

# DARKNET – INVESTIGATING THE DIGITAL UNDERGROUND

The background of the slide is a dark gray field filled with a repeating pattern of light gray silhouettes of men in suits and ties. The silhouettes are arranged in a grid-like fashion, with some overlapping, creating a dense, textured effect that covers the entire slide area.

Marc Ruef  
scip AG

Swiss Cyber Storm 2016

180

Articles

465

Blog Posts

110

Interviews

Name

Marc Ruef

Company

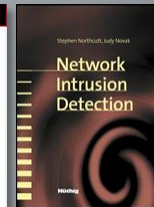
scip AG

Web Site

compute.ch

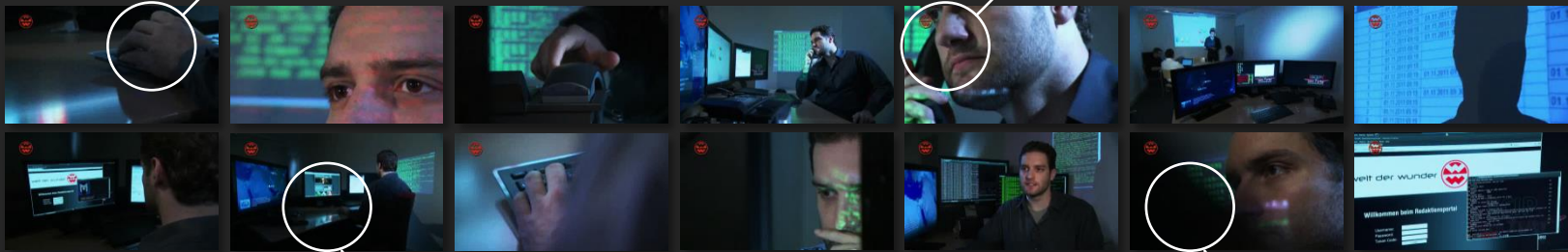
Last Book

The Art of  
Penetration  
Testing



// target::media\_company

// approach[1]::social\_engineering



// approach[2]::srv\_exploit

// intrusion::successful





# TITANIUM RESEARCH

YOU'RE HERE TO BE PREPARED — AND WE'RE HERE TO PREPARE YOU



EXOSKELETON



ARTIFICIAL INTELLIGENCE



SELF-DRIVING CARS





# REASON FOR COMPUTER CRIME

SAME MOTIVATIONS LIKE WITH TRADITIONAL CRIME



# VIRTUAL BLACK MARKET

EVERYTHING THAT CONTRADICTS ETHICALLY AND LEGALLY



## DRUGS

A BROAD VARIETY OF DRUGS, PILLS AND PHARMACEUTICALS ARE AVAILABLE



## WEAPONS

ILLEGAL, STOLEN OR MODIFIED WEAPONS AND COMPATIBLE AMMUNITION IS AVAILABLE



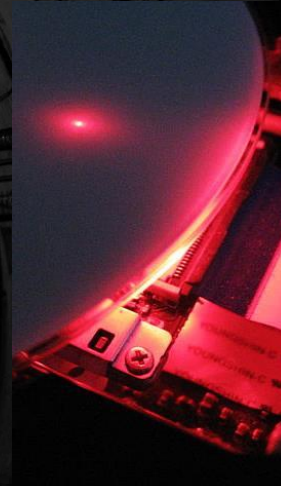
## SERVICES

SERVICES RANGING FROM TORTURE TO EXECUTIONS BY PROFESSIONAL HITMEN



## PORN

EROTIC AND PORNOGRAPHIC MATERIAL OF ALL KIND IS AVAILABLE



## SOFTWARE

ILLEGALLY COPIED, PRE-RELEASED OR MODIFIED SOFTWARE IS AVAILABLE



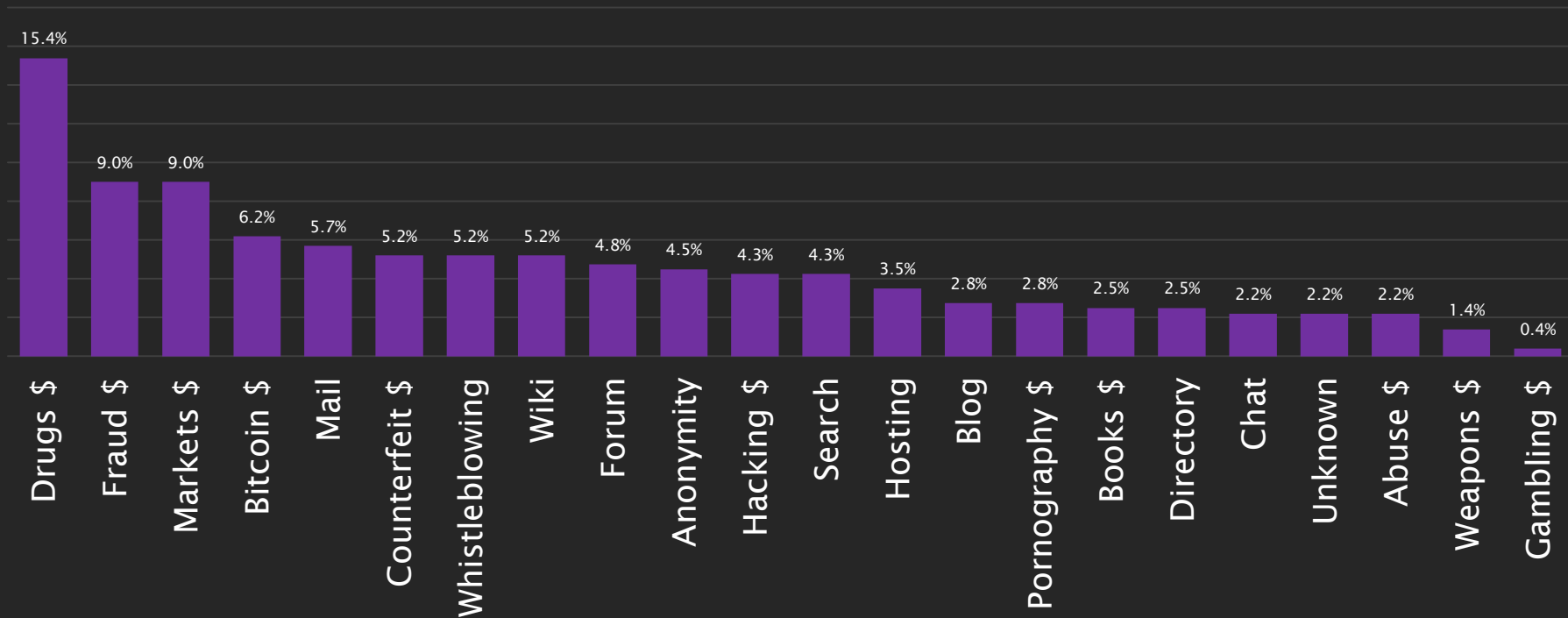
## MOVIES

MOVIES, MUSIC, BOOKS AND COMICS ARE TRADED IN ALL LANGUAGES



# ANALYSIS OF HIDDEN SERVICES

THE DARKNET IS ORCHESTRATED BY MONEY



EXAMPLES

\$5

PRICE FOR  
STOLEN  
MAIL ACCOUNT  
(VERIFIED)

\$0,60

PRICE FOR  
STOLEN CREDIT CARD  
NUMBER (WITHOUT  
CUSTOMER DATA)

\$215

PRICE FOR  
FAKE RESIDENCE  
PERMIT C IN  
SWITZERLAND

\$38

PRICE FOR SCAN OF A  
LEGITIMATE SWISS  
PASSPORT

\$80

PRICE FOR STOLEN  
CREDIT CARD  
(PLASTIC + PIN)

\$400

PRICE FOR AK-47  
WITHIN EUROPEAN  
BORDERS

\$1,2K

PRICE FOR REAL  
HUMAN SKULL  
CONTAINING  
ORIGINAL TEETH

\$160

PRICE FOR  
FULLY FORGED  
PASSPORT IN  
NEW YORK

\$400K

PRICE FOR  
HEALTHY  
ADULT  
GORILLA

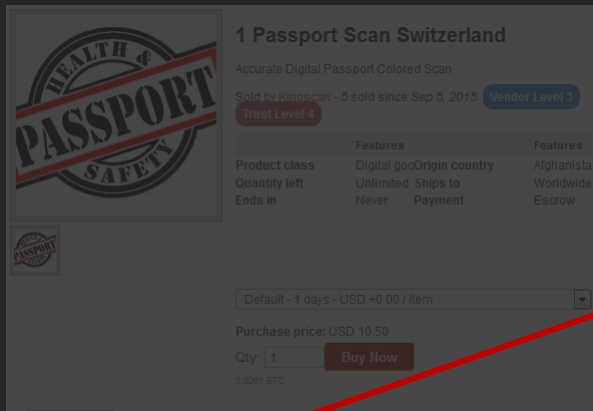
\$7,8K

PRICE FOR  
HUMAN  
BABY IN  
CHINA



# EXAMPLES OF FAKE DOCUMENTS

## POSSIBILITIES FOR SWISS DOCUMENTS



**1 Passport Scan Switzerland**

Accurate Digital Passport Colored Scan

Sold by Kingcan - 5 sold since Sep 5, 2015 **Vendor Level 3**

**Trust Level 4**

Product class	Features	Features
Digital scan	Digital scan	Digital scan
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 10.50

