REDOWL

Intsights

Detect. Analyze. Remediate.

Monetizing the Insider

The Growing Symbiosis of Insiders and the Dark Web

Ido Wulkan (IntSights)
Tim Condello (RedOwl)
David Pogemiller (RedOwl)

scan to send this
report to your email

Contents

Executive Summary

Organizations face asymmetric and unprecedented risks from insiders — employees and contractors who have valid access to enterprise networks. Insider risk is on the rise in part due to the growing influence of the dark web, a portion of the internet that enables anonymity. The dark web is being increasingly used by cybercriminals for recruiting insiders to help steal data, make illegal trades or otherwise profit.

RedOwl and IntSights collaborated to better understand how the dark web contributes to the increase of insider risk. By studying dark web forums focused on recruiting and collaborating with insiders, we found:

- The recruitment of insiders within the dark web is active and growing. We saw forum discussions and insider outreach nearly double from 2015 to 2016.
- The dark web has created a market for employees to easily monetize insider access. Currently, the dark web serves as a vehicle insiders use to "cash out" on their services through insider trading and payment for stolen credit cards.
- Sophisticated threat actors use the dark web to find and engage insiders to help place malware behind an organization's perimeter security. As a result, any insider with access to the internal network, regardless of technical capability or seniority, presents a risk.

To combat the problem, risk management teams should join the growing number of organizations that are actively building insider threat programs. Ironically, 80 percent of security initiatives focus on perimeter defenses, while fewer than half of organizations budget for insider threat programs.[1]

About the Authors

Ido Wulkan

Ido has a decade of experience in intelligence research and analysis, focusing on the deep and dark web. Ido served in one of the leading intelligence units of the Israeli Defense Force (IDF) as a cyber intelligence analyst, where he gained intimate knowledge of various threat actors and their techniques. Following his service, Ido worked at several intelligence firms as an analyst and team leader, where he expanded his knowledge of cybercrime ecosystems. Ido now leads IntSights' cyber intelligence analysts team, where he serves as a focal point for all IntSights' intelligence.

Tim Condello

Tim has worked in cybersecurity in the private sector as well as in the US military. Currently, Tim is a technical account manager at RedOwl, helping customers build and deploy insider risk programs. Tim worked as a cyber threat intelligence researcher at BNY Mellon bank. As a member of BNY's insider threat team, Tim's responsibilities included dark web investigations and working with the National Cyber-Forensics & Training Alliance (NCFTA).

David Pogemiller

As VP of strategy, David has spent the past two years leading deployments and analytic implementations for RedOwl customers putting in place insider risk programs. Prior to RedOwl, David was a manager at Bridgewater Associates, a hedge fund. Before Bridgewater, David was COO at a small economic consulting firm that was acquired by Moody's.

1 http://www.dqindia.com/insider-threat/

Insider Motivations and the Influence of the Dark Web

Verizon's annual data breach report[2] found that insiders have been one of the most persistent sources of digital attacks for years. The report cites two primary drivers: the promise of financial gain and the ease of executing an attack.

How does the dark web impact these motivations? We believe the dark web exacerbates three psychological considerations driving the calculations of an insider:

Value of Action | The dark web has created a marketplace with ready buyers and collaborators that enable the monetization of insider actions. Namely, the dark web catalyzes malicious insider activity by facilitating the ability to cash out with diminished risk of detection.

