PIPELINE INFORMATION TECHNOLOGIES

STEVE MARBURGER

- Owned Jemez Computer Consulting Group in Santa Fe, NM 1995-2014
- Opened Pipeline Information Technologies in Santa Rosa, CA 2014-Present
- Undergraduate Degree in Business
- Masters of Computer Information Information Systems University of Denver

CYBERSECURITY

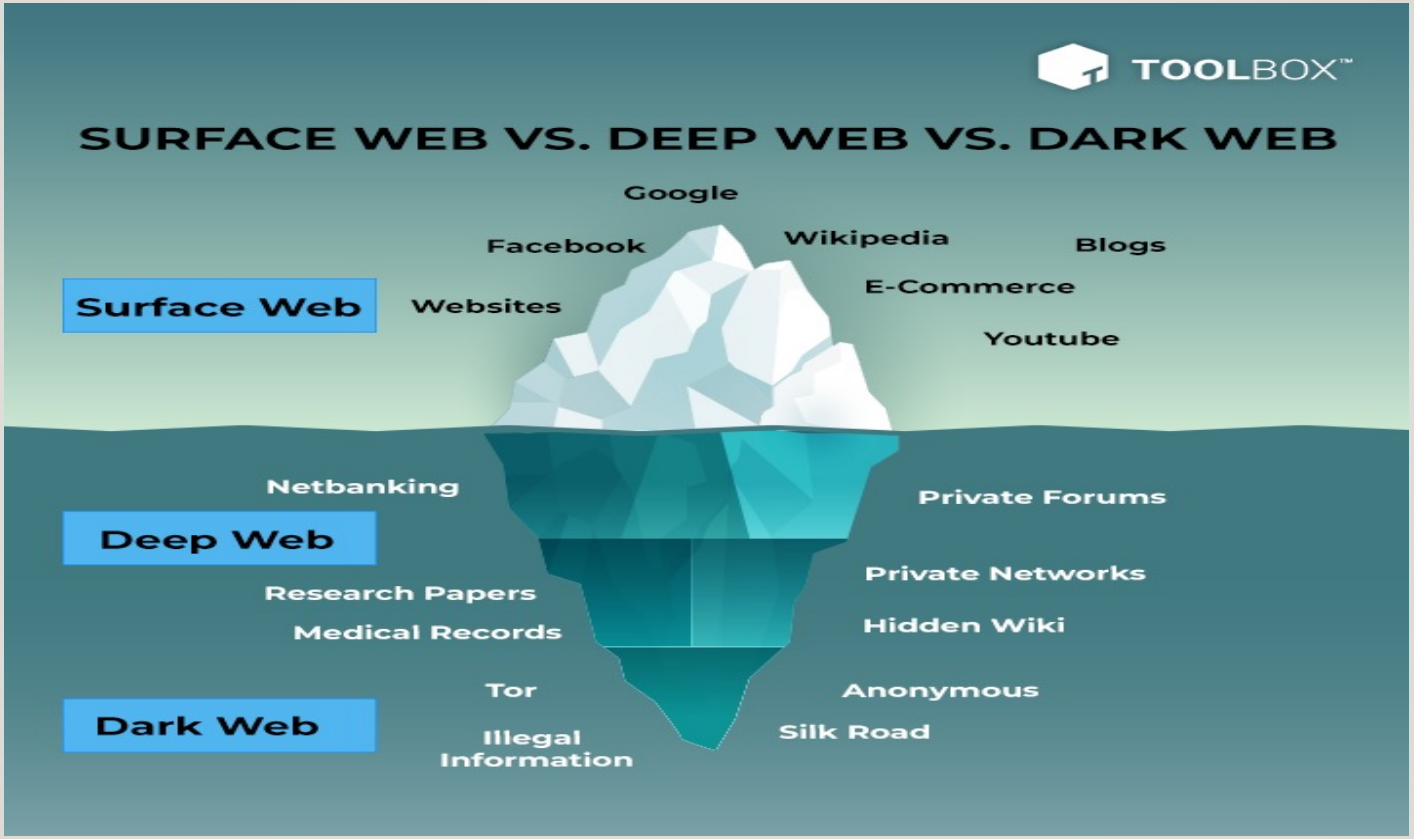
What is a cyber attack?

- A cyber attack is an attempt to disable computers, steal data, or use a breached computer system to launch additional attacks.
- Cybercriminals use different methods to launch cyber attacks including malware, phishing, denial of service attacks, and ransomware.

