Ransomware

Pay up or Else!
How the Ransomware Epidemic Can Hold You Hostage & How To Handle It.

Presented by

Darragh Fitzpatrick

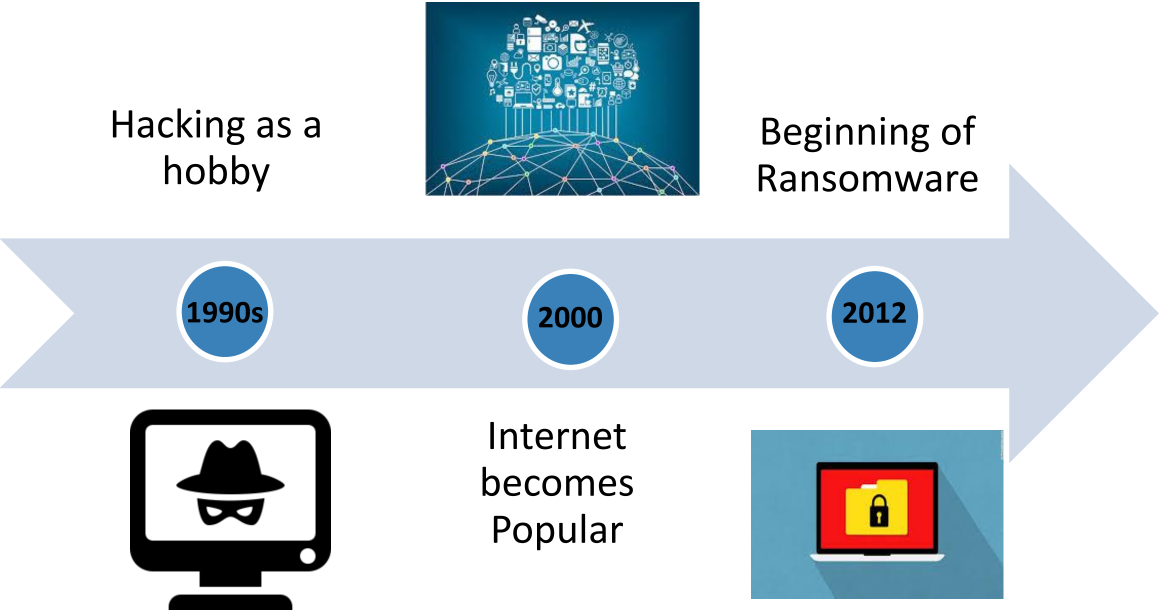
Partner & Executive VP

TabushGroup

Background

How viruses and malware came about.

History of Viruses & Malware



1990s

Hacking as a hobby

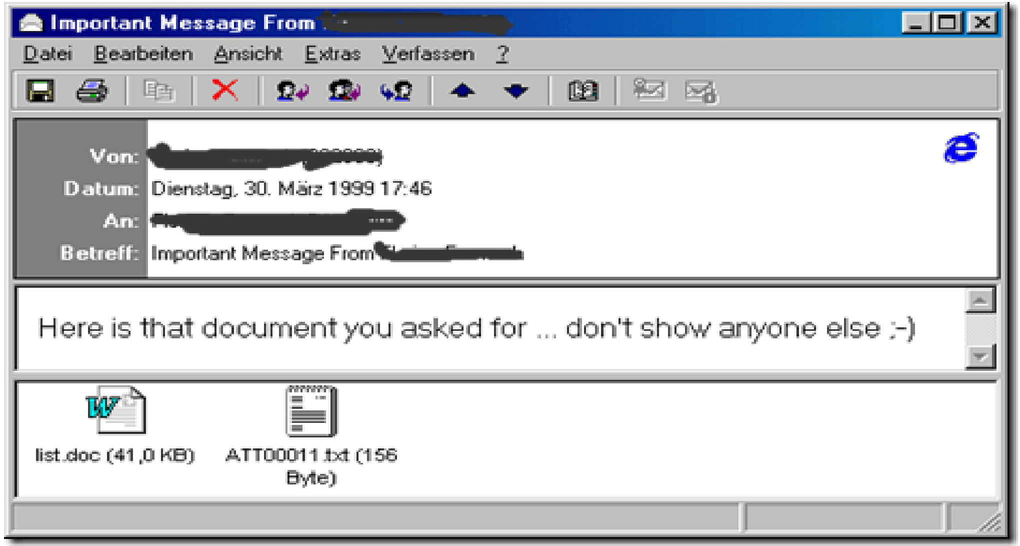
2000

Internet becomes Popular

2012

Beginning of Ransomware

The first big hits!



