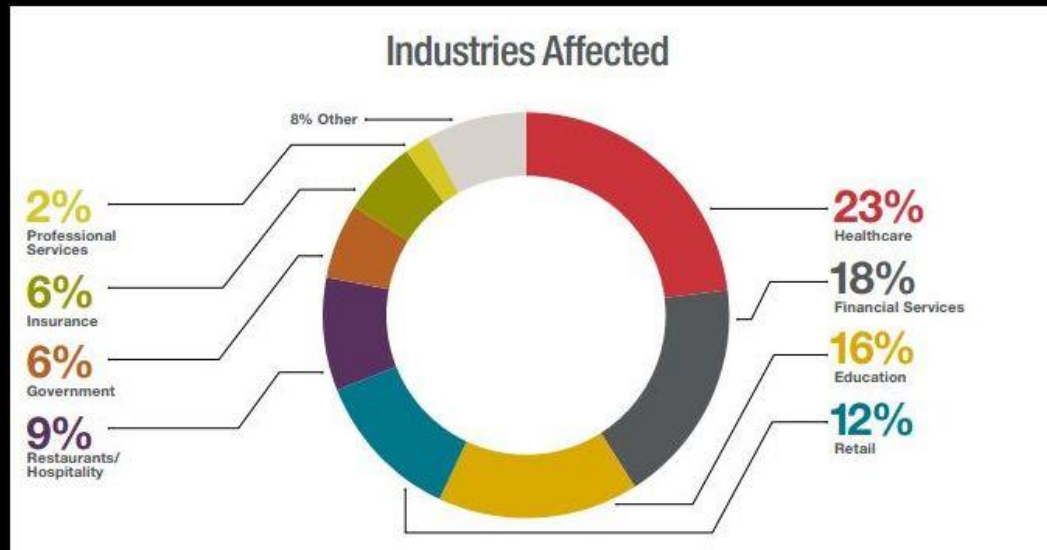


Oregon Cyber Task Force

Statewide resource to investigate complex computer intrusions and digital crimes.

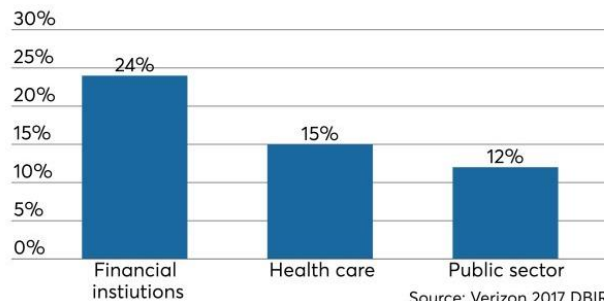
- Theft of Personal Identifiable Information (PII)
- Destruction or loss of data by malicious exploits
- Sales of PII
- Complex computer intrusions by organized crime
- Exploitation of vulnerabilities in critical infrastructure
- Network sabotage by insiders
- Education
- Forensic expertise





Top 3 industries for data breaches

Verizon's 2017 Data Breach Investigations Report revealed that 61 percent of victims were businesses with 1,000 or fewer employees

