Gold Rush on the Dark Web:

Threat Actors Target X (Twitter) Gold Accounts

Author: Rishika Desai

INDUSTRY:
SOCIAL MEDIA

REGION:
GLOBAL

White papers and reports can be downloaded from the CloudSEK website by visiting https://cloudsek.com/whitepapers-reports or by mailing to info@cloudsek.com.

INTRODUCTION

Getting official on Twitter (now known as X) gives the audience a sense of brand and recognition. We all know the impact of a tweet coming from a blue checkmark. Before Elon Musk bought Twitter and changed policies further, these blue ticks were subjected to verification. As of today, anyone can purchase a blue tick mark. In addition, Twitter also rolled out another paid feature where organizations can verify themselves and get the tag of 'Gold,' and NGO and governmental bodies can get recognized as 'Grey'. Currently, all three tags (blue, gold, and grey) are offered by Twitter through paid subscription basis every month.

Dark web forums and marketplaces have a dedicated section where social media sales are extensively observed. Recently, there has been a surge of posts where threat actors were selling accounts with Twitter Gold verification. A strikingly similar series of advertisements was also seen on Telegram channels, indicating that malicious campaigns are brooding on a large scale that requires a Twitter Gold account.

The advertisements on the dark web can be traced back to multiple online shops and their marketing partners, such as Facebook, Telegram, etc. Some X account providers have hosted their shops successfully for over four years and used the same medium to advertise Twitter Gold accounts. The amount of shops and service providers today is humongous, and most of them can be detected by running simple Google Dorks.

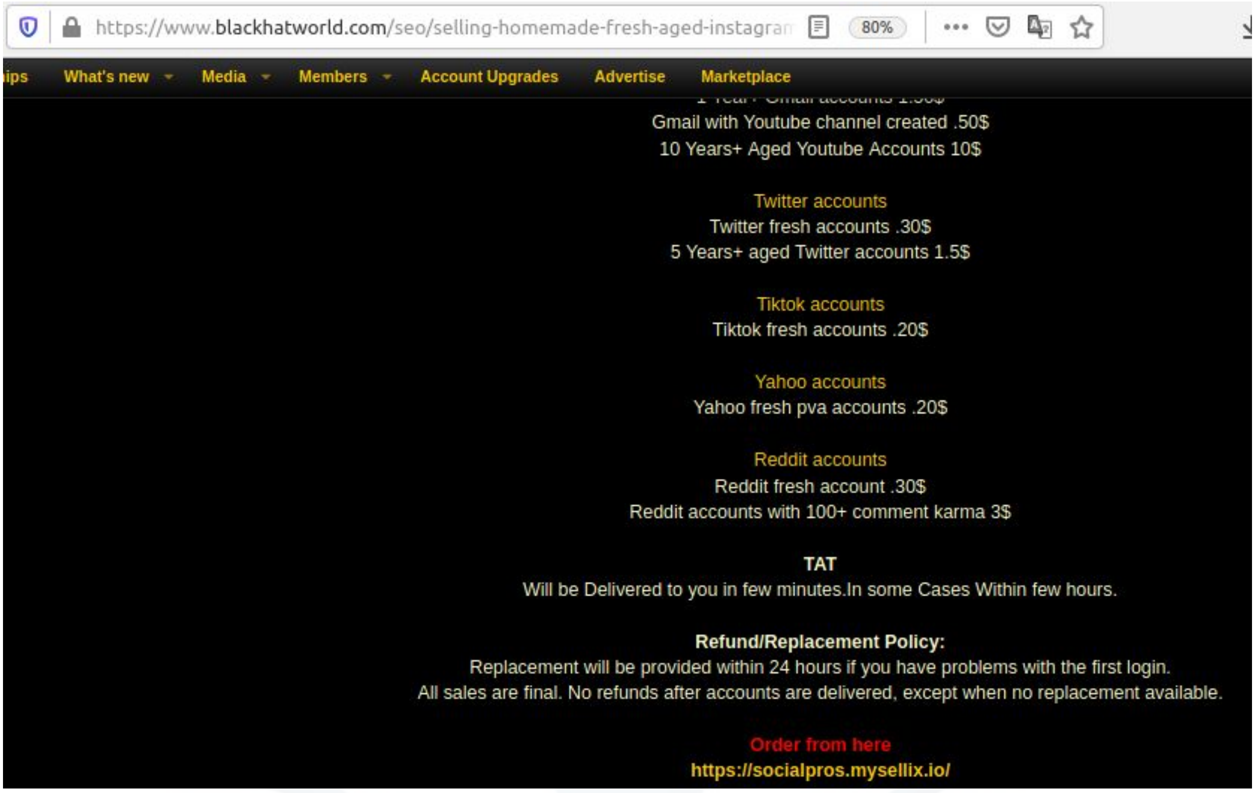
To detect on Facebook: Enter 'Twitter Gold Buy' and relevant keywords in the search box to identify users and channels offering Twitter Gold.

