NormShield

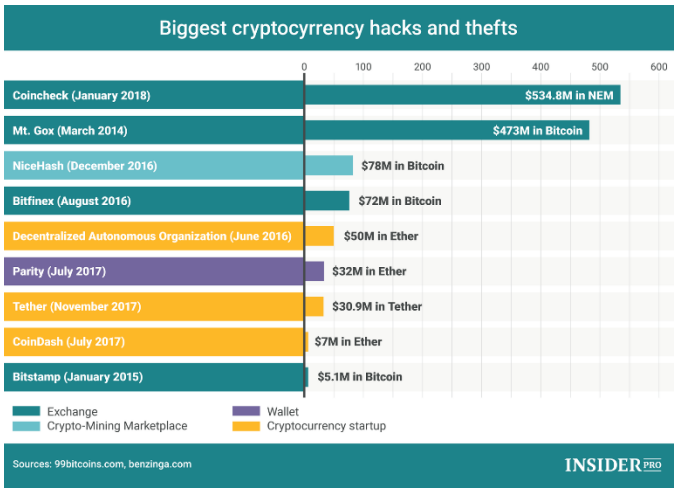
Is Your Money Safer in Cryptocurrency Exchange Markets than Banks?

Is Your Money Safer in Cryptocurrency Exchange Markets than Banks?

April 2018

Crypto coins are the new mean of investment and shopping and their exchange volume increases exponentially. There are many exchange markets handles these investments. However, the question of resiliency of these markets is on the rise with recent attacks.

In 2014, one of the largest crypto coin exchange market, Mt. Gox which was handling 70% of all bitcoin transactions back then, was hacked and lost $473 million resulting its closure and most dramatic fells in BTC. In 2016, Bitfinex suffered due to a cyber attack resulted in 120,000 BTC (≈$72 million back then). In January 2018, as the biggest cryptocurrency hack, more than half billion dollars was stolen from Coincheck. Very recently (on March 2018), Binance got reports from its customers about hijacked accounts. Binance reported that "a massive, well-coordinated phishing attempt" accumulated user accounts beginning from January. There were some fraudulent domains posed as Binance domains may have been a major part in this scam.



"The attacks on cryptocurrency markets create not only stolen money, but also manipulation on market price of crypto coins."

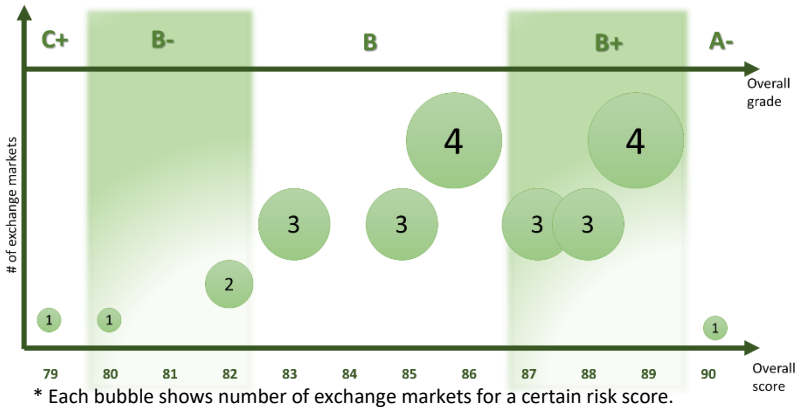
Methodology of Research

In March 2018, NormShield leveraged its proprietary Cyber Risk Scorecard platform to gather data on top 25 cryptocurrency markets (with respect to their volume), to analyze their cyber risk and security postures in 20 categories, and to compare the results in 12 selected categories. More information on our grading methodology and full list of our categories can be found here.

A Glance at Cryptocurrency Markets

The snapshot on overall grades of top cryptocurrency markets shows an acceptable level of security posture. Based on NormShield Risk Scorecard letter gradings, many markets receive B+ and B grade (ten in B and ten in B+). Only one of 25 markets could go as high as A- and one performs poorly and receives C+.

"Top 25 Cryptocurrency exchange markets receive overall scores between 79 and 80 (C+ and A- as counterpart letter grades)."



* Each bubble shows number of exchange markets for a certain risk score.

