KASPERSKY

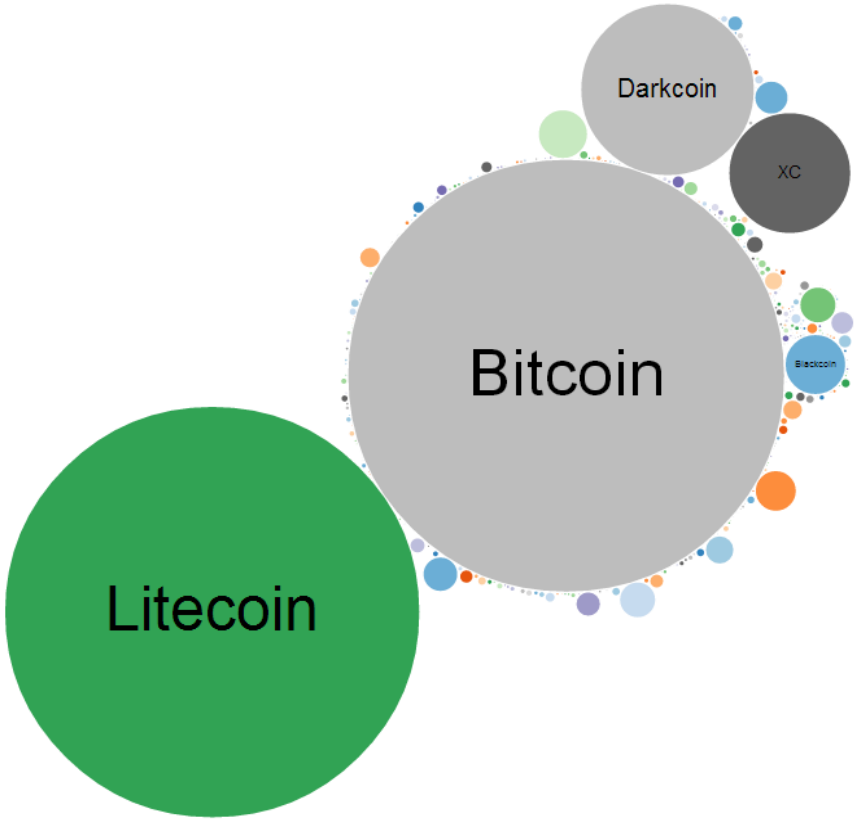
WELL… THAT ESCALATED QUICKLY

FROM PENNY-STEALING MALWARE TO MULTI-MILLION-DOLLAR HEISTS, A QUICK OVERVIEW OF THE BITCOIN BONANZA IN THE DIGITAL ERA

Santiago Pontiroli

Global Research and Analysis Team (GReAT), Kaspersky Lab Argentina

IN THE BEGINNING WE HAD BITCOIN



WHAT'S SO COOL ABOUT IT?