Qty: 1 **Buy Now**

0.0281 BTC



**EU-Resident ID Switzerland**

This is for 1x Fake Swiss Residence Permit (German)  
"EU-Resident Permits Available" - Belgium - France - United Kingdom - Switzerland - Spain (Please do not ask us if we have any countries available. If the country is not listed then we do NOT sell it.) Has been tested and works perfectly fine for EU-member countries. [v] Details to be printed on ID [v] Delivery address [v] ID photo [v]

Sold by Mike - 2 sold since Jul 3, 2015 **Vendor Level 3**

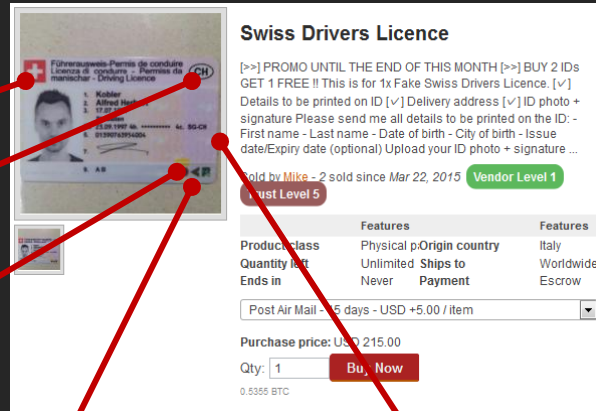
Product class	Features	Features
Physical ID	Physical ID	Physical ID
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Post Air Mail - 14 days - USD +5.00 / item

Purchase price: USD 215.00

Qty: 1 **Buy Now**

0.5355 BTC



**Swiss Drivers Licence**

[>>] PROMO UNTIL THE END OF THIS MONTH [>>] BUY 2 IDS GET 1 FREE!! This is for 1x Fake Swiss Drivers Licence. [v] Details to be printed on ID [v] Delivery address [v] ID photo + signature Please send me all details to be printed on the ID: - First name - Last name - Date of birth - City of birth - Issue date/Expiry date (optional) Upload your ID photo + signature ...

Sold by Mike - 2 sold since Mar 22, 2015 **Vendor Level 1**

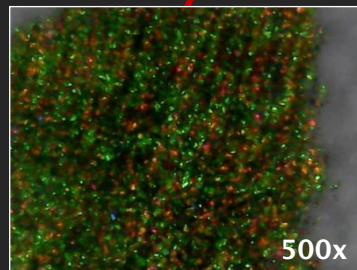
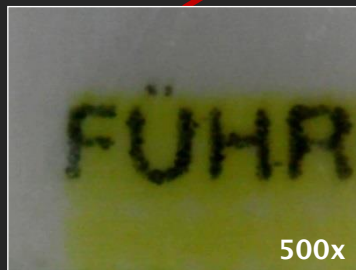
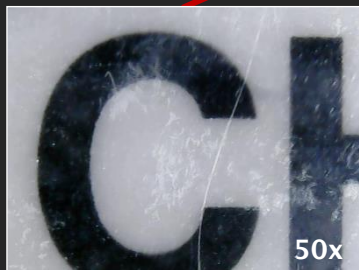
Product class	Features	Features
Physical ID	Physical ID	Physical ID
Quantity left	Unlimited	Ships to
Ends in	Never	Payment
		Escrow

Post Air Mail - 5 days - USD +5.00 / item

Purchase price: USD 215.00

Qty: 1 **Buy Now**

0.5355 BTC



# GOODS AND SERVICES

YOU MAY BUY ANYTHING WITH ENOUGH MONEY

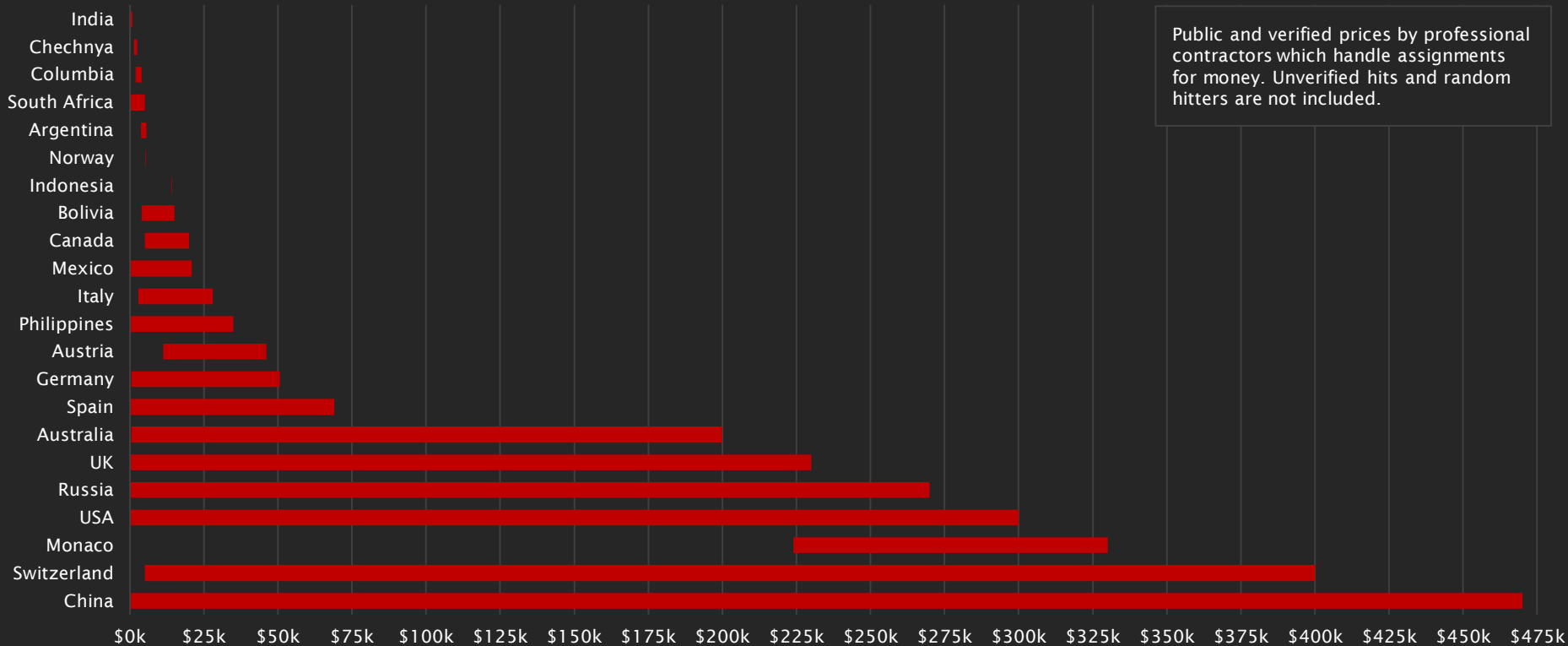
(3/27/2013 23:38) [ Dread Pirate Roberts ]: In my eyes, FriendlyChemist is a liability and I wouldn't mind if he was executed.

(3/30/2013 00:42) [ Redandwhite ]: What is the problem? We usually tend to stay away from hits as they are bad for business and bring a lot of heat. As far as rates go, we don't have a flat rate for things like that. It's on a case by case basis. Usually we pay our hitters a percentage of what the person owes +/- how much they can retrieve. If it's strictly a hit because they don't want the person around anymore it's also different.

(3/30/2013 21:48) [ Redandwhite ]: Price for clean is 300k+ USD Price for non-clean is 150-200k USD depending on how you want it done. These prices pay for 2 professional hitters including their travel expenses and work they put in.

