CTI – EU | Bonding EU Cyber Threat Intelligence

Digging into the Dark Web

Rome – Link Campus University

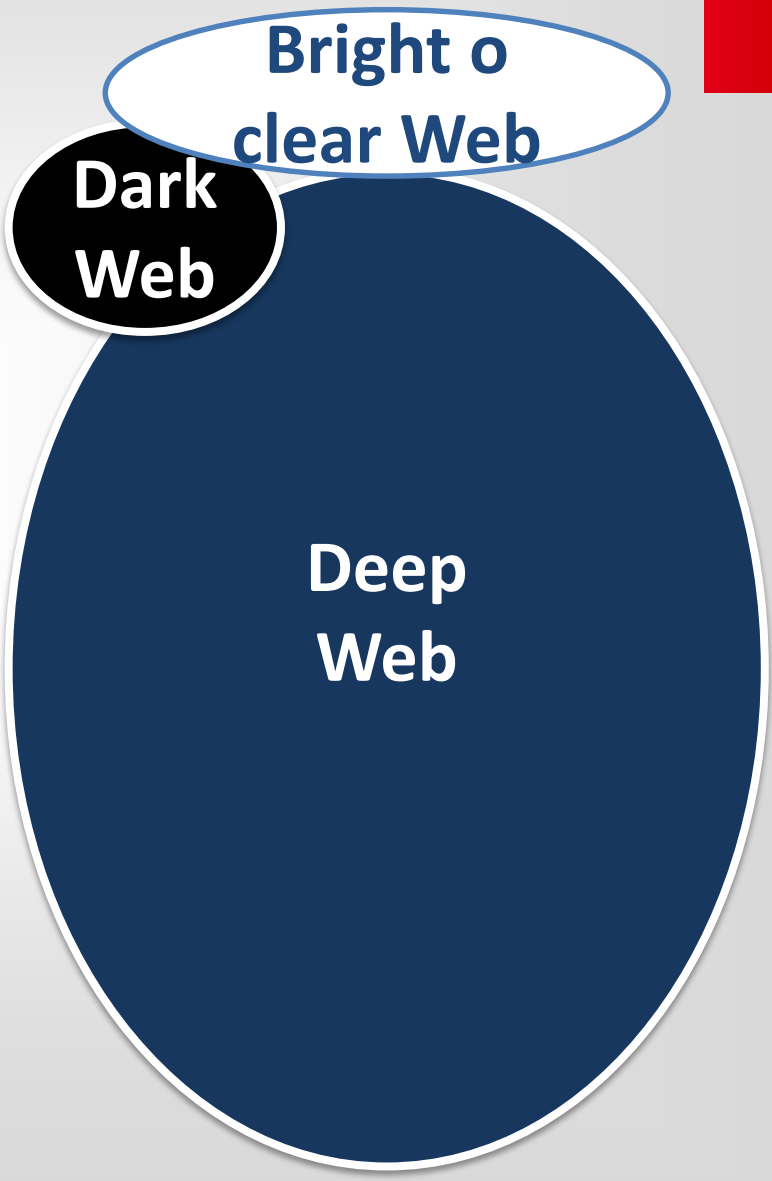
30-31 October, 2017

Pierluigi PAGANINI

Current scenario

Deep Web vs Dark Web

- **Deep Web**
  - It represents the part of the web that has not yet been indexed by common search engines
- **Dark Web**
  - Set of publicly accessible content that are hosted on websites whose IP address is hidden but to which anyone can access it as long as it knows the address
  - Set of private content exchanged in a closed network of computers for file sharing



Current scenario

Dark Web

- **The Onion Router (TOR)**
  - Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.
- **I2P - The Invisible Internet Project**
  - Network "Peer-to-Peer" (P2P)
  - I2P is an anonymous overlay network - a network within a network, Ordinary services running on a secure network
- **Freenet -** A Distributed Anonymous Information Storage and Retrieval System.
- **anoNet** is a decentralized friend-to-friend network built using VPNs and software BGP routers
- **ZeroNet** - is a new decentralized and open source web platform based on BitTorrent(p2p) technology and BitCoin cryptography.