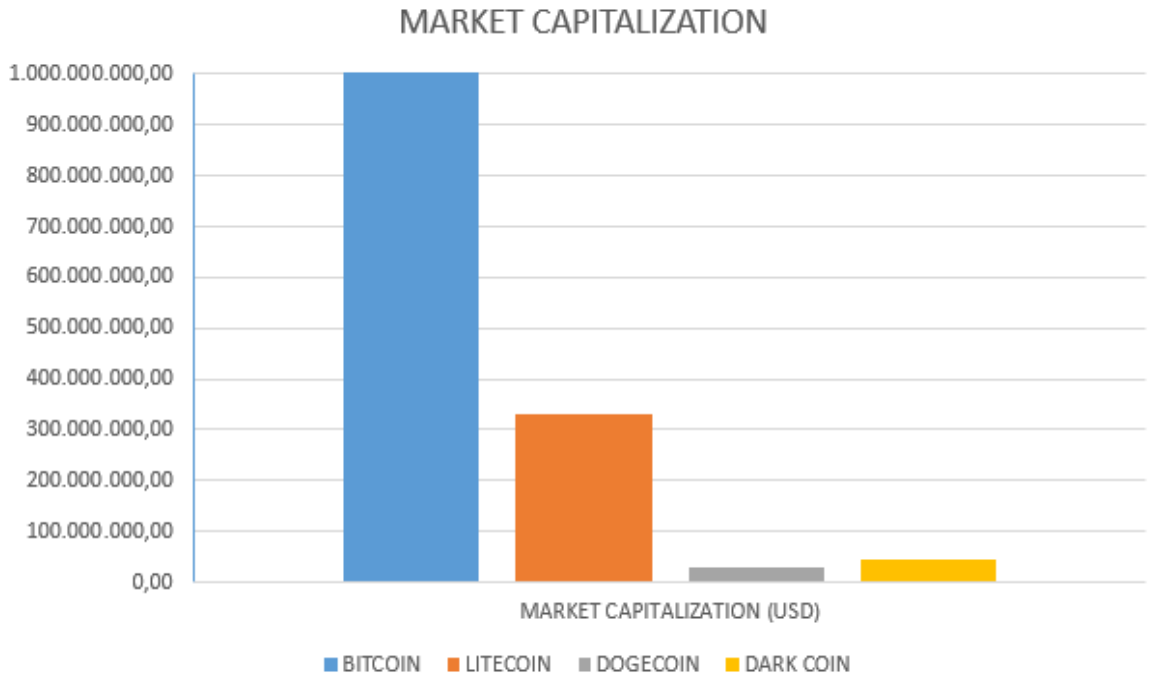
- *Sure… decentralization, privacy, transaction speed and convenience.*
- You can buy the weirdest things.
- You can "mine" the currency. The digital alchemist's dream has become real.
- It provides an alternative currency for countries where strict financial control is in place, or the inflation makes FIAT money a less appealing alternative.
- BYOB (not from System of a Down!), bring your own bank, save your money in your own computer.

DOGECOIN? WAIT, WHAT?

WHAT'S NOT SO COOL ABOUT IT?

- You can buy things like the one in the picture (yeap, weird).
- It's a nightmare for tax and money laundering agencies to control.
- Governments are not so keen on it either.
- Illegal markets found an ideal currency to use for exchange of goods.
- Fraudsters have found a new gateway into people's money.
- Value volatility.
- Storing your own money has proven difficult for some users.