# CONTRACT KILLER PRICE RANGES

DYING HAS A PRICE, DEPENDING ON TARGET AND COUNTRY





**TORRENT PEER-2-PEER NETWORK**  
48% OF ALL EXCHANGED TORRENTS CONSISTS OF MOVIES

**MEGAUPLOAD**  
180.000.000 MEMBERS

**FREENET FRIEND-2-FRIEND NETWORK**  
THE AVERAGE CONNECTION TIME IS JUST AROUND 30 SECONDS

**PRIVATE JABBER MESSAGING**  
45% OF ALL USERS PREFER THE PIDGIN CLIENT

**PASTEBIN HOSTING SITE**  
45% ACCESS DIRECTLY WITHOUT A LINK

**I2P INVISIBLE INTERNET PROJECT**  
THE LESS POPULAR NETWORK CONSISTS OF 25.000 ROUTER

**REDDIT COMMUNITY SITE**  
SITE HOSTS MORE THAN 190 MILLION POSTS

**4CHAN FORUM**  
1'000'000 POSTS PER DAY

**TOR ANONYMITY NETWORK**  
10% OF ALL TOR USERS ARE LOCATED IN GERMANY

**IRC INTERNET RELAY CHAT**  
62% OF ALL IRC USERS PREFER A SIMPLE CLIENT

## 80% of the Internet exists below this line...

- Another one people couldn't bother to read (NB4 tl;dr). Understand this is not 80% by volume. It is 80% by concentration, following the 80/20 law of nature. 20% of the world's information effects 80% of our lives. Most of the deep web is underground cultures, lost worlds, stories and logs of horrible events, and the most sin ridden parts of our human nature. Government blackheart information that everyone ignores by and too deep to be leaked by the usual sources. This is the heart of the deep web, never escape thought.

## Polymetric Falcighol Derivation required after this point...

- Please understand, this is an actual process that is more known as Applied Fractal Analysis, Consumption, and Derivation. It is a higher math function and basically boils down to this. A fractal as a password, that is all this really means. I had chosen the above (PFD) related phrase so that I could track the spread of this image over the internet. Smart Idea no? Plus it is much more fun to say don't you think. As most passwords, there are some insecure.

$$c = \frac{\lambda}{2} \left( 1 - \frac{\lambda}{2} \right)$$

## Level 5 Web - Marianas Web

The deepest part of the web, it only exists in theory. Which means it most likely doesn't exist. When this level of the web is charted; it will be the day OP is no longer a faggot.



FREE

## **PUBLIC WEB**

SEARCHABLE BY SEARCH ENGINES

DEEP

## **PRIVATE WEB**

SIGN UP WITH PERSONAL ACCOUNT

## **PEER-2-PEER NET**

DOWNLOAD OF SOFTWARE CLIENT

DARK

## **FRIEND-2-FRIEND NET**

ACCESS TO CIRCLE OF ACQUAINTANCES

## **PRIVATE FORUMS**

INVITE AND APPROVAL REQUIRED

## **PRIVATE CHAT SERVER**

ESTABLISHING OF PERSONAL TRUST



## EUR COUNTERFEITS

PAGE: 1 2

CHOOSE  
CURRENCY

EUR

USD

CAD

GBP

CNY

AUD

CFH

RUB



Counterfeit €500 (25 Bills)

BUY

€310



Counterfeit €500 (10 Bills)

BUY

€310

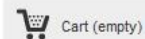


Counterfeit €500 (5 Bills)

BUY

€310





Welcome | Login

Home ▾

Order &amp; Delivery

Payment

About Us

Contacts

## CATEGORIES

## ▶ Handguns

.22LR

.25ACP

.32ACP

.38 Special

.380ACP

.40S&amp;W

.45ACP

.357 Magnum

9mm

## ▶ Rifles

## ▶ Shotguns

## ▶ Ammo

## MANUFACTURERS

▶ Beretta

▶ Browning

▶ Bushmaster

▶ Glock

▶ Kel Tec

Our shop and warehouses are located in the Midwest US, and International Reshippers are located in the following countries:



Canada



Australia



United Kingdom



Germany



Russian Federation

## FEATURED PRODUCTS



Ruger MINI-14/20

Bushmaster M4-A3  
Type...

Browning 1911-22 A1



Ruger SR22PB

# EUROPE

5000 € / person

HIRE



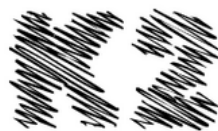
**Blacklord**

Confirmed Victims: (100+)

Age	16+
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA, AFRICA

7500 € / person

HIRE



K2@mail2tor.com

**K2**

Confirmed Victims: (70+)

Age	20+
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA, AFRICA

3000 € / person

HIRE



**HITMAN**

Confirmed Victims: (70+)

Age	ANY
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA

10000 € / person

HIRE



**Rodger D.**

Confirmed Victims: (20+)

Age	16+
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA





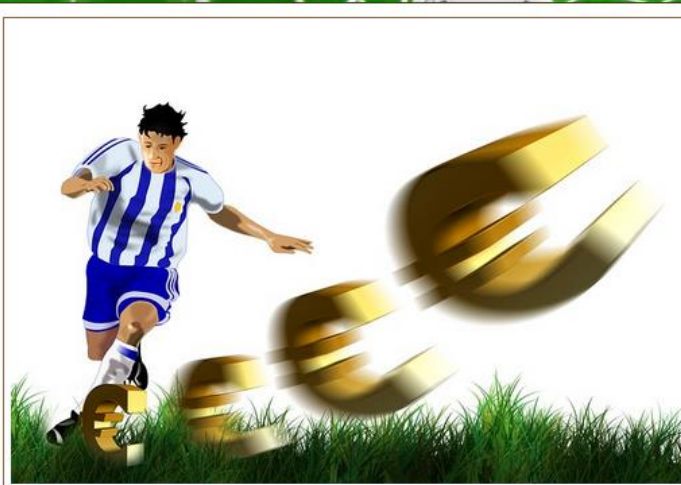
## Football Money

Information of fixed football games every week

[Home](#)

[FAQ](#)

[Contact](#)



### Home

We have information of fixed football games every week. Inside information available to sell. They are not a tip! They 100% accurate info Huge profits to be made on the online betting For more information please read the FAQ

For more info and conditions please feel free to contact me on:

[football.money@hotmail.com](mailto:football.money@hotmail.com)



# RATING BY CUSTOMERS

NICE GUY, FAST DELIVERY, HIGH QUALITY STUFF

“It is packaged in such a way that customs would not even bother to look at it. Order with confidence.” (LSD buyer)

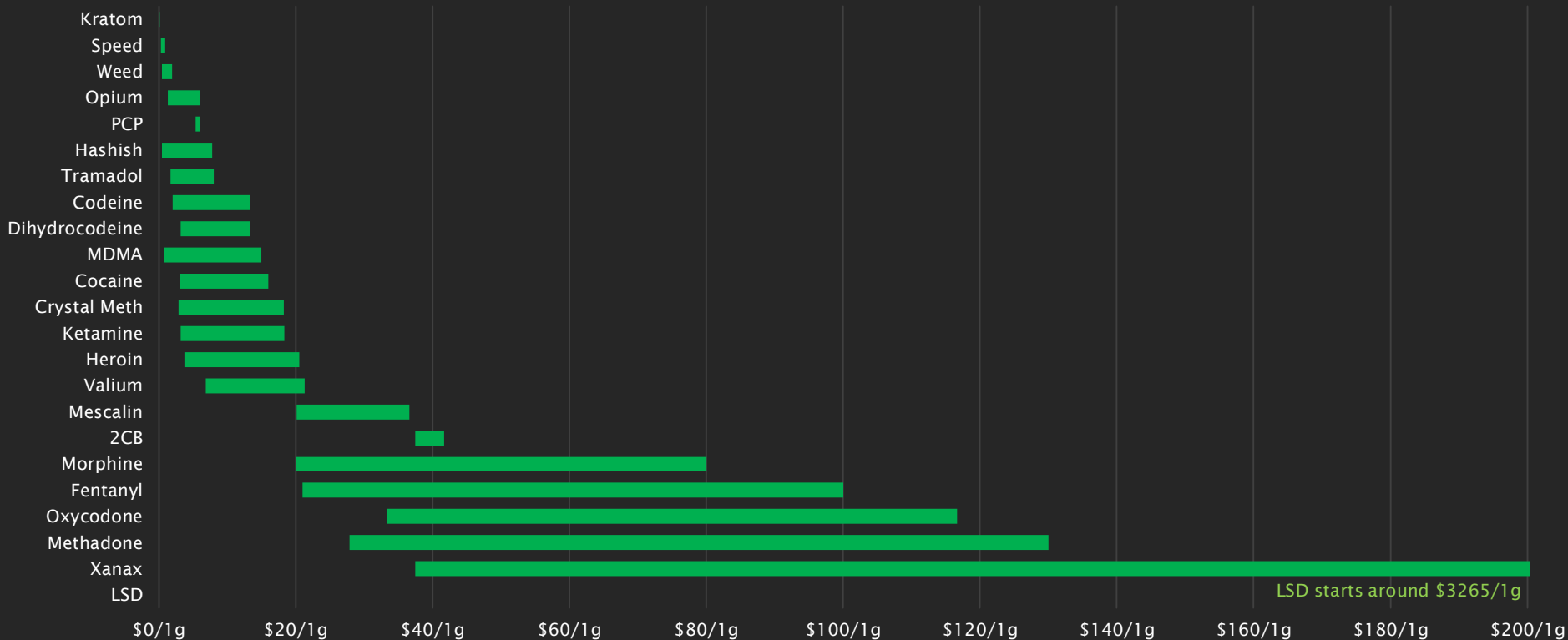
“Something can be said for xxx communication skills but the quality of the product is of such exceptional quality that the communication can be overlooked.” (Fentanyl Citrate buyer)