Compared to banking companies, grades of cryptocurrency markets are higher. This is mainly because number of assets (domains, subdomains, IPs, e-mails, employees) of banks are much larger than cryptocurrency exchange markets. Another very important factor is third-party risk that banks possess. The large number of third-party vendors of banks introduces invisible cyber risk to banking systems, which lowers the security ratings. On the other side, cryptocurrency markets are quite new and possess less number of assets that limits the attack surface for hackers.

With the increasing interest on crypto coins, cryptocurrency markets' websites and resources are visited for transactions and monitoring more often than ever. With these increased attention, we can expect increase in malicious users scans to find a vulnerability to exploit in these websites and resources.

Looking at the detail grades reveals some important risk factors of cryptocurrency markets and shows that these markets are vulnerable to similar types of attacks designed for financial institutions.

Low grades on CDN security (security and reputation of external links), fraudulent domains (domains that can be used for scams and phishing attacks), and credential management (leaked and shared credentials) are three examples of risk factors that is common for financial services. Cybercriminals desires to hijack user and employee accounts to empty wallets of crypto coin investors.

	DNS Health	E-mail Security	SSL/TLS Strength	DDoS Resiliency	Network Secuirty	Faudulent Domain	Credential Mgmt.	IP Reputation	Hacktivist Shares	Patch Mgmt.	CDN Security	Website Security
Market 1	B	D	A	B	A	D	B	A	D	D	D	C
Market 2	B	B	A	A	A	A	A	A	A	A	B	A
Market 3	B	A	A	B	D	D	A	A	A	A	D	B
Market 4	B	A	B	C	A	C	F	A	A	B	D	B
Market 5	A	A	A	A	B	A	A	D	A	B	B	A
Market 6	B	A	B	A	A	C	A	A	A	C	D	B
Market 7	A	A	D	A	B	A	A	A	A	B	B	A
Market 8	A	B	A	B	D	A	B	B	A	A	A	A
Market 9	B	A	A	A	B	A	A	B	B	A	A	D
Market 10	B	A	B	D	A	A	F	D	A	A	C	A
Market 11	A	B	B	B	A	A	C	A	A	C	A	A
Market 12	B	C	B	C	B	A	B	B	A	B	D	C
Market 13	B	A	A	B	A	A	A	B	B	A	B	C
Market 14	B	A	A	B	A	A	B	A	A	C	D	A
Market 15	B	A	B	A	A	A	A	A	A	A	B	A
Market 16	B	C	A	A	B	A	A	A	A	A	B	A
Market 17	B	A	B	A	A	D	A	A	A	A	A	A
Market 18	B	A	A	A	D	A	D	B	A	B	D	A
Market 19	C	D	B	A	B	A	C	A	A	A	D	A
Market 20	B	A	A	A	A	D	A	A	A	A	D	A
Market 21	B	A	A	A	C	A	A	D	B	C	C	A
Market 22	B	A	A	B	A	A	A	D	A	A	A	C
Market 23	A	B	A	A	A	D	A	A	A	A	B	A
Market 24	C	B	A	B	A	A	A	A	A	A	A	D
Market 25	A	B	A	B	B	A	C	D	C	B	D	B

* Letter grades of each market for selected categories.

Why cryptocurrency markets are trending targets in the hacker community?

The short answer is money. Cryptocoins, once stolen, are difficult to trace back and cyber criminals take advantage of this criminal luxury. The high market value of some crypto coins such as Bitcoin (BTC) makes it very attractive for hackers. Capturing low amount of BTC may result in high amount of US dollars in hackers hands.

Since the exchange markets are quite new to finance industry, lack of security experience makes them more attractive and vulnerable targets for cyber criminals. Manipulating currency exchange values may create huge rippling effects with the result of intentional value loss on some currencies. The financial effect makes them appealing for hacktivists whose objective is to harm certain financial institution for political reasons.

***[*Industry Insights]**
While individual company performance ranged from A to F, no industry group received higher than a C grade when measured across all categories.

