ERA
european.law

THE LIFE CYCLE OF E-EVIDENCE

HANDLING E-EVIDENCE IN ONLINE FRAUD CASES

Athens, 7-8 November 2017

UP GRADE
YOUR LEGAL EXPERTISE
Criminal Law

Professional Training (CPD)
www.era.int

Speakers & Chairs

Dominikos Arvanitis, Attorney at Law, Supreme Court, Athens Bar Association

Cormac Callanan, CEO, Aconite Internet Solutions, Dublin

Laviero Buono, Head of Section for European Criminal Law, ERA, Trier

Ilias Chantzos, Senior Director EMEA and APJ, Global CIP and Privacy Advisor, Government Affairs, Symantec Corporation, Brussels

Hein Dries, CEO, Vigilo Consult, Leiden

Jari Javanainen, Senior Security Manager, Tieto CIRT Team, Vantaa

Petr Klement, Prosecutor, Department of Serious Economic and Financial Crime, Prosecution Office, Prague

Stephen Mason, Barrister and Associate Research Fellow, Institute of Advanced Legal Studies, London

Georgios Papadopoulos, Advocate, Athens Bar Association

Michael Rachavelias, Legal Counsel, Attorney at the Court of Appeals, Larissa

Neil Walsh, Chief, Global Programme on Cybercrime, United Nations Office on Drugs and Crime (UNODC), Vienna

Key topics

- Credit card fraud: a challenge for the application of traditional fraud provisions
- Online auction fraud (cases, technical solutions and legal responses)
- Challenges in investigating and prosecuting internet fraud: phishing (including dummy corporations and boiler room ops)
- Fraud committed with electronic means of payment: experiences in EU Member States
- Involvement of the internet industry in fighting online financial crimes

Language
English

Event number
317DT62

Organiser
ERA (Laviero Buono) in cooperation with the Athens Bar Association

With the support of the Justice Programme 2014-2020 of the European Union

THE LIFE CYCLE OF E-EVIDENCE

Tuesday, 7 November 2017

08:30 Arrival and registration of participants

09:00 Welcome and introduction
President of the Athens Bar Association; Laviero Buono

I. E-EVIDENCE IN ONLINE FRAUD CASES: AN OVERVIEW

09:15 **Some considerations when dealing with electronic evidence in online fraud criminal proceedings**
- The investigation and evidence
- An issue – jurisdiction
- Presentation of evidence in court

Stephen Mason

10:15 Discussion

10:30 Break

Chair: *Stephen Mason*

11:00 **Online financial crimes and fraud committed with electronic means of payment**
- e-Evidence in internet-related money laundering
- Dissemination of false information and online extortion
- Computer-related fraud: a challenge for the application of traditional fraud provisions

Michael Rachavelias

11:45 **Fraud across Virtual Borders IRL (in real life)**
- Profiling the good, the bad and the ugly
- Filtering and blocking
- Circumvention, encryption and hiding online
- Virtual evidence – an oxymoron?
- MLAts, EIO's, collaboration – volunteers required!
- Virtual courts, virtual judges, virtual prisons

Cormac Callanan

12:30 Discussion

12:45 Lunch

II. CASE STUDIES ON ONLINE FINANCIAL CRIMES AND INTERNET FRAUD

Chair: *Georgios Papadopoulos*

14:00 **Internet fraud, Bitcoin and cryptocurrency investigation**
Neil Walsh

14:45 **The challenges in handling e-evidence in online fraud cases: a view from the coalface**
Jari Javanainen

15:30 Discussion

15:45 Break

III. PRACTICAL EXPERIENCES IN EU MEMBER STATES

Chair: *Laviero Buono*

16:15 **Criminal money flows and financial investigations on the internet**
Petr Klement

Objective

Credit card fraud is a highly profitable criminal activity which involves the unauthorised taking of another person's credit card information for the purpose of using the money available on an account or removing funds from it. To respond effectively to this threat, cooperation between law enforcement authorities and the private sector is crucial. This seminar will look at the different forms of payment fraud, at concrete examples of credit card fraud and at the key role played by the exchange of information between the public and private sectors.

Who should attend?

Judges, prosecutors and lawyers in private practice.

Location

Athens Bar Association
60 Akadimias Str.
GR-106 79 Athens

Participation fee

€ 200

This programme has been produced with the financial support of the Justice Programme 2014-2020 of the European Union.

The content of this programme reflects only ERA's view and the Commission is not responsible for any use that may be made of the information it contains

Your contacts

Laviero Buono
Head of Section
E-Mail: LBuono@era.int

Liz Klopocki
Assistant
E-Mail: EKlopocki@era.int

16:45 **Online financial offences and e-evidence in legal proceedings: the view of the defence**
Dominikos Arvanitis

17:15 Discussion

17:30 End of the first day

20:00 Dinner

Wednesday, 8 November 2017

IV. TACKLING CREDIT CARD FRAUD MORE EFFECTIVELY: THE ROLE OF THE PRIVATE SECTOR

Chair: *Stephen Mason*

09:00 **The internet industry perspective**
- General involvement of the internet industry in online credit card fraud
- Detection and prevention of internet fraud
- Policy and concrete case studies

Cormac Callanan

10:00 **Examples of digital information theft and best practices to prevent it**
Ilias Chantzos

10:30 Discussion

10:45 Break

V. LATEST TRENDS AND POSSIBLE NEW SCENARIOS IN CREDIT CARD FRAUD

Chair: *Laviero Buono*

11:15 **e-Evidence in concrete skimming and phishing cases (including also dummy corporations and boiler room ops)**
Hein Dries

12:00 Discussion

12:30 End of seminar and lunch

For programme updates: **www.era.int**
Programme may be subject to amendment.

Apply online for this seminar:
www.era.int/?126366&en

Discover Athens

Discover Athens, built on centuries of history and surrounded by diverse culture.

Experience what inspired the Ancient Greeks, immerse yourself in the city's rich and varied history, or simply take a stroll and soak up the atmosphere. Explore some of the main attractions and landmarks and visit Mount Lycabettus, the National Archaeological Museum or the Acropolis to name but a few.

CPD

ERA programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). This event corresponds to **9.5 CPD hours**.

Save the date

Annual Forum on Combating Corruption in the EU 2017
Trier, 21-22 September 2017

Annual Conference on EU Criminal Justice 2017
Trier, 23-24 October 2017

More information at:
www.era.int

e-Learning course

Fighting Child Pornography Online: 10 Key Questions

e-Presentations

Cyber Menaces and Different Types of Cybercrime Offences
Cormac Callanan

Cloud Computing: Implications for the Criminal Justice System
Ian Walden

More information at:
www.era.int/elearning

SOME CONSIDERATIONS WHEN DEALING WITH ELECTRONIC EVIDENCE IN ONLINE FRAUD CRIMINAL PROCEEDINGS

Stephen Mason, Barrister

Handling e-evidence in online fraud cases

L'Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l'Académie de droit européee

In cooperation with the Athens Bar Association

Athens, 7-8 November 2017

Co-funded by the Justice Programme of the European Union 2014-2020

Outline

The investigation and evidence

An issue – jurisdiction

Presentation of evidence in court

Investigation and evidence

Martin, R. v [2013] EWCA Crim 1420

An appeal against sentence

5 offences of unauthorised modification of computer material contrary to section 3(1) of the Computer Misuse Act 1990

1 offence of securing unauthorised access to computer material with intent contrary to section 2(1)(a) of the Computer Misuse Act 1990

1 offence of securing unauthorised access to computer material contrary to section 1 of the Computer Misuse Act 1990

2 offences of making, supplying or obtaining articles for use contrary to section 3(A) and (5) of the Computer Misuse Act 1990

Facts in brief

1. Martin launched a Denial of Service (DOS) attack on the University of Oxford web site shortly before 11.40 am on 3 March 2011

2. On 10 March 2011 Martin made an anonymous telephone call to one David Bradley, telling him that all of his personal and financial information was available on the internet

Mr Bradley immediately tried to log on to his bank account with his original password - it did not work - he tried the one given by the appellant - it worked

3. At 8.34pm on 10 February 2012 an internet order for a pizza delivery to Martin's home address was placed through the web site of Domino's Pizza using the PayPal account of one Neil Kerin

Martin had earlier obtained Mr Kerin's computer password while working for him as a self-employed computer repairman - Mr Kerin's partner identified the pizza transaction whilst going through her e-mails on 11 February 2012

Mr Kerin went to the delivery address at 8.00pm - a woman at that address denied any knowledge of the transaction - Mr Kerin recognised Martin when he came downstairs and he challenged him - Martin denied it but said Mr Kerin would be reimbursed

4. At 3.50pm on 29 January 2012 Martin launched a DOS attack on the University of Cambridge web site

5. At 9.45am on 1 February 2012 Martin launched a DOS attack on a web site belonging to the Kent Police

The evidence – Oxford DOS attack

From paragraph 6 of the law report:

On 23 March 2011, the appellant sent to that University an e-mail signed SL1NK which said: “You Just Don’t fucking learn”. On 2/3 December 2011 he sent it a further e-mail which read:

> “I have owned you once before (DDOS attack about six to seven months ago?) and I am going to do it again along with Cambridge. I have access to your SQL users and password database, they are encrypted as you obviously know but it won’t take long and by the time you have read this message I will have sold the two databases and what is needed to have been done will have been done”.

Martin made the IP address appear to come from the United States

The evidence – police investigation

On 3 May 2011 when investigating a burglary, searched Martin's home address in Dover

They seized four USB storage devices and a desktop computer

They found nothing pertaining to the burglary on those items and returned them to Martin at his home address

When they were at his home, one of the officers noticed an envelope with the name of another person on it

Martin offered to pay the officer £1,000 to say that he had not seen the envelope

He was re-arrested and interviewed

Further forensic examination was then made of the items that had been seized

The evidence – further DOS attacks

After Martin initiated the DOS attack on the University of Cambridge, he telephoned the BBC South East news desk and informed a journalist that he had hacked into the Kent Police web site

He said he was doing it ‘because I can’

He would not give his name, but gave the journalist a SL1NK e-mail address

The journalist informed her editor, who then informed the police

Martin also made a number of telephone calls to his girlfriend during the attack

He discussed the attack and suggested that he might try and attack the Metropolitan Police web site instead

Further evidence in the Cambridge DOS attack

The attack was traced and a block placed on the IUP address

Normal service was resumed after about 20 minutes

Later the University server received further connections via a tool used by network engineers to probe networked computers for information

Just after 5.00pm the University received an e-mail from SL1NK which said:

> “I have your user and password database sat on my drive and I am also guessing you have noticed your site CAM.AC.UK is under attack” and: “If you ban the IP address I will just switch it again so don't waste your time”.

Further access attempts and further e-mails from SL1NK were received, one of which read: “You will never find me and you know you won’t”.

The evidence – further police investigation

On 3 February 2012 the police executed a warrant and searched Martin's home – he said to the police 'The Kent Police website was hacked the other day'

He was arrested his computers were seized

He said they were all encrypted and refused to provide passwords until he had seen his solicitor

Conclusions by Court of Appeal judges on this particular point:

- The fact of encryption speaks of the sophistication of this operation
- It does not appear that the appellant ever accurately provided the encrypted passwords
- The information was to the effect that he had forgotten it
- The judges found that explanation lacking in plausibility
- It might have been plausible at the moment that he was initially interviewed, but not thereafter

The evidence – continued

A handwritten list headed ‘Possible Targets’ was recovered from his grandparents’ address

Next to the heading was written: ‘False ID, diplomatic immunity, prepaid cards/ccs’

The following targets were listed:

> Serious and Organised Crime Agency, BBC, Army UK, Oxford Cambridge Uni, Kent Met Police, MI5 6, Fed Reserve, Channel 5 TV, CIA, NSA, FISA, Sony again LOL, major news organisations, HMBC

A mobile telephone in Martin’s possession contained personal data belonging to Mr Kerin and his partner including passwords, e-mail addresses, bank account numbers and credit card numbers

The evidence – continued

The computer equipment seized from Martin's home address was analyzed and found to contain

- references to SL1NK
- files with titles such as 'Bank Hack' containing personal information on Mr Bradley
- personal banking and credit card details for others

A link led to a web site with a screen-shot of Mr Bradley's online bank account and information on other accounts, credit cards and loans

SL1NK's exploits were referenced on other web sites and a hacking forum

In interview Martin said that

- he had used the name SL1NK but it was 'just a pseudo name' and that many others used it
- he denied carrying out the DOS attacks

His denial was undermined by his admissions

Complex investigations

Carousel fraud (missing trader intra-Community fraud)

Pomfrett, R v [2009] EWCA Crim 1939

http://www.bailii.org/ew/cases/EWCA/Crim/2009/1939.html

One of a number of frauds and related money laundering offences investigated in the period 2002 to 2006 under code-names – Operation Vitric and Operation Devout

This prosecution arose out of Operation Devout II

His defence:

- Denied knowingly participating in the fraud
- He was an innocent victim of the dishonesty of others

One ground of appeal:

- The prosecution failed to disclose materials to the defence

Complexity of the investigation

Operation Vitric fraud was a multi-handed MTIC fraud causing a VAT loss of £100 million – it was in 3 stages:

- Stage 1, 30 November 2001 to 19 April 2002
- Stage 2, 22 April to 17 May 2002
- Stage 3, 21 May to 27 June 2002

Operation Vitric fraud was followed by the Operation Devout frauds:

- Operation Devout I was a fraud executed between 12 April and 30 April 2002, causing a VAT loss of £12.5 million
- Operation Devout II related to the fraud charged in the trial of Pomfrett his co-defendants – the fraud ended on 22 July 2002

Failure to disclose materials

The parties agreed, for the purposes of the appeal, a statement of facts arising from the Operation Vitric documents should have been, but were not, disclosed to Pomfrett for the purposes of his trial [see paragraph 39 of the judgment for a summary]

The issue was on the *consequences* of failing to disclose for the safety of Pomfrett's conviction

In essence the defence argument was that the materials would have allowed them to advance Pomfett's defence that he was the innocent victim of the dishonesty of others

Decision of the Court of Appeal

It was accepted that with the additional material the nature of the case would have been significantly different

Pomfrett's defence would have been advanced in a different context

The conspiracy alleged would have to be considered within a much wider context of fraudulent activity than appeared at the trial itself [paragraph 55 of the judgment]

However, the Court formed the view that the additional material provides no reason to doubt the safety of Pomfrett's conviction [paragraph 59 of the judgment]

'In order to test that view, we have gone on to ask ourselves whether the additional material might reasonably have affected the jury's decision to convict.' [paragraph 60 of the judgment]

Example of on-line investigations

Brian Krebs, How a Citadel Trojan Developer Got Busted, July 2017:

https://krebsonsecurity.com/2017/07/how-a-citadel-trojan-developer-got-busted/

Jurisdiction

Where a substantial measure of the activities constituting the crime takes place in a jurisdiction in the United Kingdom, the courts will claim jurisdiction

From a practical perspective, if someone in the UK is victim of an online scam organized by a nearly untraceable person on a different continent, it is likely that a prosecution will take place

Smith, R v [2004] EWCA Crim 631

Wallace Duncan Smith is a Canadian national

He established a merchant bank, Wallace Smith Trust Company

He was the Chairman and Managing Director

On 30 April 1991 the bank ceased trading and a provisional liquidator was appointed on the petition of the Bank of England

It was subsequently wound up owing its unsecured creditors approximately £92,000,000

Smith controlled other companies based in Canada including one known initially as Wallace Smith Holdings

Working from the UK and using a group of companies that he controlled, Smith set up various false deals between the bank and Wallace Smith Holdings which increased the size of the banks profits

The fraud – 1

Counts 3 and 4 related to two similar transactions, regarding a form of secured lending

There were two parts to the transaction

The first part involved a security represented by the stock being sold to Discount Bank of Switzerland, which operated from London, for the agreed duration of the transaction

In other words the lender, as security for the loan, purchases and pays the amount of the loan for the stock on the first part of the transaction

The lender owns the stock but the lender is subject to an obligation to sell it back at an agreed future date - this being the second part

While he owns the stock, the lender can trade the stock

The return for the lender is provided by the agreed increase in price payable by the borrower to the lender on the repurchase part

The fraud – 2

The stock never entered into the possession of the Discount Bank of Switzerland

It was supposedly held in Canada to that bank's order

In fact, no such stock was available to the appellant in Canada or elsewhere

Jurisdiction

The important feature of the transactions for present purposes is that:

- the dishonest arrangements were put into operation by Smith in the jurisdiction of England & Wales
- the obtaining of the money took place outside the jurisdiction when the money was paid into a bank account in New York

One of the issues the Court of Appeal had to deal with was whether the courts of England and Wales had jurisdiction over the offences

For consideration

Smith was charged with offences that might have meant there was no jurisdiction in England & Wales

The court had to decide whether the charges could be withdrawn and substitute charges put in their place

If the substitute charges were put in place, it was then a question of whether it would lead to unfairness

If there was no unfairness, the issue was then whether the correct jurisdiction was England & Wales

The court has a discretion as to whether to substitute a charge

It does not follow that because there can be substitution it will be just to make substitution

Issue

The first requirement for substitution was that Smith at the material times was in London and based there

He was therefore subject to the general criminal jurisdiction of England & Wales

The issue was whether the substituted offence would have been an offence which the courts in England & Wales would have had the jurisdiction to try

Problem

There was a conflict between two previous decisions of the Court of Appeal

The issue was an important one

It involved determining the extent to which it is appropriate for the Court of Appeal to develop the common law about jurisdiction in order to meet the changing requirements of society

The precise issue is of diminishing importance because the legislature has intervened

Harden [1963] 1 QB 8

Harden was the director and majority shareholder of a company in England which sold refrigerators and refrigeration equipment, a high proportion of the sales was on hire-purchase terms

To assist the financing of the hire-purchase business, he made an arrangement with a company registered in Jersey under which he assigned hire-purchase agreements to that company from time to time in return for the payment of a sum equal to that outstanding under the agreements, less an amount equal to the company's charges

When transmitting an agreement, Harden completed an assignment and signed a form of letter of offer of sale, the final sentence of which read 'This offer may be accepted by you at any time within one month of the date hereof by sending your cheque for the net amount'

The documents were sent by post to the company in Jersey, and Harden received in return a cheque posted in Jersey that he paid into a bank account in the name of his company

Harden – the crime

Harden occasionally included fictitious agreements, inducing the company to pay over sums as if it was a genuine agreement

The counts relating to transactions with the company in Jersey were quashed

This is because the offence of ‘obtaining by false pretences’ was the act of obtaining

By completing the ‘offers of sale’ letter, Harden agreed that the sending of the cheque by the Jersey company should complete the transaction

The parties contemplated that the cheque should be sent by post

This meant that when the cheque was posted in Jersey, property in each cheque passed to Harden

This meant that the crime of obtaining was carried out in Jersey

The consequences was that the act was not done within the jurisdiction

Harden – analysis

The offence of obtaining by false pretences lies in the act of obtaining

If this act is done within the jurisdiction, it does not matter that the false pretence was made abroad

On this approach, obtaining offences can be described as ‘result crimes’

That is, crimes that are not complete until the specified result is achieved, and crimes where the location of the result determines the jurisdiction over the crime

This is also called the ‘terminatory theory’

The court came to the conclusion that as the parties to the transaction contemplated that the cheques should be sent by post, the offences were complete at the time of posting the cheques

This meant there was no jurisdiction

From a jurisdictional point of view, it is unsatisfactory for a question of jurisdiction to be determined by an artificial concept designed for resolving contractual disputes

The solution – 1

Crime has ceased to be largely local in origin and effect

Crime is now established on an international scale and the common law must face this new reality

If the issue of jurisdiction is to depend solely upon where the obtaining took place, it is likely that the courts, and especially juries, will be confronted with complex and, at times, obscure factual issues which have no bearing on the merits of the case

The Court of Appeal recognized the need to adapt its approach to the question of jurisdiction in the light of such changes

The English courts have begun to move away from definitional obsessions and technical formulations aimed at finding a single situs of a crime by locating where the substance of the crime occurred or where it was completed

The solution – 2

The courts now:

- examine relevant policies to apply the English criminal law where a substantial measure of the activities constituting a crime take place in England, and
- restrict its application solely in cases where it can seriously be argued that the activities should, on the basis of international comity, be dealt with by another country

The decision in *Harden* was correct, but it no longer should be regarded as setting out an exclusive basis of jurisdiction

For policy reasons, particularly in relation to complex fraud, where there are no reasons of comity which require a different approach, when substantial activities constituting a crime takes place in England, the English court should have jurisdiction

There does not have to be a distinction in relation to the principles of jurisdiction between different crimes

Questions of jurisdiction, although they involve substantive law, have a strong procedural element and are less absolute than issues of pure substantive law

Agreement reached

Rogers, R v [2014] EWCA Crim 1680

Advance fee fraud operated from call centres based in Spain or Turkey

British nationals were employed to deal with calls

Consumers in the UK called the centres in responding to websites or advertisements in the national press

The telephone numbers had the prefixes 0871 or 0845, so the individuals being defrauded did not know that they were speaking to a call centre based in Spain or Turkey

They were persuaded by staff to pay advance fees on false promises

The staff received commission through a cash card provided by a legitimate UK company

The money was paid into the UK accounts of false UK companies and used to pay expenses

The profit (about £5.7m) was transferred to Spain

The new position

The criminal acts plainly took place in and had an effect upon victims in the UK

The laundering of the proceeds in Spain is directly linked to those acts in the UK by virtue of the fact that the property is criminal property

The significant part of the criminality underlying the case took place in England, including the continued deprivation of the victims of their monies

This was not an offence in which the Spanish authorities had an interest

The English courts properly had jurisdiction

This demonstrates the modern approach to jurisdiction, involving an adjustment to the circumstances of international criminality

Presentation of evidence in court

The use of technologies in England

- The police (possibly with substantive evidential consequences)
  - Interviews recorded by video (and increasingly, by digital means)
  - The use of hand-held digital devices to take statements from witnesses (presently used by Hampshire and the Isle of Wight and expanding)
- The prosecution system – mainly in an administrative capacity
  - The police, Crown Prosecution Service and lawyers use an integrated *case management system* and *witness management system* called Compass
  - E-mail is conducted over CJIT (Criminal Justice Information Technology) system providing for security and confidentiality of data
  - CJS exchange includes all systems connected together to gather all the *evidential material* and *case information*

Links with more information

Transforming the criminal justice system: strategy and action plan

https://www.gov.uk/government/publications/transforming-the-criminal-justice-system-strategy-and-action-plan

Crown Court Digital Case System training guides and videos

https://www.gov.uk/guidance/crown-court-digital-case-system-training-guides-and-videos

Crown Court Digital Case System

https://crowncourtdcs.caselines.co.uk

Rules

Streamlined Forensic Reporting has been designed to enable investigators, scientists, prosecutors and the defence to comply with the Criminal Procedure Rules in the interests of justice

There are two publications:

- *National Streamlined Forensic Reporting – Section 1* (Supporting Information)
- *National Streamlined Forensic Reporting – Section 2* (SFR Guidelines for Providers of Forensic Science and a Practical Step Guide)

http://www.cps.gov.uk/legal/s_to_u/scientific_evidence/sfr_guidance_and_toolkit/

Pre-trial management

The primary purpose is to:

- Narrow down the real issues, particularly those of a scientific nature, upon which the jury must decide
- To produce forensic evidence at court
- To reduce unnecessary costs, bureaucracy and delays in the criminal justice system

The aim is to achieve early agreement with the defence on forensic issues

Where this cannot be achieved, it is necessary to identify the contested issues

Preparation

Managing the materials

- identifying the most prominent evidence
- selecting the electronic evidence
- collating it into admissible form

Disclosure protocol

- objective assessment of the integrity of the evidence
- process must be robust and transparent

Trial: presenting the evidence – England & Wales

Educating for presentation at trial

Possible use of visual aids (e.g. powerpoint presentations) for tutorials to cover:

- any computing knowledge that is necessary for the trial
- user etiquette
- video simulations of how a user would use any system used by the court
- use of glossaries and terminology

Alternatively, to have a specific session(s) in person to deal with these issues

Dealing with technical issues

Depending on the complexity of the evidence, it might be useful for the digital evidence specialist to provide his or her evidence in two stages:

1. To explain what the technical terms and processes mean (by providing a glossary of terms in some cases – usually agreed between the parties in advance)

2. Applying the technical knowledge to the particularities of the case

The presentation can include diagrammatic and photographic illustrations

Legal guidance

Legal Guidance on digital working across the Criminal Justice System (October 2012)

Contents:

- Introduction
- Purpose of this document
- Limitations on digital working
- The legal framework
- Authenticating digital documents
- Service
- Stages in proceedings
- Definitions
- Legislation and Rules

http://www.clsa.co.uk/assets/files/general/legal-guidance.pdf

How the Magistrates' Court is beginning to look

Increasing use of digital evidence

In England & Wales, there is increasing use of evidence recorded on body video cameras (BWVs) worn by police officers

At present, over 30 police forces are using BWVs for a wide range of policing activities, including domestic violence incidents and stop and search procedures

Technical guidance for Body Worn Video (BWV) devices: CAST, 2016

https://www.gov.uk/government/publications/technical-guidance-for-body-worn-video-bwv-devices-cast-2016

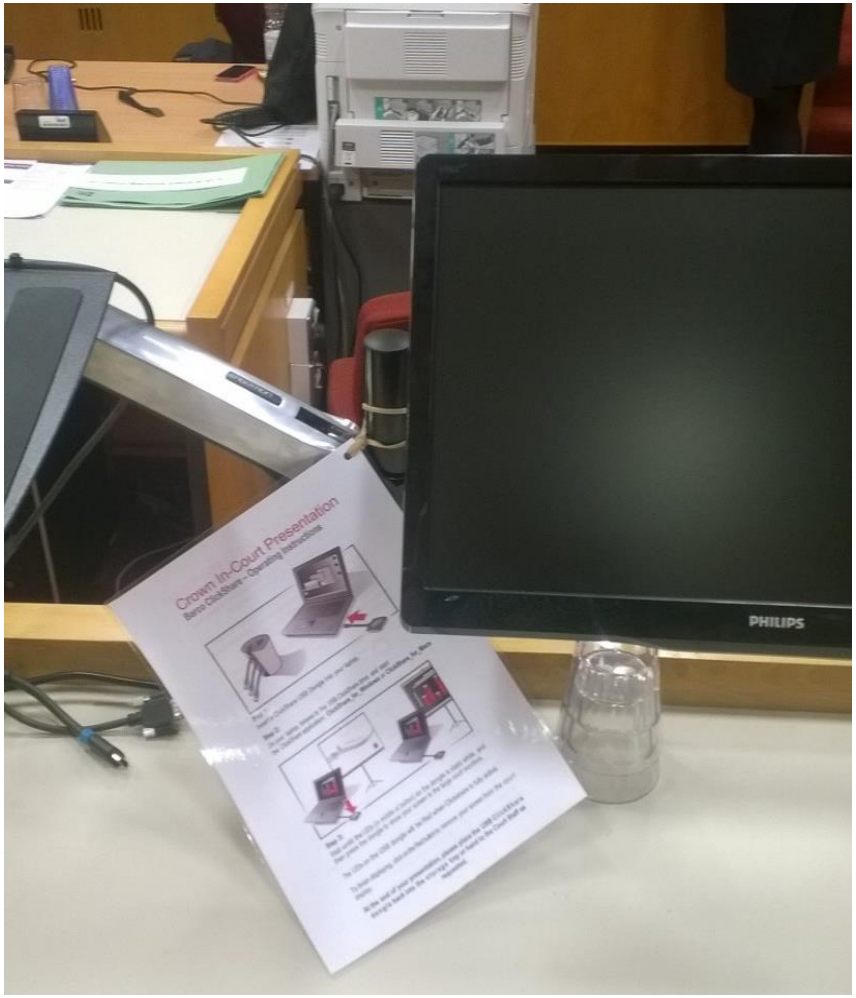
Body-Worn Video (College of Policing, August 2014)

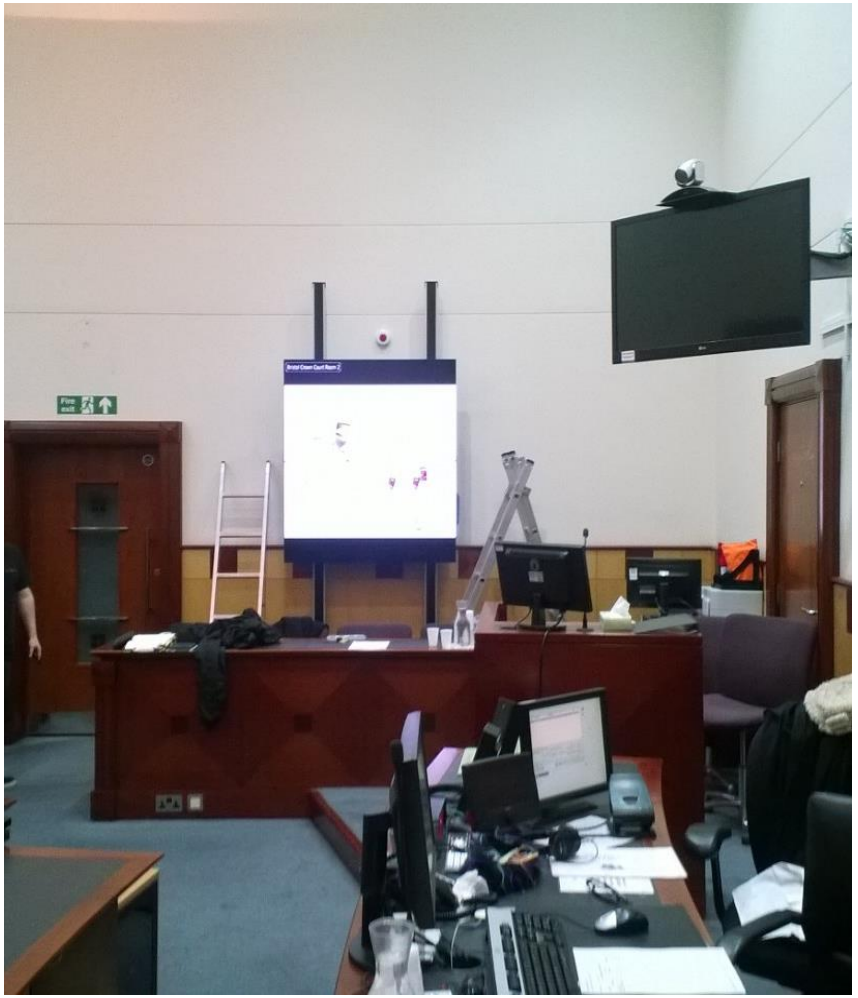
http://library.college.police.uk/docs/college-of-policing/Body-worn-video-guidance-2014.pdf

Guidance for the Police Use of Body-Worn Video Devices (Police and Crime Standards Inspectorate, July 2007)

http://library.college.police.uk/docs/homeoffice/guidance-body-worn-devices.pdf

Developments in the Crown Court





http://stephenmason.co.uk
http://ials.sas.ac.uk/about/about-us/people/stephen-mason

Free journal

Digital Evidence and Electronic Signature Law Review

http://journals.sas.ac.uk/deeslr

Draft Convention on Electronic Evidence

http://journals.sas.ac.uk/deeslr/issue/view/336/showToc

Free books

Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

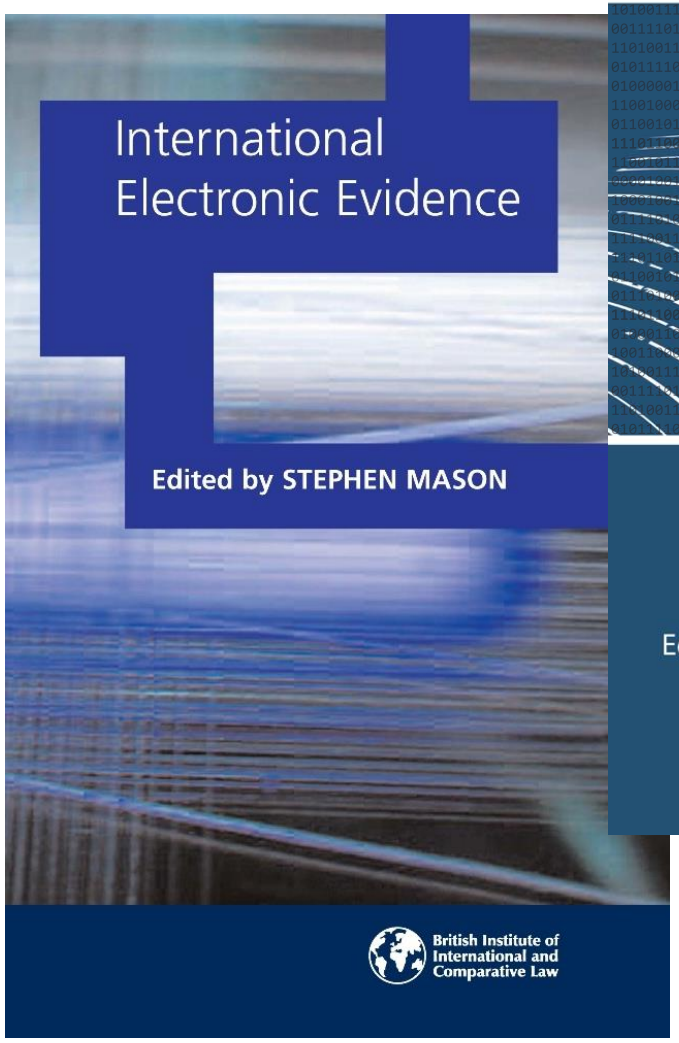
http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence