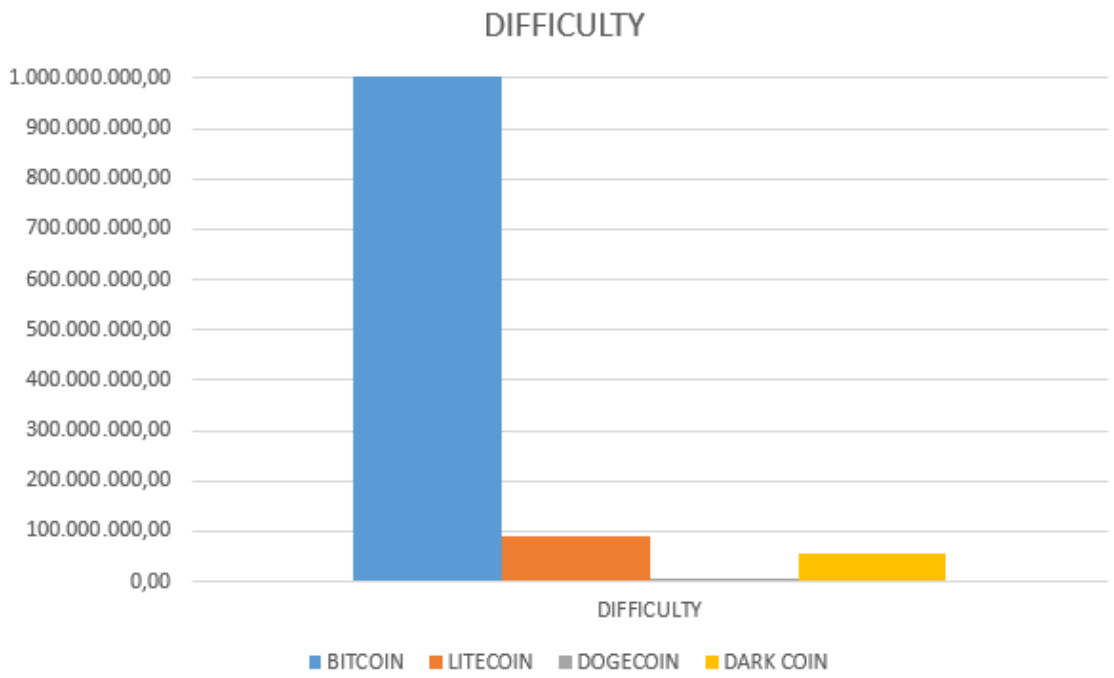
AND WE SAW IT WAS GOOD



- From coinmarketcap.com as of September 8th, 2014.
  - BTC $ 6,344,538,325
  - LTC $ 162,747,962
  - DOGE $ 16,026,770
  - DRK $ 13,177,613
- Where there's money, there's crime.

KASPERSKY lab

BUT THEN…SUCH DIFFICULTY, MUCH SAD



- With the appearance of ASICs and FPGAs the difficulty rate quickly increased, leaving many miners behind.
- Many new cryptocurrencies were a promised land for these crypto-outcasts and their computing cycles ready to be exchanged for money.
- Fraudsters and criminals were paying close attention as other coins gained momentum.

KASPERSKY lab

RICKROLLING THE BLOCKCHAIN

Will Ferrel Parc

@FillWerrel

Say the opp
1)Always.
2)Coming.
3)From.
4)Take.
5)Me.
6)Down.

