UTSA SBDC
Center for Government Contracting
https://cgc.txsbdc.org
(210) 458-2458

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

CYBER AWARE
RANSOMWARE

Institute for Economic Development
The University of Texas at San Antonio

UTSA

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

- Cyber Risk and Environment Primer
- What is Ransomware
- SMB Ransomware
- Ransomware Risk Mitigation
- Under Attack
- Available Resources
- Wrap Up Final Q&A

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

RISK WILL NEVER BE ZERO….NEVER EVER, EVER

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

CYBERSECURITY ENVIRONMENT

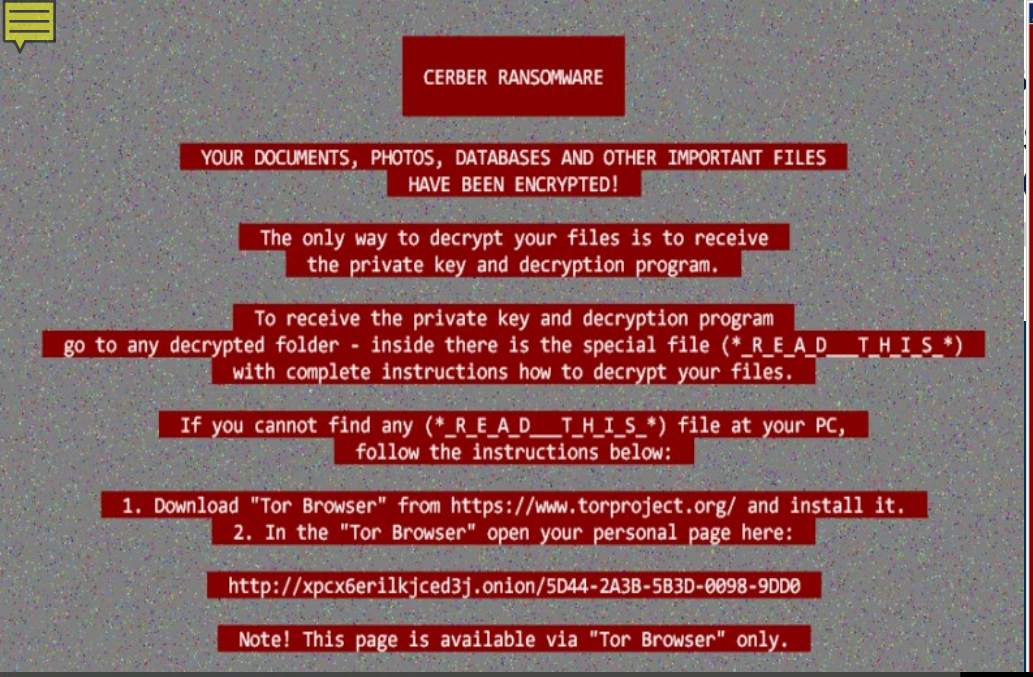
[EXPOSURE]

PHISHING is UP but RANSOMWARE IS ?

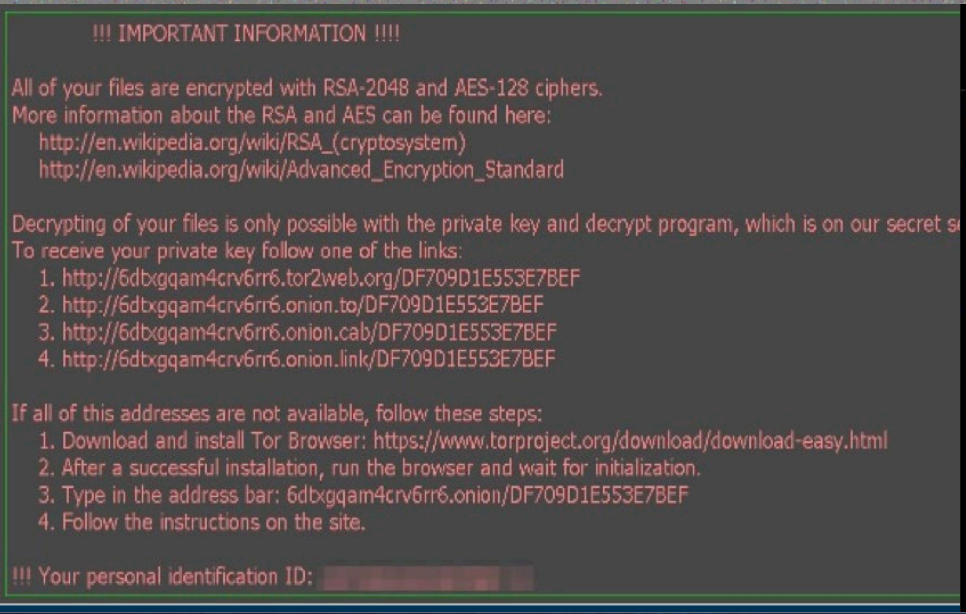
South-West Texas Border
Small Business
Development Center Network