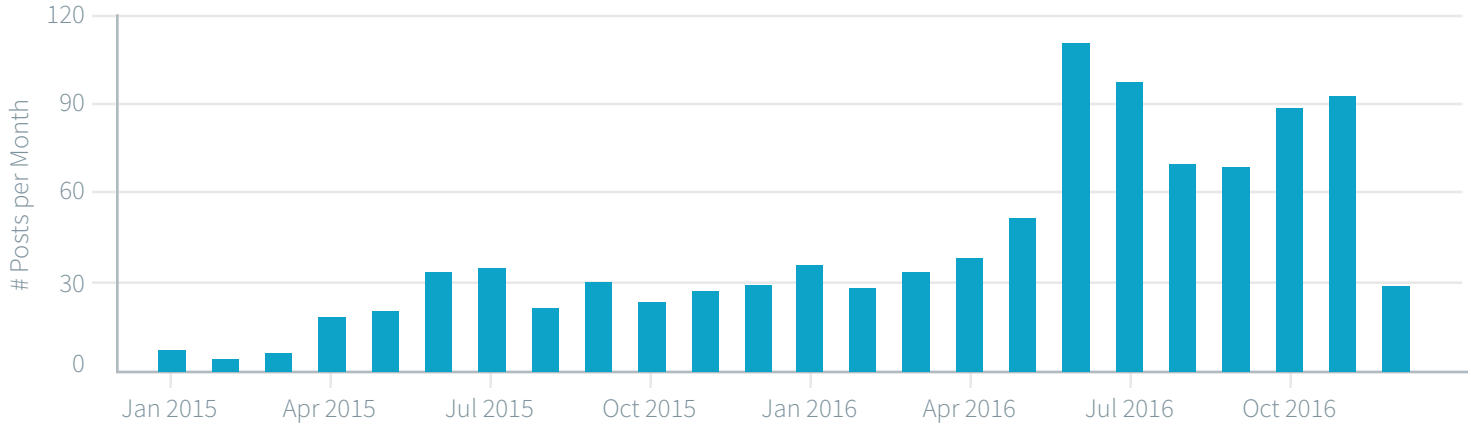
Cost of Action | Sophisticated criminals on the dark web can arm less sophisticated insiders with the knowledge and tools they need to take action. Worse, less sophisticated insiders can collude with sophisticated actors to execute more complicated attacks.

Risk of Detection | The anonymity of the dark web dramatically reduces detection concerns. Also, collusion with threat actors helps provide insiders with technical tools to enhance evasion.

Tracking Insider Activity on the Dark Web

Using a combination of covert techniques and searching, researchers monitored insider activity on the dark web and tracked the volume of references to insiders in cybercrime forums over the past two years. Each individual post referencing insiders counted as a unique instance. Also, each post was reviewed by an analyst to validate that the references to insiders were in the right context. Over the course of two years, we saw approximately 1,000 references with a spike occurring in the closing months of 2016.

Figure 1: Mentions of insiders in dark web forums, 2015-2016



2 https://msisac.cisecurity.org/whitepaper/documents/1.pdf

A Look Inside Dark Web Activity

Our research identified some areas where insiders engage on the dark web:

- Insider trading (i.e., trading on information not available to the public at large).
- Selling credit card numbers stolen from retail sector employees.
- The "weaponization" of insiders by threat actors.

Insider Trading

Threat actors use dark web forums to recruit insiders and collude. With the insider's information, the threat actor attempts to profit with more educated stock market bets. The insider receives a commission. The dark web facilitates illicit trading activity by providing anonymity, making actors difficult to identify.

The insider trading forums we investigated were exclusive. Though some activity may be happening in generic black markets, it appears that the most potent information and sophisticated actors are in closed, small groups. These groups require those who apply for membership to prove their capabilities and/or access to knowledge by sharing real inside information, which is then thoroughly checked and confirmed.

One forum (see Figure 2), the "KickAss marketplace," exists in a very prominent dark web community. This particular insider trading subforum was established on February 2016, and the forum's insider trading purposes include:

- Stock Market Trading
- Forex Trading
- Commodities
- Aggressive Business Remodeling
- The "Know What's Happening Before the Rest" Technique

