Ransomware

Prof. Zaheed Shaikh

From :Donald McArthu r and

*www.csis.pace.edu/~ctappert/cs816-15fall/slides/**ransomware**.**ppt**x*

AGENDA

- What is RansomWare
- History of RansomWare
- How RansomWare is Deployed
- Strategies to Combat RansomWare
- What to do if you are infected

RANSOMWARE IS A TYPE OF MALWARE THAT RESTRICTS ACCESS TO THE INFECTED COMPUTER SYSTEM IN SOME WAY, AND DEMANDS THE USER PAY.

TYPES OF RANSOMWARE

- THE MOST COMMON TYPE DISPLAYS MESSAGES INTENDED TO COAX THE USER INTO PAYING (EX. YOUR MACHINE IS INFECTED!)

- MORE DESTRUCTIVE TYPES ENCRYPT FILES ON THE SYSTEM'S HARD DRIVE

- A NEW RELEASED VERSION ACTUALLY LOCKS THE OPERATING SYSTEM

HISTORY OF CRYPTO RANSOMWARE

- FIRST REPORTED OCCURRENCE: CRYPTOLOCKER IN 2013

- INITIALLY POPULAR IN RUSSIA BUT QUICKLY WENT INTERNATIONAL

- THE ORIGINAL CRYPTOLOCKER IN 2013 MADE AN ESTIMATED $3 MILLION

- VARIANTS SINCE 2013 HAVE MADE AN ESTIMATED $30 MILLION

HOW RANSOMWARE IS DEPLOYED

Banner Ads

ATTACHMENTS

Most come through as ZIP files or "invoices"

ADVERTISEMENTS

Ad Networks are often targeted and exploited for these types of attacks.

SECURITY HOLES

Java, Flash, Macros (Word, Excel)

WHAT DOES IT ENCRYPT?

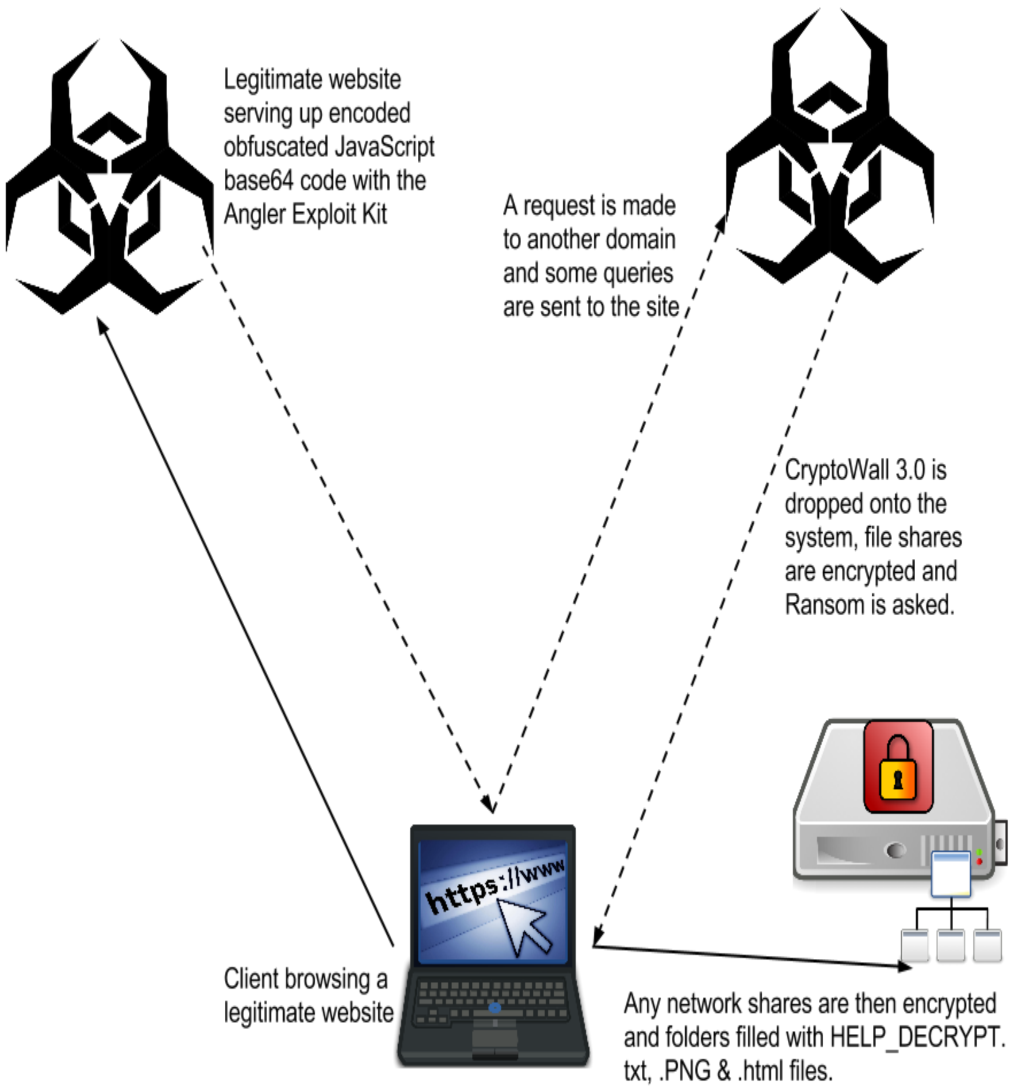
This can vary depending on the variant but usually:

- Documents
- File Drives
- Network Shares

It has been known to Encrypt

- Operating Systems
- Cloud Sync Files
- Backups

Angler Exploit Kit to Ransomware



Legitimate website serving up encoded obfuscated JavaScript base64 code with the Angler Exploit Kit

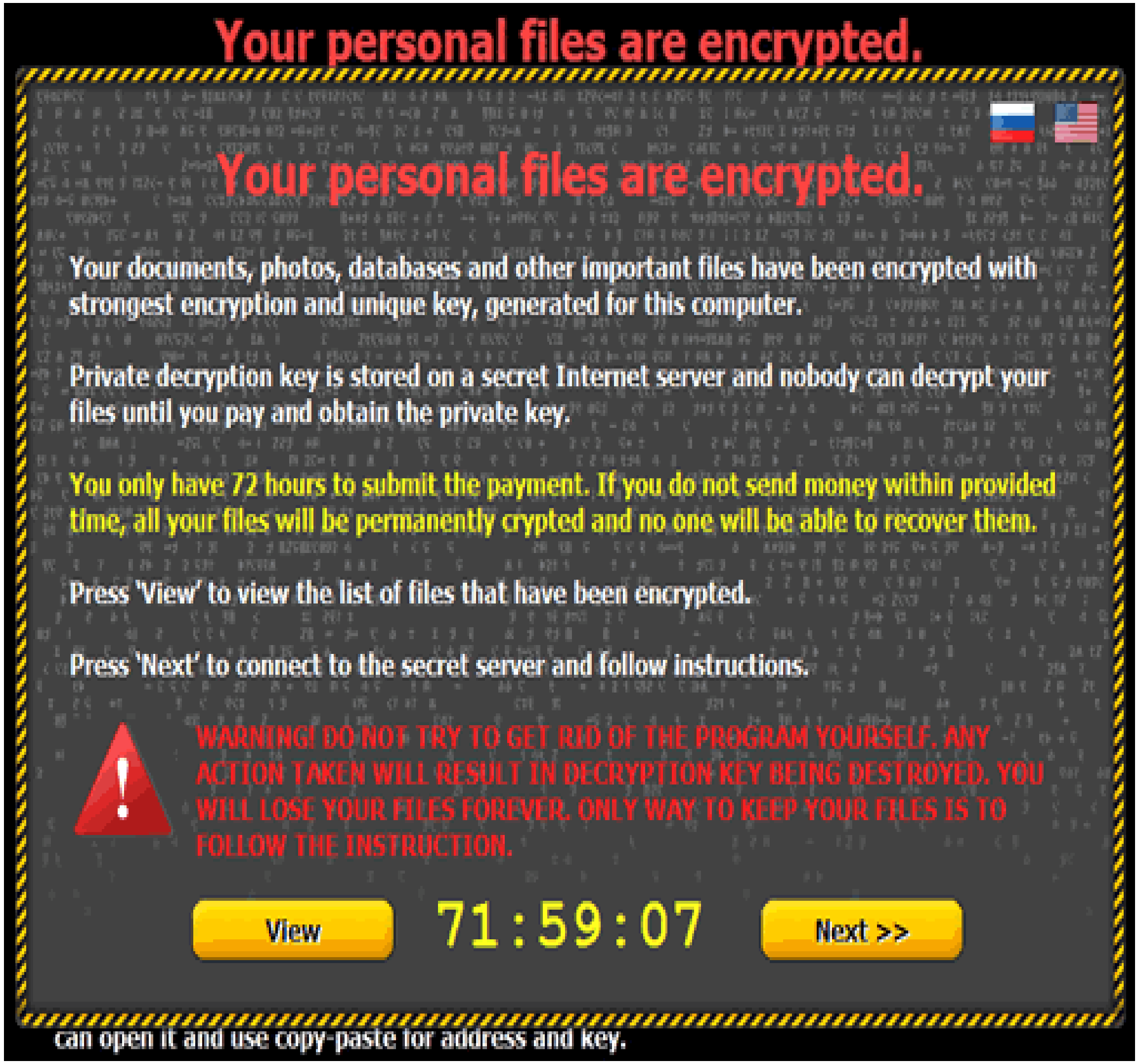
A request is made to another domain and some queries are sent to the site

CryptoWall 3.0 is dropped onto the system, file shares are encrypted and Ransom is asked.

Client browsing a legitimate website

Any network shares are then encrypted and folders filled with HELP_DECRYPT. txt, .PNG & .html files.