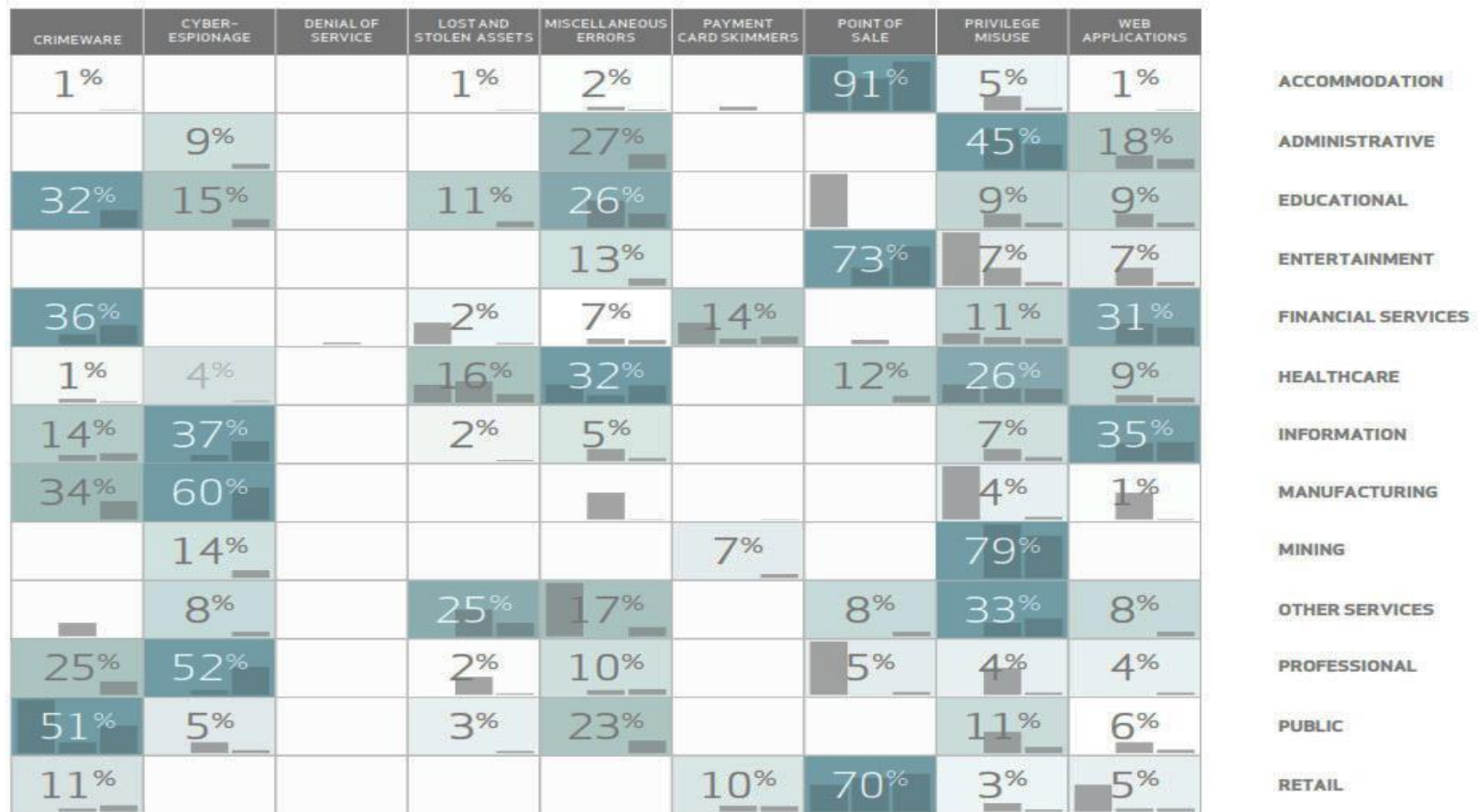


Top 10 Sub-Sectors Breached by Number of Incidents



<http://www.propertycasualty360.com/2016/04/12/what-are-the-leading-causes-of-data-security-breac/> / <https://healthitsecurity.com/news/healthcare-data-breaches-top-reported-data-security-incident/>

Frequency of breaches by incident type and victim industry



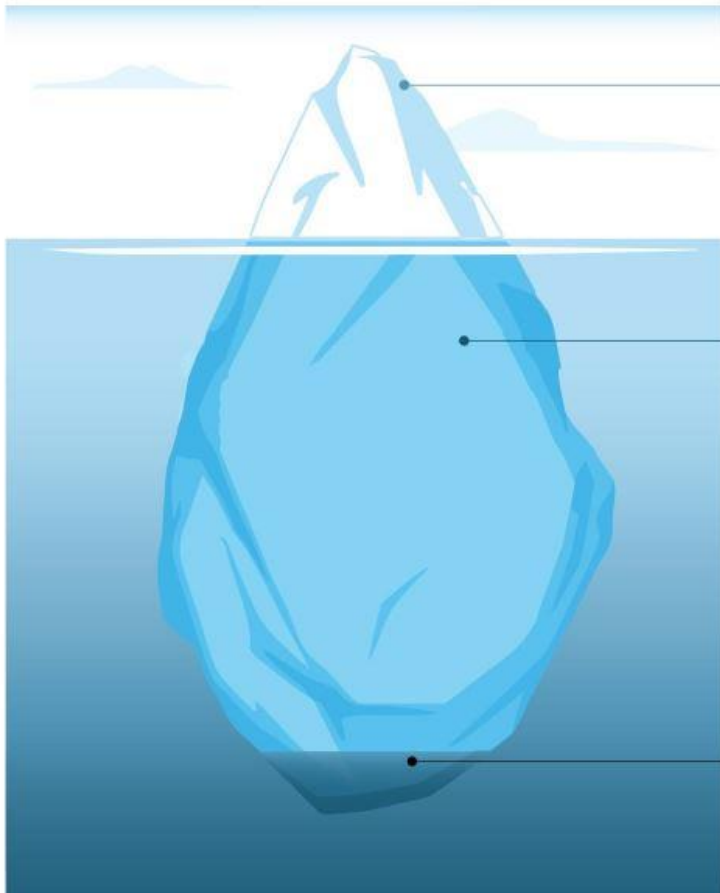
<https://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/> - Verizon Breach Report