Figure 2: Insider Trading KickAss marketplace

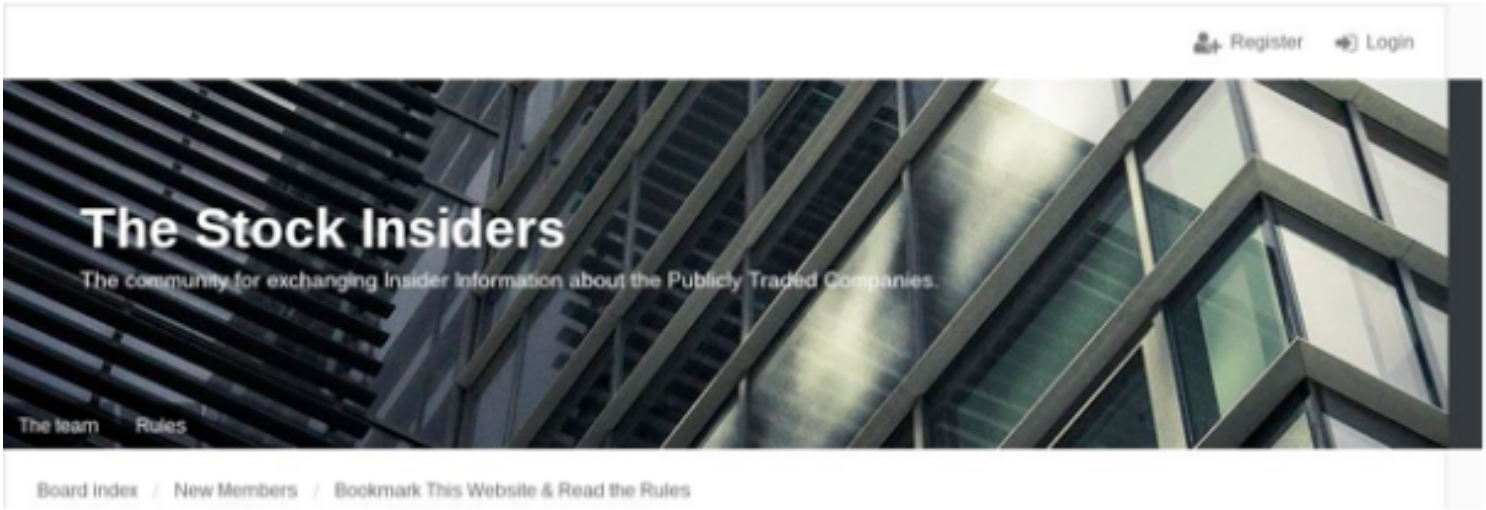
The forum's managers claim to enforce high standards. For example, the forum claims to review every post for accuracy before publication. In return for this high bar, the forum requires a significant membership fee of 1 BTC[3], or Bitcoin.

The forum appears relatively active with approximately five posts per week and a total of 40 BTC in transactions (approximately $35,800, see fee transactions in Appendix 1). According to the group's manager, there are members who make more than $5,000 USD a month using the leaked information.

3 The exchange rate as of 20 January 2017 was 1 BTC = $895.

This forum is not alone. Another forum (see Figure 3), called "The Stock Insiders," is also dedicated solely to insider trading. The forum was opened in April 2016. Its objective was to "…create a long-term and well-selected community of gentlemen who confidently exchange insider information about publicly traded companies." The administrator claims to be "a former successful (originally European) IT entrepreneur living in the U.S. […] also an active trader and has inside access to several publicly traded companies."