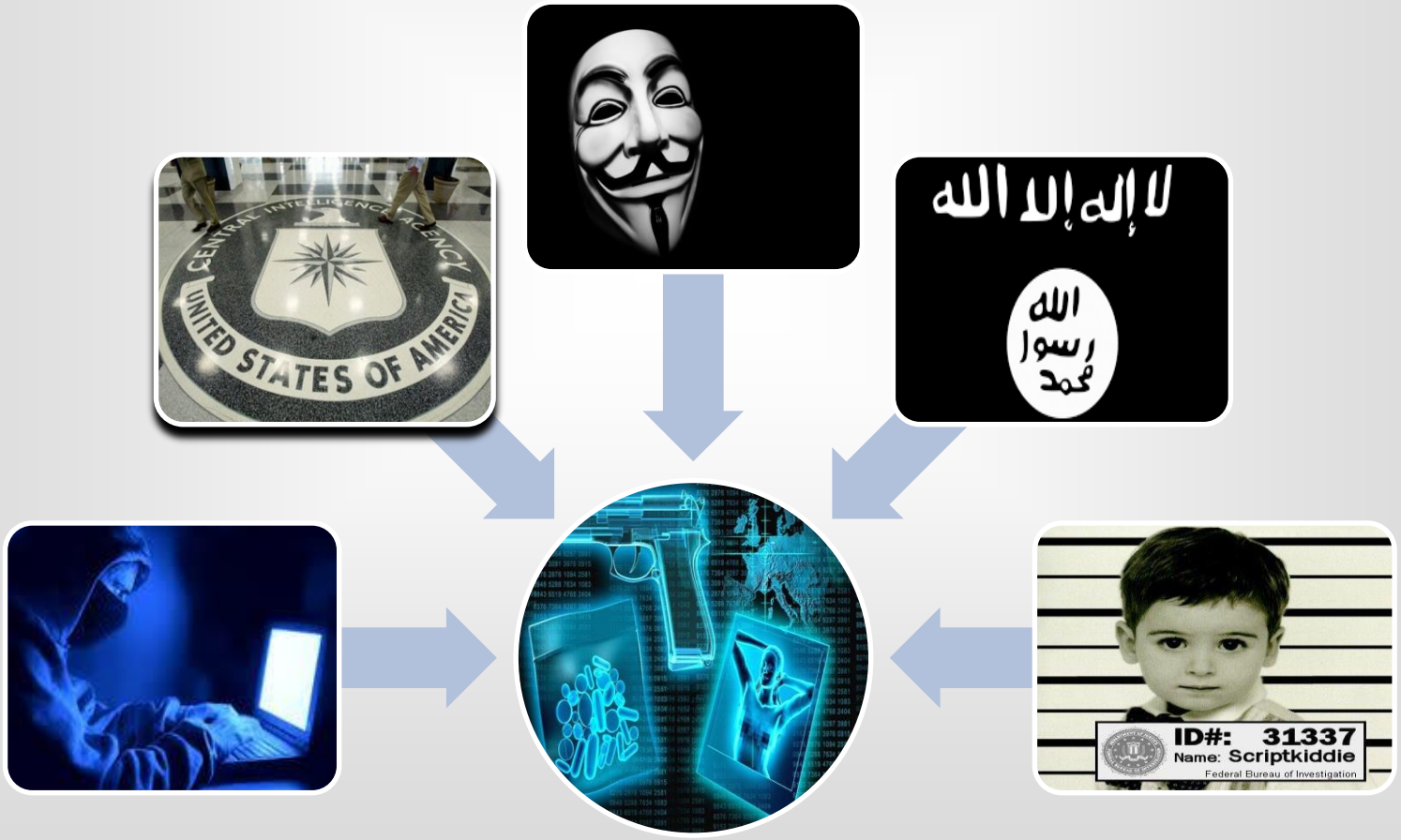
Current scenario

Why Tor is so popular in the criminal ecosystem?

- Anonymity
- TOR provides "hidden services" that could be used for several illegal activities.
- Law enforcement face difficulties in de-anonymizing TOR users.
- Impossible to conduct monitoring on a large-scale.
- Excellent aggregator - It hosts principal underground communities.
- TOR allows bypassing Internet Filtering (i.e. Censorship).

Current scenario

Bad Actors



Cybercrime

Dark Net as a facilitator for cybercrime

"Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual." *INTERPOL*

Cyber crimes can be grouped in the following categories:

- ***Attacks against computer hardware and software***
- ***Financial crimes***
- **Abuse** (i.e. child pornography)

