# Cyber-Crime, Dark Web

Paolo Falcarin

Ca' Foscari University of Venice

Department of Enviromental Sciences, Informatics and Statistics

**paolo.falcarin@unive.it**


CM0626 – Software Security

21 March 2025

# Cybercrime on TV

Ca' Foscari University of Venice

# Outline


Ca' Foscari University of Venice

- Famous Cyber-Attacks
- Advanced Persistent Threats (APTs)
  - APTs Groups
- Dark Web
- TOR (The Onion Router)

# Famous Cyber Attacks

# WannaCry

Ca' Foscari University of Venice

- WannaCry was a ransomware that exploited a vulnerability called Eternal Blue, developed by the US National Security Agency (NSA).
- In May 2017, WannaCry spread rapidly, infecting computers and encrypting files that could be decrypted with a $300 ransom.
- It was tentatively linked by Symantec and other researchers to the Lazarus Group, a cybercrime organization possibly connected to the North Korean government.
- Payment of the WannaCry ransom didn't usually result in one's files being decrypted…

https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

# Crash Override

Ca' Foscari University of Venice

- CRASHOVERRIDE caused power outages across Ukraine in 2016 and locked grid operators out of their own systems…
- During this attack, grid operators were forced to revert to analog operations and other stone age tools.

https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/

# Mirai

Ca' Foscari University of Venice

- In October 2016, the Mirai botnet leveraged insecure Internet of Things (IoT) devices to develop an army of bots for a distributed denial of service (DDoS) attack that caused an internet outage on US east coast.

https://krebsonsecurity.com/tag/mirai-botnet/
https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

# Stuxnet

Ca' Foscari University of Venice

- Stuxnet is a computer worm that was discovered in 2010 but likely developed around 2005 "*definitely not* by the United States and Israel".
- Stuxnet was successful in destroying centrifuges in Iran's Natanz uranium enrichment facility while also sending false feedback to operators
- All the while, there was no clear indication that the centrifuges had been destroyed before it was too late.

https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

# NotPetya

Ca' Foscari University of Venice

- NotPetya first targeted Linkos Group, a mom and pop Ukrainian software company, in June 2017 before going global.
- Small businesses and multinational corporations alike were paralyzed by the malware.
- NotPetya is considered to be the most expensive cyberattack, causing over $10 billion in damages.

- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/

# Sony Hack

Ca' Foscari University of Venice

- In November 2014, a group called the Guardians of Peace  (origins of the name remain unclear but what would one expect from North Korea?) took large amounts of private data off Sony's corporate network while also deleting the original files.
- The group leaked thousands of company documents and sensitive correspondence.

https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea
https://www.theguardian.com/film/2014/dec/10/sony-hack-eamils-angelina-jolie-scott-rudin-amy-pascal-david-fincher

# Conficker

Ca' Foscari University of Venice

- Conficker, first identified in 2008, is one of the older self-replicating cyberattacks.
- Conficker hardly caused any damage, since it was developed at a time when malware was primarily used to infect as many devices as possible instead of revenue generation.
- As it relies on infecting unsupported, unpatched legacy systems, it still shows up now and again.
- All in all, harmless but still cringe -worthy.

https://www.cyberscoop.com/conficker-trend-micro-2017/

# Plum Island Black Start

Ca' Foscari University of Venice

- This was in fact part of a 2018 Defense Advanced Research Projects Agency (DARPA) exercise in Plum Island, New York.
- Two electric utilities worked to defend a grid from a red team and the objective was to defend and maintain power to a building deemed a critical asset.
- This attempted relationship (and the DARPA exercise) tested how researchers and grid operators could prepare for, and respond to something devastating—and still fail.

https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/

# OPM Breach

Ca' Foscari University of Venice

- In 2015, Chinese hackers breached the Office of Personnel Management (OPM) and the personal data of approximately 22 million people was compromised.
- These data included financial records and even fingerprints, but no evidence suggests that the data from the breach has been leveraged financially.

https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html

# ShadowPad backdoor

Ca' Foscari University of Venice

- A backdoor planted in a server management software product used by hundreds of large businesses around the world.
  - When activated, the backdoor allows attackers to download further malicious modules or steal data
  - NetSarang, the software provider in Honk Kong, was able to fix it immediately
- It is one of the largest known supply-chain attacks
  - It could potentially have targeted hundreds of organizations worldwide.
- The malicious module has been activated in Hong Kong, but it could be lying dormant on many other systems worldwide

https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

# Cybercrime

Ca' Foscari University of Venice

- Monitor Threat Landscape
- https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it

# Advanced Persistent Threat

# Advanced Persistent Threat (APT)


Ca' Foscari University of Venice

- An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.
- The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks.
- The consequences of such intrusions are vast, and include:
  - Intellectual property theft (e.g., trade secrets or patents)
  - Compromised sensitive information (e.g., employee and user private data)
  - The sabotaging of critical organizational infrastructures (e.g., database deletion)
  - Total site takeovers

# Advanced Persistent Threat (APT)

Ca' Foscari University of Venice

- Executing an APT assault requires more resources than a standard web application attack.
- The perpetrators are usually teams of experienced cybercriminals having substantial financial backing.
- Some APT attacks are government-funded and used as cyber warfare weapons.

# APT Attacks

Ca' Foscari University of Venice

- APT attacks differ from traditional web application threats:
  - They're significantly more complex.
  - They're not hit and run attacks—once a network is infiltrated, the perpetrator remains in order to get as much information as possible.
  - They're manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets.
  - They often aim to infiltrate an entire network, as opposed to one specific part.

# APT Attacks

Ca' Foscari University of Venice

- More common attacks, such as remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), are frequently used by offenders to establish a foothold in a targeted network.
- Next, Trojans and backdoor shells are often used to expand that foothold and create a persistent presence within the targeted perimeter.

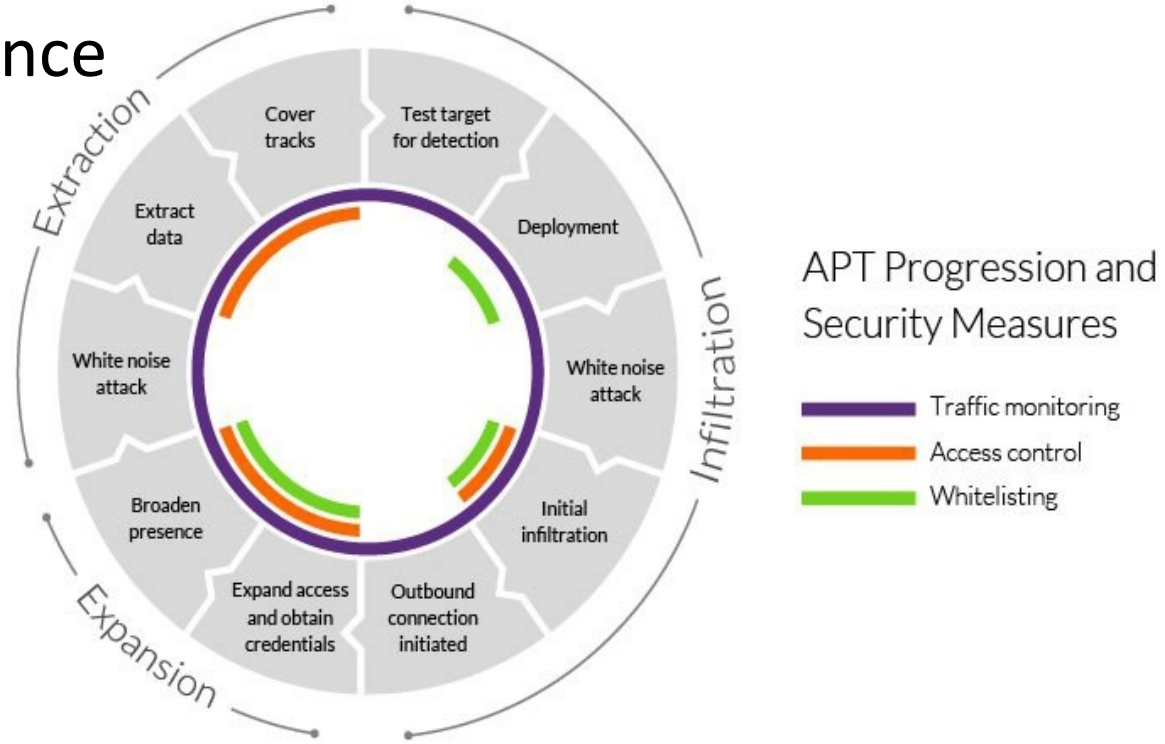
# APT Attack

Ca' Foscari University of Venice

A successful APT attack can be broken down into three stages:

1) network infiltration
2) the expansion of the attacker's presence
3) the extraction of amassed data

All without being detected.