Figure 3: The Stock Insiders Forum

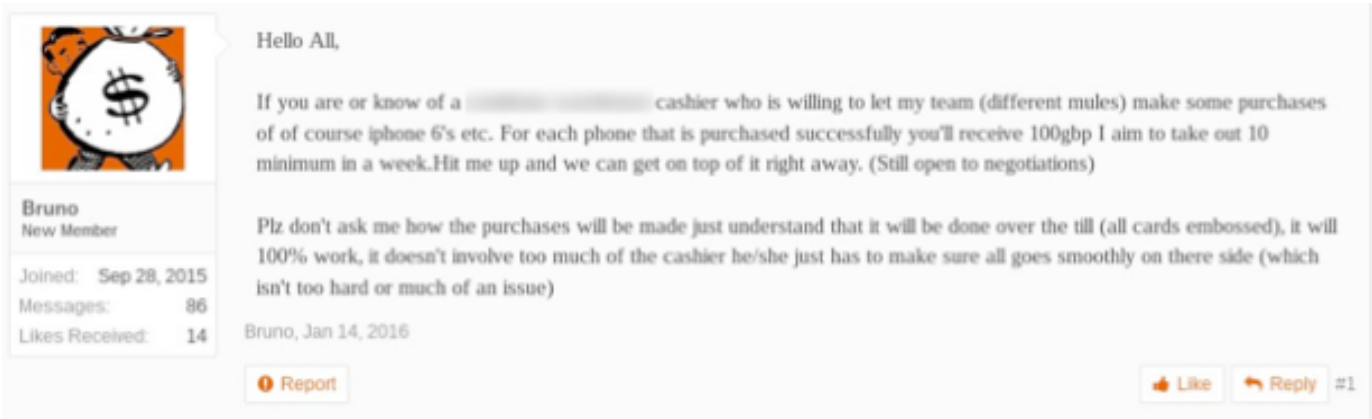


Recruiting Retail Insiders

Our research also showed continued recruiting of retail workers that have access to consumer credit card information. Sophisticated actors will then engage in carding, a generic name referring to the extraction of money from stolen credit cards, for personal profit. Typically, recruiters target lower-ranked employees, such as cashiers, whose help is needed to use stolen credit cards.

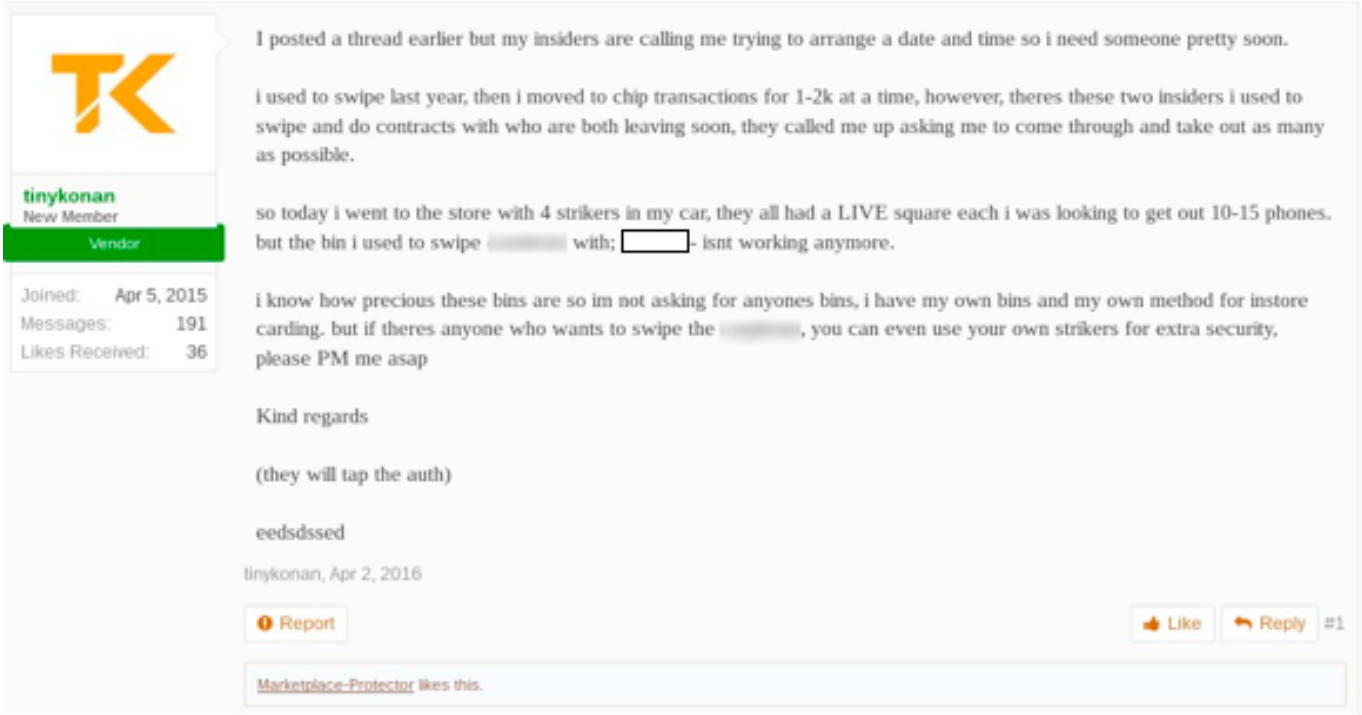
In Figure 4, a dark web forum member uploads a wanted ad in which he asks for the services of a cashier in a well-known retail chain store to help purchase iPhones:

Figure 4: Dark web member soliciting help from an insider



In Figure 5, a recruiter asks for cashiers who would be willing to swipe stolen credit card credentials:

Figure 5: Recruiter seeks insider help with credit card theft



Weaponizing the Insider

Sophisticated hackers within the dark web are able to arm insiders with the tools and knowledge necessary to help steal data and commit fraud, among other acts, and also to cover any tracks.

In one instance, a hacker solicited bank insiders to plant malware directly onto the bank's network. This approach significantly reduces the cost of action as the hacker doesn't have to conduct phishing exercises and can raise success rates by bypassing many of the organization's technical defenses (e.g. anti-virus or sandboxing).

To illustrate this activity, Figure 6 shows an ad soliciting bank employees. The poster makes it clear that the employee's rank within a bank does not matter as long as he has access to the bank's computer.

Figure 6: Dark web recruitment of an insider to defraud a bank

On the forum, in Figure 7, the attacker explains the approach to a potential collaborator, indicating that he needs direct access to computers that access accounts and handle wire transfers, and that he offers to pay “7 figures on a weekly basis” for continued access.

Figure 7: An insider collaborating with a threat actor on a dark web forum

[redacted]: I am going to have to check it more thoroughly, but specifically I can say the branch I work at has zero security awareness so I have quite a free access

(17:19:11) **lacazatte@dukgo.com/Home:** Great

(17:19:18) **lacazatte@dukgo.com/Home:** When will i hear from you?

(17:20:37)

[redacted]: Well its a 9 to 17 work, so I'm guessing in the evening

(17:20:53) **lacazatte@dukgo.com/Home:** I need access to the computers that handle transfers. If you can't get direct access to those computers, a lesser one will do. It means i'll have to escalate my privilege to the right computer, but if you give me direct access to it, that would be great.

(17:21:00) **lacazatte@dukgo.com/Home:** wire transfers.

(17:21:28)

[redacted]: got it, I don't think it will be a problem honestly

(17:21:53) **lacazatte@dukgo.com/Home:** and accounts. I don't transfer funds from the accounts of customers. I mainly create new ones stealthily. Most times no one knows what happened for a very long time.

(17:22:37)

[redacted]: fuck! that's genius! it is quite stealthy

[redacted]: how much money do I get from it?

(17:23:31) **lacazatte@dukgo.com/Home:** There's no limit to be honest with you.

(17:24:00) **lacazatte@dukgo.com/Home:** As long as i continue to have access you can earn 7 figures on a weekly basis.

(17:24:39)

[redacted]: I'll talk to you tomorrow evening

(17:24:56) **lacazatte@dukgo.com/Home:** Alright

Conclusion: The Dark Web is Tilting the Insider Threatscape

The dark web has an active community of sophisticated buyers and collaborators who are aiding in the monetization and even weaponization of malicious insider activity. The ease with which employees can now learn about and access the dark web means that it will continue to grow in its impact over the coming years.

What can security and risk teams do? To combat the problem, risk management teams should join the growing number of organizations that are actively building insider threat programs. Ironically, nearly 80 percent of security initiatives focus on perimeter defenses, while fewer than half of organizations budget for insider threat programs. That means many insider threat events often go completely undetected. According to a 2016 Gartner survey presented at the 2016 Gartner Security Summit, only 18 percent of enterprises have a formal insider threat program in place.

Enterprises hoping to build an insider threat program must consider:

Influencing Culture | A powerful lever that organizations have to mitigate the threat from insiders is culture. Enterprises should create, train and enforce consistent corporate security policies while protecting employee privacy. Ensuring that employees and contractors understand the rules — and penalties — of engaging in insider behavior carries tremendous impact.