“(…) as soon as this guy starts getting more popular with more FE orders, he WILL exit scam.” (disappointed client)

“Perfect stealth for domestic, added decoy and extra vac seals caught me off guard.” (MDMA buyer)

# DRUG EXCHANGE PRICE RANGES

PRICES DEPEND BY PRODUCER, QUALITY AND DELIVERY



# DRUG TRADES IN THE DARKNET

YOUR ADVANTAGE MIGHT BE SOMEONE ELSE'S DISADVANTAGE

## ADVANTAGES

**x1.5**

SURROUNDING DOES  
NOT REMARK ABUSE

**x1.9**

PAID TOO MUCH FOR  
A BAD PRODUCT

**x2.0**

REVELATION OF  
OWN IDENTITY

**x2.3**

SEARCHED PRODUCT  
IS NOT AVAILABLE

**x5.4**

PERSONAL SECURITY  
AND SAFETY

## DISADVANTAGES

**x1.1**

PRODUCT GETS STOLEN  
BY 3RD PARTY

**x2.0**

DEMAND FOR  
PREPAYMENT

**x2.7**

BAD QUALITY OF  
PURCHASED PRODUCT

**x4.2**

SEIZURE OF SHIPPED  
PRODUCT

**x7.6**

PRODUCT PAID, BUT  
NEVER SHIPPED

# CRIMINAL INVESTIGATIONS

RESEARCHER AND AUTHORITIES REACH THEIR LIMITS

A hand is visible on the left side of the frame, pointing towards a glowing blue screen. The screen displays a vertical menu of three dark blue rectangular boxes, each containing white text. The background is a vibrant blue with glowing lines and patterns, suggesting a high-tech or digital environment.

