IT Security Training

April 21, 2016

Presented by Benjamin Ellis

Arnett
Carbis
Toothman llp
CPAs & Advisors

Southeastern Ohio
SOOGA
Oil & Gas Association

Topics to be Covered

- What has changed to make IT security harder?
- What are the common areas your business is being attacked?
- What can you do about those areas?
- What products do we recommend to help?
- What are some things you can do to keep yourself and your family safe?

Anywhere Access

- Wireless Security
- Citrix / Terminal Services
- Intranets
- VPNs
- MiFis
- Hosted Services
- The Cloud

Multiple Devices

- Laptops
- Desktops
- Tablets
- Smartphones
- Desk Phones
- Kiosks
- Public Use Computers
- Servers

Mobile Devices

- 5-10 years ago Smartphones were just entering the workplace
  - Multiple platforms / No management tools available
- 3 years ago Tablets became an item
- Wild West from an IT security standpoint
- IT has little management over these devices
- Carriers abandon 1-year-old devices
- Android was not built with security as a concern

How is Business Being Attacked?

- Phishing
- Web Surfing:
  - Malware from ads and downloads
- Infected Files from:
  - USB
  - Emails
  - Portals
- Internet accessible services
- WHY? Big business in Ransomware, ID theft, Direct transfer from bank accounts (Zeus).

LinkedIn – Recent Exploits

- Well-developed, fake profiles linked to legitimate businesses.
- Used to send malicious links or emails to victims.
- Many of these profiles had 500 or more connections.
- *Users should "adopt a position of sensible caution" when engaging with unknown individuals who claim to have mutual connections. Just because that person is in a colleague's or friend's network doesn't mean the person is trusted.* ***Verify outside of LinkedIn who the person is before divulging information.***

Email Security

Phishing &
Spear Phishing

Phishing Attacks

- Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action.
- These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank, or your favorite online store.
- These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a message.
- Cyber criminals craft these emails to look convincing.

Phishing Attacks – The Four Types

- Harvesting information - usernames and passwords, credit cards, SSNs, etc.
- Infecting your computer with malicious links - to websites that will install Key loggers, redirectors, malware, etc.
- Infecting your computer with malicious attachments - such as PDFs, Excel, QuickBooks.
- Scams - generally asking you to send money.

Protecting Yourself

- Be suspicious of any email that requires “immediate action” or creates a sense of urgency.

- Be suspicious of emails addressed to “Dear Customer” or some other generic salutation. If it is your bank they will know your name.

- Be suspicious of grammar or spelling mistakes.

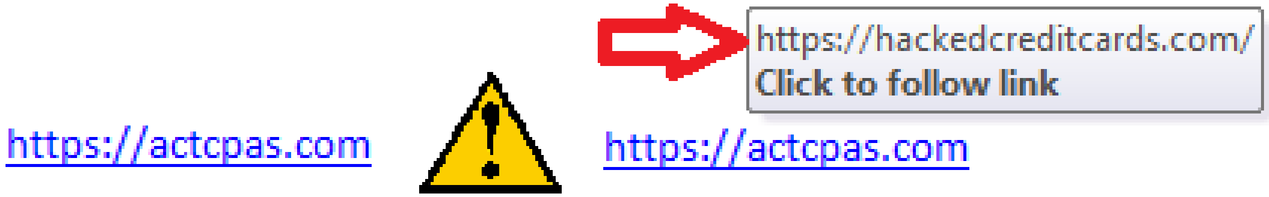
- Do not click on links.

Protecting Yourself

- Hover your mouse over the link to see true destination.
- Be suspicious of attachments and only open those that you were expecting.
- Just because you got an email from your friend does not mean they sent it.
- Stay diligent.

Validate Shortcuts/Links

- Shortcuts and Website links can easily be spoofed/faked.
- Always double check URLs for sites that deal with personal information.
  - Hovering over a link can display the actual URL you would be taken to if the link is clicked.



https://actcpas.com

https://hackedcreditcards.com/
Click to follow link

https://actcpas.com

  - If there is any doubt, manually type the address into your internet browser.

