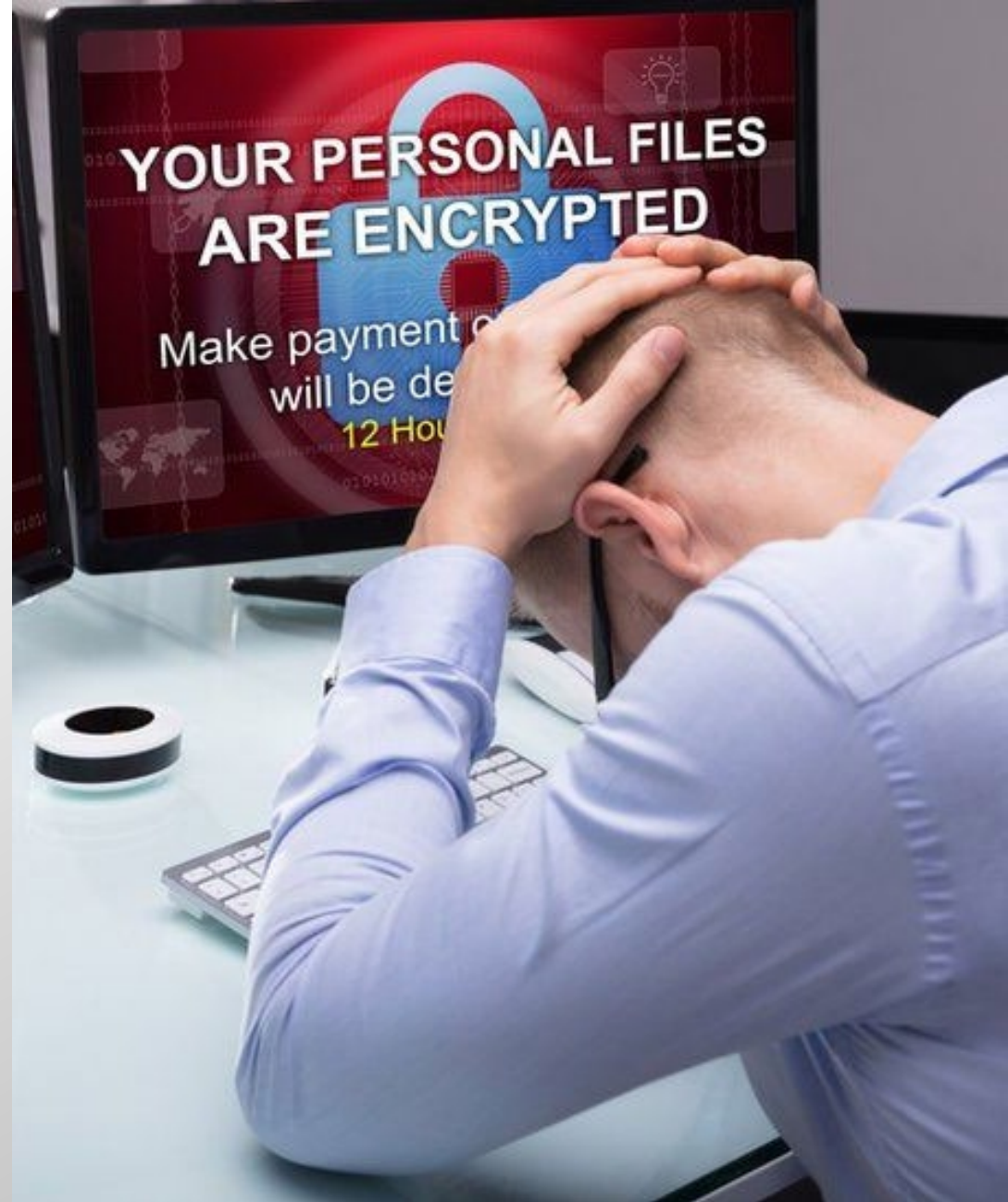




RANSOMWARE



Ransomware: Origins and evolution



AIDS Information - Introductory Diskette

Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

Instructions

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

- Step 1:* Start your computer (with diskette drive A empty).
- Step 2:* Once the computer is running, insert the Introductory Diskette into drive A.
- Step 3:* At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.
- Step 4:* When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.
- Step 5:* When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.

AIDS Information

Introductory
Diskette
Version 2.0

1. Start your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER

I N T R O D U C T I O N

Welcome to the interactive computer program called AIDS Information. This program is designed to provide up-to-date information about you and the fatal disease AIDS (Acquired Immune Deficiency Syndrome). The health information provided to you by this program could save your life.

Here is how the program works: First, the computer will ask you a series of questions about your personal background, behaviour and medical history. Then the program will calculate your chances of being infected with the AIDS virus and inform you about your present degree of risk. Then it will provide you with advice on what you can do to reduce your risk of future infection, based on the details of your own lifestyle and history. Finally, it will give you the chance to ask questions or to make comments.

Press ENTER to continue or press ESCAPE for Menu Options.

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

3) Decrypt your files.

You will receive your decrypted password file and a program called 'Spock'.
Download these both to the same place and run Spock.
Spock reads in your decrypted password file and uses it to decrypt all of the
affected files on your computer.

> IMPORTANT !

The password is unique to this infection.

Using an old password or one from another machine will result in corrupted files.

Corrupted files cannot be retrieved.

Don't around.

4) Breathe.

WAVE LONG

AND PROSEPER

Rensenware WARNING!

WARNING!

Your system have been encrypted by Rensenware!



What the HELL is it?

Minamitsu "The Captain" Murasa encrypted your precious data like documents, musics, pictures, and some kinda project files. it can't be recovered without this application because they are encrypted with highly strong encryption algorithm, using random key.

How can I recover my files?

That's easy. You just play TH12 ~ Undefined Fantastic Object and score over 0.2 billion in LUNATIC level. this application will detect TH12 process and score automatically. DO NOT TRY CHEATING OR TEMPRINATE THIS APPLICATION IF YOU DON'T WANT TO BLOW UP THE ENCRYPTION KEY!

Status

TH12 Process Status : Not Found

Score : TH12 Not Started

Decryption : Not Approved!

름	수정한 날짜	유형	크기
원본 문서.doc.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	24KB
원본 문서.hwp.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	16KB
원본 문서.pdf.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	21KB
원본 문서.ppt.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	312KB
원본 문서.rtf	2017-01-27 오후...	서식있는 텍스트(...	10KB
원본 문서.txt.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	2KB
원본 문서.xlsx.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	9KB
원본 사진.bmp	2017-01-27 오후...	BMP 파일	1,075KB
원본 사진.jpg.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	152KB
원본 사진.png.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	35KB
원본 압축.zip.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	8,063KB
원본 음악.mp3.RENSENWARE	2017-04-07 오전...	RENSENWARE 파일	6,768KB



Date modified	Type	Size
8/16/2009 3:19 PM	File folder	
8/16/2009 3:19 PM	File folder	
4/8/2017 4:43 PM	File folder	
8/1/2009 12:26 AM	Application	88 KB
7/25/2009 5:12 AM	Application	89 KB
4/8/2017 11:18 PM	RENSENWARE File	1 KB
4/8/2017 11:18 PM	RENSENWARE File	1 KB
4/8/2017 11:18 PM	RENSENWARE File	2 KB
4/8/2017 11:11 PM	DAT File	18 KB
4/8/2017 11:19 PM	CFG File	1 KB
8/1/2009 12:50 AM	DAT File	30,587 KB
8/1/2009 4:03 AM	Application	720 KB
7/28/2009 6:06 AM	DAT File	399,248 KB
4/8/2017 11:18 PM	RENSENWARE File	16 KB

th12.exe Date modified: 8/1/2009 4:03 AM Date created: 4/8/2017 4:43 PM
 Application Size: 720 KB

RENSENWARE WARNING!

WARNING!

Your system have been encrypted by Rense

What the HELL is it?

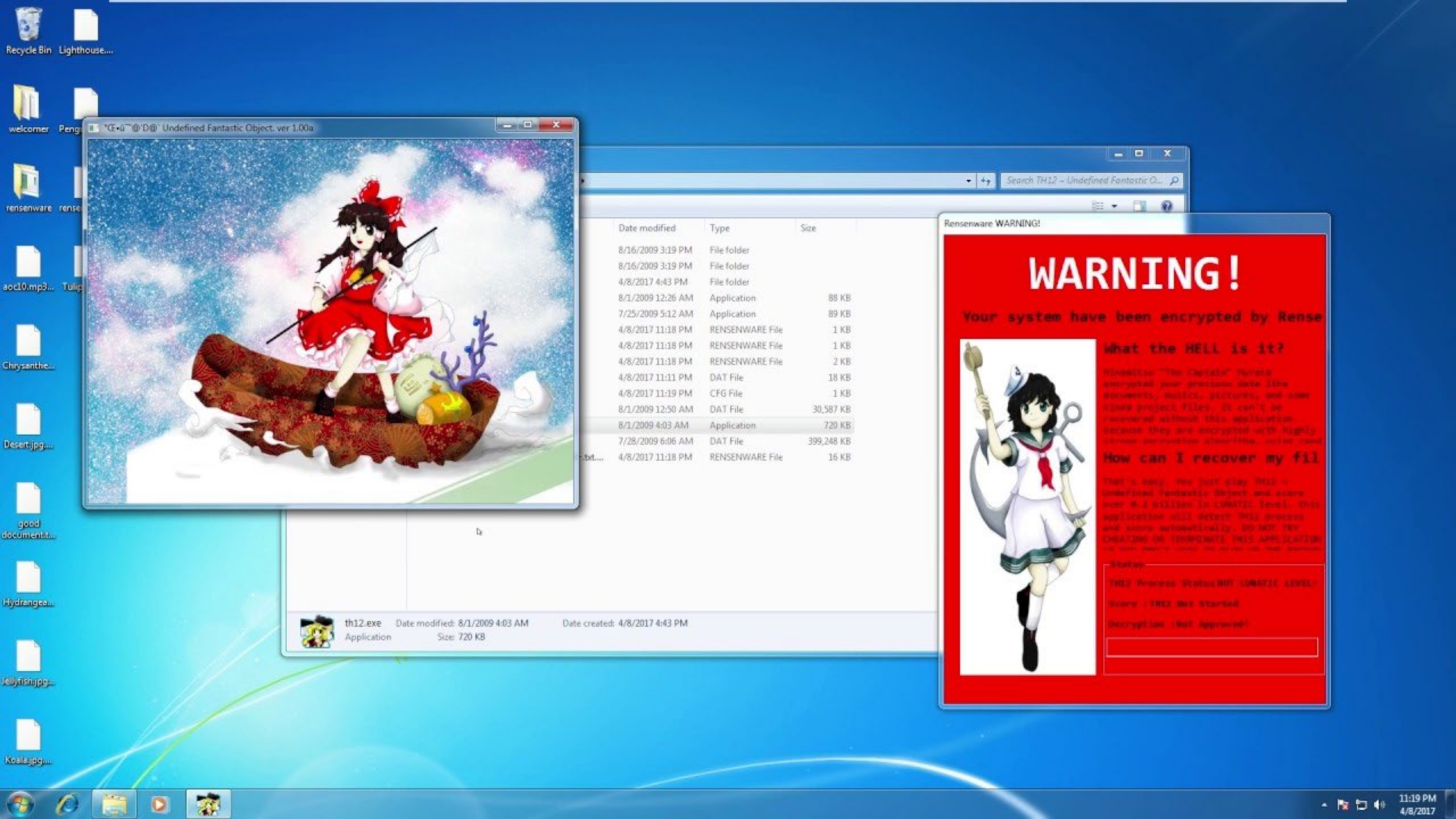
Reneware "The Captain" Rense encrypted your precious data like documents, music, pictures, and even some project files. It can't be recovered without this application because they are encrypted with highly advanced encryption algorithms. What can I do?