Darknets are the right place where search for anything related above crimes

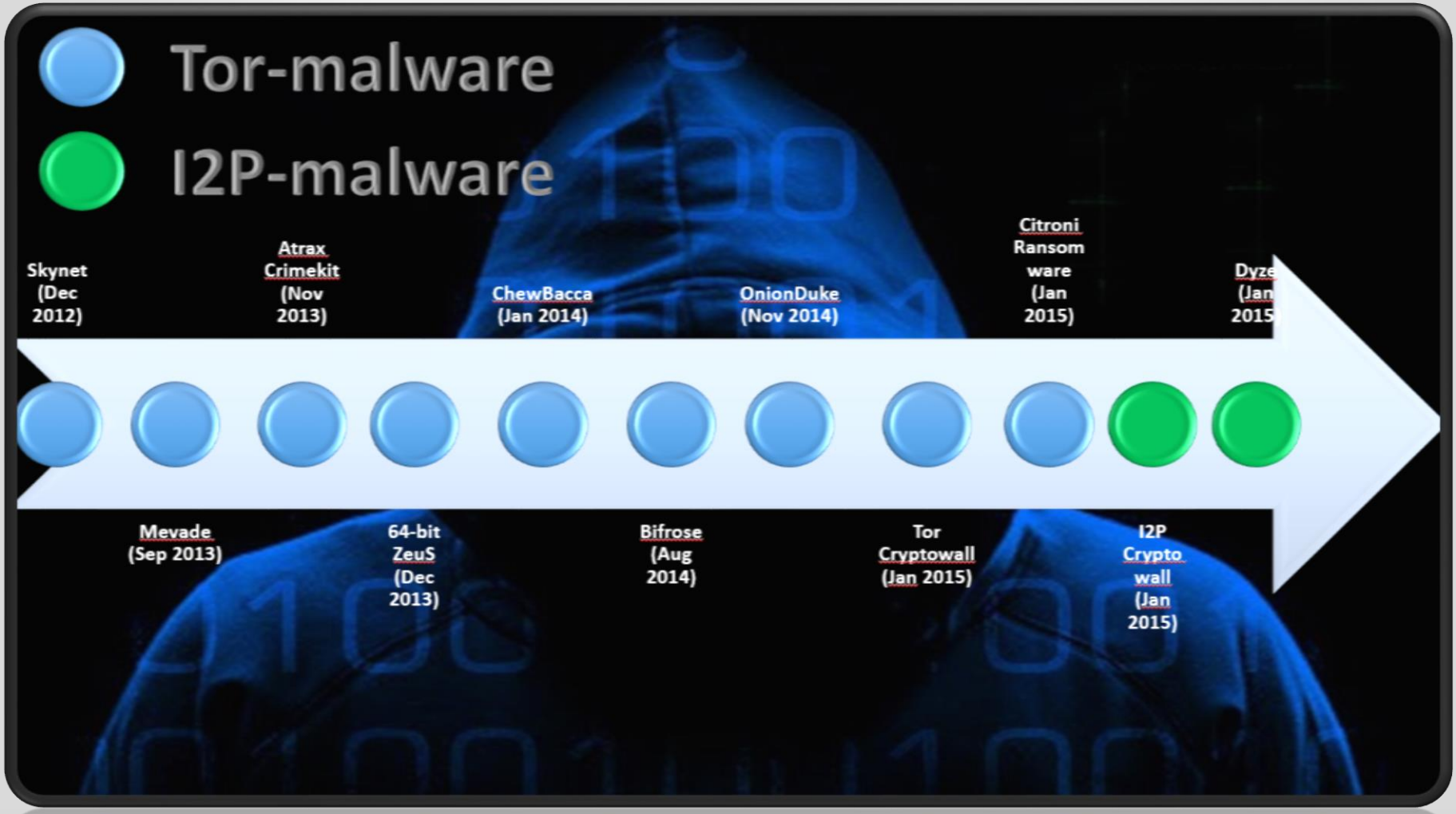
Malware and DarkNets

The offer of Darknets

- Darknet are a privileged environment for malware authors and botmasters.
- Hiding C&C infrastructure
- Availability of authenticated hidden services
- Availability of black markets to buy and sells their products.

Until 2015

The offer of Darknets



Malware and DarkNets

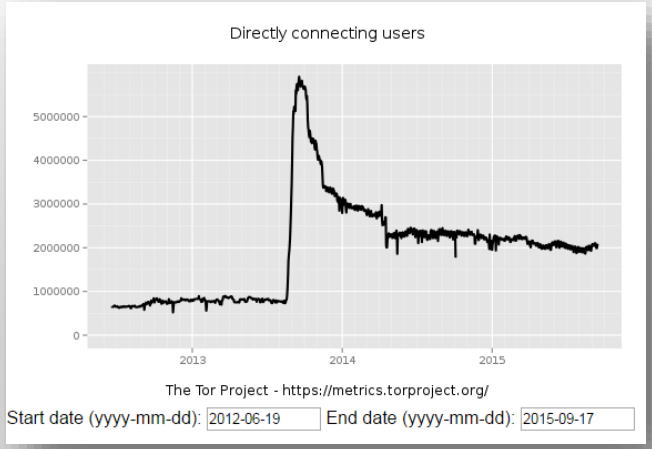
The offer of Darknets

2012: One C&C server for data exfiltration (Skynet)

2013: 3 C&C servers controlled a botnet of million machines

2014: OnionDuke Campaign - 3 C&C servers cyber espionage

2015: 2 C&C server in tor and 2 on I2P (Ransomware)



Threats from 2015
X Ransomware KeRanger (Infected BitTorrent Client Installer)
CryptoLocker/FAKBEN Ransomware
Eleanor Mac backdoor
Petya ransomware
ORX-Locker, Ransomware-as-a-service
Cryptowall (release 2.0 and up)
CSTO Ransomware uses UDP and Google Maps
Cryptolocker
Locker
TeslaCrypt ransomware (release 2.0 and up)
CTB Locker
CryptoWall 3.0 (I2P)
Nuke HTTP bot
.....

Malware and DarkNets

Malware-as-a-Service

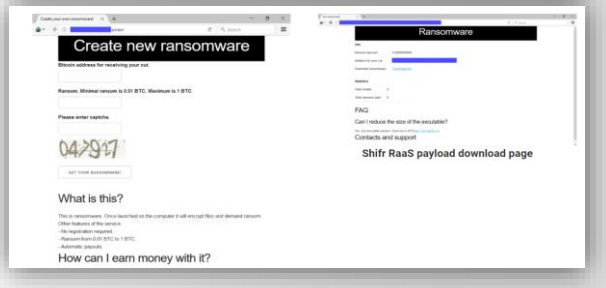
2015 – Tox ransomware-construction kits that allow easy to build malware in just 3 steps

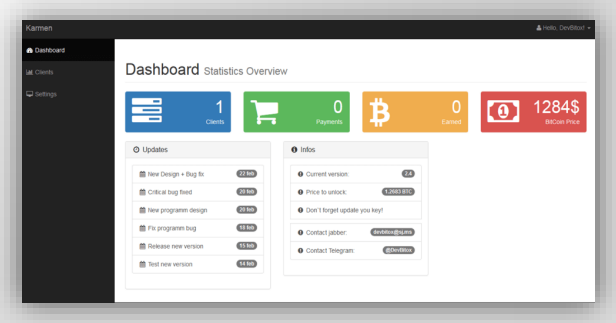
2017 - MACSPY – Remote Access Trojan as a service on Dark web

2017 – MacRansom is the first Mac ransomware offered as a RaaS Service.

2017 – Karmen Ransomware RaaS

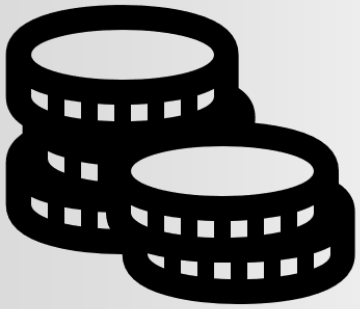
2017 –Ransomware-as-a-Service dubbed Shifr RaaS that allows creating a ransomware compiling 3 form fields.





Malware and DarkNets

Malware Price (Middle East and North African cybercrime underground)



Offering	Price
Worm	$1-12
Keylogger	Free-$19
Known Ransomware	$30-50
Malware Builder	Free-$500
Citadel (fully undetectable)	$150
Ninja RAT (fully undetectable)	$100
Havij 1.8 (cracked)	Free

Table 4: Average prices of malware

Tor network abuse in financial crimes

Tor Anonymity and Financial Frauds

- Dec. 2014 - non-public report realized by the US Treasury Department found that a majority of bank account takeovers exploits the anonymizing the Tor network.
- 6,048 suspicious activity reports (SARs) filed by financial organizations between August 2001 and July 2014, focusing for those involving one of more than 6,000 known Tor network nodes.
- 975 hits corresponding to reports totaling nearly $24 million in likely fraudulent activity.
- From October 2007 to March 2013, filings increased by 50 percent," the report observed. "During the most recent period — March 1, 2013 to July 11, 2014 — filings rose 100 percent."