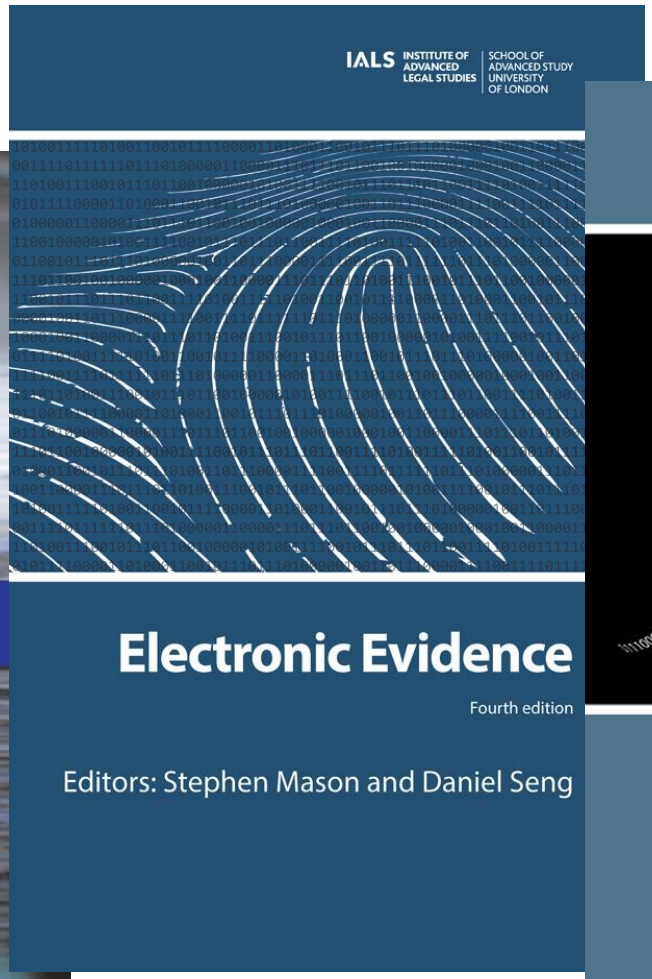
Stephen Mason, *Electronic Signatures in Law* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016)

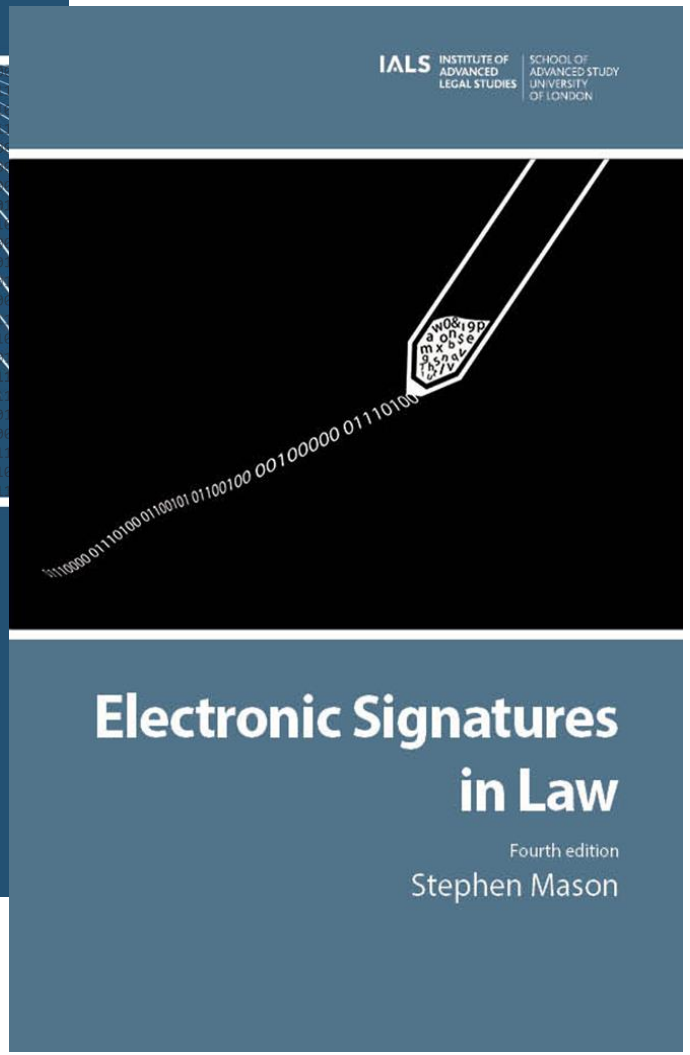
http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures

International Electronic Evidence (British Institute of International and Comparative Law, 2008)

https://www.biicl.org/international-electronic-evidence


International
Electronic Evidence
Edited by STEPHEN MASON
British Institute of
International and
Comparative Law


IALS INSTITUTE OF ADVANCED LEGAL STUDIES
SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON
Electronic Evidence
Fourth edition
Editors: Stephen Mason and Daniel Seng


IALS INSTITUTE OF ADVANCED LEGAL STUDIES
SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON
Electronic Signatures
in Law
Fourth edition
Stephen Mason

ONLINE FINANCIAL CRIMES AND FRAUD COMMITED WITH ELECTRONIC MEANS OF PAYMENT – A GENERAL APPROACH AND CASE STUDIES IN GREECE

Michael Rachavelias, Lawyer (LLM)

Handling e-evidence in online fraud cases

L'Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l'Académie de droit européee

In cooperation with the Athens Bar Association

Athens, 7-8 November 2017

Co-funded by the Justice Programme of the European Union 2014-2020

Outline

e-Evidence in internet-related money laundering

Dissemination of false information and online extortion

Computer-related fraud: a challenge for the application of traditional fraud provisions

Some thoughts about online criminal activity in general:

- Fraud, as a concept of crime, was known from the distant past, the birth of Internet gave it another aspect
- Cybercrime/Internet law is NOT a static law
- Police/Investigation authorities must obtain a high level of conception of e-crime
- The process of obtaining electronic evidence and its integrity is of high importance for its admissibility in legal proceedings
- Plans to monitor internet use – “Cyber police”… Is it something feasible?

Cybercrime faces 2 main challenges → Technical Issues
→ Legal issues (challenges)

Procedural problems: Integrity **a)** *of the evidence* **b)** *of the process of obtaining the evidence*

<u>Legal issues and challenges have to deal with:</u>
- Identifying the user
- Differences in jurisdictions (criminal activities conducted by criminals in countries where no cyber criminal law apply)
- Obtaining digital evidence
- Handling of digital evidence
- Privacy of data

Internet related money laundering

Money laundering is a generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

Money laundering most of the times consists of 3 steps: placement, layering and integration.

The basis of the current legal framework in Greece is **Act 3691/2008** (ΦΕΚ A166/5.8.2008) and all foregoing amendments, which significantly improves the mechanisms for the prevention of money laundering, and implements in the Greek legal system the provisions of Directive 2005/60/EC of the European Parliament and of the Council of 26.10.2005 (OJ L309/15), and Commission Directive 2006/70/EC of 1.8.2006 (OJ L214/29) (before they were amended by posterior directives)

http://www.bankofgreece.gr/Pages/el/Supervision/moneyl/legislation.aspx

(Sentencing Council of Orestiada) ΣυμβΠλημΟρεστ 62/2011, published in legal journal ΠοινΔικ 2012/689 (Criminal Justice)

- Prosecution of the defendant for the offense of money laundering on a continuous basis. Defendant's committal writ by the Sentencing Council.
- Unknown offenders were sending fake e-mails, encouraging users to disclose their personal details (transaction passwords etc), with the intent to intercept them and subsequently use them.
- The criminal organisation had a general methodology and used various persons. The accused was used as a third intermediary who essentially laundered the money generated by the criminal activity of the organization.
- The defendant's claim was that he was also a fraud victim by the criminal organization members, who offered him job through internet.

Case facts in brief

1. In 2007, the complainant Bank pressed charges against any liable person before the Cybercrime Investigation Division of the Financial Crime Subsidiary Division of Attica, after investigations conducted by the above Bank following a complaint by a bank's client that transfers of funds from the client's account had taken place to the accused person's deposit account, without his authorization or knowledge.
2. There were several formal complaints made by several customers, disputing money transactions via Internet, all related to the transfer of funds to other holders' accounts.
3. The bank's information security department conducted an investigation and concluded that on 4.11.2007, 7.11.2007 and 9.11.2007 the amounts of 2.500 €, 2.500 € and 2.484 € respectively were transferred from the client's account to the defendant's account. 2 additional transfers (amounts of 2.500 € and 2.469 € respectively) were also made to an unknown holder's account.

- All transfers of funds took place by the use of the account holder's internet banking passwords, which had been intercepted by unknown offender via internet. The transfers of funds to the accused's account were made via internet from third parties, unidentified during the preliminary proceedings. The role of the accused was to withdraw the money transferred to his account and to farther transfer them abroad via Western Union.
- After the accused's arrest, a lawful home search was conducted in his home and work place, and during search and seizure procedure the following evidence were found and confiscated: computer hard drives, bank account papers, debit cards, Western Union documents for funds transfer to Kyiv, Ukraine, banks' withdrawal documents, 4 photocopies of e-mail messages. In one of the seized hard drives, stored e-mail messages were found to contain all communication for the money transfers.
- Evidence (emails, employment contract, bank transactions, transfer of funds, ATM withdrawals, phone communications) were recovered from the seized hard drives by the competent Criminal Investigation

Unit, after the issuance of the deliberation of Sentencing Council for the lifting of secrecy.

- From the evidence during pre-trial stage, the conducted inquiries and the investigation documents, it has emerged that unknown offenders, were sending fake e-mails (supposedly sent by the bank) and urging the recipients to disclose their personal details and passwords, with the intent to intercept them and subsequently use them.
- From the investigation, many IP addresses that correspond to foreign service providers were found. The Prosecutor has properly submitted requests for legal assistance to the relevant foreign countries regarding the investigation of the case and the discovery of unknown perpetrators, but the competent French and Spanish judicial authorities have replied that for technical reasons it was not possible to use the IP address found to discover the real identity of the internet operator.
- The accused was found liable for the offense of money laundering, using his own bank account and acting as an intermediary and was indicted by committal writ to the competent court.

Dissemination of false information and online extortion

- To tackle the spread of misinformation online we must first understand it
- False information spreads just like accurate information
- Internet users nowadays are in danger of being defamed and insulted in cyberspace. False information (personal or corporate) disseminated on the web via websites or social media can easily destroy a reputation.
- **The problem**: “Misinformation can be very difficult to correct and may have lasting effects even after it is discredited … false information may continue to influence beliefs and attitudes even after being debunked if it is not replaced by an alternate causal explanation” (Source: *Nyhan, B., & Reifler, J. (2015). Displacing Misinformation about Events: An Experimental Test of Causal Corrections. Journal of Experimental Political Science, 2(1), 81-93. doi:10.1017/XPS.2014.22*)
- The phenomenon of public misinformation (also known as ‘hoax’) has taken new dimensions and has rapidly increased in the digital age.
- Fake news or other misinformation can be described as stories that

are presented to public as being the result of a journalistic research, but in truth they are fabricated to serve a purpose, which can be commercial (product promotion), clickbait trap or political (public opinion manipulation).

• A recent study by Oxford Internet Institute of the University of Oxford on the use of social media as manipulation tools (https://www.oii.ox.ac.uk/) has shown that "*lies, trash, misinformation of traditional propaganda have spread widely online, and in fact they are supported by the algorithms of social media like Facebook or Twitter*" and concluded that computational propaganda is now one of the most powerful tools against democracy. Social media firms may not be creating this nasty content, but they are the platform for it. They need to significantly redesign themselves if democracy is going to survive social media" (Source: http://comprop.oii.ox.ac.uk/publishing/working-papers/computational-propaganda-worldwide-executive-summary/, the whole project can be found here http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf)

• As far as criminal law is concerned, the dissemination of false information/news has not been harmonized at European Level.

• In Greece, a relevant provision is article 191 Penal Code that covers the dissemination of false news, which concerns any individual who, acting intentionally disseminates in any way false news that could concern to citizens.

• The most recent **case in Greece**, related to social media, is the Court of Misdemeanors of Veroia **582/2016** (ΜονΠλημ Βέρ 582/2016, ΠοινΔνη 216/493), related to the publication in a social network of an article about a vaccine that causes cancer, according to the writer of the article.

• The court held that the accused (a columnist on the internet), acting intentionally, has spread fake news that are capable of causing concern to citizens, because of his article (that he published on the internet in 2014) about the story of a young girl who died of cancer a few months after her parents vaccinated her, without citing any details of the child's identity or the doctors' identity. According to the court, the accused did not cite or prove any evidence that proves the truth of his writings.

Computer-related fraud: a challenge for the application of traditional fraud provisions

There are three types of evidence that might need to be obtained in legal proceedings:

-Evidence from publicly available websites, such as (this list is only indicative) blog postings and images uploaded to social networking websites,

- The substantive evidence (or evidence of content), that is the e-mail or documents in digital format that are not made publicly available and which are held on a server,

- Purported user identity and traffic data (‘meta data’) that is used to help identify a person by finding out the source of the communication, but not the content.

In criminal proceedings in Greek courts, the evidence that can by submitted in courts are predicted in art. 178 Code of Criminal Procedure (CCP). Documents are among these evidence and their broad definition is described in Article 13 s. C of the Greek Penal Code, which among other provides a satisfactory definition for the document as any medium used by a computer or the peripheral memory of a computer, by electronic, magnetic or [an]other way, for the purpose of writing, storing, production or reproduction of

evidence, that cannot be read directly, as well as any magnetic, electronic or other type of material used to store any information, image, symbol or sound in sole [*sic*] or in combination, provided that these media and material are destined to prove facts of lawful meaning.

- Under this definition, digital evidence is accepted in Greek courts as any other form of document
- Recent amendments in 2016 (Act 4411/2016) introduce 2 additional definitions in the Greek legal system, the “information system” and the “digital data”, both necessary for the interpretation of such provisions today.

Computer Fraud – Legislation

EU

Convention on Cybercrime (Ref: ETS 185)

Budapest, 23 Nov. 2001

- The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.
- Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (OJ L218/8/14.8.2013)

This directive establishes minimum rules concerning the definition of criminal offences and sanctions in area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities (article 1).

The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity, as companies and citizens are more interconnected and interdependent across sectors and borders than ever before. European citizens' and businesses' trust in digital services is essential for a flourishing digital single market

- Last initiative: Commission Recommendation (EU) 2017/1584 of 13.9.2017 on coordinated response to large-scale cybersecurity incidents and crises (L 239/36, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.ENG&toc=OJ:L:2017:239:TOC)

GREECE

The above acts (convention and directive) were recently implemented in the Greek legislation, after many years of delay.

Law 4411/2016 (FEK A’ 142/2016), published in 3 August 2016 amends a lot of the existing general provisions of Greek Penal Code, introduces some new terms and definitions and supplies the necessary tools to combat computer-related crime in Greece.

Article 386A Penal Code
Fraud by means of a personal computer

Whoever, with the intent of procuring for oneself or another person illegal economic benefit causes damages to foreign property by affecting the result of a digital data processing operation either through incorrect software configuration or by use of incorrect or deficient data or by unauthorised data use or by unauthorised interference against information systems, he/she shall be punished with the sanctions that the previous article imposes. (PS: those sanctions are: imprisonment of at least 3 months; and if the damage is of quite a significant value, imprisonment of at least 2 years. The sanctions imposed can be incarceration of up to 10 years if: i) the person that commits these offenses has this fraudulent conduct by habitual criminal and additionally, the damage caused is more than 15.000 Euros, or ii) the profit of the criminal or the damage caused is more than 120.000 Euros).

Property damaged is suffered even if the persons who have suffered are unfounded. To estimate the damage is indifferent if the suffering party are one or more persons.

(Original text in greek)

«Άρθρο 386Α Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα».

**** Το άρθρο 386Α,το οποίο είχε προστεθεί με το άρθρο 5 Ν.1805/1988 (ΦΕΚ Α 199) αντικαταστάθηκε ως άνω με το άρθρο δεύτερο παρ.11 Ν.4411/2016, ΦΕΚ Α 142/3.8.2016.*

(Supreme Court – Areios Pagos)
ΑΠ 813/2015, published in legal database ΝΟΜΟΣ, ΠοινΧρ 2017/179

- Condemnation for theft and computer fraud on a continuous basis.
- Distinction of fraud crime to computer-related fraud.
- Computer-related fraud occurs when the offender intervenes directly in the program's development or in computer components and, by use of incorrect or deficient data when programming the system, causes a different result to that resulting from the processing of the correct data.

Case facts in brief

1. The accused stole an envelope containing a credit card and the notice in writing to receive the card's Personal Identification Number (PIN) from the local post office.
2. The accused forged an authorization, fake in its context, and received the PIN from the post office using this false authorization. Then, in the period between 12 June and 18 June the accused made continuous cash withdrawals from the bank's ATM.
3. The accused entered the credit card in the bank's ATM, typed the (correct) PIN and withdrew a total amount of 7.900 Euros, providing the computer with the conclusion that every time the withdrawal was made by the legitimate holder of the credit card. This way, the accused affected the results of the computer's digital data processing operation.

The court held in the above case that, according to article 386A Penal Code, computer-related fraud occurs when the damage occurs, not by misleading a natural person who is capable of making decisions or conducting control or approving or granting, but only by influencing computer components, that is, by the offender's intervention in system programming and data processing, at any stage of a computer’s operation. Thus, in the event that the offender directly intervenes in the program’s development or in computer components and by incorrect software configuration or by use of incorrect or deficient data causes a different result to that resulting from the processing of the correct data, then there is no common fraud, but computer-related fraud.

(Supreme Court – Areios Pagos) ΑΠ 131/2013, published in legal database ΝΟΜΟΣ

- Condemnation for computer fraud on a continuous basis, repeatedly and by habit. Prosecution for felonious forgery.
- The fraudsters trapped ATMs of various bank branches, using self-made devices in order to trap clients' debit and credit cards by the use of skimming.
- Skimming is the technique used to copy the data stored on the magnetic stripe of a bank card when one puts the card in a cash dispenser. An almost invisible device is installed right in front of the card slot on the card dispenser in order to copy the data without the customer being aware of this. At the same time, fraudsters try to see the PIN number by making use of a nano-camera or (sometimes) via shoulder surfing. The data that have been stolen will then be used for making a false card (a "clone" card).

Case facts in brief

1. In May 2006, the complainant Bank realized that unknown offenders had trapped ATMs of various branches, using self-made devices in order to trap clients' debit and credit cards by the use of skimming. That kind of trapping is only used in close dates and for few dates a month. These devices contained: i) a, difficult to spot, electronic mechanism that was capable of copying the data of each card's magnetic card, which was placed under the card reader, ii) a metal bar, in which they had carefully installed a mobile phone with a digital camera, which detected the card number and the PIN(s).
2. After collecting all necessary data, the offenders created false cards, used special computer software to activate them with the relevant PIN numbers, and then used them in various ATMs to withdraw money and charge the bank accounts of the legitimate card holders, as they provided the computer with the conclusion that every time the withdrawal was made by the legitimate holder of the credit card. Using this technique, they withdrew a total amount of 72.160 Euros from various bank account's holders.

The court held in the above case that:

- the created false cards are “documents’, by the meaning of art. 13 s. c Penal Code,
- the offenders, with the intent of procuring for themselves illegal economic benefit caused damages to foreign property by affecting the computers’ data through unauthorised interference against the computer’s information system,
- the offenders committed the felony of computer-related fraud under article 386A Penal Code.

(Felonies Appellate Court of Athens) ΠεντΕφΑθ 96/2016, published in legal journal Ποινική Δικαιοσύνη (Criminal Justice) 10/2016, p. 903

- Condemnation for forgery on continuous basis. Prosecution for forgery on continuous basis and unauthorized interference in personal data archive.
- The case facts are the same as the previous case: fraudsters trapped ATMs of various bank branches, using self-made devices in order to trap clients' debit and credit cards and steal their PIN numbers by the use of skimming and the creation of false credit/debit cards, which they then used in order to withdraw money from ATMs.
- **Evidence used in court** for the condemnation of the defendants:

  -Testimonies of the police officers

  - Investigation of the CCTV recording circuit of videotapes

  - Relevant photographs submitted before the court

The court held in this case that:

- the created false cards are “documents’, by the meaning of art. 13 s. c Penal Code, which are forged, by the meaning of art. 216 para. 1 Penal Code.
- the offenders have intentionally drawn up forged document in order to mislead others, and subsequently they have used these forged documents
- the defendants were found guilty of the offense of forgery after use on continuous basis, and not guilty for the unauthorized interference in personal data archive.
- No legal connection to the offense of computer-related fraud (art. 386A Penal Code) was made.

(Sentencing Council of Kilkis) ΣυμβΠλημΚιλκίς 54/2012, published in legal journal ΠοινΔικ 2014/238

- Prosecution of the accused for the breach of IP law and the offense of computer fraud on a continuous basis. Defendant's committal writ by the Sentencing Council.
- The offender intervened and affected the computer's digital digital data by use of incorrect and deficient data, thus resulting to the manipulation of the input of the data. The accused, by using special network devices illegally intercepted, decrypted and unlawfully distributed to other internet users pay-TV signal, for a sum of money.
- The place where the offense of "internet fraud" is committed is not just the place where the offense took place (that is, the place where the false facts were presented as true or the unlawful concealment or defamation of the true facts), but also the place where the afflicted party suffers the damages.

- After the issuance of the deliberation of Sentencing Council of Athens for the lifting of secrecy of communication, the ID's of the user that had the above-described illegal activity was revealed.
- A lawful home search was conducted in the accused party's home, and he plead guilty and disclosed to the police enforcement officers the technological equipment he used. Besides the equipment, the following evidence were found and confiscated: 2 internet digital satellite receivers, a modem router with its power supply, 3 internal hard drives, 3 card readers, 2 external usb-sticks storage units.
- The accused admitted the existence of the decoder, but has refused the accusation of commercial exploitation of the equipment.
- The accused was found liable for the offense of computer fraud and was indicted by committal writ to the competent court.

Investigation in case of data cloud storage (Sentencing Council of Athens) ΣυμβΠλημΑθ 613/2016, published in legal journal ΠοινΔικ (Criminal Justice) 2016/424

- Legal issue: Whether the procedure for the lifting of secrecy of communication should be followed, in order to search and use in trial digital data/files which are illegal to maintain and distribute (ie child pornography files) and are stored in a cloud storage, to which computers and smart phones are connected.
- According to Greek law, types and forms of communication which are subject to lifting of secrecy include teletype, telephone communication (SMS included), data communication via networks, internet communications etc (art. 3 pd 47/2005). Thus, computer's hard drive, its accessories and components are not a form of communication and accordingly, the data stored on a computer's hard disk or in a digital camera or other carrier material (and which do not refer to any form of response or communication) do not fall within the protection of

confidentiality of communication.

- The majority had the opinion that the procedure of lifting of the secrecy of communication should be followed. So, when a person creates an account and uses a password to use the storage service on a provider's service, it is doubtful whether this cloud storage (which may as well be located on another country or even continent) may be considered a computer component and there is a danger that evidence might be inadmissible in a trial.

- One member of the Sentencing Council had the opposite opinion, that these kind of data do not fall within the protective frame of the secrecy of communication, because a user who keeps illegal data stored in cloud computing has the same power over them as he would if he stored it in a local storage medium, since he can manage the data as he wishes (i.e the user can reproduce, modify, delete or send them to third parties) (provided that he has full access rights to that "cloud" site). It is, in fact, a virtual, remote external disk or other storage medium (cd, usb flash drive etc) and as such should be dealt in regards to the lifting of the secrecy of communications.

Relevant to the previous case is the most recent decision of the Plenary of the Supreme Court Areios Pagos (ΟλΑΠ 1/2017, published in legal database NOMOS), relating to the search and recovery of e-mails from corporate computer's hard drive, which were used by former employees who refused to submit the relevant documents to the firm.

- The Court held in this case that these recovered data (emails) do not fall within the protective frame of the secrecy of communication, because they were not intercepted during communication and were not removed from a personal computer file of the employees using a password hack, but from the corporate computer's hard disk (which was used by the former employees when they worked for the firm), and as such no procedure relevant to the lifting of the secrecy of communications should be followed for them to be admissible in Court.

Fraud across Virtual Borders IRL (in real life)

Cormac Callanan
Aconite Internet Solutions
Dublin, Ireland
cc@aconite.com
m: +353 87 257 7791

Co-funded by the Justice Programme of the European Union 2014-2020

Who am I?

- IANAL
- IANAP

- Cybercrime Expert for
  - Council of Europe
  - OSCE
  - EC
- Industry background
- First ISP in Ireland
- Past-President of EuroISPA
- Past-CEO INHOPE International Network of Internet Hotlines
- MSc
  - Computer Systems Design 1991
  - Advanced Security and Digital Forensics 2017

Agenda

- Profiling the good, the bad and the ugly
- Filtering and blocking
- Circumvention, encryption and hiding online
- Virtual evidence – an oxymoron?
- MLATs, EIO's, collaboration – volunteers required!
- Virtual courts, virtual judges, virtual prisons

TRENDS

Attack Vectors

Big Data

ACONITE
INTERNET SOLUTIONS

Virtualization - Cloud

ACONITE
INTERNET SOLUTIONS

Mobile

ACONITE
INTERNET SOLUTIONS

IOT

ACONITE
INTERNET SOLUTIONS

Complex Security Challenges

ACONITE
INTERNET SOLUTIONS

Joint Investigation Teams

ACONITE
INTERNET SOLUTIONS

Log Files

ACONITE
INTERNET SOLUTIONS

e-evidence

ACONITE
INTERNET SOLUTIONS

Empowering Targets

Questions?

Cormac Callanan
CEO, Aconite Internet Solutions

email: cc@aconite.com gsm: +353-87-257 7791

UNODC
United Nations Office on Drugs and Crime

CYBERCRIME

Neil J. Walsh

Chief – Global Programme on Cybercrime

Blockchain *investigations*

ERA Conference: the lifecycle of E-Evidence

Co-funded by the Justice Programme of the European Union 2014-2020

UNODC
United Nations Office on Drugs and Crime

UNITED NATIONS OFFICE ON DRUGS AND CRIME

CYBERCRIME

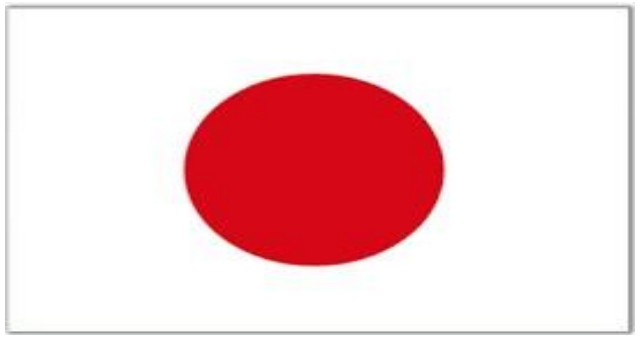
UNODC
United Nations Office on Drugs and Crime

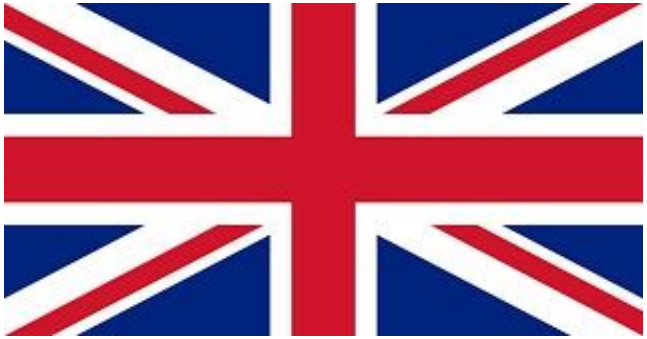
- UNODC tasked by UN Member States via the Commission on Crime Prevention and Criminal Justice in 2010.
- Established an Open-Ended Intergovernmental Expert Group on Cybercrime in 2011.
- Published, in draft, a Comprehensive Study on Cybercrime in 2013.
- Established a Global Programme also in 2013.

Global reach, *local delivery*

UNODC
United Nations Office on Drugs and Crime

Funded entirely *by donors*





UNODC
United Nations Office on Drugs and Crime

Building a *cross-government response*

Diplomacy: working with Permanent Missions to the UN and Ministries.

Policy: Ministries of Justice, Communication, Foreign Affairs, Home Affairs, National Security, Education…

Law Enforcement: National Police, National Security, Local Police, International Law Enforcement and Intelligence.

Prosecution / Judiciary: State & National Prosecutors and Judges.

Prevention: Ministry of Education, NGOs, Faith Groups, Private Sector and more.

What are *cryptocurrencies*?

Digital assets designed to work as a medium of exchange using cryptography:

- to secure the transactions and
- to control the creation of additional units of the currency.

UNODC
United Nations Office on Drugs and Crime

UNODC
United Nations Office on Drugs and Crime

All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$64,707,533,879	$3903.07	16,578,625 BTC	$1,191,100,000	-0.63%	
2	Ethereum	$26,910,869,449	$284.03	94,747,575 ETH	$418,687,000	0.29%	
3	Bitcoin Cash	$7,835,551,274	$472.04	16,599,338 BCH	$346,309,000	-2.39%	
4	Ripple	$6,968,571,480	$0.181739	38,343,841,883 XRP *	$30,215,400	-1.10%	
5	Litecoin	$2,744,312,463	$51.75	53,030,807 LTC	$140,941,000	-1.14%	
6	Dash	$2,711,795,477	$358.20	7,570,534 DASH	$138,650,000	9.06%	
7	NEM	$2,041,002,000	$0.226778	8,999,999,999 XEM *	$3,246,180	-3.13%	
8	IOTA	$1,511,447,418	$0.543778	2,779,530,283 MIOTA *	$10,161,200	-2.78%	
9	Monero	$1,426,525,408	$94.44	15,104,906 XMR	$26,420,800	-0.64%	
10	Ethereum Classic	$1,063,431,154	$11.11	95,721,822 ETC	$31,058,500	-1.86%	

UNODC
United Nations Office on Drugs and Crime

Origins of *Bitcoin?*

White paper on published in 2008 by Satoshi Nakamoto

SAmsung TOSHIba
NAKAmichi MOTOrola

Bitcoin was developed open source from 2009

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

UNODC
United Nations Office on Drugs and Crime

About *bitcoin*?

- Bitcoin is open source software
- It uses peer-to-peer networking
- Decentralized digital currency
- It has similar characteristics to gold

UNODC
United Nations Office on Drugs and Crime

What do bitcoins look like?

UNODC
United Nations Office on Drugs and Crime

16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

Public key: 32 characters starting with 1 or 3

Private key: 51 characters starting with 5

UNODC
United Nations Office on Drugs and Crime

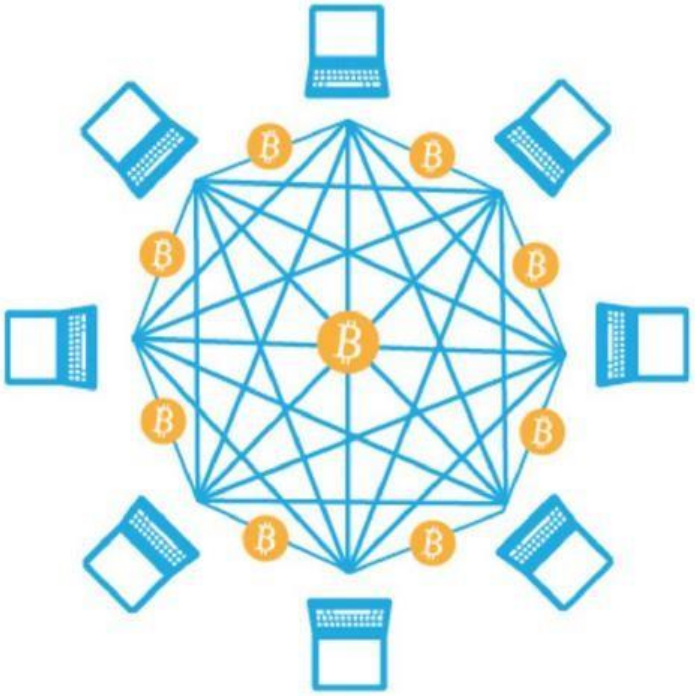
The Bitcoin *network?*

The bitcoin network, consists of +10m users & evolved over 8 years. Transactions are between $1bn-$9bn a day in an open ledger system

UNODC
United Nations Office on Drugs and Crime

Bitcoin is **Transparent**

About *blockchain*?



The Blockchain

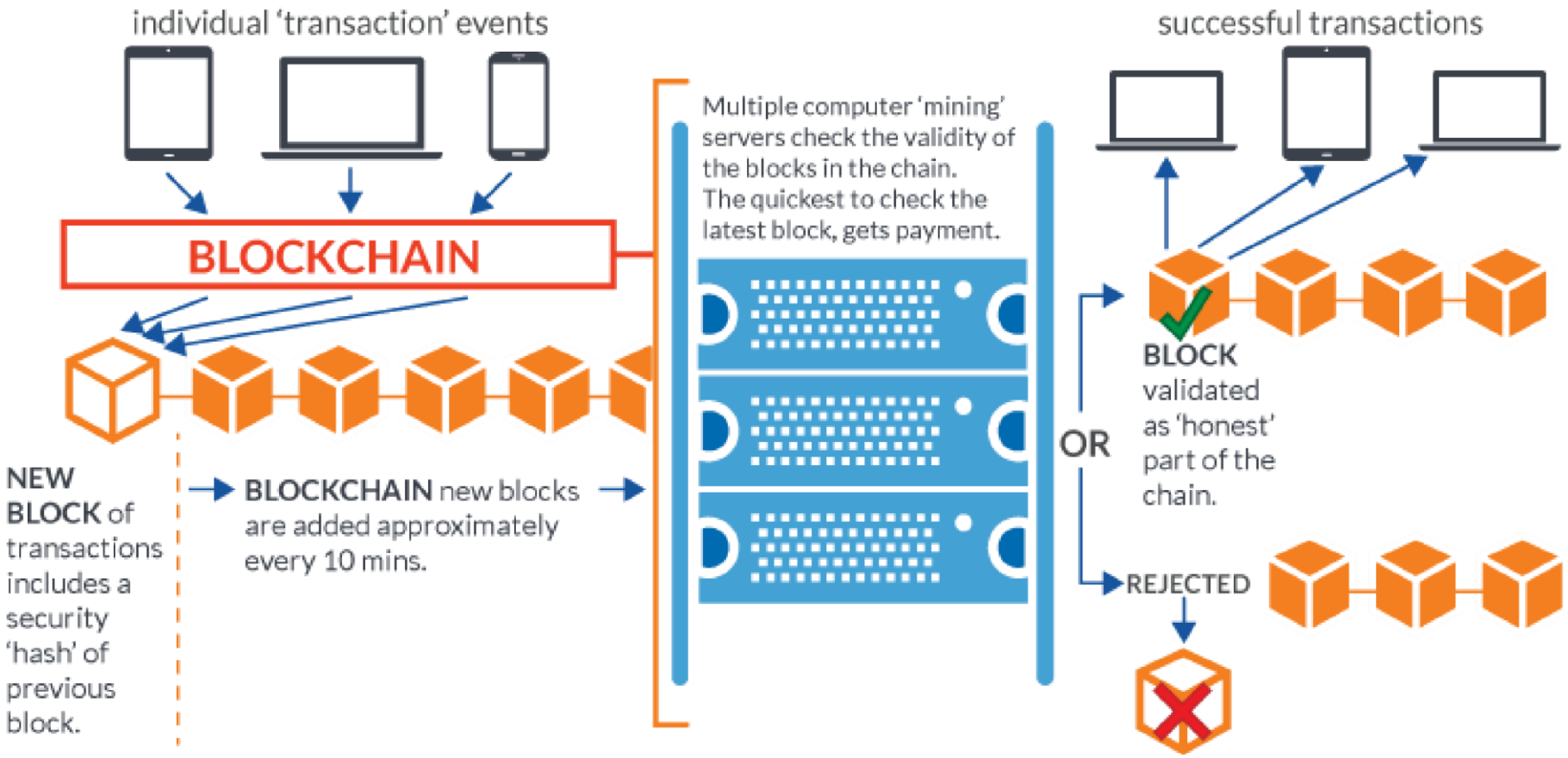
- Public, distributed ledger that contains the history of *every* bitcoin transaction.
- Shared between users and *anyone* can access.
- *Pseudonymous:* contains a record of every transaction, but is not inherently linked to real life identities.