# Stage 1 - Infiltration

Ca' Foscari University of Venice

- Enterprises are typically infiltrated through the compromising of one of three attack surfaces: web assets, network resources or authorized human users.
- This is achieved either through malicious uploads (e.g., RFI, SQL injection) or social engineering attacks (e.g., spear phishing)—threats faced by large organizations on a regular basis.
- Additionally, infiltrators may simultaneously execute a DDoS attack against their target. This serves both as a smoke screen to distract network personnel and as a means of weakening a security perimeter, making it easier to breach.
- Once initial access has been achieved, attackers quickly install a backdoor shell—malware that grants network access and allows for remote, stealth operations.
- Backdoors can also come in the form of Trojans masked as legitimate pieces of software.

# Stage 2 - Expansion

Ca' Foscari University of Venice

- After the foothold is established, attackers move to broaden their presence within the network.
- This involves moving up an organization's hierarchy, compromising staff members with access to the most sensitive data.
  - to gather critical business information, including product line information, employee data and financial records.
- Depending on the ultimate attack goal, the accumulated data can be sold to a competing enterprise, altered to sabotage a company's product line or used to take down an entire organization.
- If sabotage is the motive, this phase is used to subtly gain control of multiple critical functions and manipulate them in a specific sequence to cause maximum damage.
  - For example, attackers could delete entire databases within a company and then disrupt network communications in order to prolong the recovery process.

# Stage 3 - Extraction

Ca' Foscari University of Venice

- While an APT event is underway, stolen information is typically stored in a secure location inside the network being assaulted.
- Once enough data has been collected, the thieves need to extract it without being detected.
- Typically, white noise tactics are used to distract your security team so the information can be moved out.
- This might take the form of a DDoS attack, again tying up network personnel and/or weakening site defences to facilitate extraction.

# APT Security Measures

Ca' Foscari University of Venice

- Proper APT detection and protection requires a multi-faceted approach on the part of network administrators, security providers and individual users.
- Traffic Monitoring
- Application and domain whitelisting
- Access Control
- Additional Measures

# Traffic Monitoring

Ca' Foscari University of Venice

- Best practice for preventing the installation of backdoors and blocking stolen data extraction.
- Inspecting traffic inside your network perimeter => help alert security personnel to any unusual behaviour / malicious activity.
- A web application firewall (WAF) filters traffic to your web application servers – the most vulnerable attack surfaces.
  - WAF can help weed out application layer attacks, such as RFI and SQL injection attacks, used during the APT infiltration phase
- Remote file inclusion (RFI) is an attack targeting vulnerabilities in web applications that dynamically reference external scripts.
  - Their goal is to exploit the referencing function in an application to upload malware (e.g., backdoor shells) from a remote URL located within a different domain.

# Traffic Monitoring

Ca' Foscari University of Venice

- Internal traffic monitoring services can provide a granular view showing how users are interacting within your network
  - help to identify internal traffic abnormalities
    - irregular logins
    - unusually large data transfers => APT attack is taking place
    - monitor access to file shares or system honeypots.
- Incoming traffic monitoring services could be useful for detecting and removing backdoor shells.
  - Identified by intercepting remote requests from the operators

# Application and Domain Whitelisting


Ca' Foscari University of Venice

- Whitelisting is a way of controlling domains that can be accessed from your network, as well as applications that can be installed by your users.
  - Reducing the success rate of APT attacks by minimizing available attack surfaces
- However, even the most trusted domains can be compromised.
- Malicious files commonly arrive under the guise of legitimate software.
- Older software product versions are prone to being compromised and exploited.
- For effective whitelisting, strict update policies should be enforced to ensure your users are always running the latest version of any application appearing on the list.

# Access Control

Ca' Foscari University of Venice

- Employees are the largest and most vulnerable soft-spot in the security perimeter.
  - Careless users who ignore network security policies and unknowingly grant access to potential threats.
  - Malicious insiders who intentionally abuse their user credentials to grant perpetrator access.
  - Compromised users whose network access privileges are compromised and used by attackers.
- Classifying data on a need-to-know basis helps block an intruder's ability to hijack login credentials from a low-level staff member, using it to access sensitive materials.
- Key network access points should be secured with two-factor authentication (2FA).
  - Second form of verification when accessing sensitive areas (typically a passcode sent to the user's mobile device).
  - Prevent unauthorized actors disguised as legitimate users from moving around your network

# Additional Measures



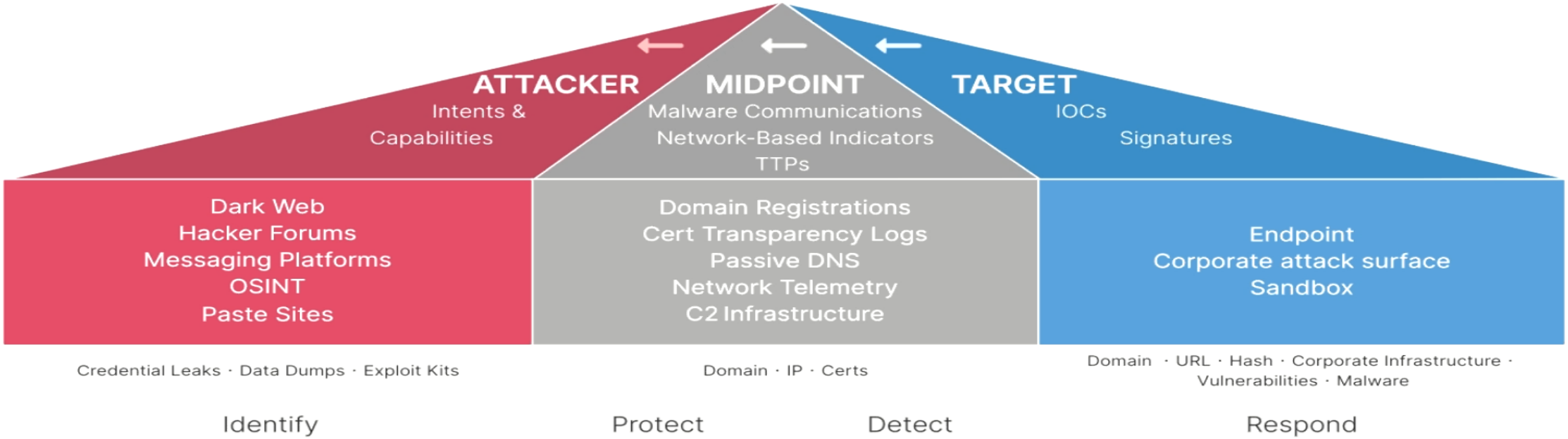
- Patching network software and OS vulnerabilities as quickly as possible.
- Encryption of remote connections to prevent intruders from piggy-backing them to infiltrate your site.
- Filtering incoming emails to prevent spam and phishing attacks targeting your network.
- Immediate logging of security events to help improve whitelists and other security policies.

# Threat Intelligence

Ca' Foscari University of Venice

## End-to-End View of Threats

*Visibility From Attackers Through Midpoint to Targets*




Recorded Future

# APT Groups

# Cobalt Spider

Ca' Foscari University of Venice

- Cobalt Spider (also known as Cobalt Gang), a financially motivated criminal group that has targeted financial institutions in Russia, Central Asia, and Eastern Europe.
- Cobalt Spider sends spear-phishing emails that attack corporations and generate revenue—and infamy—by compelling ATMs to spit out money.