To detect on Telegram: Hunt for keywords ‘Twitter Gold' to check the channels offering Twitter Gold. [1]

To detect by OSINT: Some primary resources can be accessed by typing "Buy Twitter Gold" in the search bar. [2]

There are different price ranges offered for Twitter accounts. Dark web forums have a list sheet and a dedicated social media accounts section that offers Facebook, Instagram, Yahoo, and TikTok accounts. These accounts are provided in multiple ways:

1. The advertisers are people who manually make accounts, get them verified, and are ‘ready to use’ for their buyers. This is ideal for criminals who need pseudo-identity and do not want to be attributed to their actions.
2. Cybercriminals brute force the existing accounts by users using a generic username and password combo list. Various tools and pre-made configurations are available for free on the cybercrime forums. The tools used in this case are Open Bullet, SilverBullet, and SentryMBA.
3. Information stealer malware has a centralized botnet network, where credentials from infected devices are harvested. These credentials are then further validated according to buyers' requirements, such as individual or corporate accounts, number of followers, region-specific accounts, etc.


https://www.blackhatworld.com/seo/selling-homemade-fresh-aged-instagram
80%
ips
What's new
Media
Members
Account Upgrades
Advertise
Marketplace

Gmail with Youtube channel created .50$
10 Years+ Aged Youtube Accounts 10$

Twitter accounts
Twitter fresh accounts .30$
5 Years+ aged Twitter accounts 1.5$

Tiktok accounts
Tiktok fresh accounts .20$

Yahoo accounts
Yahoo fresh pva accounts .20$

Reddit accounts
Reddit fresh account .30$
Reddit accounts with 100+ comment karma 3$

TAT
Will be Delivered to you in few minutes.In some Cases Within few hours.

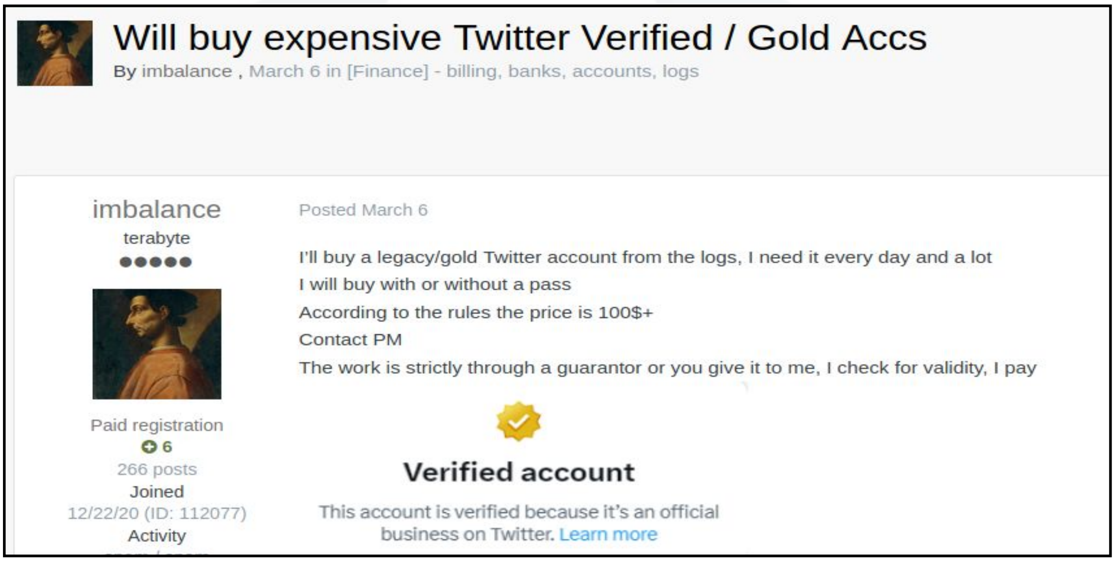
Refund/Replacement Policy:
Replacement will be provided within 24 hours if you have problems with the first login.
All sales are final. No refunds after accounts are delivered, except when no replacement available.

