

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-F03

Bitcoin's Future Threats: Expert's Roundtable based on 150 Case Studies

MODERATOR:

Wayne Huang

VP Engineering
Proofpoint, Inc.
@waynehuang
whuang@proofpoint.com
wayne.armorize@gmail.com

PANELISTS:

Charlie Lee

Creator, Litecoin
Engineering Director, Coinbase
@SatoshiLite

Danny Yang

Founder & CTO, MaiCoin, Inc.
@huuep

Fyodor Yarochkin

Senior Threat Researcher, VArmour, Inc.
@fygrave

Kristov Atlas

Security Engineer, blockchain.info
@kristovatlas

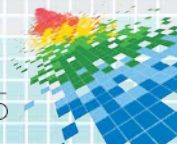
CHANGE

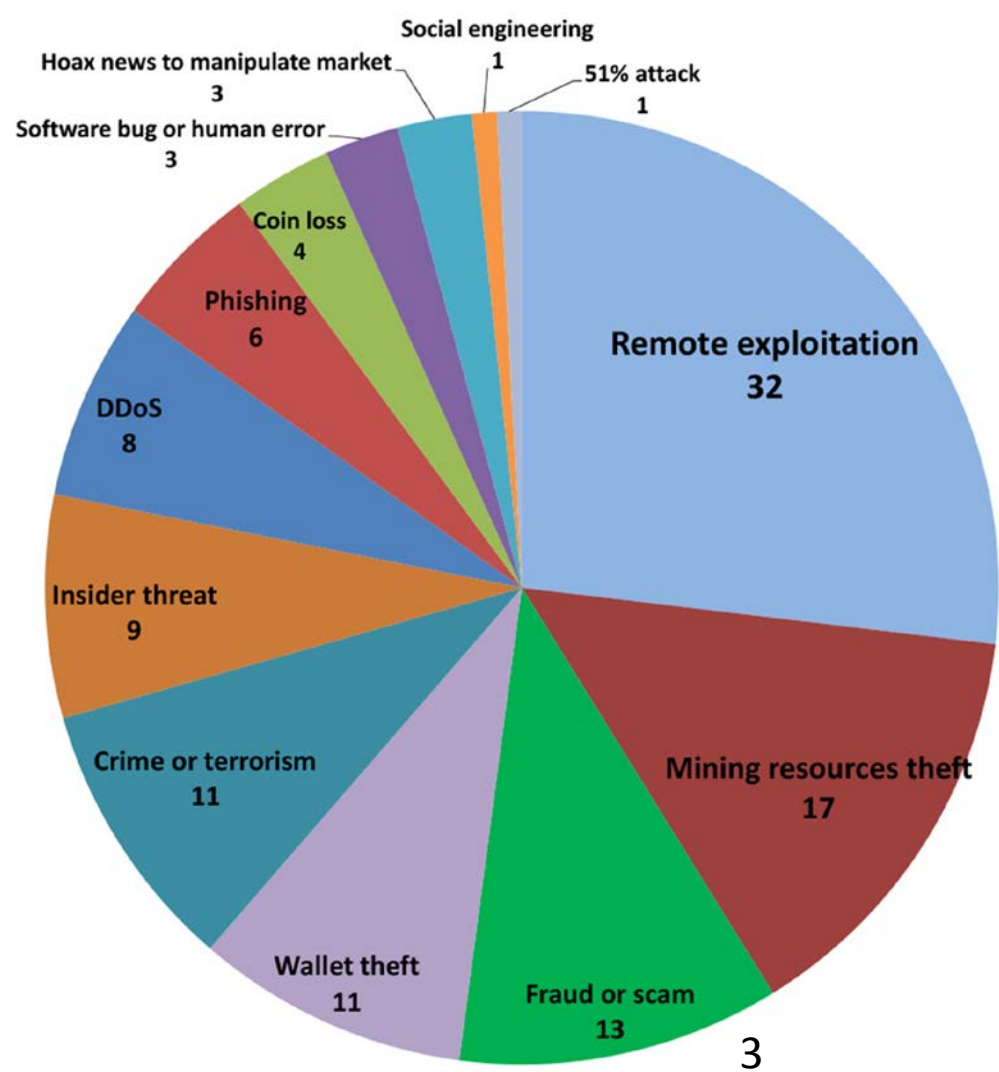
Challenge today's security thinking



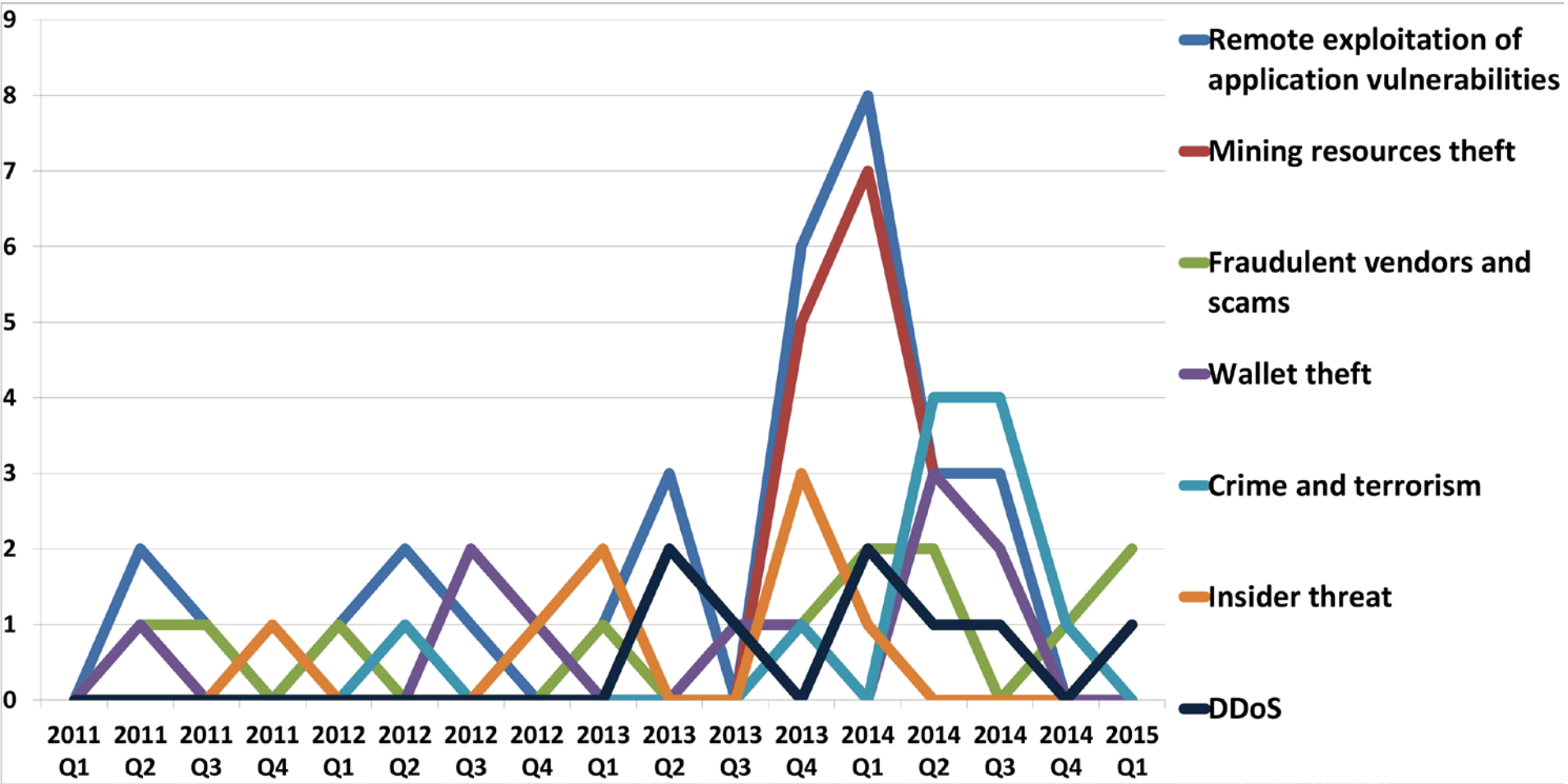
The BIG question...