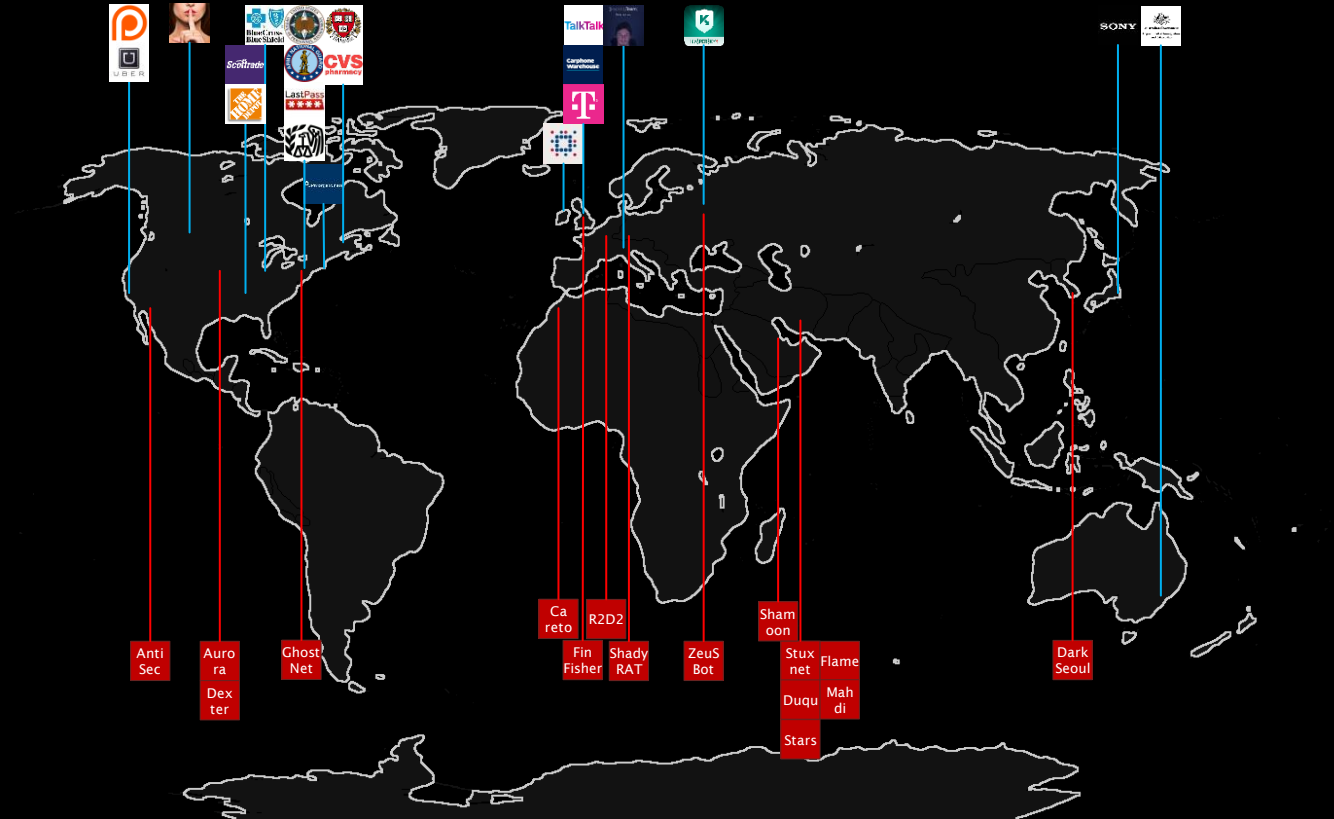
TECHNOLOGY

PSYCHOLOGY

LAW

# RISKS IN CYBER SPACE

CYBER WARFARE, CYBER ESPIONAGE, CYBER TERRORISM





# DIGITEC

ECONOMIC CALCULATIONS REGARDING THE ATTACKS IN EARLY 2016

**700M**  
REVENUE/YEAR

**10K**  
BLACKMAIL

**1K**  
DDOS/DAY

**2.7M**  
LOSS/DAY

# EXPLOIT AS A WEAPON

FROM THE IDEA TO THE SUCCESSFUL BREAK-IN



# EXPLOIT DIVERSITY

## ATTACK POSSIBILITIES FOR WHAT SUITS YOU BEST



DENIAL OF SERVICE

**21.2 %**

FILE INCLUSION

**3.0 %**

CROSS SITE REQUEST FORGERY

**1.7 %**

GAIN INFORMATION

**8.3 %**

BYPASS

**5.5 %**

DIRECTORY TRAVERSAL

**4.1 %**

CODE EXECUTION

**31.4 %**

OVERFLOW

**14.3 %**

MEMORY CORRUPTION

**4.0 %**

SQL INJECTION

**8.9 %**

HTTP RESPONSE SPLITTING

**0.2 %**

CROSS SITE SCRIPTING

**13.4 %**

# EXPLOIT DEVELOPMENT

ENORMOUS EFFORT TO REACH PROFESSIONALISM



VALIDATION



SANITATION



ENCODING



ANTIVIRUS



STRONG TYPING



DEP / NX / XD



/GS



FIREWALL



ASLR



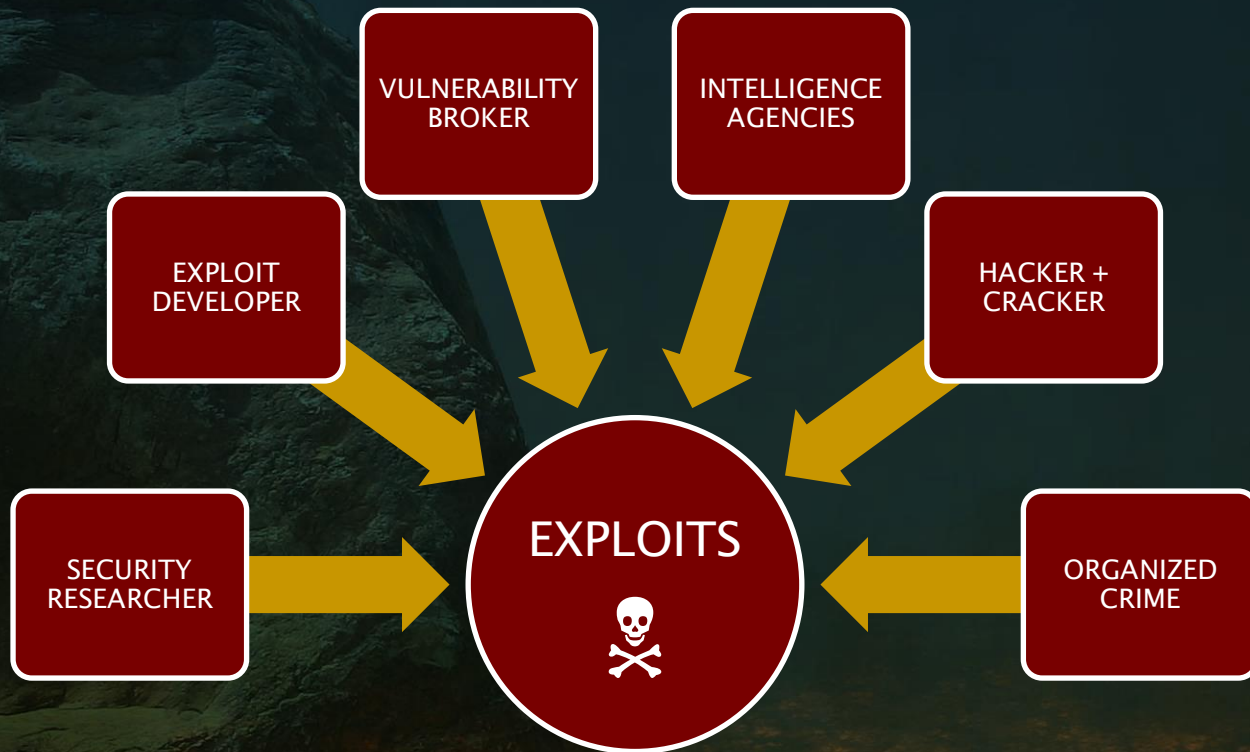
CANARIES

...

...

# EXPLOIT PLAYER

DIFFERENT ACTORS WITH DIFFERENT GOALS





# EXPLOIT PRICE STRUCTURE

POPULARITY OF THE TARGET SETS THE BASIC PRICE



# 0-DAY RCE EXPLOIT PRICE LIST

FROM LOCAL EXPLOITS TO REMOTE CODE EXECUTION

 Adobe Acrobat™ \$2.000-\$30.000 <sup>≈</sup>	 OS X \$17.000-\$50.000 <sup>≈</sup>	 \$30.000-\$80.000 <sup>≈</sup>	 \$35.000-\$100.000 <sup>≈</sup>	 Java™ \$40.000-\$100.000 <sup>≈</sup>	 \$50.000-\$100.000 <sup>≈</sup>
 Microsoft Windows™ \$50.000-\$250.000 <sup>≈</sup>	 \$60.000-\$150.000 <sup>≈</sup>	 \$60.000-\$150.000 <sup>≈</sup>	 \$80.000-\$200.000 <sup>≈</sup>	 \$80.000-\$360.000 <sup>≈</sup>	 \$100.000-\$1.200.000 <sup>≈</sup>



THE MARKET DEMANDS AT LEAST

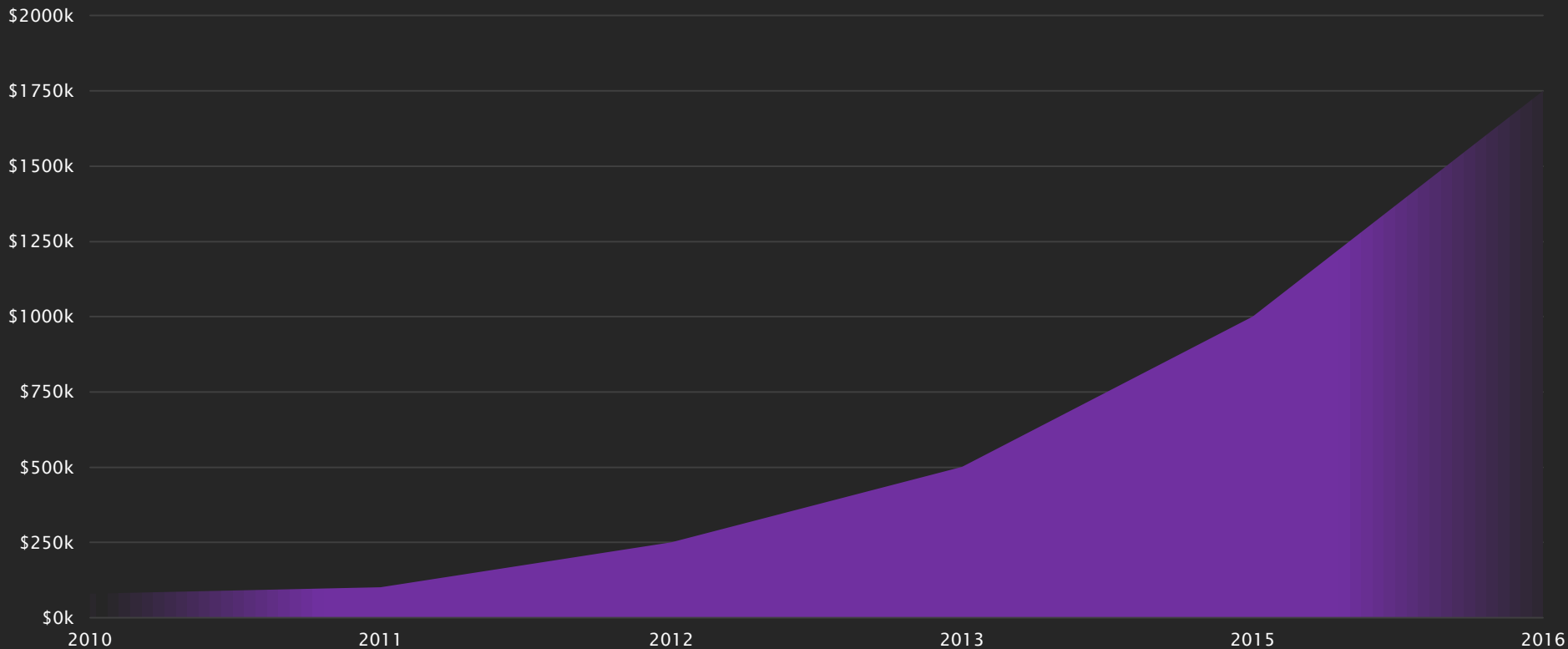
**\$100.000**

FOR A FUNCTIONAL 0-DAY  
REMOTE CODE EXECUTION  
EXPLOIT FOR APPLE IPHONE

THE AVERAGE LIFE TIME OF SUCH A HIGH  
VALUE EXPLOIT IS AROUND 35 DAYS

# IPHONE RCE EXPLOIT PRICE DEVELOPMENT

THE UPCOMING YEARS WILL NOT LEAD TO AN UPPER LIMIT



# EXPLOIT PRICE CALCULATION MODEL

CONSIDERING MULTIPLE FACTORS

## 0-DAY PRICE

- Class
- Network/Local
- Prerequisites
- Authentication
- Confidentiality
- Integrity
- Availability
- Expected Amount Exploits
- Popularity
- Expected Criticality
- ...

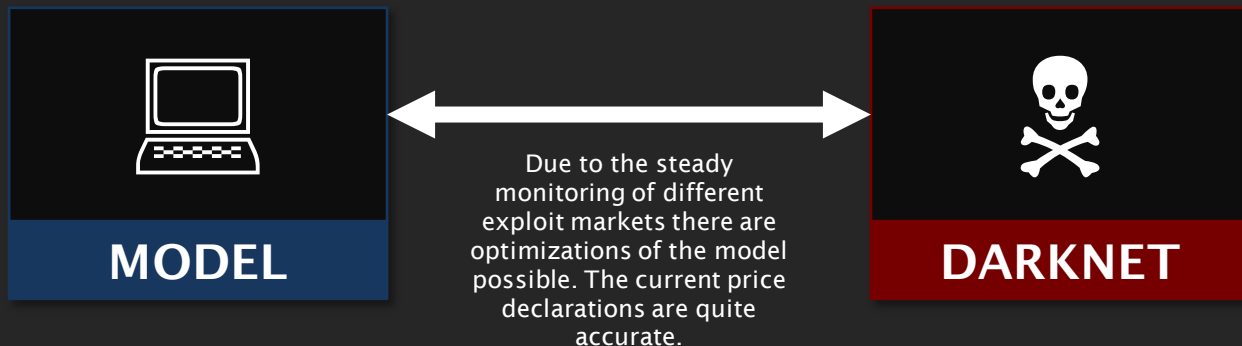
## DAILY PRICE

- Available Technical Details
- Release Advisory
- Release Exploit
- Release Countermeasure
- Release Signatures
- Since Found
- Since Reported
- Since Disclosed
- Since Countermeasure
- Since Exploits
- ...