SUCH POSSIBILITIES, MANY ATTACKS

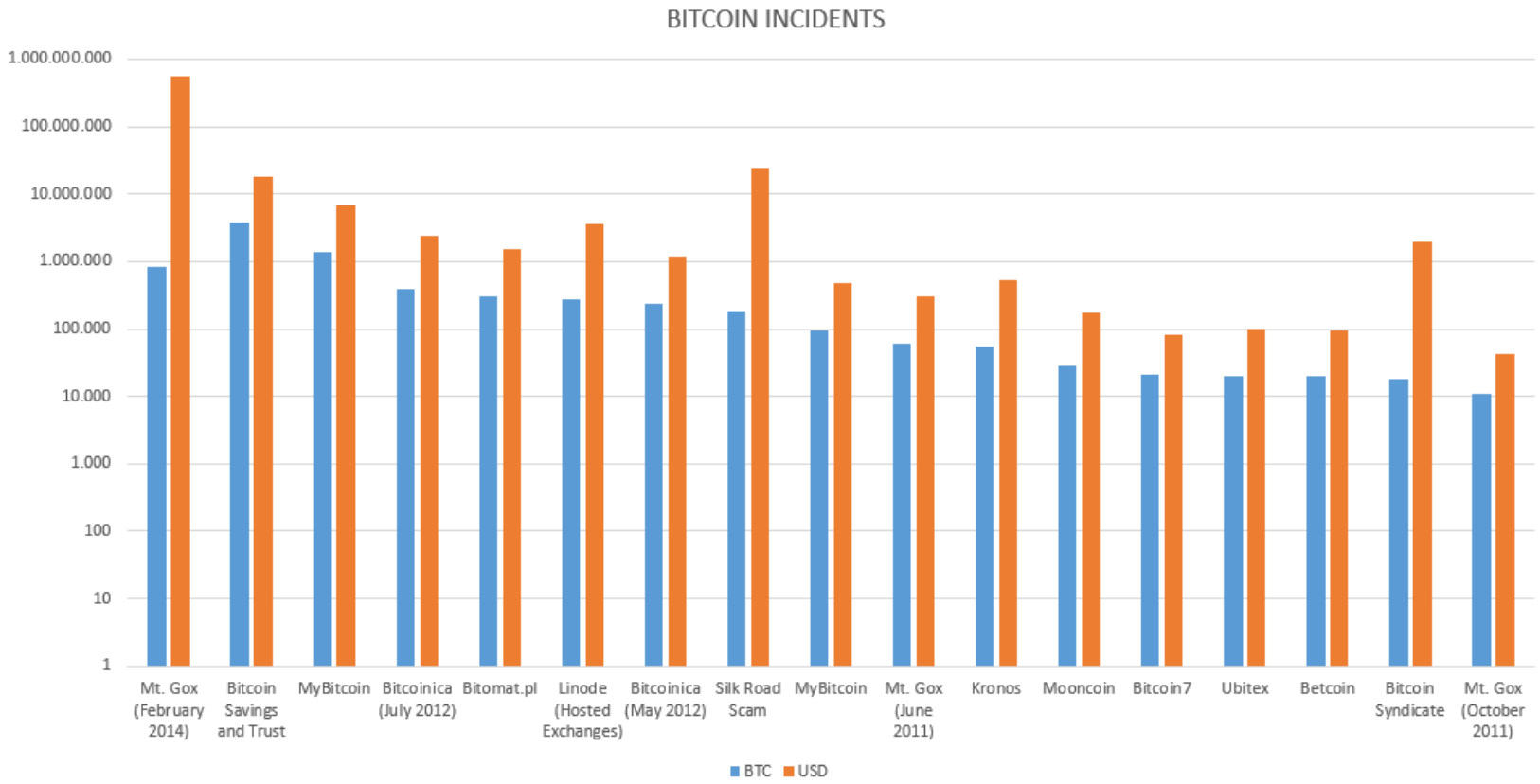
ONLY CHUCK NORRIS CAN WITHDRAW FUNDS FROM MT. GOX

- Transaction malleability.
- Illegal content in the blockchain.
- The 51% attack.
- Denial of Service.
- Software vulnerabilities.

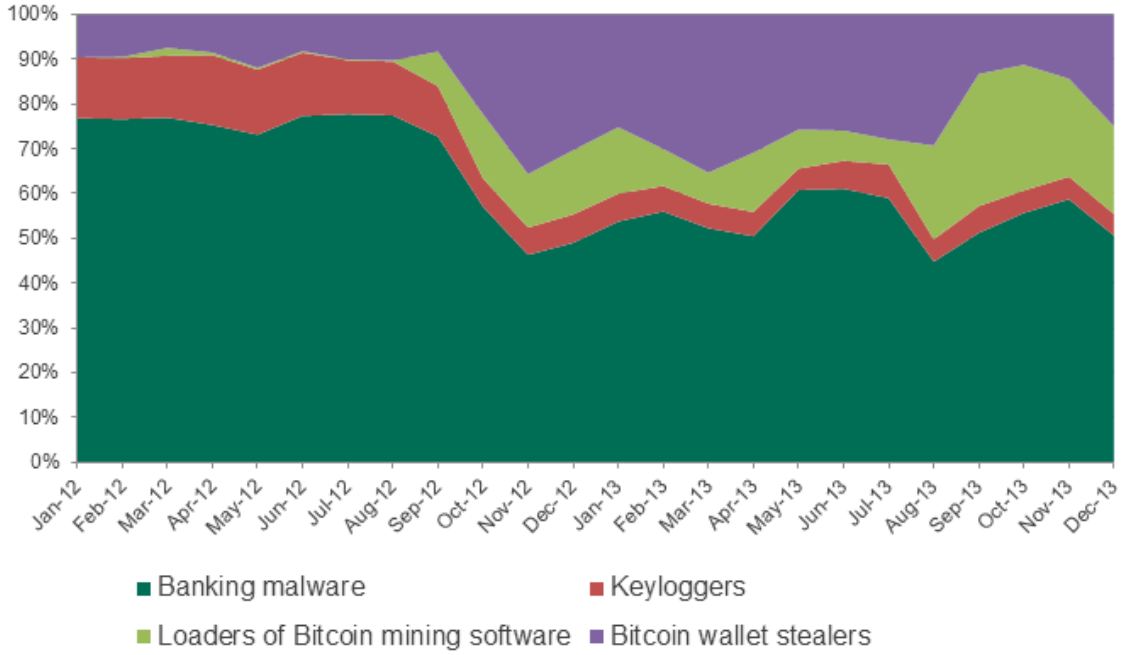
- And, of course… malware!