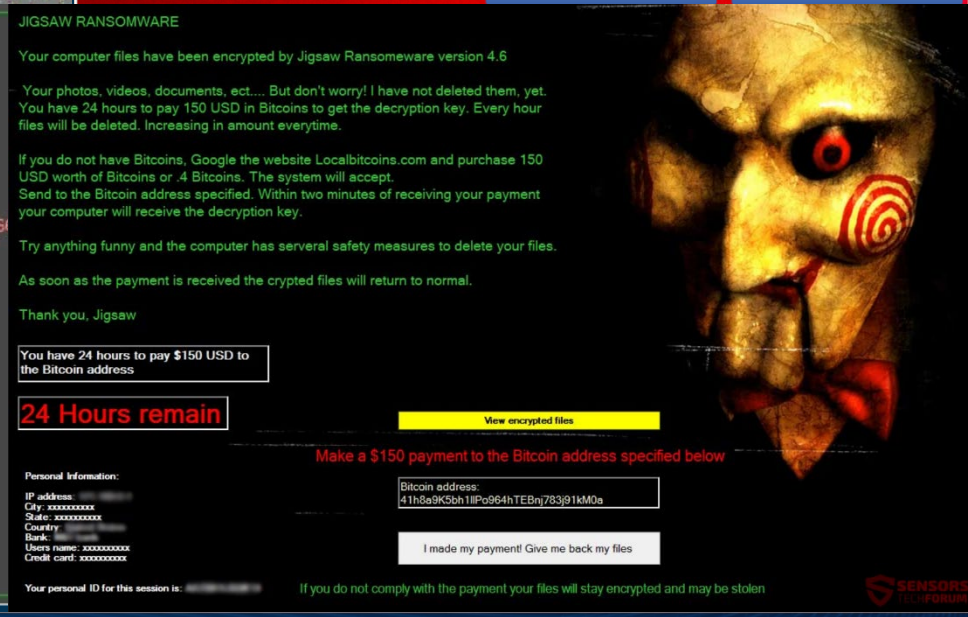
UTSA SBDC Center for Government Contracting

Ransomware is a type of malware cyber criminals use to deny access to data for the purpose of extortion.


CERBER RANSOMWARE
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt your files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*_R_E_A_D___T_H_I_S_*) with complete instructions how to decrypt your files.
If you cannot find any (*_R_E_A_D___T_H_I_S_*) file at your PC, follow the instructions below:
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://xpcx6erilkjced3j.onion/5D44-2A3B-5B3D-0098-9DD0
Note! This page is available via "Tor Browser" only.


CryptoLocker
Payment for private key
Choose a convenient payment method and click «Next»:
Bitcoin
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.
You have to send 0.5 BTC to Bitcoin address 1gVi7gzrnJEP3eZusZ5CYxvJTzHVKeFfH and specify the Transaction ID on the next page, which will be verified and confirmed.
Home Page
Getting started with Bitcoin
Private key will be destroyed on
11/24/2013
7:36 PM
Time left
71 : 58 : 56
<< Back
Next >>


!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret s
To receive your private key follow one of the links:
1. http://6dbxgqam4crv6rr6.tor2web.org/DF709D1E553E7BEF
2. http://6dbxgqam4crv6rr6.onion.to/DF709D1E553E7BEF
3. http://6dbxgqam4crv6rr6.onion.cab/DF709D1E553E7BEF
4. http://6dbxgqam4crv6rr6.onion.link/DF709D1E553E7BEF
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dbxgqam4crv6rr6.onion/DF709D1E553E7BEF
4. Follow the instructions on the site.
!!! Your personal identification ID:


JIGSAW RANSOMWARE
Your computer files have been encrypted by Jigsaw Ransomeware version 4.6
Your photos, videos, documents, ect.... But don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key. Every hour files will be deleted. Increasing in amount everytime.
If you do not have Bitcoins, Google the website Localbitcoins.com and purchase 150 USD worth of Bitcoins or .4 Bitcoins. The system will accept.
Send to the Bitcoin address specified. Within two minutes of receiving your payment your computer will receive the decryption key.
Try anything funny and the computer has serveral safety measures to delete your files.
As soon as the payment is received the crypted files will return to normal.
Thank you, Jigsaw
You have 24 hours to pay $150 USD to the Bitcoin address
24 Hours remain
View encrypted files
Make a $150 payment to the Bitcoin address specified below
Personal Information:
IP address:
City: xxxxxxxxxx
State: xxxxxxxxxx
Country:
Bank:
Users name: xxxxxxxxxx
Credit card: xxxxxxxxxx
Bitcoin address:
41h8a9K5bh1IlPo964hTEBnj783j91kM0a
I made my payment! Give me back my files
Your personal ID for this session is:
If you do not comply with the payment your files will stay encrypted and may be stolen