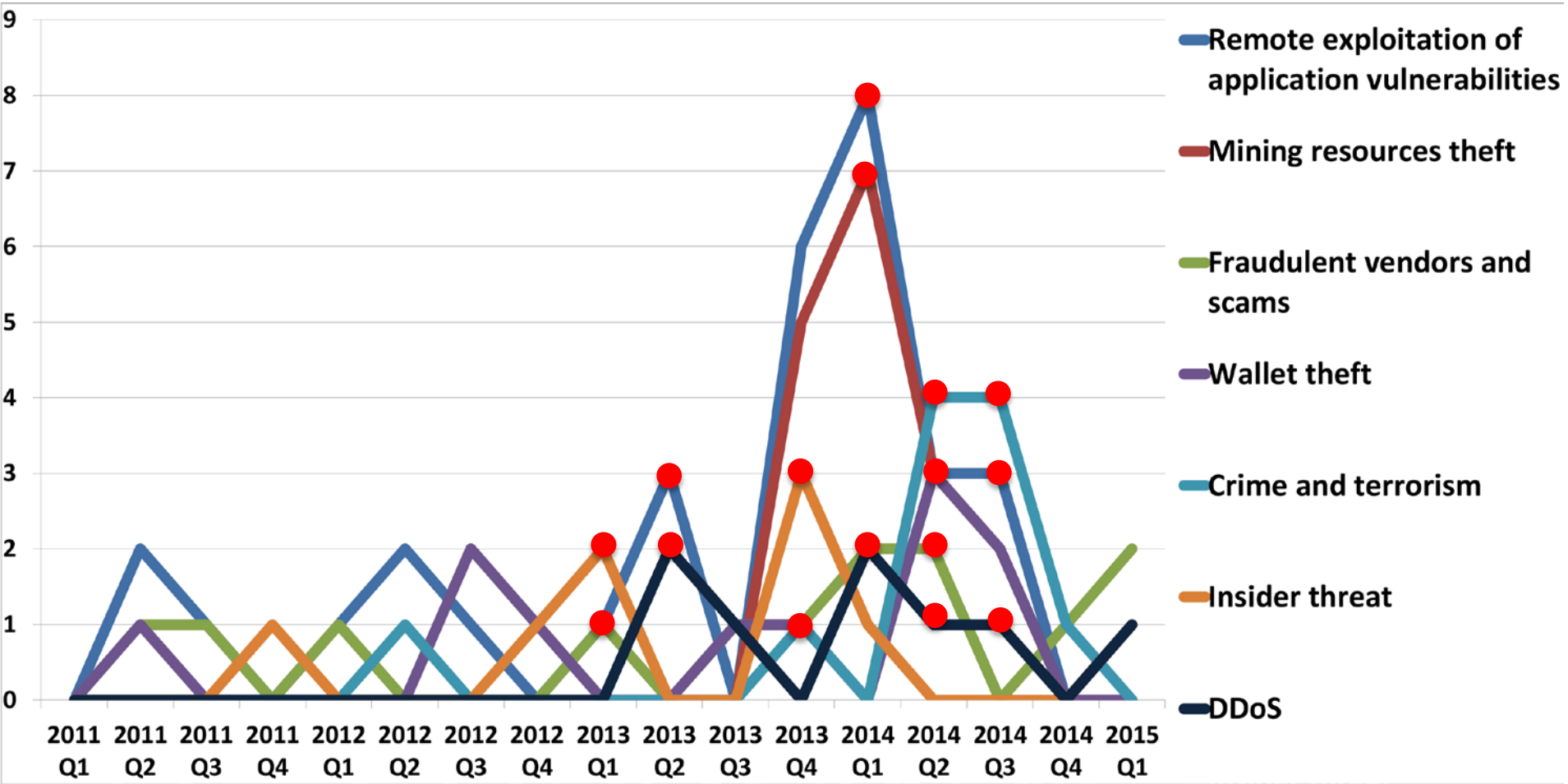
Why are Bitcoin targets so attractive?