How can I recover my files?

That's easy. You just play TH12 - Undefined Fantastic Object and score over 8.1 million in UNLIMITED level. This application will detect TH12 process and score automatically. DO NOT TRY CHEATING OR TEMPERATE THIS APPLICATION OR YOU WILL LOSE THE DATA ON THE SYSTEM.

Status:

TH12 Process Status: NOT UNLIMITED LEVEL
 Score : TH12 Not Started
 Decryption : Not Approved!



Merry X-Mas!

MERRY
CHRISTMAS

ALL SERVER DATA ENCRYPTED!

03 days 23:57:30 0109

TIME AFTER ALL FILES WILL BE DELETED

YOUR ID

NOW YOU NEED TO PAY TO RECOVER YOUR DATA
AFTER MONEY TRANSFER YOU WILL RECIEVE THE DECRYPTOR

CONTACTS

TELEGRAM @comodosecurity
EMAIL comodosec@yandex.com

Any attempts to return your files with the third-party tools can be fatal for your encrypted files!
The most part of the third-party software change data within the encrypted file to restore it but
this causes damage to the files.

Finally it will be impossible to decrypt your files! There are several plain steps to restore your
files but if you do not follow them we will not be able to help you!

Merry X-Mas!

COMODO
comodo group property



YOUR CLIENT-ID: 9608CC35B9C3568A9ED34209EEB7AC2B

YOUR FILES ARE ENCRYPTED!

Discovered a serious vulnerability in your network security.
No data was stolen and no one will be able to do it while they are encrypted.
For you we have automatic decryptor and instructions for remediation.

To restore files and retrieve decryptor contact us

TELEGRAM @comodosecurity
EMAIL comodosec@india.com

ALL FILES WILL BE DESTROYED AFTER:

06 days 05:58:51 0434

Attention!

Do not attempt to remove the program or run the anti-virus tools
Attempts to self-decrypting files will result in the loss of your data
Any attempts to return your files with the third-party tools will be fatal

Your computer files have been encrypted. Your photos, videos,
But, don't worry! I have them, yet.
You have 24 hours to pay 150 Bitcoins to get the decryption key.
Every hour files will be deleted in amount every hour.
After 72 hours all the files will be deleted.

If you do not have Bitcoins, go to the website localbitcoins.com
Purchase 150 American Dollars worth of Bitcoins or .4 BTC.
Send to the Bitcoin address: [1A1zP1eP5QGefi2DMPTfTL5SLmv7Dicf](https://blockchain.info/address/1A1zP1eP5QGefi2DMPTfTL5SLmv7Dicf)
Within two minutes of payment your computer files will be decrypted.
Try anything funny and I will delete your files. I have several safety measures.
As soon as the payment is received the crypted files will be decrypted.

Thank you



**You've been
locked out of
your data...**



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

**You've been
locked out of
your company...**



**...and the locks
can't be broken**



A photograph of a computer monitor displaying a ransomware message in a terminal window. The text is white on a black background. The message reads: "You Hacked, ALL Data Encrypted, Contact For Key(crypton27@yandex.com) ID:681 ,Enter Key: Missing operating system_". The monitor is slightly tilted, and the background shows a blurred office or home environment.

You Hacked, ALL Data Encrypted, Contact For Key(crypton27@yandex.com) ID:681 ,Enter
Key:
Missing operating system_

HURTIGRUTEN

Sorry, the website isn't working right now

In the meantime, keep exploring the Hurtigruten universe:

- See pictures from our destinations on [Instagram](#)
- Learn more about Hurtigruten cruises on [Youtube](#)
- Hunt the northern lights in [Svalbard](#)