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

To Pay or Not to Pay……

1. If you don't pay, it's simple, you don't receive the public key

OR

2. If you pay….
   - You might be given the public key to decrypt the files
   - You might be asked for more money
   - You might be attacked again
   - Nothing

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

43%

$377,000

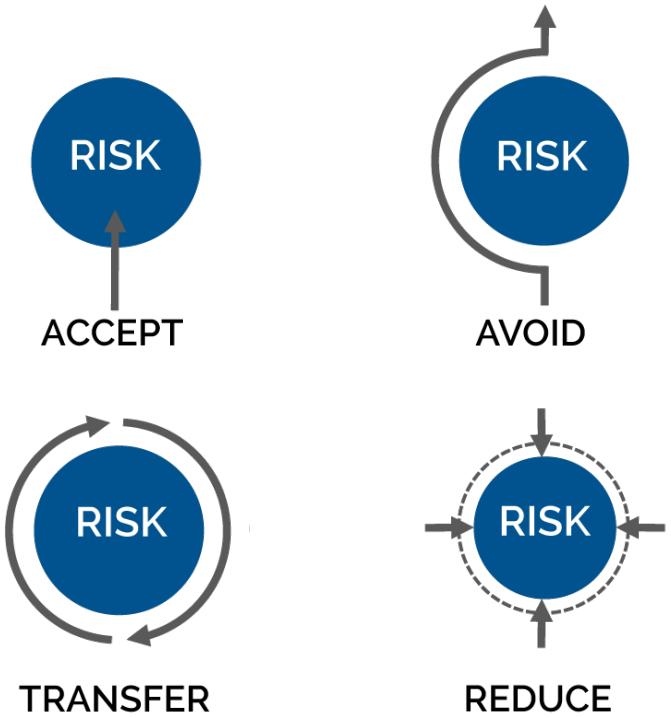
20%

$20 BILLION!!!!

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

Four Risk Mitigation Strategies



South-West Texas Border
Small Business
Development Center Network
UTSA SBDC Center for Government Contracting

Ransomware Mitigation Recommendations

- Training and Awareness
- Backup your data / files
- System-level protections
- Network-level protections
- Cyber insurance
- Update regularly