MARLON BRANDO
ROBERT DUVALL
MARTIN SHEEN
DENNIS HOPPER
LAURENCE FISHBURNE
AND HARRISON FORD
FRANCIS FORD COPPOLA
PRESENTS
MtGoxcalypse Now

SHOW ME THE MONEY



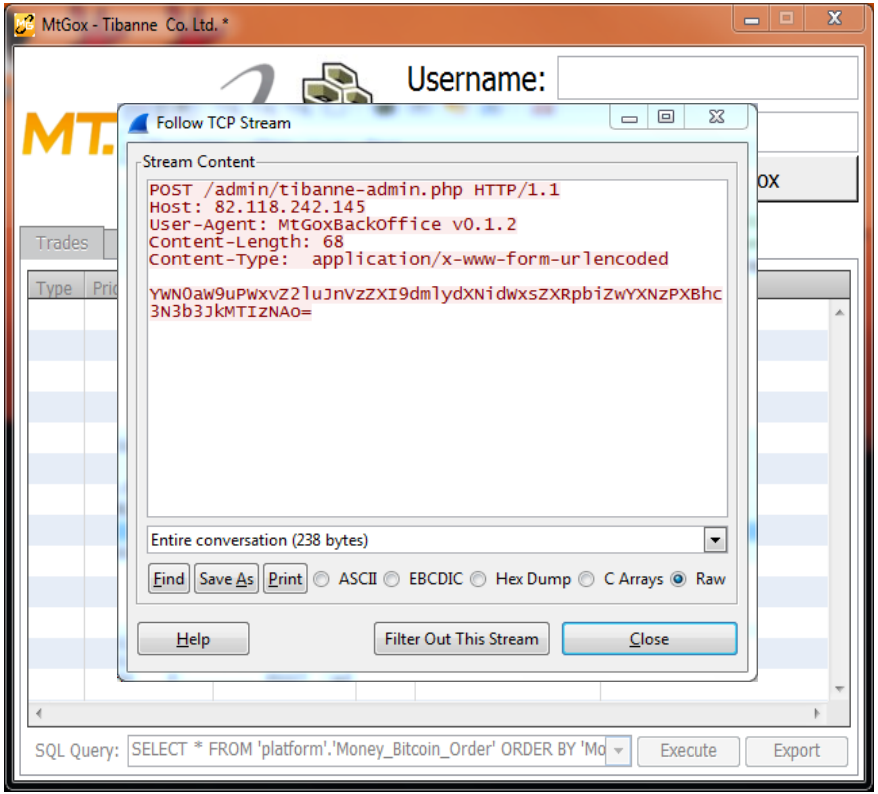
MALWARE TRENDS IN THE BITCOIN WORLD



- At first mining was profitable.
- Malware writers got greedy and aimed to mine cryptocurrencies in any device with a CPU.
- Phishing and scams were always there, just needed to be adapted.
- Targeting exchanges was easier, then it wasn't. Users were caught in the crossfire.