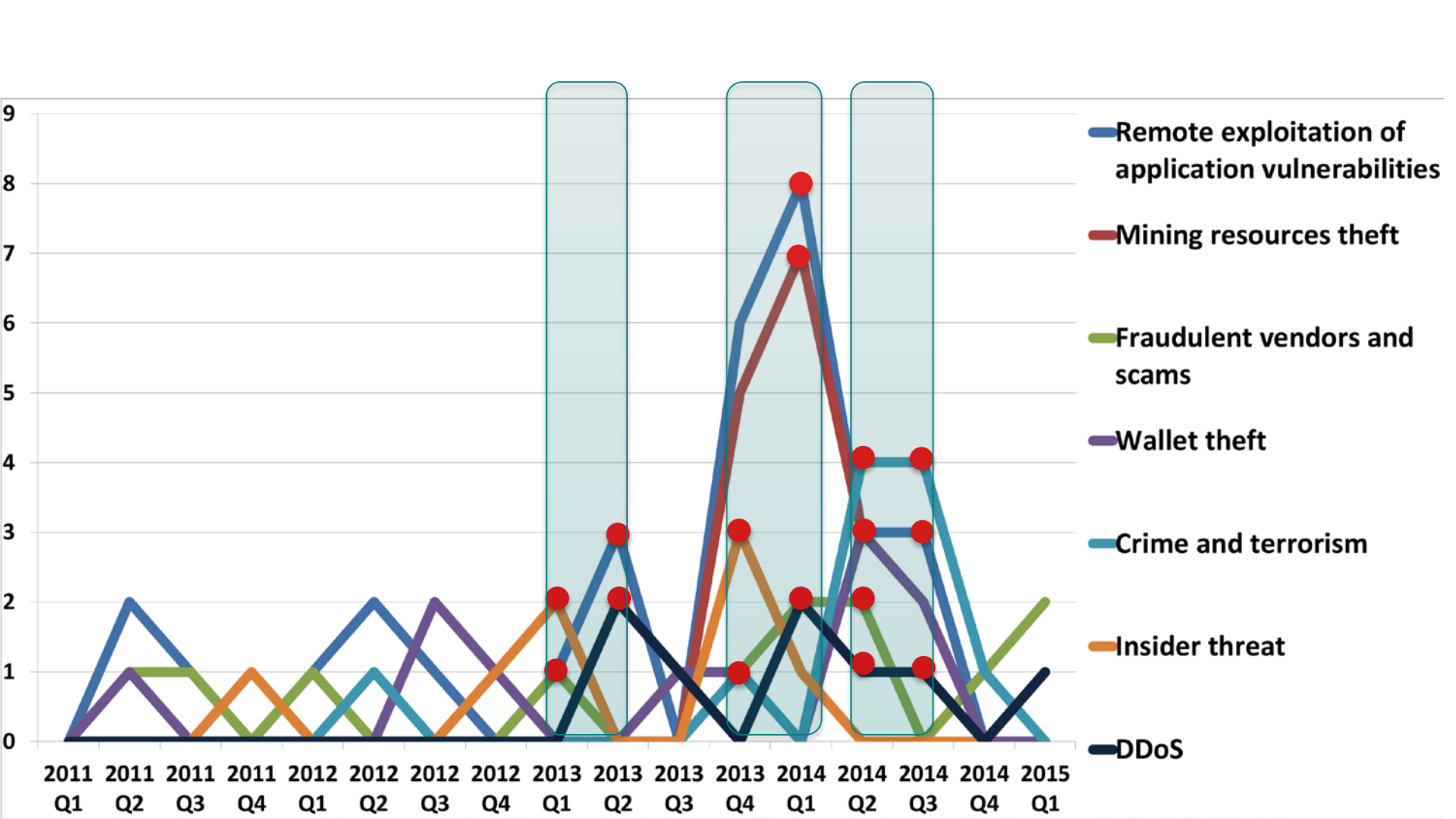


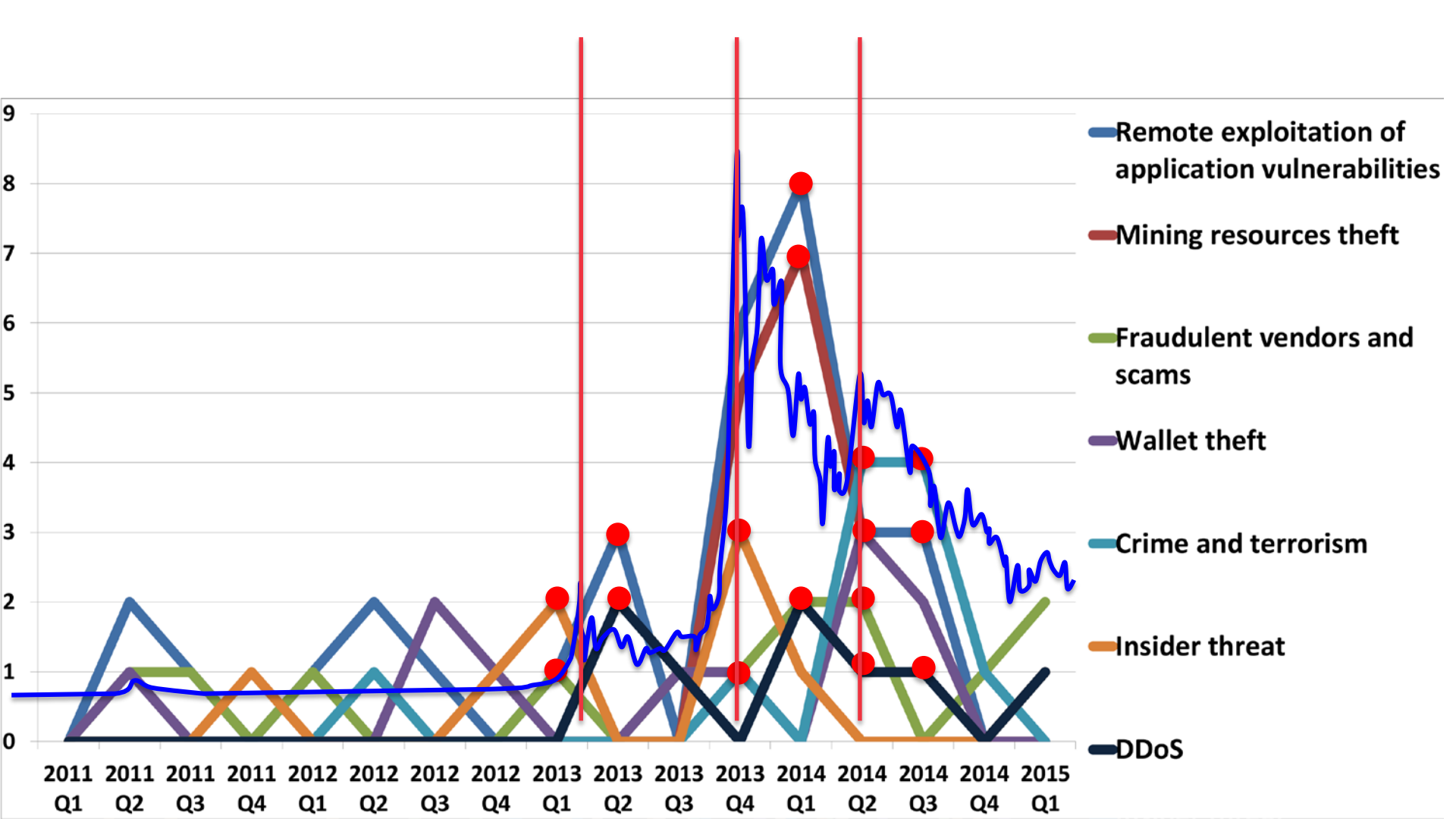


- Remote exploitation
- Mining resources theft
- Fraud or scam
- Wallet theft
- Crime or terrorism
- Insider threat
- DDoS
- Phishing
- Coin loss