A permissionless distributed database that maintains a continuously growing list of data records hardened against tampering and revision, even by operators of the data store's nodes.

UNODC
United Nations Office on Drugs and Crime

Transactions

UNODC
United Nations Office on Drugs and Crime



UNODC
United Nations Office on Drugs and Crime

Blockchain

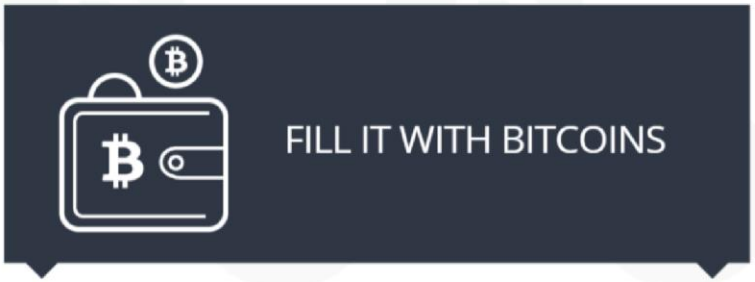
Last documents registered:

Document Digest	Timestamp
1b6621689cf6f02631f7ff79bdb51ee27eb694e353b94791183645a57e16acf0	2017-08-31 10:00:34
b9bb01ea27a2cf9c225e1c6e083e62b6cf354435336aa94647ddc6838a63e799	2017-08-31 09:46:07
a66bdbd03881173747281e4f751c6ee34bc66baa2dfc2ee8a5aaf15e28def5f2	2017-08-31 09:26:25
d5c1d770fb2774da97f38e0e93bf61397e1fa7755a90b5f9ae5f928c528479f9	2017-08-31 08:26:34
693081b55997fde5ccf72d80725f449891a3a1f9ec6a892c1949a40a5dca5bc6	2017-08-31 07:10:54

Last documents confirmed in the blockchain:

	Document Digest	Timestamp
✓	b9bb01ea27a2cf9c225e1c6e083e62b6cf354435336aa94647ddc6838a63e799	2017-08-31 09:46:07
✓	f876b39413eb7c2d5f3fbf13c067f06f3b35d83c5307851d8fb8a5307a38356a	2017-08-27 14:41:23
✓	c537f1958d002da831edca9aa7692c581983f1c32fdba8b276112ccb351d3dab	2017-08-26 18:56:07
✓	6963f46fdd449d1cd79cebdf0e42894c9ec53b8b24dbceb698fd67dcdcd936f2	2017-08-26 11:43:39
✓	d0d12f128b6ae6d438863488e46bd7a7cf8f661ce75bb1842bd2c002ca86d96c	2017-08-26 11:17:33

UNODC
United Nations Office on Drugs and Crime



BUY BTC

With wire transfer or cash $,£,€, etc...

at online BTC exchanges

at online deposit platforms

from other people in person

At current exchange rates

Negotiate price

or

MINE BTC

You can do this by...

Buy a mining rig

Join mining pool(s)

Collect block reward

UNODC
United Nations Office on Drugs and Crime

Your Bitcoins are stored in

ANONYMOUS ONLINE ADDRESSES.

Each address is like a glass safe:
everybody sees what's inside but only you hold a private key to open it and spend. Addresses and private keys are long sequences of letters and numbers.

NETWORK		YOUR WALLET
Your BTC address #1	Balance BTC 0.01	Private key #1
Your BTC address #2	Balance BTC 0.02	Private key #2
Your BTC address #3	Balance BTC 3.00	Private key #3
Your BTC address #n	Balance BTC 2.00	Private key #n

*People can see the address but not who owns it. So your identity can remain anonymous, if you choose.

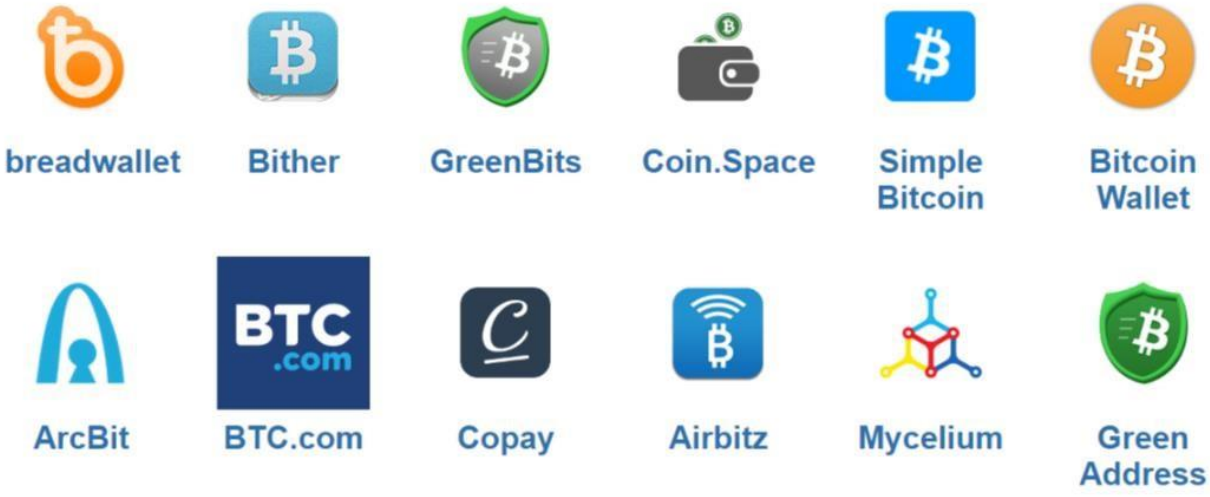
Everybody can see

Only you can see

UNODC
United Nations Office on Drugs and Crime

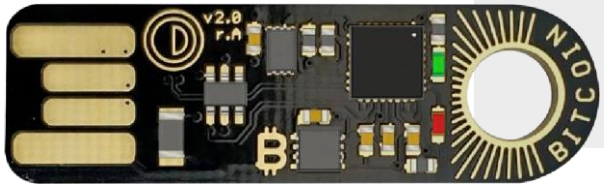
bitcoin wallet

Mobile | Desktop | Hardware | Web



UNODC
United Nations Office on Drugs and Crime

hardware wallet



UNODC
United Nations Office on Drugs and Crime

How to make *transactions*

UNODC
United Nations Office on Drugs and Crime

at

ONLINE SHOPS

for goods and services

at

POINTS OF SALE

in BTC-friendly cafés and shops

at

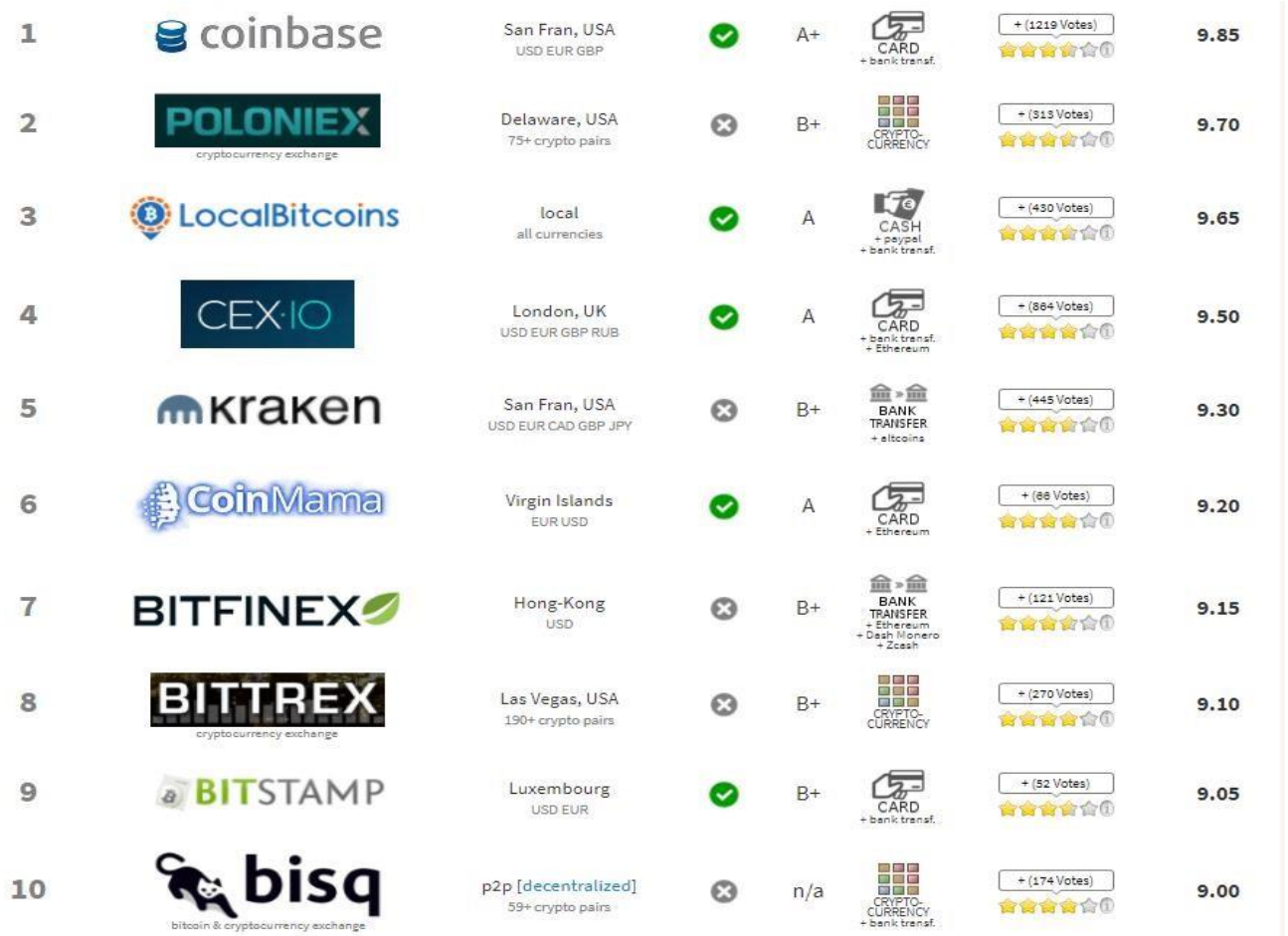
BITCOIN EXCHANGES

for other digital currencies

UNODC
United Nations Office on Drugs and Crime

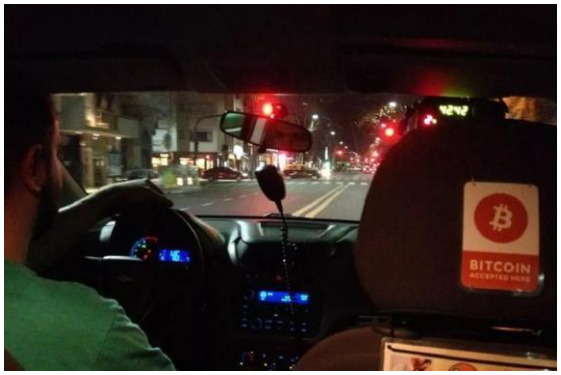
Where to buy *bitcoins*?

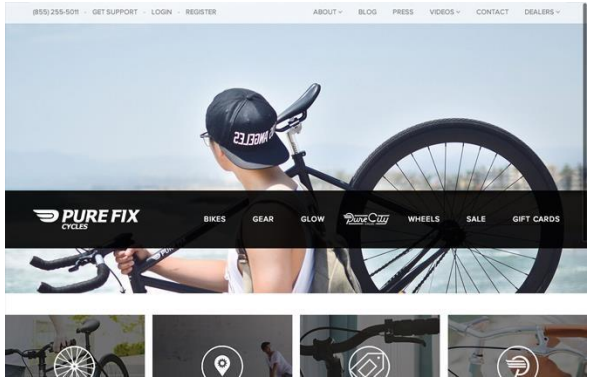
- Exchange



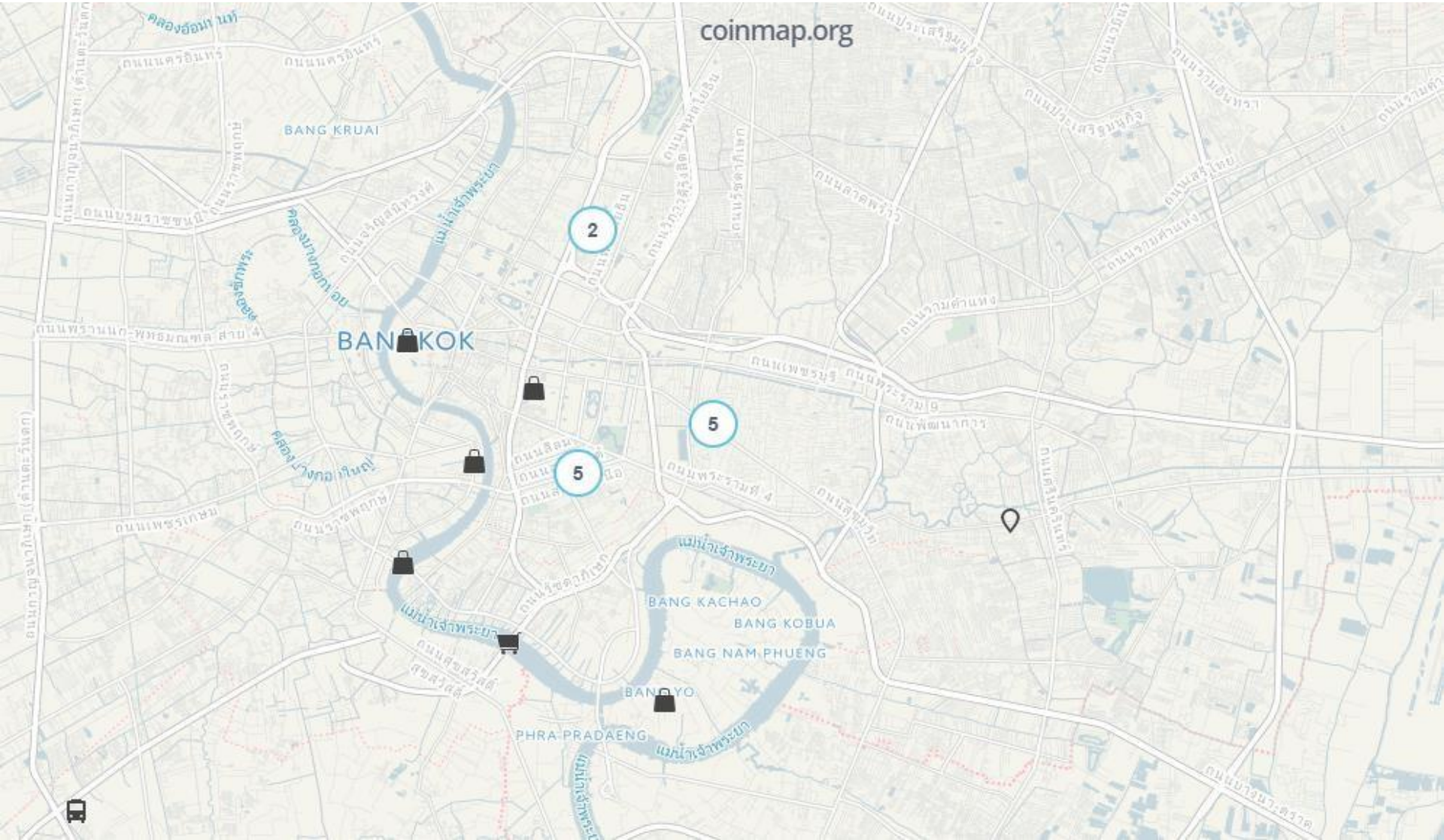
UNODC
United Nations Office on Drugs and Crime

What can you buy with *bitcoins*?





UNODC
United Nations Office on Drugs and Crime



UNODC
United Nations Office on Drugs and Crime

Cryptocurrency can be used *for terrorism and crime*

UNODC
United Nations Office on Drugs and Crime

Kidnappers Around the World Want Their Ransoms Paid in Bitcoin

JOSEPH COX
Jul 4 2017, 10:17pm

Liudmyla Matviiets, 271 EAK MOTO/Shutterstock

Another episode of crime trying to take what it can from tech.

AlphaBay Market

Alternate Onion Links

alphabaywyjrktqn.onion

pwoah7foa6au2pul.onion

stbux7lrtpegcra2.onion

jsbpbdf6mpw6s2oz.onion

zdfvqospmrbvzdn3.onion

CC / Account Autoshop

Access the CC autoshop

Access the account autoshop

Browse Categories

Fraud	7158
Drugs & Chemicals	17457
Guides & Tutorials	3231
Counterfeit Items	1322
Digital Products	2682
Jewels & Gold	428
Weapons	402
Carded Items	660
Services	1612
Other Listings	550
Software & Malware	354
Security & Hosting	129

Search Options

Search terms:

Listing type:

All Fixed Price Auction

Search: Search

Featured Listings

1 GRAM of high quality MDMA (80%+-) # 14093 - Ecstasy - Qualitywhite
Buy: USD 17.00

[MS] ▪▪▪8 Powerful Methods to cashout CC and Paypal™▪▪▪ # 9746 - Fraud - 19 hours left - Police™
Buy: USD 9.99

[FE 100%] [RedSon] CC/CVV USA OLD MAGIC QUALITY # 1103 - CVV & Cards - RedSon
Buy: USD 9.20

5 GRAM AMNESIA REST WEED # 9329 - Cannabis & Hashish - wakikiweedshop
Buy: USD 22.35

[MS] ★NOMETHAZINE MEDICATED SYRUP★ 2oz Bottle 420 Purple SYRUP # 31566 - Cannabis & Hashish - DabKing
Buy: USD 80.00

[MS] ★Kurupt's MOONROCKS★ ™DNM EXCLUSIVE™ 51% THC Weed/Wax/Keif + FREE DVD # 31741 - Cannabis & Hashish - DabKing
Buy: USD 60.00

Welcome, [redacted]

Personal phrase: [redacted]
The sentence above is here to ensure that you are on the real Alphabay Market site and not on a phishing site.

We wish you welcome to AlphaBay market, an auction-style marketplace for all black market items. Any question, feedback or suggestion can be directed to the forum and our staff members will look into it. We appreciate any feedback you can provide to make AlphaBay a better place!

News

August 13th, 2015
Products in the account autoshop tab can now be disputed for up to 1 hour after purchase. In addition to the anti-scam team, this should deter scammers. We also cleaned the autoshop and banned several vendors.

June 30th 2015
In addition to sticky listings, we have now added front page bidding. You can use the links above to place a bid on your listing to make it appear on the front page. The full terms are explained on the link in the box just above.

June 8th 2015
We are now introducing the Order Queuing feature, where you can place orders in a queue to be automatically done when your balance tops up. No need to wait for confirmations anymore!

June 2nd 2015
The autoshop now has a checker! All card checks cost $0.60 regardless of the check result, and dead or invalid cards will be refunded, minus the usual comission fees.

May 17th, 2015
We now have a fully-functional autoshop for all members looking to buy fulls or credit cards! The link is on the top-left of the page. You can search by DOB, BIN, city, state, and much more. The process is completely automated and all cards are dispatched immediately. We also added support for Jabber notifications when an order is placed so you stay alerted at all times.

May 12th, 2015
We now have an affiliate program! Go in your Affiliate Stats table and give your referal link to any new buyer / seller and get 20% of

(more photo)

PTR GREEN GI SPECIAL EDITION .308 G3

Caliber: .308 Winchester / 7.62x51mm NATO
Capacity: One 20 round magazine included
Barrel: 18" Match Grade Barrel, 1:10 twist rate
Length: 40.5"
Weight: 9.5 pounds

$890 (0.7532 BTC)
amount 0

(more photo)

CENTURY ZASTAVA N-PAP M70 AK-47

Caliber: 7.62x39mm
Capacity: Two 30 round magazines included
Barrel: 16.25" Hammer Forged Barrel, 1:10" twist
Dimensions: 36" long
Weight: 7.9 pounds

$590 (0.4993 BTC)
amount 0

(more photo)

KRISS VECTOR SDP .45 ACP SPECIAL DUTY PISTOL

Caliber: .45 ACP
Capacity: One 13 round magazine included
Barrel: 5.5", 1:16" twist, threaded muzzle
Length: 16"
Weight: ~5.4 pounds

$1450 (1.2271 BTC)
amount 0

(more photo)

BLUEGRASS ARMORY MOONSHINER BULLPUP .308 WINCHESTER

Caliber: .308 Winchester
Capacity: One magazine included
Barrel: 21" 4140 Chrome Moly steel tapered heavy Barrel, threaded muzzle
Dimensions: 36" long
Weight: ~12.2 pounds

$2300 (1.9464 BTC)
amount 0

(more photo)

CENTURY ARMS CENTURION 39 AK 7.62X39

Caliber: 7.62x39MM
Capacity: 2 30 Round Tapco magazines included
Length: 37.25"
Barrel: 16.5", 1:10" Twist

$930 (0.787 BTC)
amount 0

(more photo)

FN SCAR 17S 16.25" 7.62X51

Caliber: 7.62x51mm NATO
Capacity: One 20 round magazine included
Barrel: 16.25" Chrome-Lined Hammer Forged steel
Length: 28" with stock folded, 35.5" with stock collapsed, 38" with stock extended
Weight (unloaded): ~7.9 pounds

$2450 (2.0734 BTC)
amount 0

UNODC
United Nations Office on Drugs and Crime

Registered GERMAN Passport

You will get an real registered German Passport with your data and picture. The Passport is registered at the German government system, so its means you can use it to travel around the world without any problems. The biometric chip will be not active coz we wont to have your fingerprint :) But if you want that the chip is active tell us this. in this case we need a picture with your finge...

Level 1






Canadian Passport Blanks (Not Counterfeit)

Discuss PM me. With this you ARE a Canadian citizen to border inspection personnel. Trafficking US-Canada border,with convenience,efficiency and ease. Use as counterfeiter's example sample for selling/making mass production. Passport Blank Contains: *36 pages with: -Security Patterned Unique Paper. -UV Fibers. -Canadian State Department Hologram Overlays. -Et...

Level 1

	Features		Features
Product class	Physical package	**Origin country**	Canada
Quantity left	6 items	**Ships to**	South America
Ends in	Never		Europe
			Asia
			Canada
			United States
		Payment	Escrow

USPS - 1 days - USD +0.00

Current bid price: USD 12,000.00

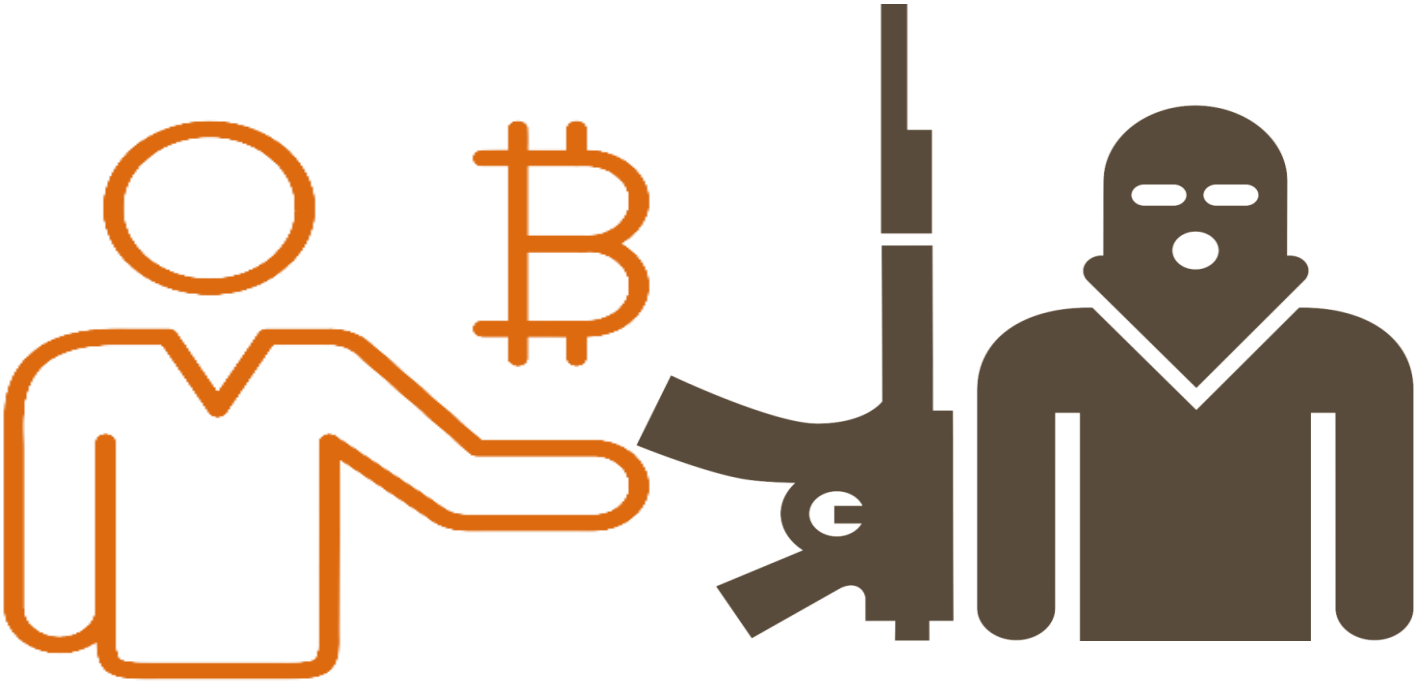
Bid: 12001.0 Place Bid

Purchase price: USD 17,000.00

Qty: 1 Buy Now

72.1317 BTC

Terrorist *financing*



Selected Episodes of *terrorists using cryptocurrencies*

January 2015

Supporter Abu Mustafa is able to raise five bitcoins (aprox. $1000) before his account was shut down by the FBI.

May 2015

Abu Ahmed al-Raqqa appeals to supporters of ISIS for donations in the form of bitcoins on the dark web.

June 2015

Ali Shukri Amin used socilal media to instruct donors on the use of Bitcoin to provide untraceable financial support to ISIS.

August 2015

"Albanian Hacker" demands two bitcoins (aprox. $500) from an Ilinois internet retailer in exchange for removing bugs from its computer.

July 2016

Mujahideen Shura Council in the Environs of Jerusalem receives around 0.929 bitcoins (aprox. $540) after adding the option of Bitcoin donation in June 2016.

January 2017

Indonesia`s financial transactions agency announces that Bitcoin was used by IS to fund terrorist activities in Indonesia

Is bitcoin really *anonymous*?

The blockchain stores data about all transactions

This data is publicly available and searchable by anyone (unlike bank transactions)

But no identity related information is stored

Only details regarding the addresses involved in transactions are provided

HOW DO WE INVESTIGATE THE BLOCKCHAIN?

Blockchain investigations

- the link analysis method -

- **Find the source of bitcoins (from money to crime)**

- Find where the bitcoins are now (from criminal proceeds)
- Identify other wallets/persons involved (expand the investigation)
- Explain the scheme to end-users (prosecutors, judges)

Raw bitcoin *transaction data*

100100101010101010101010010101010000010111110100101010100101
0100101010101010010101010010111101010100101011010000001000
1
1111010010010101100100101011011111101010010101011010010010101
0
1010101010100101010100000101111010010101010010101010010101010
0
1010010101010010111101010101001010110100000100001111101001001
0101100100101011011111101010010101011010010010101010101010
0101010100000101111101001010101001010101010100101010
1

All bitcoin transactions have *3 basic components*

TRANSACTION ID (HASH)

The unique identifier for a specific transaction. You can enter a given transaction ID into any Bitcoin service, and it will always return the exact same Bitcoin transaction.

INPUT ADDRESS(ES)

A user sends Bitcoin from one or more Bitcoin addresses that he controls.

OUTPUT ADDRESS(ES)

Bitcoins from input addresses are transferred to one or more output addresses.

Inputs and outputs

Each transaction has an input and an output side. All addresses on the input side will be fully spent

Input: shows where the bitcoins are coming from

Output: shows where the bitcoins are going to

SUM OF INPUTS = SUM OF OUTPUTS + A FEE

Reminder: Address A may send bitcoins to Address B, but these two addresses may reside in the same wallet.

1 input and 1 output

Not how the majority of transactions look

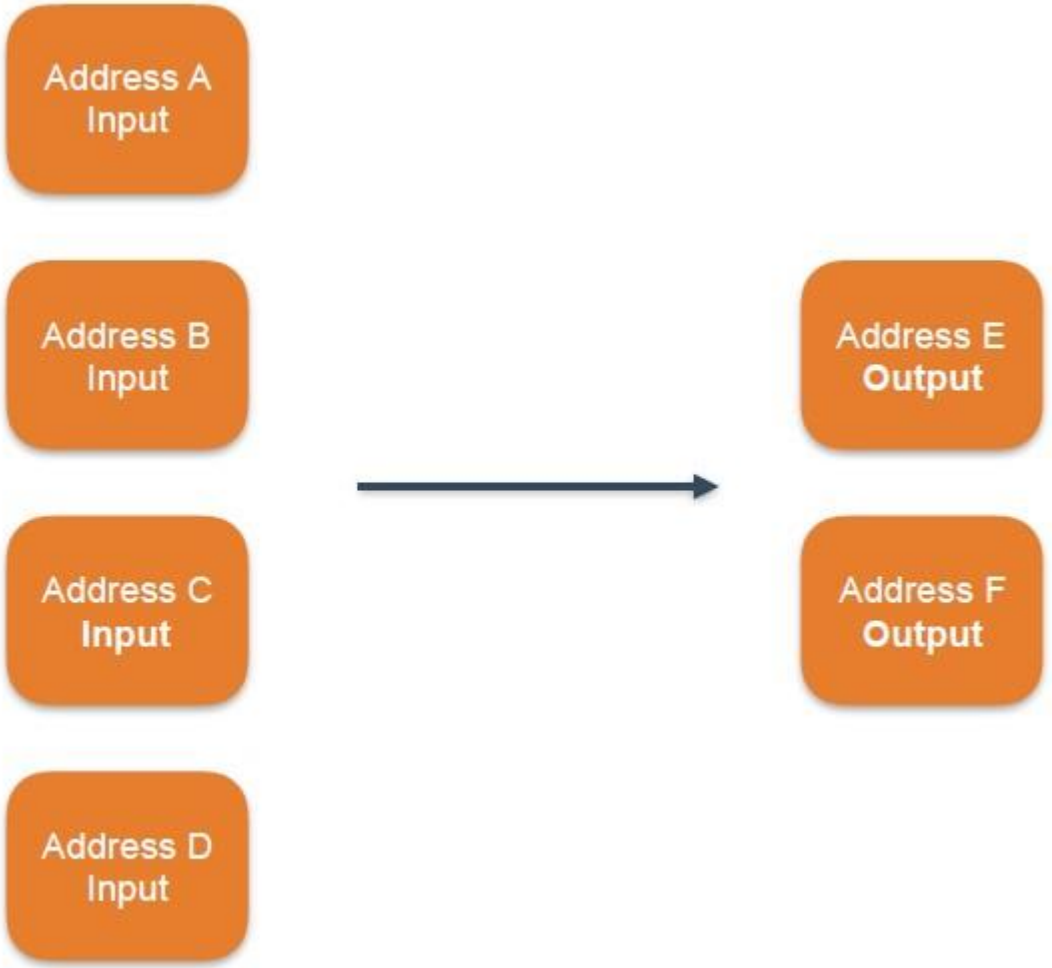
- All the bitcoins in Address A have to be sent from Address A to Address B.

There is no need to spend multiple input addresses or to create a change address.