Tor network abuse in financial crimes

Tor Anonymity and Financial Frauds

Diversity of Filers						
FILER	Money Services Businesses	Depository Institutions - Banks	Broker Dealers	MSB - Prepaid Card Providers	Depository Institutions- Credit Unions	MSB - Virtual Currency Exchangers
SARS	138	133	27	15	3	2
%	43%	42%	8%	5%	1%	1%

Filers Awareness of IP Association		
FILER	Knew IPs were Tor-related	Did NOT know IPs were Tor-related
# of SARS	10	308
% of Filers	3%	97%

Types of Suspicious Activity in Tor-related SARs		
SUSPICIOUS ACTIVITY	# of SARs	Percentage
Other[1]	164	52%
Identity Theft	140	44%
Money Laundering	110	35%
Unusual use of money transfer(s)	78	25%
Account Takeover	77	24%
Unauthorized electronic intrusion / Computer Intrusion	13	4%
Provided questionable or false documentation	12	4%
Suspicious concerning the source of funds	11	3%
Two or more individuals working together	9	3%
Forgeries	8	3%
Transaction with no apparent economic, business, or lawful purpose	8	3%
Suspicious use of multiple accounts	6	2%

[1] A review of Suspicious Activity referred to as "Other" determined that the majority of these activities were associated with Account Takeover and/or Identity Theft.

Black Markets

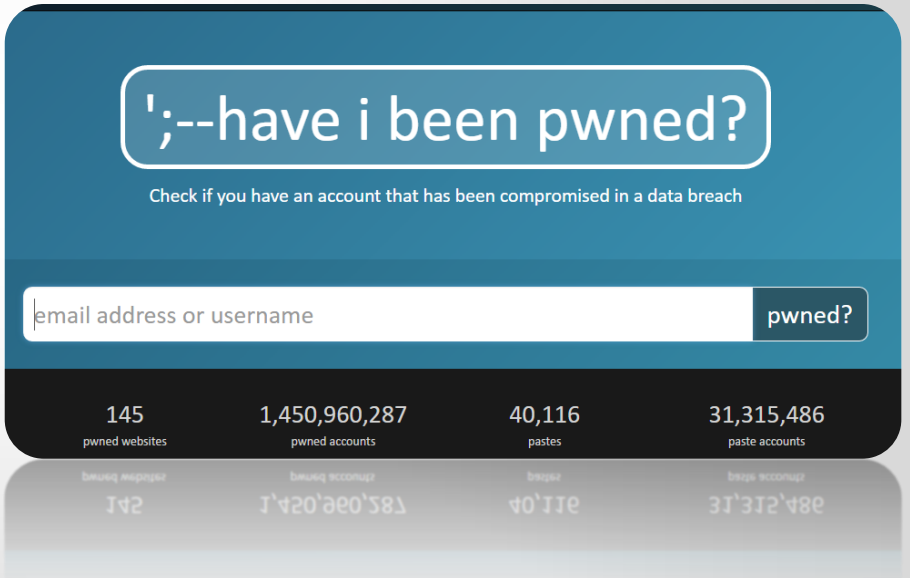
Criminal aggregators

- Black Markets are places on the web where it is possible to acquire or rent "malicious" services and products.
- Anonymity and virtual currencies.
- Efficient facilitators of criminal activities.
- Most commercialized products are drugs, user's PII, stolen card data and hacking services.
- The Feedback mechanism and escrowing services increase mutual trust between buyers and sellers.
- Competition (Mr Nice Guy hired a blackmailer to hit TheRealDeal and its competitors. TheRealDeal hacked back.)

Data Leakage

Users data in the underground

- Anomali Labs analyzed availability in the Dark Web of FTSE 100 employees data.
- 5,275 employee email and clear text password combinations from FTSE 100 companies available on the Dark Web, on crime forums, on paste sites
- An average of 50 employees for each FTSE 100 company have had their credentials exposed online.