Validate Shortcuts/Links

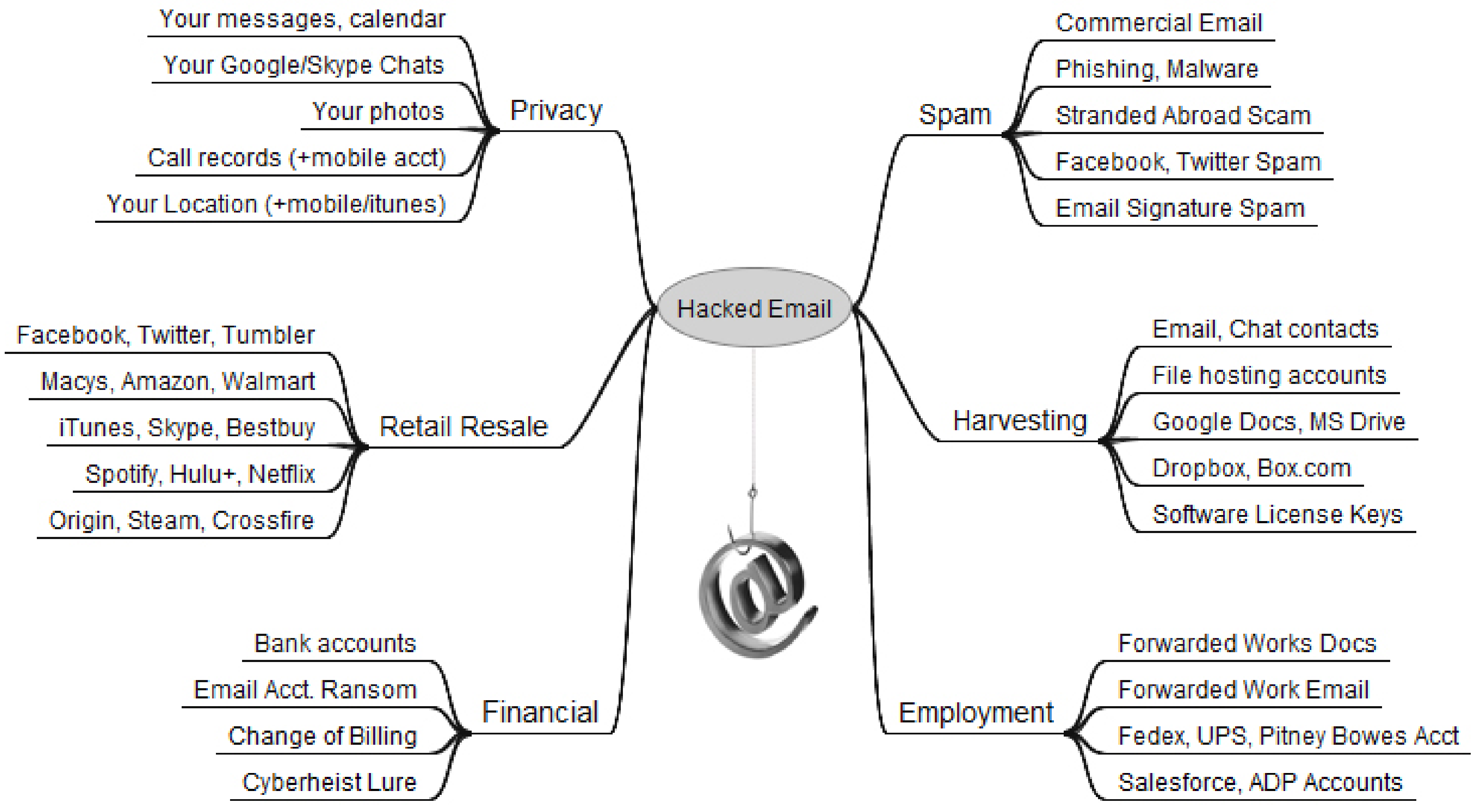
- Be mindful of search results.
  - The first result is not always the right one.
  - Sponsored /ad redirected results cannot always be validated.
- Many malicious websites attempt to mimic legitimate sites either in appearance or by the domain name.

- **Example:** MonPower.com
  - http://Monpower.com is a website on the internet.
  - The URL and site are designed to mimic **the real** utility website.
  - https://www.firstenergycorp.com is **the real** website.