Important Message From [redacted]

Von: [redacted]

Datum: Dienstag, 30. März 1999 17:46

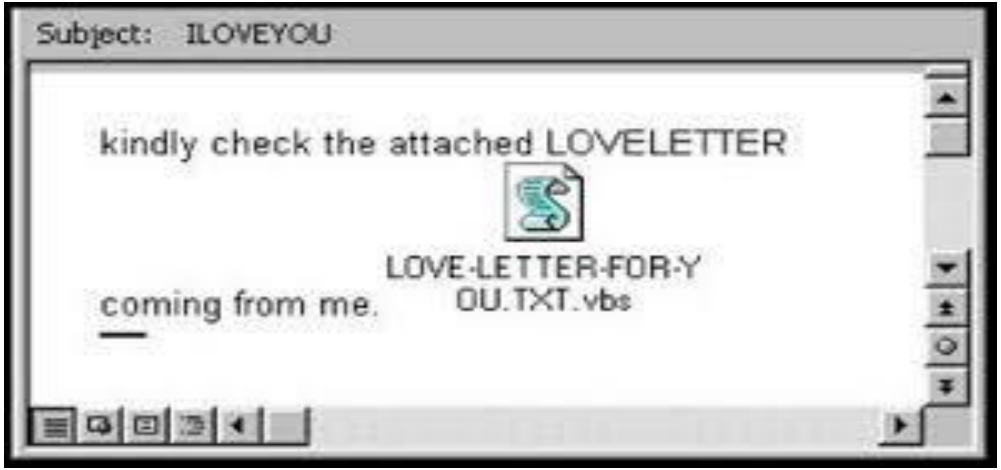
An: [redacted]

Betreff: Important Message From [redacted]

Here is that document you asked for ... don't show anyone else ;-)

list.doc (41,0 KB)

ATT00011.txt (156 Byte)



Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Cyberattacks
The common perception

- *Targeted attacks*
- *Mainly big companies*
- *Often political/other motivations*

Bitcoin

- *Completely anonymous*
- *No central owner/authority*
- *Enabled Ransomware*

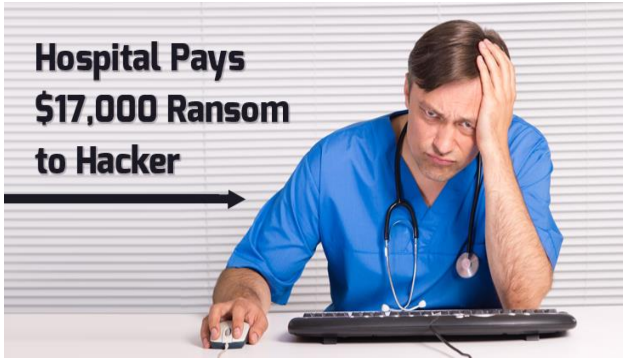
The Dangers of Ransomware

- *Makes all your files/documents inaccessible*
- *Spreads itself to other computers*
- *The only way to get them back is to pay ransom*
- *Non-targeted*

Ransomware as a Business

- *Ransomware is a real business, done for-profit*
- *Hackers are untraceable*
- *Small companies are just as vulnerable as big ones*
- *No effective law enforcement to protect us*

University pays $20,000 to Hackers
PAY
$$$



2. Prevention

How to make sure you’re not vulnerable to attack.

Backups

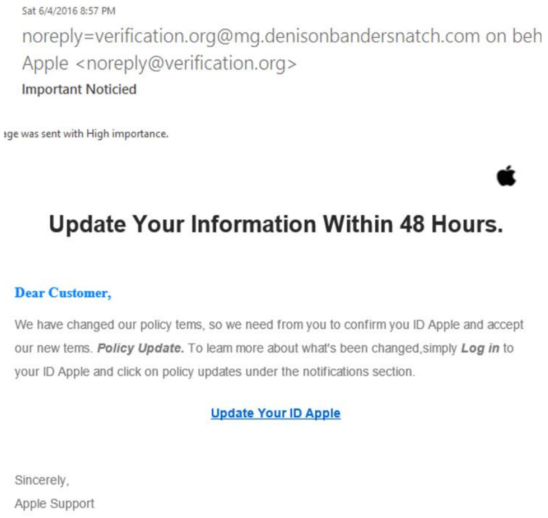
- *Have good "offline" backups*
- *Use a trusted backup product or service*