RECENT SECURITY BREACHES

- AT&T – 73 million customers.
- Data was sold to the DARK WEB.

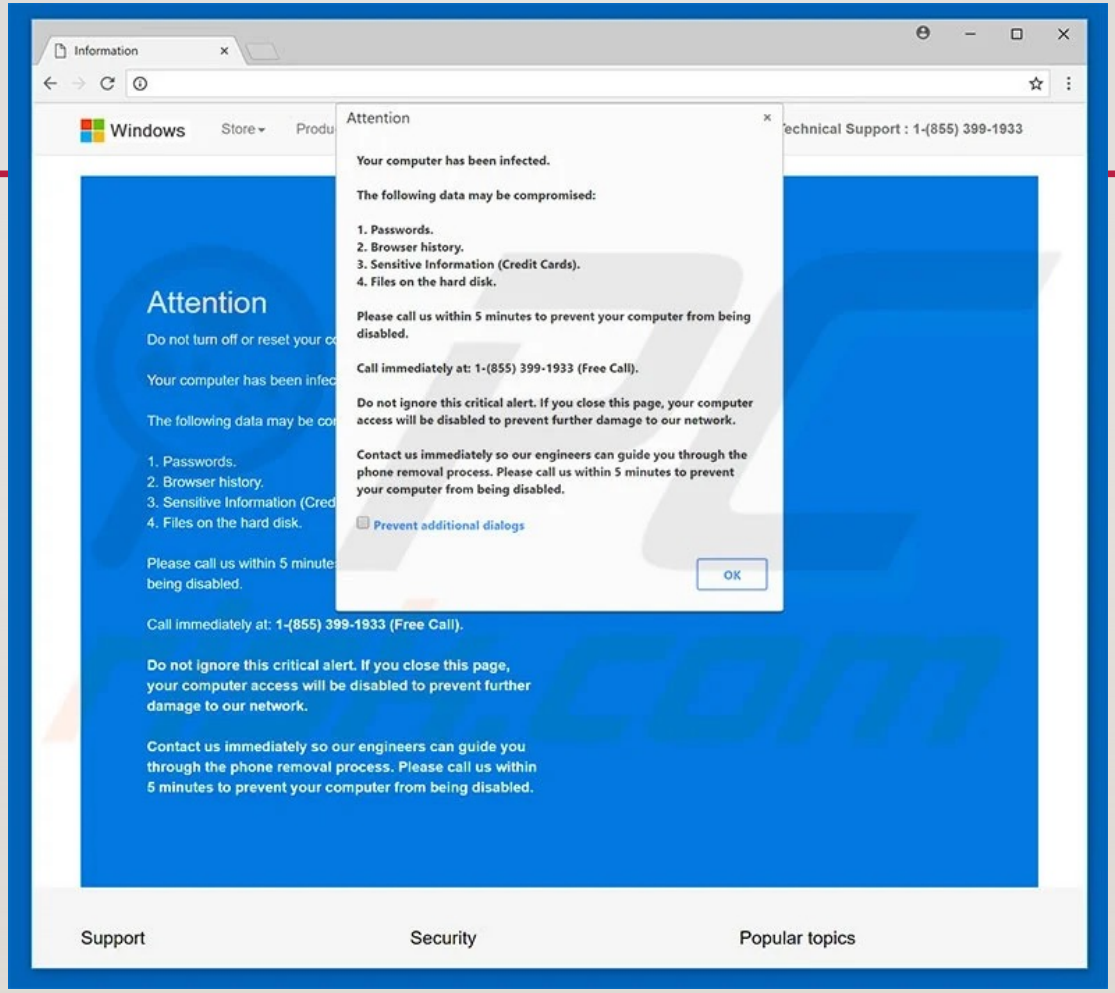
DARK WEB VS DEEP WEB



TYPES OF ATTACKS

- Ransomware
- Malware, Spyware
- Viruses
- Infected websites - fake warnings asking you to call someone
- Phishing
- Spoofing