CBT-Locker (Critoni-Onion Ransomware)



Your personal files are encrypted.

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

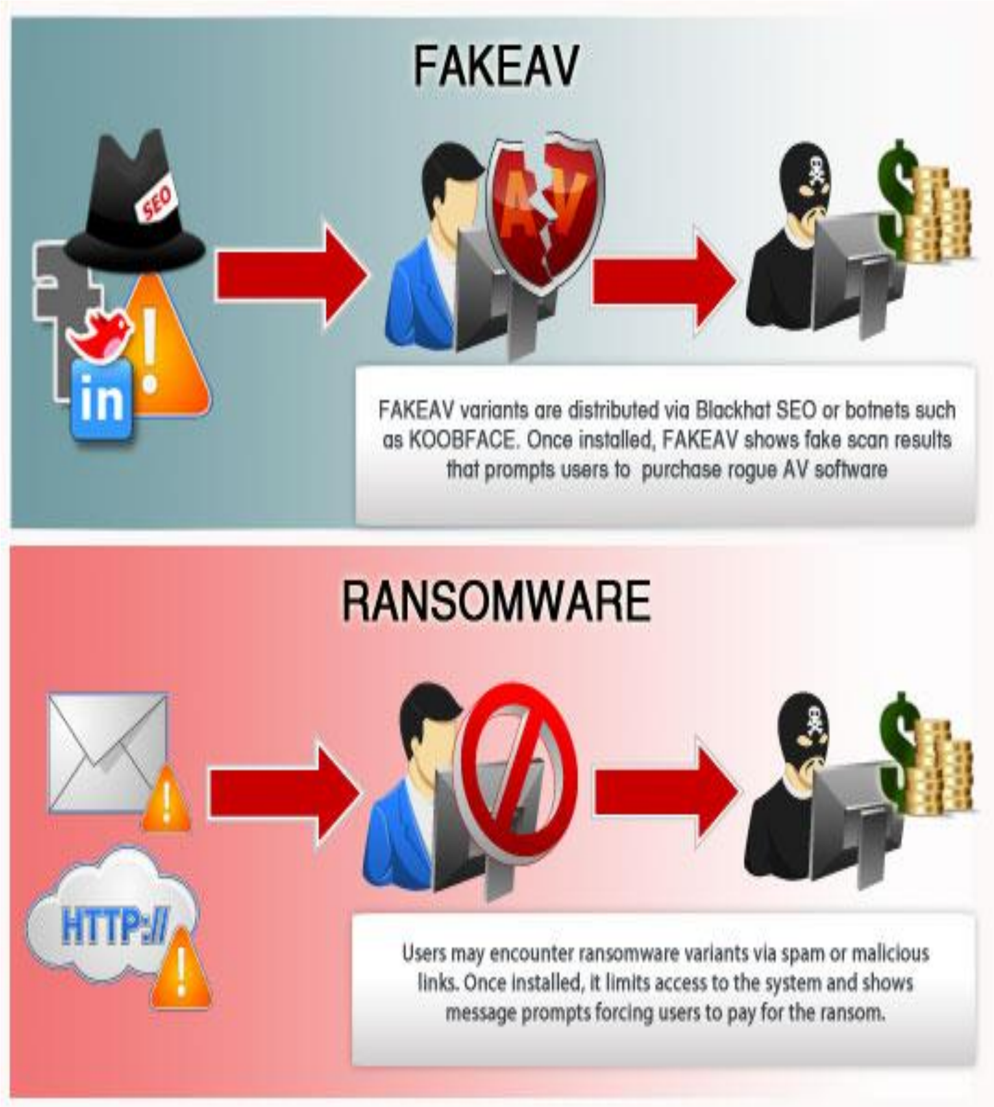
Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

can open it and use copy-paste for address and key.