- Darkweb and Hidden Services
- Cryptocurrency
- Organized Cyber Crime



(U) The Deep Web and the Dark Web

Cyber Division



The WEB

Searchable and Indexed

Accessed by Ordinary Web Browsers | Indexed by Traditional Search Engines

The DEEP WEB

Non-Searchable and Non-Indexed: Limited Access, Dynamic, or Unlinked Content

Accessed by Ordinary Web Browsers | Not Indexed by Traditional Search Engines

Login Sites and Forums | Mail Servers | Databases (Lexis Nexis, NOAA)

Private, Internal Networks | Search Results | Real-Time Feeds | Non-Indexed File Types

Contextual Web: Web Content Dependent on User Browsing Circumstances

IP Address Restriction (Great Chinese Firewall),

Platform (Mobile vs. Desktop), Protocol (HTTPS)

The DARK WEB

Hidden Content: Requires Anonymizing Software To Access (includes Tor*, I2P, Freenet)

Legal or Illegal | Dark Marketplaces (Silk Road): Controlled Substances

Child Pornography | Fraud | Money Laundering | Stolen Credit Cards | Pirated Content

Deeper into the DarkNet

The **DarkNet** consists of overlaying networks that use the public Internet but require specific software, configuration, or authorization to access.

Examples of tools to access the DarkNet include:

- **TOR**
- I2P
- Freenet



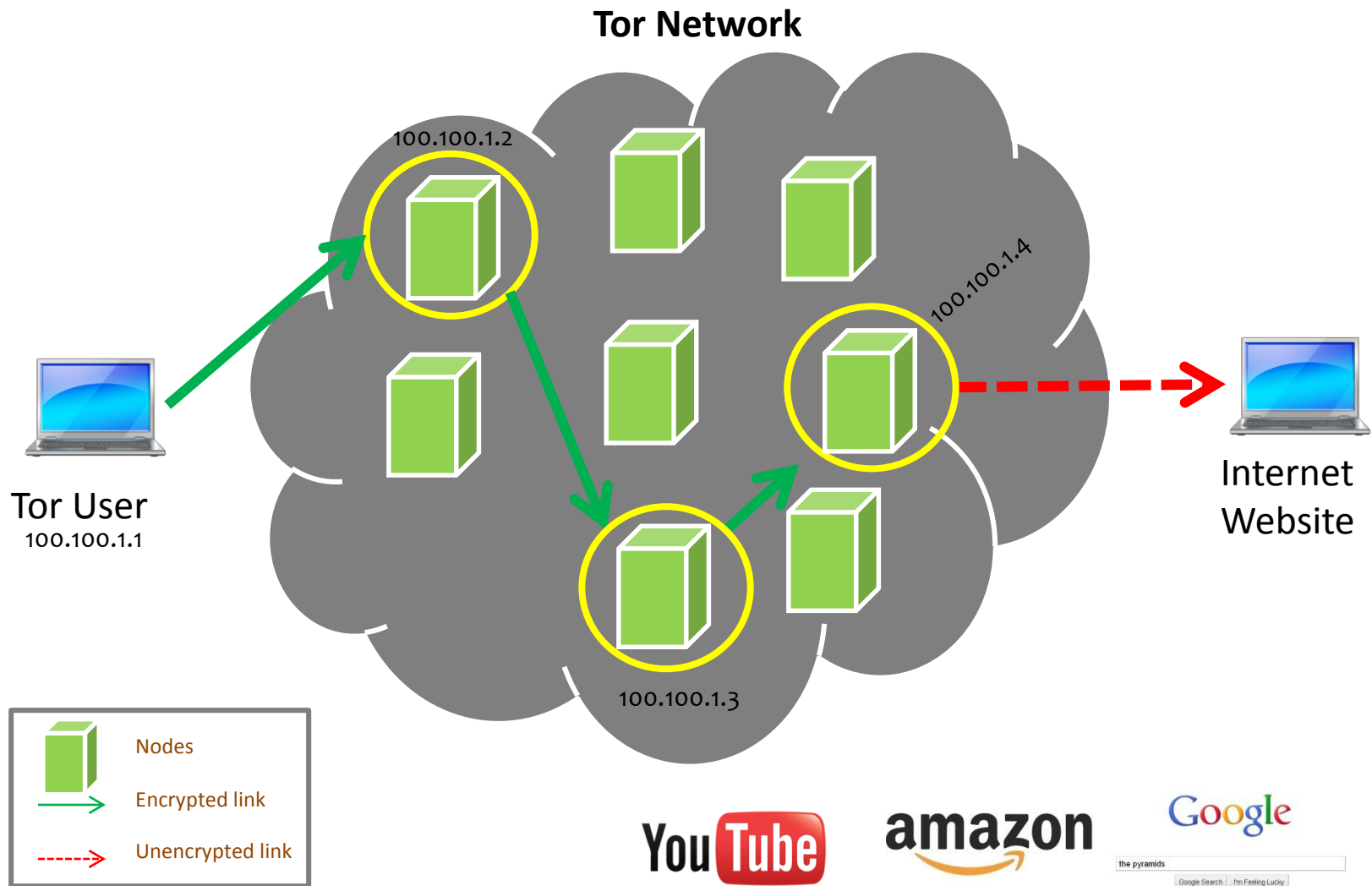
History of TOR

The Tor network is a group of volunteer operated servers that allows people to minimize their digital footprint, and increase privacy and security on the Internet. Tor connects through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.

- Derived from US Naval Research Laboratory's the onion routing project
- Managed by the non-profit agency The Tor Project
- Why would people use this technology?



How Tor Works



Hidden Services Websites

A website that anonymously resides on the Tor network

- Approximately 50-60k onion addresses on Tor
- Hidden services use the **.onion** domain

Example: **3g2upl4pq6kufc4m.onion**.

- 16-character alpha-semi-numeric hash value created from a key
- Can be made up of any letter of the alphabet, and decimal digits from 2 to 7
- Vanity .onion addresses can be created as well through a hash (facebookcorewwi.onion)

Key:

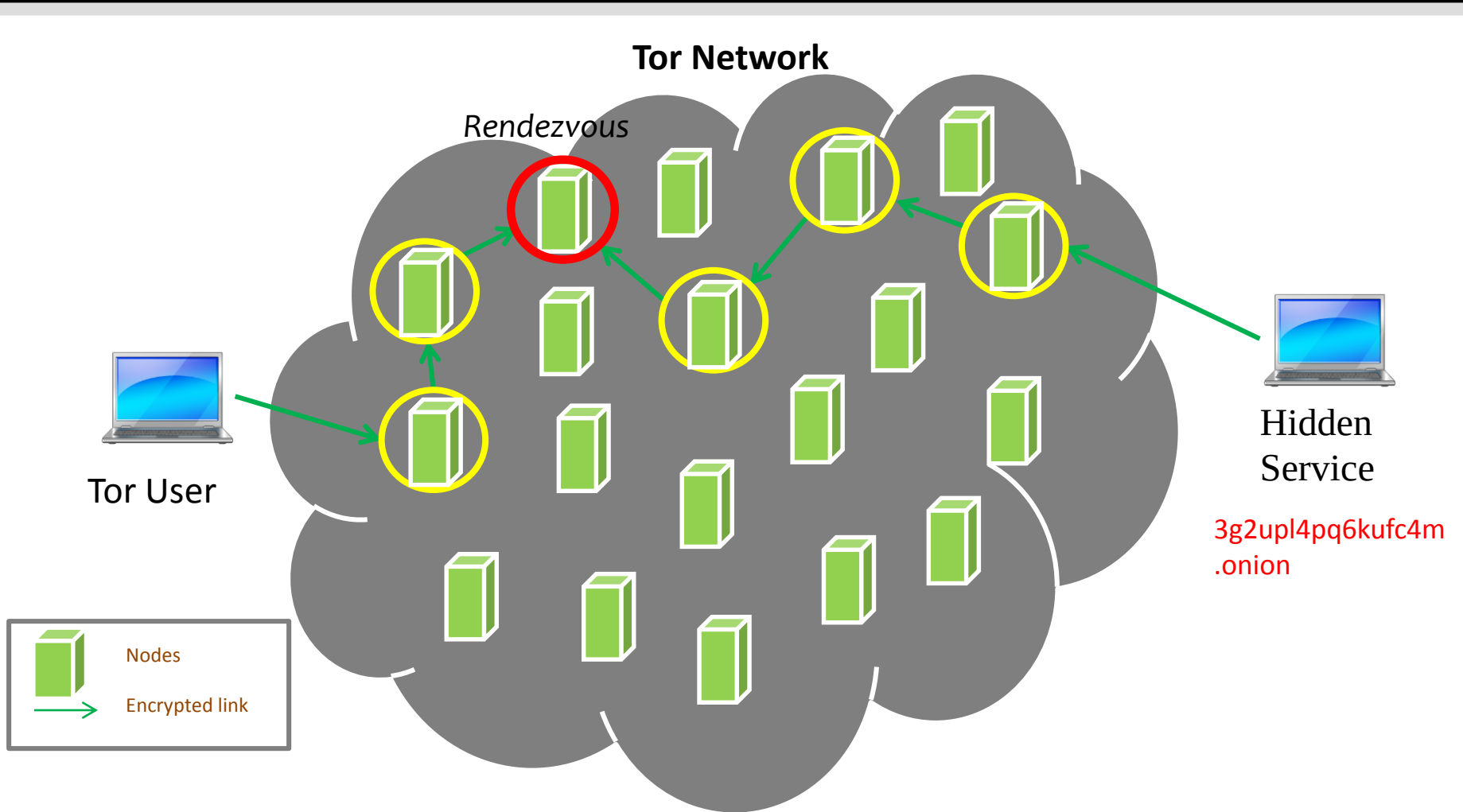
A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm.