Security Software

- *Watches activity on each PC*
- *Every PC & server on the network needs AV software*
- *Antivirus is only the tip of the iceberg, look for software that adds other forms of protection*

E-mail Filtering

- *Don't only rely on free filters*
- *Filter content such as ZIP files*
- *Block access to insecure e-mail systems*



Sat 6/4/2016 8:57 PM

noreply=verification.org@mg.denisonbandersnatch.com on beh
Apple <noreply@verification.org>

Important Noticied

ıge was sent with High importance.

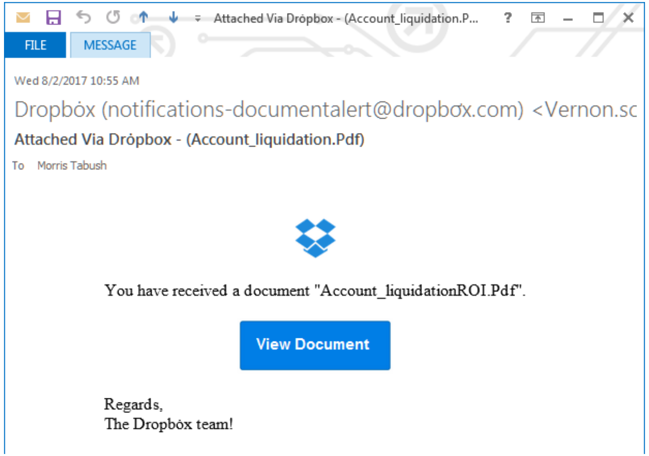
Update Your Information Within 48 Hours.

Dear Customer,

We have changed our policy tems, so we need from you to confirm you ID Apple and accept our new tems. ***Policy Update.*** To leam more about what's been changed,simply ***Log in*** to your ID Apple and click on policy updates under the notifications section.

Update Your ID Apple

Sincerely,
Apple Support



Wed 8/2/2017 10:55 AM

Dropbȯx (notifications-documentalert@dropbσx.com) <Vernon.sc

Attached Via Drȯpbox - (Account_liquidation.Pdf)

To Morris Tabush

You have received a document "Account_liquidationROI.Pdf".

Regards,
The Dropbȯx team!

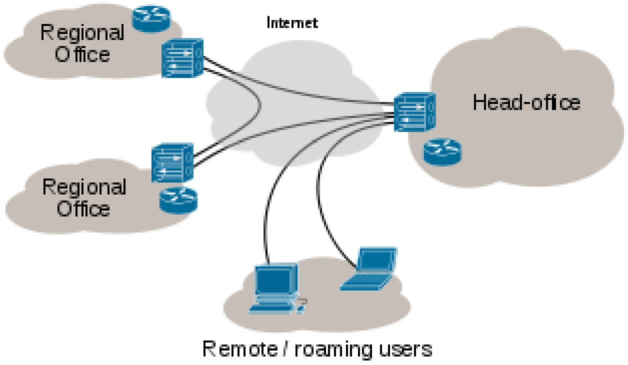
Web Filtering

- *Ransomware & viruses don’t just come from e-mail*
- *Web browsers should be secured*

Secure Your VPN & Firewall

- *An infected computer on a VPN could take down the entire company*
- *Firewalls need to be checked periodically*