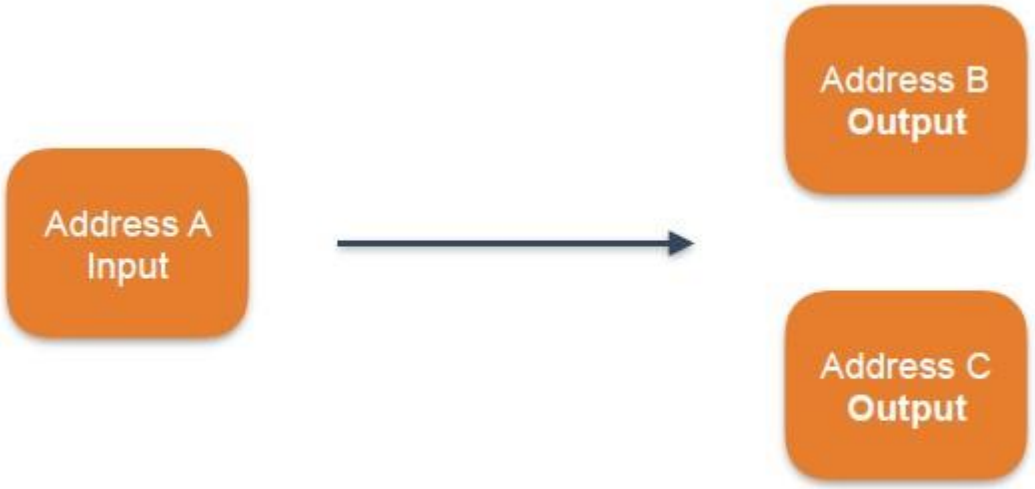
Address B receives slightly less BTC, due to a transaction fee (.000003 BTC)

Multiple input transactions

Usually the input addresses belong to a single wallet



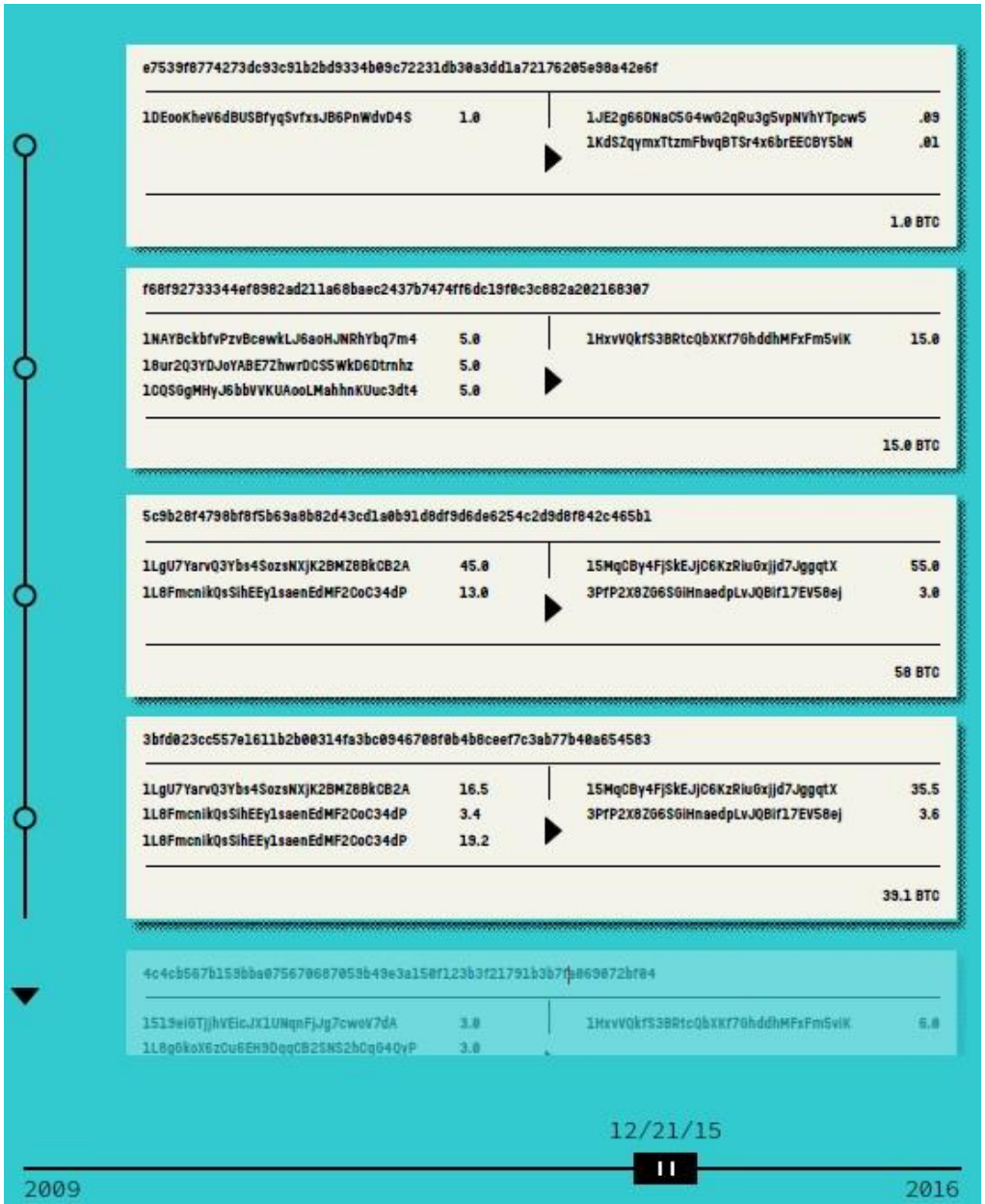
- **1 input and 2 output**



- Input address is fully spent and all bitcoins are moved to two different output addresses.

EVERY BITCOIN TRANSACTION IS RECORDED IN THE *BLOCKCHAIN*

The complete blockchain is freely available, and everyone can view the raw transaction information in ***blockchain explorers*** such as www.Blockchain.info



Height	Block created	Transactions	Size (kB)	Block value (Btc)	Pool	Hash
439,983	9 min ago	1	946	12.50 BTC	BTCC Pool	x00..f3170
439,982	10 min ago	2,508	999,939	9,887.24 BTC	F2Pool/Discus Fish	x00..7249f
439,981	31 min ago	1,611	998,189	4,400.27 BTC	AntPool	x00..985cb
439,980	39 min ago	2,116	998,116	2,922.22 BTC	unknown	x00..09fb5
439,979	40 min ago	2,449	998,182	11,344.99 BTC	AntPool	x00..ff981
439,978	an hour ago	5	2,143	36.37 BTC	AntPool	x00..794c6
439,977	an hour ago	2,095	998,929	7,812.20 BTC	BTCC Pool	x00..d65ab
439,976	an hour ago	1,097	749,152	4,971.73 BTC	unknown	x00..ffd32
439,975	an hour ago	2,472	989,844	2,991.91 BTC	BTCC Pool	x00..b36e2
439,974	an hour ago	2,848	998,196	13,044.32 BTC	AntPool	x00..55aad

BLOCKCHAIN info

Home Charts Stats Markets API Wallet English

Transaction View information about a bitcoin transaction

1203ec2e6465e8392713074be011b5c321fd1b84a0bc3d36ea7c008833814df0

19iVyH1qUxgywY8LJSbpV4VavjZmyuEyxV (25.34415906 BTC - Output)

157p475z6pq7hyxJbXXqfGVhXQp6Hw1cvC - (Spent) 5.429 BTC

1MEe2mebed8wopvy8xyjjHcEQHUPVJn2UC - (Unspent) 19.91405906 BTC

1 Confirmations 25.34305906 BTC

True IP address of the sender??

Summary	
Size	226 (bytes)
Received Time	2016-06-16 15:08:40
Included In Blocks	416578 (2016-06-16 15:23:02 + 14 minutes)
Confirmations	1 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	25.34415906 BTC
Total Output	25.34305906 BTC
Fees	0.0011 BTC
Estimated BTC Transacted	5.429 BTC
Scripts	Hide scripts & coinbase

Network Propagation (Click to view)

Investigative limits and challenges*?*

- Don’t trust IP information (due to the way bitcoin works)
- Don’t trust click and trace - more context is needed

Tools?

Open Source Solutions:

Web based explorers

BlockSeer

Maltego – has a free version

Commercial Solutions:

Chainalysis

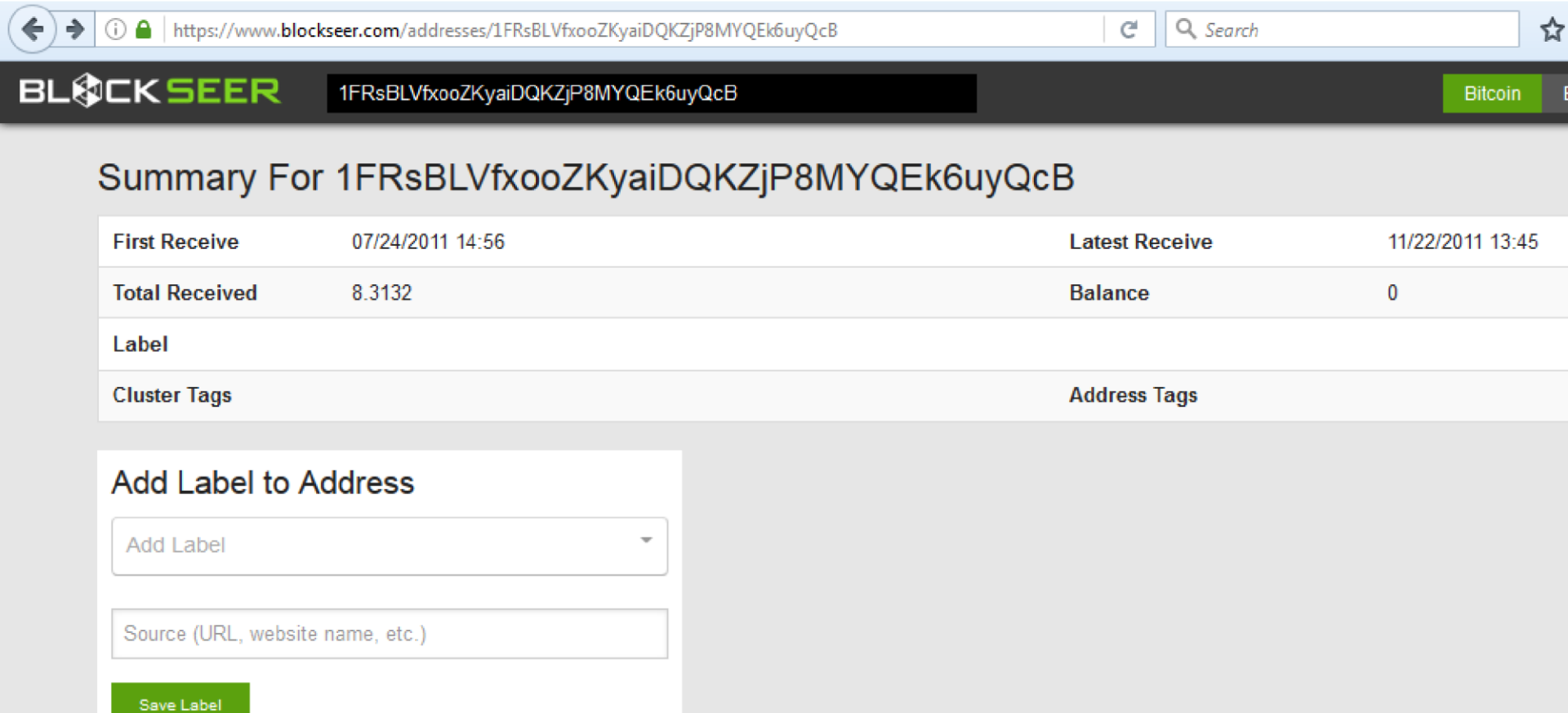
Elliptic

BlockSEER

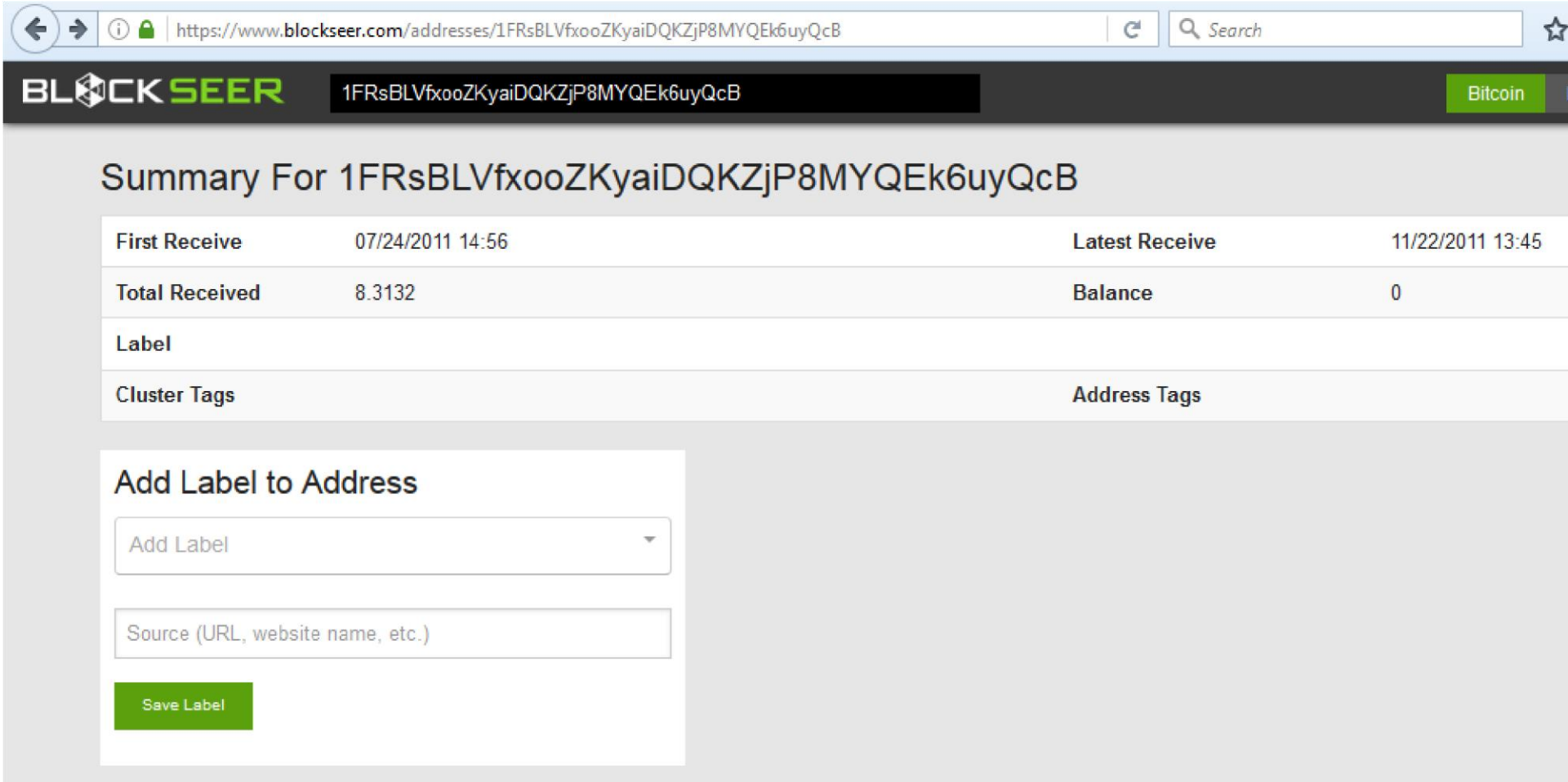
www.blockseer.com

– Register

– Sign in and start using



Enter the address



Click on transactions

BLOCKSEER 1FRsBLVfxooZKyaiDQKZjP8MYQEk6uyQcB Bitcoin Ethereum (Beta)

Summary For 1FRsBLVfxooZKyaiDQKZjP8MYQEk6uyQcB

First Receive	07/24/2011 14:56	Latest Receive	11/22/2011 13:45
Total Received	8.3132	Balance	0
Label			
Cluster Tags		Address Tags	

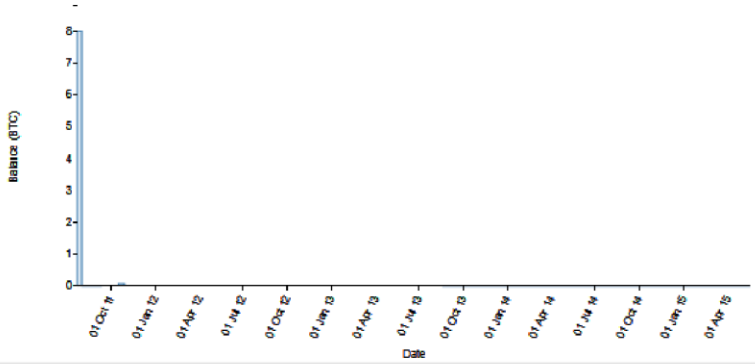
Add Label to Address

Add Label

Source (URL, website name, etc.)

Save Label

Balance Over Time

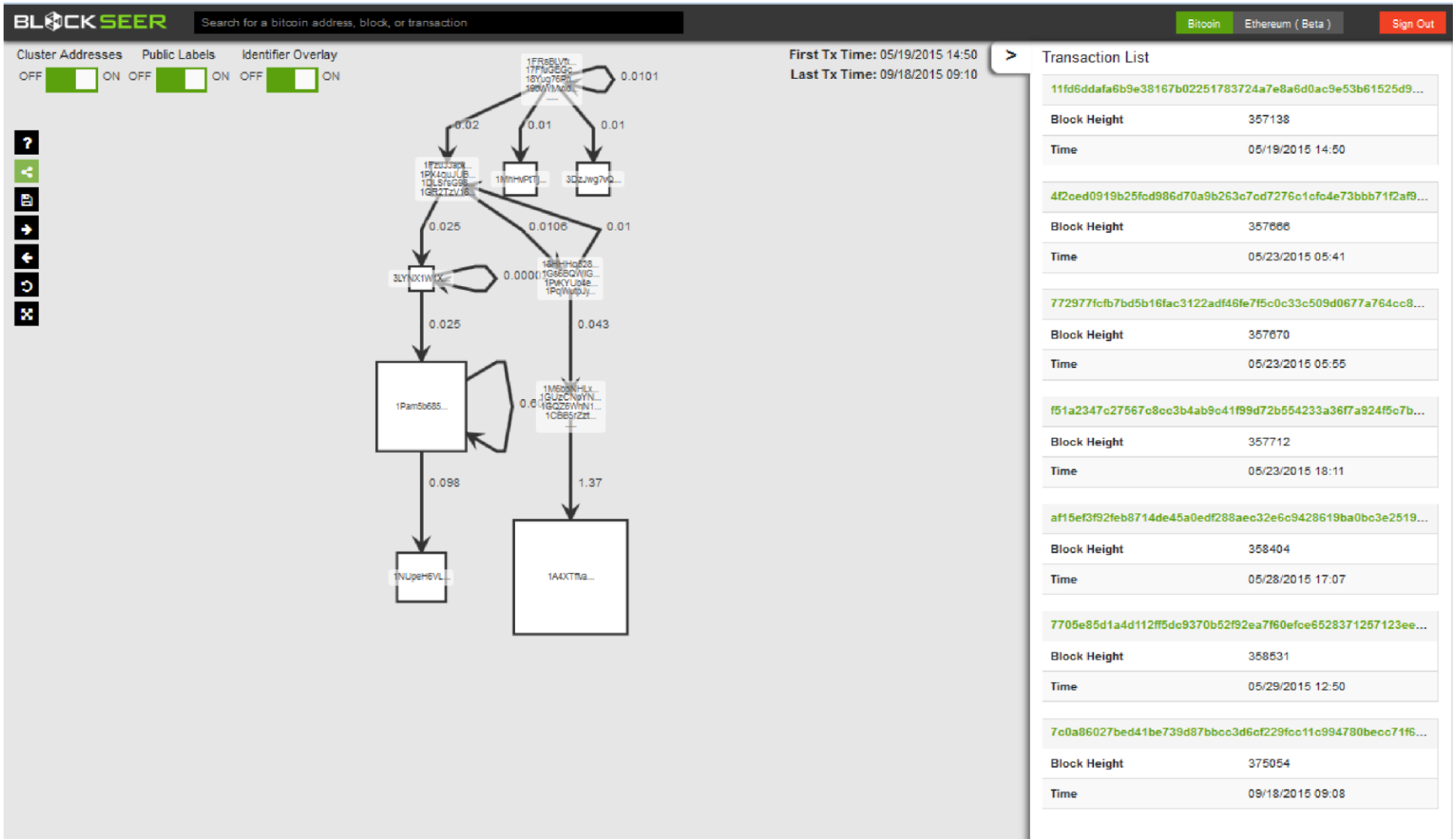


Transaction List

All

Block Date ▼	Block Height ▼	Net Balance Change	USD Amount	Fee	Tx Hash
05/19/2015 14:50	357138	-0.005	$ -1.16	0.0001	11fb6ddafa6b9e38167b0225178372 4a7e8a6d0ac9e5...
11/22/2011 13:45	154388	-0.001	$ 0.00	0.0005	940be1867bc7e1bb3bfe2949f514ccc74f9a259edff23...
11/22/2011 12:12	154344	-0.001	$ 0.00	0.0005	252099fa3711b9193a42145001d0fdd70642c18bd340...
11/14/2011 09:23	153225	-0.001	$ 0.00	0.0005	be9d7e82681d428cc289eead2c24e30d9a6d7c98b8...
11/12/2011 12:36	152959	-0.001	$ 0.00	0.0005	c95c76498673c3415040ae56f419be8e462af32006d3...
11/12/2011 11:36	152955	-0.001	$ 0.00	0.0005	7b7625921abb73f8f89c8c1f1ac8aa031dd015a6730b6...
11/12/2011 11:14	152952	-0.001	$ 0.00	0.0005	ffba9f218d705b5e77bc24b7aa83d3455919d32b5437e...

Explore the graph

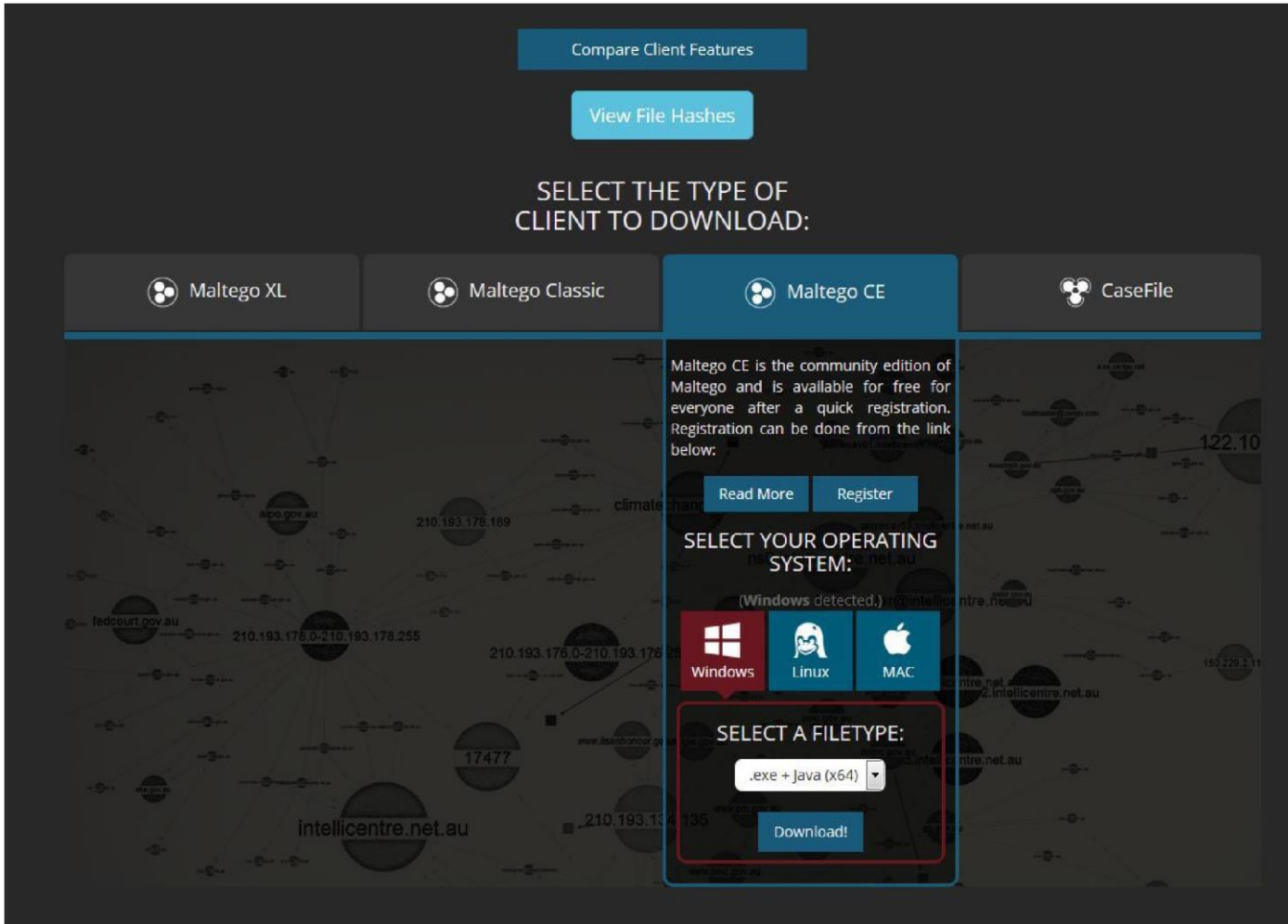


Maltego

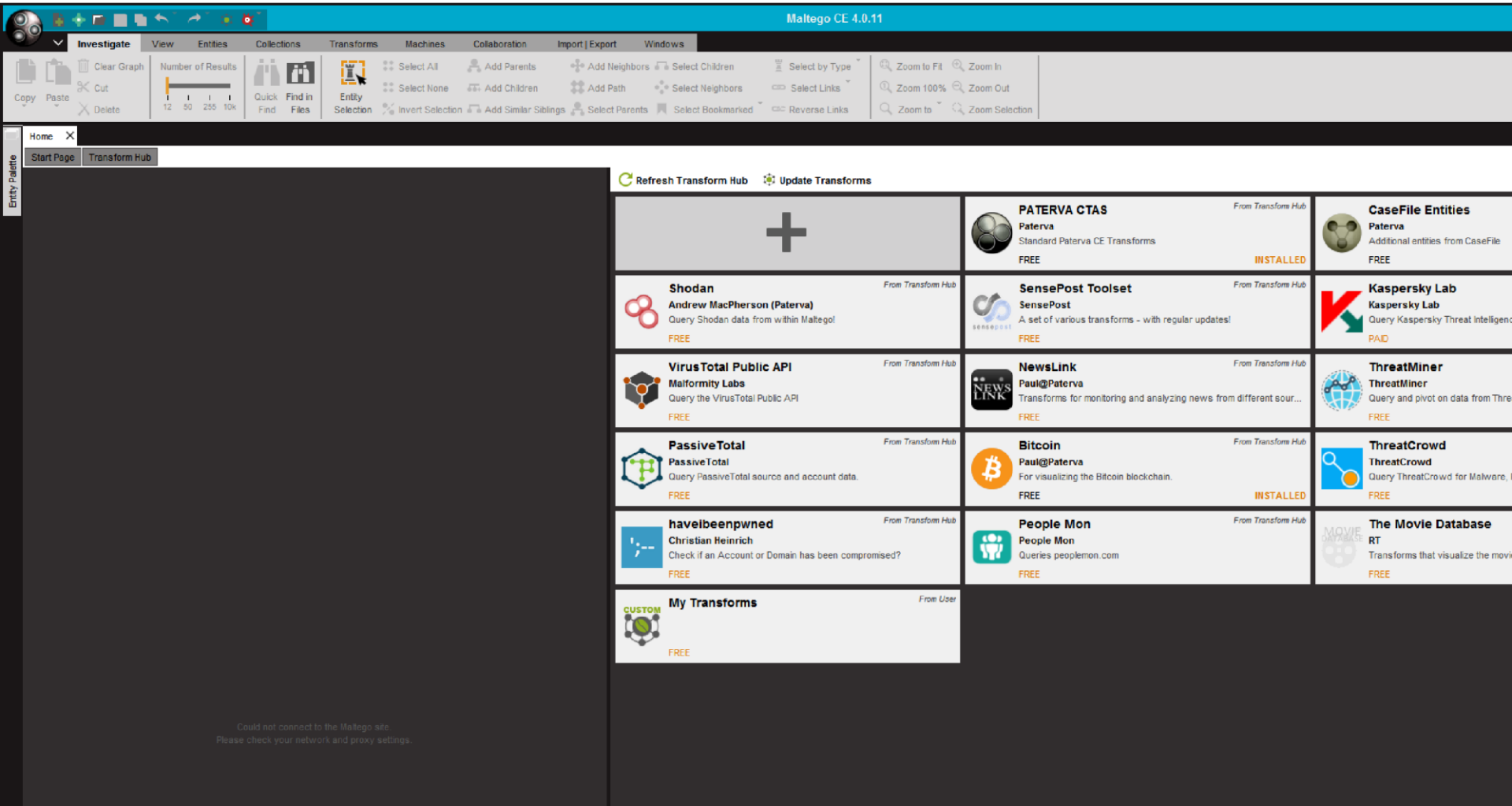
https://www.paterva.com/web7/downloads.php#tab-