Why Does Anyone Want My Email?

- Access to your personal information.
- Access to your company information.
- To send spam or Spear-phishing attacks.
- To access your online accounts through password changes.

Value of Hacked Email Account

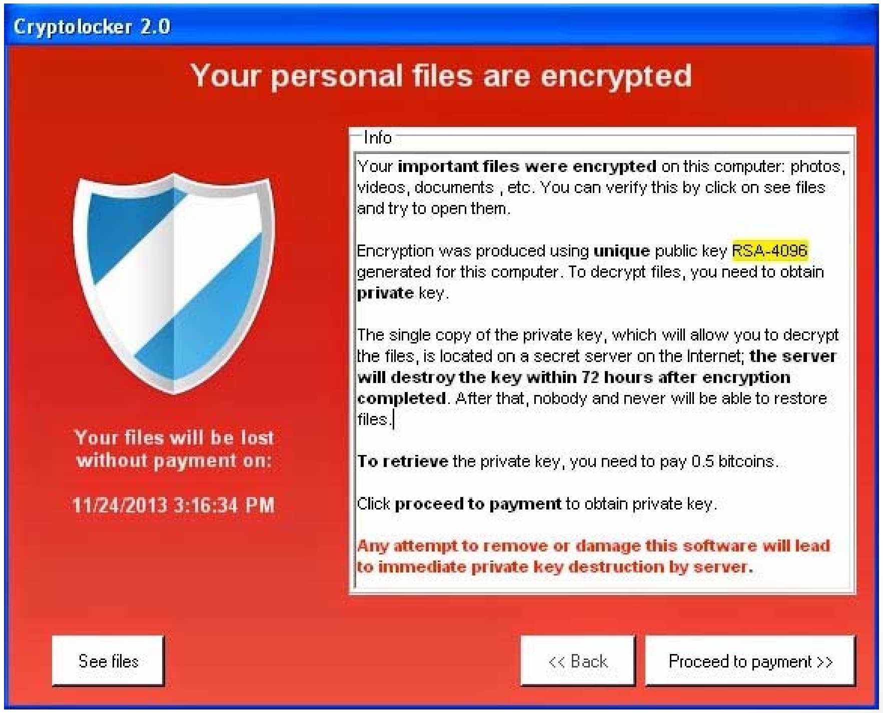


Hacked Email

- Privacy
  - Your messages, calendar
  - Your Google/Skype Chats
  - Your photos
  - Call records (+mobile acct)
  - Your Location (+mobile/itunes)
- Retail Resale
  - Facebook, Twitter, Tumbler
  - Macys, Amazon, Walmart
  - iTunes, Skype, Bestbuy
  - Spotify, Hulu+, Netflix
  - Origin, Steam, Crossfire
- Financial
  - Bank accounts
  - Email Acct. Ransom
  - Change of Billing
  - Cyberheist Lure
- Spam
  - Commercial Email
  - Phishing, Malware
  - Stranded Abroad Scam
  - Facebook, Twitter Spam
  - Email Signature Spam
- Harvesting
  - Email, Chat contacts
  - File hosting accounts
  - Google Docs, MS Drive
  - Dropbox, Box.com
  - Software License Keys
- Employment
  - Forwarded Works Docs
  - Forwarded Work Email
  - Fedex, UPS, Pitney Bowes Acct
  - Salesforce, ADP Accounts

Web Security

- Viruses / Malware from ads and downloads



Cryptolocker 2.0

Your personal files are encrypted

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Your files will be lost without payment on:

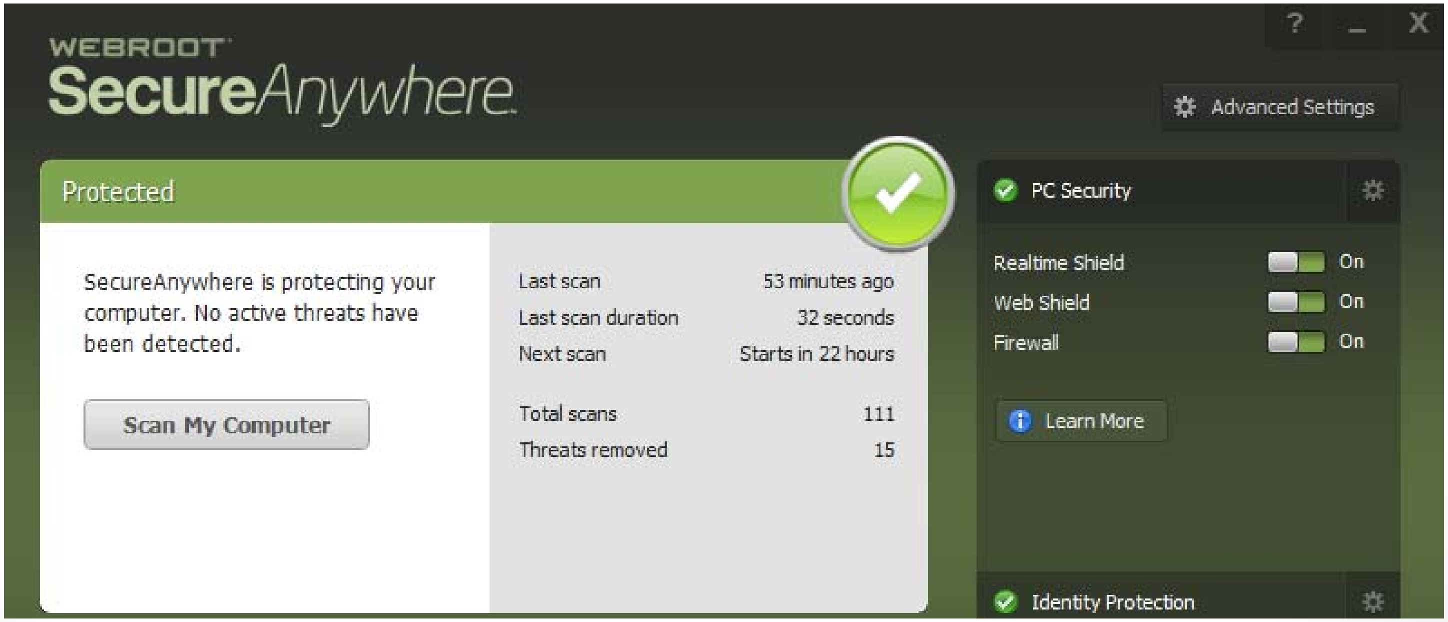
11/24/2013 3:16:34 PM

Types of Malware

- Malware - a program designed to damage your computer.
  - Virus - Looks to corrupt or delete data.
  - Worms - Replicate themselves.
  - Trojans - Disguised as a different application.
- Spyware - Captures user data and sends to remote user.
- Adware - Advertising.
- Ransomware - Prevents or limits users from accessing their system until users pay the ransom.

Run a good Anti-Virus

- Must Be Centrally Managed
- Should report infections to IT immediately
- Needs Real-time scanning and reporting
- Necessary to prevent well-known attacks



SecureAnywhere is protecting your computer. No active threats have been detected.