Done < > AA travelex.co.uk

Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```

<!-- Web.Config Configuration File -->

<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configuration>

```

Hackney Menu ☰

Cyberattack on Council services

Due to the cyberattack, you may experience difficulty accessing online services, such as One Account and payments today. We're trying to fix this ASAP

GARMIN.

We are currently experiencing an outage that affects Garmin.com and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

🔒 Ransomware forced hospitals to cancel 2,800 operations and shut down systems

Graham Cluley | December 6, 2016 5:58 pm

Ransomware is a serious enough threat for most organisations, but just imagine if you're in the business of keeping people healthy and saving lives.

Read more in my article on the Hot for Security blog.

[Read more...](#)



🔒 Ransomware hits San Francisco transport system. Free rides for all as \$73,000 demanded

Graham Cluley | November 28, 2016 10:37 am

San Francisco's transport system, known as Muni, was hit hard by a ransomware attack this weekend that forced the network to offer free rides to passengers.

Read more in my article on the Tripwire State of Security blog.

[Read more...](#)



🔒 Ransomware forces hospital networks to shut down, resort to paper

Graham Cluley | March 29, 2016 10:24 am

A strain of ransomware has infected the computer systems of MedStar Health, a healthcare provider that operates ten hospitals across the Washington DC and Baltimore region.

Read more in my article on the Tripwire State of Security blog.

[Read more...](#)



Hackers demand \$3.6 million ransom for return of hospital's data

David Bisson | February 16, 2016 10:20 am

Hackers are demanding a ransom payment of \$3.6 million following an attack against a Southern California hospital.

David Bisson reports.

[Read more...](#)



Major US oil pipeline shut down after ransomware attack

Finger of suspicion pointed towards DarkSide extortion gang rather than state-sponsored attackers.



Graham Cluley • [@gcluley](#)

12:14 pm, May 10, 2021



A ransomware attack has caused the shutdown of one of the largest oil pipelines in the United States.

The 5,500 miles of Colonial Pipeline, which carry over 100 million gallons of fuel every day, from Houston, Texas to the New York Harbor, has been offline since May 7 [according to the company which manages it](#):

Ooops, your important files are

you see this text, but don't see the "Wana
your antivirus removed the decrypt soft
om your computer.

you need your files you have to run the d
e find an application file named "@wana
older or restore from the antivirus qua

BOARDWAY

the heart of the nation
In remembrance of His Majesty
King Bhumibol Adulyadej



ก. วิทย์
Withhayu Rd.

DAILY NEWS
NEW YORK'S HOMETOWN NEWSPAPER

Tapes & leaks
TRUMP THREATENS COMEY - PAGES 6-7

COMING SUNDAY
SPECIAL TRIBUTE TO YANKEES GREAT DEREK JETER

HISTORY

GLOBAL HACK HORROR

- Ransom malware hits 100 countries
- 'Shadow Brokers' swiped NSA code
- British health care system crippled

PAGE 5

DAILY Mirror FIGHTING FOR YOU

Glossy 7-day TV mag