Order from here
https://socialpros.mysellix.io/

Image: Cybercriminal marketplaces offering Twitter Gold and other social media accounts

A hacked or compromised Twitter account can be exploited to mass spread phishing campaigns. This, in turn, damages the reputation and brand of the company whose account was compromised, clearly displaying a lack of stringent security policies and a weak incident response plan.

Since Twitter Gold was announced in December 2022, these services are not older than a year. The first advertisement can be traced back to March 2023, when a threat actor was looking to buy Twitter Gold accounts.



Will buy expensive Twitter Verified / Gold Accs

By imbalance , March 6 in [Finance] - billing, banks, accounts, logs

imbalance
terabyte
●●●●●
Paid registration
6
266 posts
Joined
12/22/20 (ID: 112077)
Activity

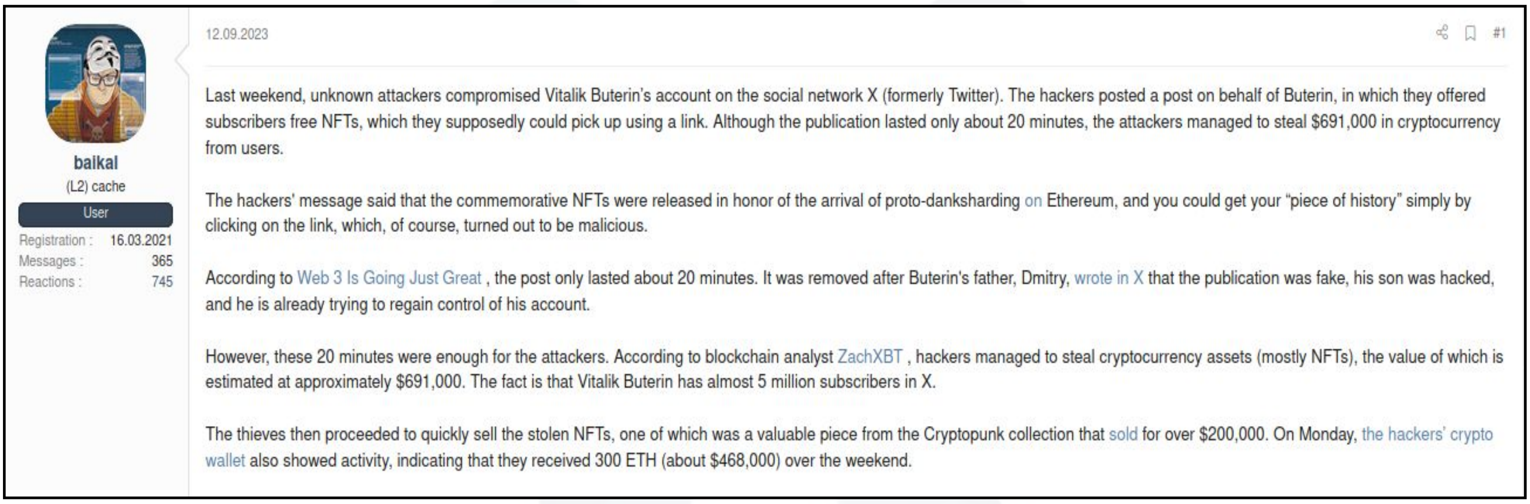
Posted March 6

I'll buy a legacy/gold Twitter account from the logs, I need it every day and a lot
I will buy with or without a pass
According to the rules the price is 100$+
Contact PM
The work is strictly through a guarantor or you give it to me, I check for validity, I pay

Verified account
This account is verified because it's an official business on Twitter. Learn more

Image: Threat actors advertising to buy Twitter Gold accounts on dark web marketplaces

An example is when, in September 2023, Vitalik, the co-founder of Ethereum, fell victim to a cyberattack that compromised his X (formerly Twitter) account. The perpetrators seized control of Buterin's profile and exploited his large following by posting a deceptive message offering free non-fungible tokens (NFTs) to unsuspecting users. The malicious link embedded in the tweet directed users to a fake website designed to drain cryptocurrency from their wallets. Despite being active for about 20 minutes, the hackers managed to siphon off a staggering $691,000 digital assets before removing the fraudulent post.



baikal
(L2) cache
User
Registration : 16.03.2021
Messages : 365
Reactions : 745

12.09.2023 #1

Last weekend, unknown attackers compromised Vitalik Buterin's account on the social network X (formerly Twitter). The hackers posted a post on behalf of Buterin, in which they offered subscribers free NFTs, which they supposedly could pick up using a link. Although the publication lasted only about 20 minutes, the attackers managed to steal $691,000 in cryptocurrency from users.