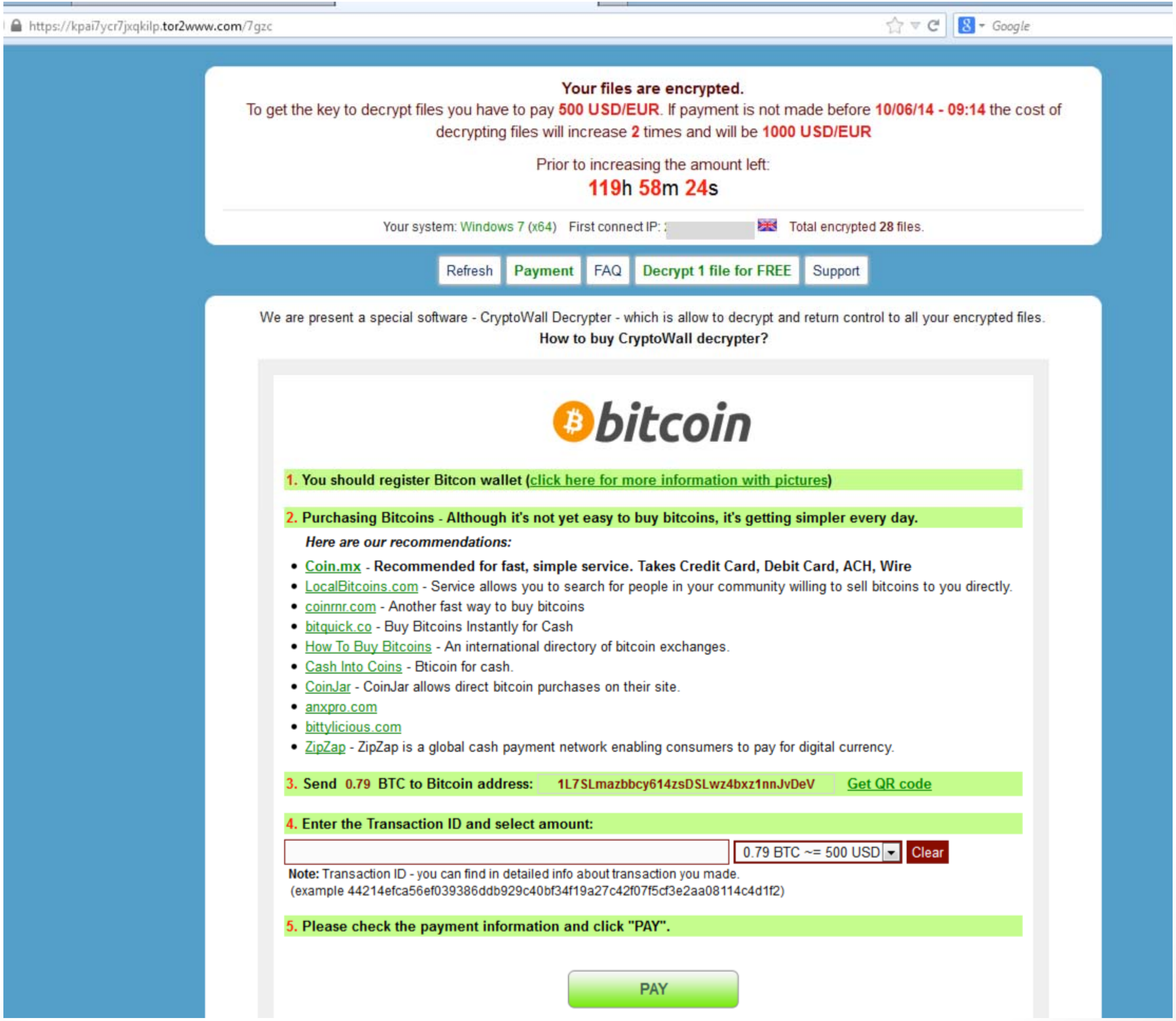
Last scan	53 minutes ago
Last scan duration	32 seconds
Next scan	Starts in 22 hours
Total scans	111
Threats removed	15

Realtime Shield	On
Web Shield	On
Firewall	On

The Best Anti-Virus Is You!

- Awareness and knowledge.
- Knowing the risks and being cautious.
- Only using reputable sources.
- Knowing that eventually you will be attacked and have the appropriate anti-virus protection.
- Viruses evolve and adapt too fast for AV companies to keep up.

CryptoWall



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **10/06/14 - 09:14** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

119h 58m 24s

Your system: Windows 7 (x64) First connect IP: [redacted] Total encrypted **28** files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- Coin.mx - **Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 0.79 BTC to Bitcoin address: 1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV **Get QR code**