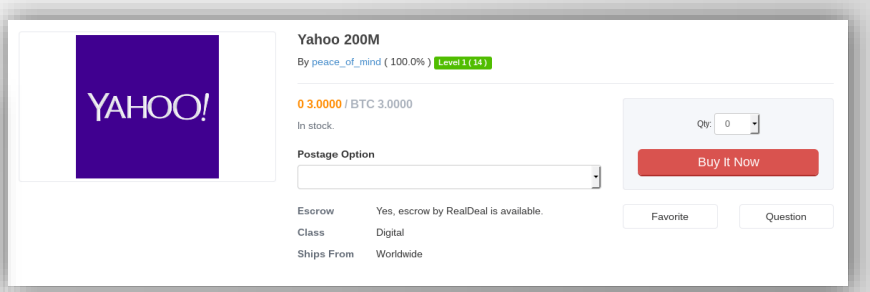


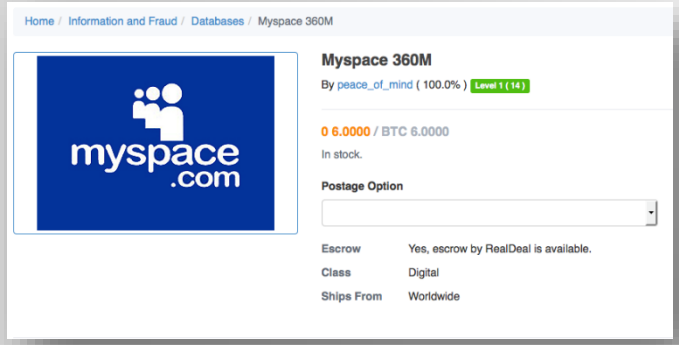
Data Leakage

Criminal aggregators

Dropbox Data Breach, more than 68 Million account details leaked online

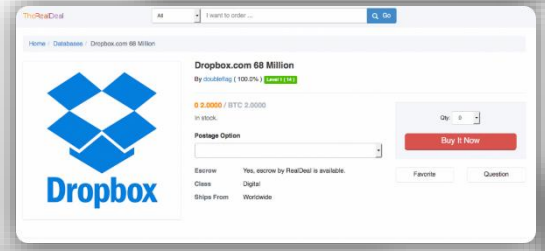
August 31, 2016 By Pierluigi Paganini

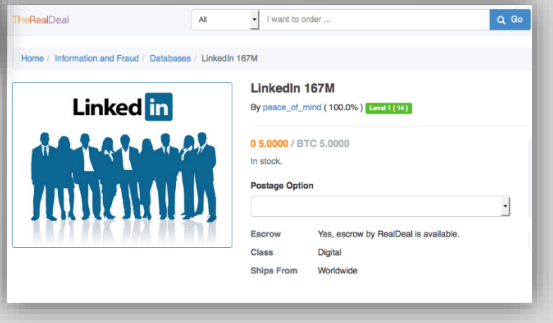




100 million credentials from the Russian Facebook VK.com go on sale

June 6, 2016 By Pierluigi Paganini





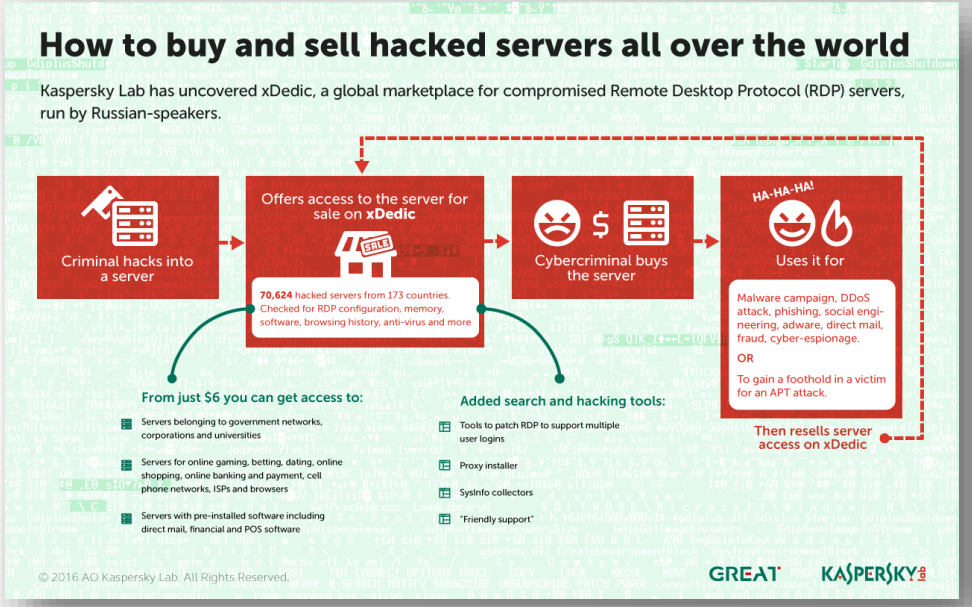
Hundred Million Stolen MySpace Passwords for sale in the darkweb

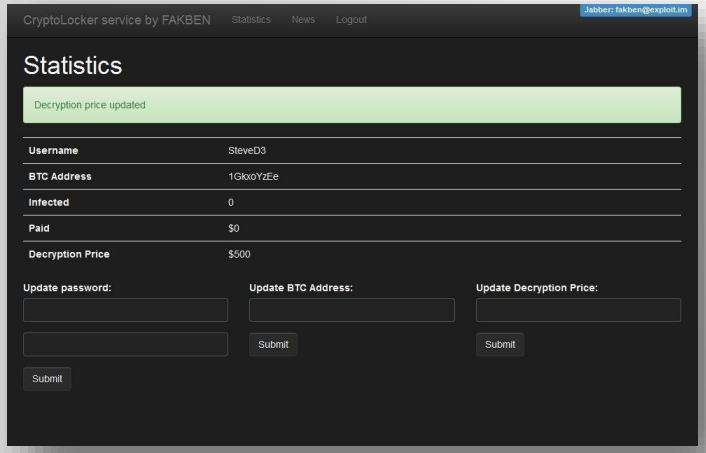
May 28, 2016 By Pierluigi Paganini

Crime-as-a-Service

CaaS

June, 2016 - [xDedic marketplace](#) is offering everyone from entry-level cybercriminals to APT groups fast, cheap and easy access to legitimate organizational servers.





FAKBEN is offering a professional Ransomware-as-a-service that relies on a new CryptoLocker ransomware which can be downloaded through the executable file.

Black Markets

Dark markets are crowded places

Different Levels of Participants in the Underground Market

Proportion of Participants
Sophistication/skill levels and various roles

Examples:

Sophisticated/ highly skilled

Administrators

Subject-matter experts

- Elite researchers
- Exploit developers
- Zero-day researchers
- Malware writers
- Identity collectors
- Programmers
- Tech experts

Can be sophisticated or unsophisticated

Intermediaries/brokers

Vendors

- As-a-service providers
- Virtual money mule services
- Spammers
- Botnet owners
- Drop service
- Distributors
- Hosted systems providers
- Cashiers
- ID/financial data providers

Mules (witting)

Unsophisticated/ less skilled

General members

- Buyers
- Observers

Mules (unwitting)

SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.

Black Markets

Tor Black Markets

MARKETS LIST & AVAILABILITY STATUS

TOP MARKETS!