The hackers' message said that the commemorative NFTs were released in honor of the arrival of proto-danksharding on Ethereum, and you could get your "piece of history" simply by clicking on the link, which, of course, turned out to be malicious.

According to Web 3 Is Going Just Great , the post only lasted about 20 minutes. It was removed after Buterin's father, Dmitry, wrote in X that the publication was fake, his son was hacked, and he is already trying to regain control of his account.

However, these 20 minutes were enough for the attackers. According to blockchain analyst ZachXBT , hackers managed to steal cryptocurrency assets (mostly NFTs), the value of which is estimated at approximately $691,000. The fact is that Vitalik Buterin has almost 5 million subscribers in X.

The thieves then proceeded to quickly sell the stolen NFTs, one of which was a valuable piece from the Cryptopunk collection that sold for over $200,000. On Monday, the hackers' crypto wallet also showed activity, indicating that they received 300 ETH (about $468,000) over the weekend.

What did CloudSEK uncover?

Assuming the above example, the CloudSek research team identified such accounts on X (formerly Twitter), with a gold tick mark subscribed, posting links to malicious domains. These domains had the following:

A. Company's name but were hosted on a different top-level domain.
B. Different platforms, insisting their followers to join random channels based on crypto.
C. Content that can be tagged as spam.

Technical Analysis

Analysis of advertisements

After carefully inspecting the advertisements across deep and dark web advertisements, the price distributions varies based on the reasons below:

Type of X Account	Price
Fresh Account Homegrown	Avg $0.30
Fresh Account Blue Tick	Avg $35
Aged account (5 Years)	Avg $1.5
Aged account converted into Gold	Avg $1200- $2000
Addition of Blue Affiliates	Avg $150 per account
Addition of Gold Affiliates	Avg $500 per account

Boosting profitable opportunities for cybercriminals

Such advertisements also allow multiple opportunities for cybercriminals to become a guarantor of the deals since large amounts are involved. Additionally, such accounts are resellable, enabling a whole reseller market behind compromised accounts.

Different threat actors across the open and dark web had multiple claims while providing Twitter Gold accounts.