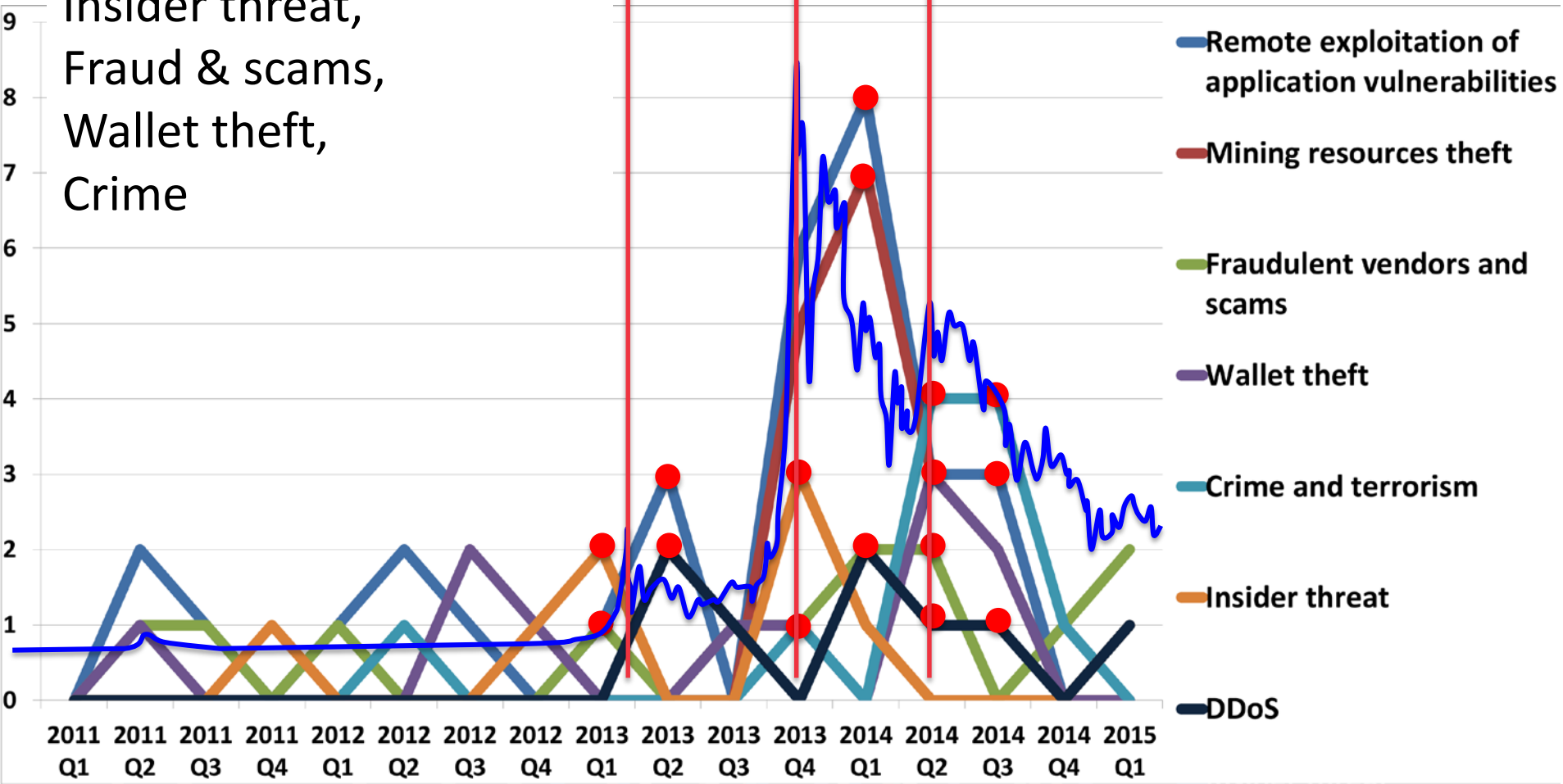






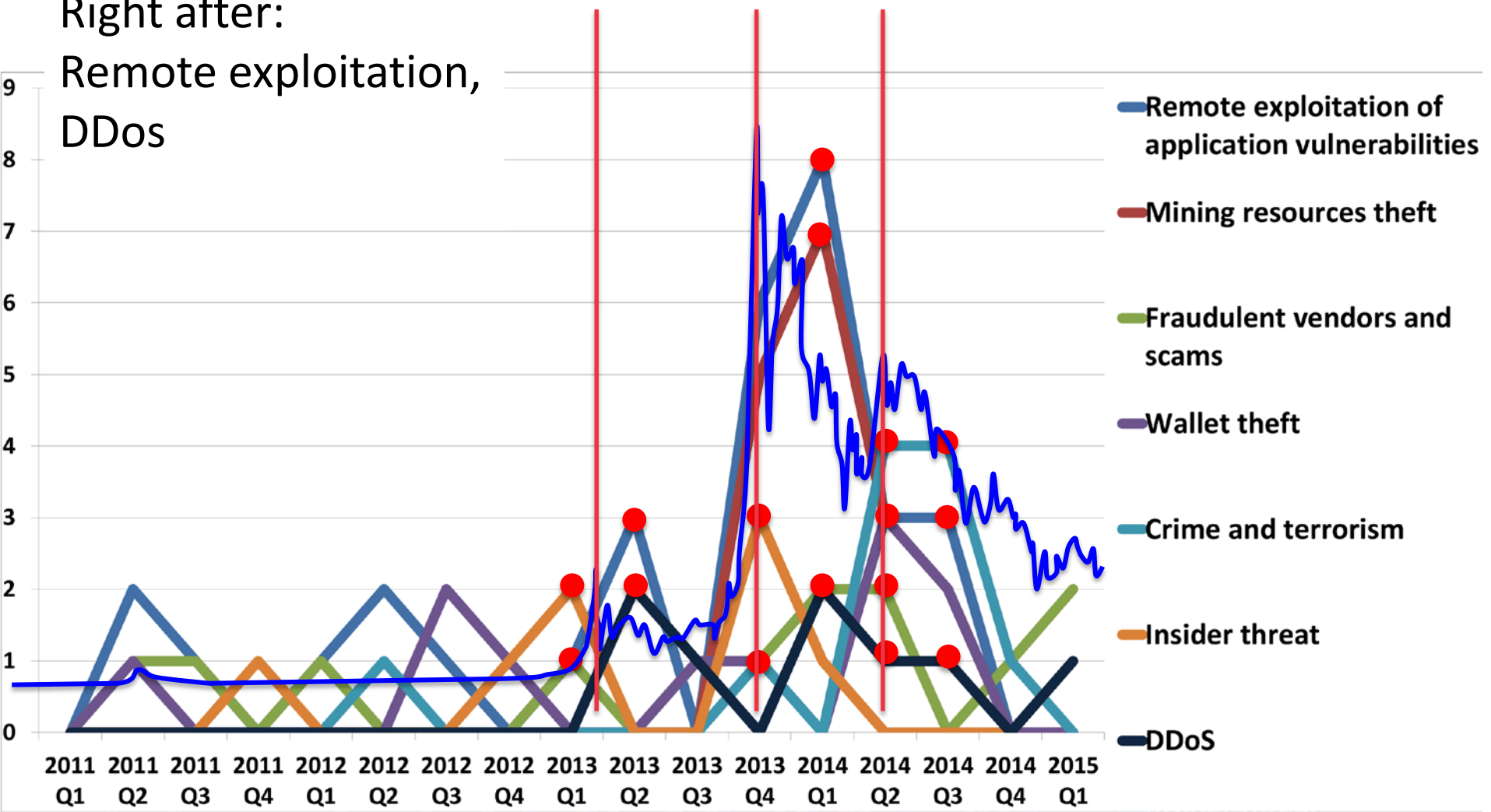


Just before or in parallel:
Insider threat,
Fraud & scams,
Wallet theft,
Crime



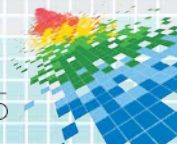
Right after:

Remote exploitation,
DDoS



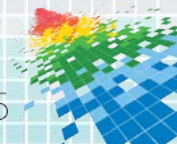
The BIG question...

Why are Bitcoin targets so attractive?



Questions

- ◆ Does Bitcoin facilitate money laundry, or its detection? Both? Neither?
- ◆ How anonymous is Bitcoin?
- ◆ How does an attack against an exchange usually start?
- ◆ Does cryptocurrency promote ransomware
- ◆ Will we see more of CryptoLocker clones in the future demanding Bitcoin for encrypted file ransom?
- ◆ Which threat vector will impact Bitcoin's future most?
- ◆ What opportunities does Bitcoin bring to the security industry?
- ◆ How will Bitcoin impact the security industry?
- ◆ How to boost Bitcoin's wide adoption?
- ◆ Which threat vector is likely under-rated?



POLONIEX



BetCoin™

Doge Vault

flexcoin

LocalBitcoins.com



HACKED

coinbase



Bitcoin Forum

coin x.p



POKER.COM

BITSTAMP

Bitcoin Forum



50BTC

Bitcoinica

BTC Guild



MT.GOX

Bitmit

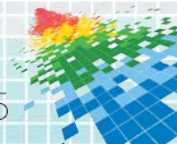
Vircurex

bitcash.cz



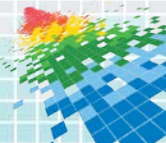
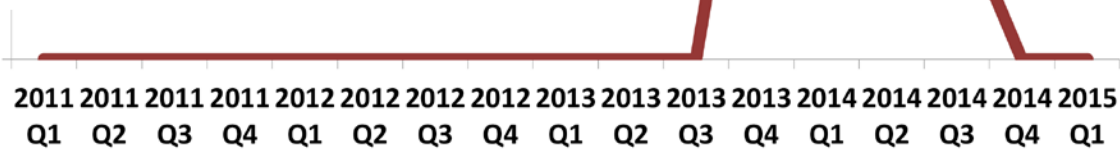
Remote exploitation of server-side vulnerabilities

- ◆ Vulns in open source Bitcoin projects
- ◆ 3rd party vulns
- ◆ Application vulns (OWASP)



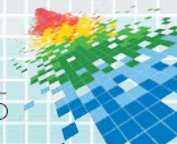
Mining resources theft

- ◆ Seizing pro miners, Dell: stealing \$9,000 a day
- ◆ German police: botnet mined €700,000 bitcoins
- ◆ Miner botnets (ex: DVRs, cams, NAS...)
- ◆ University servers
- ◆ Hidden miners (ex: games)
- ◆ Android app miners (ex: wallpapers apps)



Mining resources theft: Embedded Devices

- ◆ Compromises: embedded ARM, PPC, MIPS or X86 machines
- ◆ Attack vector: default passwords, a vuln in /cgi-bin/php
- ◆ Primary targets: cheap Linux-based embedded devices, ex:
 - ◆ Dahua camera - arm
 - ◆ AFoundry switch - mips
 - ◆ Tera EP Wifi Broadband Switch - mips
- ◆ Mines MNC coin via p2pool.org



Mining resources theft: Embedded Devices



Mining resources theft: Embedded Devices



Mining resources theft: Embedded Devices

+	2014/09/26 17:08:28	2014/09/26 17:08:30	213.5.67.223 NLD	54053	80	14	1,710 / 2,650	moloch	///	///	///	/cgi-bin/php-cgi /cgi-bin/php.cgi /cgi-bin/php4
+	2014/09/26 17:08:30	2014/09/26 17:08:31	213.5.67.223 NLD	59505	80	14	1,930 / 2,870	moloch	///	///	///	7/cgi-bin/php-cgi 7/cgi-bin/php.cgi 7/cgi-bin/php4
+	2014/09/26 17:08:33	2014/09/26 17:08:34	213.5.67.223 NLD	55444	80	13	1,155 / 2,029	moloch	///	///	///	5/cgi-bin/php-cgi 5/cgi-bin/php.cgi 5/cgi-bin/php4
+	2014/09/26 17:10:18	2014/09/26 17:10:20	213.5.67.223 NLD	42450	80	14	1,554 / 2,494	moloch	///	///	///	4/cgi-bin/php-cgi 4/cgi-bin/php.cgi 4/cgi-bin/php4
+	2014/09/26 17:10:26	2014/09/26 17:12:16	213.5.67.223 NLD	40937	80	9	1,022 / 2,059	moloch	///	///	///	/cgi-bin/php4? %6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
+	2014/09/26 17:25:32	2014/09/26 17:25:33	213.5.67.223 NLD	52326	80	10	450 / 1,126	moloch	/	/	/	/cgi-bin/php4
+	2014/09/26 22:11:46	2014/09/26 22:14:09	78.188.238.228 TUR	51749	80	13	3,056 / 3,960	moloch	/	/	/	/cgi-bin/php4? %2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
+	2014/09/26 22:12:49	2014/09/26 22:15:24	78.188.238.228 TUR	35317	80	16	3,056 / 4,178	moloch	/	/	/	/cgi-bin/php4? %2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E

Mining resources theft: Embedded Devices

MNC/Address

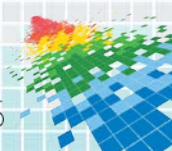
MNC address, block, height, transaction, etc.