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-september-cobalt-spider/

# Cozy Bear

Ca' Foscari University of Venice

- Cozy Bear (aka APT 29), linked to the Russian Foreign Intelligence Service, is similarly known for its flexibility and ability to adapt its toolset to different realms.
- This APT casts a wide net in its attacks, sending phishing emails to thousands of targets, including US think tanks, NGOs, and foreign governments.
- Cozy Bear has seen great success by sending emails containing Super Bowl ads and links to videos on "YovTube.com," and played an active role in the 2016 DNC hack.

https://www.crowdstrike.com/blog/who-is-cozy-bear/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

# Fancy Bear

Ca' Foscari University of Venice

- Fancy Bear  (APT 28) seeks with panache to sow discord and intimidate those perceived as hostile to Russian interests.
- Believed to be affiliated with Russia's military intelligence unit (GRU), Fancy Bear was responsible for several high-profile attacks, including the 2016 hacking of the US Democratic National Committee and the targeting of the 2017 French election.
- Fancy Bear is known for engaging in extensive reconnaissance operations against its targets, even sifting through their social media and LinkedIn profiles in order to customize attacks on governments and political organizations around the world.
- Fancy Bear uses cheap, unsophisticated techniques to penetrate high-profile targets

https://www.forbes.com/sites/kateoflahertyuk/2018/08/23/midterm-election-hacking-who-is-fancy-bear/#31dfc3942325
https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/
https://www.vice.com/en/article/ez35p7/russian-hackers-fancy-bear-targeted-french-presidential-candidate-macron

# Venomous Bear

Ca' Foscari University of Venice

- Venomous Bear (sometimes called Turla) is a Russia-based APT employing novel and complex tools (e.g. trojanised software, infection of removable storage devices), supported by a network of sophisticated signals intelligence (SIGINT) capabilities.
- Venomous Bear is believed to have launched increasingly sophisticated attacks against targets in the government, aerospace, NGO, defence, cryptology, and education sectors.
- Such a broad portfolio of targets highlights Venomous Bear's overachieving nature…which probably makes it unpopular among its Russian APT peers.

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/

# Voodoo Bear (Sandworm)

Ca' Foscari University of Venice

- Voodoo Bear, also known as Sandworm, which has employed tools to manipulate energy industrial control systems (ICS) and supervisory control and data acquisition (SCADA).
- Believed to be behind the 2015 power outages in Ukraine, Voodoo Bear leverages zero-day vulnerabilities to target Ukrainian organizations.

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/

https://www.wired.com/story/sandworm-russia-cyberattack-links/

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

# Wicked Spider

Ca' Foscari University of Venice

- Wicked Spider, also known as Winnti Group or Wicked Panda. Wicked Spider is believed to be a China-based criminal group whose members also serve as hackers for hire.
- This APT accordingly specializes in financially motivated activity
- It is also contracting out its services for targeted intrusion operations against organizations in the engineering, manufacturing, and technology  sectors on behalf of the Chinese government.
- Chinese economic espionage

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/

# Mustang Panda

Ca' Foscari University of Venice

- Mustang Panda, an APT that often targets NGOs, US-based think tanks, and minority groups in China for intelligence collection.
- Mustang Panda has demonstrated an ability to rapidly assimilate new strategies into its operations and even mix malware with legitimate tools.
- It has recently focused on accessing the communications of the Vatican.

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

https://www.cybersecurity-help.cz/blog/1774.html

# Standard Chollima

Ca' Foscari University of Venice

- Stardust Chollima (aka APT 38), known for its intense focus on revenue generation.
- This cyber APT is associated with the Democratic People's Republic of Korea and procures liquid funds for the North Korean regime.
- Stardust Chollima's operations are characterized by long timelines and carefully executed attacks.
- Cash rules everything around Stardust Chollima.

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/

# Mythic Leopard

Ca' Foscari University of Venice

- Pakistan-based Mythic Leopard is skilled in sensing and manipulating the relationships of its targets and seeks to create a geopolitical power balance with Pakistan's rival India.
- This espionage group uses social engineering and spear-phishing to target Indian military and defence entities, though its attacks demonstrate low technical sophistication.
- During the pandemic, this group used a decoy health advisory to spread the Crimson RAT (remote administration tool) malware in India.

https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/

https://www.scmagazine.com/home/security-news/cybercrime/foreign-apt-groups-use-coronavirus-phishing-lures-to-drop-rat-malware/

# Refined Kitten (APT 33)

Ca' Foscari University of Venice

- Refined Kitten (aka APT 33 or Elfin)—with likely ties to Iran's Islamic Revolutionary Guard Corps—executes carefully planned espionage operations against Iranian state adversaries in Saudi Arabia, the UAE, and the United States.
- The group is also suspected of having been involved in the destructive Shamoon malware attacks against Saudi Arabia, displaying its desire for vengeance.
- In the case of a future clash between the United States and Iran, American companies may find traces of this APT's persistent and strategic footprints (or pawprints ☺ ) across their networks.

https://www.crowdstrike.com/blog/who-is-refined-kitten/

https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/

# Charming Kitten

Ca' Foscari University of Venice

- Charming Kitten (APT35 or Phosphorus), an Iranian espionage group that targets political dissidents, human rights activists, academics, journalists, and other threats to authoritarianism.
- Charming Kitten specifically leverages its targets' social networks, to collect information before breaching their accounts.

https://attack.mitre.org/groups/G0058/

https://www.clearskysec.com/charmingkitten/

# Helix Kitten

Ca' Foscari University of Venice

- Helix Kitten (also known as APT 35 or OilRig) is a skilled navigator of vast online networks, moving across an array of organizations
  - aerospace, energy, finance, government, hospitality, and telecommunications.
- Helix Kitten has a consistent track record of developing meticulous spear-phishing attacks.

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

# RedFoxtrot

Ca' Foscari University of Venice

- Group linked to Chinese Military Intelligence, active since 2014
- Links found between them and People Liberation Army (PLA) Unit 69010 located in Urumqi, Xinjiang
- RedFoxtrot intrusions identified targeting defence, military, government, and telecommunications in South and Central Asia
- Activity undermines China's claims of innocence and status as a "victim of cyber aggression"….

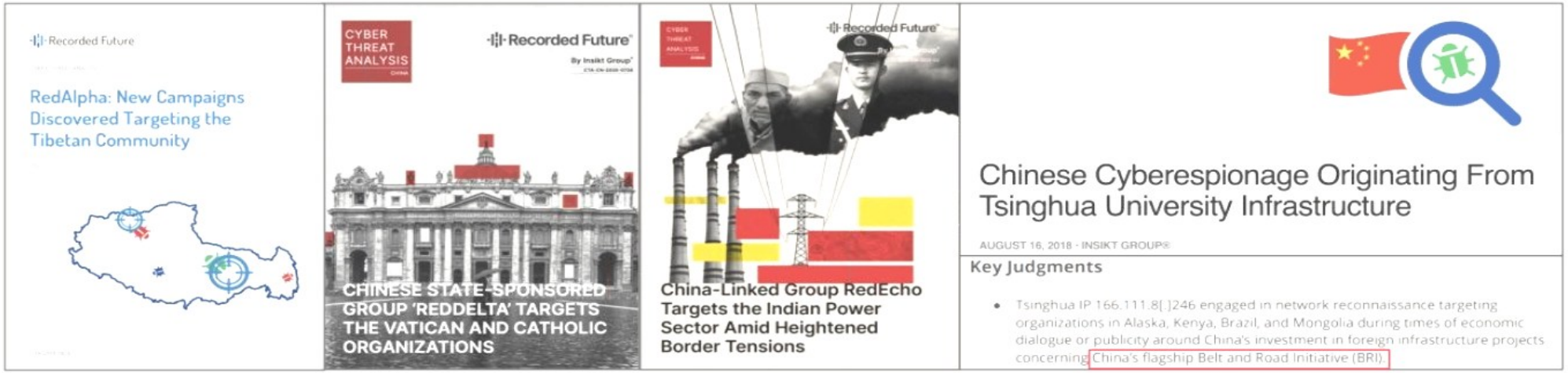

Source: Radio Free Asia

Image: Entrance to PLA Unit 69010 compound in Urumqi

# Chinese Espionage

RedAlpha, RedDelta, RedEcho, Redfoxtrot used by China to:

- Gathering Intelligence on military technology, national security issues, political developments and foreign relations
- Monitoring ethnic and religious minorities as Uyghurs, Tibetans, Catholics
- Supporting strategic economic policies