X Factor in secret talks to sign up Mariah

HEALTH SERVICE CHAOS

Oops, your files have been encrypted!

What happened to My Computer?

How do I pay?

HACKERS HOLD NHS TO RANSOM

Ops axed, A&Es closed as IT systems are shut down in global cyber attack

THE Sun 40p

STARTS TODAY

HOLS FROM £15

BAT'S WAY TO DO IT!

OLA-LA!
Sexy star's Strictly Sun Dancing

UK'S BIGGEST CYBER BREACH

NATIONAL HACKED SERVICE

- Scores of hospitals hit
- Attackers want ransom

60p

Weekend

Huge NHS cyber attack paralyses hospitals

- Ambulances diverted, patients told not to come to A&E, surgery cancelled
- Staff turn to pen and paper after computers and phone lines in lockdown
- At least 74 countries hit by mass ransomware infection

Little chefs
Top family recipes to cook together - with new Saturday Kitchen host Matt Tebbutt

Brace yourself!
It's Eurovision, the Brexit edition!

Bloody Sunday prosecutors consider charging 18 soldiers

INQUIRITOR TV GUIDE CULTURE WEEKEND MONEY

DAILY EXPRESS

FREE ICE CREAM FOR EVERY READER

FREE LAVENDER PLANTS FOR EVERY READER

NOW 20p

NHS CHAOS AFTER HACKER ATTACK

Patients hit as computer crooks demand ransom

80F and thunderstorms ...Britain gets tropical

Adventures made easy

Escorted tours

cosmos

Cruses

Exotic beach holidays

Daily Mail

FREE INSIDE Healthy Gut Diet Magazine

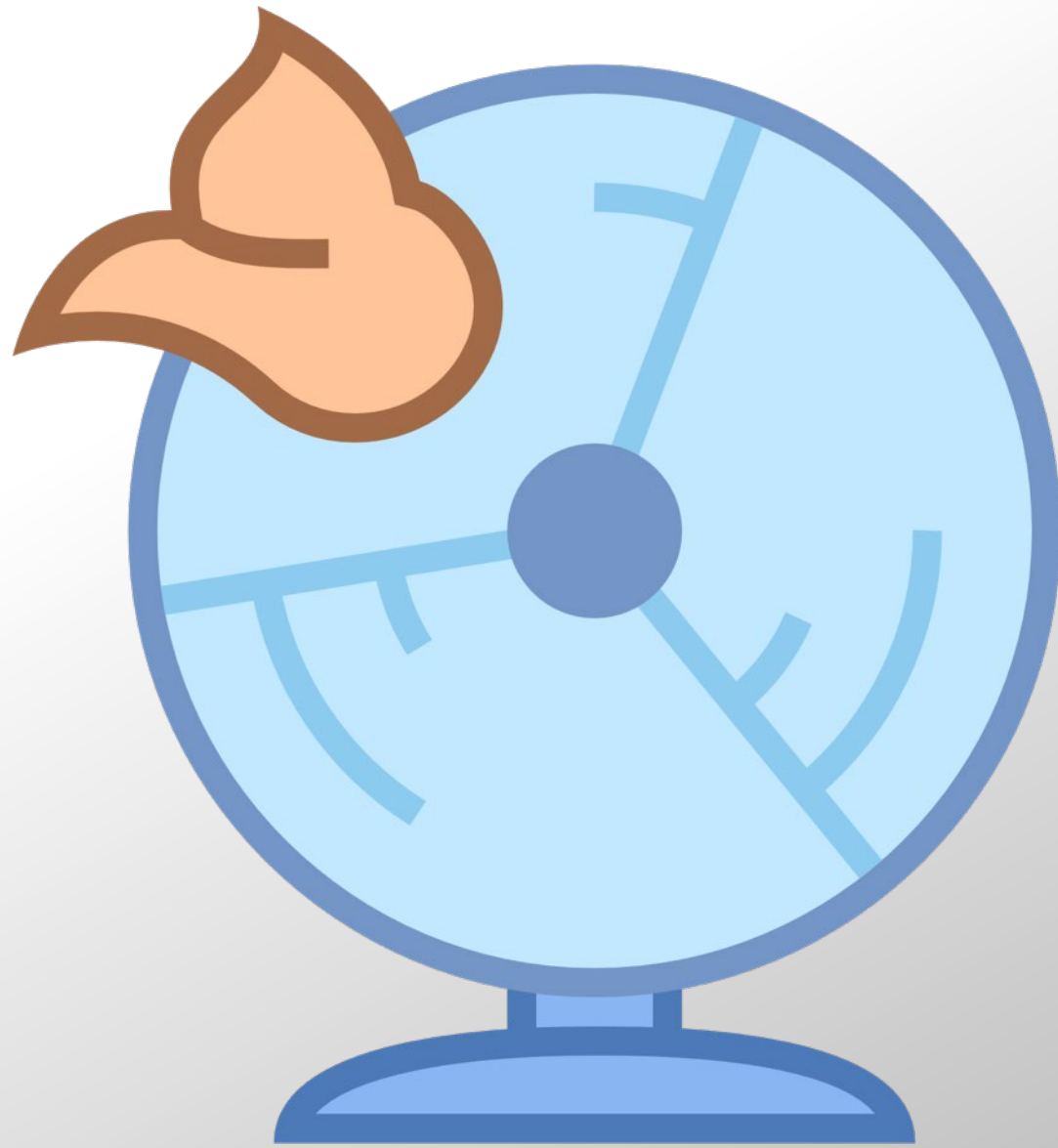
Fight disease and lose weight naturally

By 5:2 diet creator Dr Michael Mosley

Hospitals held to ransom ++ Operations cancelled ++ Patients turned away from A&E ++ But why WERE warnings ignored?

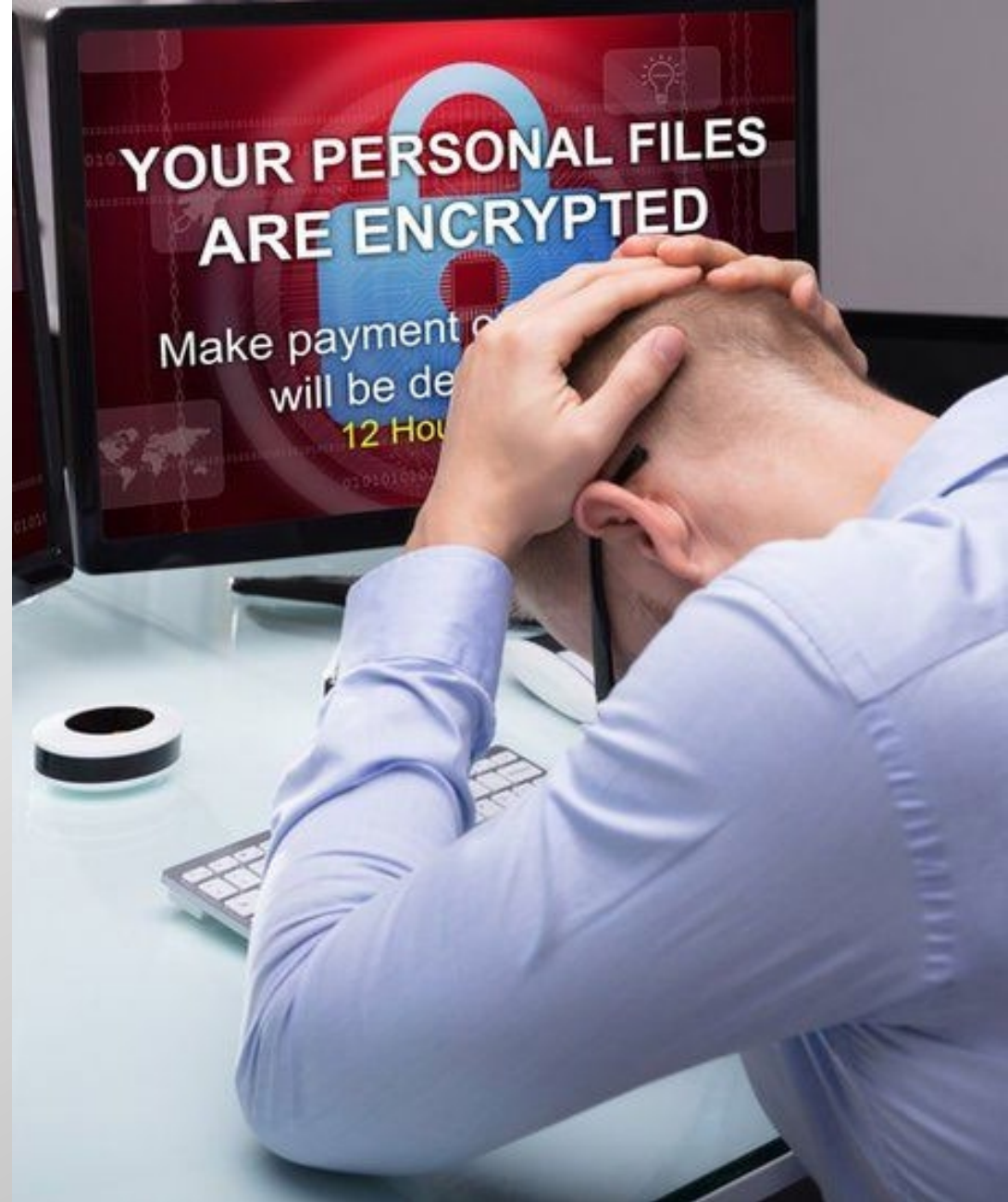
CYBER HACKERS CRIPPLE THE NHS

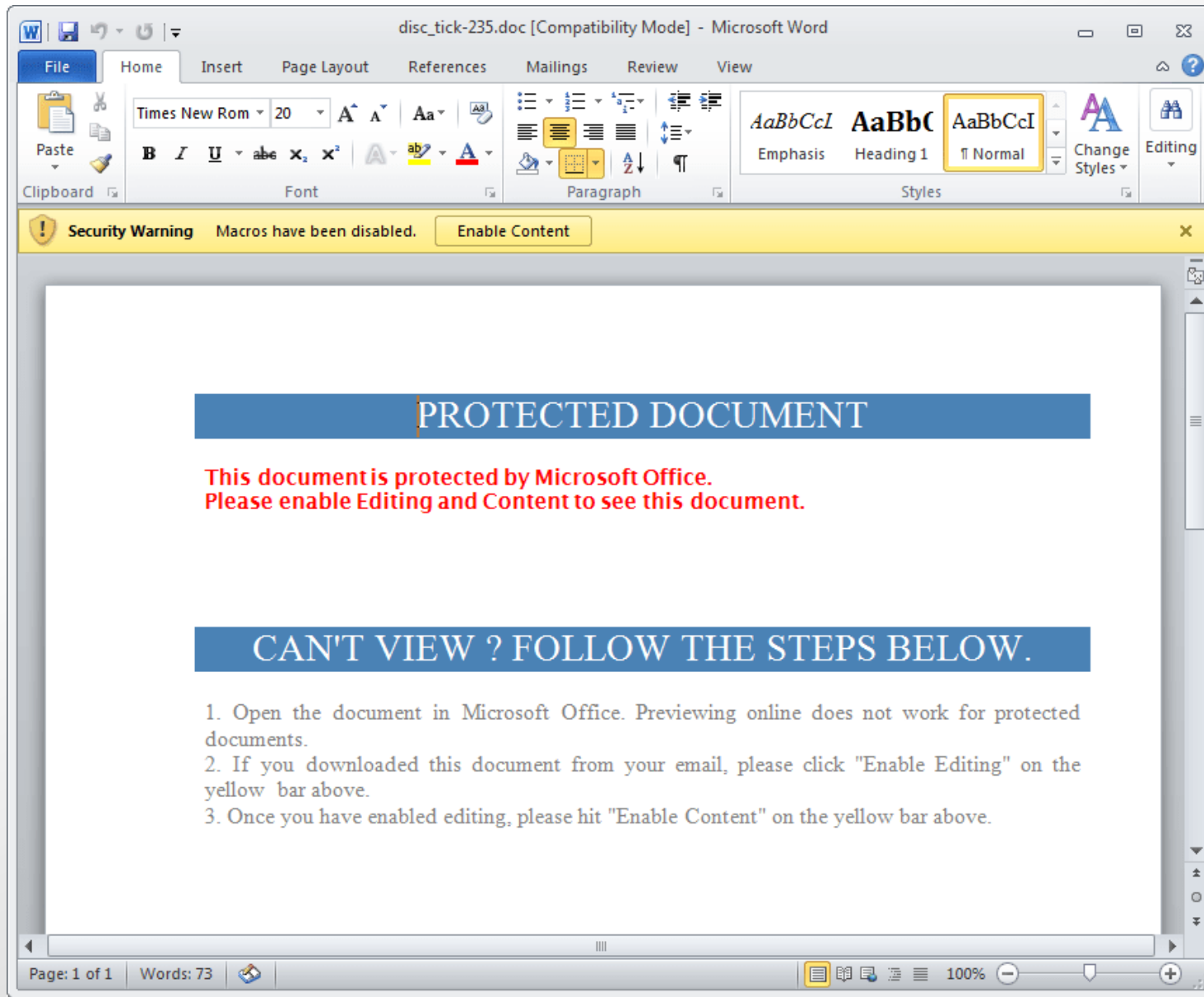
Hospitals held to ransom ++ Operations cancelled ++ Patients turned away from A&E ++ But why WERE warnings ignored?



Ransomware:

How do you get hit by it?





Important Message From American Express



○ **American Express** <admin@americanexpress-supportcenter.ml>

○ [REDACTED]

Monday, April 8, 2019 at 7:13 AM

[Show Details](#)



AMEXPDF (1).pdf

107.1 KB



[Download All](#)



[Preview All](#)

Dear American Express User:

Attached is a secured PDF file from American Express. View to reconfirm your account information to avoid termination.

Sincerely,

American Express Customer Service.

From: [REDACTED]
Sent: Thursday, November 22, 2018 12:18:30 PM
To: update@sharepoint.ms
Subject: Notification - Review Doc

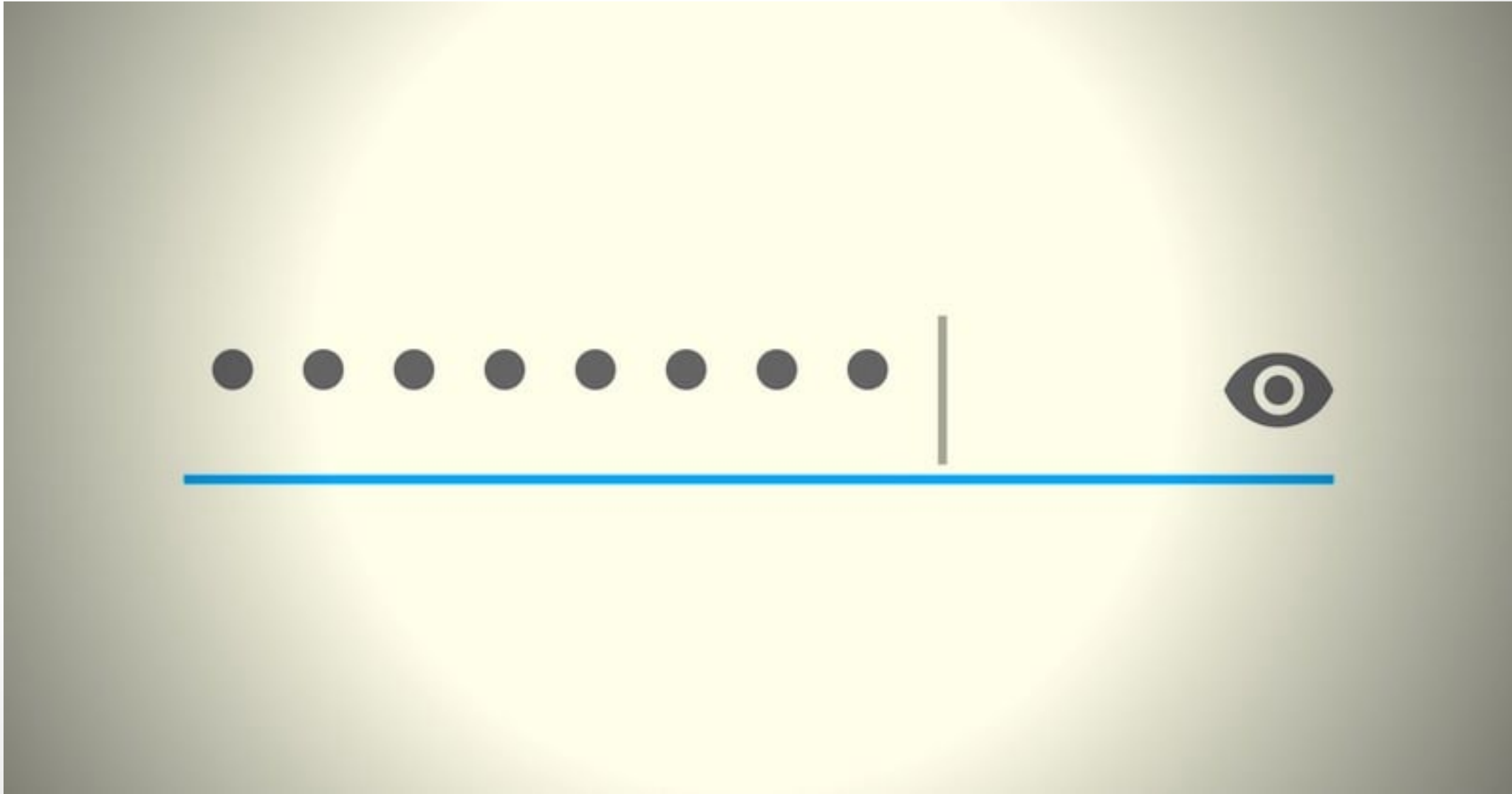
You have received a new shared document on OneDrive and it is said to be important

[Click Here](#)

Your document is ready!



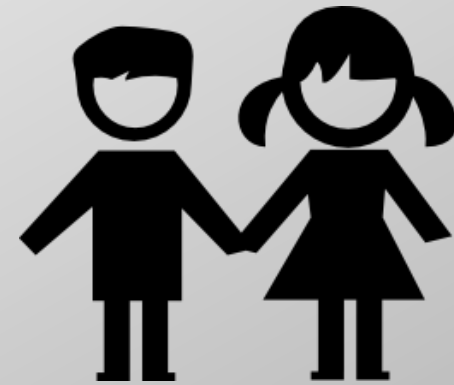
If you are having trouble signing the document, please visit the [Help with Signing](#) page on our Support Center.

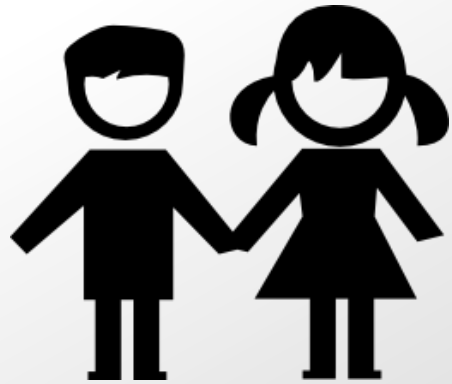




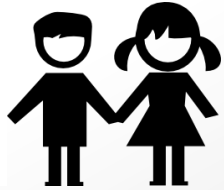


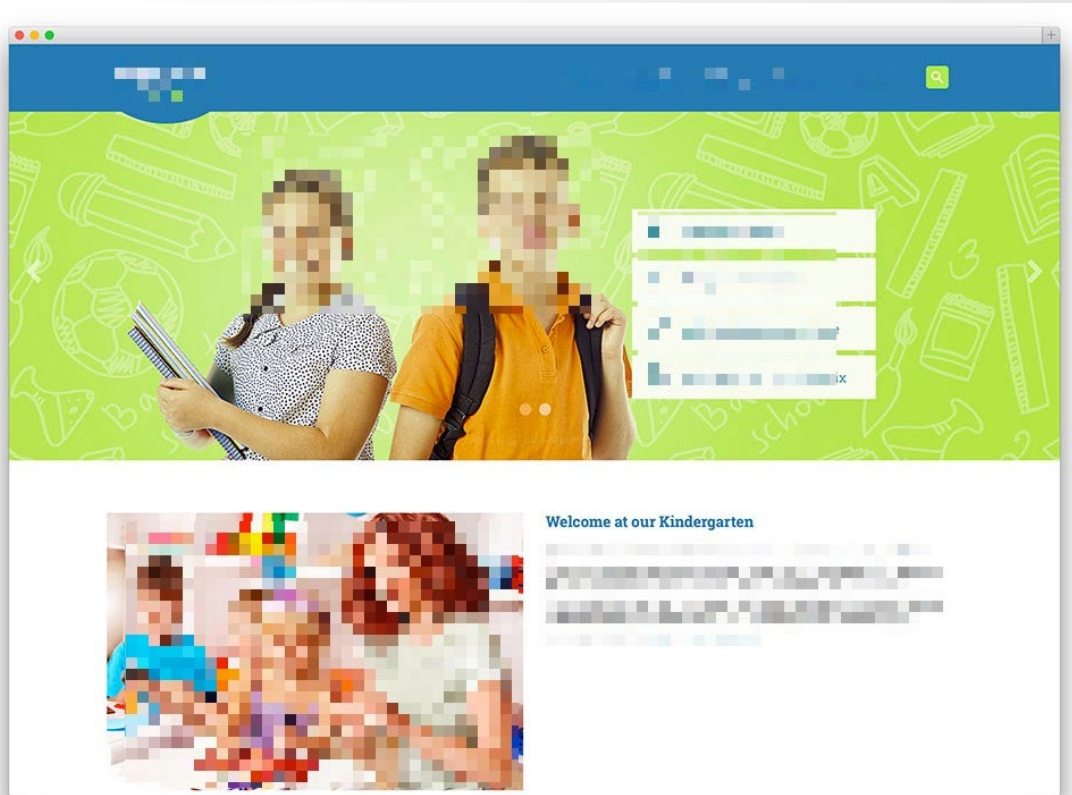
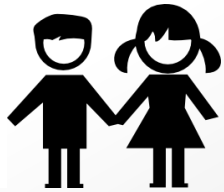


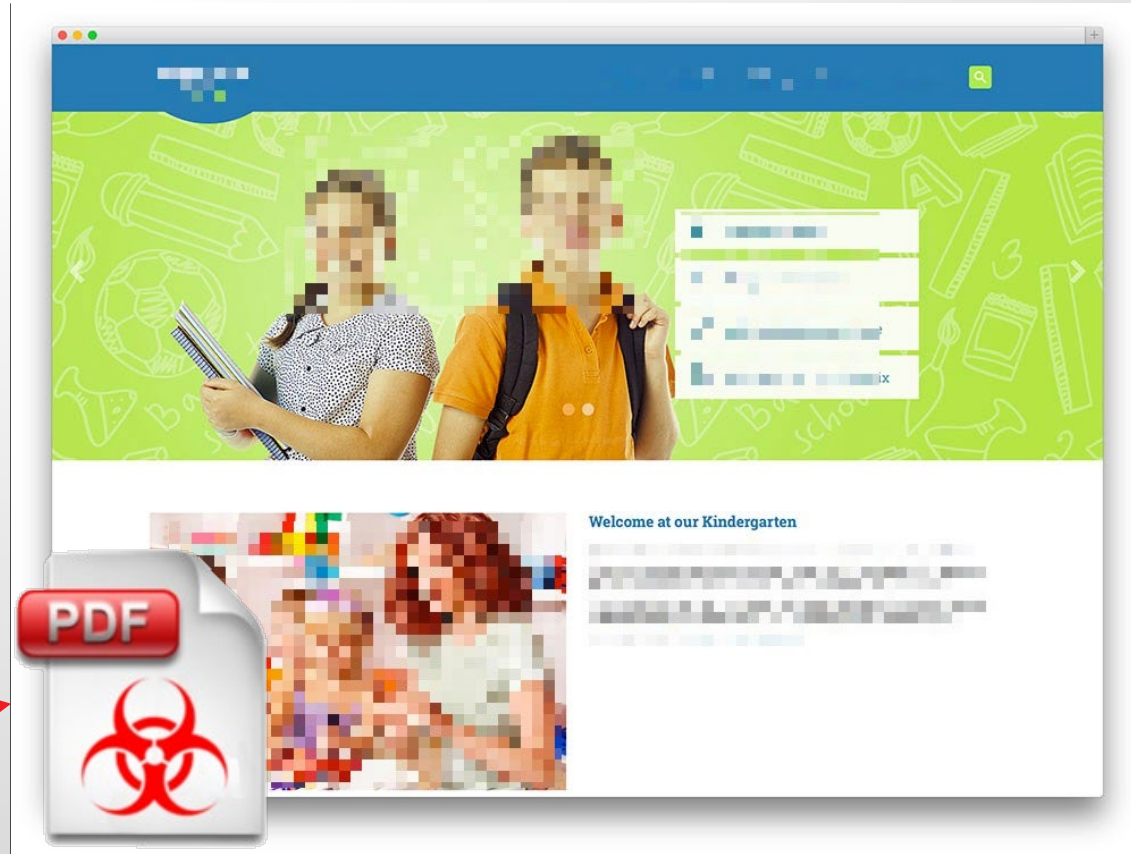
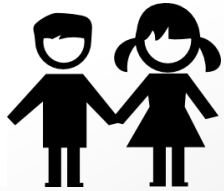


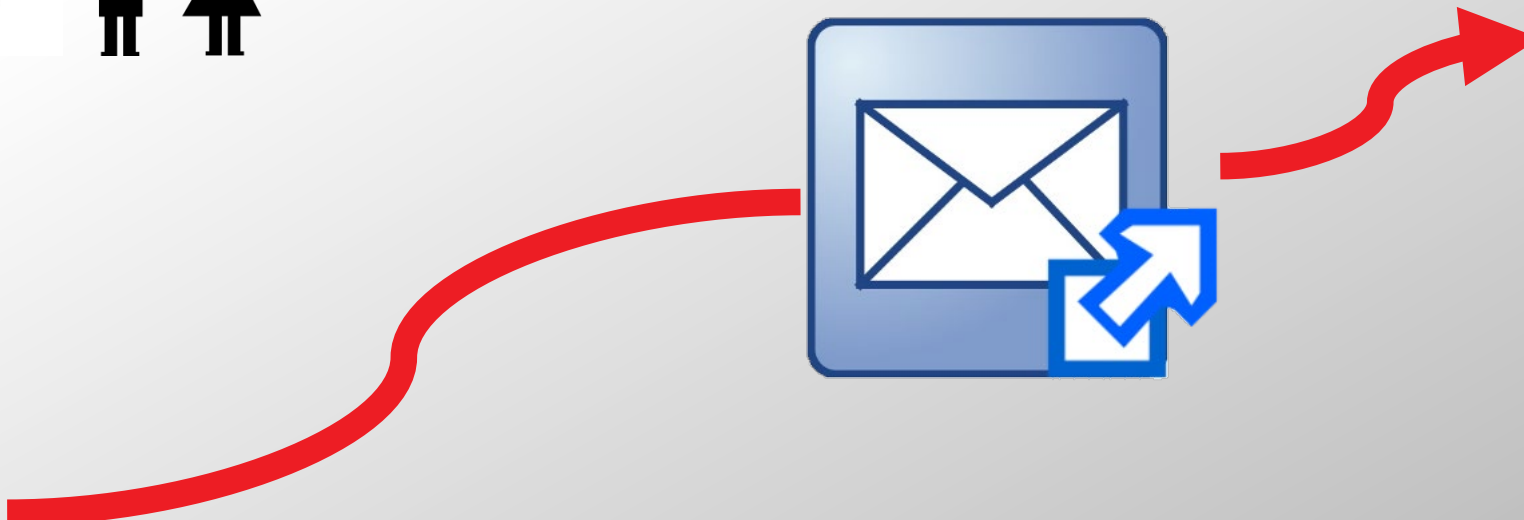
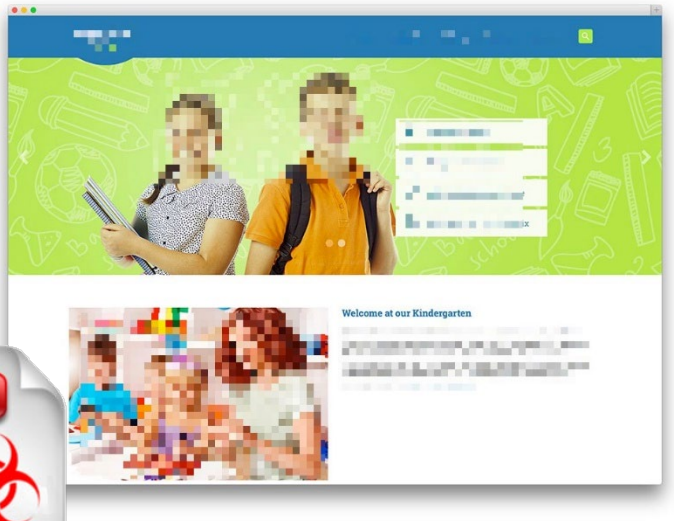
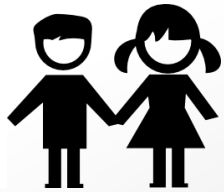


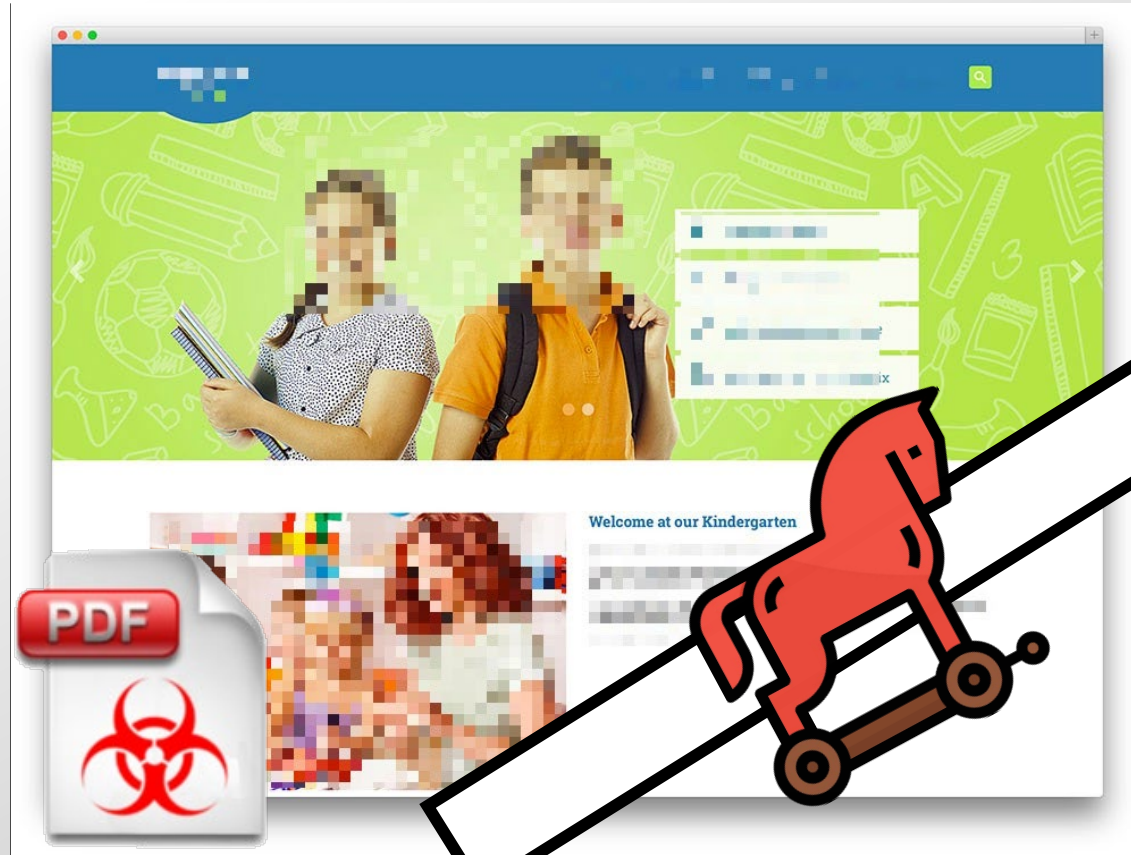
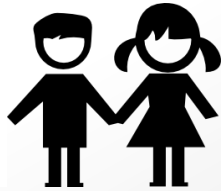