Hash value:

A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash). The hash value is a representative of the original string of characters, but is normally smaller than the original.



How Hidden Services Work



Hides physical location of hidden service by using a rendezvous point.

Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845	AMEX	Charles A. B.	US	LA 90015	Y	N	Y	40\$	☐
528713	MasterCard	Christopher B.	US	Chicago IL 60604	Y	N	Y	40\$	☐
645450	DISCOVER	David M. Kelly	US	LA 90015	Y	N	Y	40\$	☐
371527	AMEX	J. B. Brown	US	LA 90015	Y	N	Y	40\$	☐
646880	DISCOVER	John M. Kelly	US	LA 90015	Y	N	Y	40\$	☐
651920	DISCOVER	John J.	US	LA 90015	Y	N	Y	40\$	☐
645857	DISCOVER	J. B. Brown	US	LA 90015	Y	N	Y	40\$	☐
371198	AMEX	J. B. Brown	US	LA 90015	Y	N	Y	40\$	☐
534248	MasterCard	Robert M.	US	LA 90015	Y	Y	Y	40\$	☐
371726	AMEX	Greg B.	US	LA 90015	Y	N	Y	40\$	☐
537161	MasterCard	Robert M.	US	LA 90015	Y	N	Y	40\$	☐
447639	VISA	Robert M.	US	LA 90015	Y	N	Y	40\$	☐
371730	AMEX	J. B. Brown	US	LA 90015	Y	N	Y	40\$	☐
528730	MasterCard	J. B. Brown	US	LA 90015	Y	N	Y	40\$	☐
653659	DISCOVER	J. B. Brown	US	LA 90015	Y	N	Y	40\$	☐
									Buy

CRYPTOCURRENCY



Virtual Currencies / Cryptocurrencies

Internet-based peer-to-peer (P2P) virtual currency having an element of cryptographic security wherein value is electronically transmitted between parties, without an intermediary.



Bitcoin | BTC



Monero | XMR



Ethereum | ETH



Dash | DASH



Litecoin | LTC

HOW TO USE BITCOINS

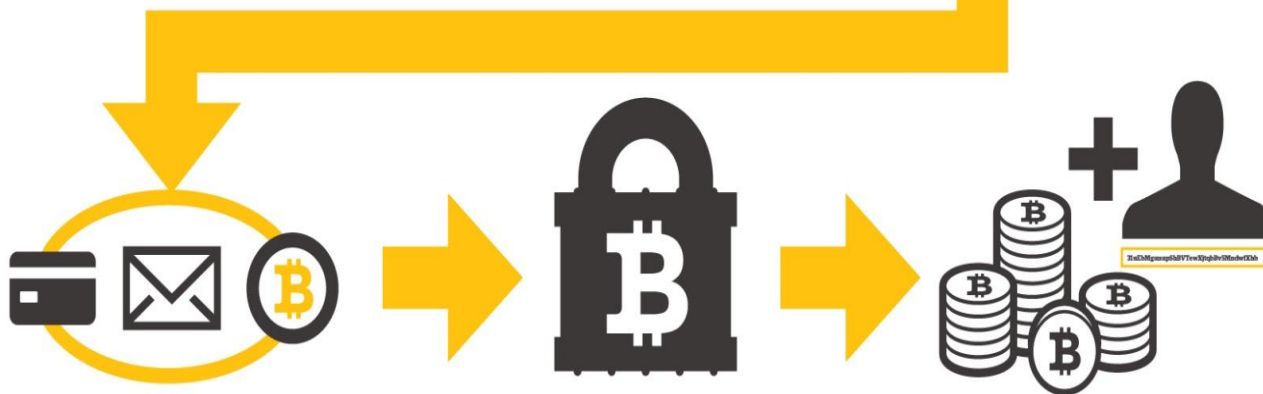


Download software to your computer or phone to set up a Bitcoin wallet. This gives you the basic facilities to send, receive and store Bitcoins