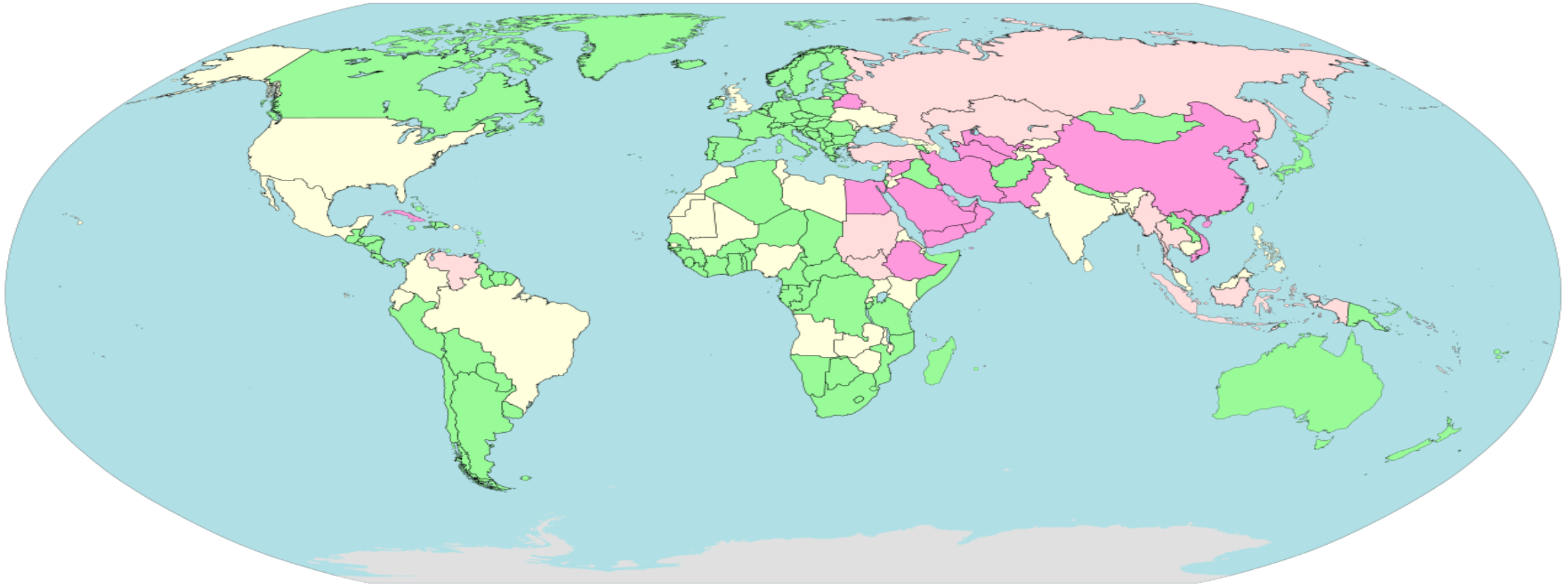
# Hacktivism

Ca' Foscari University of Venice

- In Internet activism, hacktivism is the use of hacking as a form of civil disobedience to promote a political agenda or social change, related to free speech, human rights, or freedom of information movements.
- Hacktivist activities span many political ideals and issues.
  - Freenet, a peer-to-peer platform for censorship-resistant communication, is a prime example of translating political thought (anybody should be able to speak freely) into code.
  - Hacking as a form of activism can be carried out through a network of activists, such as Anonymous and WikiLeaks
- In some countries some of these activities are considered illegal

# Internet Censorship (2018)

Ca' Foscari University of Venice



# Internet Censorship Example

Ca' Foscari University of Venice

- Social Media on Internet used to track and arrest dissidents in Thailand

# Internet Censorship China

Ca' Foscari University of Venice

- Facebook is blocked in China.
  - Users who attempt to access the website from the mainland will be greeted with an error page.
  - On the app, the feed will not refresh and users will not receive notifications.
  - The same goes for Facebook Messenger.
- Facebook was first blocked in China in 2009 following a series of riots in the western capital of the Xinjiang province, Urumqi.
  - Independence activists mainly made up of minority Muslim Uyghurs, reportedly used Facebook as part of their communications network.

# References

Ca' Foscari University of Venice


- https://www.recordedfuture.com/blog
- https://www.recordedfuture.com/resources
- https://nakedsecurity.sophos.com/
- https://www.itpro.com/security
- https://www.itsecurityguru.org/
- https://www.guerredirete.it/
- https://www.gzeromedia.com/
- https://www.economist.com/
- https://www.bbc.com/

# Dark Web

# Surface Web, Deep Web and Dark Web

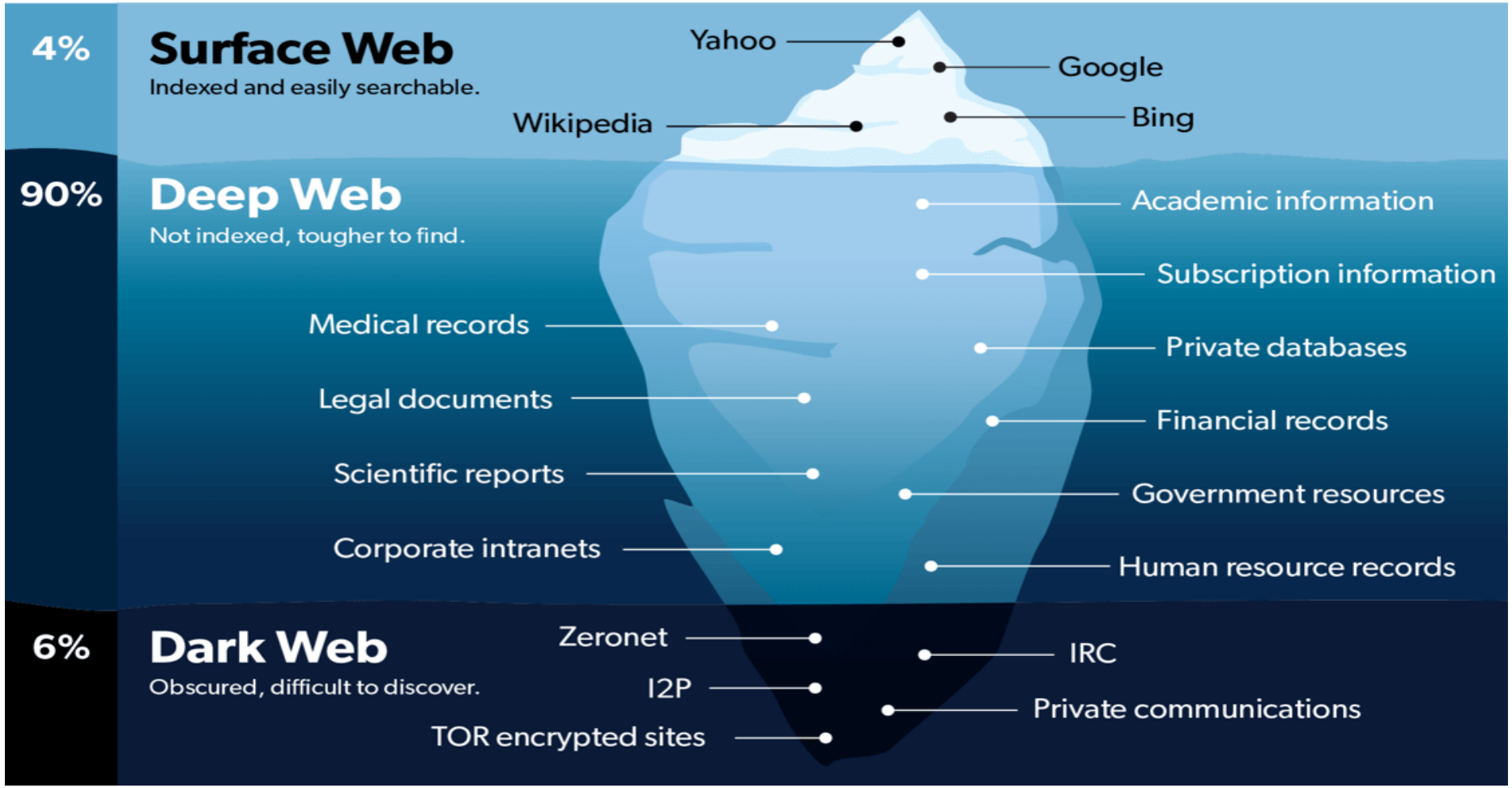
Ca' Foscari University of Venice

- The "size" of the Internet shows the number of hosts has surpassed one billion in early 2016
- More than 5 billion users have now access to the Internet.
- The Surface Web includes publicly available websites, indexed by search engines.
- Regardless of the indexing effort of search engines, some of the contents available on the internet are yet not indexed.
  - That's what we call the Deep Web.