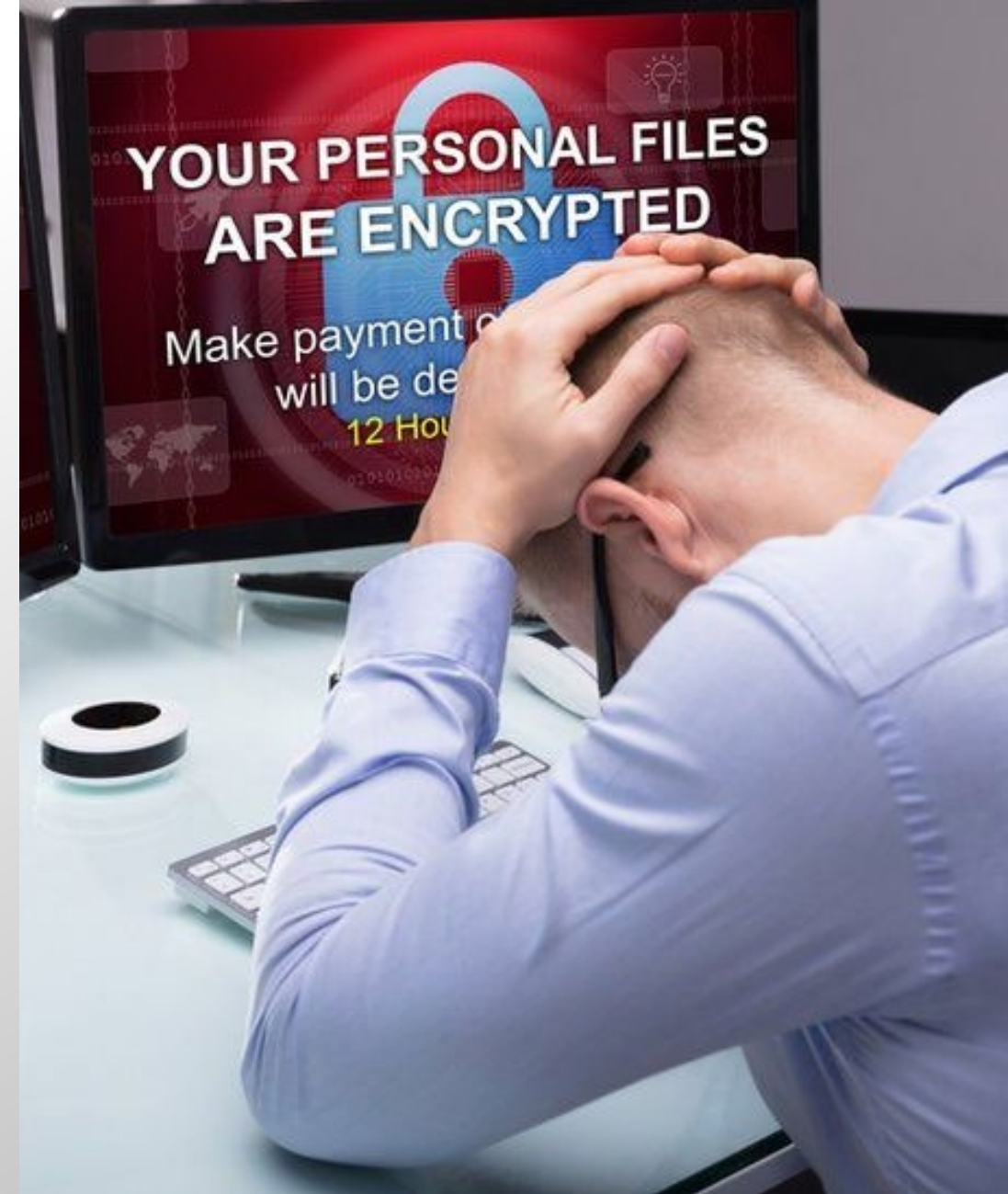






Ransomware:

Who is behind these attacks?





Ransomware gangs

REvil

Babuk

DarkMatter

DarkSide

Ryuk

Hello Kitty

Clop


Conti

Ragnar Locker

Evil Corp / Hades

Hades ransomware

← → ↻ 🏠 🔍 Search



Hades

ransomware.

Contact Us

We have hacked your network, downloaded and encrypted your data.

You can recover your data and prevent data leakage to the public.

For further details contact us via TOX messenger:

2F5338DABD40348C71D858459FE7B [REDACTED]

Attention! Your documents, photos, databases, and other important files have been encrypted!

The only way to decrypt your files, is to buy the private key from us.

You can decrypt one of your files for free, as a proof that we have the method to decrypt the rest of your data.

In order to receive the private key contact us via email:

getmyfilesback@airmail.cc

Remember to hurry up, as your email address may not be available for very long.
Buying the key immediatly will guarantee that 100% of your files will be restored.

Below you will see a big base64 blob, you will need to email us and copy this blob to us.
you can click on it, and it will be copied into the clipboard.

If you have troubles copying it, just send us the file you are currently reading, as an attachment.

Base64:

U1ihwTdfE7tvRrNEfMGvCz1lhw7o5THt5dI An63TORTBde1slmKndI VwRi3T07YF0WQWd2zOngVdn8m3STwDIdGm9QW4PH1wdI lD207+YRMHfCe10PkSk9yT0rUeP1TulVpTvPYc1YwR01e1YC /oDRV7TAVTgh/H8z-iK10Dl III DFU9+2uSDSAerTVic890d9HWI P9

Your computer have been infected!



Your documents, photos, databases and other important files **encrypted**



To **decrypt your files** you need to buy our special software - *2r6s1t3-Decryptor*



You can do it right now. **Follow the instructions below.** But remember that you do not have much time

2r6s1t3-Decryptor costs

You have **2 days, 23:59:30**

* If you do not pay on time, the price will be doubled

* Time ends on **May 1, 19:48:07**

Current price

0.47217028 btc
≈ 2,500 USD

After time ends

0.94434056 btc
≈ 5,000 USD



Popcorn Time

Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **[1LEIPgvh6S9VEXWV2dZTytSRd7e9B1bWt3](#)**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in at 2 hours after payment made.

Restoring your files - The nasty way

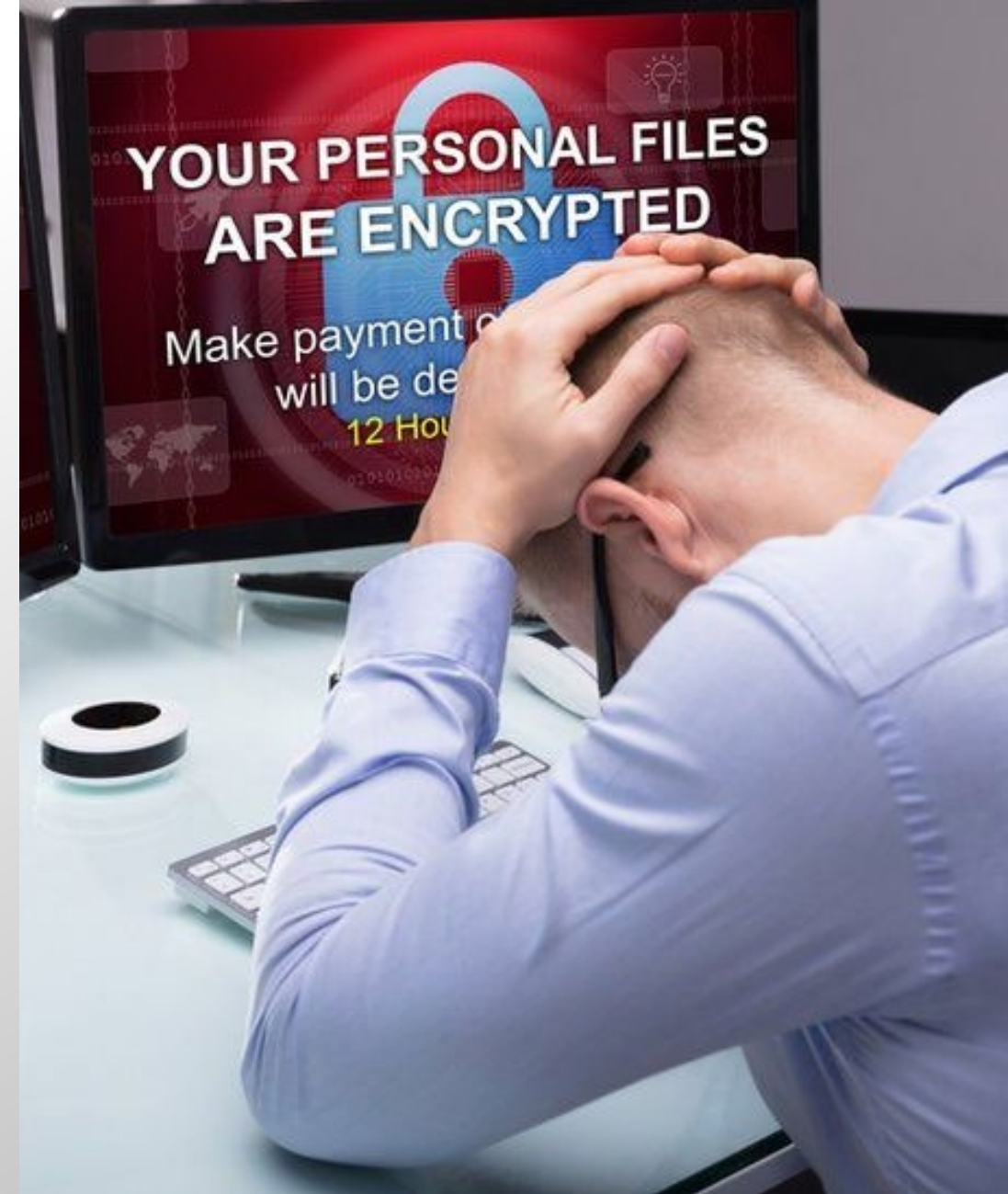
Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

<https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5>



Ransomware:

How does it extort millions of dollars?









New Clients

- CU Collections
- Academy Mortgage Corp.
- TechnoOrbits
- Talon Logistics
- Johnson Air Products
- Affordacare Urgent Care Clinic
- Woods And Woods
- Hotels Hoster
- Bouygues Construction
- North American Roofing

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!
P.S. We have the second domain: newsmaze.top.

Full dump



- Cutrale (oranges)
- Busch's Inc.
- L&F DISTRIBUTORS (LNF)
- City Of Pensacola
- Groupe Igréc, igrec.fr
- Baker Wotring LLP
- Saxbst & Bstco (all passwords)
- SALUMIFICIO FRATELLI
- BERETTA S.P.A. O
- Southwire (US, GA)

North American Roofing **Added**

<http://www.narooming.com/>

North American Roofing locked by maze's ransomware