3 Instal a CE

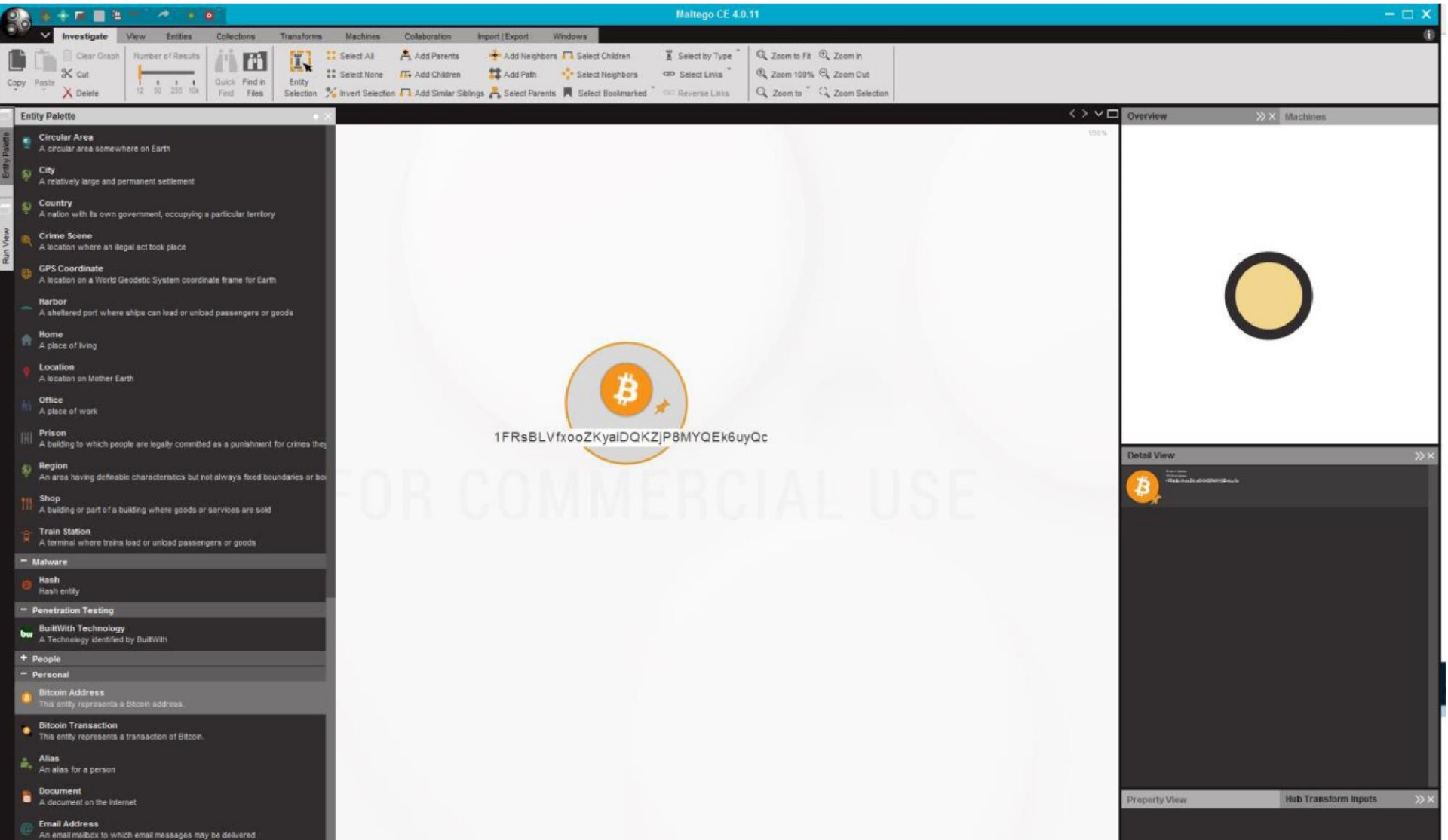
Eddition register



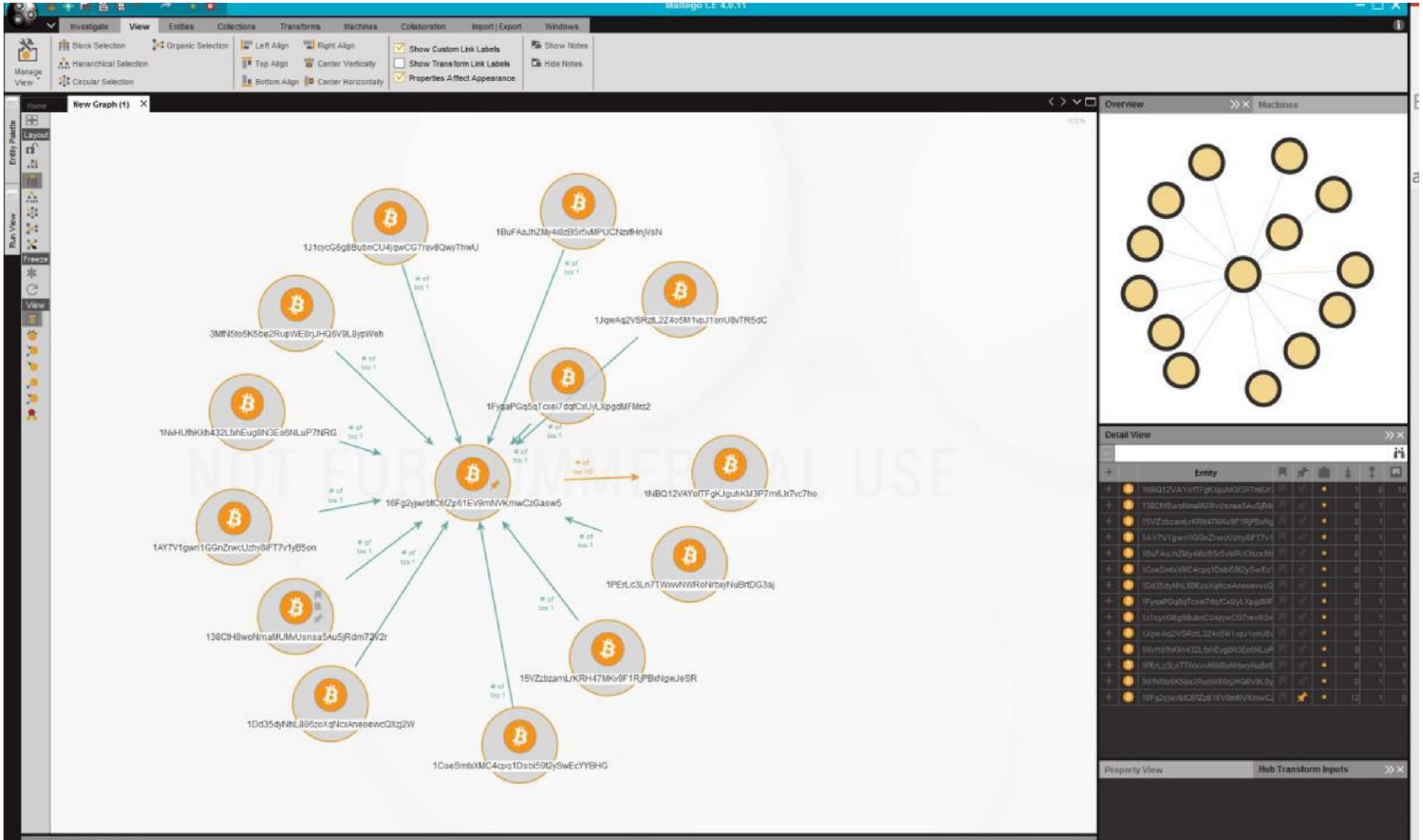
Install a bitcoin transform



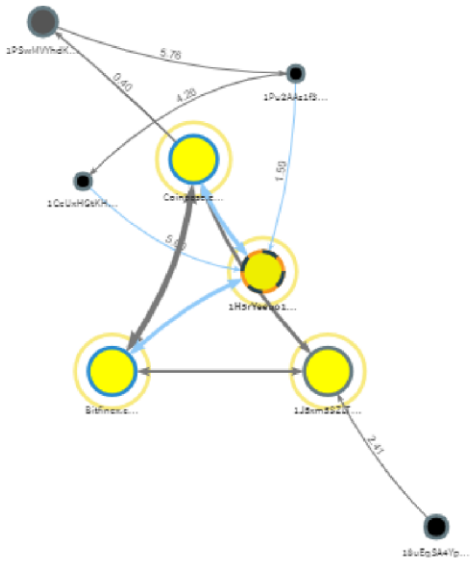
Add a bitcoin address to your graph



Run transforms and explore graphs



Chainalysis



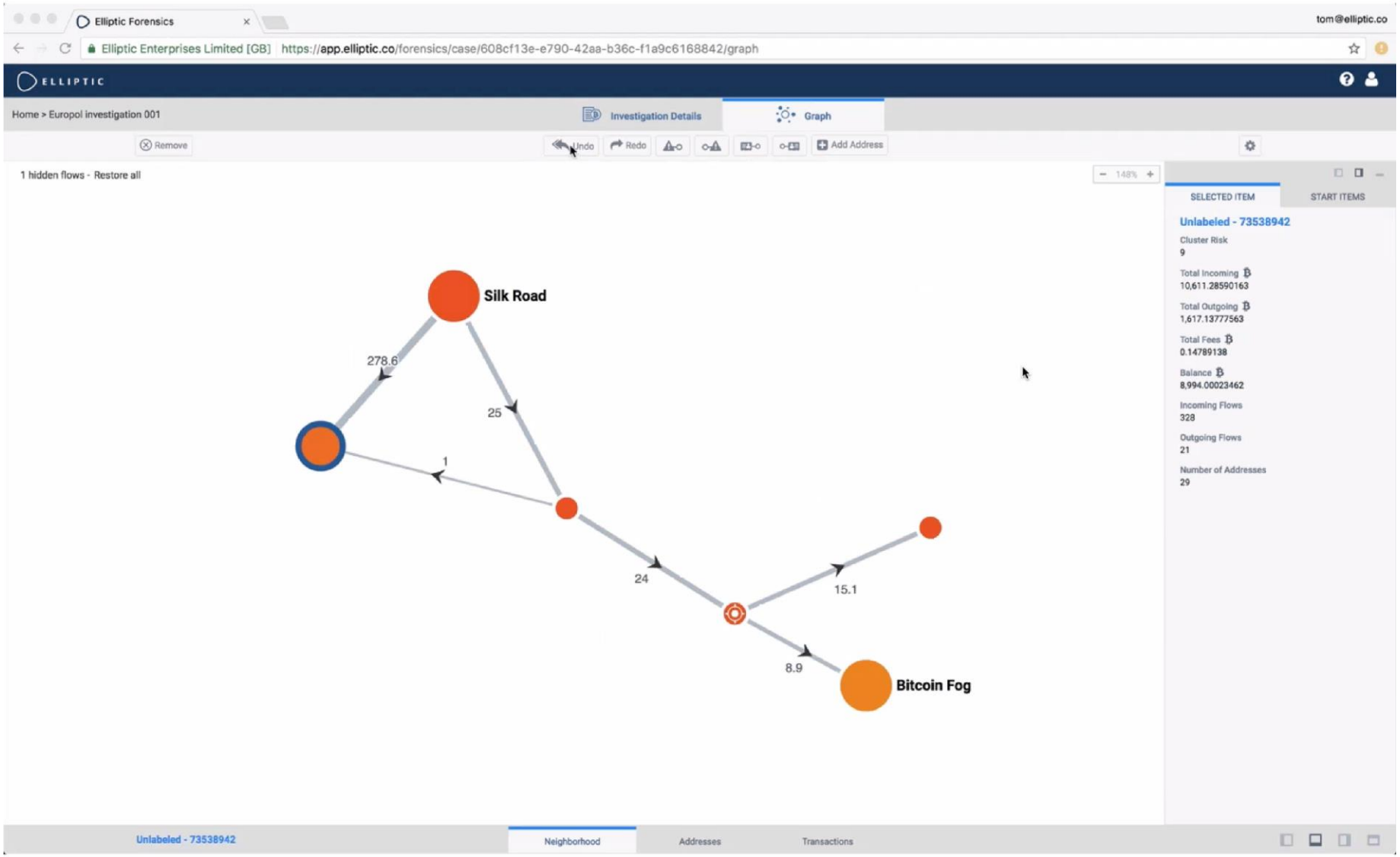
SUMMARY | EXPOSURE | COUNTERPARTIES | TRANSACTIONS | ADDRESSES | OSINT

Graph name	Organization Name	Chainalysis Name	Root Address	Category
Enter name	Enter name	*None*	1H5rYeeuo1X8Ts...	Unknown

Add notes

0 / 32000

Balance:	2.29217499 BTC	Transactions:	30,676
Sent:	5,468.07363418 BTC	Withdrawals:	12,255
Received:	5,478.55656392 BTC	Deposits:	20,666


Elliptic Forensics
tom@elliptic.co
Elliptic Enterprises Limited [GB] https://app.elliptic.co/forensics/case/608cf13e-e790-42aa-b36c-f1a9c6168842/graph
ELLIPTIC
Home > Europol investigation 001
Investigation Details
Graph
Remove
Undo
Redo
Add Address
1 hidden flows - Restore all
148%
SELECTED ITEM
START ITEMS
Unlabeled - 73538942
Cluster Risk
9
Total Incoming
10,611.28590163
Total Outgoing
1,617.13777563
Total Fees
0.14789138
Balance
8,994.00023462
Incoming Flows
328
Outgoing Flows
21
Number of Addresses
29
Silk Road
278.6
25
1
24
15.1
8.9
Bitcoin Fog
Unlabeled - 73538942
Neighborhood
Addresses
Transactions

BITCOIN INVOICE

Peer-to-Peer Encrypted Invoice System - Blockonomics and third parties won't be able to read your invoice content

Search your bitcoin address and click on Create P2P Invoice

SEARCH

Waiting for a Bitcoin transaction to confirm?

Search By Transaction ID

Bitcoin Address/Wallet Balance

Search mutliple bitcoin addresses/xpub separated by spaces

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 115p7U

ADDRESS	BALANCE	UNCONFIRMED AMOUNT
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	0 BTC	0 BTC
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	0.09 BTC	0 BTC
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	1.19658268 BTC	0 BTC
Total Balance:	1.28658268 BTC	0 BTC

Web-based *explorers?*

- ✓They require a lot of knowledge and a lot of work
- ✓Very hard to aggregate multiple addresses
- ✓Cannot link multiple addresses to the same wallet (clustering)


CryptoLocker
Payment for private key
Choose a convenient payment method:
Bitcoin
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.
You have to send below specified amount to Bitcoin address 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh and specify the transaction ID, which will be verified and confirmed.
Home Page
Getting started with Bitcoin
Enter the transaction ID and press «Pay»:
1 BTC
Private key will be destroyed on
9/13/2013
11:25 AM
Time left
71 : 55 : 23
Bitcoin payment
<< Back
PAY

Cryptolocker virus Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh
Hash 160	c9a0729b5bbe1775bf55e36cff7a8660846de720
Tools	Related Tags - Unspent Outputs

Transactions		
No. Transactions	40	
Total Received	54.9083 BTC	
Final Balance	0 BTC	

Request Payment Donation Button

Transactions (Oldest First)

Filter

Featured sponsor

52a6cac56ad95bb4de4bc6964671f76288d2da3edd7182efe096a33123d49c5a — **2013-11-19 14:01:09**

Cryptolocker virus	161yYpWYCx8cWGYW95QaZ9NUuR3fd5n4xt 1FscKAWjfRAF7SQ787psJYtHcKRrCsTZC7	15 BTC 0.01000008 BTC

-0.0002 BTC

47f1dd4af19a5a4175ad2f85224fd654c785b5c9c65405ecda4f8bee3fa43155 — **2013-10-15 15:16:17**

Cryptolocker virus	1HSN65qWF7EtBgrD85kjqeuYH7P5UaaSaZ 1AEoiHY23fbBn8… (Cryptolocker ransom)	0.20780439 BTC 127 BTC

-3.9995 BTC

SUMMARY | EXPOSURE | COUNTERPARTIES | TRANSACTIONS | ADDRESSES | OSINT

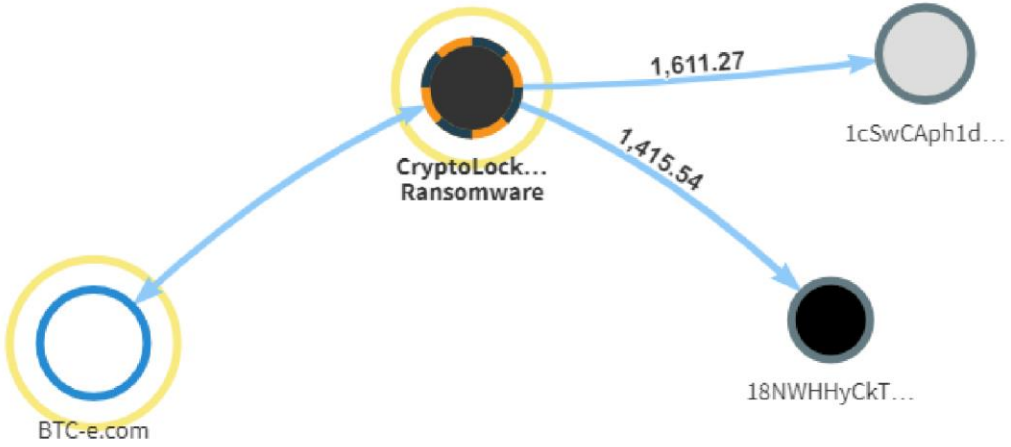
Graph name	Organization Name	Chainalysis Name	Root Address	Category
Enter name	Enter name	CryptoLocker Ransom...	1KP72fBmh3XBRf...	Ransomware

Add notes

0 / 32000

Balance:	0.00010025 BTC	Transactions:	5,620
Sent:	4,538.55768934 BTC	Withdrawals:	113
Received:	4,538.93499261 BTC	Deposits:	5,559
Total Fees:	0.37720302 BTC	Addresses:	4,457

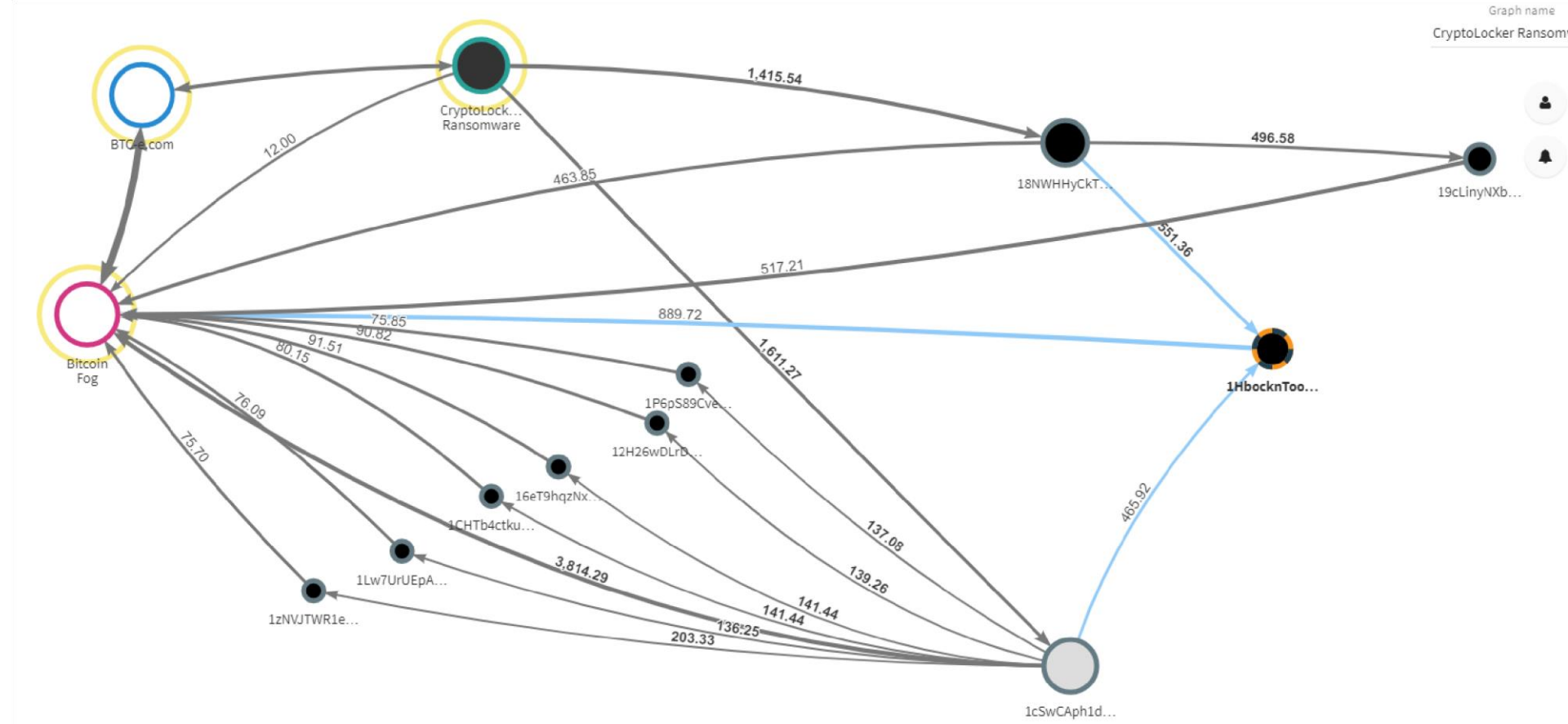
Open In New Graph



SUMMARY | EXPOSURE | COUNTERPARTIES | TRANSACTIONS | ADDRESSES | OSINT

Cluster: CryptoLocker Ransomware Balance: 0.000 Sent: 4,539 Received: 4,539 Fees: 0.377 Addresses: 4,457 Transactions: 5,620

Counterparty	#TXO	Sent	Received	Flow	First	Last
1cSwCAph1dBMri5mwpAeaL3apadSdGne5	15	1,611.274	0	-1,611.274	3/9/16	5/16/16
18NWHHyCkTfsDPQJaMu5uGhpviS87hWfWk	61	1,415.538	0	-1,415.538	5/19/16	10/6/16
BTC-e.com	39	1,208.457	23.823	-1,184.634	9/11/13	8/31/16
18TbmQ42TZekptuQ3is3zwaPT1AdaJUkkr	1	40.000	0	-40.000	10/12/13	10/12/13
1EZdbrwVuTtGZijezWmvvzDRjLmNVN2owm	1	40.000	0	-40.000	10/13/13	10/13/13
17DubUSP8SKe4ZUi7WogaXtLwy1fm9vhQS	1	40.000	0	-40.000	10/11/13	10/11/13
1HFT1rkHQWHPWsAaqa1g1VWaFbS7Do2Usq	1	40.000	0	-40.000	10/15/13	10/15/13
15gjdP9HbWr7sM1yryG7PL8vrFcLFMtCVM	1	30.000	0	-30.000	10/10/13	10/10/13
1J5YCtttAhc4L72pFmxpXCuZyCiPupRjoE	1	20.000	0	-20.000	10/8/13	10/8/13
1MVAdyP2EHWUnP4D61jBrzfX9oQH5FGFJX	1	20.000	0	-20.000	10/7/13	10/7/13
1GA17Pk7kC6bPLUQpeCZXmzwgjrXbUEWSD	1	15.000	0	-15.000	10/3/13	10/3/13


Graph name
CryptoLocker Ransom
BTCe.com
CryptoLock...
Ransomware
1,415.54
12.00
463.85
18NWHHyCkT...
496.58
19cLinyNXb...
551.36
517.21
889.72
75.85
90.82
91.51
80.15
76.09
75.70
Bitcoin
Fog
1,611.27
1P6pS89CVe...
12H26wDLrD...
16eT9hqzNx...
1CHTb4ctku...
1Lw7UrUEpA...
1zNVJTWR1e...
3,814.29
141.44
141.44
136.25
203.33
137.08
139.26
1HbocknToo...
465.92
1cSwCAph1d...

Mixing Bitcoins with Bitcoin Fog

POSTED BY: ADMIN OCTOBER 1, 2016

[avg] ([per]) [total] vote[s]

Bitcoin Fog is the Bitcoin Mixing and Tumbling service that covers up your tracks in the Bitcoin world.

- **Bitcoin Fog Darkent link**: http://foggeddriztrcar2.onion
- **Registreation URL**: http://foggeddriztrcar2.onion/?page=register
- **Bitcoin Fog login Link**: http://foggeddriztrcar2.onion/?page=index
- **Twitter updates clearnet link** : https://twitter.com/#!/@BitcoinFog

Russian arrested over bitcoin laundering linked to BTC-e exchange: Sources

- A Russian national was arrested on suspicion of laundering criminal funds through Bitcoin.
- Alexander Vinnik, which sources say was a key figure behind the BTC-e cryptocurrency exchange, was arrested in Greece on a U.S. warrant.
- Vinnik is suspected of laundering at least $4 billion.

8 Hours Ago

REUTERS

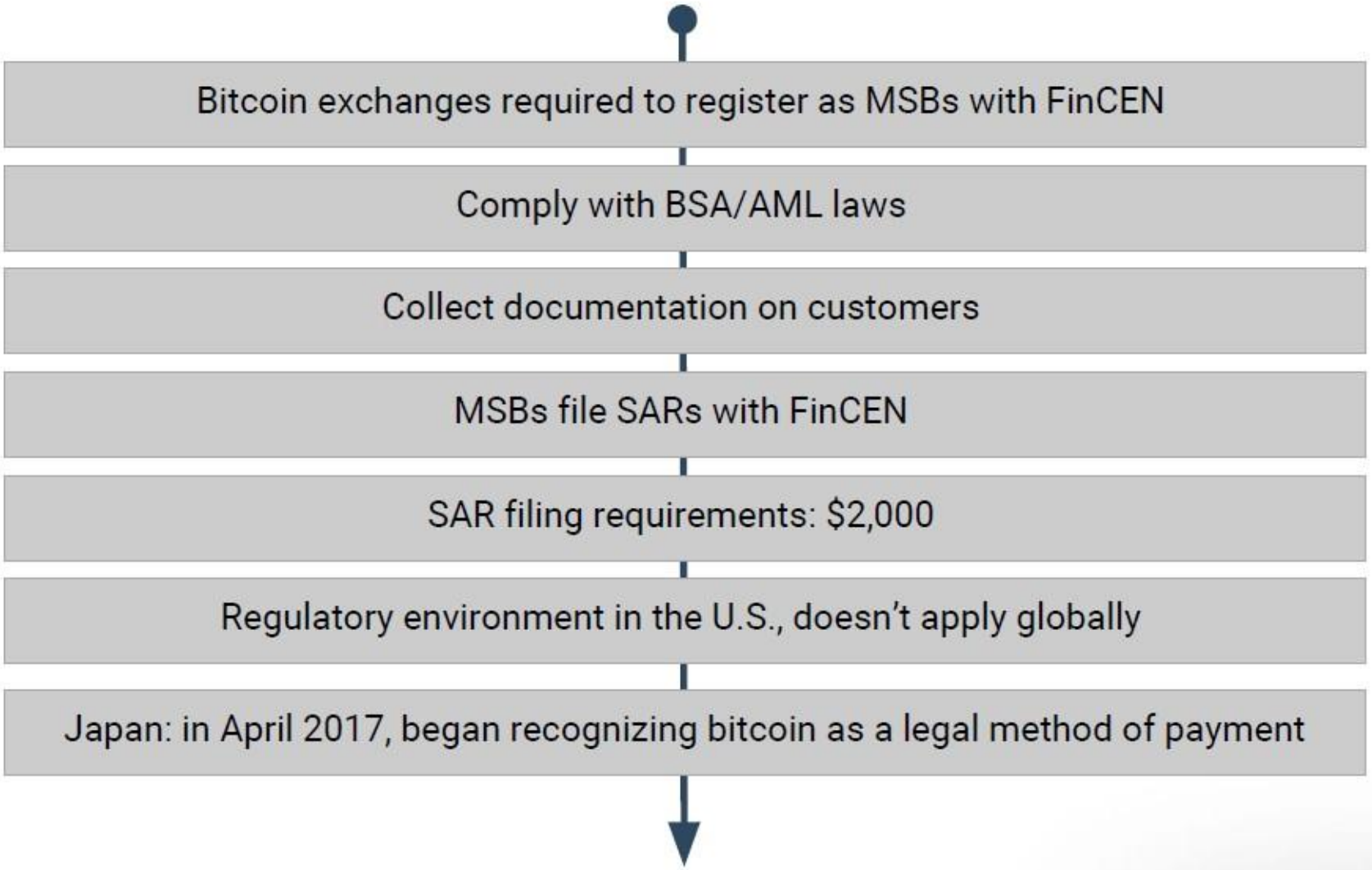
Alexandros Avramidis | Reuters

Alexander Vinnik, a 38 year old Russian man (L) suspected of running a money laundering operation, is escorted by a plain-clothes police officer to a court in Thessaloniki, Greece July 26, 2017.

Founded in 2011, BTC-e is one of the oldest and most obscure virtual currency exchanges, allowing users to trade bitcoin anonymously against fiat currencies, such as the U.S. dollar, and other virtual currencies. Until today, the people behind it had remained anonymous.

It is known in crypto-currency markets as the one with the most relaxed standards for checking the identity of its users, to combat money laundering, and for not collaborating with law enforcement.

This helped make it "a favorite money laundering location" and the exchange has been connected to recent ransomware attacks, said James Smith, chief executive of Elliptic, a company that works with law enforcement to track illicit bitcoin transactions.


Bitcoin exchanges required to register as MSBs with FinCEN
Comply with BSA/AML laws
Collect documentation on customers
MSBs file SARs with FinCEN
SAR filing requirements: $2,000
Regulatory environment in the U.S., doesn't apply globally
Japan: in April 2017, began recognizing bitcoin as a legal method of payment

Conclusion

Bitcoin transactions are not anonymous

We are potentially able to trace the transactions back to their owners through a lot of work

Proper regulation is needed to require bitcoin exchangers to follow KYC and AML compliance

Thank *you*

UNODC
United Nations Office on Drugs and Crime

CYBERCRIME

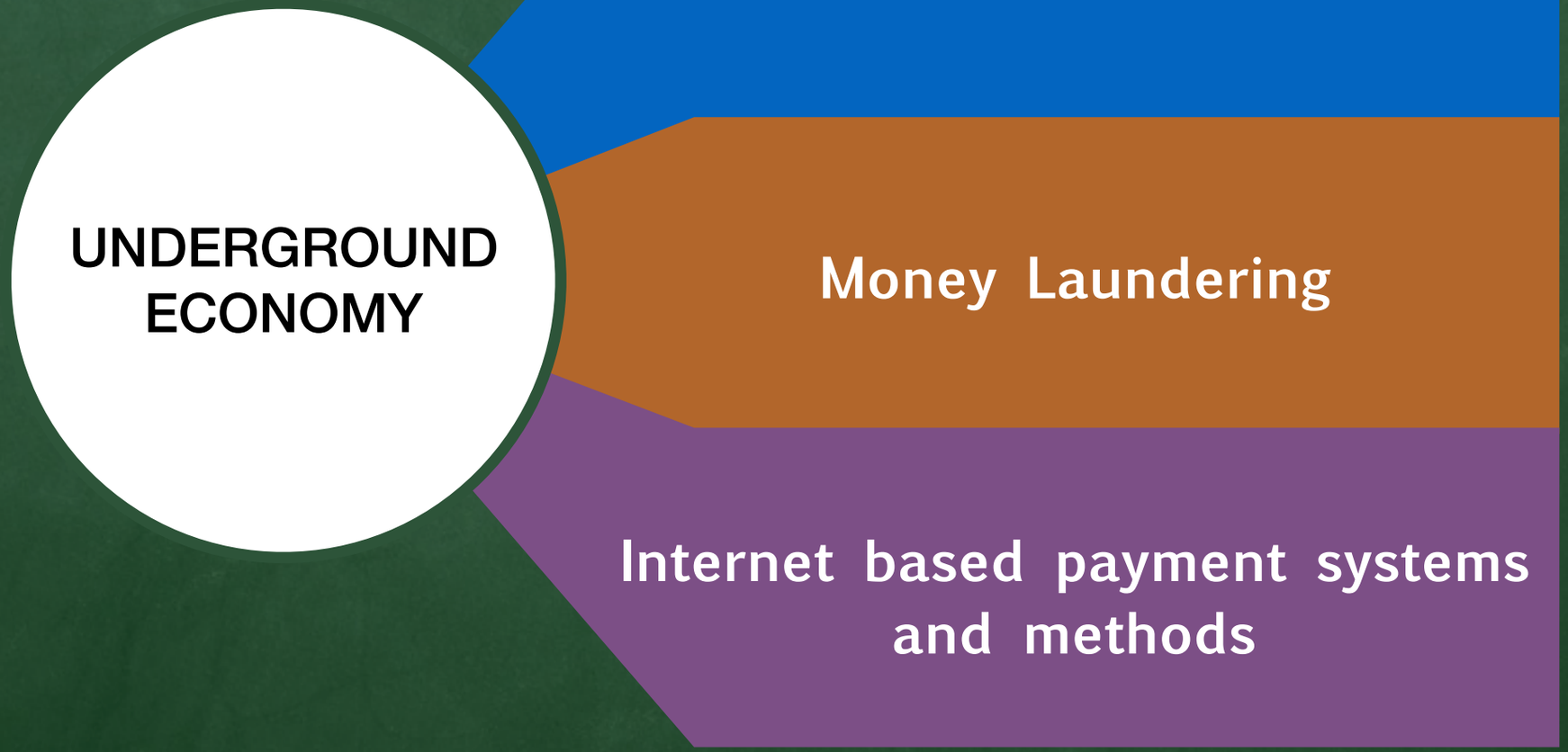
neil.walsh@un.org
https://www.linkedin.com/in/neiljwalsh
https://twitter.com/neil_w_unodc

Criminal Money Flows - Investigation Online

Athens, 7 November 2017
ERA

Co-funded by the Justice Programme of the European Union 2014-2020

BLACK MONEY


UNDERGROUND ECONOMY
CYBERCRIME
Money Laundering
Internet based payment systems and methods

Proceeds generating offences on the Internet

FRAUD. Identity theft, Payment Card Fraud, Online Banking Attacks, Misuse and Account Take-over, Mass-marketing Fraud, Auction Fraud, Investment Fraud nil. Stock Market Manipulation, Pyramid and Other Multi-level marketing schemes

CHILD ABUSE MATERIALS

SALES OF COUNTERFEITS

VIOLATION OF COPYRIGHTS AND RELATED RIGHTS

ONLINE EXTORITION

Most Popular Internet Based Payment Solutions

- PayPal
- Skrill
- Stripe
- 2CheckOut
- ACH Payments
- WePay
- Authorize.Net
- Amazon Payments
- Dwolla
- Google Wallet
- Braintree
- Apple Pay
- Gumroad
- Klarna
- AliPay
- Tenpay
- Union Pay
- 99Bill
- ChinaPnR
- YeePay

Prepaid Cards - Responsible Entities

Acquirer

Distributor

(Incl. Retailer)

Payments network operator

Issuer

Programme manager

Agent

Mobile Payments - responsible entities

Mobile Network Operator

Distributor (Incl. Retailer)

Electronic Money Issuer

Business models can vary greatly depending on which service provider has the lead role, pre-paid or post-paid services and the technical platform used.

Typical features can be generalized as: a *bank-centric model* and a *mobile-network-operator-centric model*

Internet-based Payment Services

- Customers access pre-funded accounts to transfer e-money or value to other individuals or businesses which hold accounts with the same provider. Withdrawals by transferring to a bank account, pre-paid card or another money/value service

- Variety of business models: digital wallets, digital and virtual currencies, electronic money..., which may be interconnected with other payment methods

- Digital currency providers may allow third parties to undertake the exchange of national currencies with the electronic currency or value.

- Sales of virtual precious metals...
  Online auction payments...
  Online gambling...

Factors in Determining the Responsible Entity

- The entity which has visibility and management of the payment products and services
- The entity which maintains relationship with customers
- The entity which accepts funds from customer
- The entity against which the customer has a claim for those funds

Risks in Methods of Funding

- ✓ **Prepaid Cards** - Cash funding, In rare cases reloadability with no limit or customer due diligence requirements
- ✓ **Mobile payment services** - cash and non-bank payment options; improper identification at funding by third parties
- ✓ **Internet Based payment services** - anonymous third party funding; virtual *bureaux de change*
- ✓ **Virtual Currencies** - all of the above mentioned funding risks
- ✓ **Segmentation of services** - several parties spread among jurisdictions involved in execution of payments

The phenomenon of virtual currencies...

Follow the money..?

"I *still* haven't found what I'm looking for."

Following the Trails...

- ✓ TI/OLAF E-Tool for disclosure of ownership structures and beneficial ownership
- ✓ Social Networks and other open source (OSINT)
- ✓ PGP Keys (Dark Web)
- ✓ Covert Online Investigations
- ✓ Automated re/searching and analysis software

FIU as a Tool

- FIU.NET

- The Egmond Group

Suspicious banking transactions (examples)

- Transactions which do not correspond to regular business activities
- Several companies represented by the same individual
- Irregularities at loans (e.g. early high cash deposits)
- Frequent transactions with persons from countries with strict bank secrecy or known for trade in narcotics
- Only nominees manage rented safe deposit boxes
- “Sudden income to sleeping accounts”, or multiple incomes under 10.000€ followed by high cash withdrawals or transfers
- Short time period opening and closing of BA combined with transfer of funds to another bank
- Absence of non-cash transactions (BA of a legal entity or entrepreneur)

International Cooperation

EUROPOL
EC3 | European Cybercrime Centre

EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

EUROPEAN JUDICIAL
E01000101
J01001010
C01000011
N01001110
CYBERCRIME NETWORK

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

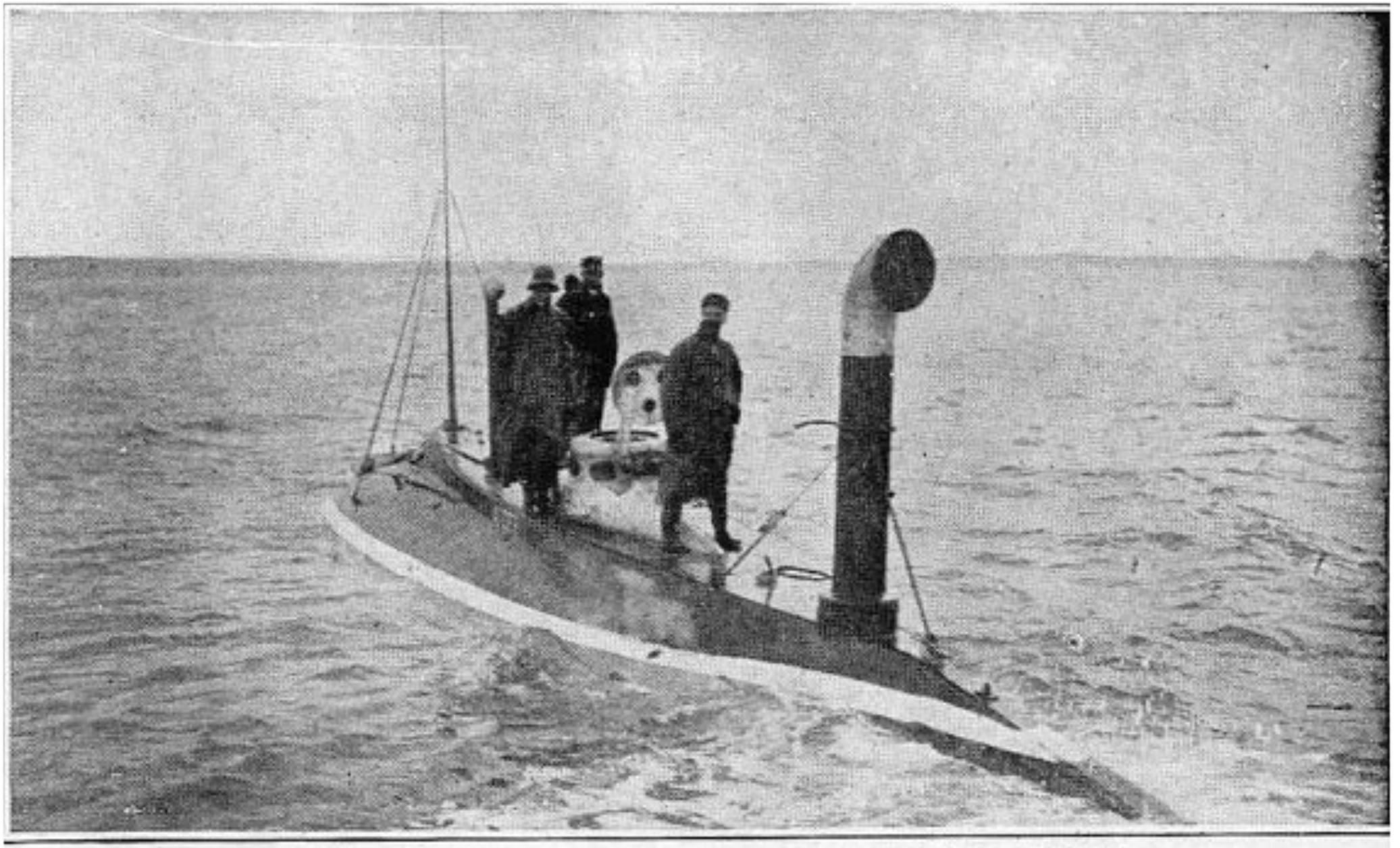
OLAF
OFFICE EUROPÉEN DE LUTTE ANTI-FRAUDE
EUROPEAN COMMISSION
EUROPEAN ANTI-FRAUD OFFICE

carin

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR

LEGAL TOOLS

- ✓ European Investigation Order
- ✓ Warsaw (AML) Convention - Articles 3-5, 13, 17-24
- ✓ Budapest (Cybercrime) Convention - Articles 16-21, 29, 32
- ✓ EU Anti-Money-Laundering Legislation (Revision of the 4th AML Directive)
- ✓ Direct cooperation with internet service providers...(?)