https://www.internetworldstats.com/stats.htm

# Surface Web, Deep Web and Dark Web

Ca' Foscari University of Venice



# Dark Web

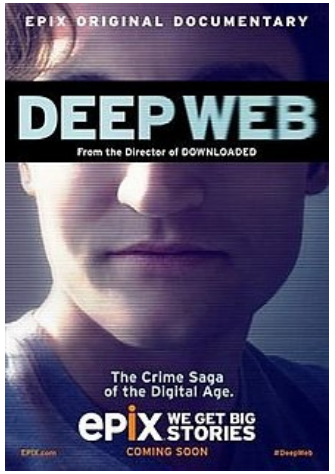
Ca' Foscari University of Venice

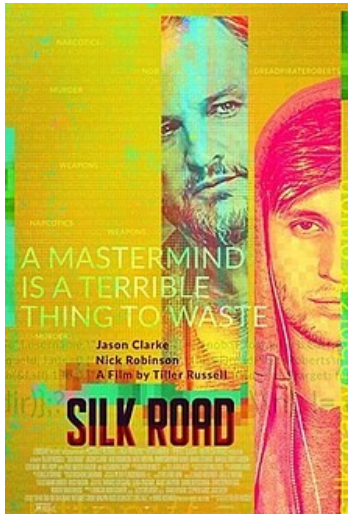
- We can define the Dark Web as "a collection of websites that are publicly visible but hide the IP addresses of the servers that run them" (Egan, 2016).
- These web sites can be visited by users, but it is hard to identify where they are hosted and who hosts them,
- Hidden behind encryption protocols
  - Tor (The Onion Routing) or I2P (Invisible Internet Project).
- The Dark Web usually relies on the combination of **crypto currencies** such as bitcoins and **anonymized access** as the foundations in creating a marketplace for dealing illegal drugs, weapons and other illegal contrabands.
- Recently, the Dark Web has been under scrutiny and investigations from legal authorities around the globe.

# The Silk Road (Feb 2011 – Feb 2013)

Ca' Foscari University of Venice

- Considered the first Dark Web hosted black market e-commerce platform.
- Any user could register anonymously to buy or sell goods with Bitcoins as currency driver.
- February 2013: FBI and Europol operation to close The Silk Road.




https://en.wikipedia.org/wiki/Ross_Ulbricht

# Post Silk-Road Era

Ca' Foscari University of Venice

- **February 2013 – November 2014:** Several market places, amongst which were Evolution, Hydra and The Silk Road 2.0.
  - November 2014: Europol and FBI seize the vast majority of them during "operation Onymous".
- **February 2014 – September 2015:** The rise of Agora, surviving operation Onymous: closed possibly because of vulnerabilities in Tor
- **September 2015 - now**: More than 50 markets.
  - Alphabay supports reputation, multisig transactions, coin tumbling and Monero, and it's nearly 20 times the size of Agora at its best.

# Agora

Ca' Foscari University of Venice

- Agora was a portal selling both products and services, with a minimal set of rules.
  - The only items that couldn't be sold were body parts, and the only service that was forbidden to sell was assassination, and later weapons were also forbidden
- Agora changed host and domain name several times, trying to avoid cyber-crime law enforcers over its almost two years of existence.
  - One of the instances of this marketplace (agorahooawayyfoe.onion) was analysed in detail by academic research
  - Baravalle, Andres, Mauro Sanchez Lopez, and Sin Wee Lee. "Mining the dark web: drugs and fake ids." In *2016 IEEE 16th international conference on data mining workshops (ICDMW)*, pp. 350-356. IEEE, 2016.

# Agora Market Analysis (2016)

Ca' Foscari University of Venice

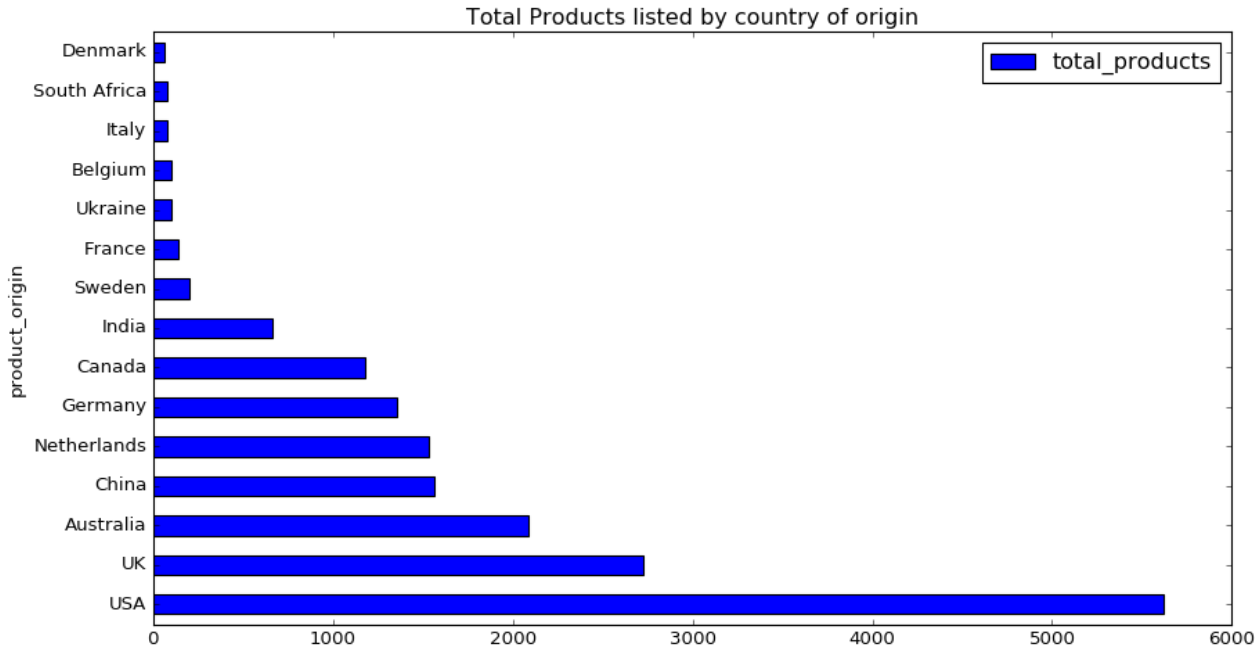
- **Over 30,000 products on sale**, mostly drugs and IDs, worth at least 170691.12 Bitcoins (£26 million).
- A staggering 1,233 sellers spread across 20 countries, with the largest number located in the USA and UK.
- 90% of the market was dominated by the largest 10% of sellers, with 80%  of the market share going to the selling and purchase of drugs.
- The highest number of drug sellers were from the USA (388), Australia (138) and the UK (137),
- Top countries by market size were Germany (£7.8 million), USA (£6.06 million) and Netherlands (£2.9 million).


Baravalle, Andres, Mauro Sanchez Lopez, and Sin Wee Lee. "Mining the dark web: drugs and fake ids." In *2016 IEEE 16th international conference on data mining workshops (ICDMW)*, pp. 350-356. IEEE, 2016.

# Agora: Drug Market

Ca' Foscari University of Venice

- 80% of the market was drugs, dominated by USA and UK
- One seller, RADICALRX, was offering a cache of £10 million pounds worth of drugs, including Hydromorphone, Oxycodone, Fentanyl and Meth.
- A US-based seller, HonestCocaine, offered £1.24 million of cocaine for sale.



# Agora: Counterfeit Documents

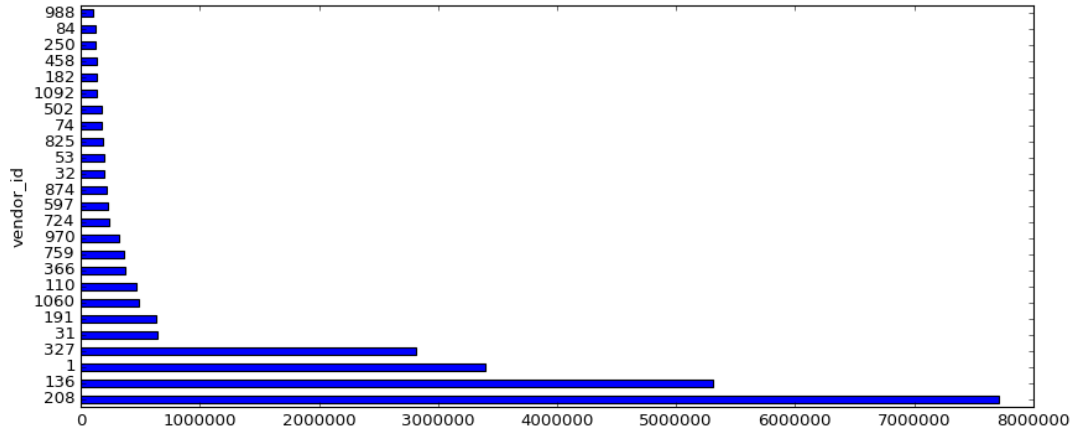
Ca' Foscari University of Venice

- The total size of the counterfeit documents market was ~ 3,700 bitcoins about £650,000 at the time (2016); ~ 2.6% of the market
  - 84 scans and photos of passports were on sale, with 12 physical passports also being offered
- Physical UK passport for £752,
- Scanned passports for £7, and can be bought in bulk
- Counterfeit EU identity cards for £142
- US state id cards, ranging from £25 to £92
- US driving licenses ranged between £51-300;
- European driving license up to £419