 Cryptoransomware


 admin ,  902

[Read More >](#)

Lawyers network

All three companies of Lawyers network blocked

Maze locked already 3 law companies

 Cryptoransomware

Bouygues Construction

<https://www.bouygues-construction.com/>

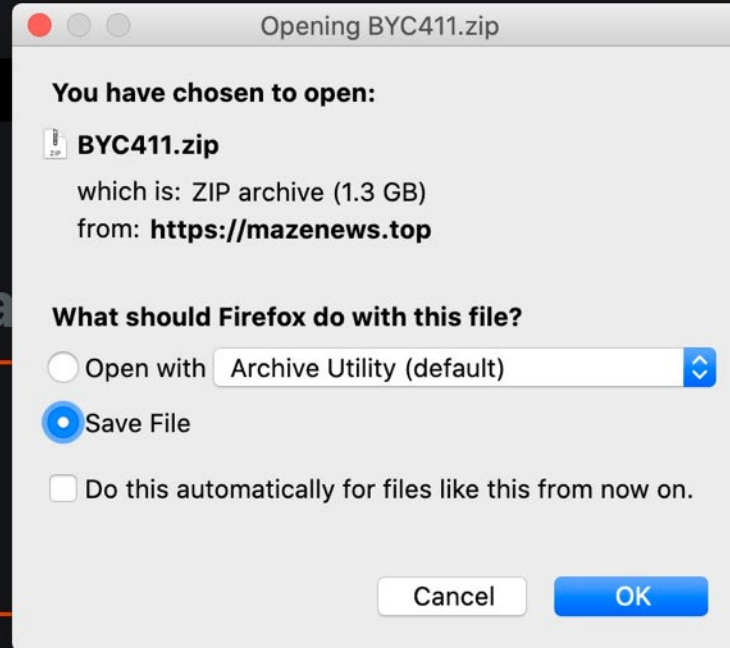
admin, Cryptoransomware,

Lock Date a

Lock date 30.01.2020

Proofs

BYCN.rar
BYC1.zip
BYC411.zip
BYC414.7z





Extorting the customers of hacked companies





Urgent Patient Advisory - Please Read Carefully

www.davisrhinoplasty.com/patient-advisory.html

RICHARD DAVIS MD FACS
THE CENTER FOR FACIAL RESTORATION

MIRAMAR, FLORIDA
(954) 442-5191

Home Meet Dr. Davis Rhinoplasty Other Facial Procedures Photo Gallery Testimonials Patient Info

Urgent Patient Advisory – Please Read Carefully

Dear Current or Former Patients of Richard E Davis MD FACS:

I am dismayed to report that in early November of 2019, The Center for Facial Restoration, Inc. (TCFFR) located in Miramar, Florida (Richard E. Davis MD FACS), was the victim of a criminal cyberattack. On November 8, 2019, I received an anonymous communication from cyber criminals stating that my "clinic's server (was) breached". The hackers claimed to have "the complete patient's data" for TCFFR that "can be publicly exposed or traded to third parties". They demanded a ransom negotiation, and as of November 29, 2019, about 15-20 patients have since contacted TCFFR to report individual ransom demands from the attackers threatening the public release of their photos and personal information unless unspecified ransom demands are negotiated and met.

On November 12, 2019, I filed a formal complaint with the FBI Cyber Crimes Center and two days later met with the FBI where they recorded detailed information regarding the cyberattack and ransom demands. The investigation is currently ongoing. The FBI requests that patients receiving

Philosophy & Technique

- Introduction
- Eyes Wide Open
- Open vs. Closed Rhinoplasty
- Structural vs. Excisional Rhinoplasty
- To Graft or Not to Graft
- The Importance of Nasal Skin
- Aging and the Nasal Skeleton
- Computer Imaging
- The Risks of Rhinoplasty
- Anesthesia Options
- Is Rhinoplasty Right for You?

Lähetä vastaus

Vastaamo.fi

■ Psykoterapiakeskus Vastaamo

ransom_man##HibGCf 2020-10-21 (Ke) 04:xx:yy X No.

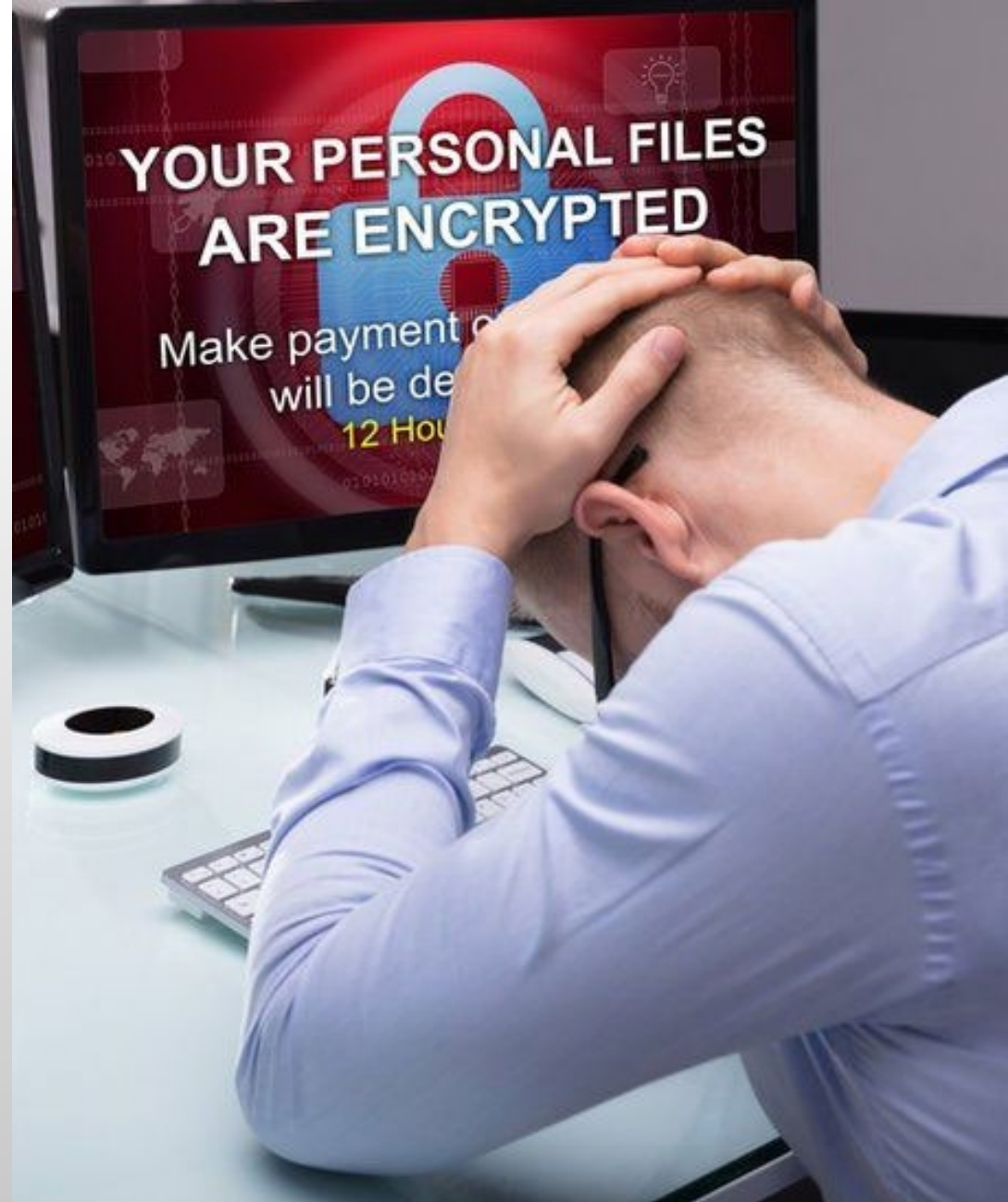
(8 KB 400x95 PNG)
>>18465 >>18476 >>18485 >>18494 >>18497 >>18563 >>18583 >>18855 >>18920 >>18923
>>18201 >>18264 >>18270 >>18272 >>18403 >>18420 >>18421
>>19040 >>19093 >>19103 >>19190 >>19192 >>19389

Hello Finnish colleagues.

We have hacked the psychotherapy clinic "vastaamo.fi" and taken tens of thousands of patient records including extremely sensitive session notes and social security numbers.

We requested a small payment of 40 bitcoins (nothing for a company with yearly revenues close to 20 million euros), but the CEO has stopped responding to our emails. We are now starting to gradually release their patient records, 100 entries every day.

Ransomware: Future trends in ransomware





More ransomware attacks on smartphones

CryDroid
v1.1



<https://github.com/thelinuxchoice/crydroid>