Fake AV to Ransomware



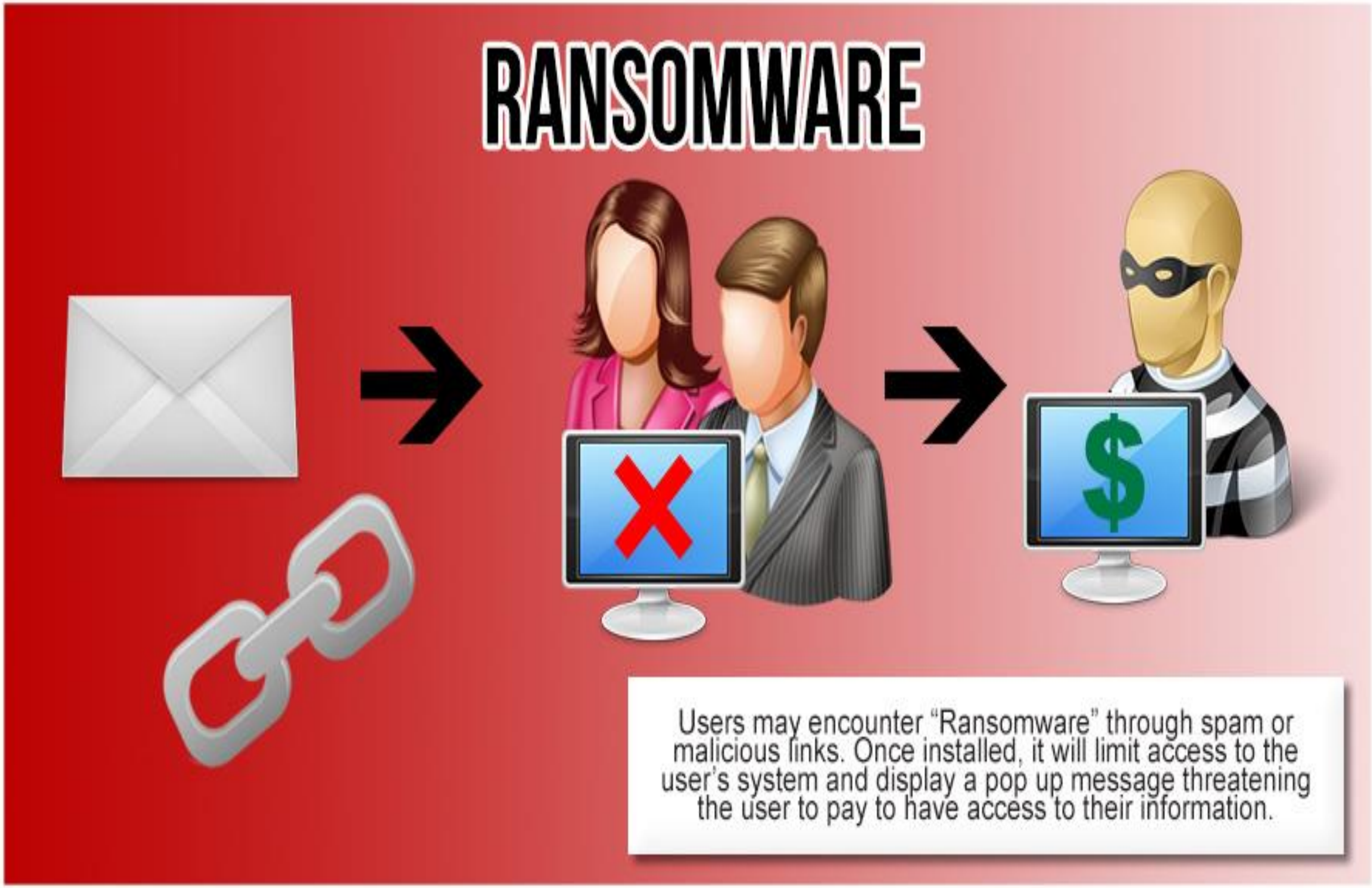
FAKEAV

FAKEAV variants are distributed via Blackhat SEO or botnets such as KOOBFACE. Once installed, FAKEAV shows fake scan results that prompts users to purchase rogue AV software