MDFepZz9SpSbFSugUsXVE3CmrdTaKg1SWi

Details	
Operations count:	1590
Total received:	307.92301622 MNC \$2.17
Total spent:	307.92301622 MNC \$2.17
Final balance:	0 MNC \$0



Date	Address	Amount
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.5263152 MNC
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.81916537 MNC
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.54161601 MNC
3/3/2014 5:58:47 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.5160554 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.53463671 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.95114204 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.28149311 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.82143478 MNC
3/3/2014 5:56:18 AM (UTC)	MKGCaZwEbRPWU7PnE8BTb5sYUZcWVwxUe5	- 0.79605472 MNC



Mining resources theft: Embedded Devices

MNC/Address

MNC address, block, height, transaction, etc. Search

MRsa7HTrEJvsGk3BABrgzZMjXh6wzTdU8r

Details	
Operations count:	89
Total received:	192,443.85455633 MNC \$1,485
Total spent:	141,972.18843046 MNC \$1,095
Final balance:	50,471.66612587 MNC \$389

Request address recalculation



Date	Address	Amount
10/21/2014 6:30:14 PM (UTC)	MKcwHtCc2EkPpKdt49Bvar4BxqNG3zNHRr	see tx - 2,999.90 MNC
10/21/2014 6:18:03 PM (UTC)	MRVEdNWrgPhVvknMsS5sSs8BBjrSo3d2sR, MKcwHtCc2EkPpKdt49Bvar4BxqNG3zNHRr	see tx - 4,797 MNC
10/21/2014 6:15:20 PM (UTC)	MKcwHtCc2EkPpKdt49Bvar4BxqNG3zNHRr	see tx - 999.90 MNC
10/21/2014 11:16:15 AM (UTC)	MDUqF1bXeKY3UDoka35AKhL8P7fzXwrkeo	see tx - 29,997 MNC
9/29/2014 4:05:23 AM (UTC)	MRSFMaffikBm1ZGd42t8kPre4CYzRxpV5A	see tx - 7,496.90 MNC
9/4/2014 2:23:23 PM (UTC)	MQtRNvWhG9Lf1FJ5qucpZoqHewYgfcS1hQ, MUgSkj1bJEULBNLXFgP8fbjeNJ7rLFgoT	see tx - 24,688.5486078 MNC
8/31/2014 7:09:53 AM (UTC)	MSwNUNBMPNf1mcmSPJzouzM4AJpJYs1Xkz, MJEdq3q7tuZzw7x3qQVCq1Xe86erbE3nXP, MTcrbNisbQ6C3NyqSswHy7QAiV2AcT6F9, MKu2gHLVBkpgFn7kBTHT9z59rmgjAAmi3m, MwC8QVw4K5QvYUfUwzTzGv1Mf1d1Q	see tx + 29,997 MNC

Bitcoin mining botnet: sale

OFFLINE Ekira



Забанен

Регистрация: 20 Dec 2014

Сообщений: 14

Отправлено 07 January 2015 - 20:41

Вирус троян для майнинга, профит вируса за 1000 зараженных компьютеров вы получите от 10-30 долларов в день.

Инструкцию по распространению предоставляем.

Антивирусная программа не реагирует на вирус.

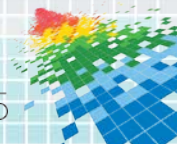
Заработок завит от количества зараженных компьютер и не чем не ограничен.

Цена 100 \$.

Работаю через Гарант-Сервис приветствую.

Isq 683469315

OFFLINE Raiden



CLOUD COMPUTING



Dashboard

Dashboard Pools Workers About

Last updated on : Tuesday, 24th of April 2012 at 16:52:44




Recent work submissions

Worker	Pool	Result	Time
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:42 CEST

Recent failed work submissions

Worker	Pool	Time
user	BTCguild	24-04-2012 18:52:13 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:08 CEST
user	BTCguild	24-04-2012 18:52:04 CEST

Worker status

Worker	Last work request	Last accepted submission	Shares [*]	Rejected [†]	Hashing speed [†]	Actions
user	At: 24-04-2012 18:52:43 CEST from BTCguild	At 24-04-2012 18:52:43 CEST to BTCguild	1483	25 (1.69%)	10615.727 MHash/s	  
Totals			1483	25 (1.69%)	10615.727 MHash/s	

Source:
<http://habrahabr.ru/post/147635/>

Mining resources theft

- ◆ Botnets - Some also have injects for bitcoin theft, i.e this Zeus modification:
<https://bigrc.biz/threads/%D0%BF%D1%80%D0%BE%D0%B4%D0%B0%D0%BC-botnet-evolution-%D0%B1%D0%BE%D1%82%D0%BD%D0%B5%D1%82.9505/>

[+] Граббер банковских аккаунтов, с возможностью добавления новых банков в список в

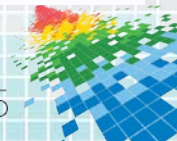
режиме онлайн.

[+] Встроенные автоподмены: Киви, ЯД, РБКмани, Перфектмани, ЛР, ВМ, **bitcoin**.

[+] Граббер сертификатов IE , FF

[+] Ddos-модуль (get, post, slowlogis запросы)

[+] Новый механизм инжектирования в процессы, на замену устаревшему WriteProcessMemory



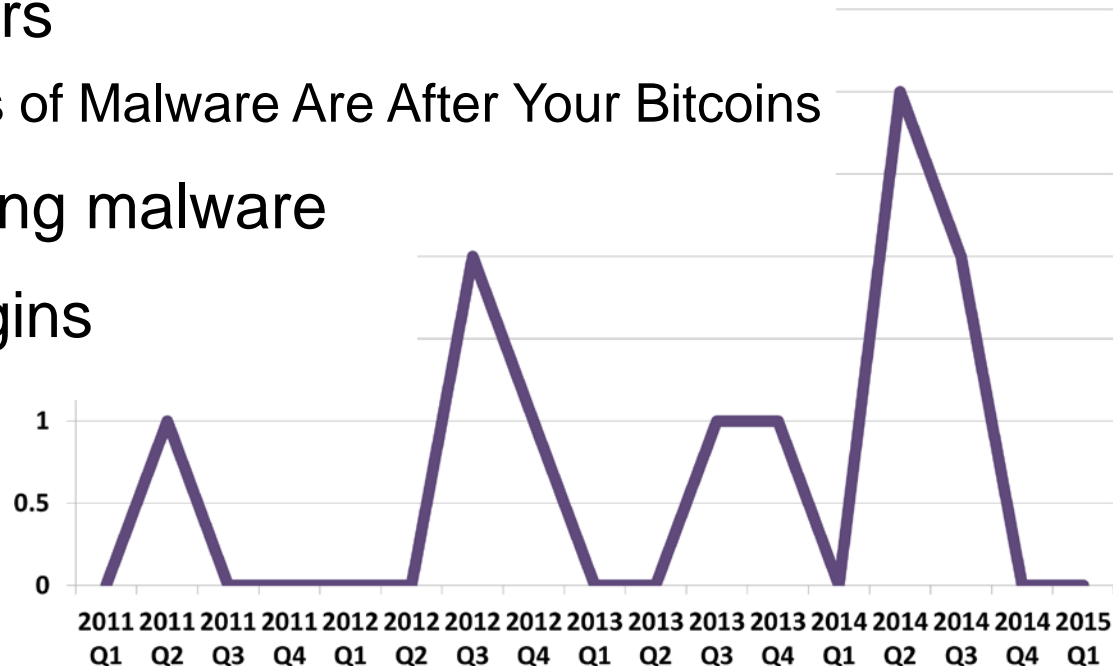
Fraudulent vendors and scams

- ◆ Bitcoin startup scams (taking investor money)
- ◆ Miner scams (no shipment)
- ◆ Bitcoin-denominated ponzi scheme
- ◆ Exchange scams
- ◆ Bitcoin asset scams



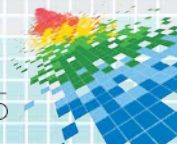
Wallet theft

- ◆ Endpoint wallet stealers
 - ◆ Dell: Nearly 150 Strains of Malware Are After Your Bitcoins
- ◆ Bitcoin-featured banking malware
- ◆ Trojaned browser plugins