```
[::] Android Ransomware source code for researchers [::]  
[::] This code was sent to virustotal to prevent it [::]  
[::] from being used for malicious purposes. [::]
```

Usage of CryDroid is COMPLETE RESPONSABILITY of the END-USER
Developers assume no liability and are NOT responsible for
any misuse or damage caused by this program.

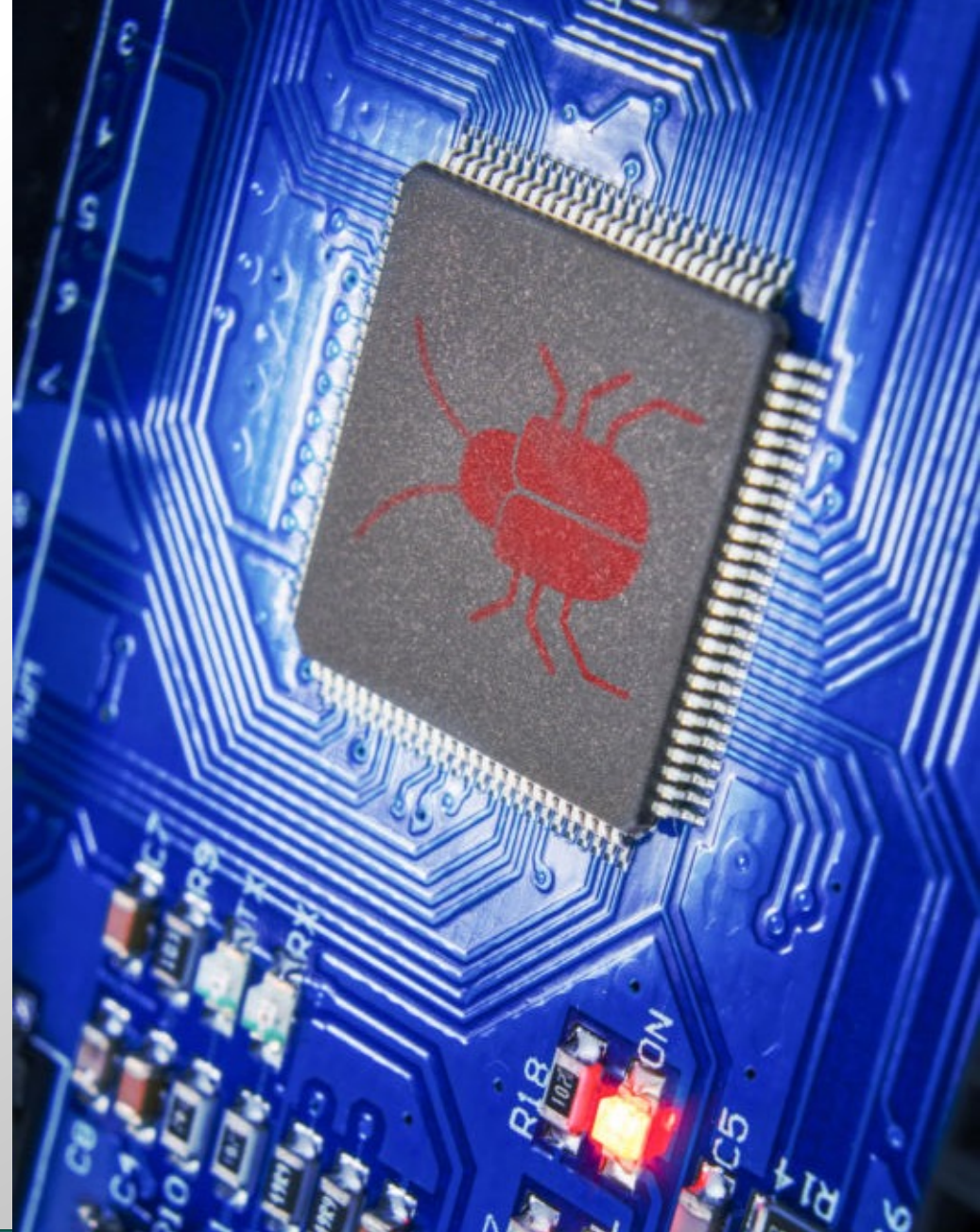
```
[1] Generate Crypter  
[2] Generate Decrypter
```