RANSOMWARE

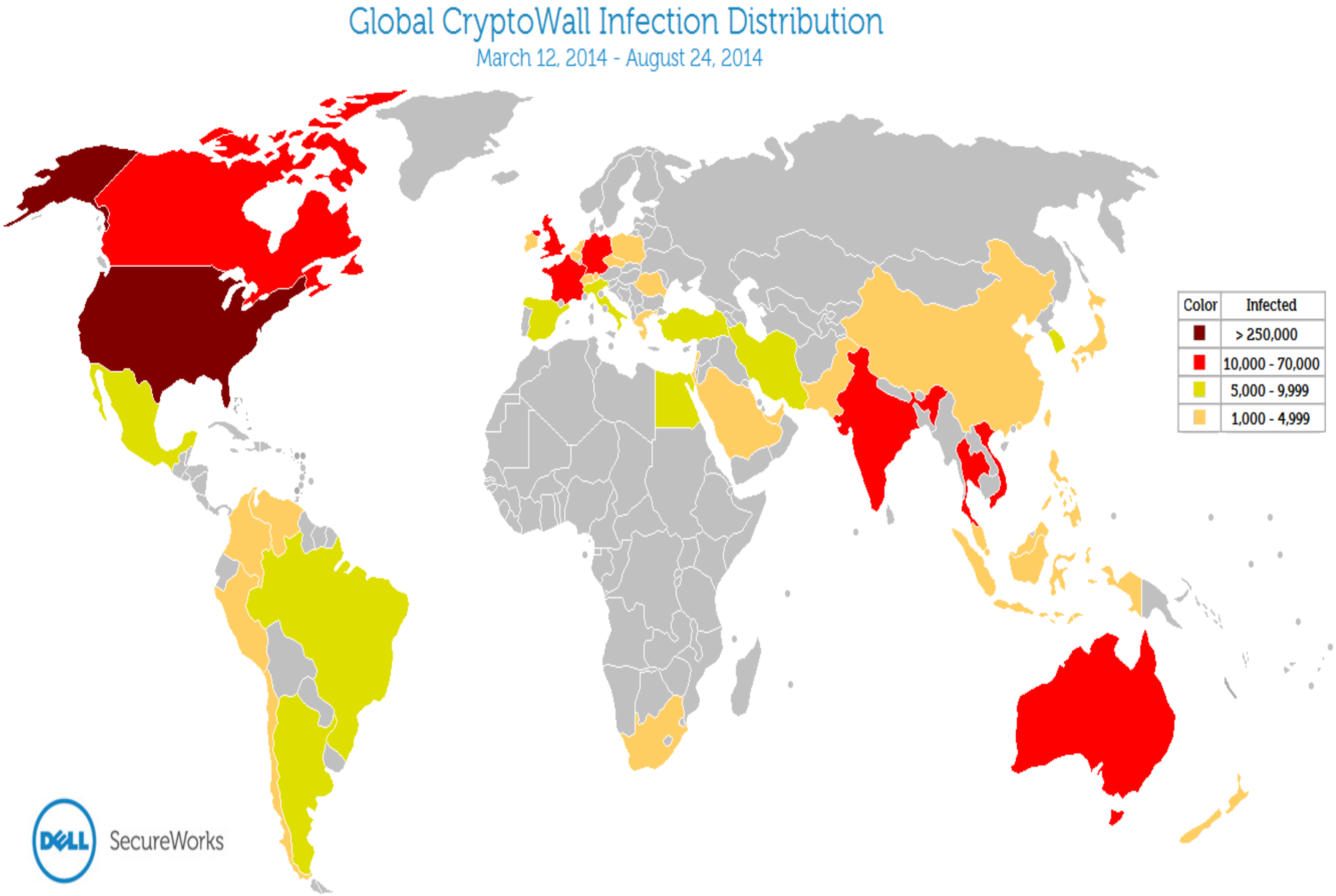
Users may encounter ransomware variants via spam or malicious links. Once installed, it limits access to the system and shows message prompts forcing users to pay for the ransom.

Ways of Getting Ransomware



Users may encounter "Ransomware" through spam or malicious links. Once installed, it will limit access to the user's system and display a pop up message threatening the user to pay to have access to their information.