NormShield Cyber Security Risk Brief 2018

Top Three Risk Factors

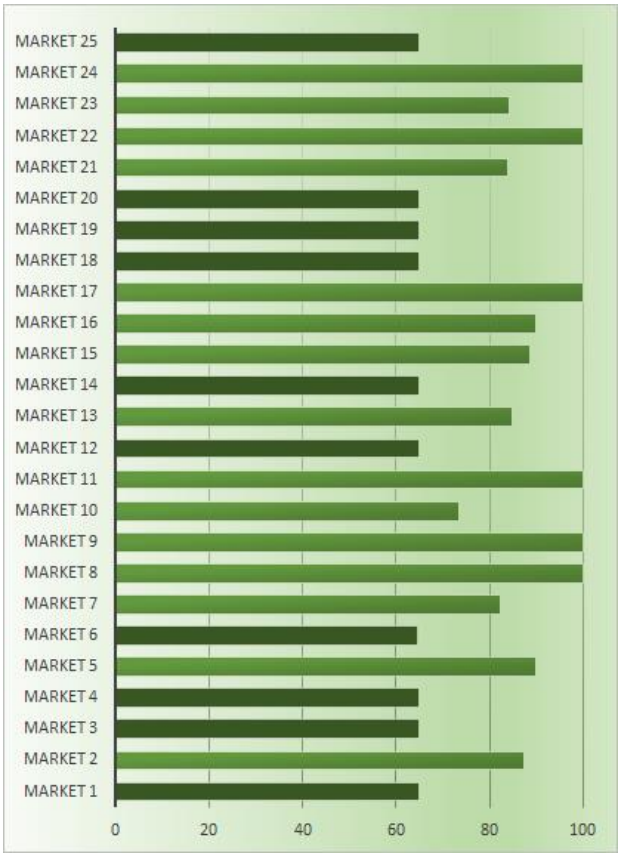
Companies and corporations in all industries encounter different cyber risks every day and experience difficulties while mitigating them. Cryptocurrency exchange markets perform poorly in CDN Security, Fraudulent Domains, and Credential Management.

CDN Security

"We observe that 9 out of 25 exchange markets perform very poorly in CDN security"

A content delivery network (CDN) is a large distributed system of servers deployed in multiple data centers across the Internet. Companies use a CDN for online libraries like JQuery.

Normshield analyzes the CDN content to detect possible vulnerabilities. Ensuring the security of files obtained from a CDN ultimately requires a layered set of controls -- including malware scanning, content filtering, and threat intelligence -- that can analyze and block malicious code when it's detected.



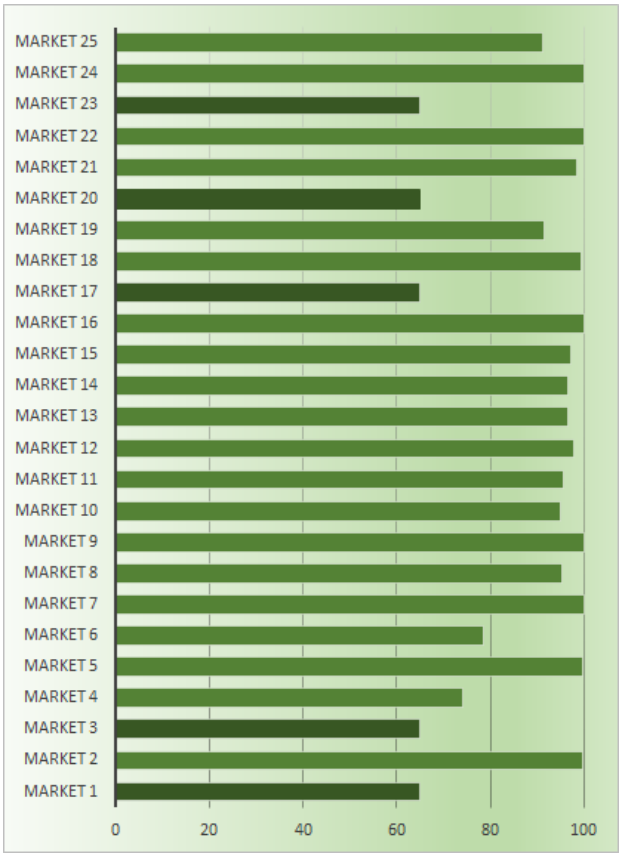
* CDN Security scores for each market.

Fraudulent Domains

Domain name scams are types of Intellectual property scams or confidence scams in which unscrupulous domain name registrars attempt to generate revenue by tricking businesses into buying, selling, listing or converting a domain name. Fraudulent or scam domains are frequently used by phishing attacks those targeting either a company's employees or customers. Potential phishing domains can be searched by one of NormShield free services here.