Phishing

Social Engineering

Dangers of WiFi

BYOD

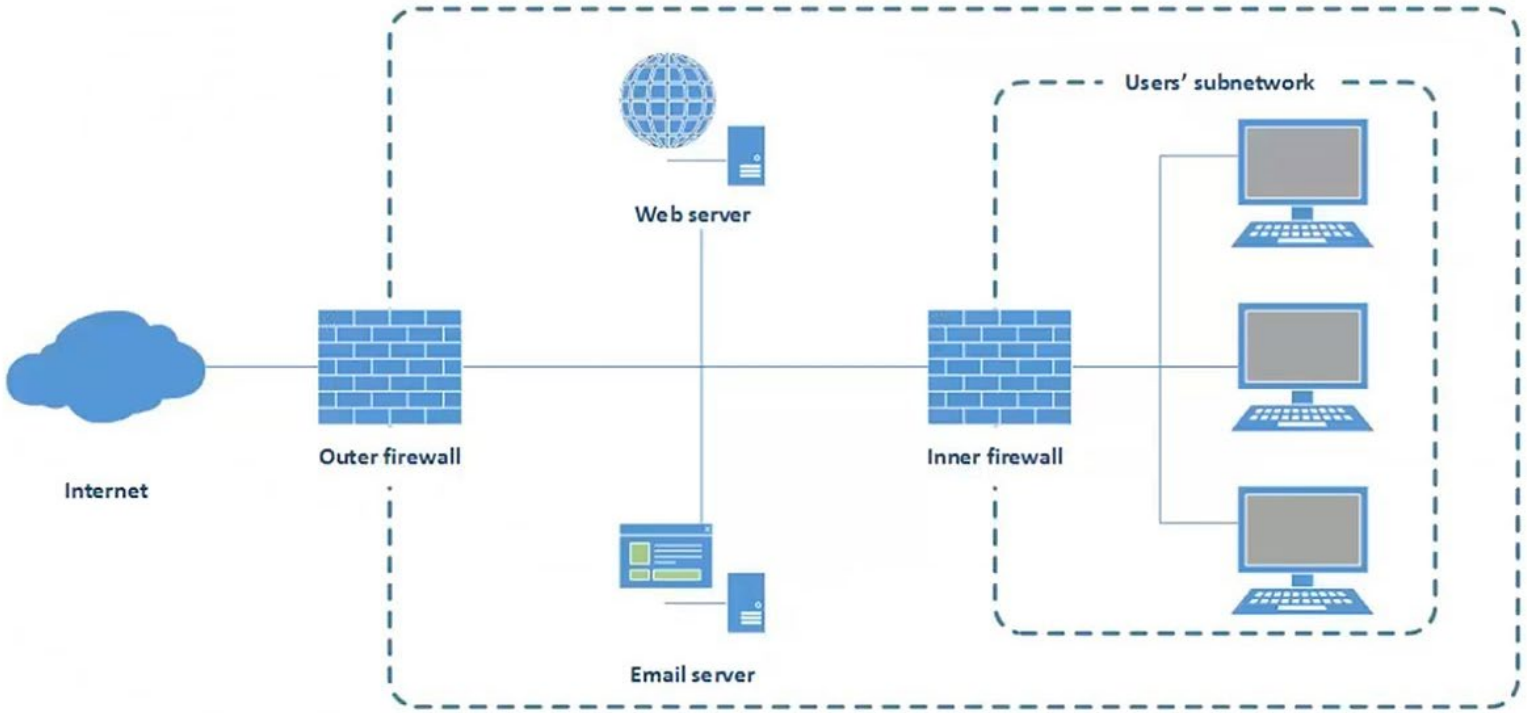
5 Keys To Data Backup

1. 3-2-1 Backup Strategy
2. Determine Data to be Backed Up
3. Type of Backup
4. Backup Frequently
5. Test Backups

System-Level Protections

MALWARE

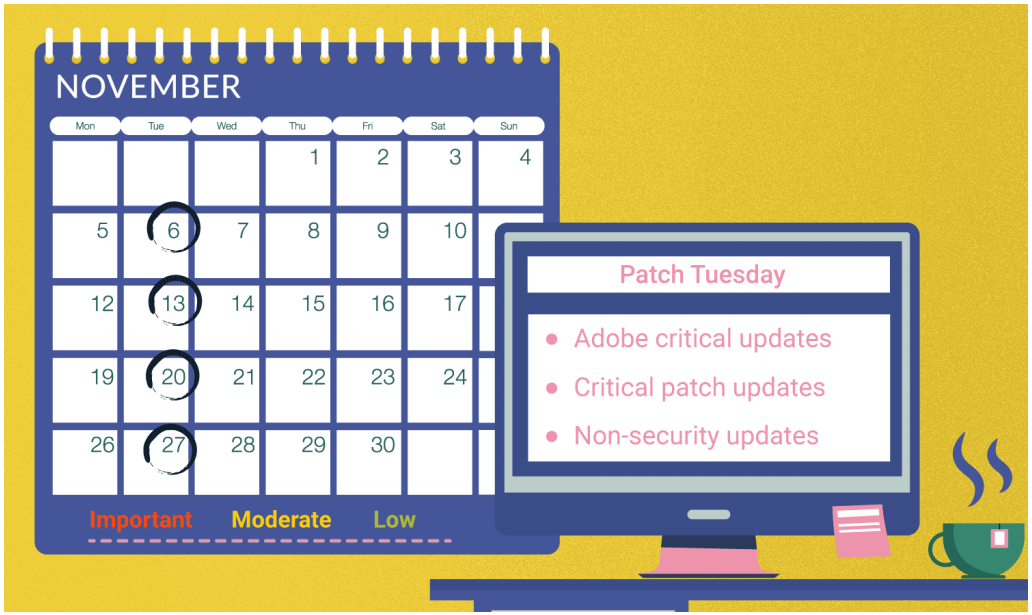
Network-Level Protections



"With ransomware attacks increasing, cyber insurance now seen as a necessity, not a luxury"

- Security Magazine, June 2020


UPDATE


NOVEMBER
Mon
Tue
Wed
Thu
Fri
Sat
Sun
1
2
3
4
5
6
7
8
9
10
12
13
14
15
16
17
19
20
21
22
23
24
26
27
28
29
30
Important
Moderate
Low
Patch Tuesday
Adobe critical updates
Critical patch updates
Non-security updates

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

Steps to Minimize Ransomware Damage

1. Seek assistance
2. Identify the infection
3. Isolate the infection
4. Report
5. Determine your options
6. Restore
7. Prevent

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

NoMoreRansom.org

https://cgc.txsbdc.org/cybersecurity-for-small-business/

And last, but certainly not least……ME!

South-West Texas Border
Small Business
Development Center Network

UTSA SBDC Center for Government Contracting

Building the Texas Economy One Business At a Time

UTSA SBDC

Center for Government Contracting

https://cgc.txsbdc.org

(210) 458-2458

(Search for “UTSA SBDC Center for Government Contracting” on Facebook)

Each program within the Institute is funded through various state and federal programs, and respective service areas differ according to that particular program's mission.