SUBMARINE ON SURFACE AT FULL SPEED

Questions?

pklement@nsz.brn.justice.cz

Co-funded by the Justice Programme of the European Union 2014-2020

ERA Seminar, "The life cycle of e-evidence", Athens 7-8 November 2017

"***ONLINE FINANCIAL OFFENCES AND E-EVIDENCE IN LEGAL PROCEEDINGS: THE VIEW OF THE DEFENCE***" (presented by *Dominikos Arvanitis*)

A. Introduction

B. The protection of individuals

1. The right to a fair trial

2. The right to have access to a lawyer

3. The principle of legality

4. The principle of proportionality

C. Conclusion

The internet Industry Perspective

Cormac Callanan
Aconite Internet Solutions
Dublin, Ireland
cc@aconite.com
m: +353 87 257 7791

Co-funded by the Justice Programme of the European Union 2014-2020

Who am I?

- IANAL
- IANAP

- Cybercrime Expert for
  - Council of Europe
  - OSCE
  - EC
- Industry background
- First ISP in Ireland
- Past-President of EuroISPA
- Past-CEO INHOPE International Network of Internet Hotlines
- MSc
  - Computer Systems Design 1991
  - Advanced Security and Digital Forensics 2017

Agenda

- Credit Card Fraud
- Detection and Prevention
- Policy
  - Concrete case Studies

Online platforms

Self-Regulation

CREDIT CARD FRAUD

Payment Details
Card not present

DETECTION AND PREVENTION

Data Retention

Encryption

Suspicious Transactions Reports

Profiling Systems

ACONITE
INTERNET SOLUTIONS

International Payment Systems

ACONITE
INTERNET SOLUTIONS

Advice

ACONITE
INTERNET SOLUTIONS

Electronic Currencies

New Challenges

ACONITE
INTERNET SOLUTIONS

POLICY
CONCRETE CASE STUDIES

ACONITE
INTERNET SOLUTIONS

Examples

Sextortion
Ransomware
CEO Fraud

ACONITE
INTERNET SOLUTIONS

Examples

Sextortion

2010 - Keith Hudson (39)/ Tyler Schrier (23)
docket number 2:11-cr-01175-SJO, USA v. Schrier, filed in the Central District of California

POKER PLAYERS

Sep 2011 - Leaked Photos

SCARLETT JOHANSSON

Case Study - Suicide Victim

AMANDA TODD

Case Study

GSK CHINA

HTTP://WWW.BBC.COM/NEWS/WORLD-ASIA-28712420

Examples

Ransomware

Examples

CEO Fraud

Questions?

Cormac Callanan
CEO, Aconite Internet Solutions

email: cc@aconite.com gsm: +353-87-257 7791

Internet Security Threat Report

ISTR

Examples of digital information theft and best practices to prevent it

Ilias Chantzos, Senior Director Government Affairs EMEA & APJ

Volume

22

Symantec

Co-funded by the Justice Programme of the European Union 2014-2020

Agenda

- Will discuss modus operandi, i.e. how the bad guys are thinking
- Will discuss some generic attack tactics that can apply on mobile or PC
- Will discuss specific figures on information theft and
  - Mobile
  - IoT
  - Data breaches
  - Underground economy
- Will close with best practices to protect yourself
- Q&A

It doesn’t matter who you are…. It is what you have access to

Living off the Land

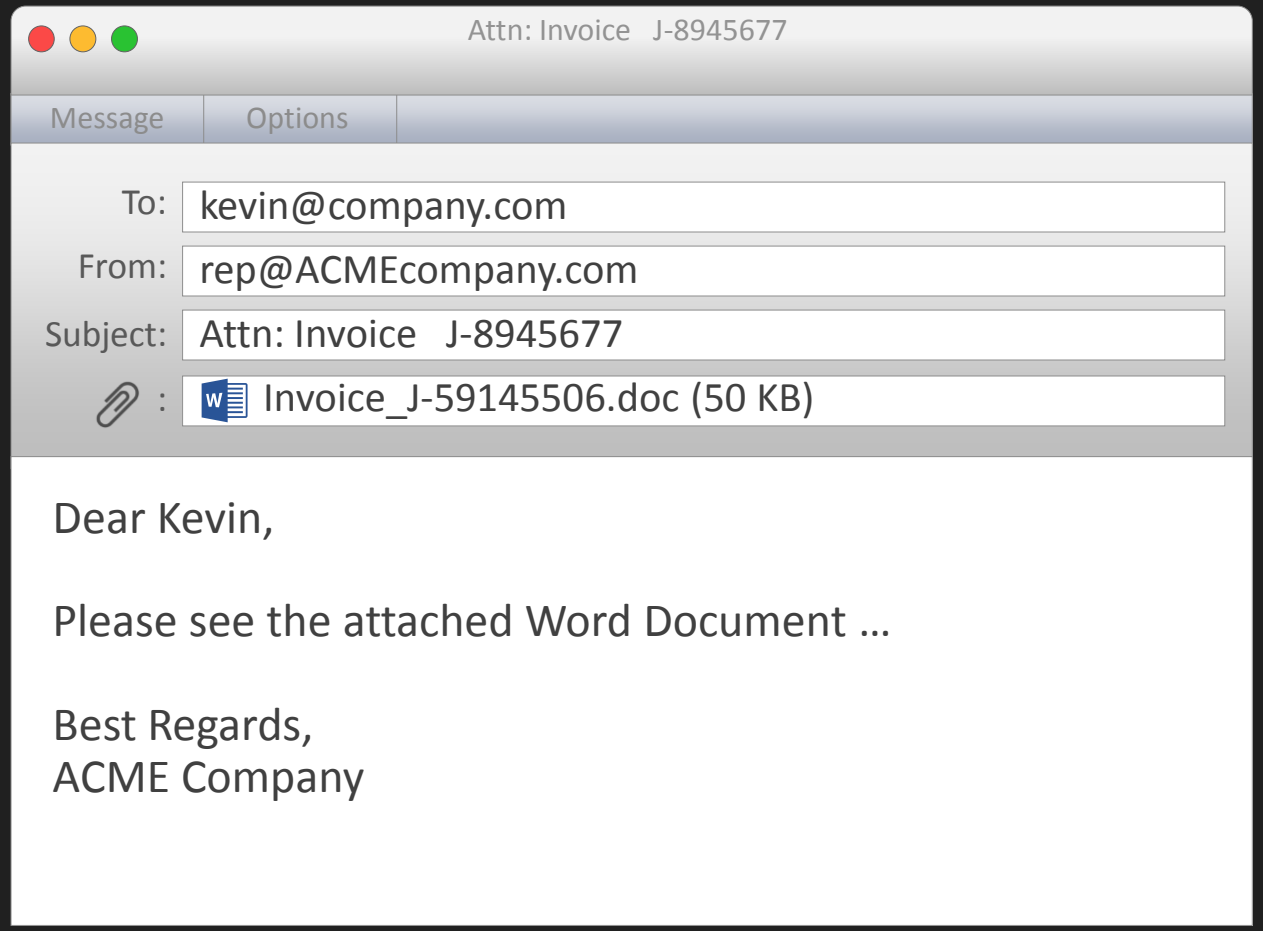
Attackers are using what's available to attack us

- These tools are ubiquitous
- These tools are easy to use for malicious purposes
- These tools don't arouse suspicion, and can be difficult to determine intent.

Number of Powerball Lottery tickets with a $7 payoff: 1 out of **317**

Emails that have attached malware or links to malware: 1 out of **131**

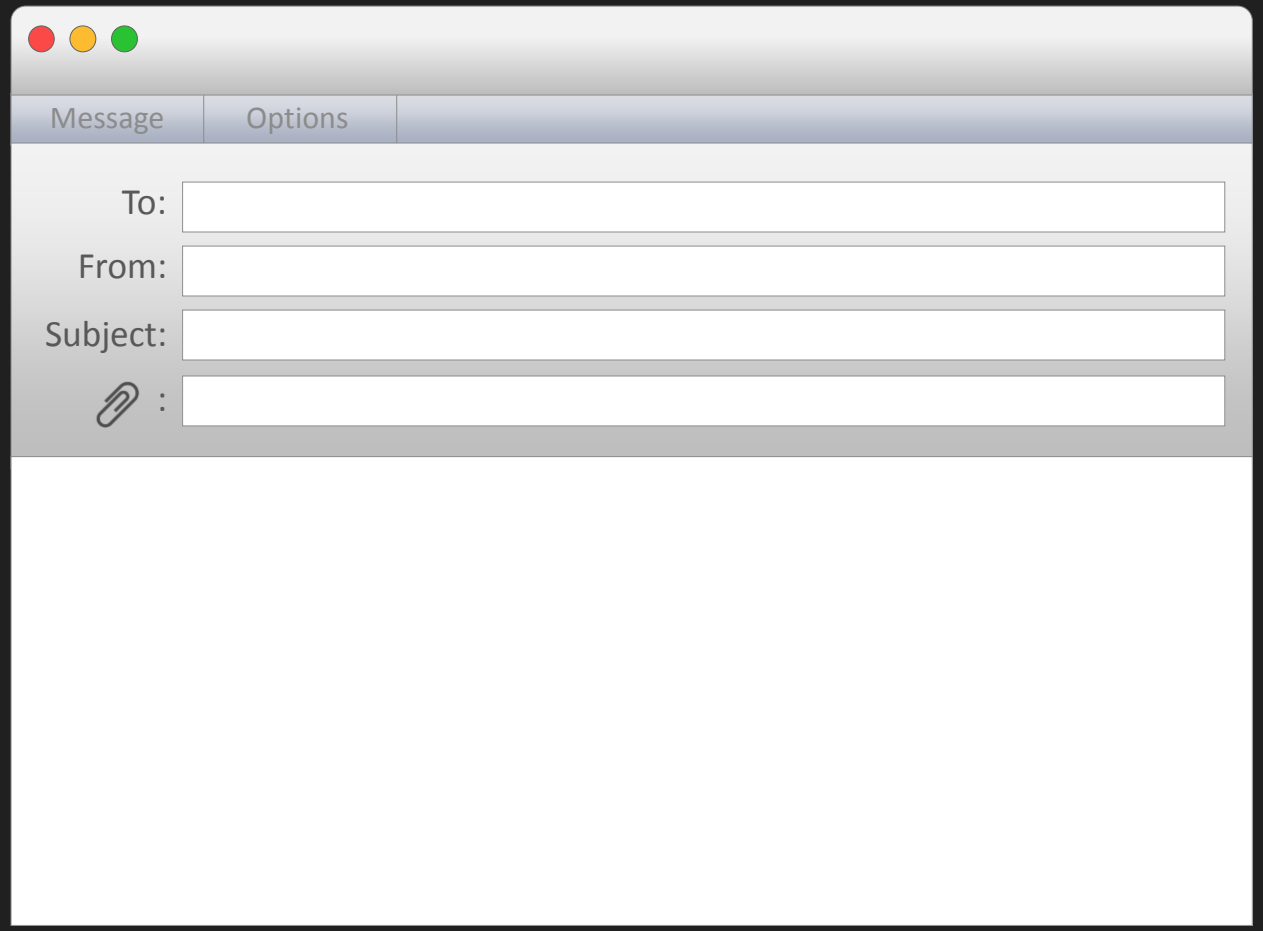
Email Attacks



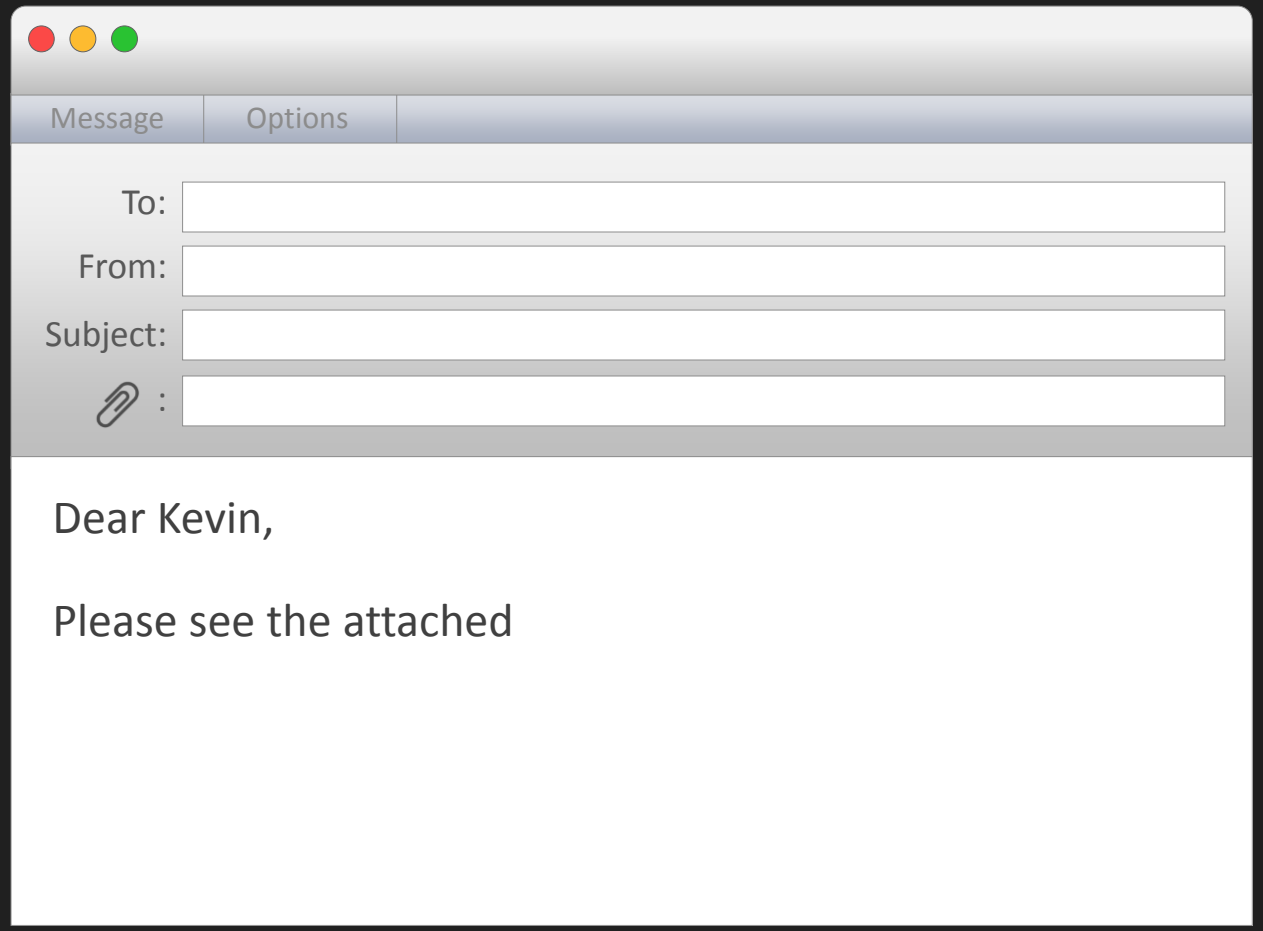
Symantec Sees Millions of Attacks per day sent via **Malicious Email**

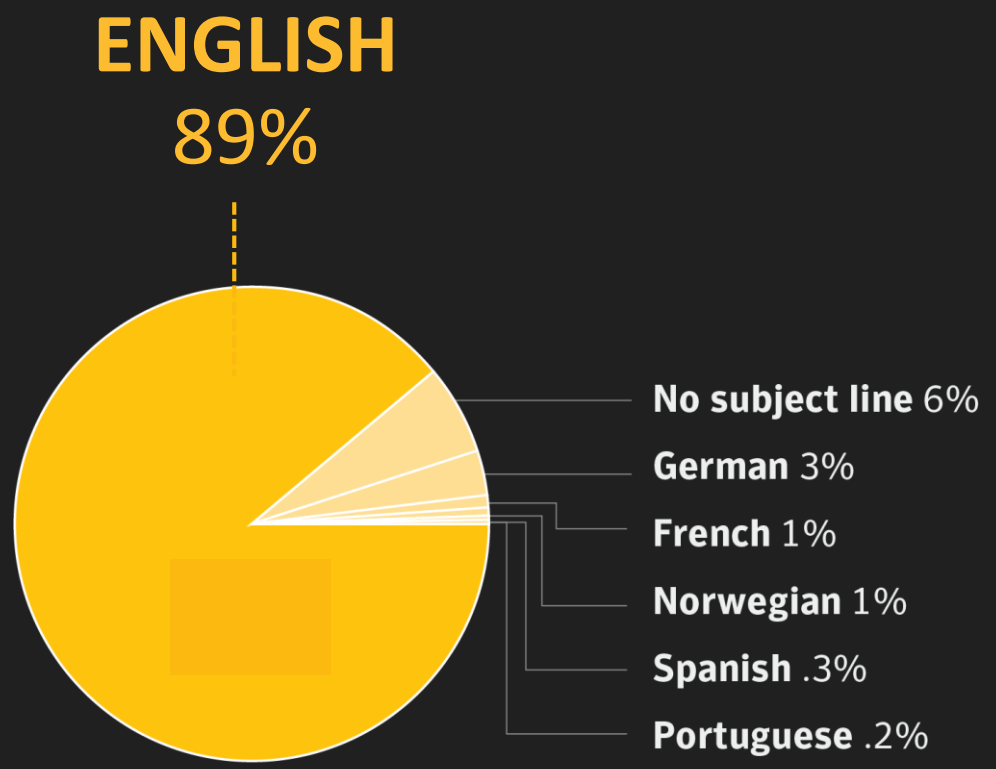
Malicious Emails Hit the Highest Rate in Five Years

Building Malicious Email

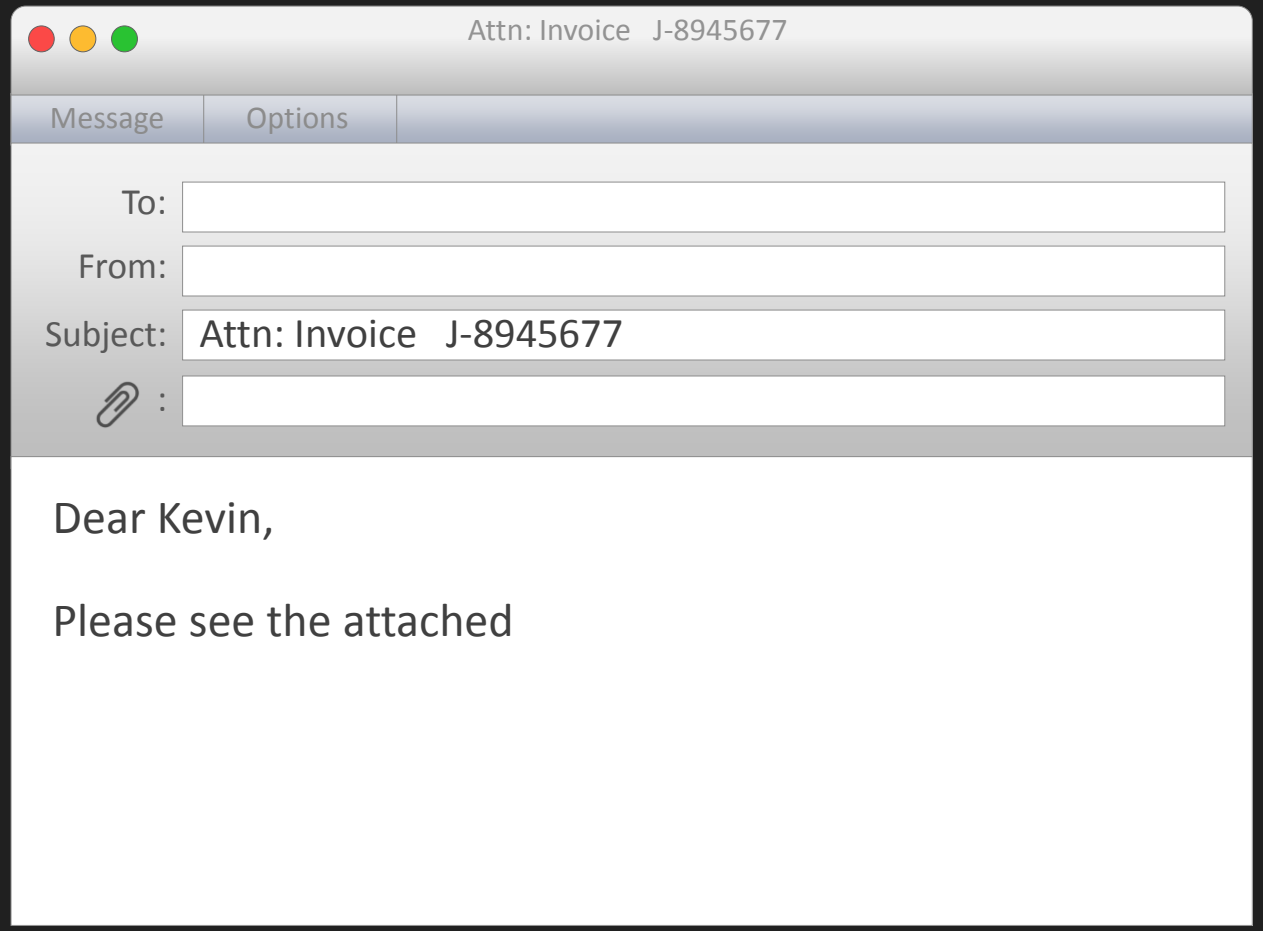


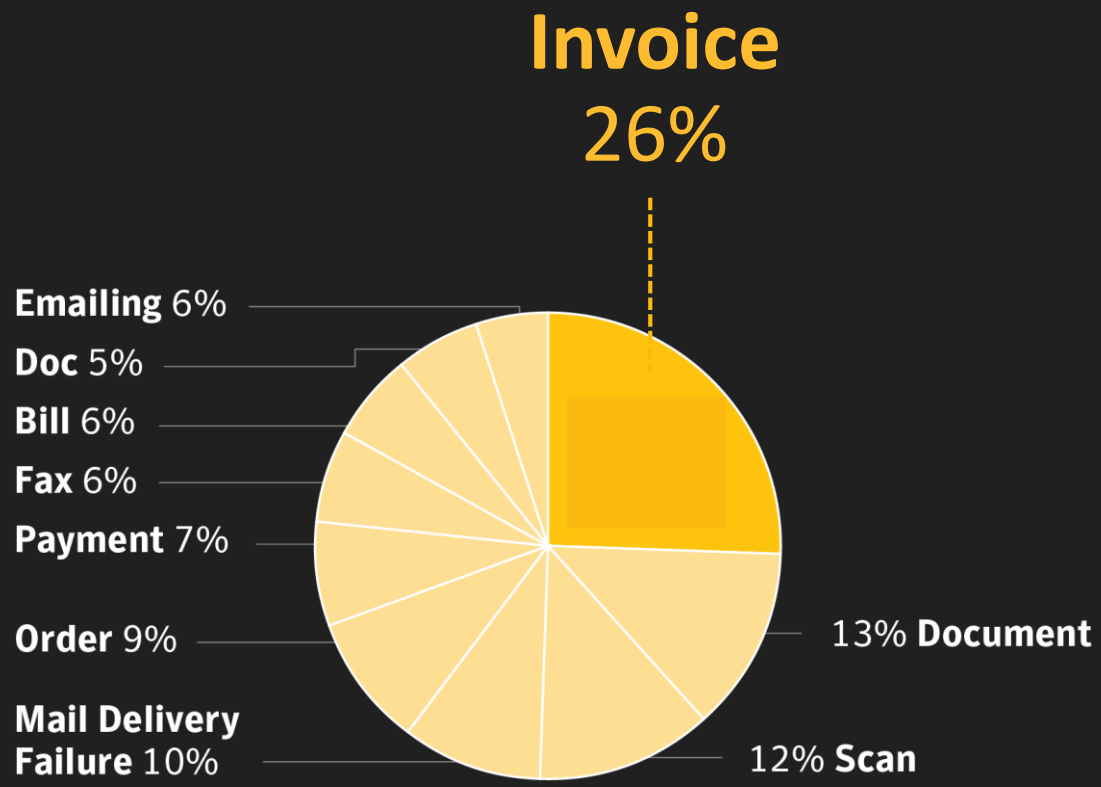
Building Malicious Email: Language





Building Malicious Email: Subject

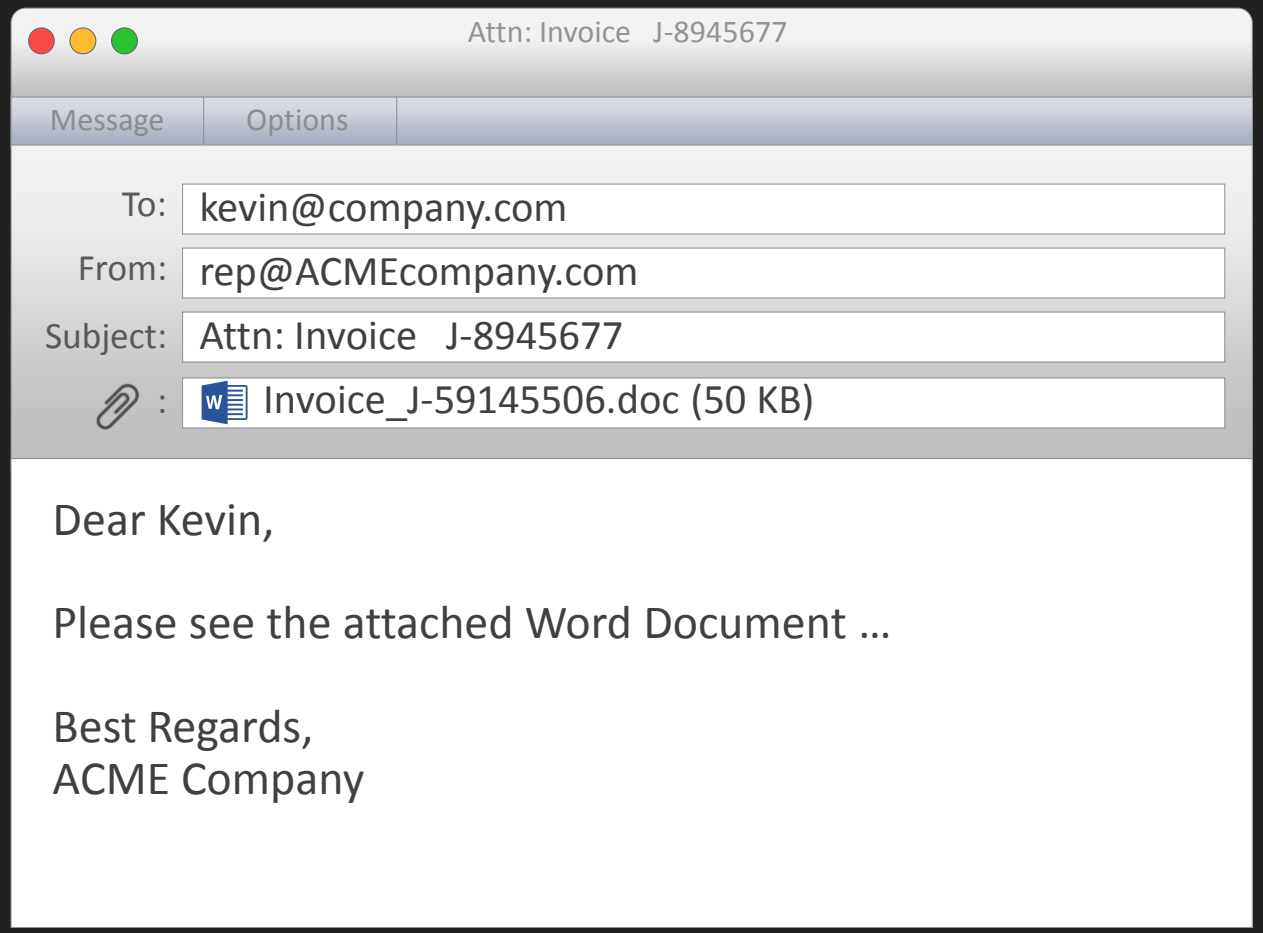




Building Malicious Email: To/From

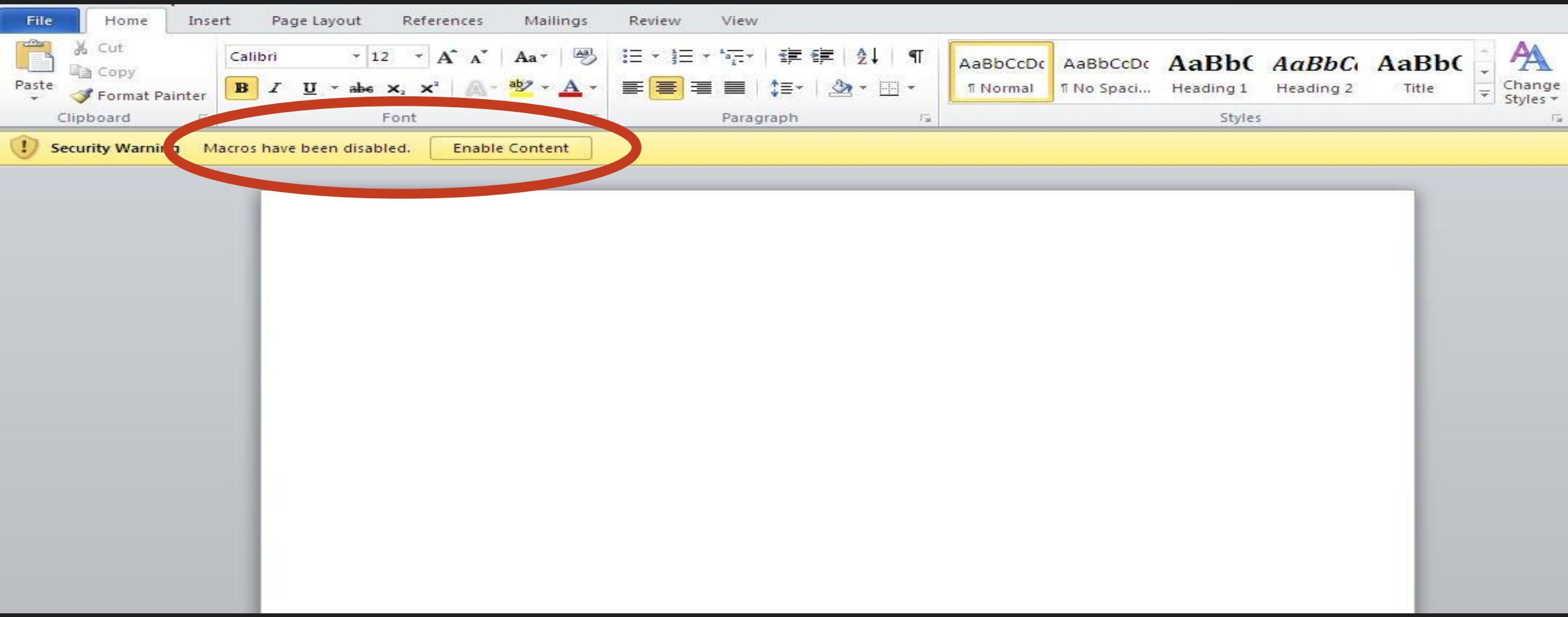
- The Sender is often spoofed to be a well known company, region specific.