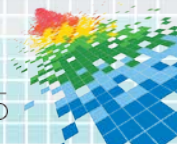
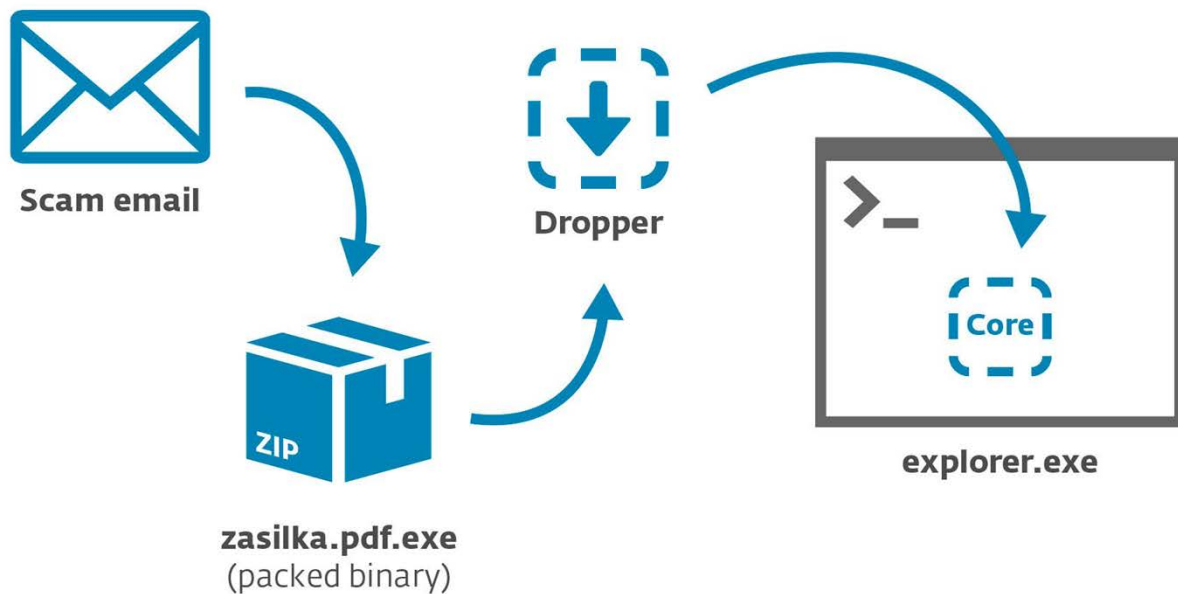


Bitcoin malware trends

- ◆ Malware is and will be an important tool for coin thieves against end users
- ◆ Attack wallet files or website logins
- ◆ Desktop and mobile
- ◆ Interest from malware authors is proportional to the Bitcoin price and adoption in their target demographic
- ◆ Dropped in 2014 along with price [Symantec]
- ◆ As adoption grows, average technical savvy of user will drop



Win32/Spy.Hesperbot



Trojan.Dyre/Dyreza



Figure 7. Geographic distribution of Dyre C2 servers. (Source: Dell SecureWorks)

```

dyre-10-15-2014 - Notepad
File Edit Format View Help
<server>
<sal>srv_www_cardonebanking_com</sal>
<saddr>63.141.253.186:26881</saddr>
</server>
<server>
<sal>srv_www_cardonebanking_com</sal>
<saddr>63.141.253.186:26981</saddr>
</server>
<server>
<sal>srv_bitpay_com</sal>
<saddr>63.141.253.186:27081</saddr>
</server>
<server>
<sal>srv_safello_com</sal>
<saddr>63.141.253.186:27181</saddr>
</server>
<server>
<sal>srv_accounts_expresscoin_com</sal>
<saddr>63.141.253.186:27281</saddr>
</server>
<server>
<sal>srv_anxbtc_com</sal>
<saddr>63.141.253.186:27381</saddr>
</server>
<server>
<sal>srv_blockchain_info</sal>
<saddr>63.141.253.186:27481</saddr>
</server>
<server>
<sal>srv_localbitcoins_com</sal>
<saddr>63.141.253.186:27581</saddr>
</server>
<server>
<sal>srv_bitbargain_co_uk</sal>
<saddr>63.141.253.186:27681</saddr>
</server>
<server>
<sal>srv_secure_coinjar_com</sal>
<saddr>63.141.253.186:27781</saddr>
</server>
<server>
<sal>srv_www_coinbase_com</sal>
<saddr>63.141.253.186:27881</saddr>
</server>
<server>
<sal>srv_www_bitstamp_net</sal>
<saddr>63.141.253.186:28081</saddr>
</server>

```

Malware Kits

UNIVERSAL Stealer

Welcome,

Perhaps you remember my last thread about an Electrum BTC wallet stealer. Well, I have taken this idea and improved upon it. I am pleased to c

Universal BTC Stealer is a BTC stealer which targets 3 of the most popular wallet clients, and employs a general stealing technique. There are tw
 1) The software detects any BTC addresses copied to the clipboard of the PC, and replaces them with a customer specified address. So whenev
 2) The software also scans the system's drives for wallet files of the following 3 wallet clients: Multi-Bit, Electrum, and Bitcoin-QT.

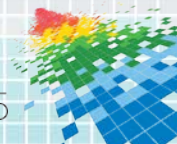
After finding wallet files on the system, the software is able to detect whether or not the wallet is encrypted with a password. It then social eng
<http://i.imgur.com/>
 This function targets both Multi-Bit and Electrum wallets.

Stolen wallet files along with general infection statistics are viewed in the following HTTP panel, which is available in both English and German.

Universal BTC Stealer features:

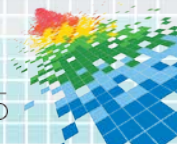
- Tested on Windows XP-8, x86 + x64
- Full Unicode support
- Stub size of 75kB
- Startup through registry
- Replaces copied BTC addresses with customer provided address
- Wallet stealing + password stealing capabilities for most common wallet clients
- Extensive error logging system to pinpoint any issues quickly and effectively
- HTTP control panel offered in English and German

Price for bin and panel: \$ 120 USD / (4848 RUB at this time), bitcoin / darkcoin only



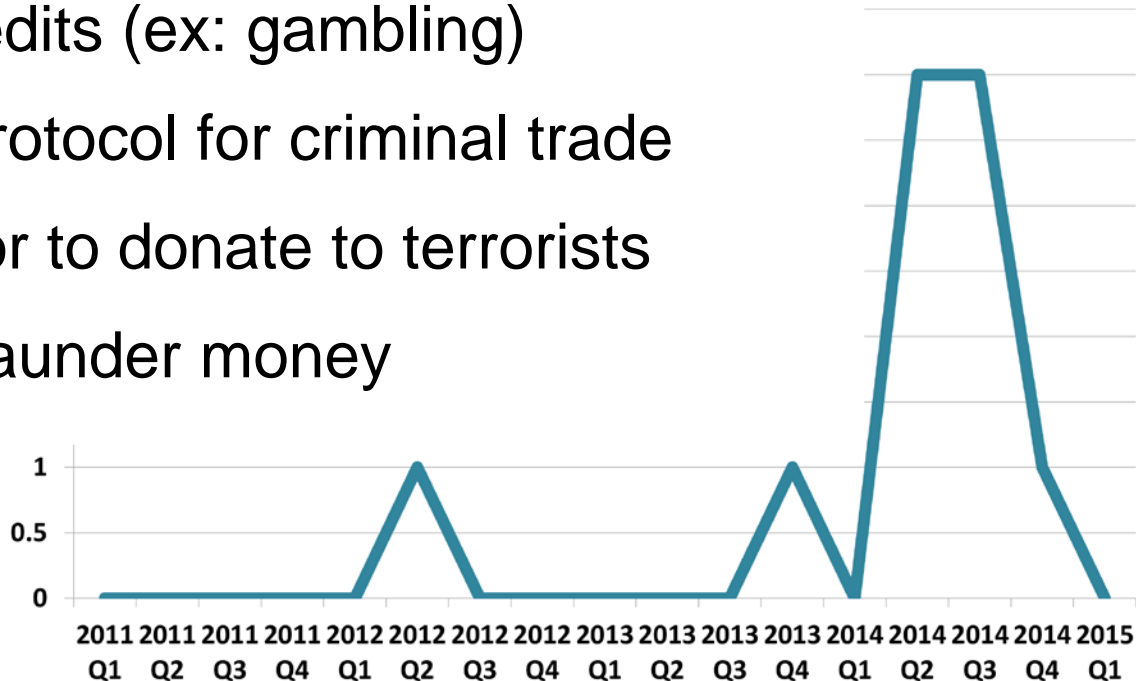
Defending Against Bitcoin Malware

- ◆ For now, most Bitcoin malware will simply be standard financial trojans. Use traditional methods of detection
- ◆ Behavioral analysis: processes scanning for 'wallet.dat', 'wallet.aes.json' or Base58Check strings all potentially suspicious
- ◆ Put private keys offline and into cold storage; use offline signing
- ◆ Security proportional to amount of funds stored, even during upward price swings
- ◆ Multi-stage signing protocols such as P2SH multisig, Shamir's Secret Sharing, or threshold sigs distribute risk