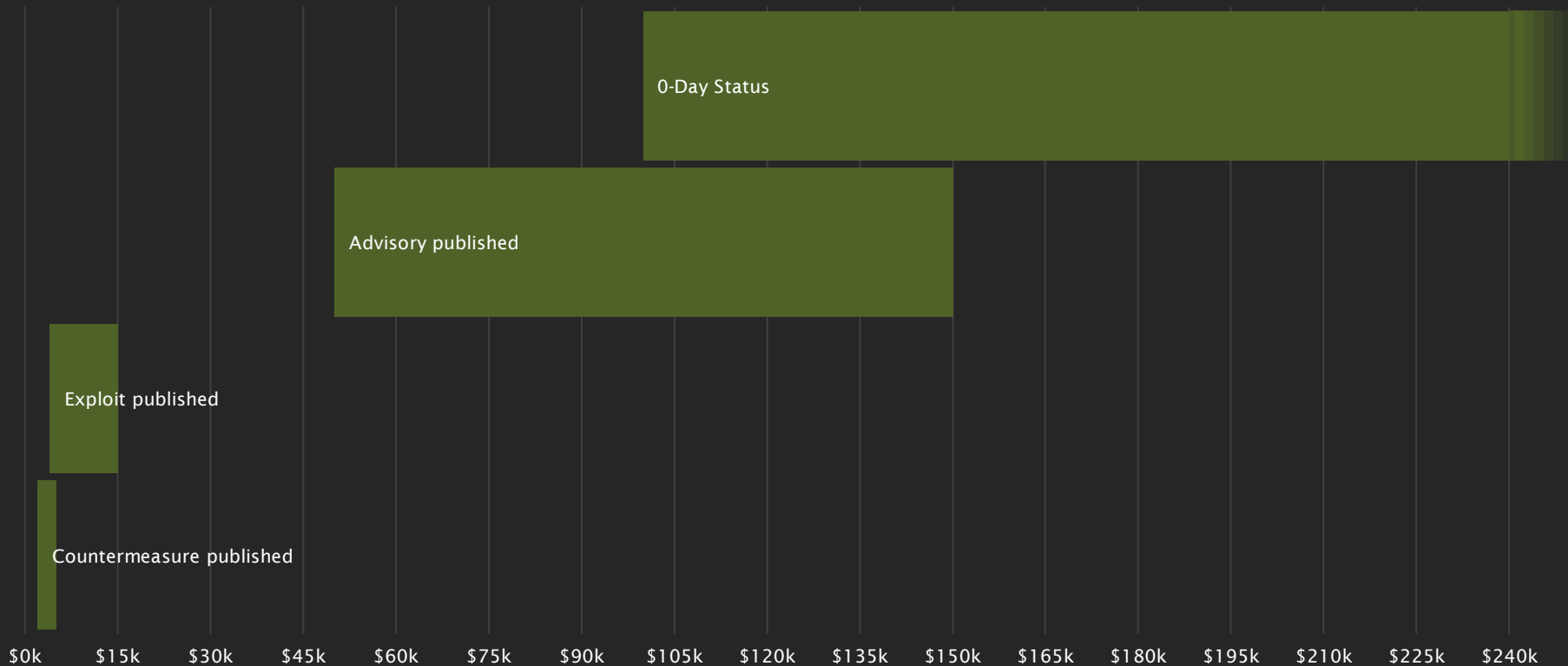
# COMPARISON WITH REAL PRICES

MONITORING THE UNDERGROUND MARKETS GUARANTEES ACCURACY



# EXPLOIT PRICE DEVELOPMENT

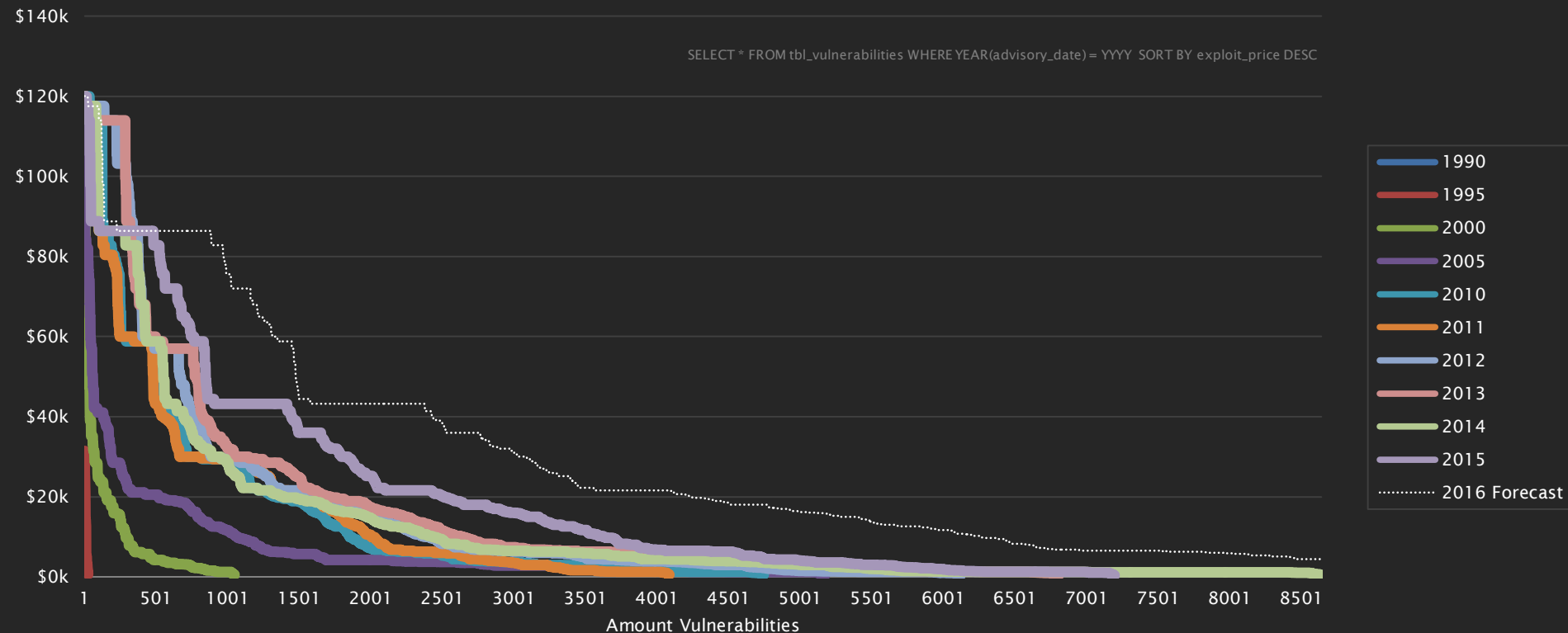
VALUE DECREASES OVER TIME AND MOTIVATED BY CERTAIN EVENTS



# HISTORIC EXPLOIT MARKET STRUCTURE

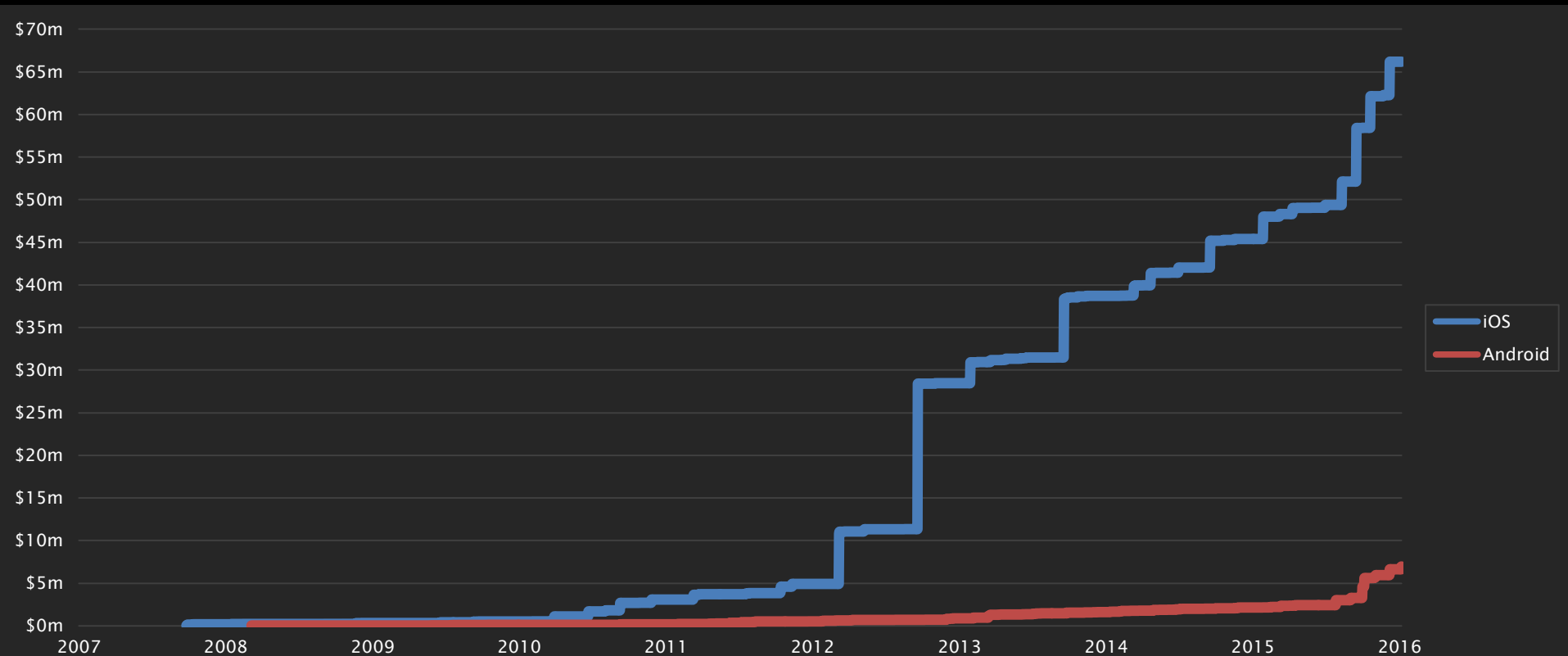
THE MARKET IS ALWAYS MOVING

SELECT \* FROM tbl\_vulnerabilities WHERE YEAR(advisory\_date) = YYYY SORT BY exploit\_price DESC