INFECTED WEBSITE SCAM



RANSOMWARE


XINOF v4.4.1
All Of Your Files Have Been Encrypted By XINOF!
All your files have been encrypted due to a security problem with your PC.
If you want to restore them, please send an email to bds24@tutanota.com
XINOF
You have to pay for decryption in Bitcoin. The price depends on how fast you contact us. After payment we will send you the decryption tool.
You have to 48 hours(2 Day) To contact or paying us After that, you have to Pay Double.
in case of no answer in 6 hours email us at = bds24@ProtonMail.com
The crypter person username : bds24
your SYSTEM ID is : FDC9B3EA
06d,20:58:25
Attention!
DO NOT pay any money before decrypting the test files.
DO NOT trust any intermediary, they wont help you and you may be victim of scam. just email us , we help you in any steps.
DO NOT reply to other emails, ONLY this two emails can help you.
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
What is our decryption guarantee?
Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)
You only have LIMITED time to get back your files!
if timer runs out and you dont pay us , all of files will be DELETED and yuor hard disk will be senously DAMAGED.
you will lose some of your data on day 2 in the timer.
you can buy more time for pay. Just email us .
THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)
Regards-FonixTeam

PHISHING


NETFLIX
Please update your payment details
Hi Dear,
We're having some trouble with your current billing information. We'll try again. but in the meantime you may want to update your payment details.
UPDATE ACCOUNT NOW
Need help? We're here if you need it. Visit the Help Center or contact us now.
- Your friends at Netflix

Microsoft account unusual sign-in activity

S

support <info_support@lives-msn.com>
Sun 5/24/2020 9:39 AM
To: support

Your Microsoft account is about to expire due to inactivity

We want to inform you that the expiration date of your Microsoft e-mail account will be May 23, 2020.

When the expiration date has elapsed, the following services will be disabled:

- Sending and receiving messages
- Web applications that have been linked to your account

Simply click here and login into your Microsoft account and let us know that you are currently using this e-mail.

Thanks,

HOW TO PROTECT YOURSELF

- **Be on the lookout for suspicious links, attachments, and downloads.** Malware and ransomware can be embedded in links, attachments, and downloads. Make sure a link is authentic before clicking on it.
- **Create and use strong passwords.** Always use strong passwords that are difficult to hack. Use a different password for each account. Passwords should be at least 8 characters long and contain numbers, special characters, and capitalized letters.
- **Use multi-factor authentication whenever possible.** Multi-factor authentication adds an extra layer of security. If a service offers multi-factor authentication, use it.

HOW TO PROTECT YOURSELF

- **Use secure internet communications.** Use sites that use “HTTPS” if you will access or provide any personal information. Don’t use sites with invalid certificates.
- **Update your anti-virus software regularly.** Make sure your anti-virus software is up to date and updates are installed regularly.
- **Don’t open or respond to any suspicious offers via e-mail or telephone.**
- **Never text or e-mail password for your computer or e-mail.**
- **Use an agency that offers ID Protection.**

HOW TO PROTECT YOUR COMPUTER

- Update your operating system, Microsoft Office and install security updates.
- Password protect your computer.
- Use multifactor authentication.
- Install antivirus and malware protection.
- Backup your data.

SMART PHONE SECURITY

- Security software exists for both iPhone and Android systems.
- Do we need it?
- Create a backup of your system!!!!!!

BACKUPS!!!!!!!!

- Use an external hard drive, create a system image, and backup your data to the Cloud.
- Cloud based systems:
  - Carbonite
  - CrashPlan
- External hard drive demo for PC, Mac

CASE STUDY # 1

- Location: Trader Joes on Santa Rosa Avenue
- Method of attack: Physical
  - Two-person operation. First person smeared grease on door lock.
  - Second person had some tissues and asked to help.
  - Second person said there was grease on the victim's shirt, started wiping it off.
  - First person then stole his wallet. They took all cash, drivers license, medical information, and returned the wallet to his pocket.
  - Thieves spent $5k at the Apple store. Private info sold to the Dark Web.
  - The next day the criminals called them in a professional phishing operation and gained access to their computer.
  - Outcome

CASE STUDY #2

- Location: At home on the computer.
- Type of Attack: Spelling error on an infected website.
  - Infected website sent message to computer screen stating the computer was infected and they must call a number.
  - Victim called and allowed them into the computer.
  - Outcome

CASE STUDY #3

- Type of Attack: Email
  - Victim was infected by an e-mail. This allowed the people to install software on his computer which recorded keystrokes.
  - Criminals now had access to his bank, credit card and Social Security information.
  - Outcome

WHAT TO DO IF YOU HAVE BEEN HACKED

- Change your passwords to any exposed accounts, Banks, Amazon, Finances, etc.
- Have a forensic audit done on your computer.
- Reformat your computer.
- Go to the following website IdentityTheft.gov.
- Monitor your data via ID Shield.
- Watch out for suspicious phone calls, email, txt.

PIPELINE INFORMATION TECHNOLOGIES

505-470-1224

steve@pipelineit.net

Thank You