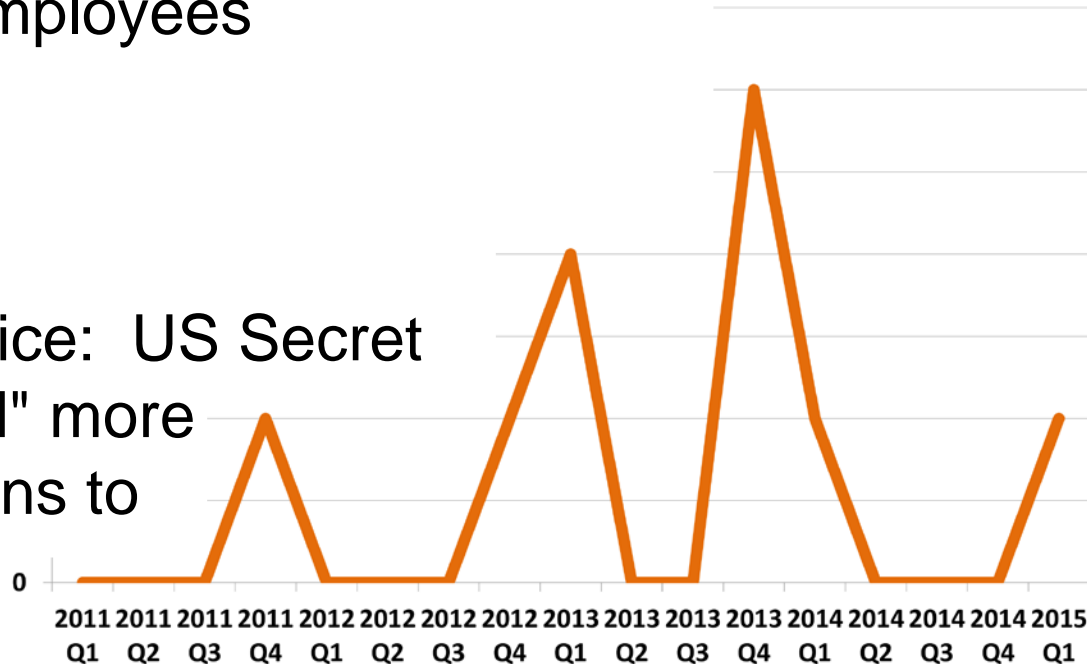
Crime and terrorism

- ◆ Bitcoin as gaming credits (ex: gambling)
- ◆ Bitcoin as payment protocol for criminal trade
- ◆ Bitcoin used to fund or to donate to terrorists
- ◆ Bitcoin as means to launder money

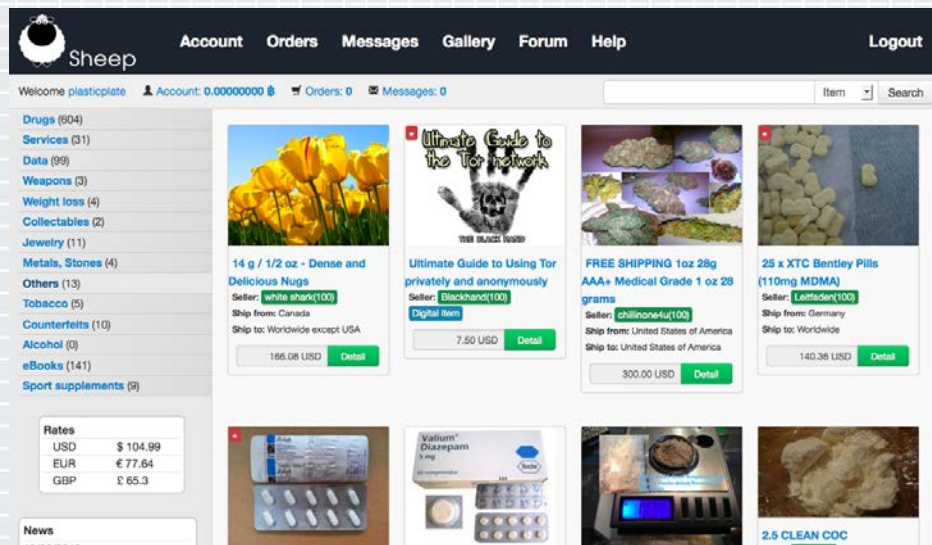
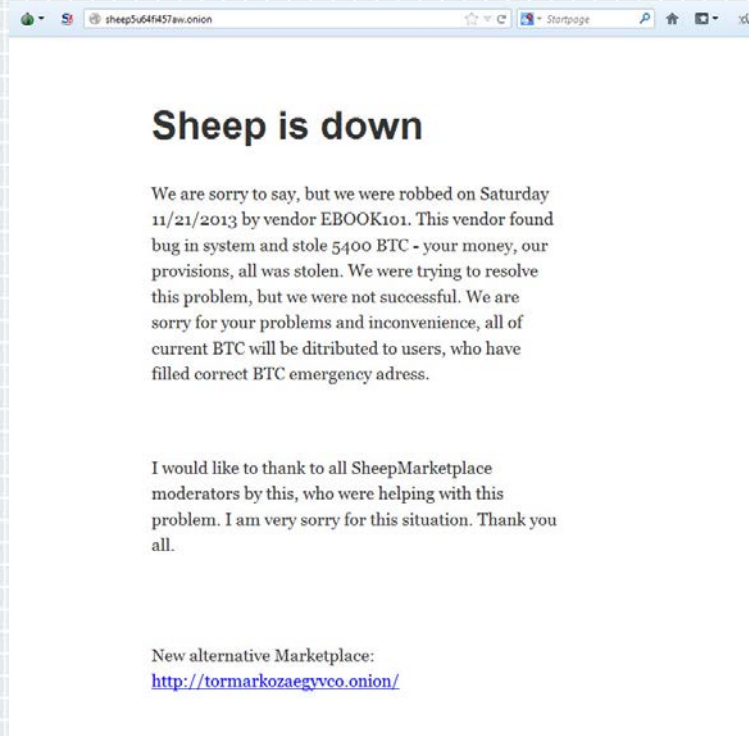


Insider threat

- ◆ Current operators or employees
- ◆ Ex-employees
- ◆ Fake “compromises”
- ◆ US Department of Justice: US Secret Service agent "diverted" more than \$800,000 in Bitcoins to his personal accounts



Insider Threat: Sh33p Marketplace

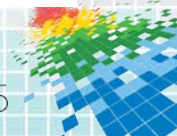



Sheep is down

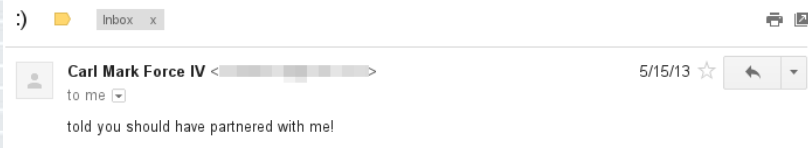
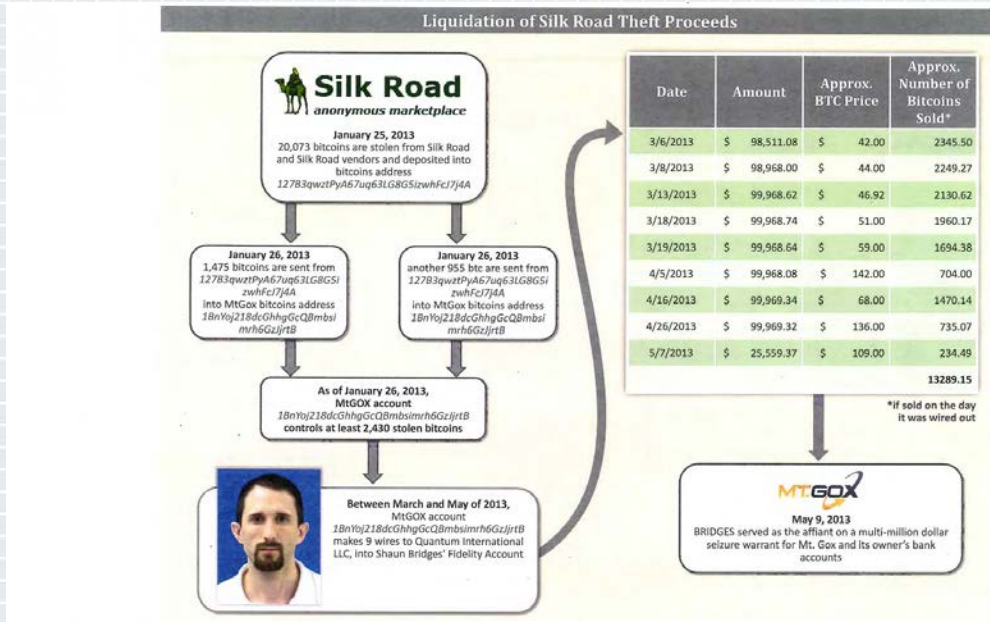
We are sorry to say, but we were robbed on Saturday 11/21/2013 by vendor EBOOK101. This vendor found bug in system and stole 5400 BTC - your money, our provisions, all was stolen. We were trying to resolve this problem, but we were not successful. We are sorry for your problems and inconvenience, all of current BTC will be distributed to users, who have filled correct BTC emergency adress.