Your software will generate a unique string of letters and numbers: your Bitcoin address. The address isn't tied to your name or any other personal data, but it identifies you to the Bitcoin network. Give this address to anyone who needs to pay you

1EFgJf8F384dro29ryx3R8TGxy9P1FJPis



Buy Bitcoins with a standard offline currency, either from another user or through a dedicated Bitcoin exchange. Your new digital funds are added to your wallet

The Bitcoin network authenticates transactions by recording them in the 'block chain' - the underlying code that preserves the integrity of the currency

Use your software to send payments to other addresses. Divisions as small as 100,000,000th of a Bitcoin are possible - a unit called a 'Satoshi', after the currency's enigmatic inventor



BOTNET

Rentals can be used by crooks to stress test networks or distract their target during a larger cyber heist.

Rental Costs

- Daily: \$60
- Weekly: \$400

Discounts

- 10% on orders of \$500
- 15% on orders of \$1000



EXPLOIT KITS

Offer criminals a turnkey way to jump right into an attack with very little technical abilities.

Costs

“Nuclear Exploit Kit” Lease:
\$50/day,
\$400/week,
\$600/month

“Sweet Orange Exploit Kit” Lease:
\$450/week,
\$1800/month



RANSOMWARE RENTAL

“Radamant”
Ransomware

Costs

Kit for One Month:
\$1000

Average cost for Basic
Malware: \$10



Compromised Web Access

Compromised websites and servers are a favorite means for distributing malware and launching attacks.

Costs

- Cpanel: \$3-\$5
- RDP: \$10-\$25



STOLEN IDENTITY AND FINANCIAL INFORMATION

All sorts of shapes, sizes and packaging.

Costs

US Payment Card
Number With CVV2:
\$5-\$8
Plus Bank ID
Number: \$15
Card Number with
details about card &
owner ("Fullz"): \$30

Significant Cyber Incidents in Oregon

- Point of Sale Malware
- Online Extortion
- Ransomware
- Business Email Compromises
- Data Breaches
- Internet Fraud
- Insider threats
 - Theft or destruction of data
 - Sabotage of infrastructure
 - Intentional leaking of information



Ransomware – Putting It Together

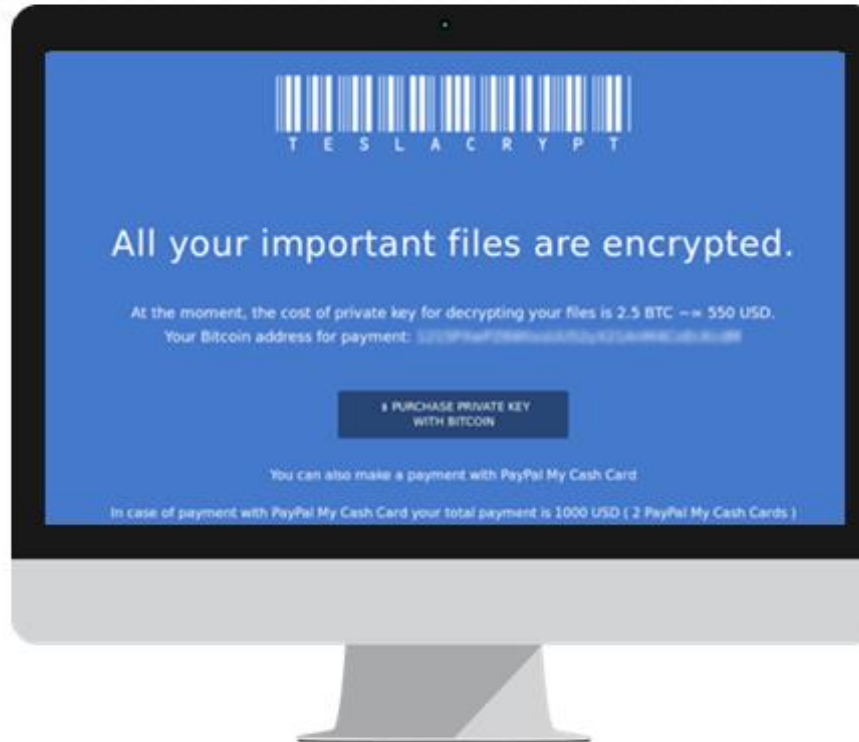
What is It?



How does it infect devices?



What happens after infection?