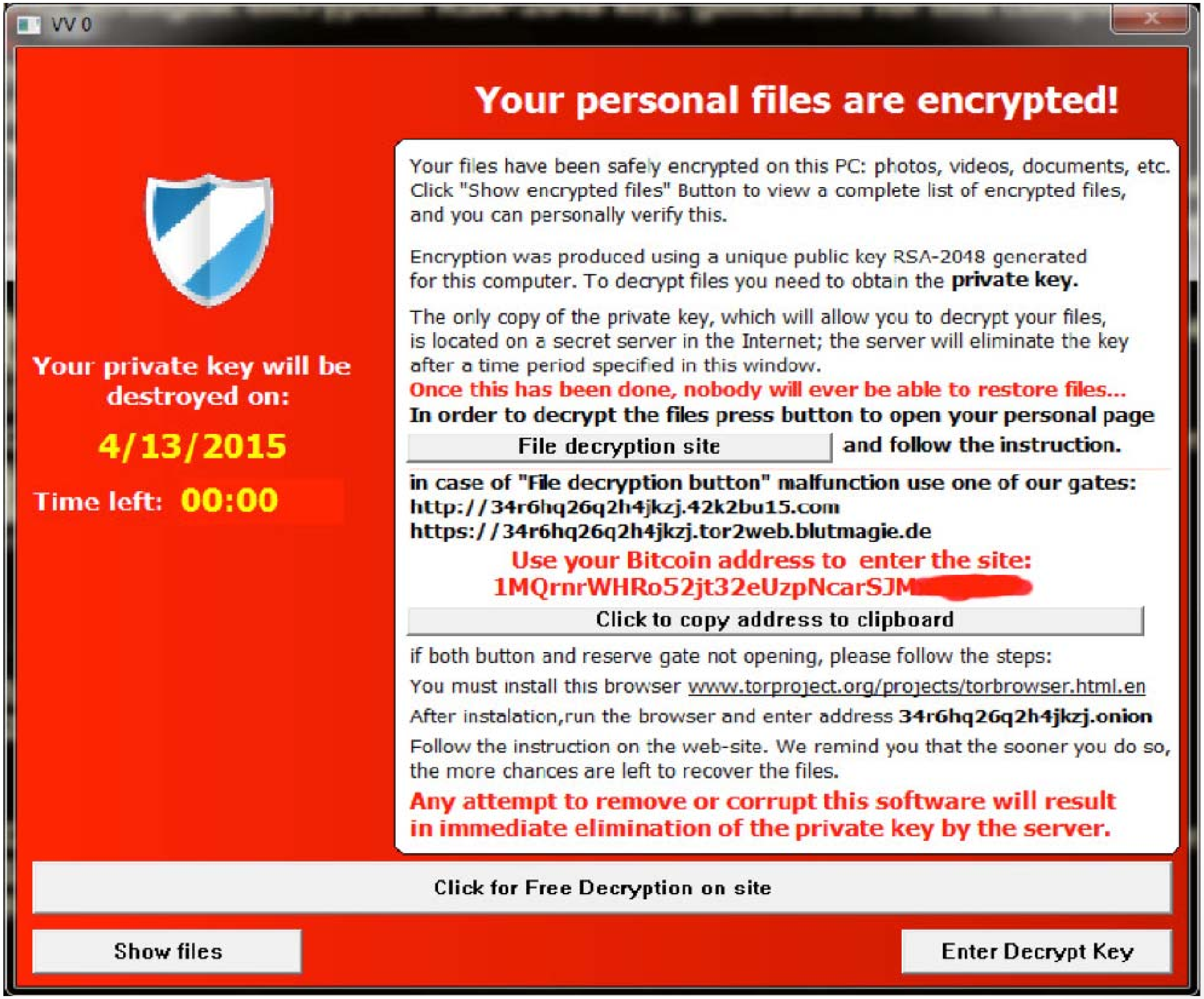
4. Enter the Transaction ID and select amount:

0.79 BTC ~= 500 USD Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

TeslaCrypt


VV 0
File decryption site
Click to copy address to clipboard
Click for Free Decryption on site
Show files
Enter Decrypt Key

Your personal files are encrypted!

Your private key will be destroyed on:

4/13/2015

Time left: 00:00

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
and follow the instruction.