I would like to thank to all SheepMarketplace moderators by this, who were helping with this problem. I am very sorry for this situation. Thank you all.

New alternative Marketplace:
<http://tormarkozaegyvco.onion/>

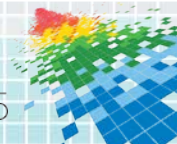
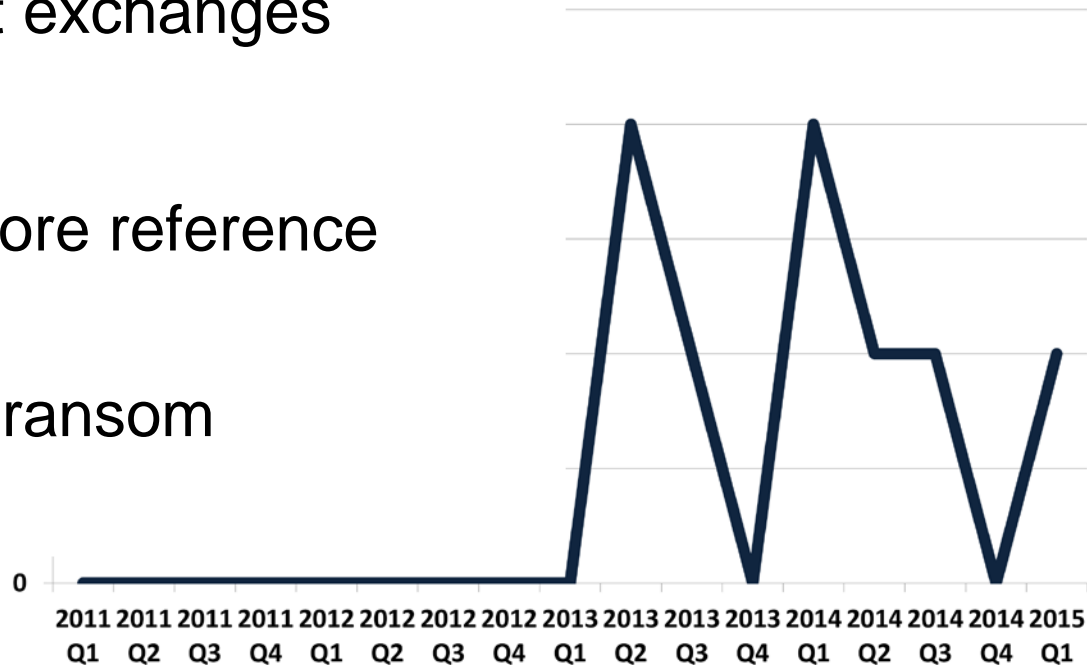


Federal Agents Accused of Stealing SR Funds



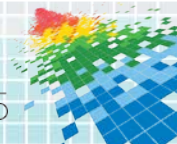
DDoS

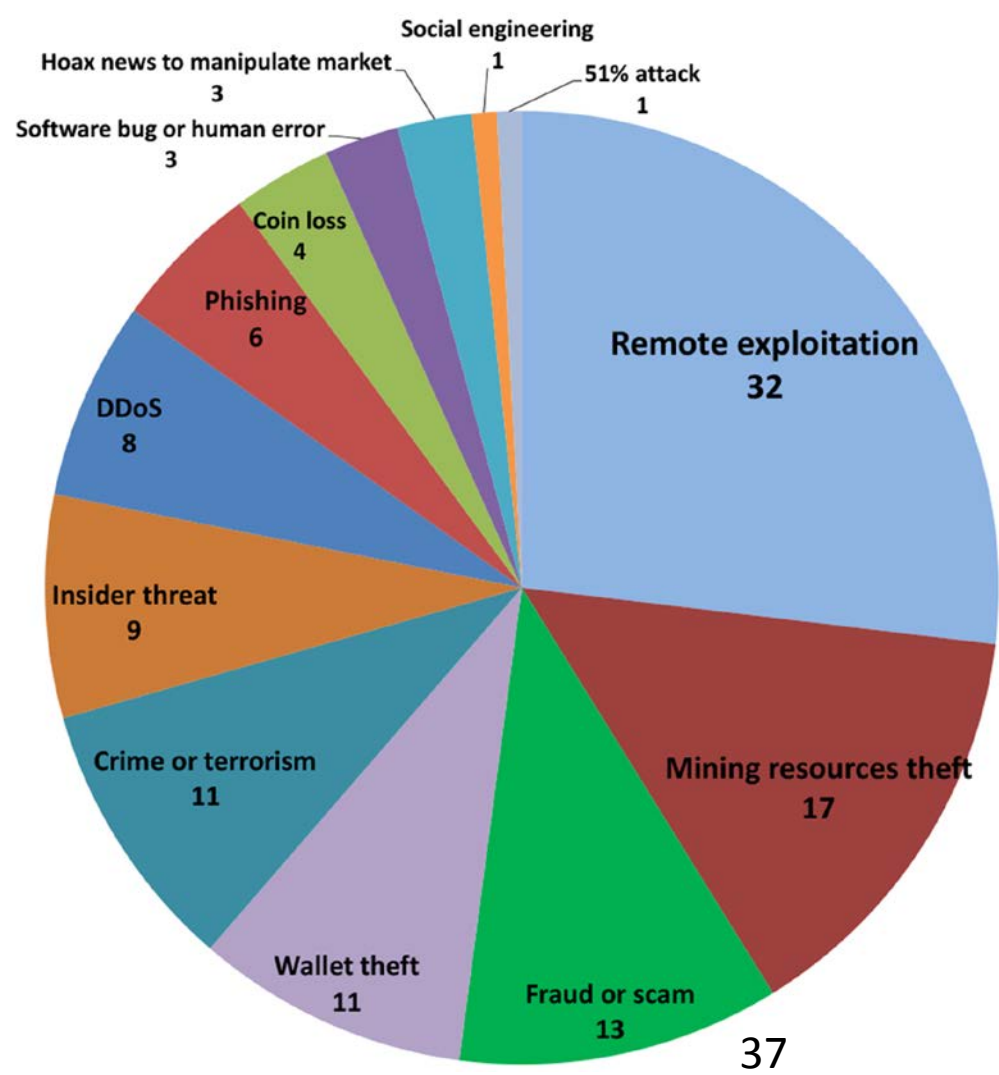
- ◆ Targeted DDoS against exchanges
- ◆ Cross-exchange DDoS
- ◆ DDoS against Bitcoin core reference design
- ◆ DDoS mining pools for ransom



Phishing

- ◆ Phishing emails seemingly from blockchain wallet
 - ◆ High click rate
- ◆ Spear-phishing Silk Road auction enquirers
- ◆ Phishing Bitcoin exchange users

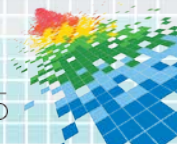




- Remote exploitation
- Mining resources theft
- Fraud or scam
- Wallet theft
- Crime or terrorism
- Insider threat
- DDoS
- Phishing
- Coin loss

Questions

- ◆ Does Bitcoin facilitate money laundry, or its detection? Both? Neither?
- ◆ How anonymous is Bitcoin?
- ◆ How does an attack against an exchange usually start?
- ◆ Does cryptocurrency promote ransomware
- ◆ Will we see more of CryptoLocker clones in the future demanding Bitcoin for encrypted file ransom?
- ◆ Which threat vector will impact Bitcoin's future most?
- ◆ What opportunities does Bitcoin bring to the security industry?
- ◆ How will Bitcoin impact the security industry?
- ◆ How to boost Bitcoin's wide adoption?
- ◆ Which threat vector is likely under-rated?



RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

<http://bit.ly/rsabitcoinpanel>



 #RSAC

RSA®Conference2015

San Francisco | April 20-24 | Moscone Center

**Questions:
Please Ask!**