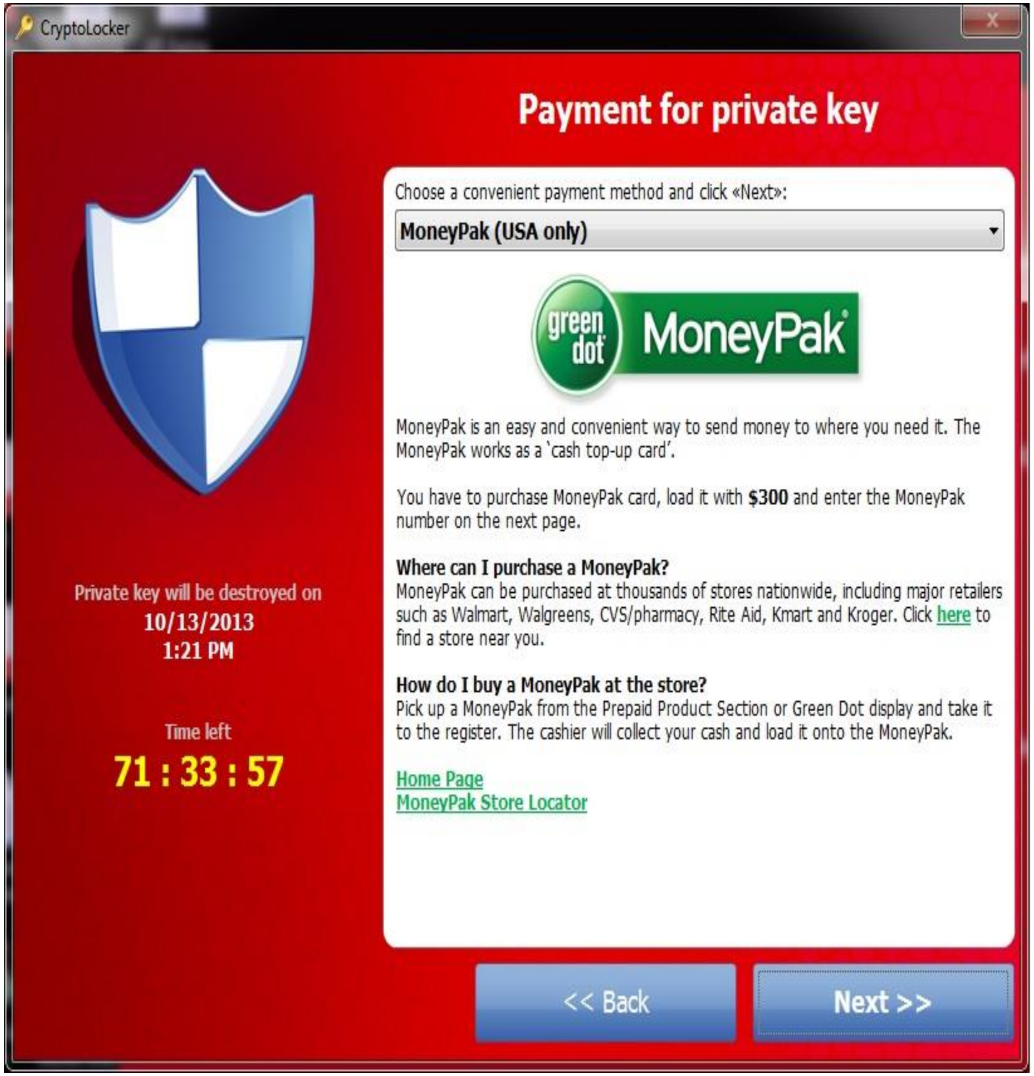
Global CryptoWall infections



Global CryptoWall Infection Distribution

March 12, 2014 - August 24, 2014

MoneyPak Ransomware



Payment for private key

Choose a convenient payment method and click «Next»:

MoneyPak (USA only)

MoneyPak is an easy and convenient way to send money to where you need it. The MoneyPak works as a `cash top-up card'.

You have to purchase MoneyPak card, load it with **$300** and enter the MoneyPak number on the next page.

Where can I purchase a MoneyPak?
MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Walmart, Walgreens, CVS/pharmacy, Rite Aid, Kmart and Kroger. Click here to find a store near you.

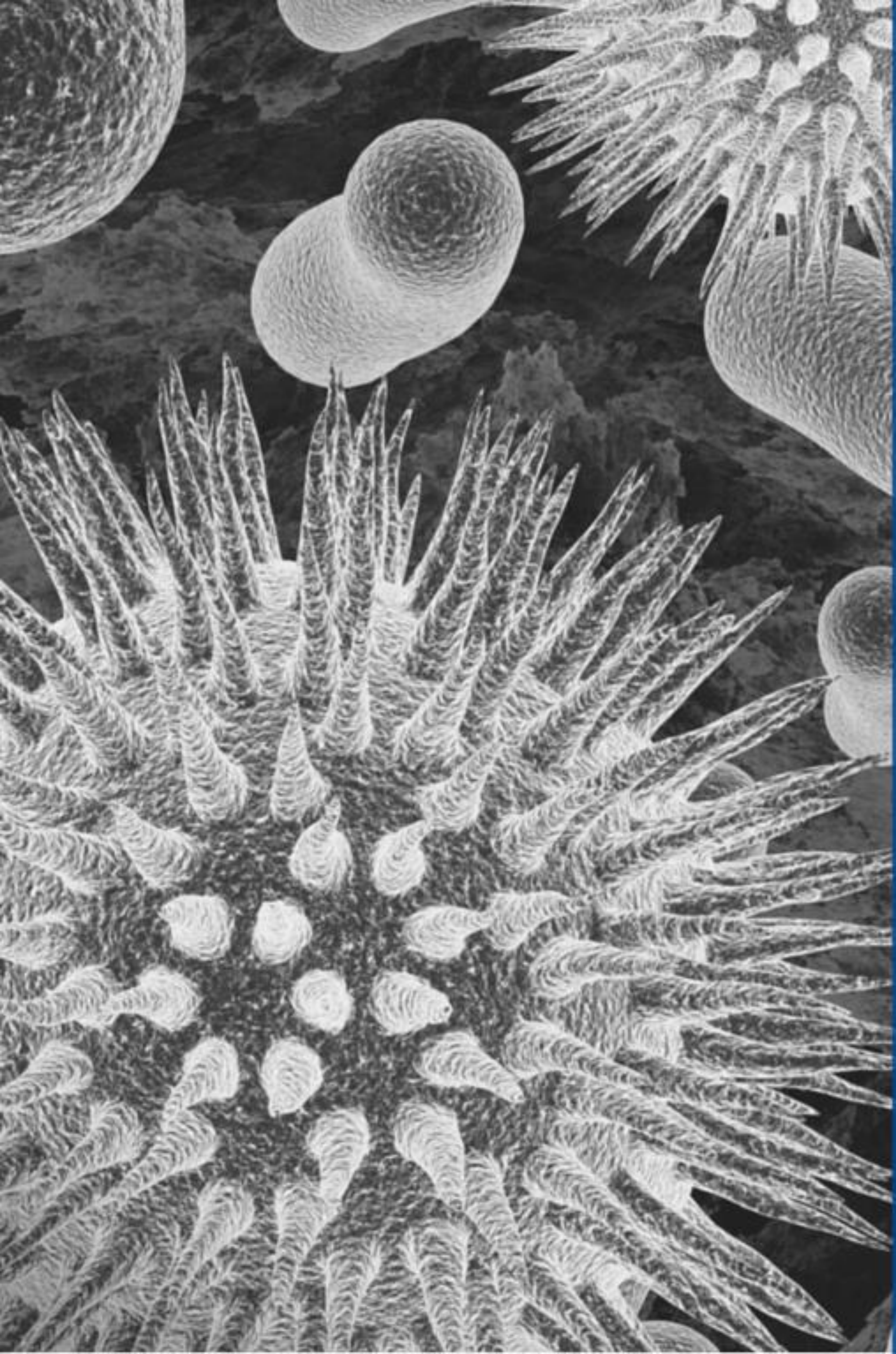
How do I buy a MoneyPak at the store?
Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.