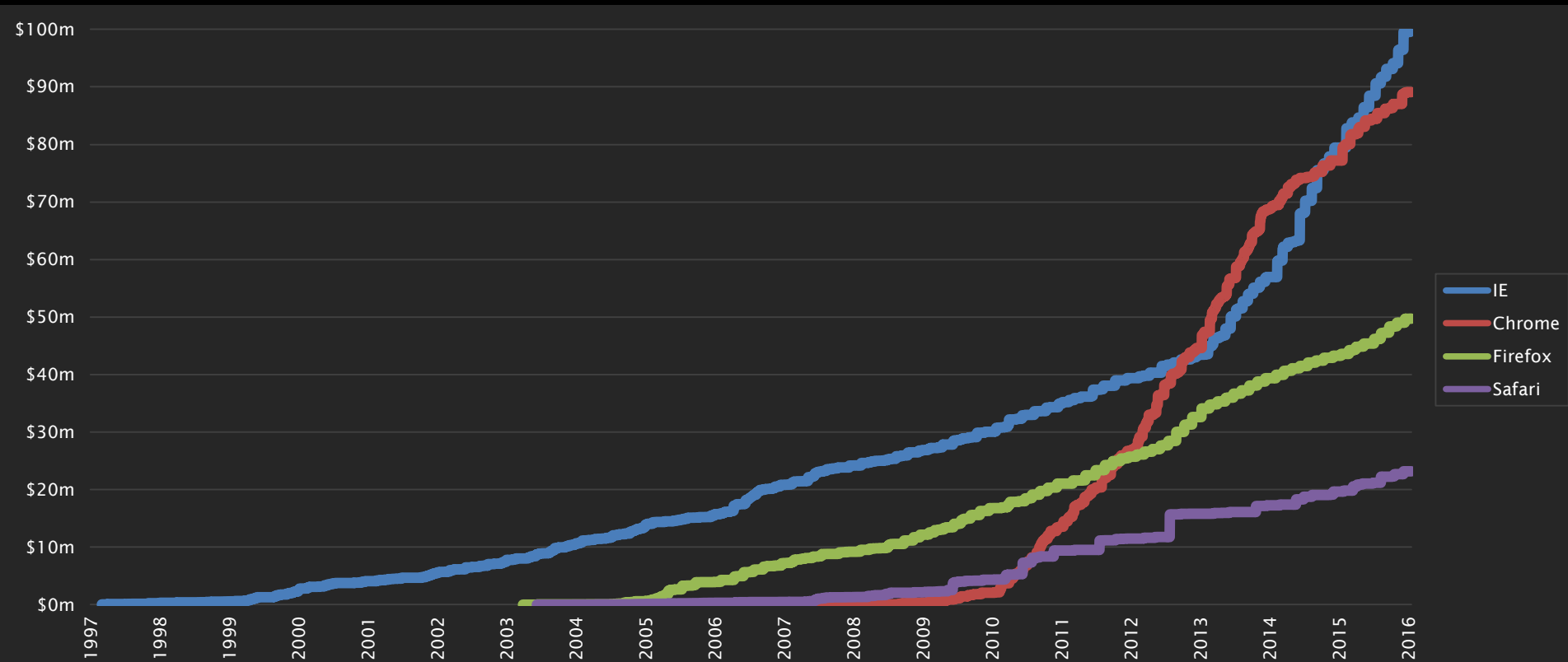
# MOBILE EXPLOIT MARKET ANALYSIS

IOS DOMINATES THE UPPER PRICE SEGMENT



# BROWSER EXPLOIT MARKET ANALYSIS

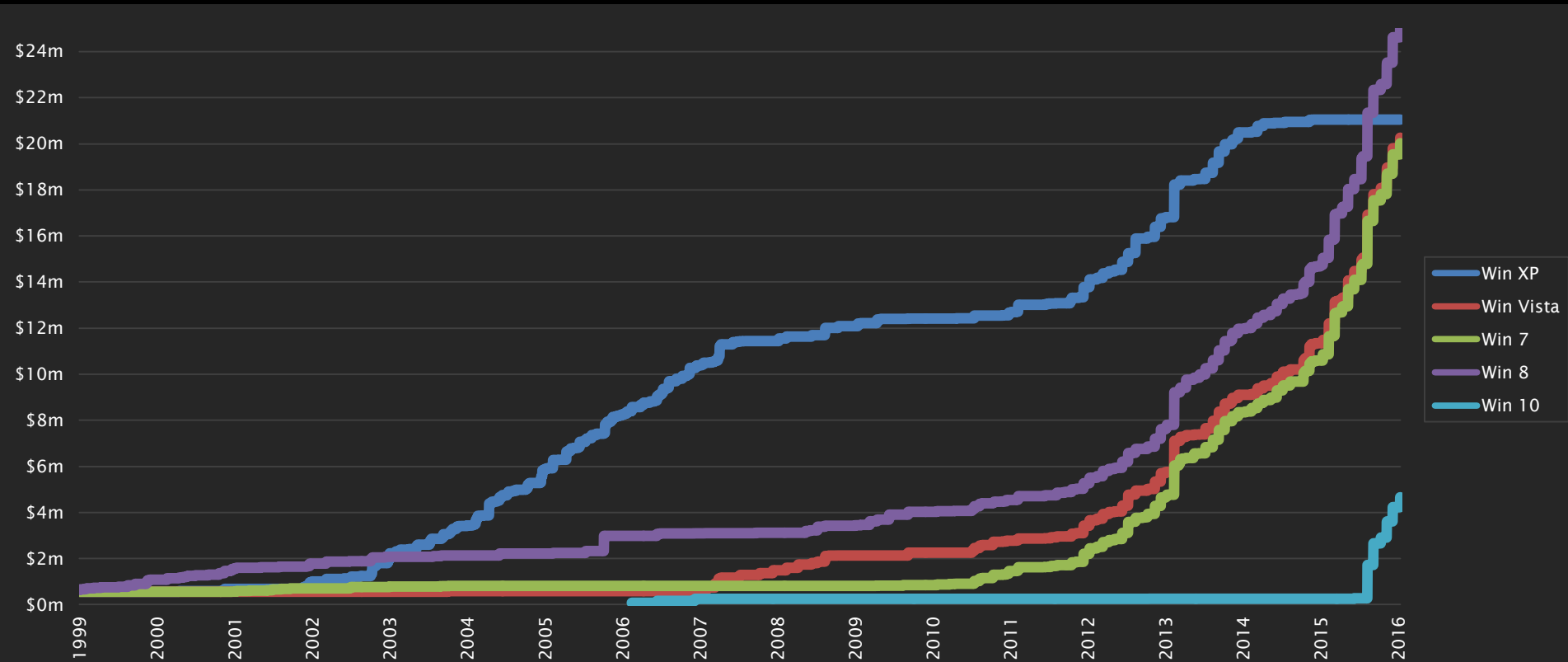
THE MARKET OF IE AND CHROME HAS CHANGED OVER TIME





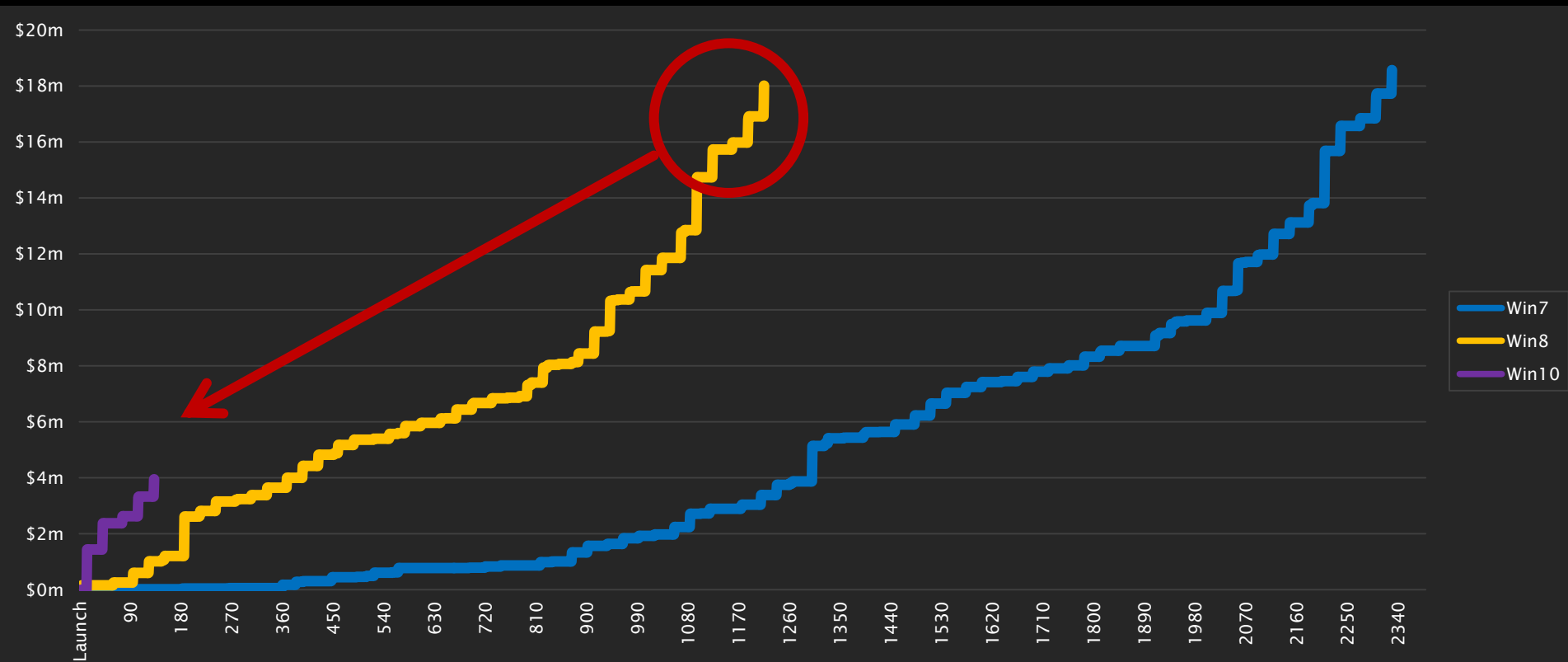
# WINDOWS EXPLOIT MARKET ANALYSIS

SINCE WINDOWS XP THE DYNAMICS HAVE CHANGED



# WINDOWS EXPLOIT MARKET PREDICTIONS

EXPONENTIAL GROWTH WITH MICROSOFT WINDOWS AS EXAMPLE



# EXPLOIT PURCHASE PROCESS

INITIAL AND STAGGERED PAYMENTS



PROVIDING  
EXPLOIT

AS SOURCE CODE

INITIAL  
PAYMENT

JANUARY 25.000 CHF

SECOND  
PAYMENT

FEBRUARY 15.000 CHF

THIRD  
PAYMENT

MARCH 10.000 CHF

# UNDERGROUND MARKETS

## VIRTUAL BLACK MARKET FOR LEGAL AND ILLEGAL GOODS

The motivation for computer crime consists of various shades and ranges from approval to power and money. Money is the main driver of the Darknet which is a hidden part of the Internet. Accessing this invisible net requires additional software and relationships. There it becomes possible to buy illegal goods and services like drugs, weapons and human beings. The investigation for authorities is difficult due to technological and legal restrictions.

For more details see:

- ★ <https://www.scip.ch/en/?labs.20160114> (Darknet)
- ★ <https://www.scip.ch/en/?labs.20161013> (Exploits)

# START YOUR OWN BLACK MARKET

BUY CODE AND SERVER IN THE DARKNET

\$7959





scip AG  
Badenerstrasse 623  
CH-8048 Zürich

Tel	+41 44 404 13 13
Mail	info@scip.ch
Web	<a href="https://www.scip.ch">https://www.scip.ch</a>
Twitter	<a href="https://twitter.com/scipag">https://twitter.com/scipag</a>

- ☒ Offense
- ☒ Defense
- ☒ Research



#### Images:

Anonymous Crowd: anon617, <https://www.flickr.com/photos/anon617/2272309405>  
Dark Forest: unsplash.com, <https://www.pexels.com/photo/nature-forest-trees-fog-4827/>  
Keyboard: DeclanTM, <https://www.flickr.com/photos/declanjewell/3009644612>  
Money: Tracy O, [https://www.flickr.com/photos/tracy\\_olson/61056391](https://www.flickr.com/photos/tracy_olson/61056391)  
Barbwire: Non-dropframe, [https://en.wikipedia.org/wiki/File:Artistic\\_barbwire.JPG](https://en.wikipedia.org/wiki/File:Artistic_barbwire.JPG)  