Vigilance Across the Employee Base | A recent Forrester report on insider threats noted, "Treating insiders as a technology problem ignores the human aspects of motivation and behavior."[4] Security teams must monitor employee behavior across a broad array of channels that identify suspicious employee activity, but also help understand negative employee sentiment.

The Right Technology | Building an effective insider threat program requires a robust security ecosystem built on a foundational capability to see across all employee activity and spotlight unwanted behavior while respecting employee privacy.

4 *Hunting Insider Threats, Forrester's Model For Establishing An Insider Threat Team*, July 20, 2016, by Joseph Blankenship.

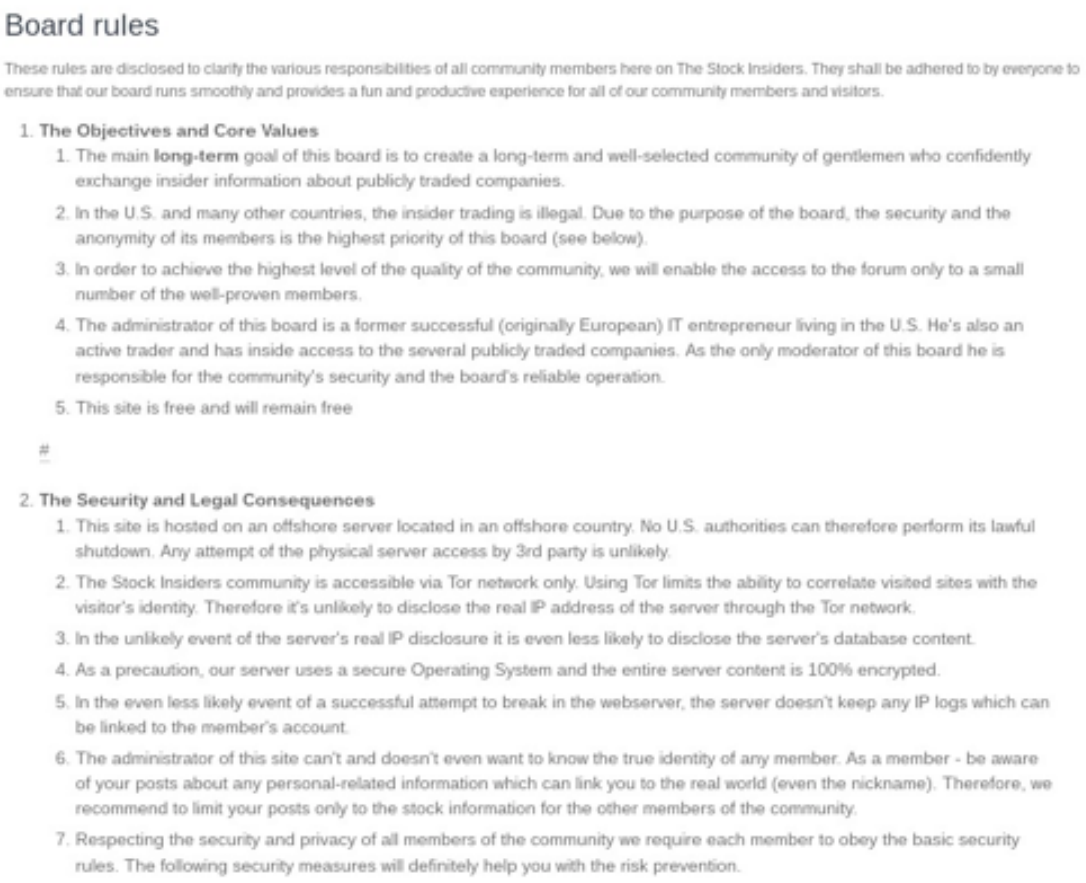
Appendix I: Transactions to Insider Trading Forum

The chart below is the list of BTC accounts that are used by the Kick Ass marketplace forum.