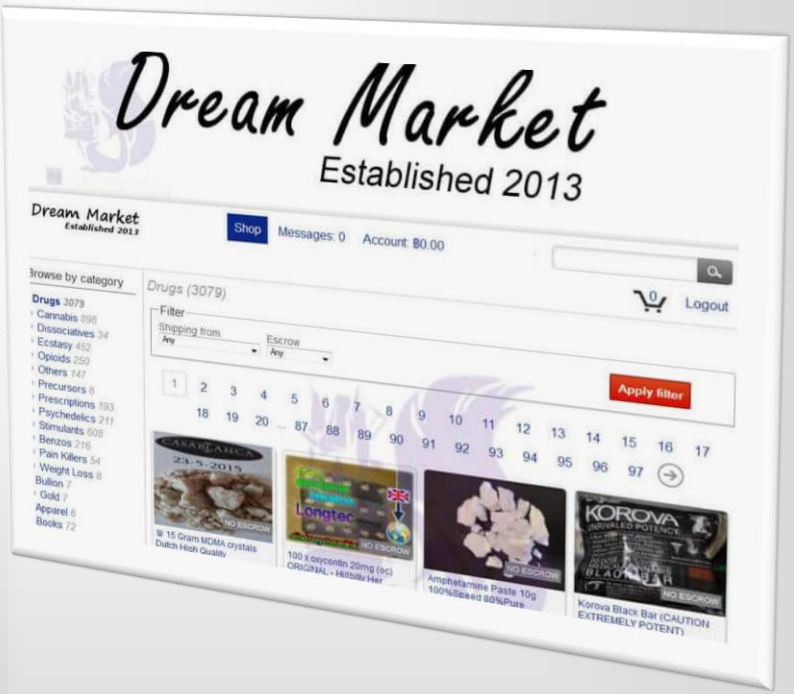
- Dream market - 86.27%
- Point / T•chka Free Market - 51.41%
- Wall Street Market - 84.98%

INVITE / REFERRAL MARKETS

- AERO Market - 33.06%
- Libertas Market (Monero Only) - 36.33%

MARKETS

- The Majestic Garden - 89.07%
- Sourcery Market - 81.91%
- CGMC - 95.07%
- Berlusconi Market - 92.51%
- RsClub Market - 83.18%



Black Markets

- PII record for $1. (Trend Micro)
- PayPal and eBay go up to $300 each.
- Bank account offered for a price ranging from $200 and $500).
- Document scans from $10 to $35 per document. (Trend Micro)
- Credit card fraud CVVs ($3-$25), Dump ($20-$60), Fullz ($25-$125)

Product Pricing List Sample

Credit Card's Country of Origin	Description	Price
Canada	Visa/Mastercard	$11–15 per number
	Amex/Discover	$22–28 per number
	Full	$35–50 per fullz
United States	Visa/Mastercard	$5 per number
	Amex/Discover	$8 per number
	Full	$25 per fullz
United Kingdom	Visa/Mastercard	$30 per number
	Amex/Discover	$38 per number
	Full	$53 per fullz
Israel	Full	$33 per fullz
Russia	Full	$25 per fullz
Turkey	Full	$18 per fullz

- Counterfeit documents, including non-US passports, from $200 to $1000. Fake US driver's licenses run for $100-$150, meanwhile counterfeit Social Security cards run between $250 and $400 on average.

Black Markets

Services - Pricing List

- *Hacking services*
  - ✓ Social media account hacking $50-$100 (FB, Twitter, etc.)
  - ✓ Remote Access Trojan $150-$400 (FB, Twitter, etc.)
  - ✓ Banking Malware Customization (i.e. Zeus source code) $900 - $1500
  - ✓ Rent a botnet for DDoS attack (24 hours) $900 - $1500

- *Carding*
- *Money Laundering Services*
- *Assassinations services*
- *Training and Tutorials*

Hacking	
Hacking web server (vps or hosting)	USD 250 (1,04 BTC at the time I'm writing)
Hacking personal computer	USD 200 (0,83 BTC at the time I'm writing)
Hacking Social Media Account (Facebook, Twitter)	USD 300 (1,25 BTC at the time I'm writing)
Gmail Account Take over	USD 300 (1,25 BTC at the time I'm writing)
Security Audit	
Web Server security Audit	USD 400 (1,66 BTC at the time I'm writing)
Malware	
Remote Access Trojan	USD 150 – 400 (0,62 – 1,66 BTC at the time I'm writing)
Banking Malware Customization (Zeus source code)	USD 900 (3,75 BTC at the time I'm writing)
DDoS attack	
Rent a botnet for DDoS attack (24 hours)	USD 150 – 500 (2,08 – 1,66 BTC at the time I'm writing)

Black Markets

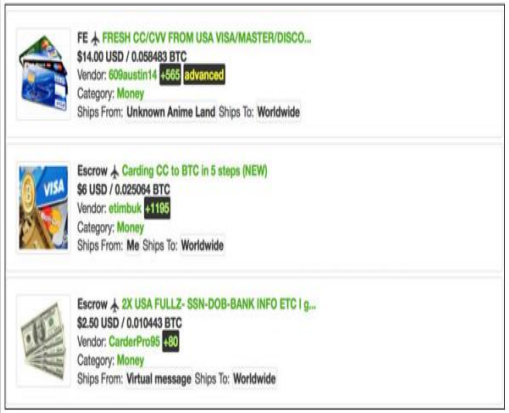
Most active criminal underground communities

Offering	Price
Classic US-issued credit card credentials	US$19–22 (100 sets)
Gold, Platinum, or Business US-issued credit card credentials	US$36–42 (50 sets)
Classic Canada-issued credit card credentials	US$47–50 (40 sets)
Gold, Platinum, or Business Canada-issued credit card credentials	US$50–65 (35 sets)
Fake US-issued credit card (physical)	US$210–874

Table 3: *Credit-card-related offerings in the North American underground*

Country	Selling price	Number of accounts for sale
Credit cards		
Japan	US$14–78 (Average: ~US$60)	207
US	US$2–84 (Average: ~US$7)	126,707
Brazil	US$6–10 (Average: ~US$8)	17,385
UK	US$8–61 (Average: ~US$8)	28,336
Canada	US$3–60 (Average: ~US$16)	36,423