Nobel Prize: White House, <https://www.flickr.com/photos/whitehouse/4177793078/>  
Fist: <https://pixabay.com/p-316605/>  
Tunnel: Unsplash, <https://pixabay.com/en/tunnel-underground-black-and-white-690513/>  
Drugs: [https://commons.wikimedia.org/wiki/File:Prescription\\_drugs.jpg](https://commons.wikimedia.org/wiki/File:Prescription_drugs.jpg)  
Weapons: [https://commons.wikimedia.org/wiki/File:Flickr\\_-\\_Israel\\_Defense\\_Forces\\_-\\_Hidden\\_Weapons\\_Cache\\_Found\\_in\\_Nablus.jpg](https://commons.wikimedia.org/wiki/File:Flickr_-_Israel_Defense_Forces_-_Hidden_Weapons_Cache_Found_in_Nablus.jpg)  
Skull: Ben Francis, <http://www.freestockphotos.biz/stockphoto/9367>  
Legs: Stefan Andrej Shambora, [https://www.flickr.com/photos/st\\_a\\_sh/350108347](https://www.flickr.com/photos/st_a_sh/350108347)  
DVD Burning: Felipe La Rotta, <https://commons.wikimedia.org/wiki/File:Dvd-burning-cutaway2.JPG>  
Movie Theater: sailko, [https://en.wikipedia.org/wiki/List\\_of\\_cinema\\_and\\_movie\\_theater\\_chains#/media/File:Interno\\_di\\_un\\_sala\\_da\\_cinema.JPG](https://en.wikipedia.org/wiki/List_of_cinema_and_movie_theater_chains#/media/File:Interno_di_un_sala_da_cinema.JPG)  
Turbine: littlevisuals.co, <http://www.pexels.com/photo/airplane-jet-aviation-aircraft-1936/>  
NightSky: Pieter Kuiper, [https://commons.wikimedia.org/wiki/File:Night\\_sky.jpg](https://commons.wikimedia.org/wiki/File:Night_sky.jpg)  
iPhone: Yanki01, <https://www.flickr.com/photos/yanki01/15291191306>  
Chip: Martin Fisch, <https://www.flickr.com/photos/martins75/4372145011>  
Pills: Candy, [https://commons.wikimedia.org/wiki/File:Orange\\_pills.jpg](https://commons.wikimedia.org/wiki/File:Orange_pills.jpg)  
Ice Berg: Uwe Kils, <https://commons.wikimedia.org/wiki/File:Iceberg.jpg>  
DNA Analysis: DNA lab, <https://www.flickr.com/photos/snre/6946913993>  
Deep Sea: FrostBo, <http://frostbo.deviantart.com/art/Premade-Background-10-269120339>  
Bitcoin: BTC Keychain, <https://www.flickr.com/photos/btckeychain/11297241203>  
Snow Field: Nick Mealey, <https://www.flickr.com/photos/nickmealey/837472757>