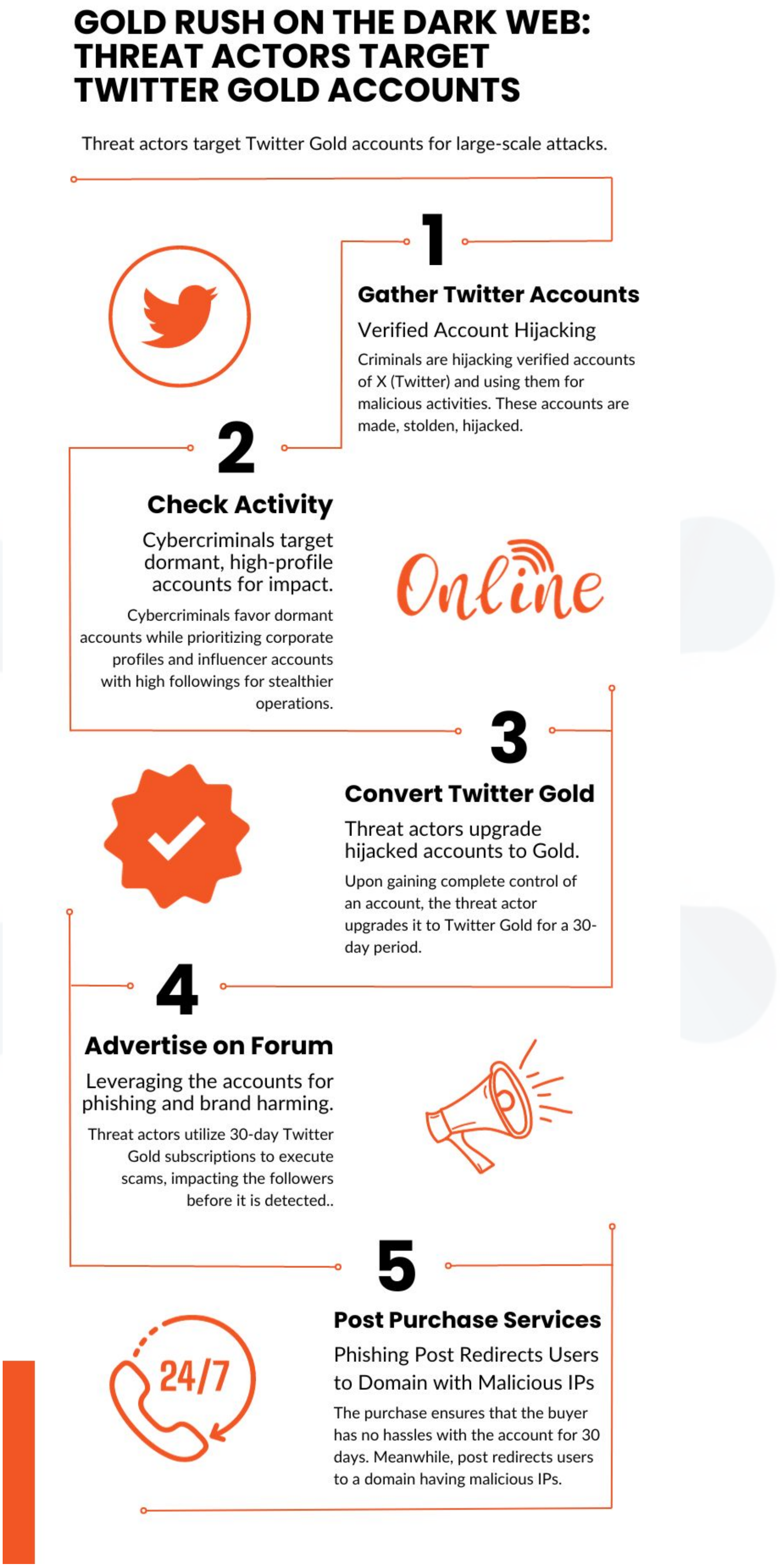
1. An actor engaged with our source mentioned providing 15 inactive accounts every week that should be further converted into gold subscriptions by the purchaser. This makes over 720 accounts annually. The price for each account was USD 35, totaling a little over USD 500 for 15 corporate and dormant accounts on Twitter.
2. Another set of advertisements openly mentioned the companies that were offered for sale, and depending on the brand and followers of this account, the accounts with a gold badge ranged from USD 1200 to USD 2000.
3. All purchases are conducted through a middleman, who ensures the genuineness of the accounts from sellers and funds from the purchaser.
4. The sellers can also boost the followers of the purchased accounts. The boost ranges from 30000-50000 followers for as low as USD 135.
5. The buyer can add multiple affiliates for free. However, after adding a certain number of affiliates to an existing gold account for X, the purchaser must pay USD 50 per affiliate. (that indicates the sub-account is a part or affiliated with the prime Gold account of X)

Information from Cyber Threat Intelligence

Based on our sources, who were engaged with several threat actors while investigating the surge of Twitter Gold advertisements, it was understood that such accounts are mostly dormant. When an unused and inactive account is replaced with threat actors' data, the primary user is locked out from recovering the account. Once a complete account takeover occurs, the threat actor subscribes to the Twitter gold package for 30 days.

The service package offered by the threat actors ensures that the buyer has no hassles with the account for 30 days (which is also the standard duration of Twitter gold subscriptions). And in the meantime, the scam campaign has achieved its goal through that account.

Mass analysis is complex for such campaigns until a researcher visits a Twitter Gold-enabled profile and observes anomalies in the series of posts. However, over one month, the researchers at CloudSEK collected ***six such accounts*** that were announced to be on sale by the cybercriminals. These accounts had followers ranging from 2000 to over 72,000. One such account that has been dormant since 2016 had 28,000 followers and was advertised for $2000-$2500 on the cybercriminal Telegram channel.



GOLD RUSH ON THE DARK WEB: THREAT ACTORS TARGET TWITTER GOLD ACCOUNTS

Threat actors target Twitter Gold accounts for large-scale attacks.