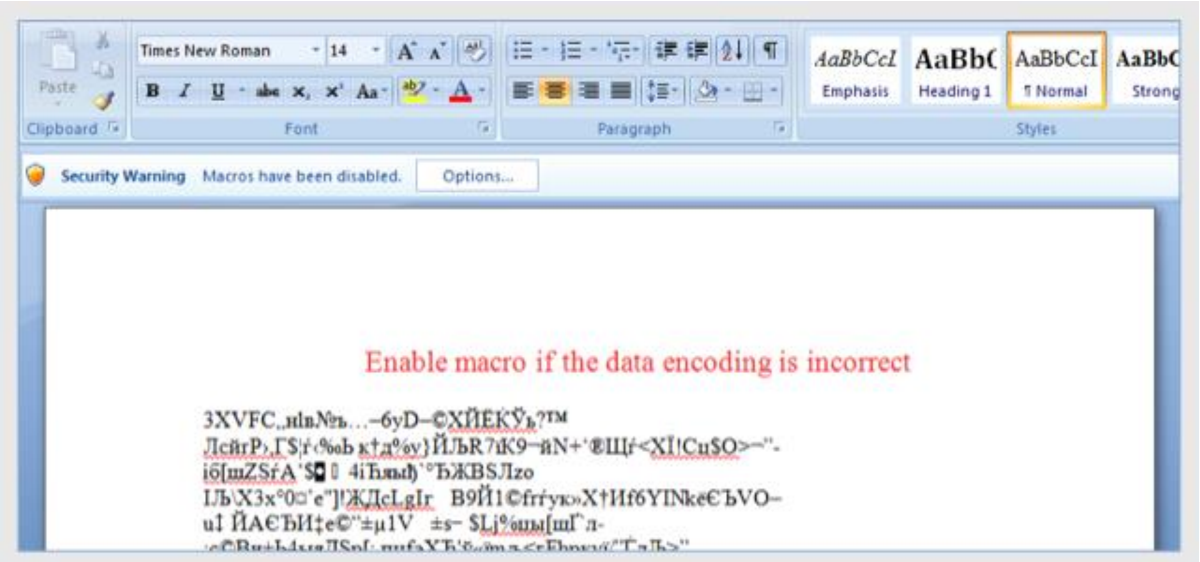
Internet VPN



Block Malware From Executing

- *Set group policies to prevent malware from executing in temporary directories on Windows*

- *Disable unsigned macros in office*



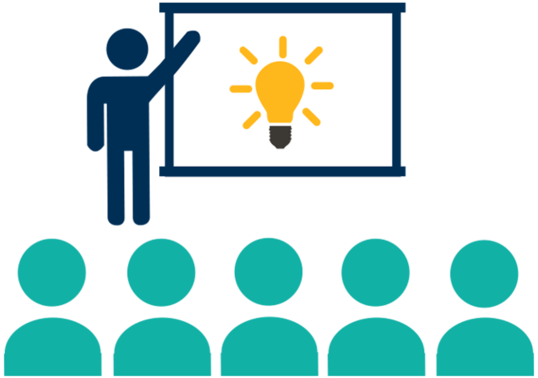
Security Warning Macros have been disabled.

Enable macro if the data encoding is incorrect

3XVFC„нlв№ъ…–6yD–©ХЙЁЌЎъ?™
ЛсйrP›‚Г$¦ѓ‹%оЬ к†д%v}ЙЉR7ıK9¬йN+'®Щѓ<ХI!Cu$O>¬".
іб[шZSѓA'$◘ ▯ 4iЋлыd)`°ЂЖBSЛzo
IЉ\X3x°0¤'e"]!ЖДcLgIr B9Й1©frѓук»X†Иf6YINkėЄЪVO–
u‡ ЙАЄЪИ‡e©"±µ1V ±s– $Lj%шы[шГл-

Training

- *WE are the biggest vulnerabilities on the network*
- *Implement routine training*



Prevention: Summary

- *Backups*
- *Security software*
- *E-mail filtering*
- *Web filtering*
- *Secure VPN & Firewall*
- *Block malware from executing*
- *Training, training, training!*

3. Response

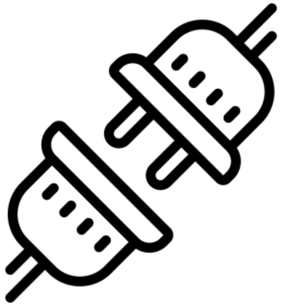
What to do if you’re attacked.

Backups

- *First, check your backups*
- *Freeze/preserve them*

Determine who's infected

- *Find out which computers are infected*
- *Disconnect them immediately to stop the spread*



If you have good backups…

- *Clean out and patch infected computers*
- *Delete infected files*
- *Restore from backups*
- *See "Prevention" steps*

If you don’t have good backups…

- *DO NOT plead with hackers*
- *Get Bitcoin and pay the ransom*
- *Input the decryption code before time runs out*
- *See “Prevention” steps for next time*

Just to wrap up …

- *Ever increasing threat landscape*
- *Cybercrime is a business on the rise*
- *Malware is ever changing*
- *Don’t be Scared, be more Prepared*

Q & A

TabushGroup

Darragh Fitzpatrick

dfitzpatrick@tabush.com

212-252-0571

www.linkedin.com/in/darraghfitzpatrick

www.tabush.com / www.goboxtop.com