"NormShield scorecard found more than 800 potential fraudulent domains (possibility over 75%)."

NormShield extracts fraudulent domains and subdomains from the domain registration database. The registered domains database holds more than 300M records.

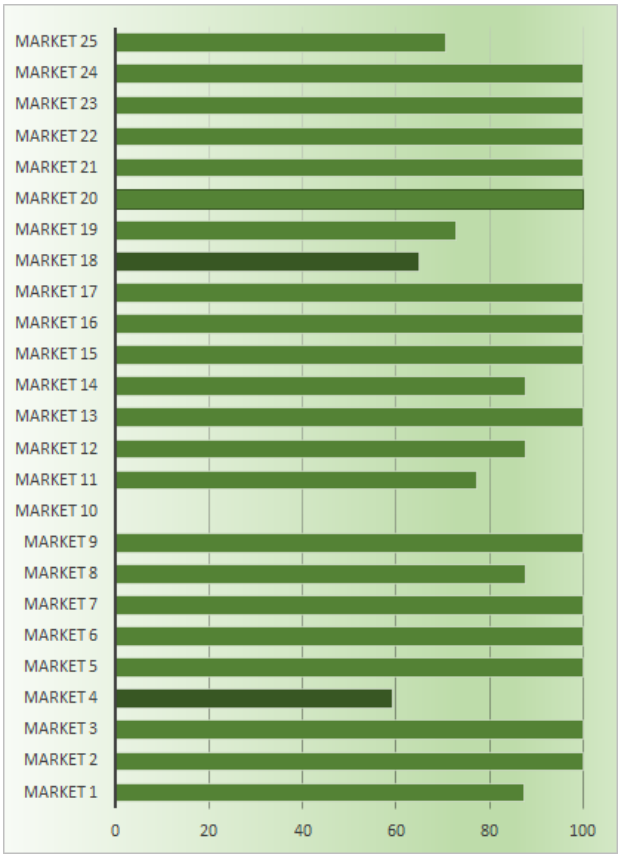


* Fraudulent Domain scores for each market.

Credential Management

There are more than 5 billion hacked email / password available on the internet and underground forums. NormShield finds and shows the leaked or hacked emails & passwords. In the simplest form, email list of employees can be used for phishing attack. Most of internet users use same passwords for different web application accounts.

In this search, NormShield found 27 leaked credentials for a specific exchange market (marked as Market 10) shared in last 90 days.



* Credential Management scores for each market.

Conclusion

Cryptocurrency exchange markets must vigorously mitigate cyber risks to reduce exposure to cyber attacks, improve incident response time, continue use of necessary security services, and proactively take measurements against potential cyber threats. Considering the impact of cyber attacks against those markets, exchange markets should discover possible attacks in advance to avoid huge financial and reputational loss. Some on-site security services might not be sufficient to identify some threats such as phishing attacks by using fraudulent domains. If credentials of legitimate users are leaked and shared in hacker forums, it might be too late to avoid the loss when the attack is detected.

Cryptocurrency exchange markets can leverage use of an external risk management product such as NormShield Risk Scorecard to detect such threats and proactively mitigate the risk raised by these threat actors.

About NormShield

We provide Cyber Risk Scorecard for companies just like FICO score. Cyber security is on every Board's agenda, and the average total cost of a data breach has risen to $4 million (Ponemon/IBM). NormShield Cyber Risk Scorecards provide the information necessary to protect business from cyber-attacks. The scorecards provide a letter grade and a drill down into the data for each risk category so that remediation of vulnerabilities can be prioritized. Unified Threat & Vulnerability Orchestration Platform and Cyber Risk Scorecard.

To learn your company's risk score, please visit https://www.normshield.com/ and click on Learn Now.

There are five main reasons to find your organization's risk scores.

- Provide Intelligence for Decision-Making

- Help Determine ROI

- Justify Cyber Budgets

- Manage Vendor Risk

- Evaluate Cyber Insurance Subscribers

www.normshield.com

1 (571) 335 02 22

info@normshield.com

NormShield HQ
8200 Greensboro Drive
Suite 900
McLean, VA
22102