Home Page
MoneyPak Store Locator

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 57

WHY DOES IT SUCCEED?



DOES NOT ACT LIKE A VIRUS

- Runs as a logged in user
- Morphs quickly so AV cannot detect

BACKUPS

Honestly, How often do you backup?

How often do you test your backup?

SECURITY HOLES

If you are using a computer you have to keep up with software updates.

That includes but not limited to:

- Windows
- Office
- Flash
- Java
- Silverlight

WHAT TO DO IF YOU ARE

INFECTED

01
Power Down

Power off your computer immediately.

02
Call For Help

Call Person in Charge of IT

03
Describe

Everyone makes mistakes BE HONEST about what happened, what you saw and what you were doing.

ap Rock

STRATEGIES

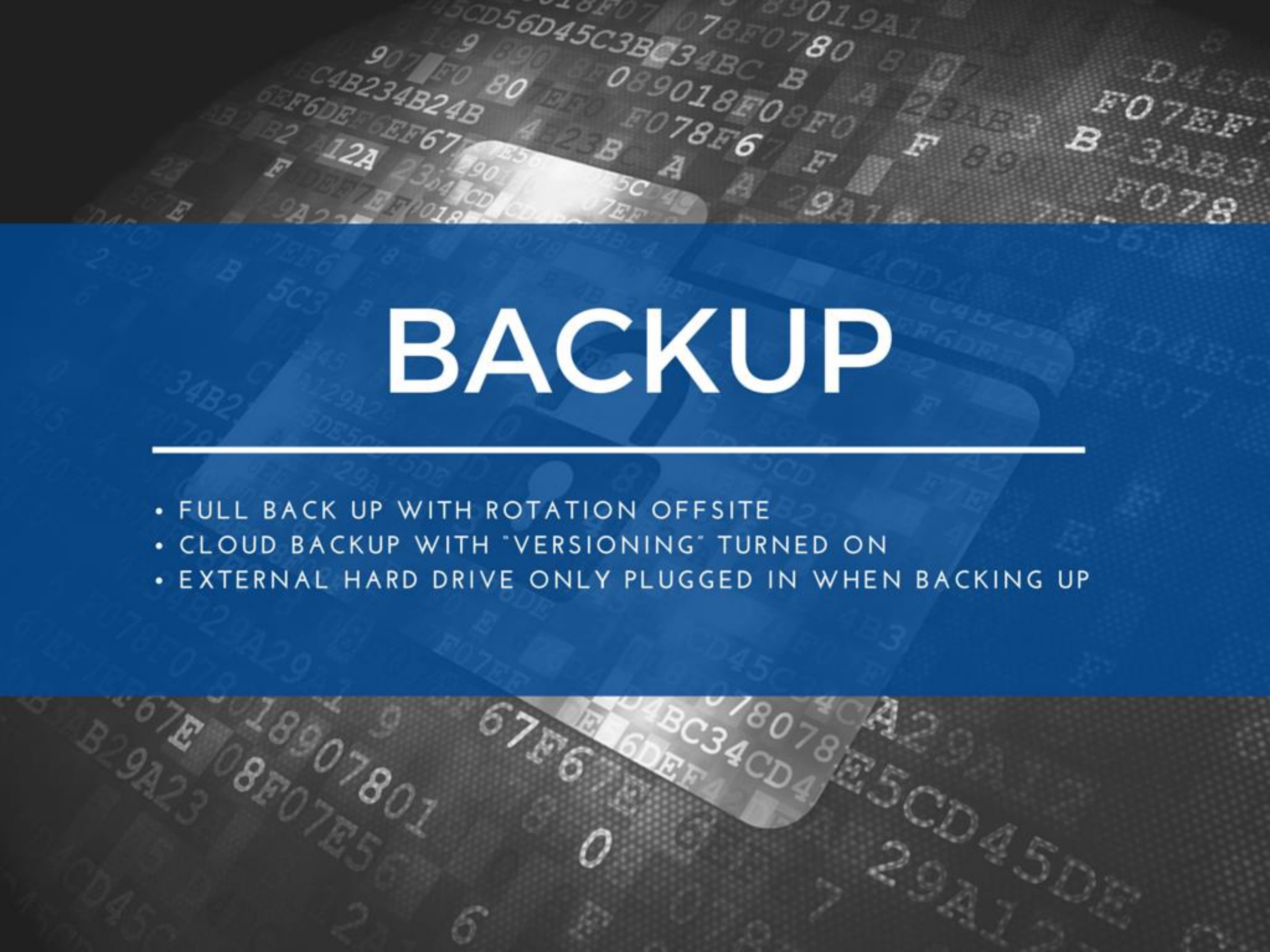
TO COMBAT RANSOMWARE

TRAINING

HOW TO SPOT THREATS

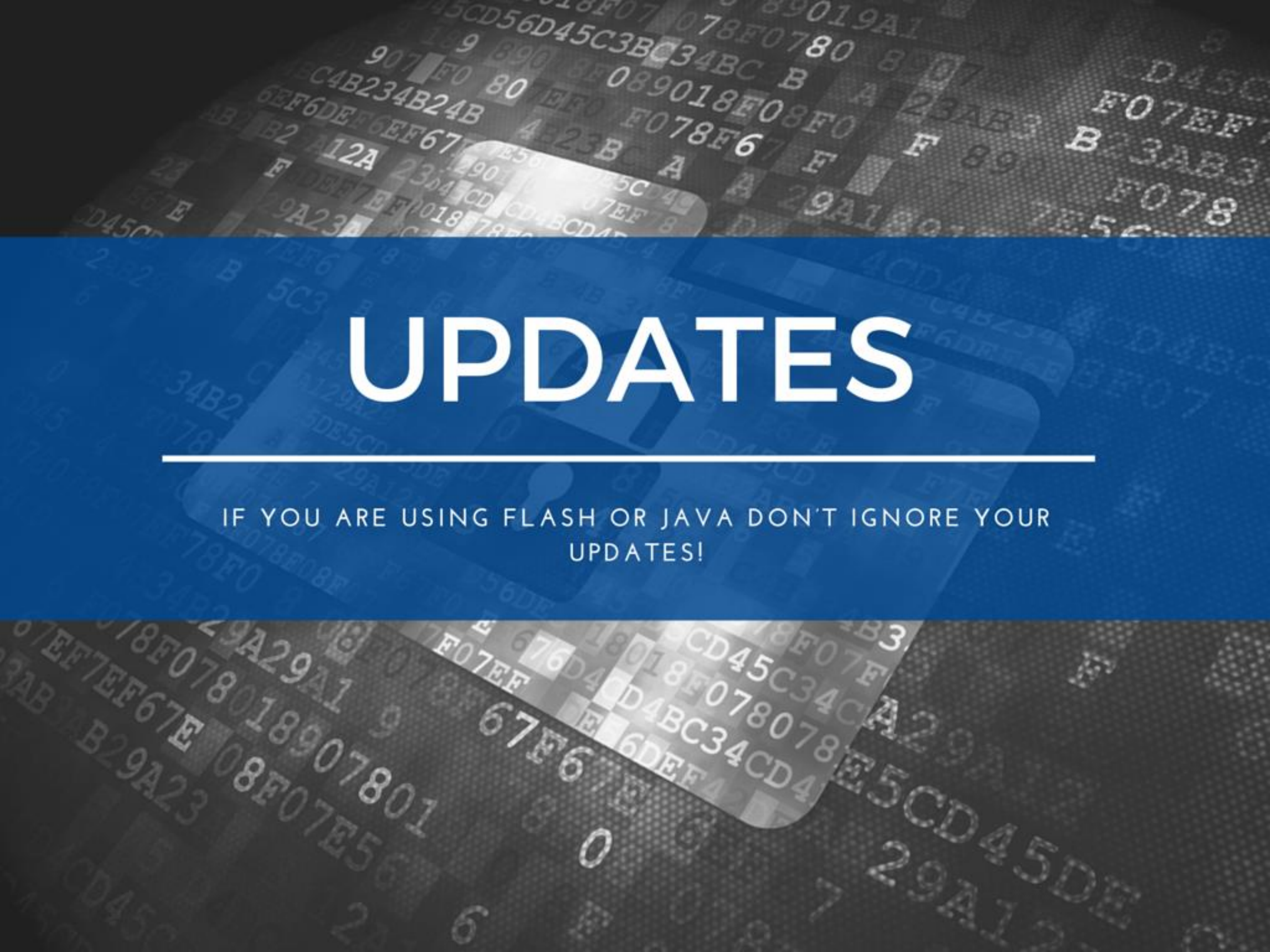
ATTACHMENTS

ONLY OPEN THEM IF YOU WERE EXPECTING THEM.



BACKUP

- FULL BACK UP WITH ROTATION OFFSITE
- CLOUD BACKUP WITH "VERSIONING" TURNED ON
- EXTERNAL HARD DRIVE ONLY PLUGGED IN WHEN BACKING UP



UPDATES

IF YOU ARE USING FLASH OR JAVA DON'T IGNORE YOUR UPDATES!

ANTI - VIRUS & MALWARE

THE FREE STUFF IS GREAT JUST MAKE SURE IT'S ENABLED AND UPDATED.

FIREWALL

A FIREWALL IS YOUR FIRST LINE OF DEFENSE AGAINST ANY ATTACK.