Address	Total Received	Final Balance	# of Transactions
19JTncP1EwBvpsTpfmMpg7weJFJCQsoqUL [5]	0-BTC/$0.00	0-BTC/$0.00	0
17oUCfkt3kQqstbsSpujYyQwH5Hk5D9Q3b [6]	8-BTC/$7,160.00	0-BTC/$0.00	34
178GrbdgyXUNSrUpsDhDeXADba4PcFAZbF [7]	92.1-BTC/$82,429.50	$0.43	184

Appendix II: Transactions to Insider Trading Forum

The chart below is the list of BTC accounts that are used by the Kick Ass marketplace forum.



Board rules

These rules are disclosed to clarify the various responsibilities of all community members here on The Stock Insiders. They shall be adhered to by everyone to ensure that our board runs smoothly and provides a fun and productive experience for all of our community members and visitors.

1. **The Objectives and Core Values**
   1. The main **long-term** goal of this board is to create a long-term and well-selected community of gentlemen who confidently exchange insider information about publicly traded companies.
   2. In the U.S. and many other countries, the insider trading is illegal. Due to the purpose of the board, the security and the anonymity of its members is the highest priority of this board (see below).
   3. In order to achieve the highest level of the quality of the community, we will enable the access to the forum only to a small number of the well-proven members.
   4. The administrator of this board is a former successful (originally European) IT entrepreneur living in the U.S. He's also an active trader and has inside access to the several publicly traded companies. As the only moderator of this board he is responsible for the community's security and the board's reliable operation.
   5. This site is free and will remain free

#

2. **The Security and Legal Consequences**
   1. This site is hosted on an offshore server located in an offshore country. No U.S. authorities can therefore perform its lawful shutdown. Any attempt of the physical server access by 3rd party is unlikely.
   2. The Stock Insiders community is accessible via Tor network only. Using Tor limits the ability to correlate visited sites with the visitor's identity. Therefore it's unlikely to disclose the real IP address of the server through the Tor network.
   3. In the unlikely event of the server's real IP disclosure it is even less likely to disclose the server's database content.
   4. As a precaution, our server uses a secure Operating System and the entire server content is 100% encrypted.
   5. In the even less likely event of a successful attempt to break in the webserver, the server doesn't keep any IP logs which can be linked to the member's account.
   6. The administrator of this site can't and doesn't even want to know the true identity of any member. As a member - be aware of your posts about any personal-related information which can link you to the real world (even the nickname). Therefore, we recommend to limit your posts only to the stock information for the other members of the community.
   7. Respecting the security and privacy of all members of the community we require each member to obey the basic security rules. The following security measures will definitely help you with the risk prevention.

5 *19JTncP1EwBvpsTpfmMpg7weJFJCQsoqUL | https://blockchain.info/address/19JTncP1EwBvpsTpfmMpg7weJFJCQsoqUL*
6 *17oUCfkt3kQqstbsSpujYyQwH5Hk5D9Q3b | https://blockchain.info/address/17oUCfkt3kQqstbsSpujYyQwH5Hk5D9Q3b*
7 *178GrbdgyXUNSrUpsDhDeXADba4PcFAZbF | https://blockchain.info/address/178GrbdgyXUNSrUpsDhDeXADba4PcFAZbF*

About RedOwl

RedOwl provides an insider risk management platform. Only RedOwl unlocks the power of existing corporate data to identify and mitigate unwanted behavior by ingesting structured, unstructured, and business data to analyze interactions between employees, contractors, devices, files, and applications. Using a combination of statistical pattern matching, machine learning, and content analytics to profile user behavior, RedOwl gives risk management professionals the in-depth narratives required to effectively pinpoint and distinguish negligent, compromised, and malicious employees.

www.redowl.com

About IntSights

IntSights brings together threat intelligence coming from the dark web. IntSights infiltrates the dark web to detect and analyze planned or potential attacks. IntSights provides customers with a one-stop-shop solution combining rapid and actionable intelligence with threat mitigation and remediation.

www.intsights.com

REDOWL

Intsights

Detect. Analyze. Remediate.