# Agora: Organized Crime

Ca' Foscari University of Venice

- Over **90% of the market was dominated by the largest 10% vendors**.
- When looking at the hashish category, the mean amount on sale is 47g, with a median of 10g, but with some sellers selling up to 1 kg at the time.
- This is a reasonable indicator that organized crime is involved.
- Some use of sock-puppets (fake accounts managed by one account)
  - Evidence from Image analysis, NLP analysis, Stylometry
- Entities as RADICALRX have over 10 million dollars of product on sale on Agora
  - Hardly teenagers in basements – the scale is the one of organized crime



# References


M. Splitters, F. Klaver, G. Koot and M. Van Staalduinen, "Authorship Analysis on Dark Marketplace Forums," in proceeding of Intelligence and Security Informatics Conference (EISIC), Manchester, 2015.

K. Bharat and A. Broder , "A technique for measuring the relative size and overlap of public Web search engines," Computer Networks and ISDN Systems, vol. 30, no. 1-7, pp. 379-388, 1998.

M. Bergman, "White Paper: The Deep Web: Surfacing Hidden Value," The Journal of Electronic, vol. 7, no. 1, 2001.

M. Eddy, "Inside the Dark Web," 04 02 2015. [Online]. Available: http://uk.pcmag.com/security/39461/guide/inside-the-dark-web. [Accessed 17 06 2016].

M. Egan, "What is the Dark Web? How to access the Dark Web. What's the difference between the Dark Web and the Deep Web?," 2016 06 28. [Online]. Available: http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautfiulpeople-3593569/. [Accessed 17 06 2016].

H. Oman, "Security Technology Progress: The 37th IEEE-AESS Carnahan Conference, Taiwan," IEEE Aerospace and Electronic Systems Magazine, vol. 19, no. 2, pp. 35-40, 2004.

H. Chen, "The Terrorism Knowledge Portal: Advanced Methodologies for Collecting and Analyzing Information from the 'Dark Web' and Terrorism Research Resources," 08 2003. [Online]. Available: http://www.slideshare.net/suyu22/the-terrorism-knowledge-portal-advanced-methodologies-for-collecting-and-analyzing-information-from-the-dark-web-and-terrorism-research-resources. [Accessed 17 06 2016].

A. Greenberg , "End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market," 2 10 2013. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market. [Accessed 16 6 2016].

A. Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains," 11 07 2014. [Online]. Available: https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/. [Accessed 16 6 2016].

A. Greenberg, "Drug Market 'Agora' Replaces the Silk Road as King of the Dark Net," 18 11 2015. [Online]. Available: http://www.wired.com/2014/09/agora-bigger-than-silk-road. [Accessed 17 06 2016].

# Anonymizing Network Technologies (TOR)

# Problem



- Internet surveillance like traffic analysis threatens users' privacy.
- Encryption does not work, since packet headers still reveal a great deal about users.
- End-to-end anonymity is needed.
- Solution: a distributed, anonymous network

# What is Tor

Ca' Foscari University of Venice

- Tor is a distributed anonymous communication service using an overlay network that allows people and groups to improve their privacy and security on the Internet.
- Individuals use Tor to keep websites from tracking them, or to connect to those internet services blocked by their local Internet providers.
- Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site.

# Design

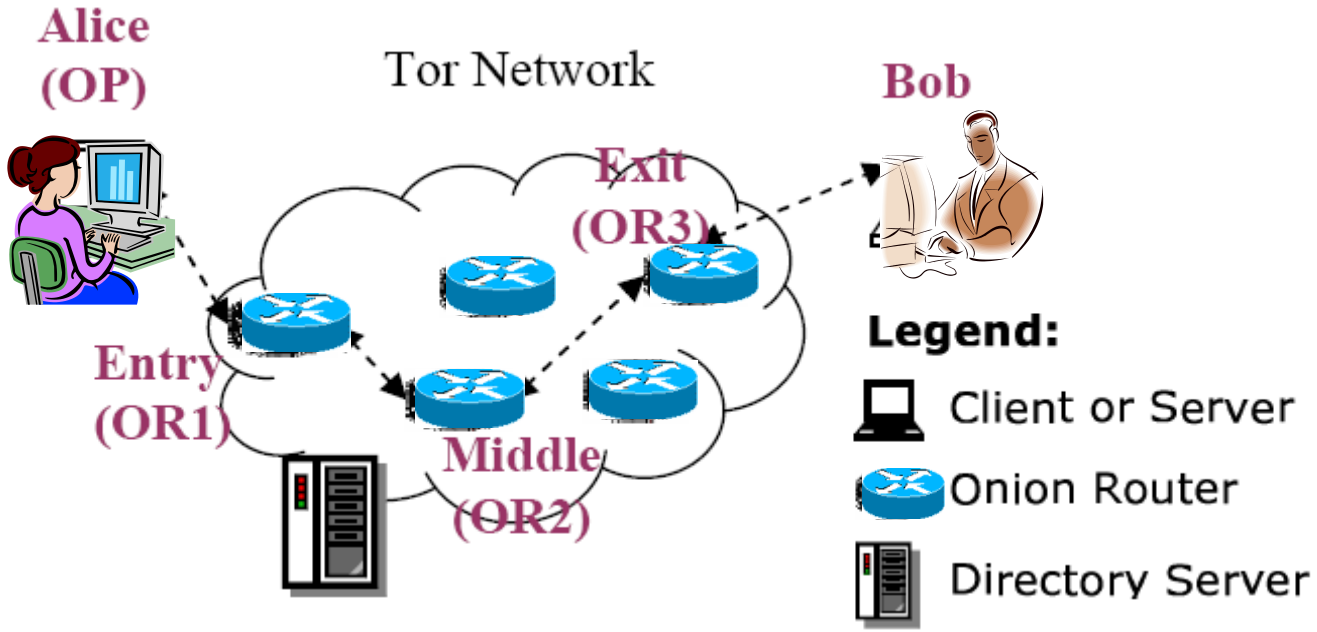


- Overlay network on the user level
- Onion Routers (OR) route traffic
- Onion Proxy (OP) fetches directories and creates virtual circuits on the network on behalf of users.
- Uses TCP with TLS
- All data is sent in fixed size (bytes) cells

# Components of Tor

Ca' Foscari University of Venice

- Client: the user of the Tor network
- Server: the target TCP applications such as web servers
- Tor (onion) router: the special proxy relays the application data
- Directory server: servers holding Tor router information