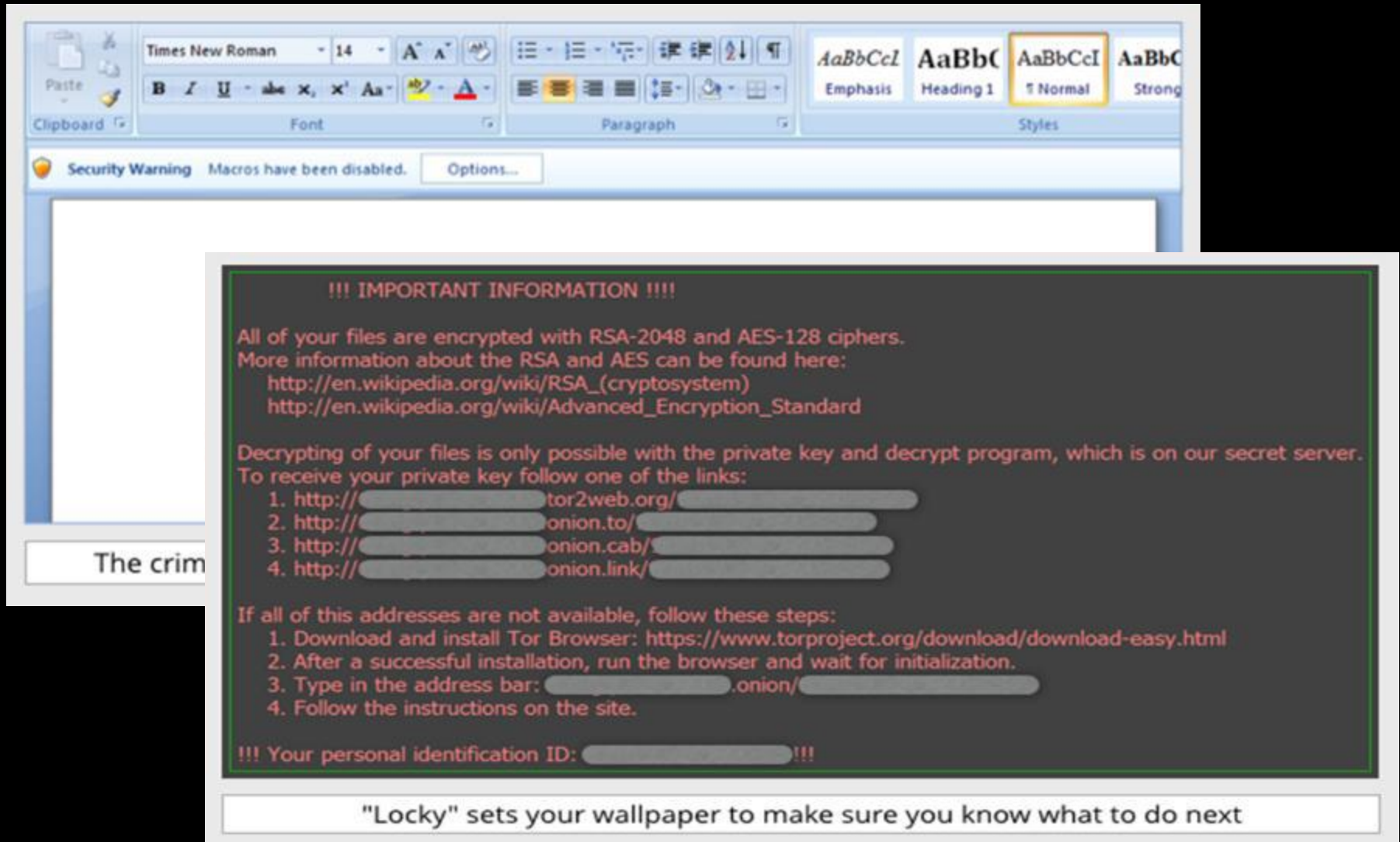
Should I pay the ransom?



How do I avoid infection?



Before/After



!!! 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/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 server.
 To receive your private key follow one of the links:

1. [http://\[redacted\]tor2web.org/\[redacted\]](http://[redacted]tor2web.org/[redacted])
2. [http://\[redacted\]onion.to/\[redacted\]](http://[redacted]onion.to/[redacted])
3. [http://\[redacted\]onion.cab/\[redacted\]](http://[redacted]onion.cab/[redacted])
4. [http://\[redacted\]onion.link/\[redacted\]](http://[redacted]onion.link/[redacted])

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: [\[redacted\].onion/\[redacted\]](http://[redacted].onion/[redacted])
4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted] !!!

"Locky" sets your wallpaper to make sure you know what to do next

CryptoWall Ransom and Personal Pages

CryptoWall 4.0 Ransom Page

Personal Page

Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?

Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key. In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?

The first thing you should do is to read the instructions to the end.

Your files have been encrypted with the CryptoWall software; the instructions that you find in folders with encrypted files are not viruses, they are your helpers.

After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions.

Think logically - we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them.