Russian Cybercriminal Underground Market Product Offerings			
Product	**2011 Price**	**2012 Price**	**2013 Price**
Credit card credentials (per card):			
• American	US$2.50	US$1	US$1
• Australian	US$7	US$5	US$4
• Canadian	US$5	US$5	US$4
• German	US$9	US$7	US$6
• British	US$7	US$6–8	US$5



Black Markets

A successful Business Model

2012

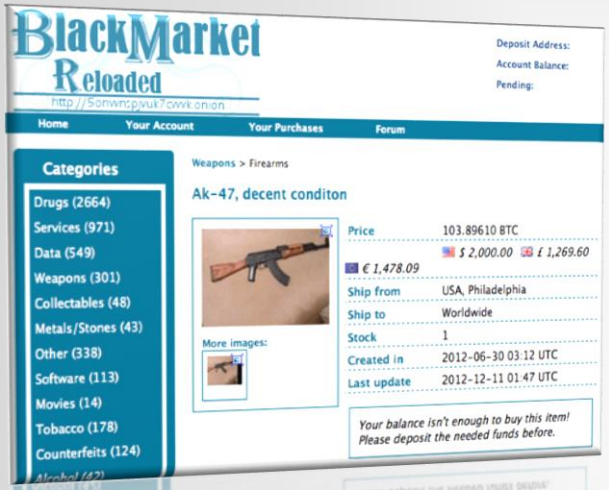
- Silk Road realized $22 Million In Annual Sales only related to the drug market. (Carnegie Mellon 2012)
- USD 1.9 million per month Sellers' Total revenue
- Silk Road operators earned about USD 143,000 per month in commissions.

2015

- Principal Dark 35 marketplaces raked from $300,000 to $500,000 a day.
- About 70% of all sellers never managed to sell more than $1,000 worth of products. Another 18% of sellers were observed to sell between $1,000 and $10,000 but only about 2% of vendors managed to sell more than $100,000

A paradise for scammers

The dark web is the reign of scammers.



- Many sellers claim to have products that will never send to buyers.
- Weapons are probably one of the goods that most of all suffer this kind of problems.
- Producers from the German broadcaster ARD tried to buy an AK-47 rifle, they paid $800 worth of bitcoin, but never received it.

- The site offers "hitman" services and act as between customers and killers to hire.
- The truth behind the popular hitman service was clear after the website was hacked and data leaked online.
- "These guys have made at least 50 bitcoins [nearly $23,000]" (Chris Monteiro)

Defferences within Criminal Underground

Characterization of the criminal underground

Pedophilia

Pedos in the dark

- A study conducted by the University of Portsmouth revealed that over 80% of Tor network visits is related to pedo sites.
- The portion of Tor users who search for child abuse materials is greater that the one that use it to buy drugs or leak sensitive documents to a journalist.
- *"Unstable sites that frequently go offline might generate more visit counts. And sites visited through the tool Tor2Web, which is designed to make Tor hidden services more accessible to non-anonymous users, would be underrepresented. All those factors might artificially inflate the number of visits to child abuse sites measured by the University of Portsmouth researchers" said Tor executive director Roger Dingledine.*

Pedophilia

Pedophilia in the dark

- Trend Micro Research identified 8,707 "suspicious" pages. The analysis of the "Surface Web" sites that those sites linked to revealed that the majority of them fall into the following categories:
  - ✓ Disease vector (drive-by download) sites (33.7%).
  - ✓ Proxy avoidance sites (31.7%).
  - ✓ **Child exploitation (26%)**.
- Diffusion of Pedo material in the Deep Web is anyway serious phenomenon.

Terrorism

Terrorists in the Dark Web

- The Dark Web is difficult to monitor for intelligence agencies and it is not so easy to de-anonymize members of terrorist organizations.

Izumi Nakamitsu, chief of UN's Disarmament Affairs stated:

- The dark web is as the primary enabler of easing access to WMDs.

- Terrorist groups can now trade and collaborate over the dark web and make illegal dealings without being noticed by authorities.

- Propaganda
- Purchasing wepons
- Purchasing stolen card data
- Counterfeit documents
- Recruiting
- Download Mobile Apps used for secure communications
- Purchase of malicious code
- Fund-raising (??)
- Doxing

The response of the law enforcement.

We are going in the dark

- (Dec. 22nd, 2014) In a court case the investigators were informed about the usage of an FBI's "Network Investigative Technique" (NIT) to deanonymize suspects while exploiting Tor network. The NIT allowed them to identify the IP address of TOR users.

- Law enforcement relied on the popular Metasploit framework to first de-anonymize operators of child porn websites in the Tor network.

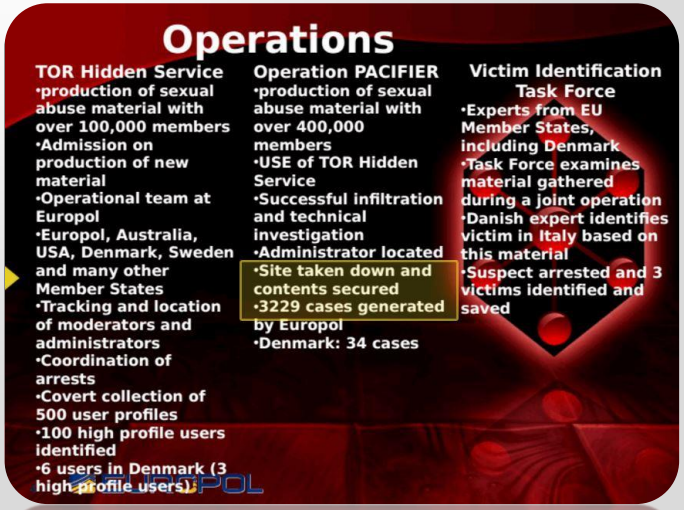
- The operation is coded Operation Tornado and the FBI relied upon an abandoned project of Metaploit dubbed the "Decloaking Engine" to de-anonymized users in the 2012.

