



Darkweb, a look back at 2015 events and 2016 predictions

December 28, 2015 By Pierluigi Paganini



Which are the main events observed in the darkweb during the 2015 and what to expect in the next 12 months?

The DarkWeb is a 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. The same term is used to indicate a set of private content exchanged in a closed network of computers for file sharing.□

A Darknet like the Tor network is so popular in the criminal ecosystem due to the anonymity it offers under specific conditions, law enforcement, and intelligence agencies face difficulties in de-anonymizing users and are not able to conduct a large-scale monitoring.

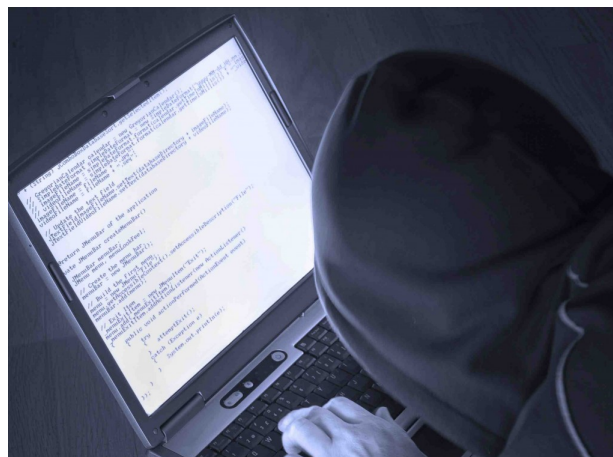
In 2015 the Darknet, and in particular the **black markets** assumed a crucial role in the **criminal underground**, it worked as an aggregator for the principal underground communities.

exploited the anonymity of this part of the web to launch attacks against computer hardware and software, to conduct financial crimes and for **child pornography**.

Malware authors and botmasters have exploited **darknets** like the Tor Network and I2P to hide the Command and Control infrastructure.

Critroni, **Cryptowall**, **Vawtrak** and **Dyre** just a few samples of malware that exploit the Darknet to hide their control infrastructure.

Another phenomenon linked to the development of malware that exploit the darknet is the increase of the threat actors that started offering product and services to advantage the development and the deployment of malware.



In the **criminal underground** it is easy to find malware-construction kits that allow easy to build malicious code from existing templates. In May experts at McAfee discovered a sort of easy to use **Ransomware** builder, this family of malware is becoming even more popular in the criminal ecosystem and crooks are trying to capture this opportunity.

The ransomware-construction kits, dubbed **Tox**, was available online for free in the Dark Web since May 19.

Apart the sale of drugs, in 2015 we have assisted in the rapid growth of hacking communities in the darknet which were specialized in the sale of product and services for payment card frauds, in the sale of stolen data and hacking services and tools.

The most active underground communities were the Russian one, the US one, the Brazilian one, the Chinese one and also the emerging Japanese one.

Below a list of products/services offered in the principal black markets:

- PII record for \$1. (Trend Micro)
- PayPal and eBay go up to \$300 each. (Trend Micro)
- Bank account offered for a price ranging from \$200 and \$500 per account (balance, history).
- Document scans from \$10 to \$35 per document. (Trend Micro)
- Credit card fraud CVVs (\$3-\$25), Dump (\$20-\$60), Fullz (\$25-\$125) [*Data Preview -Annual Card Fraud Report IT Ministry of Treasury and Finance*]
- 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.
- 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

Giving a look to the principal 35 black marketplaces, security experts observed that they 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.

But 2015 is considered the year of the terrorism, the ISIS terror is dramatically increased its power becoming the principal threat for the Western countries. The members of the IS exploited the **darkweb** to share videos and images for propaganda.

Hidden services were also used as repository of mobile apps used by the jihadists to communicate securely.

What to expect in the next 12 months?

Darkweb will continue to be a privileged environment for cyber criminal groups and terrorists.

Malware authors will exploit the Darknets basically as a backup mechanism for their botnet and to make them more resistant to various kinds of attacks operated by law enforcement.

The most interesting trend we will observe related to the growth of **criminal-as-a-service** model that will attack organized crime in the cyber criminal underground.


Pierluigi Paganini

(Security Affairs – Gomasom Ransomware, malware)

Share it please ...   
    

1. Cyber Crime Course



 Hacking malware cyber terrorists

Crime-as-a-Service criminal underground

ISIS Darkweb

SHARE ON





Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, 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 sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS
ARTICLE

**The Ramnit Botnet is
back after the law
enforcement takedown**

NEXT ARTICLE

**CVE-2015-8562 -
16,000 Daily
Attacks on
vulnerable Joomla
servers**

YOU MIGHT ALSO LIKE

Turkish hackers took over a Russian
Govt Instagram account

January 3, 2016 By Pierluigi Paganini

@FFD8FFDB Twitter bot spies on
poorly configured cameras

January 3, 2016 By Pierluigi Paganini



1. Cyber Crime Course



2. Cyber Criminals



3. Ticket Prices



4. Music Clubs



5. Acoustic Guitarist



◦ +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group,

he is also a Security Evangelist,
Security Analyst and Freelance Writer.
Editor-in-Chief at "Cyber Defense
Magazine".



1. Cyber Crime Course 

2. Cyber Criminals 

3. Ticket Outlets 

4. Local Music Events 

5. Music Group 

6. Live Performance 

7. Main Event 

8. Best Music Clubs 