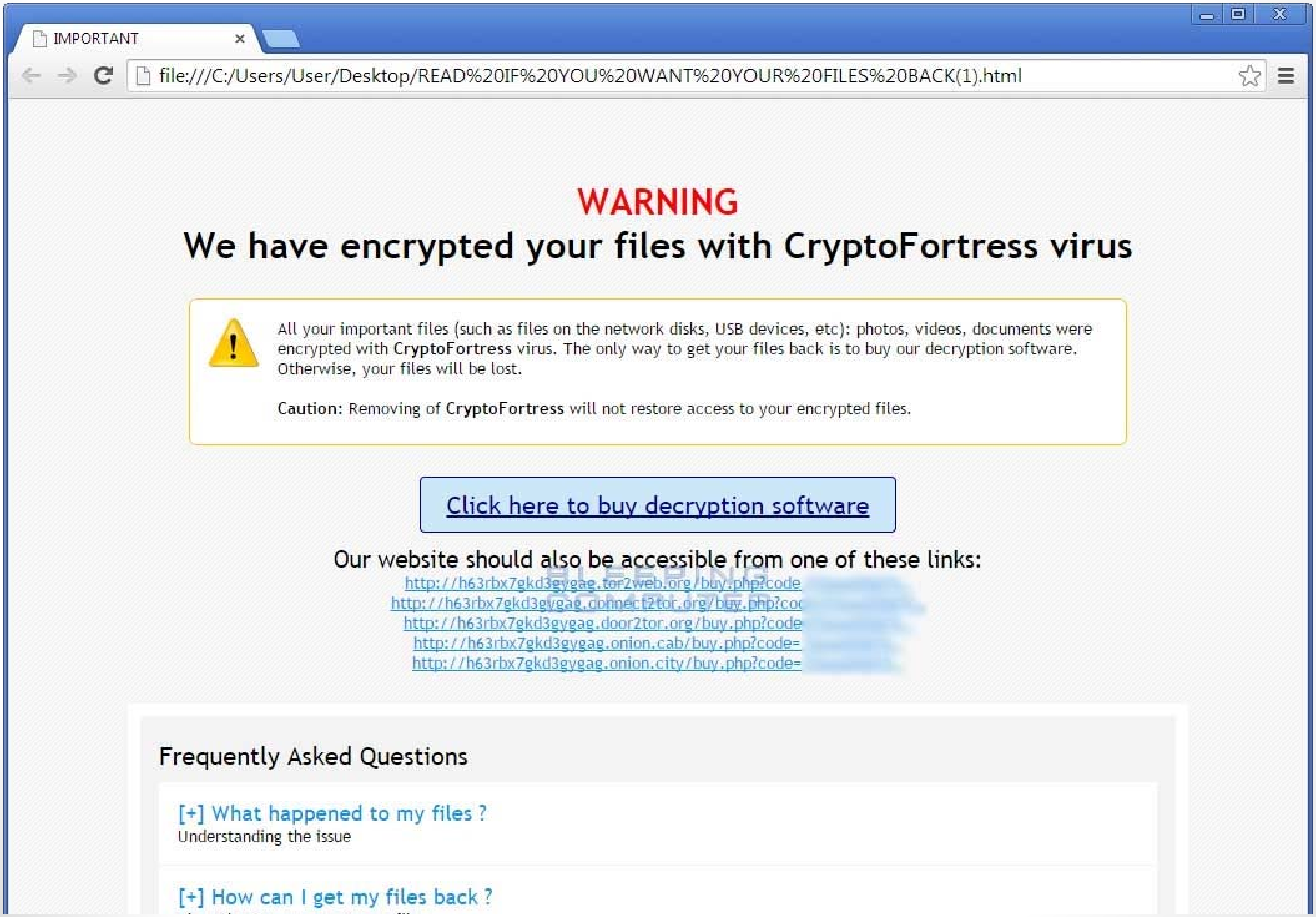
in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.42k2bu15.com
https://34r6hq26q2h4jkzj.tor2web.blutmagie.de

Use your Bitcoin address to enter the site:
1MQrnrWHRo52jt32eUzpNcarSJM[redacted]

if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

CryptoFortress



IMPORTANT
file:///C:/Users/User/Desktop/READ%20IF%20YOU%20WANT%20YOUR%20FILES%20BACK(1).html

WARNING

We have encrypted your files with CryptoFortress virus

All your important files (such as files on the network disks, USB devices, etc): photos, videos, documents were encrypted with **CryptoFortress** virus. The only way to get your files back is to buy our decryption software. Otherwise, your files will be lost.