- *"The NIT was a Flash based application that was developed by H.D.Moore and was released as part of Metasploit. The NIT, or more formally, Metaspolit Decloaking Engine was designed to provide the real IP address of web users, regardless of proxy settings." states the forensic report.*

The response of the law enforcement.

Operation Onymous

- Operation Onymous (On 5 and 6 Nov. 2014) – Law enforcement around the globe conducted a joint action against dark markets on Tor networks.
- Over 400 websites were shut down including black markets on Tor network (Silk Road 2.0, Cloud 9 and Hydra), *17 vendors and administrators behind 410 hidden services were arrested.*
- $1 million in Bitcoin was seized, along with €180,000 in cash, gold, silver and drugs.



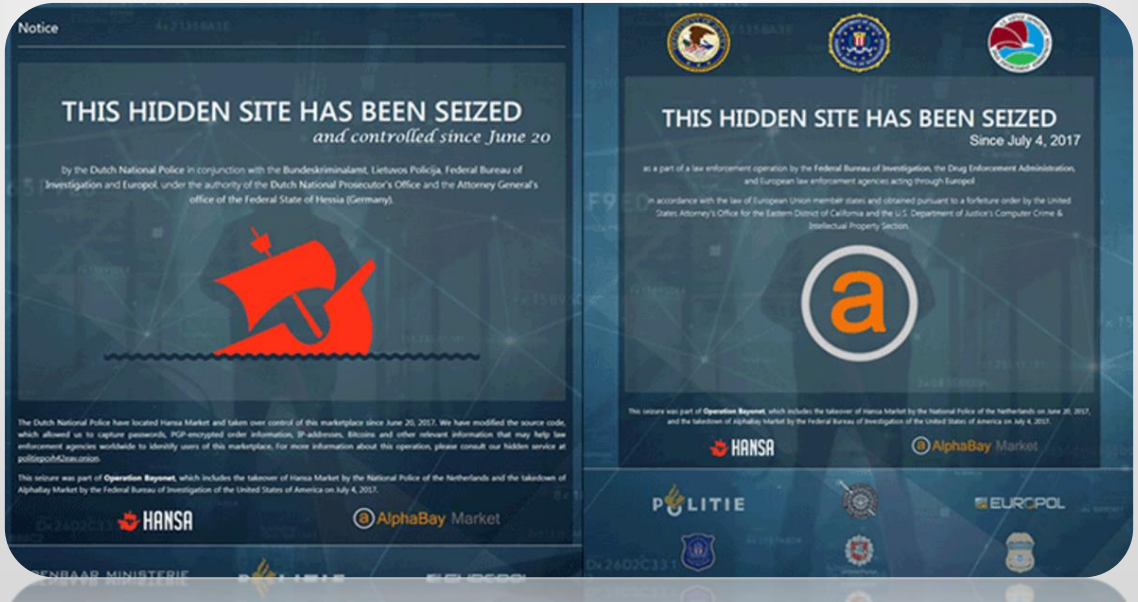
- Operation Pacifier is the FBI massive hacking campaign on computers worldwide (2015).
- The web child porn website under investigation was Playpen hosted on the Tor Network.
- The FBI was able to harvest around 1300 IPs

The response of the law enforcement.

Police shut down Hansa and AlphaBay

2017 - Huge blow to the criminal underground in the dark web, authorities shut down AlphaBay and Hansa black marketplaces

In a coordinated International operation, Europol along with FBI, US DEA and Dutch Police have seized and taken down AlphaBay and HANSA black markets.



DeAnonymizing the cyber crime on Tor

Operation Onymous

- Security experts hypothesized that law enforcement has exploited one of the following scenarios:
  - ✓ Lack of Operational Security of hidden services.
  - ✓ Exploitation of bugs in the web application.
  - ✓ Bitcoin de-anonymization.
  - ✓ Attacks on the Tor network (i.e. Traffic Analysis Correlation attacks).

- The number of black markets seized by law enforcement led to speculation that a weakness in the Tor network had been exploited.

- Andrew Lewman, a representative of the not-for-profit Tor project, excluded it by suggesting that execution of traditional police work such as following Bitcoins was more likely.

Law enforcement

New dedicated cyber units

Dec. 2014 - Prime Minister Cameron announced that a newborn cyber unit composed by officials from GCHQ and NCA will fight online pedophiles even in the Deep Web.

Interpol's Cyber Research Lab completed the first training program, as part of the course the participant built its own private "Darknet" network simulating the management of an underground marketplace.

Law enforcement

New dedicated cyber units

- July 2016 - David S., the Munich gunman has purchased the weapon on the Dark Web
- August 2016 - The German Government announced last week the creation of a new cyber security unit named ZITiS to tackle terrorists online in a wake of terror attacks.
- The ZITiS will be also focused on the monitoring of the Dark Web, the staff of the new cyber units will include experts in the monitoring of "darknet."
- The experts are concerned about the abuses of Darknets, terrorists could exploit them to cover communications or to acquire illegal weapons.

About me

About Pierluigi Paganini:

Pierluigi Paganini is Chief Technology Officer at CSE - CybSec Enterprise SpA.
Pierluigi Paganini is a member of the ENISA (European Union Agency for Network and Information Security))Threat Landscape Stakeholder Group, member of Cyber G7 Workgroup of the Italian Ministry of Foreign Affairs and International Cooperation, Director of the Master in Cyber Security at the Link Campus University.
He is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing, and a strong belief that security is founded on the information sharing lead Pierluigi to launch the security blog "Security Affairs" recently awarded as the Best European Personal Security Blog.
Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

Ing. Pierluigi Paganini

Chief Technology Officer CSE - CybSec Enterprise SpA. Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co

pierluigi@csecybsec.com


Thank you