Any of your attempts to restore your files with the third-party tools can be fatal for encrypted files.

The fact is that changing data within the encrypted file (as 100% of software to restore files do this, except the special decryption software) you break damage to the file and it will be impossible to decrypt the file.

This is the same as to collect a mosaic: when some mosaics items were lost, broken or not put in its place - the picture will not emerge, the software to restore the files will not be able to lay down the picture, and ruin it completely and irreversibly.

Using the software to restore files can ruin your files forever, only through your fault.

Remember that any intervention of the extraneous software to restore files encrypted with the Cryptowall software may be the point of no return.

In case if these simple rules are violated we will not be able to help you, and we will not try because you have been warned.

For your attention the software to decrypt the files (as well as the private key that come fitted with it) is a paid product.

After purchasing the software package you can:

1. Decrypt all your files.
2. Work with your documents.
3. View your photos and other media content.
4. Continue your habitual and comfortable work at the computer.

If you are aware whole importance and criticality of the situation, then we suggest you go directly to your personal page where you will be given final instructions, as well as guarantees to restore your files.

There is a list of addresses below through which you can get on your personal page:

1. [http://www.cryptowall.com/personal](#)
2. [http://www.cryptowall.com/personal](#)
3. [http://www.cryptowall.com/personal](#)
4. [http://www.cryptowall.com/personal](#)

What do you have to do with these addresses?

If you browse the instructions in TXT format (if you have instruction in HTML (the file that has an icon of your internet browser) then for the sake of simplicity it is better to run it).

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: **192.168.1.1** Total encrypted 28 files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

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.
- [coinmr.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](#) - Bitcoin 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: **1L7SLmazbby614zsDSLwz4bxz1nnJvDeV** [Get QR code](#)

4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cd3e2aa08114c4d1f2)

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

PAY

How To Spot A **PHISH**



Types of Phishing Attacks



Spear Phishing: A highly targeted form of phishing that hones in on a specific group of individuals or organization.



Whaling: A form of phishing, targeted at executive level individuals.



Cloning: Whereby a legitimate email is duplicated but, the content is replaced with malicious links or attachments.

PARTNERS
HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

What is Phishing? A technique used to fraudulently obtain usernames, passwords, credit card numbers, and other sensitive information.



Fraudulent emails typically ask you to:

- Open an attachment or,
- Click on a link, redirecting you to a malicious website.
- You may be prompted to enter personal information.

Anatomy of a Phishing Email

Contains links or attachments

Poor grammar and spelling

Requests personal or sensitive information

High sense of urgency and/or privacy

Discusses confidential subjects like salaries

Incentivizes through threat or reward



**KEEP IT
SAFE
AND
SECURE**

For more information visit: www.ispo.partners.org.

What Can You Do?

How Does it
Work?
Types of
Schemes
Statistics
How is the
Money
Moved?
Why is it
Growing?
What Can
You Do?

PASSWORD DISCIPLINE

- Use long passwords
- Don't re-use passwords for more than one account
- Consider changing passwords frequently
- Consider using a Password manager



What Can You Do?

How Does it
Work?
Types of
Schemes
Statistics
How is the
Money
Moved?
Why is it
Growing?
What Can
You Do?

INFORMATION TECHNOLOGY SAFETY

- Patch and Update Immediately.
- Use Antivirus and anti-Spyware.
- If you run a company, consider setting up a stand-alone network for employees to use for personal email and web activity.

What Can You Do?

How Does it
Work?
Types of
Schemes
Statistics
How is the
Money
Moved?
Why is it
Growing?
What Can
You Do?

EMAIL TIPS

- If suspicious activity is ever suspected with your email:
 - Change your password right away & Log out all others
 - And then check for new “Rules” on your account
- Look for Webmail that allows for monitoring logins to your account and gives you the ability to log out others.



What Can You Do?

How Does it
Work?
Types of
Schemes
Statistics
How is the
Money
Moved?
Why is it
Growing?
What Can
You Do?

IT SECURITY & STAFF

- If you run a company large enough to have IT staff, allow them to attend conferences and training to stay current with industry trends.
 - Consider Penetration testing services
- If you outsource IT needs, ask your provider what they are doing to protect you from cyber attacks.



What Can You Do?

How Does it
Work?
Types of
Schemes
Statistics
How is the
Money
Moved?
Why is it
Growing?
What Can
You Do?

SOCIAL MEDIA

- Posting of business or vacation travel of company staff could let scammers know when executives are out of reach.
- Social Media can also provide scammers with information about friends, family, and business deals.





Questions?

**Oregon Cyber Task Force
9109 NE Cascades Parkway
Portland, Oregon, 97220
Tele: (503) 460-8000**