KASPERSKY lab

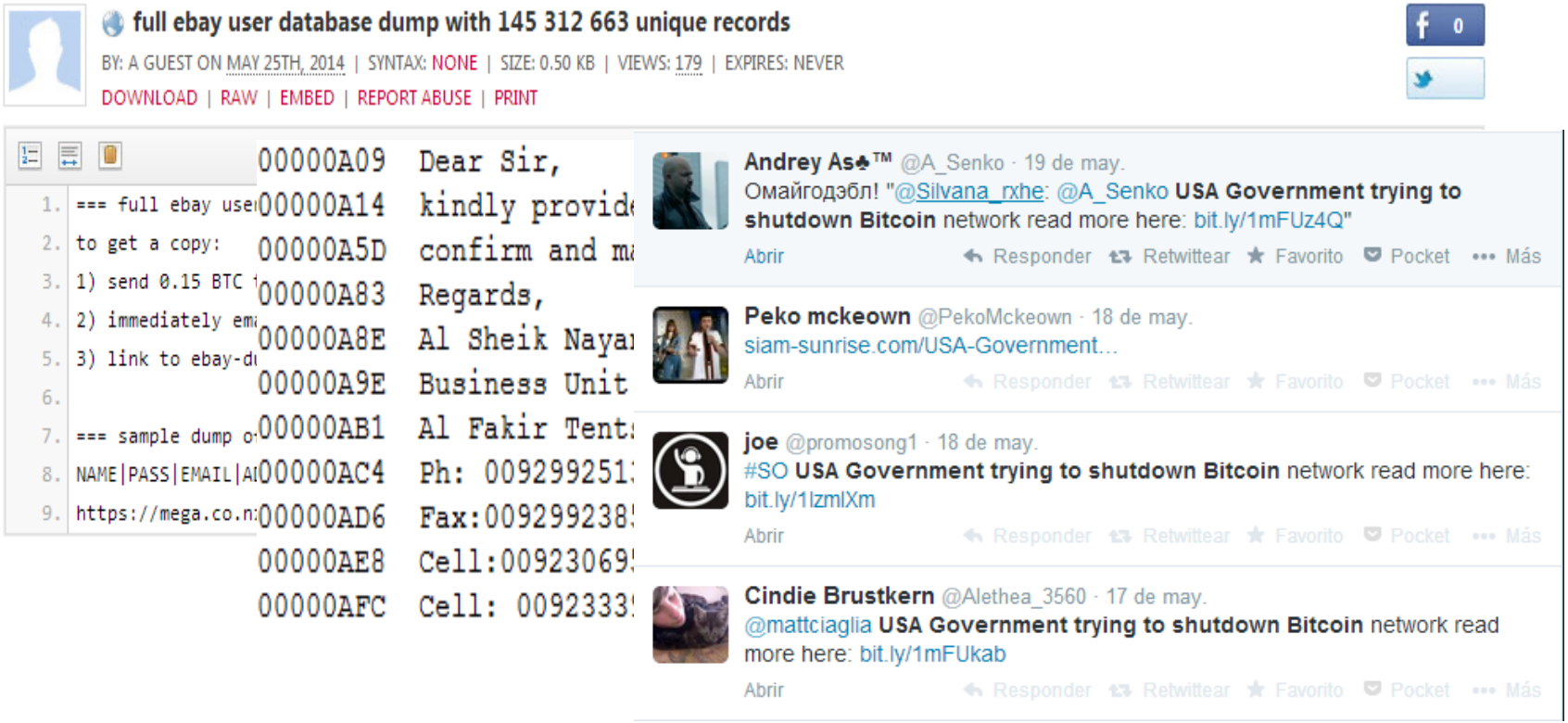
THE GOOD OL' MALWARE, SIMPLE YET EFFECTIVE



TROJAN.WIN32.COINSTEALER

- Was supposedly a Mt. Gox leak, "MtGox2014Leak.zip".
- Included several fake spreadsheets and a customized back-end client to access the information.
- It was nothing more than a wallet and credentials stealer.
- Using base64 encoded strings, it sent the information to a remote server in Sofia, Bulgaria.
- Programmed in Livecode, to support also Mac OSX.

PHISHING AND SCAMS



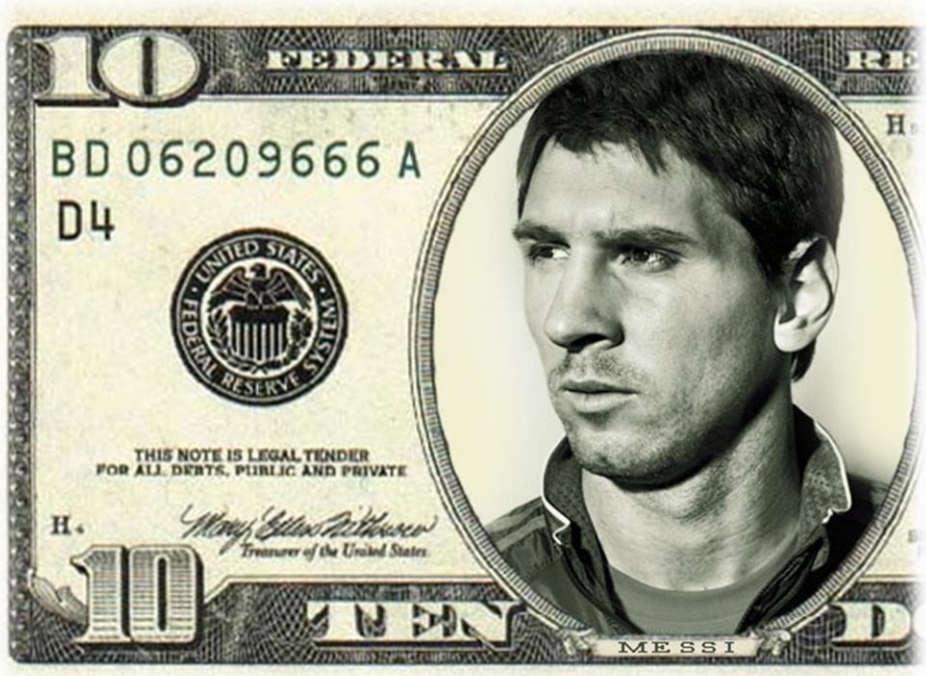
WHAT ABOUT SOME INTERESTING STUFF?