Caution: Removing of **CryptoFortress** will not restore access to your encrypted files.

Click here to buy decryption software

Our website should also be accessible from one of these links:

http://h63rbx7gkd3gygag.tor2web.org/buy.php?code
http://h63rbx7gkd3gygag.connect2tor.org/buy.php?coo
http://h63rbx7gkd3gygag.door2tor.org/buy.php?code
http://h63rbx7gkd3gygag.onion.cab/buy.php?code=
http://h63rbx7gkd3gygag.onion.city/buy.php?code=
[redacted]

Frequently Asked Questions

[+] What happened to my files ?
Understanding the issue

[+] How can I get my files back ?

IT Security Best Practices

Tips and tricks to keep you safe

Suspicious Emails & Links

- Don’t let curiosity get the best of you.
- Always delete suspicious emails and links
- Even opening or viewing these emails and links can compromise your computer and create unwanted problems without your knowledge.
- Remember, if something looks too good to be true, it probably is.

Don’t Be Tricked into Giving Away Confidential Information

- Don’t respond to emails or phone calls requesting confidential company information including employee information, financial results, or company secrets.

- It’s easy for an unauthorized person to call us and pretend to be an employee or one of our business partners.

- Stay on guard to avoid falling for this scam.

- Report any suspicious activity to IT.

- Protect your personal information just as closely.

Always Use Hard-to-Guess Passwords

- Don’t use obvious passwords like “password,” “cat,” or obvious character sequences on the qwerty keyboard like “asdfg” and “12345.”

- Create complex passwords by including different letter cases, numbers, and even punctuation.

- Try to use different passwords for different websites and computers. So if one gets hacked, your other accounts aren’t compromised.

- Use Password Haystacks.

How to Create Strong Passwords

- **Size Does Matter: 8 Characters, Minimum**
  - You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 8 characters in length. A longer password would be even better.
- **Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters**
  - Use a mix of different types of characters to make the password harder to crack.

Firewalls

- UTM (Unified Threat Management) firewall combines:
  - Packet filtering
  - Anti-Virus
  - Content filtering
  - Intrusion detection
  - Intrusion prevention monitoring and control
  - Country blocking
  - VPN access
- Software firewalls
  - Domain / home or work / public

Best Small Business Firewalls

UTM Firewalls:

- Sophos
- Watchguard
- SonicWall

AntiVirus Products:

- Webroot
- Sophos
- Kaspersky

How to Create Strong Passwords

- **Isn’t a Dictionary Word or Combination of Dictionary Words**
  - Stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they’re obvious, is also bad. For example, “house” is a terrible password. “Red house” is also very bad.

- **Doesn’t Rely on Obvious Substitutions**
  - Don’t use common substitutions either - for example, “H0use” isn’t strong just because you’ve replaced an o with a 0. That’s just obvious.

How to Create Strong Passwords

- Try to mix it up - for example, “BigHouse$123” fits many of the requirements here. It’s 12 characters and includes upper-case letters, lower-case letters, a symbol, and some numbers. But it’s fairly obvious — it’s a dictionary phrase where each word is capitalized properly. There’s only a single symbol, all the numbers are at the end, and they’re in an easy order to guess.

- Password Haystacking – Added characters to every password.
  - Example: Tinker or Tinker11-=-=-=

Areas that need to be Covered?

- Antivirus
- Firewalls
- Passwords
- Wireless Networks (especially public)
- Public Computers
- Mobile Devices (tablets, phones, etc)
- Copiers
- USB and other external devices
- I think I have a Virus
- Encryption
- Software Updates and Update Management
- Backups, Online Backups, and offsite Backups
- Secure Browsing
- Content Filters
- Pop Up Blockers
- Training end users (especially on security)
- Protecting yourself at home
- And More…

Tools and Resources

- https://www.grc.com/haystack.htm?id=1
- http://www.sonicwall.com/furl/phishing/index.php
- https://www.opendns.com/phishing-quiz/
- http://www.networkworld.com/article/2991570/security/fake-linkedin-profiles-lure-unsuspecting-users.html

Questions?

Arnett
Carbis
Toothman llp
CPAs & Advisors

Call us!
304.346.0441