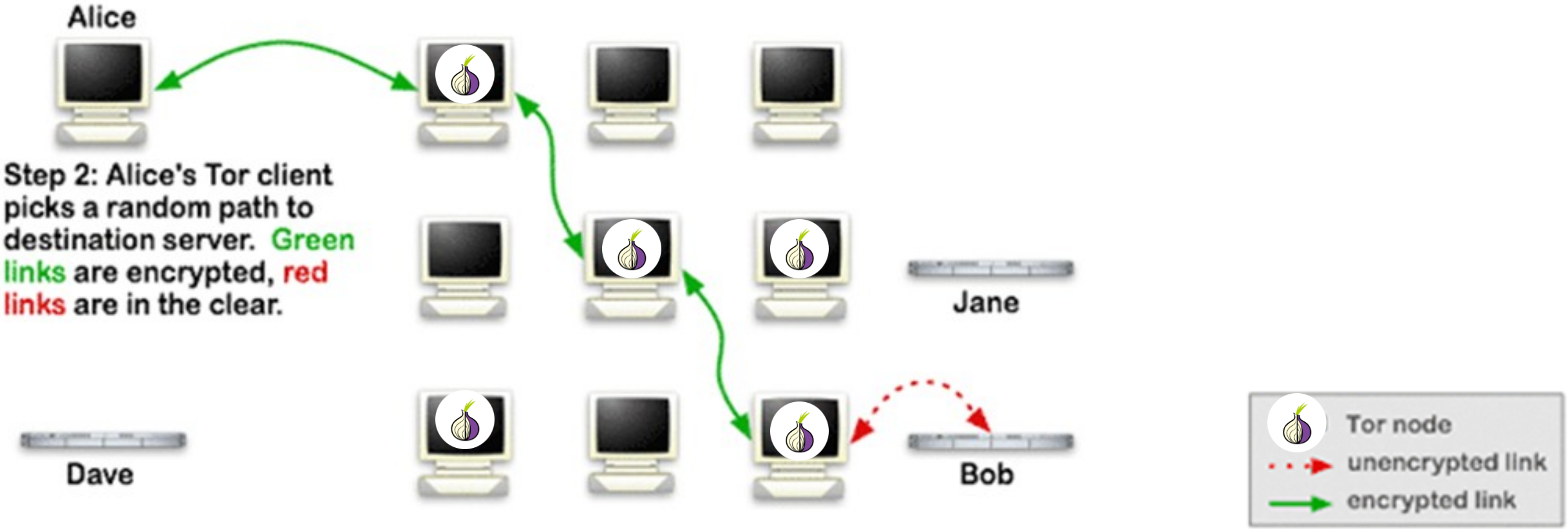


# How does Tor work?

Ca' Foscari University of Venice

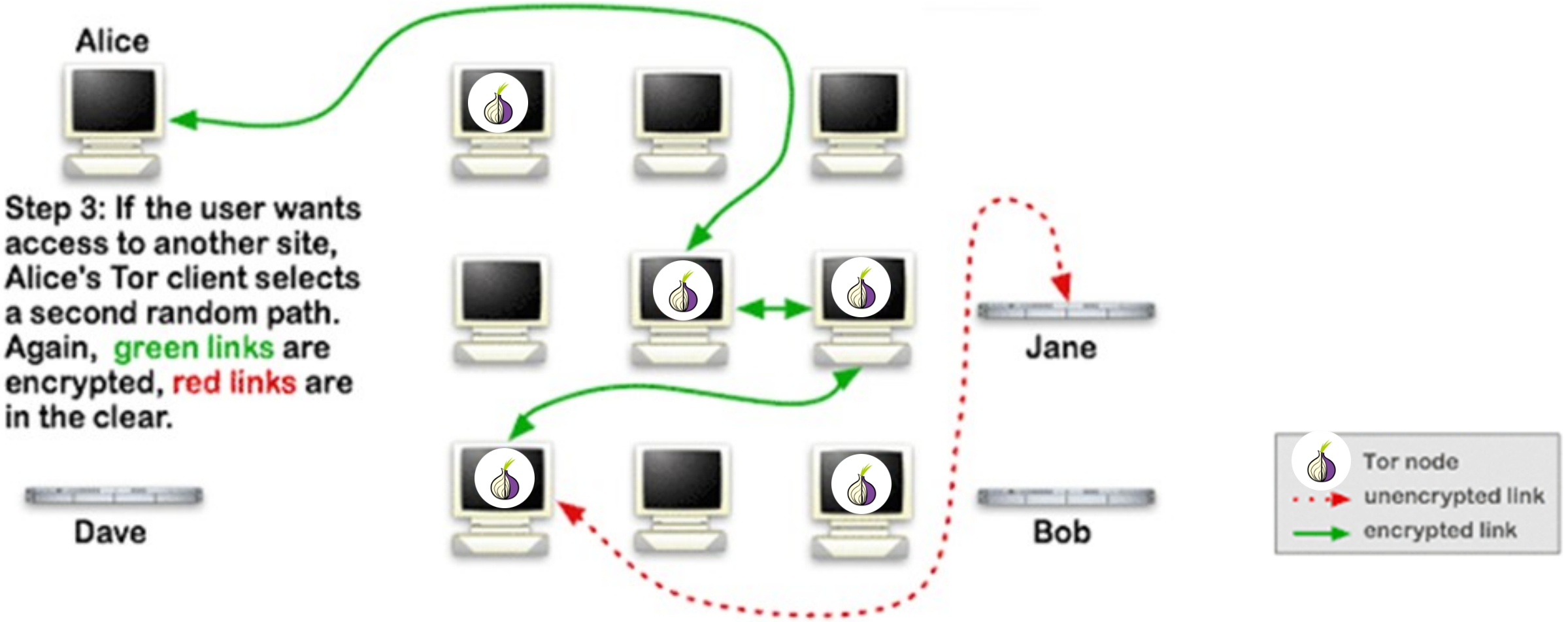
# How does Tor work?

Ca' Foscari University of Venice



# How does Tor work?

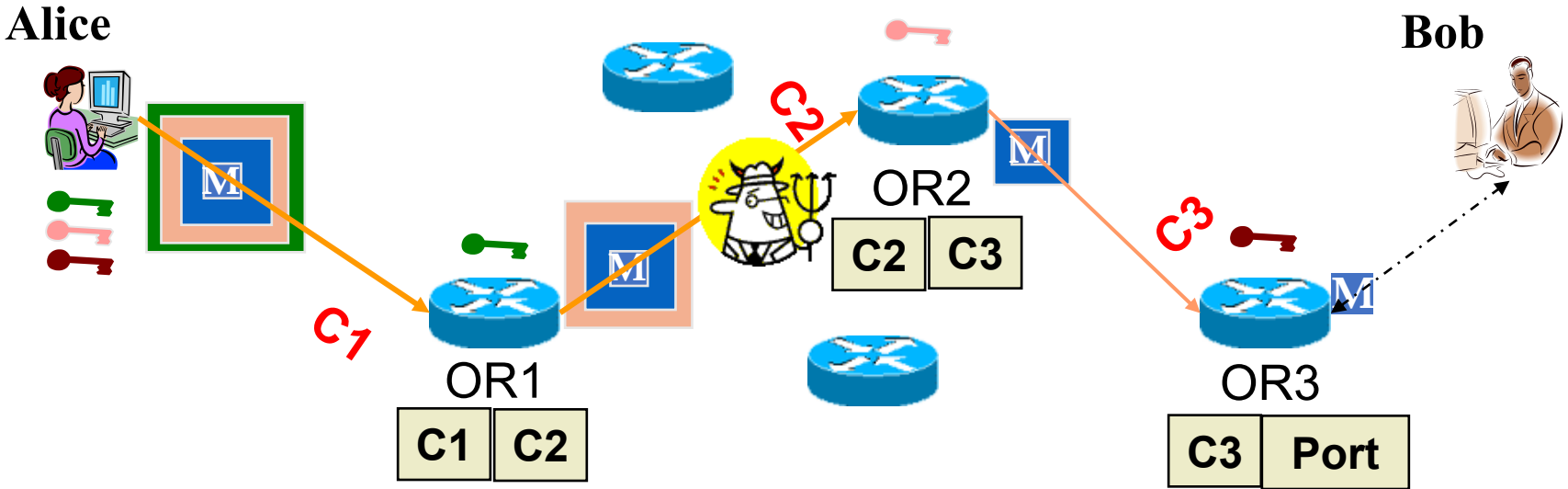
Ca' Foscari University of Venice



# Onion Routing

Ca' Foscari University of Venice

- A circuit is built incrementally one hop by one hop
- Onion-like encryption
  - Alice negotiates an AES crypto key with each router
  - Messages are divided into equal sized cells
  - Each router knows only its predecessor and successor
  - Only the Exit router (OR3) can see the message, however it does not know where the message is from



# Hidden Service and Rendezvous Points


Ca' Foscari University of Venice

- Location-hidden services allow Bob to offer a TCP service without revealing his IP address.
- Tor provides receiver anonymity by allowing location hidden services
- Design goals for location hidden services
  - Access Control: filtering incoming requests
  - Robustness: maintain a long-term pseudonymous identity
  - Smear-resistance:
    - a social attacker should not be able to "frame" a rendezvous router by offering an illegal or disreputable location-hidden service and making observers believe the router created that service
  - Application transparency
    - Special software to access location-hidden servers, but users are not required to modify their apps.
- Location hidden service leverage rendezvous points

# What is I2P?



- The Invisible Internet Project
- An anonymizing P2P network providing end to end encryption.
- Utilizes decentralized structure to protect the identity of both the sender and receiver.
- It is built for use with multiple applications including email, torrents, web browsing, IM and more.
- UDP based (unlike Tor's TCP streams)

