



PROTECT
DETECT
RESPOND

Addressing the Dark Side of the Digital Economy: Protecting Yourself and Your Business

Oct 2021

Cybersecurity

 Wana Decrypt0r 2.0



Payment will be raised on

1/4/1970 01:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 01:00:00

Time Left

00:00:00:00

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
CMT from Monday to Friday

 **bitcoin**
ACCEPTED HERE

Send \$600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Check Payment

Decrypt

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

36 billion

compromised records in
2021H1

197 days average time
to discover a breach

88% of organizations
worldwide experienced
spear phishing attempts

109.000 Euros

average ransomware
extortion amount

Worsening **Threat** Landscape...



Number of cyber
attacks continues to
break records every
year



Ransomware attacks
have proven to be
quite **effective** for
attackers



Supply Chain attacks
compromise **thousands**
in a single blow



Major rise in number of
vulnerable devices on
the internet (ex IoT)
and overall **complexity**

Cyber attacks are ever-
more **sophisticated** and
professionalized.



Opening up to **remote
work** has enlarged the
attack surface

400,000 phishing sites are created each month

65% of people reuse password across multiple accounts

Google estimates it blocks **18 million** COVID-19 scam emails a day

bad bot traffic amounted to **25.6%** of all website traffic in 2020

... Cyber Security Challenges for Individuals

Password brute force & discovery



- *Top 20 passwords account for 10,3% of passwords*
- *Weak passwords are breakable in seconds.*
- *Hackers actively exploit password reuse*

Social engineering



- *Email phishing attacks spiked over 600% since the end of February 2020 due to pandemic*
- *Phishing, vishing, smishing were the most prevalent threat in 2020*

Malware attacks



- *Attackers scan the internet with millions of bots (compromised systems) looking for unpatched machines*
- *Machines that aren't patched are sitting ducks for hackers.*

PASSWORD LENGTH

POSSIBLE COMBINATIONS

TIME TO CRACK

S = SECONDS

H = HOURS

M = MINUTES

Y = YEARS

4	45697	< 1 S
5	1 188 1376	< 1 S
6	3089 15776	< 1 S
7	803 181 0176	~ 4 S
8	208827064576	~ 1.5 M
9	5429503678976	~ 45 M
10	1 41 1677095653376	~ 19 H
11	3670344486987780	~ .1 Y
* 12	95428956661682200	~ 1.5 Y
13	2481 15287320374E4	~ 39.3 Y
14	645099747032972E5	~ 1,022.8 Y
15	167725934228573E7	~ 26,592.8 Y
16	436087428994289E8	~ 691,412.1 Y
17	1 13382731538515E10	~ 17,976,714 Y
18	2947951020001390E10	~ 467,394,568 Y

93% of SOC's have problems filtering alarms adequately

More than **50%** of all incidents are false positives

70% of SOC analysts are overloaded with the volume of alerts

3.5 million unfilled cyber security jobs

... Cyber Security **Challenges** for Organizations



Low cyber security awareness.

*"it is often perceived that it **only** concerns IT related people".*



Inadequate protection for critical information.

*"organizations are **unaware** of the **importance** of the **data** and legal obligations"*



Lack of cybersecurity specialized **personnel** & expertise.

*"loss of security focus given that it is quite common that individuals **multitask** and may have **conflicting roles** assigned to them."*

Cybersecurity preparedness efforts entail **investments** from various aspects...



...such as **awareness** training, implementation of cybersecurity **controls** & engaging external **experts**.

1 million passwords
are stolen every week

One in three
breaches are caused by
unpatched vulnerabilities

5.6 Billion: annual
number of malware attacks
in 2020

1 in every **99** emails is a
phishing attack

Protecting Yourself

Passwords

Use password managers to handle *distinct*,
and *robust*, passwords across sites



Patch

Update your systems with the *latest* versions



Anti-virus

Use an *anti-malware* software and a *firewall*



Don't be fooled (phished)

Check the email address & the link before
you click



Look for wording and terminology

Avoid emails that insist you act now

Beware of bargains

Never supply any personal or financial
information and passwords to anyone

Strong Customer Authentication

Dual factor

(Two of the three factors)

Something
you **know**



- *Password*
- *PIN*

Something
you **have**



- *Phone*
- *Payment card*

Something
you **are**



- *Fingerprint*
- *Facial Recognition*

Payments
Strong Customer Authentication

Protecting your organization

- **people**: security awareness for employees, clients and suppliers.
- **infrastructure**: specialized security services that will help to prevent, detect and respond to incidents.
- **endpoints**: preventing attacks on the most common point of initial intrusion.
- **external exposure**: monitoring social networks, deep & dark web for intelligence.

SIBS CyberWatch provides expertise at all levels of Cyber Security Services, namely:

- Through its 24x7 **SOCs** (Security Operations Centers) supported on 20 security analysts monitoring all relevant events, processing alarms and ready to respond to incidents.
- With **EDR** (Endpoint Detection and Response) managing the detection of endpoint threats including management of personalized policies, user management and application blacklisting.
- Via its **CTI** (Cyber Threat Intel) identifying emerging global threats and alerting on new dangers through intelligence shared or found on the various webs and social networks

**Security
Operations
Center**

**Endpoint
Detection &
Response**

**Cyber
Threat
Intelligence**



SIBS[®]
CyberWatch

PROTECT
DETECT
RESPOND

www.sibs.com

The information contained in this document is owned by SIBS and cannot be copied, published or provided in whole or in part to third parties without SIBS' the prior consent.