```
[+] Option: 1  
[+] Encryption Password:  
[+] Email to request rescue:  
[+] Crypter source code created. Build using Android Studio
```

Ransomware attacks on IoT devices

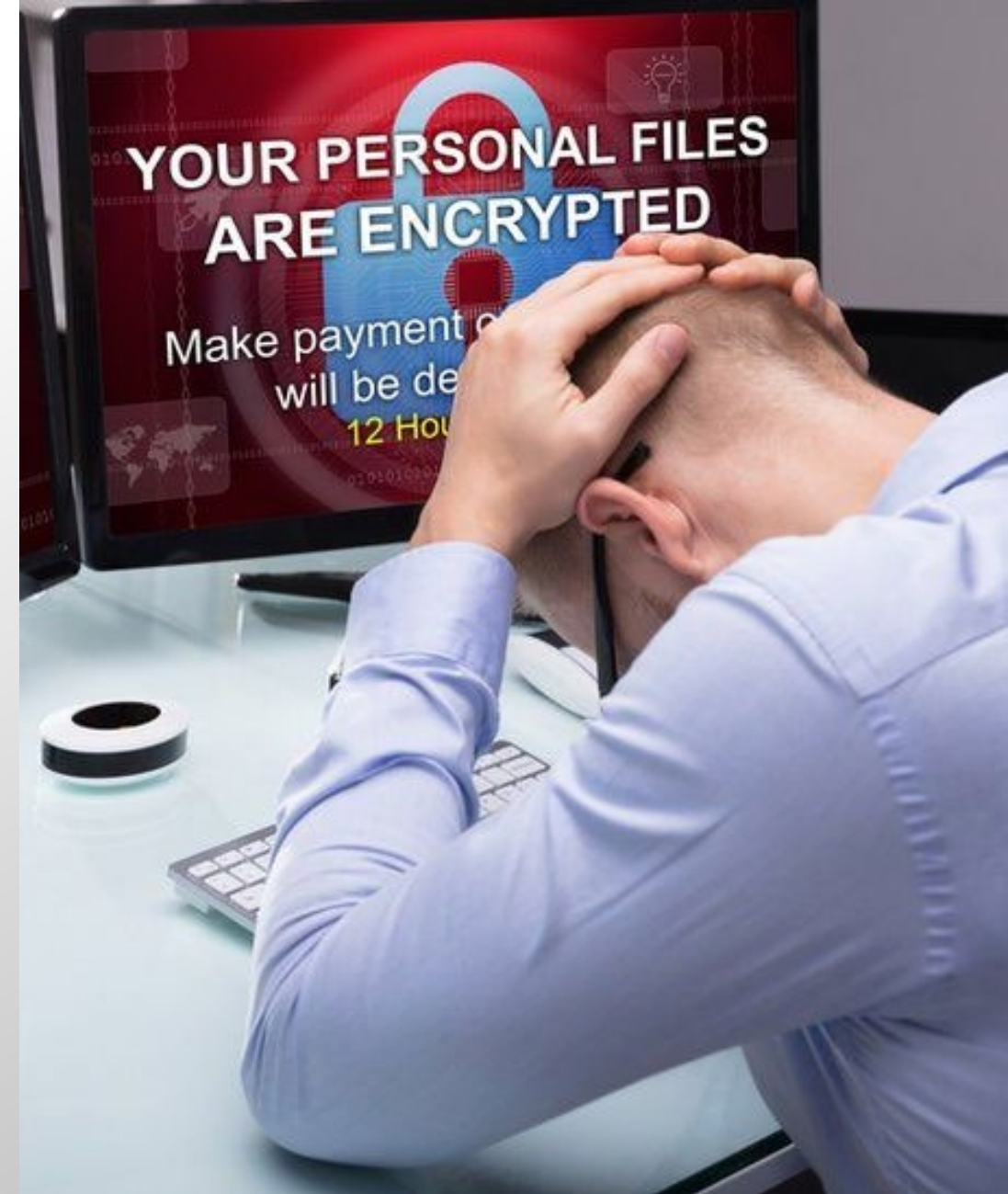


Ransomware threatening to brick your computer's hardware



Ransomware:

What can you do to prevent ransomware attacks?



Layered defence

- **Security software**
- **Password best practices**
- **Multi-factor authentication**
- **Vulnerability patching**
- **Encryption**
- **...and backups for recovery**



**Even if you do get hit, it
doesn't have to be a disaster**





Norsk Hydro
@NorskHydroASA



Mar 18 2019

Hilde Merete Aasheim appointed new CEO of Hydro: "I am honored, and I very much look forward to leading Hydro into the next chapter, together with 35,000 competent and engaged colleagues around the world," says [@AasheimHilde](#). hydro.com/en/press-room/...



6:11 AM · Mar 18, 2019 · [TweetDeck](#)

Hilde Merete Aasheim appointed new CEO of Hydro: "I am honored, and I very much look forward to leading Hydro into the next chapter, together with 35,000 competent and engaged colleagues around the world," says [@AasheimHilde](#). hydro.com/en/press-room/...



6:11 AM · Mar 18, 2019 · [TweetDeck](#)

Hydro is currently under cyber-attack. Updates regarding the situation will be posted on Facebook: m.facebook.com/story.php?stor...

8:44 AM · Mar 19, 2019 · [Twitter for Android](#)

19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security



Norsk Hydro
@NorskHydroASA



Hydro is currently under cyber-attack. Updates regarding the situation will be posted on Facebook: m.facebook.com/story.php?stor...

8:44 AM · Mar 19, 2019 · [Twitter for Android](#)

Norsk Hydro refused to negotiate with their attackers

Became an example to businesses around the world about how to respond to an attack, and *improve* your image

**Should you pay the
ransom or not?**

**DON'T
PANIC**

Thank you

Graham Cluley
Independent security analyst
Host “Smashing Security” podcast



Security Tips



Security Tips



➤ Protect

- Advanced Email Threat Protection
- Multi-factor Authentication
- Advanced Email Encryption

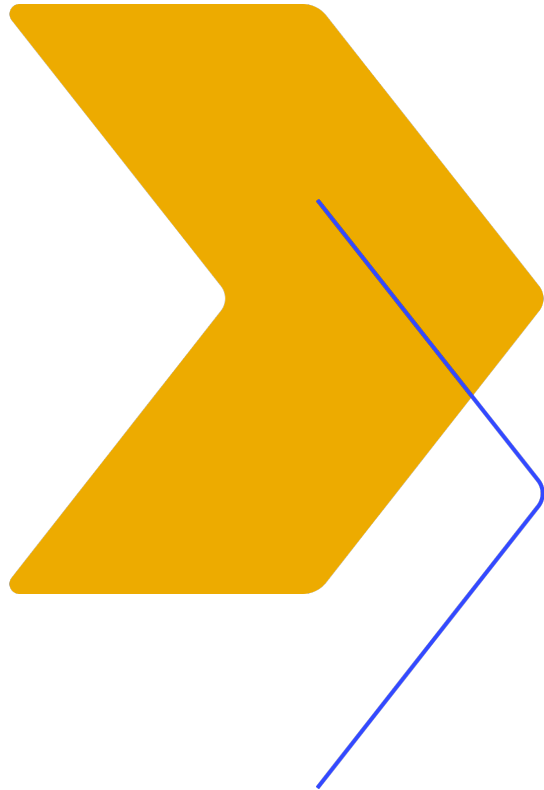
➤ Detect

- Security Audit
- Threat Analysis Team / Tools
- Data Loss Prevention Scanning

➤ Respond

- Threat Investigation / Analysis
- Vulnerability Remediation
- Backup and Recovery





Thank you.



Graham Cluley
Independent security analyst
Host “Smashing Security” podcast



Andrew Murphy
Director of Product Marketing

Questions?