Building Malicious Email: Attachment



- Most users are not suspicious of a Word file
- And they are harmless unless users can be tricked into enabling macros
- Social Engineering becomes more important to bad guys as defenses get better

Building Malicious Email: Social Engineering



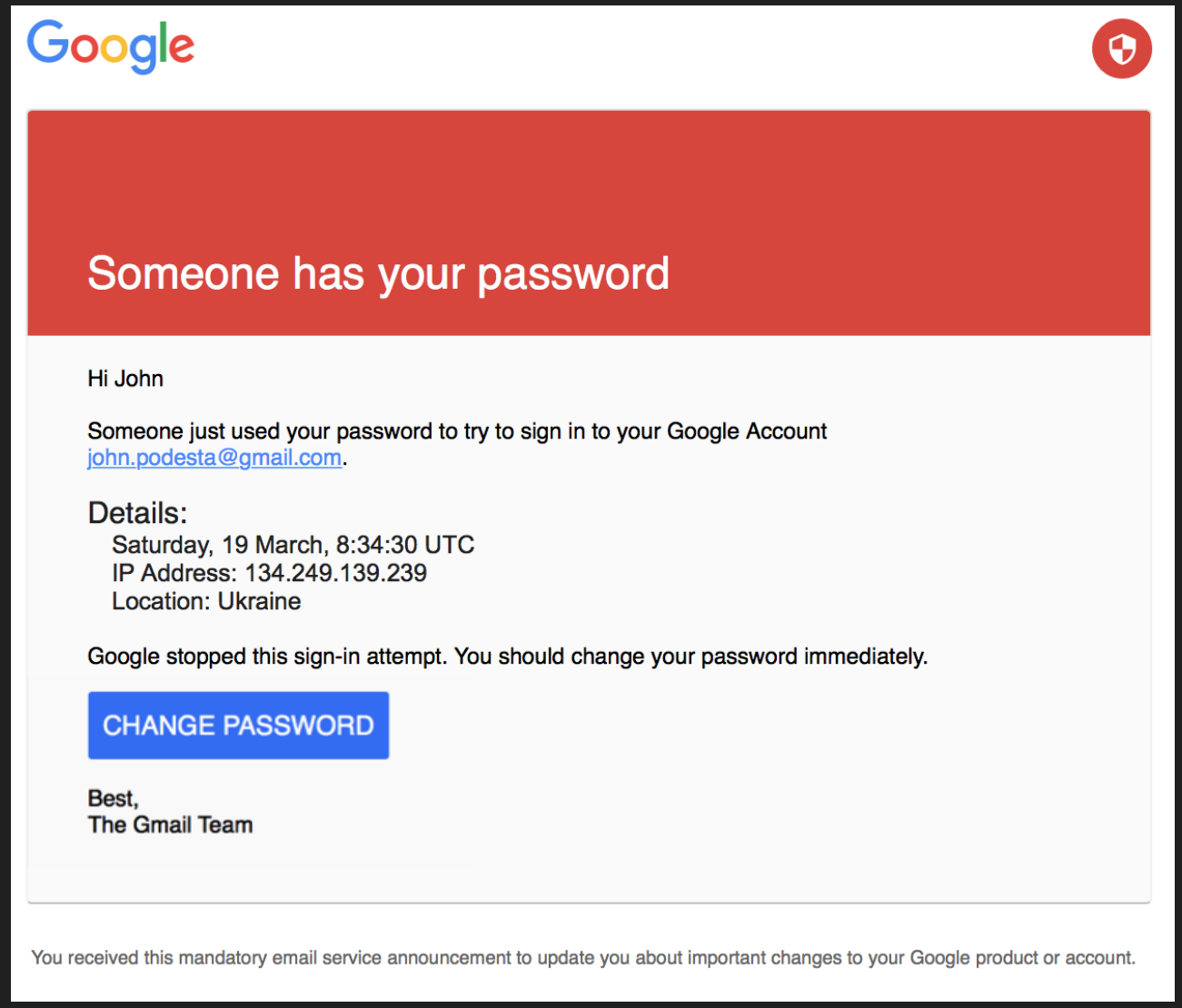
John Podesta

From Wikipedia, the free encyclopedia

John David Podesta (born January 8, 1949) is a columnist and former chairman of the 2016 Hillary Clinton presidential campaign.[1] He previously served as chief of staff to President Bill Clinton and Counselor to President Barack Obama.[2]

He is the former president, and now Chair and Counselor, of the Center for American Progress (CAP), a liberal think tank in Washington, D.C., as well as a Visiting Professor of Law at the Georgetown University Law Center. Additionally, he was a co-chairman of the Obama-Biden Transition Project.[3][4]

Anatomy of a Targeted Phishing Attack



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

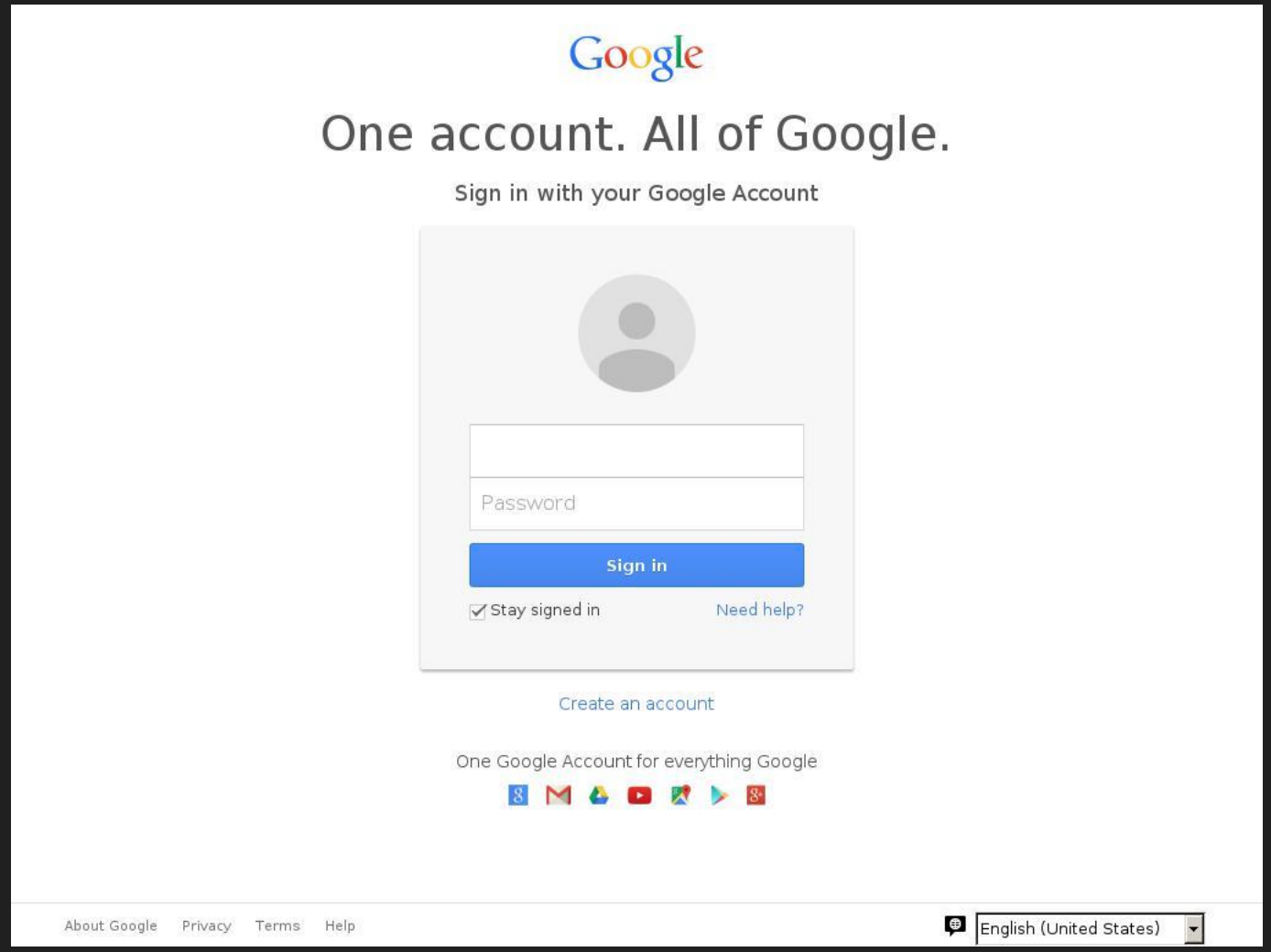
Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

- The branding looks consistent (Google logo, shield logo)
- The email is addressed to the recipient (not “Dear Sir”)
- The English is not broken

Anatomy of a Targeted Phishing Attack

Anatomy of a Targeted Phishing Attack



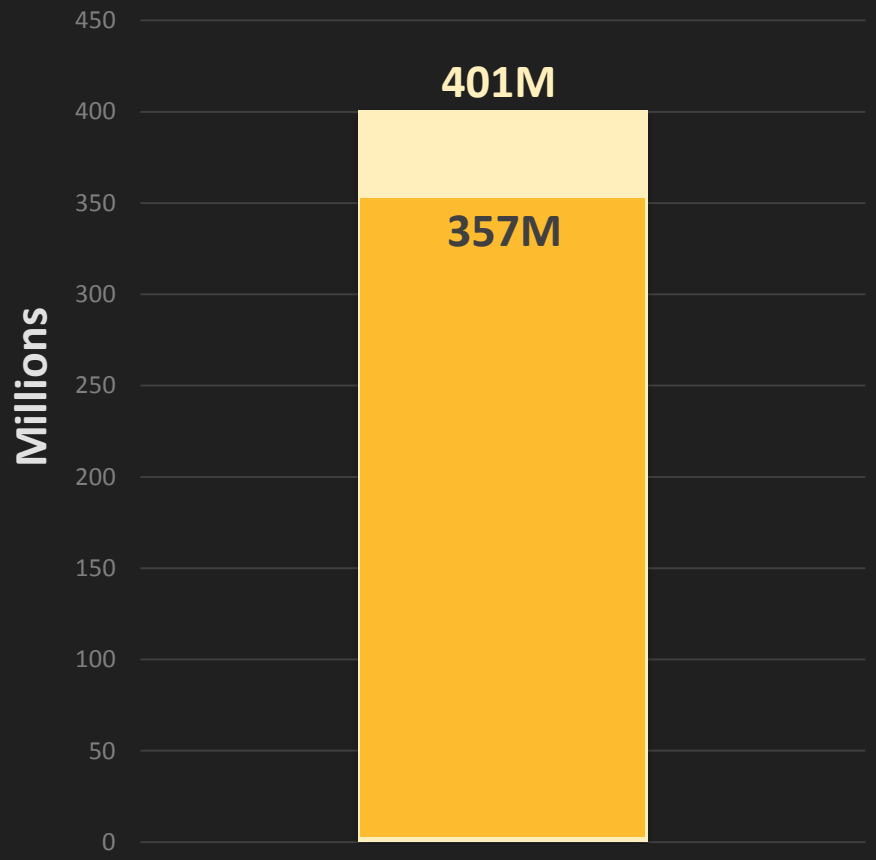
- The login page looks identical to the actual login page (HTML was cloned)
- Once the user submits the username/password combination, it doesn't matter what happens next
  - Typically, the phishing page redirects users back to Google.com

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this be done ASAP.

Two Factor Authentication Should Not Be An Option for Cloud Apps

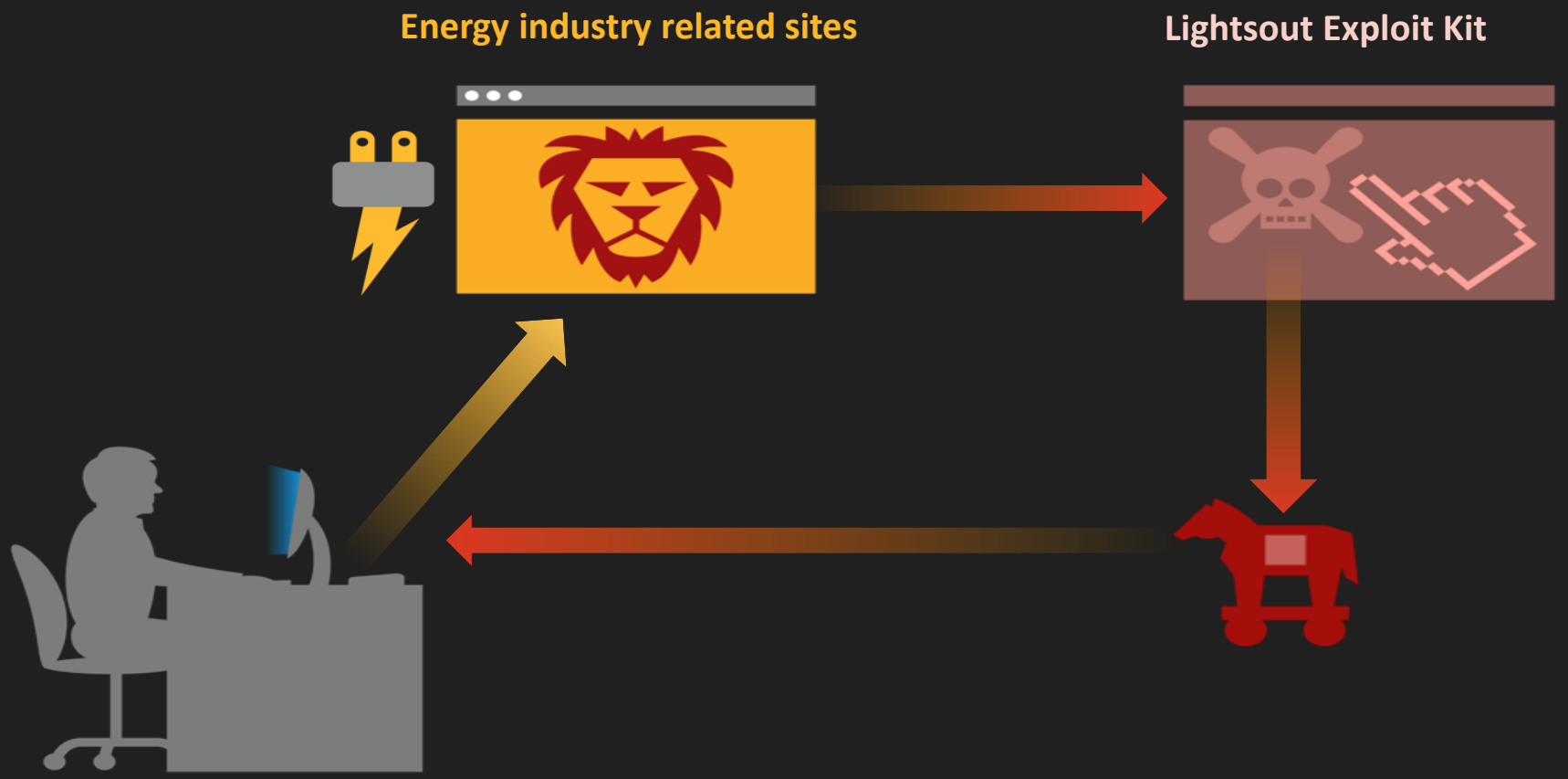
Unique Malware in 2016



401M Unique Pieces of Malware

- **89%** of that malware first seen in 2016
- **20%** of all malware VM aware
- **4%** use cloud services
- **3%** use SSL for C&Cs communication (79% increase)
- **1%** use Tor

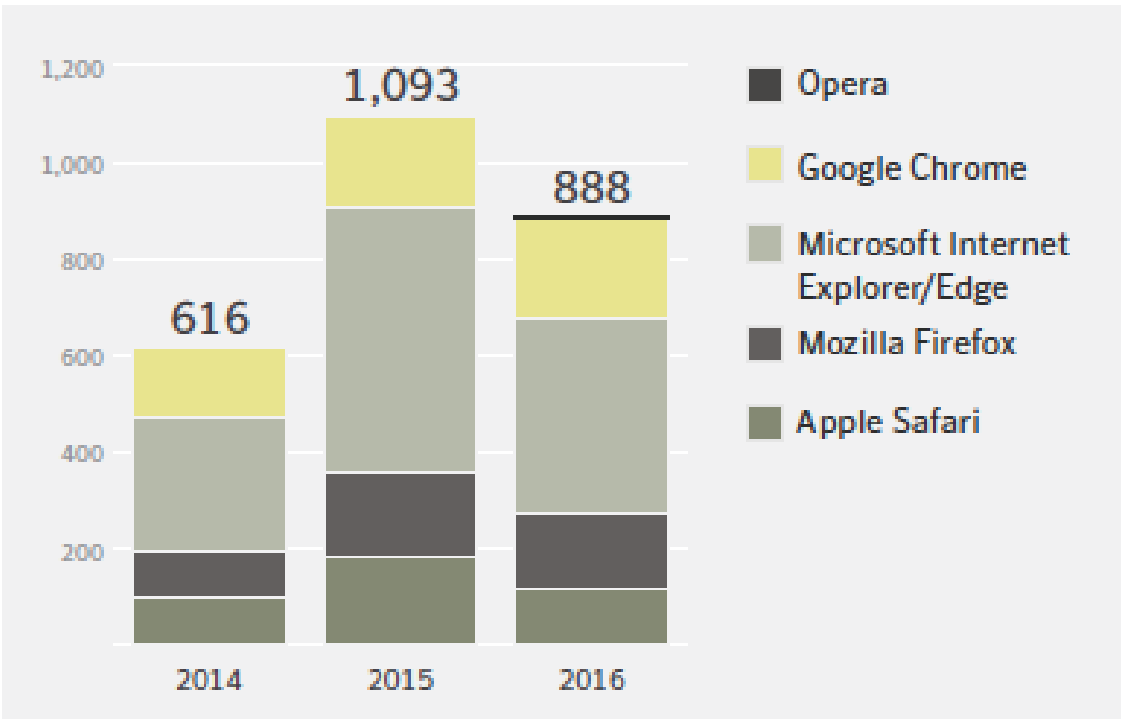
Waterhole attacks



Web attacks

Browser vulnerabilities

The number of browser vulnerabilities discovered dropped from 1,093 in 2015 to 888 in 2016.



What were the most frequently exploited websites?

Classification of most frequently exploited websites

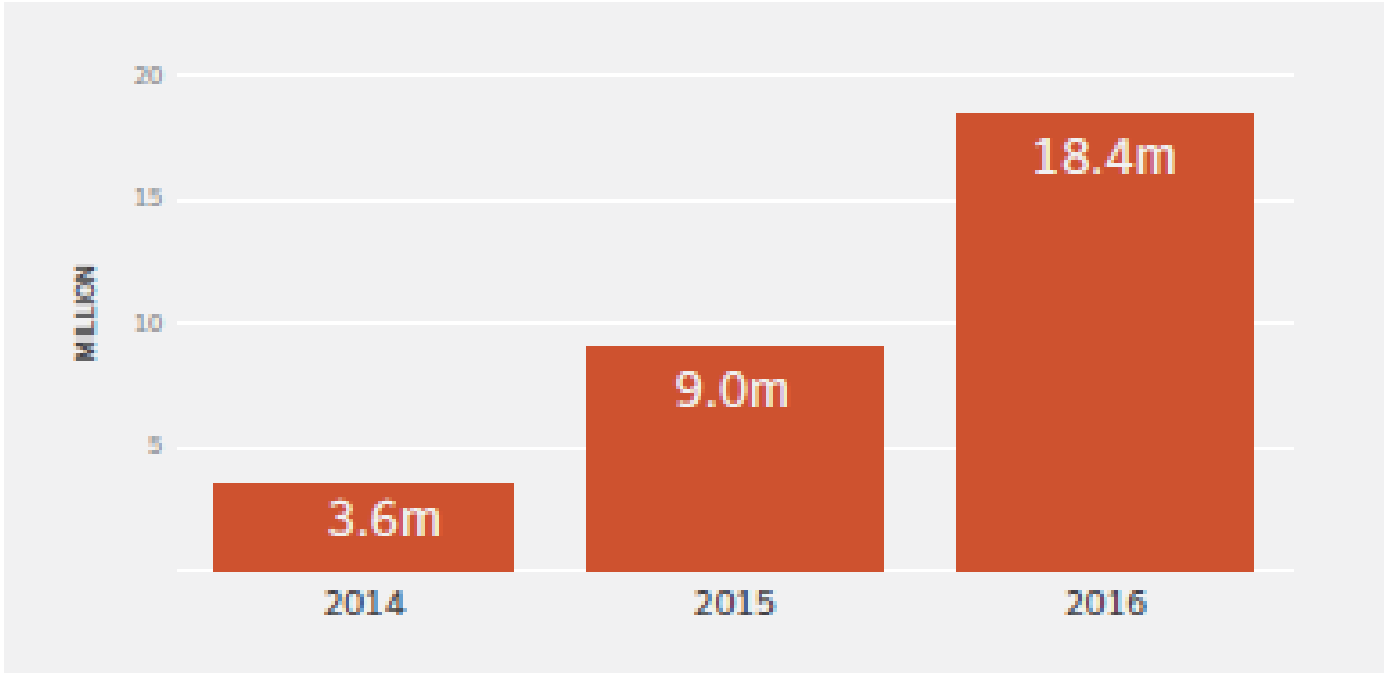
Technology- and business-related websites were the most popular for hosting malicious content and malvertising in 2016.

Rank	Domain Categories	2015 (%)	2016 (%)	Percentage Point Difference
1	Technology	23.2	20.7	-2.5
2	Business	8.1	11.3	3.2
3	Blogging	7.0	8.6	1.6
4	Hosting	0.6	7.2	6.6
5	Health	1.9	5.7	3.8
6	Shopping	2.4	4.2	1.8
7	Educational	4.0	4.1	< 0.1
8	Entertainment	2.6	4.0	1.4
9	Travel	1.5	3.6	2.1
10	Gambling	0.6	2.8	2.2

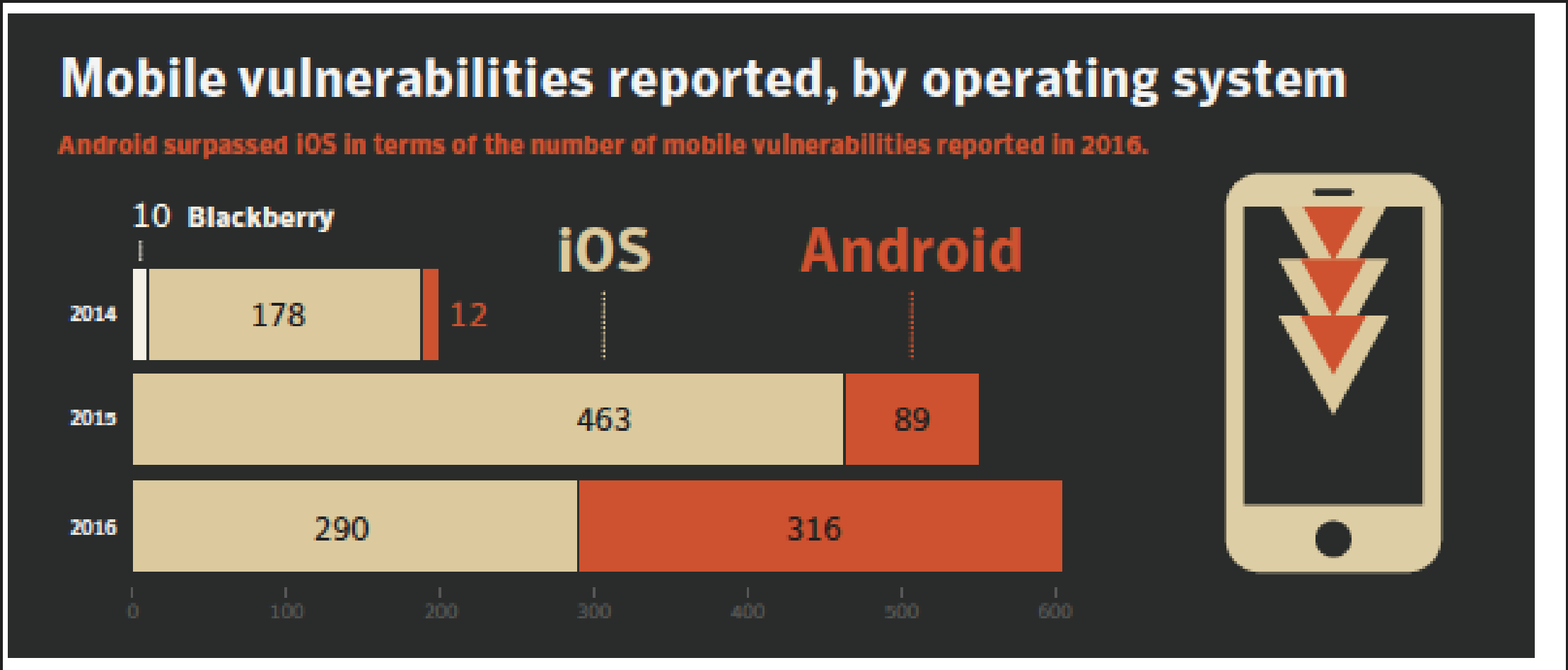
Mobile threats

Number of overall mobile malware detections per year

Symantec observed 18.4 million mobile malware detections in total in 2016, an increase of 105 percent on 2015.



Vulnerabilities per OS



In 2004 security researchers put a PC on the internet

- Without any patches installed
- Without any security software

It was attacked within

4 minutes

In 2016 Symantec researchers put an IoT device on the internet

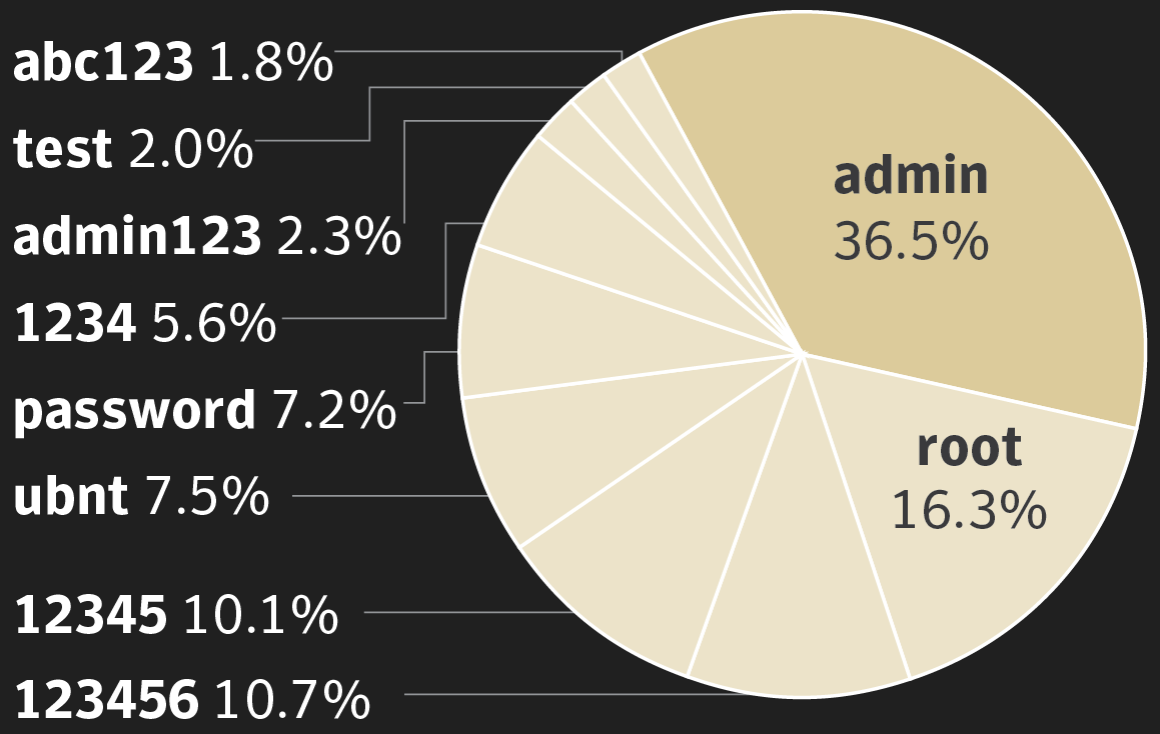
It was attacked within

2 minutes

The security shortcomings of IoT

- No system hardening
- No update mechanism
- Default/hardcodes passwords

Top 10 passwords used by malware to break into IoT devices



Data breaches – An overview – 15 mega breaches in 2016

Data breaches, 2014-2016

While the number of data breaches in 2016 remained fairly steady, the number of identities stolen increased significantly.

Year	Breaches	Identities stolen	Average per breach	Mega breaches
2014	1523	1,226,138,929	805,081	11
2015	1211	563,807,647	465,572	13
2016	1209	1,120,172,821	926,528	15

Cause of breach vs Effectiveness of cause (stolen identities)

Top 10 causes of data breaches in 2016

Theft of Data led the way as the main cause of data breaches in 2016, accounting for more than a third of breaches.

Rank	Cause	2015 (%)	2016 (%)	Percentage point difference
1	Theft of Data	42.4	36.2	-6.2
2	Improper Use of Data	20.4	19.3	-1.1
3	Unclassified or Other Cause	11.9	19.2	7.3
4	Phishing, Spoofing, or Social Engineering	21.8	15.8	-6.0
5	Accidental Data Loss	1.7	3.2	1.5
6	Loss or Theft of Device	0.6	3.1	2.5
7	IT Errors Leading to Data Loss	0.5	1.6	1.1
8	Network Disruption or DDoS	0.3	1.6	1.3
9	Extortion, Blackmail, or Disruption	0.1	0.2	0.1
10	Identity Theft or Fraud	0.1	0	-0.1

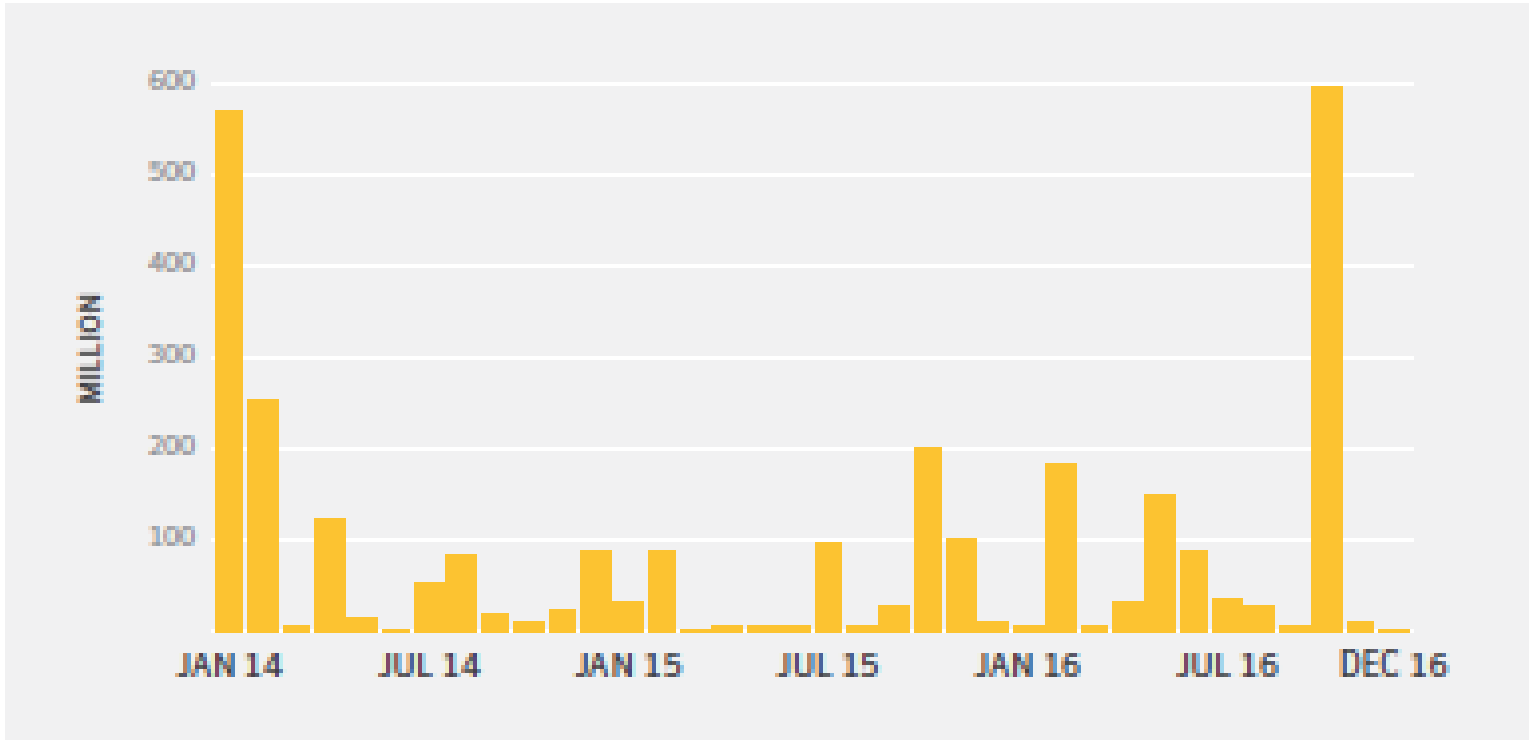
Top 10 causes of data breaches by identities stolen in 2016

Theft of Data was responsible for the vast majority of identities stolen in 2016.