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00013C70	98	07	04	E0	9A	07	07	E0	91	08	08	E0	9A	01	01	E0	▮ à▮ à´ à▮ à
00013C80	08	80	97	E0	01	18	81	22	08	48	94	E0	28	18	A1	E0	▮▮à " H▮à(¡à
00013C90	04	00	A0	E1	95	13	24	E0									
00013CA0	F0	85	BD	E8	28	3											
00013CB0	10	40	2D	E9	04	4											
00013CC0	02	F0	A0	E1	04	2											
00013CD0	10	80	BD	E8	08	6											
00013CE0	0D	C0	A0	E1	F0	D											
00013CF0	F0	AF	1B	E9	2F	7											
00013D00	00	00	00	00	72	2											
00013D10	25	64	2E	25	64	2											
00013D20	32	31	39	2E	35	3											
00013D30	2F	6B	2E	70	68	7											
00013D40	50	2F	31	2E	30	0											
00013D50	2E	32	31	39	2E	3											
00013D60	41	67	65	6E	74	3											
00013D70	0A	43	6F	6E	6E	6											
00013D80	73	65	0D	0A	0D	0											
00013D90	32	30	30	20	4F	4											
00013DA0	26	6D	69	6E	6F	7											
00013DB0	26	6A	75	6E	69	6											
00013DC0	71	75	65	3D	73	7											
00013DD0	47	45	54	20	2F	7											
00013DE0	2E	63	67	69	3F	6											
00013DF0	31	2E	30	0D	0A	4											
00013E00	30	30	0D	0A	55	7											
00013E10	4D	6F	7A	69	6C	6C	61	2F	34	2E	30	20	28	63	6F	6D	Mozilla/4.0 (com

KASPERSKY lab


AND IT’S GOOOONE

LATIN AMERICA AND BITCOIN



DOLLAR MESSI AND BITCOIN AS THE ALTERNATIVE

- Argentina, a thriving black market for dollars.
- Citizens looking to beat the inflationary process.
- Lack of cryptocurrency regulation seems quite tempting.
- Along with Sao Pablo, Mexico City and Santiago the Chile, leading the pack in bitcoin adoption.
- Anti money laundering agencies are not enthusiastic about it.

LATIN AMERICA AND BITCOIN RELATED MALWARE

RANSOMWARE, NOPE?

- Besides your everyday malware, phishing and scams, ransom now has gone digital.
- Companies are learning about bitcoin when their files appear encrypted out of the blue.
- If you think getting bitcoins is hard, try getting dollars in Latin America.
- Cybercriminals targeting wallets and bitcoins through ransomware are the new kid in town.

KASPERSKY lab

WE'RE NOT IN KANSAS ANYMORE

BEING YOUR OWN BANK IS MORE DIFFICULT THAN IT SEEMS

- From mining botnets to wallet and credential stealing.
- Latin America is an emerging market, in cybercrime too.
- Cryptocurrencies are seen as a viable method for saving your hard earned pesos, but do citizens have the knowledge to protect their virtual vault?

PREGUNTAS? LET'S TALK

KASPERSKY lab

@spontiroli