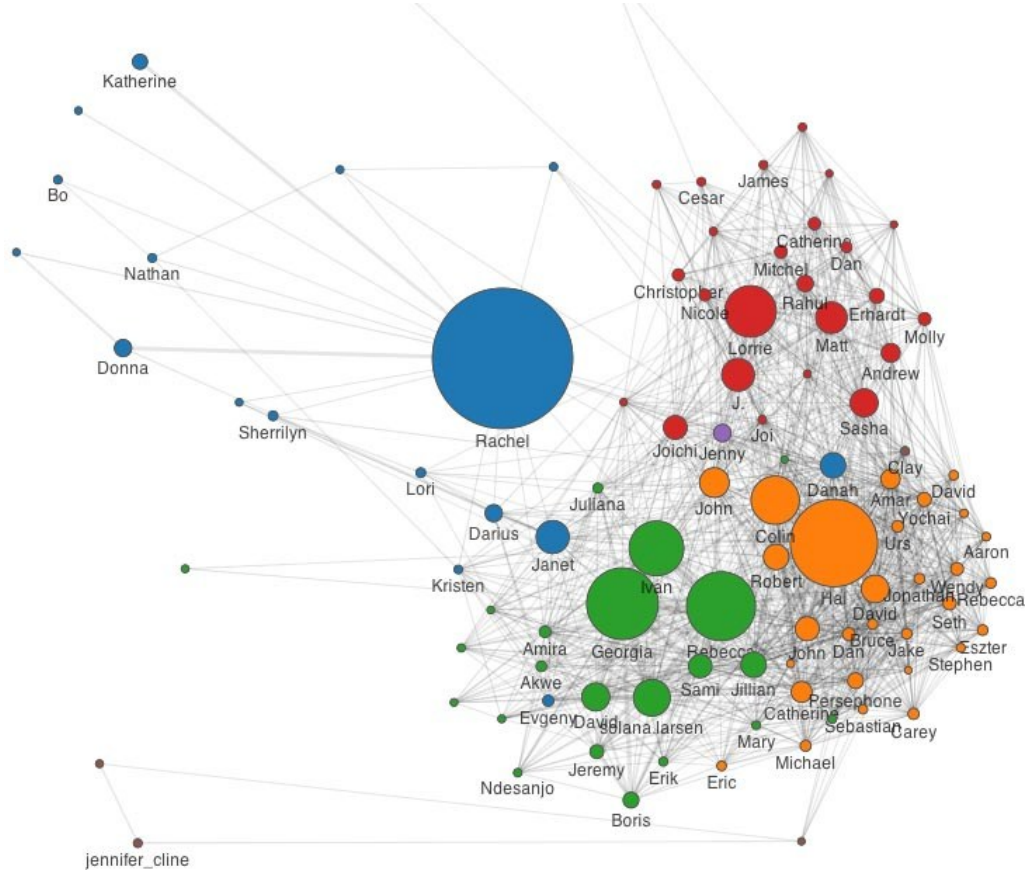
# Meta-data leakage

Ca' Foscari University of Venice

- Is Encryption protecting the content of communications sufficient? No.
- Meta-data is unprotected:
  - Who talks to whom?
  - How often?
  - At what times?
  - What volumes?
  - In which sequence?
  - What are the groups?
  - From which locations?
- Social Network Analysis.
- Machine Learning to learn private attributes.
- Profiling for price and other discrimination.

- 'We Kill People Based on Metadata'

- Gen. Hayden (former director of the CIA & NSA)

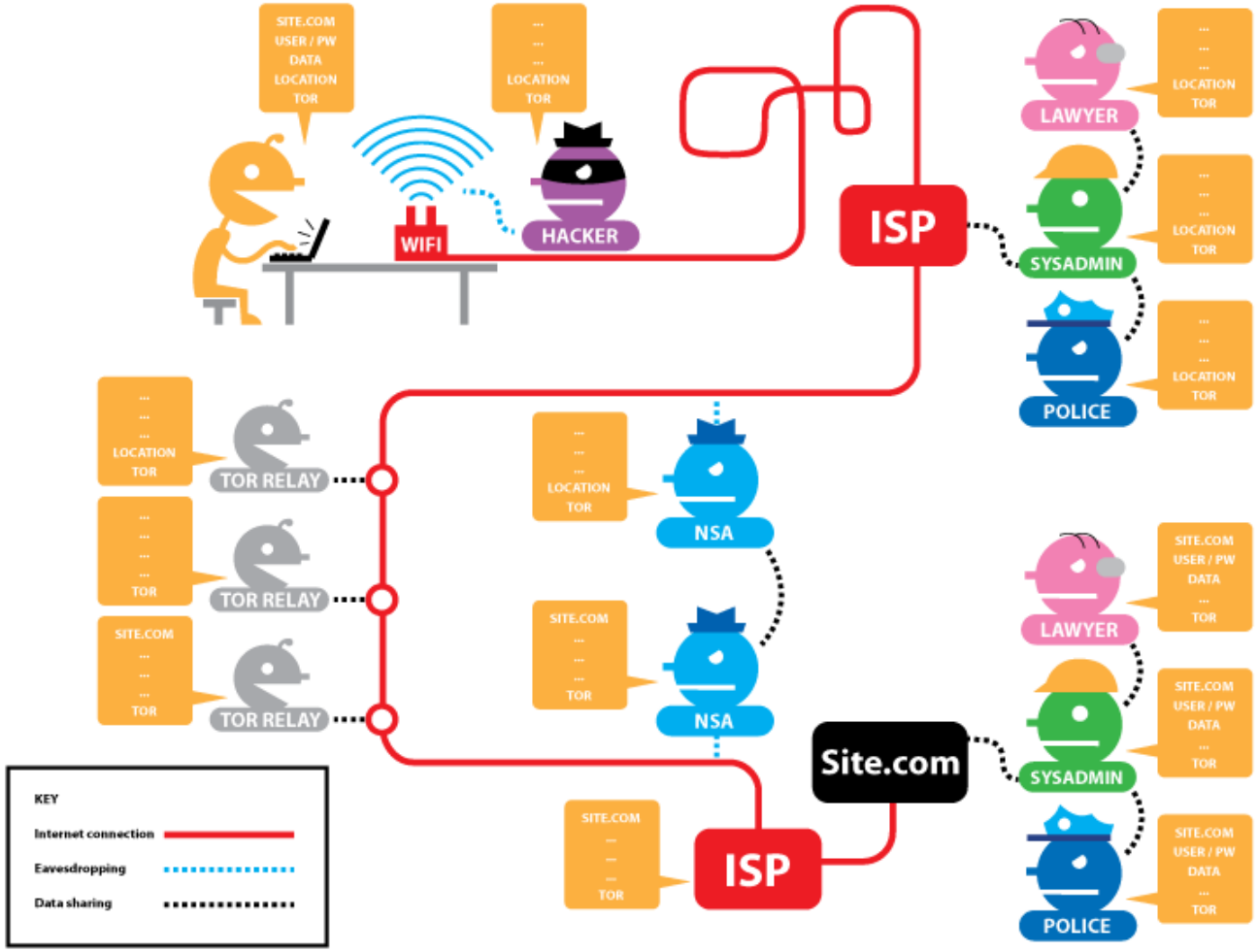



Social Graph: http://www.ethanzuckerman.com/blog/2013/07/03/me-and-my-metadata-thoughts-on-online-surveillance/

# How Tor works? (according to the EFF.org)

Ca' Foscari University of Venice

- Architecture:
  - Fixed guards
  - 3 relays
  - All cells travel on same path
  - No delay or cover traffic
- Threat model:
  - Adversary can only observe 1 location.
- The 2nd gen. onion router tor
  - Sequential Ephemeral Diffie-Hellman.
  - All packers transit on the same route.




https://www.eff.org/files/tor-https-2.png

# Forward Secrecy

Ca' Foscari University of Venice

- Property of encyption usually.
  - Ensures that a leaked key cannot compromise past (or future) messages.

- Can a mix system implement forward secrecy?
  - Consider time between public (encryption) keys creation and deletion.
  - Short: limits the time messages can be in flight; short-term replies.
  - Long: limits forward secrecy benefits.

- Tor: interactive circuit creation allows for Perfect Forward Secrecy.
  - Under compulsion threat model Tor / OR is more secure.

# Conclusions

Ca' Foscari University of Venice

- Tor is both too much and too little:
  - Too little: real adversaries can gain near GPA capabilities, or enough to break Tor. The Snowden revelations confirm this.
  - Too much: if it is trivial to link two points simpler design is possible:
    (1) No need for multiple layers of encryption.
    (2) A single hop security is all you get after a long time.

In conclusion:

- Tor is great if you want to hide from a relatively weak adversary.
- Not so great against more powerful adversaries…