Rank	Cause	2015 (%)	2016 (%)	Percentage point difference
1	Theft of Data	85.3	91.6	6.3
2	Phishing, Spoofing, or Social Engineering	9.8	6.4	-3.4
3	Accidental Data Loss	1.1	1.0	-0.1
4	IT Errors Leading to Data Loss	< 0.1	0.9	0.9
5	Network Disruption or DDoS	< 0.1	< 0.1	< 0.1
6	Improper Use of Data	3.3	< 0.1	-3.3
7	Loss or Theft of Device	< 0.1	< 0.1	< -0.1
8	Unclassified or Other Cause	0.4	< 0.1	-0.4
9	Extortion, Blackmail, or Disruption	< 0.1	< 0.1	< 0.1
10	Identity Theft or Fraud	< 0.1	0	< -0.1

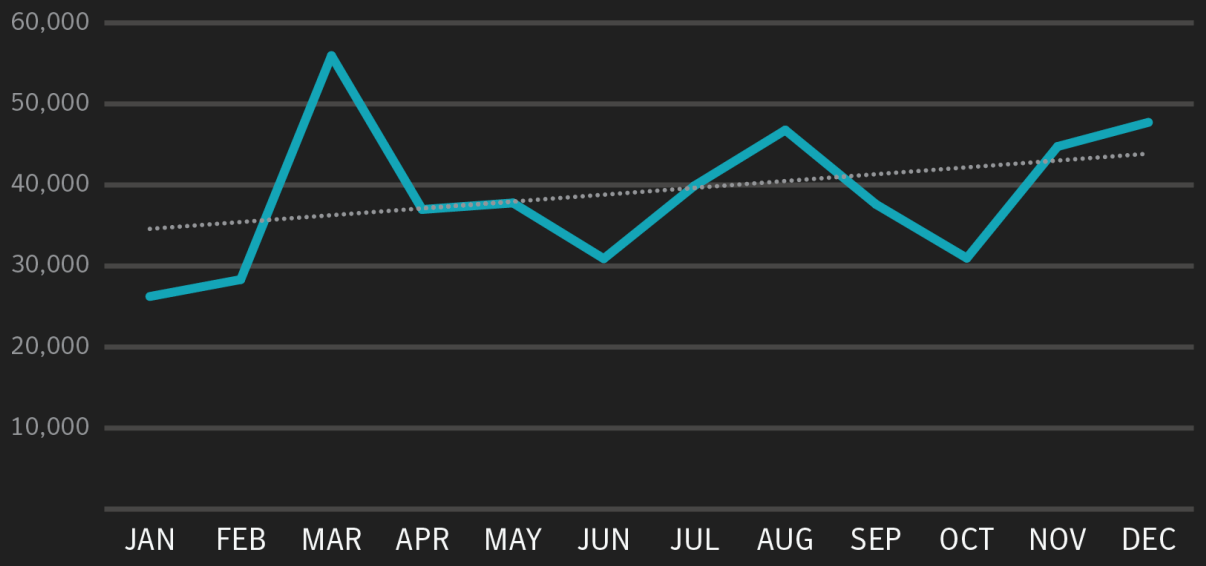
Identities stolen per month

There was a spike in identities stolen in October 2016, which was largely caused by a breach of Friend Finder Networks.

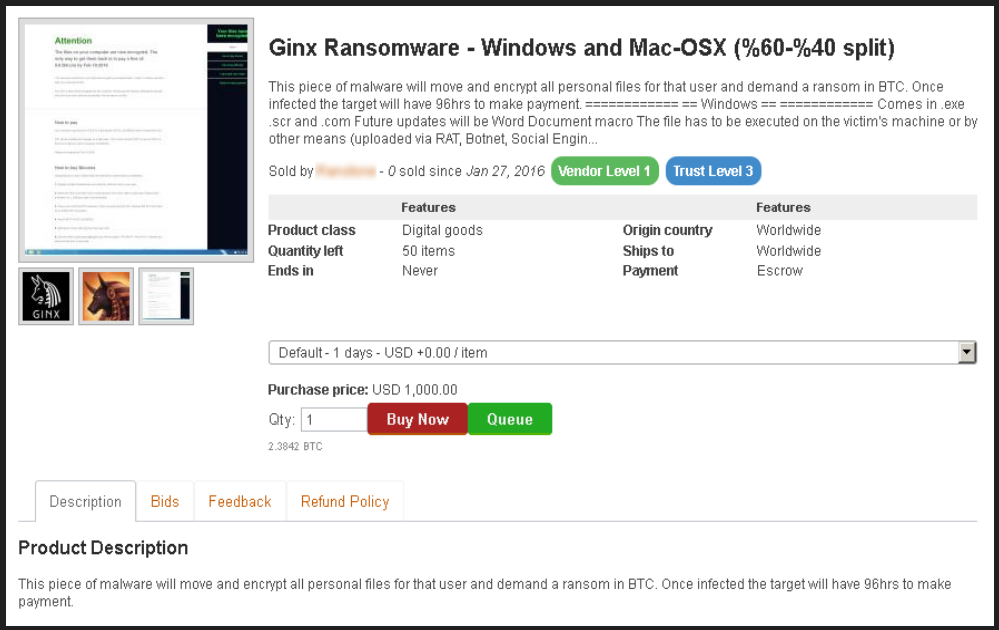


What you can buy in the underground economy at what price?

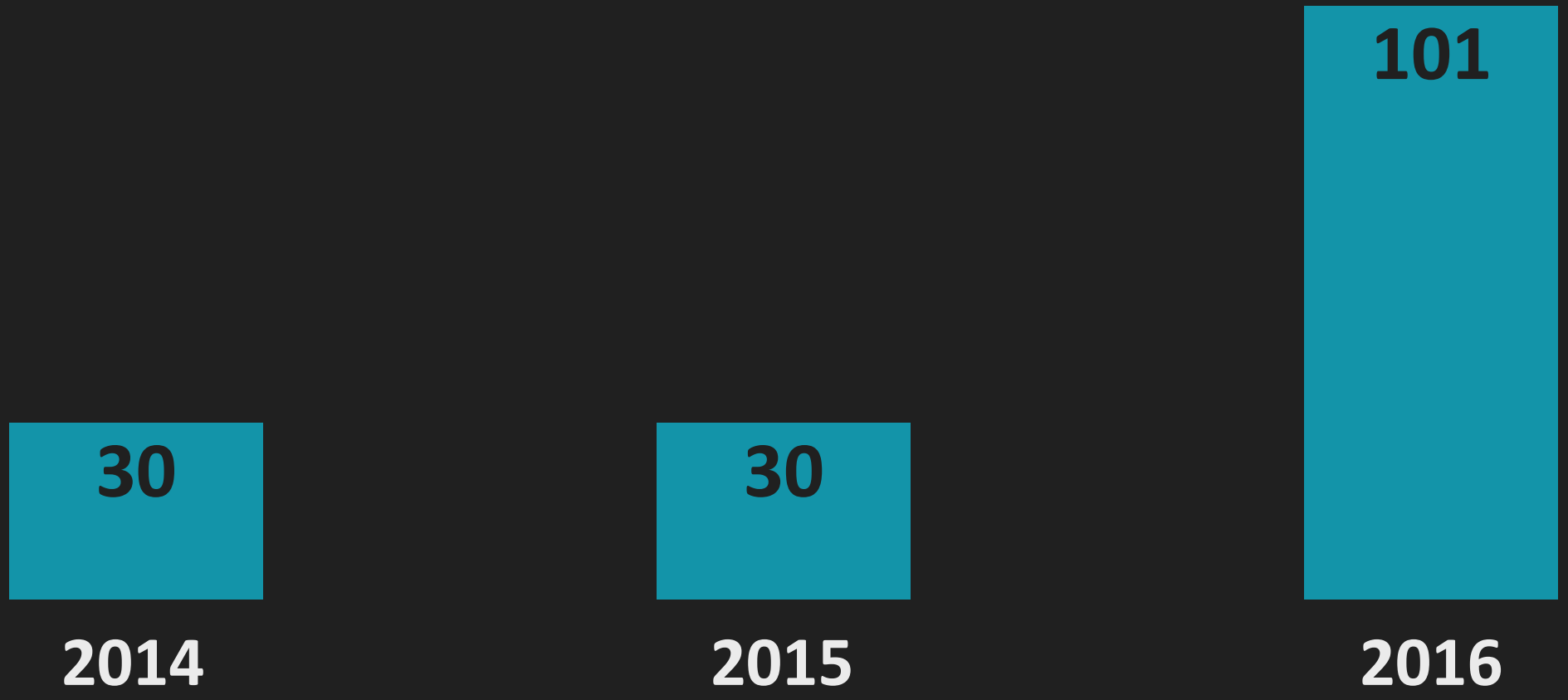
36% Increase in Ransomware Attacks



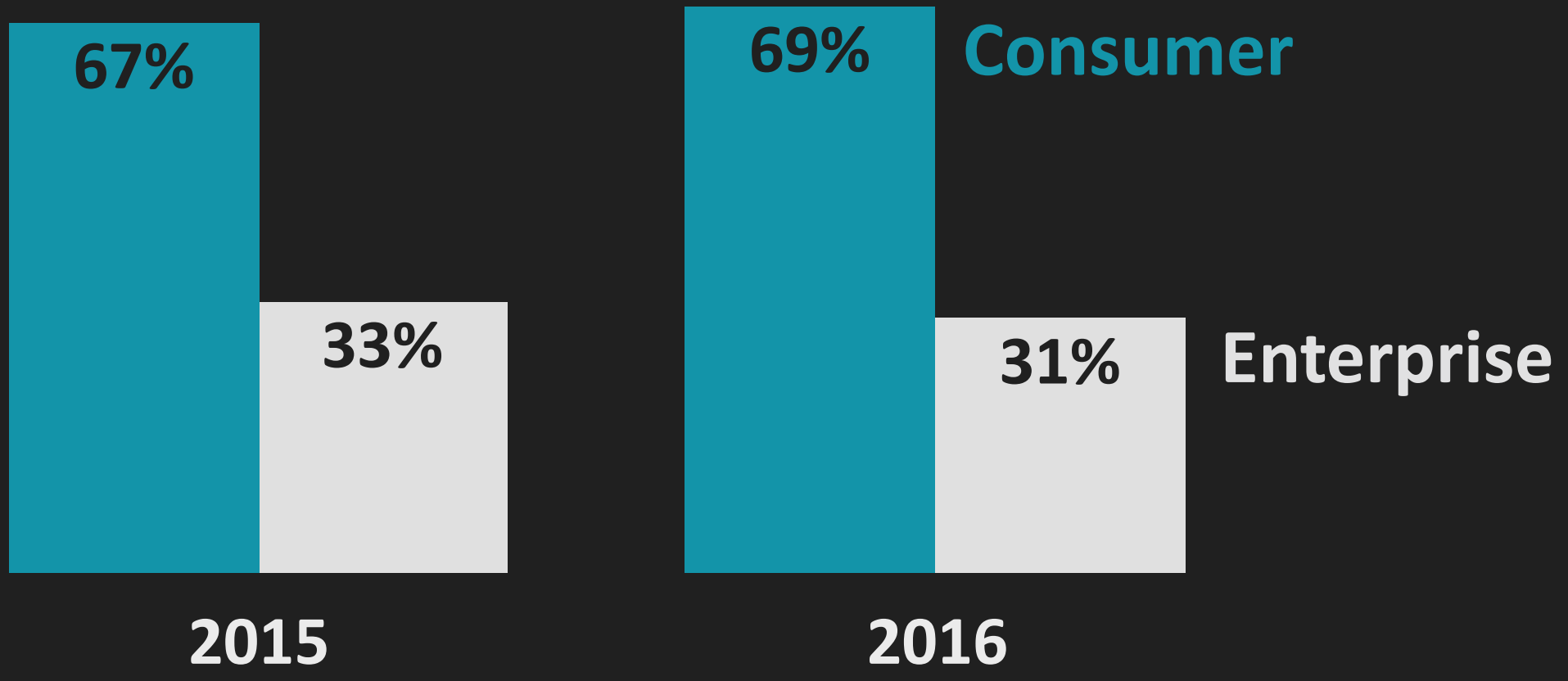
- Highly profitable
- Low Barrier to Entry
  - Multiple Software as a Service offerings available



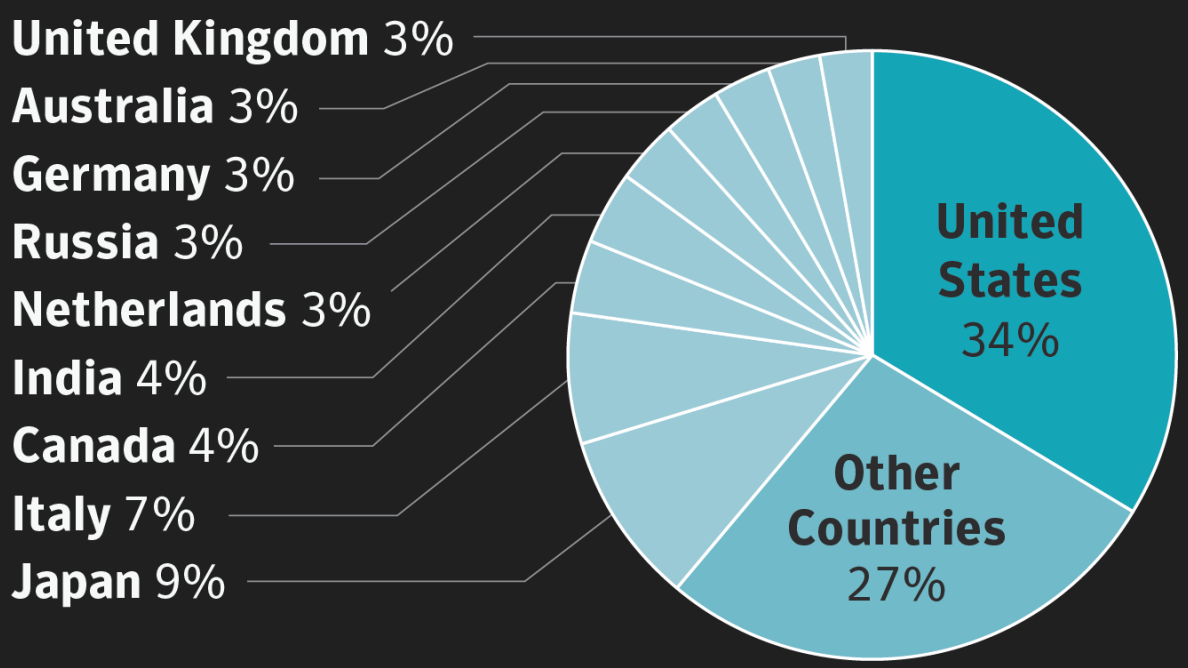
3x as many new ransomware families in 2016



Consumers Continue to see the Majority of Attacks

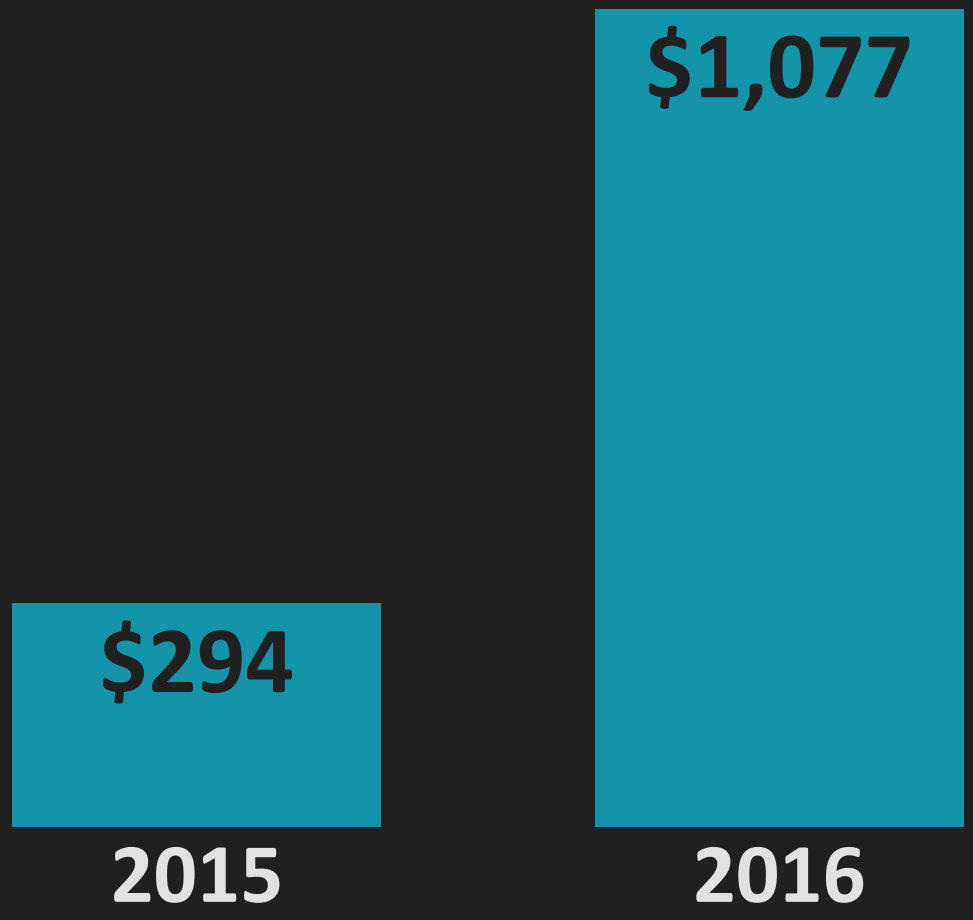


Ransomware Detections by Country



- With 34% of all attacks, US the region most affected by Ransomware
- Attackers target countries that can pay the largest ransom
- Number of internet connected computers also effect the numbers
- But US also has characteristic that is driving up the cost of the ransom

Average Ransom Demand



- The average starting ransom demand soared in 2016.
- Once infected many threats raise price if ransom not paid by deadline
- Some criminals will negotiate
- Targeted businesses will see higher demands
- Highest ransom demand for single machine seen in 2016 - $28,730 (Ransom.Mircop)

What is Driving Up the Ransom Demand?

Percentage of Consumers Who Pay Ransom

34%
Globally

- There does not appear to be price sensitivity among victims, especially in the US
  - As long as victims willing to pay, criminals can raise the price

64%
US

How is Ransomware Spreading

- **Secondary Infections** – infected machines download additional threat
- **Brute-force passwords** – ex. Ransom.Bucbi
- **Exploiting servers** – ex. Ransom.SamSam
- **Self-Propagation** – ex. W32.ZCrypt
- **3rd party app stores** – Android.Lockdrod.E
- **Social Networking** – ex. Locky
- **Exploit Kits** – 388k attacks blocked a day in 2016
- But mainly ransomware spreads via email

Best practices to protect yourselves

Internet Security Threat Report

ISTR

Volume

22

Thank You!

Symantec

VIGILO consult

Skimming and Malware (And a boilerroom)

Digital evidence

ERA Madrid
May 2016

Co-funded by the Justice
Programme of the European Union 2014-2020

Introduction

Me:

- Leiden University (eLaw)
- ISPA NL (ISPs)
- OPTA (Telecom regulator)
- VIGILO
  - EC, CoE, CRTC, BTPU, OFT, ACM (…)
  - Forensics, OSINT, Cybersecurity
  - Currently: Capacity building (ML, TF)

VIGILO consult

Program

- How to part consumers and businesses from money?
- Topics
  - Creditcards: card present (skimming)
  - Creditcards: card not present (malware)
  - Other options:
    - Boiler room and business email compromise frauds
    - Financial frauds in general
- ..And related digital evidence

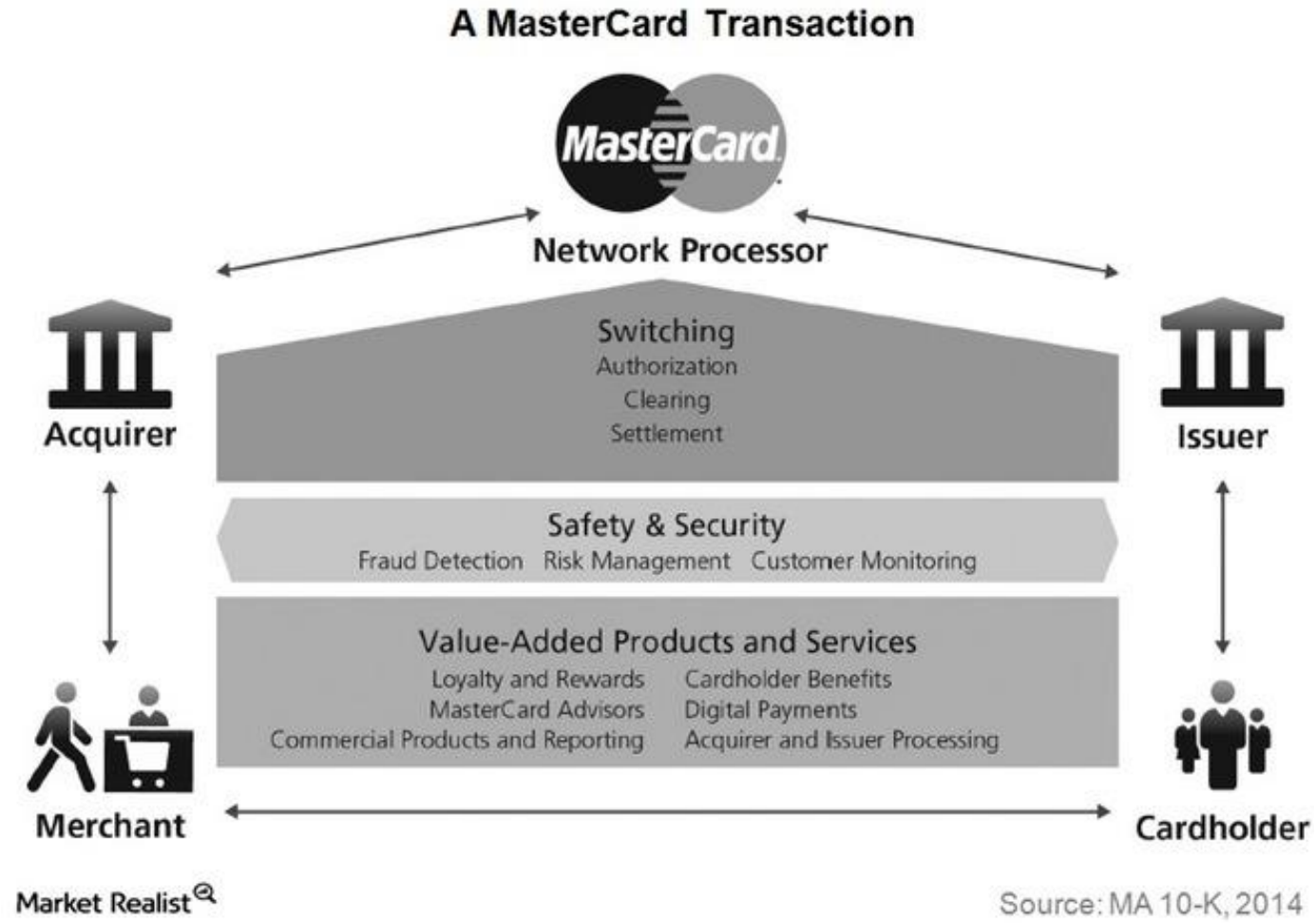
VIGILO consult

VIGILO consult

Card present (skimming)

Of strips and chips

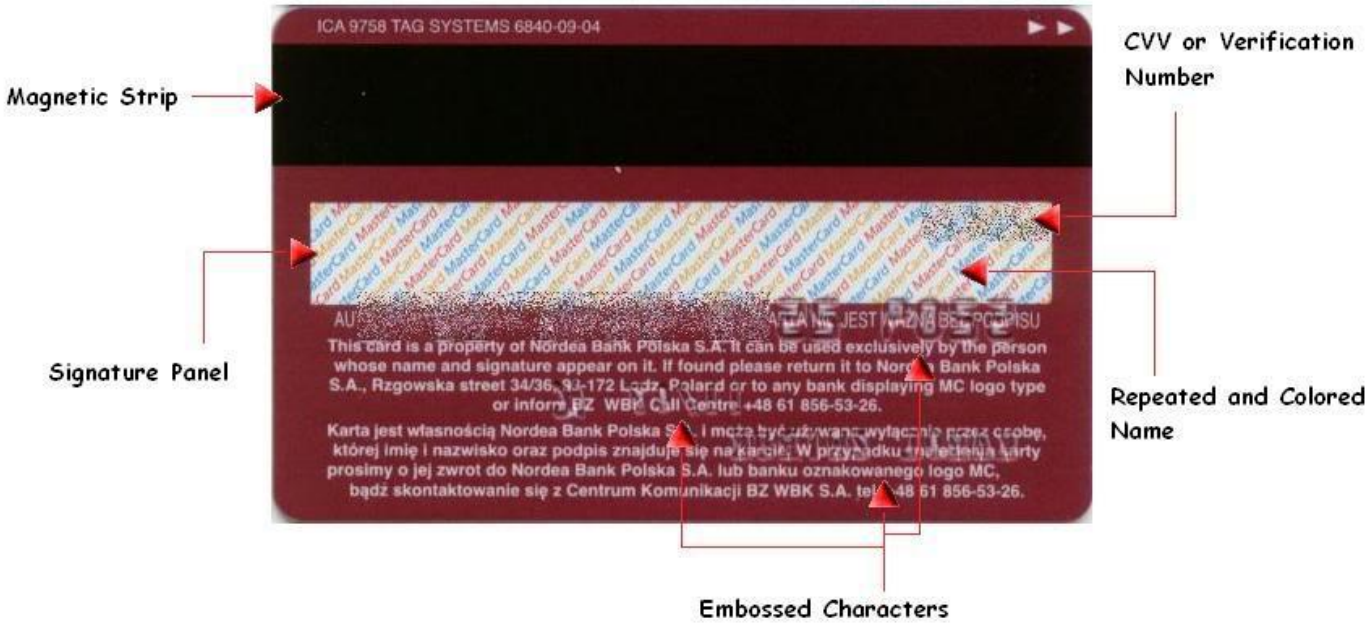
Overview



VIGILO consult

Creditcard

- What is on a creditcard?



VIGILO consult

Magnetic strip?

- Invented in 1969 by IBM, lead to ATM
- Universal System – but mostly banking and public transport
- Content is divided on tracks
  - Track 1: Name, BIN: (IIN and PAN), CVV, Exp.
  - Track 2: BIN, CVV Exp.
  - (..)
  - Discretionary data

VIGILO consult

Fraud (<2000)

- ATM: PIN
  - Issue: skimming
  - ATM: hard
- POS: Signatures
  - Cards stolen
  - Signatures forged (easy)
- Idea:
  - PIN
  - Plot spoiler: This backfired!

VIGILO consult

Why?

Fraud?

- Increase in card-present fraud (skimming)
- Use for card-not-present fraud (internet)
- Capture:
  - Stripe (CVV1, BIN)
  - PIN (camera or over te shoulder)
  - CVV2 (visual only)

VIGILO consult

Discretionary Data (→CVV)

- CVV/CVC (2 versions)
  - Not stored
  - Less vulnerable to database compromise
- CVV1/CVC1 (2001)
  - Present on stripe
  - Proves possession of card (in card present)
  - Skimming captures CVV1!
- CVV2/CVC2:
  - Different number on card (print) than on stripe
  - Differentiates card-present and card-not-present
  - Impossible to use stripe-skimmed CVV1 online

VIGILO consult

Skimming examples

So far

- Very insecure system!
- Based on offline and limited online verification
- Easy to defraud

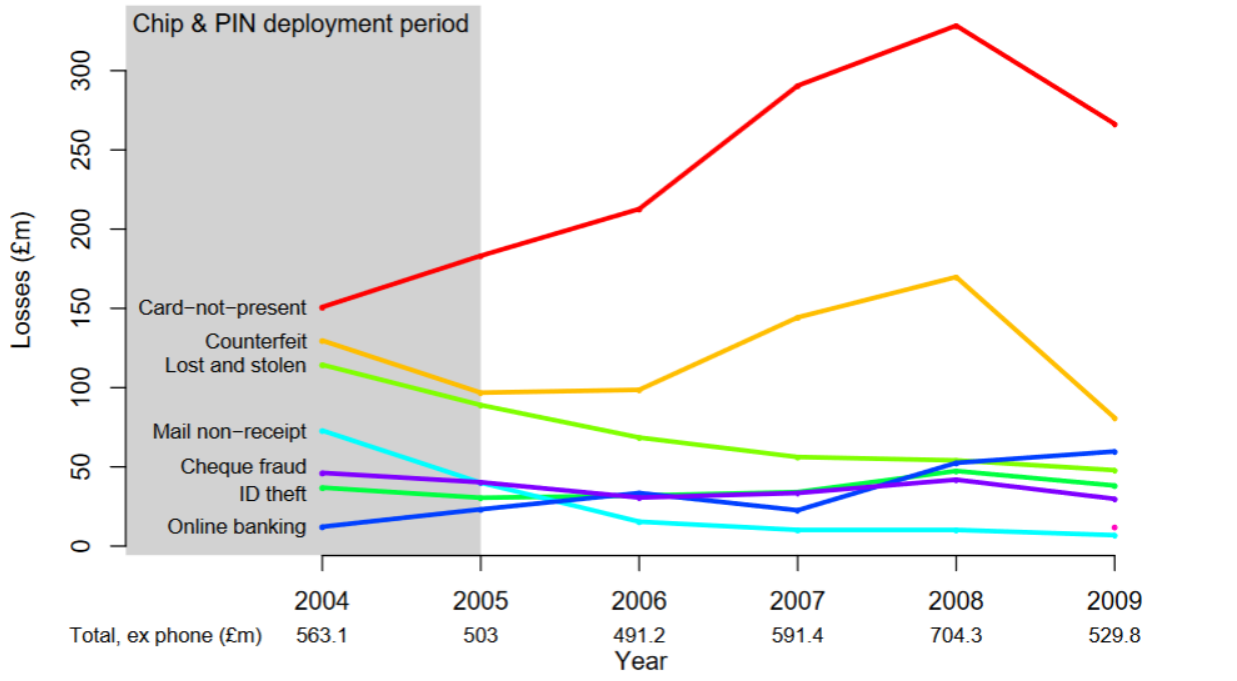
VIGILO consult

Issue

- Banks carry security risk, but…
- Customers
  - Limited liability with customers
  - Obligation to check statements, report fraud
- Merchants
  - Limited ability to prevent fraud
- Rationale: creditcard is a low transaction cost, high(er) fraud risk payment method.
  - Risk mainly at issuer/processor

VIGILO consult

Issue: rise of fraud, need for EMV



Source: UK Cards Association, 2010

VIGILO consult

EMV (chip&pin)

- Chip
  - Contains applications
  - Authentication
  - PIN (offline)
- Stripe retained for backward compatibility
  - Code on strip: chip present
  - Chip: used by default

VIGILO consult

Chip

- “Small computer”
- Can verify transaction
  - Online
  - Offline (limits)
- Can verify pin
- Used by default and strip has a “bit” that indicates chip is to be used
  - IF terminal has chip & stripe

VIGILO consult

Advantages

- Some processes take place on the chip: more secure
- Offline authentication and PIN verification
- Terminal authentication
- Chip can take base inputs, not easy to clone (plot spoiler: or so they thought)
- Offline transactions are more secure
- Use of PKI (public key crypto): secure
- Strip can be phased out

VIGILO consult


Mr. Bin
dumps store
Waar?
Europa
In Europa betalen en geld opnemen met uw Betaalpas(sen).
Wereld
Wereldwijd betalen en geld opnemen met uw Betaalpas(sen).
Welke landen vallen onder Europa? Bekijk de landenlijst 'Europa'.
Begindatum
22-03-2016
Einddatum
30-06-2016
Tip: houd bij het kiezen van een einddatum ook rekening met tijdsverschil en vertraging.
*its important to send selected bins in special format
*SAMPLE: 491204-7 or 510286=5 or 435098(2), etc.
*send ALL bins You need to buy in SAME mesage, plz
If bins not matter - You can request mix pack
Check price-list for price`s per 1pc/bulk/discounts
mrbin.cc
mrbin.tv
TOR: misterbin2usbole.onion
(please, save to Bookmarks)
Bonus pcs for feedback on forum
More questions?
Check FAQ page
with common answers
SIGN IN

Enter Cambridge

- Cambridge:
  - Man in the Middle
  - Card attached to a computer via wire
  - Allows attacker to type any PIN
  - Detectable by internal card counter value.
  - Detection delay (risk)
  - Practical?

VIGILO consult

MiTM attack on EMV

VIGILO consult

Digital evidence

VIGILO consult

Digital evidence

- Lists of creditcards (BIN lists)

VIGILO consult

VIGILO consult

Card not present

Malware

Malware

- Software
- Malicious
- Can go on many systems:
  - POS
  - End user PC/Laptop
- Capabilities:
  - MiTM

VIGILO consult

Example

11 Wendy's: Breach Affected 5% of Restaurants

MAY 16

Wen …nwide fast-f… 300 of the c… breach is con…

"Base… the in… the … instal… comp… crede… point of sale system at fewer than 300 of approximately 5,500 franchised North America Wendy's restaurants, starting in the fall of 2015." Wendy's

Banking Trojans

- Invade browser
- Capture credentials
- Trend: mobile (mTAN OTP)
  - Capture the login
  - Capture the One Time Password
  - Then execute transaction in background

VIGILO consult

FakeToken

VIGILO consult

VIGILO consult

BEC and boiler rooms

Bank robbery 2.0

BEC

- Business email compromise
- Latest trend
- Social engineering: pay into a bank account controlled by the criminals
- Issue:
  - Use of open source information
  - Often hacked email accounts used
  - Very convincing

VIGILO consult

BEC

- 4 phases:
  - Select target
  - Study/monitor/hack target
  - Social engineering
  - Exfiltration
- The latter is actually money laundering
  - Often: shell companies
  - Mules
  - Virtual currencies

VIGILO consult

Issue:

VIGILO consult

Reporting

- Often late (social engineering)
- Victims take time to get convinced (both ways)
- Detection is late
- Banks don't always detect or report
  - IBAN check?
- Use of time zones
- Many subjective indicators
  - Hiearchy, Urgency, Senior official

VIGILO consult

Main issue for evidence

- Spoofing:
  - Email
  - VOIP

VIGILO consult

Boiler room

- Use of call centers (outbound) for sale of risky financial products

VIGILO consult

Evidence

- Often not easy
- Requires advanced research onto connections between:
  - Financial institutions (follow the money)
  - Internet Services (comms, digital money)
  - Virtual currencies
  - International cooperation (FIU/MLA etc)

VIGILO consult

VIGILO consult

Conclusions

Legal issues

- CETS 185 (Budapest Convention)
  - Predicate offence of Computer related fraud and/or forgery
- CETS 198 (Warsaw Convention)
  - Proceeds (Freeze, Seize, Confiscate)
  - Money Laundering
- Various others
- Temporary measures
- Consumer protection vs. Risk Aversity

VIGILO consult

Conclusions

- EMV Broken?
  - Liability shift?
  - Redesign?
- End point security
  - Never perfect

VIGILO consult

Questions?

- Hein Dries
  - +31 71 7113243
  - hein@vigilo.nl

Technical means: give an example.. Non-technical means, for example. All: What could this be.

VIGILO consult