1

Gather Twitter Accounts

Verified Account Hijacking

Criminals are hijacking verified accounts of X (Twitter) and using them for malicious activities. These accounts are made, stolden, hijacked.

2

Check Activity

Cybercriminals target dormant, high-profile accounts for impact.

Cybercriminals favor dormant accounts while prioritizing corporate profiles and influencer accounts with high followings for stealthier operations.

3

Convert Twitter Gold

Threat actors upgrade hijacked accounts to Gold.

Upon gaining complete control of an account, the threat actor upgrades it to Twitter Gold for a 30-day period.

4

Advertise on Forum

Leveraging the accounts for phishing and brand harming.

Threat actors utilize 30-day Twitter Gold subscriptions to execute scams, impacting the followers before it is detected..

5

Post Purchase Services

Phishing Post Redirects Users to Domain with Malicious IPs

The purchase ensures that the buyer has no hassles with the account for 30 days. Meanwhile, post redirects users to a domain having malicious IPs.

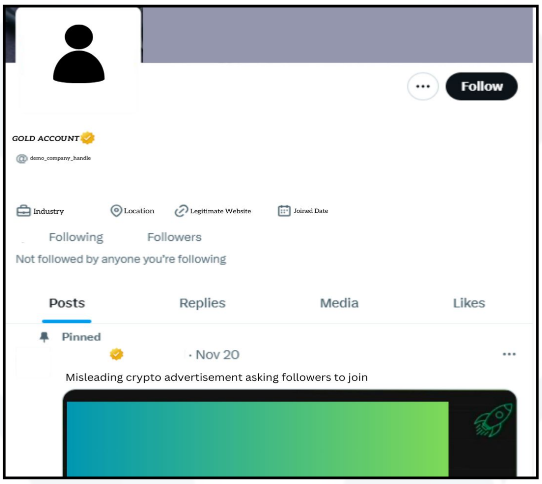
Step by step operations to execute a scam/phishing campaign through Twitter Gold

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

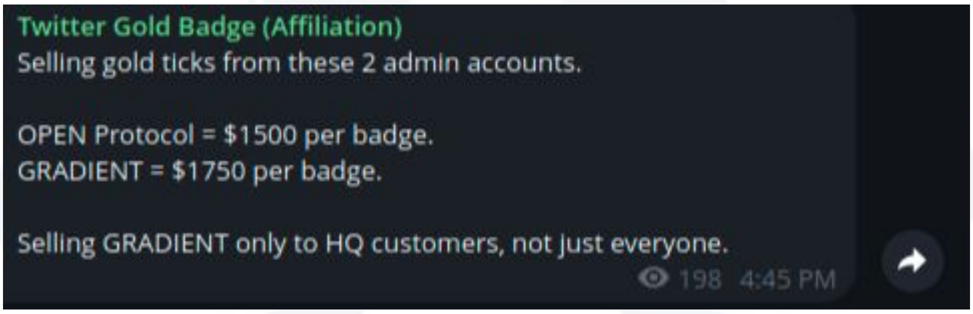
In one such instance, a Twitter Gold account had its main domain as abc.com. The last post was made in 2019. After 2019, another post was created in 2022, conveniently chaining us to the fact that the post made in 2022 was made after purchasing gold from cyber criminals.

Following this thread, the post was redirecting its readers to another domain, 'ABC.XYZ, ' which was created two months ago. Upon checking the passive DNS resolution, the IPs interacting with this redirecting domain had malicious detections.

Below is the accurate representation of a compromised X account, inspired mainly by identifying one in the wild.



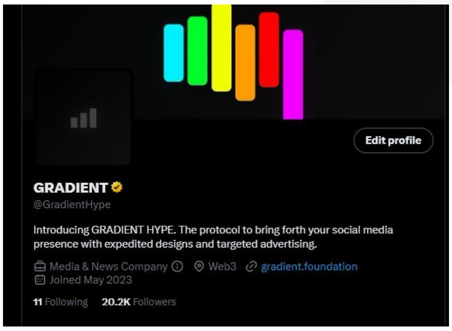
GOLD ACCOUNT
@ demo_company_handle
Industry Location Legitimate Website Joined Date
Following Followers
Not followed by anyone you're following
Posts Replies Media Likes
Pinned
· Nov 20
Misleading crypto advertisement asking followers to join



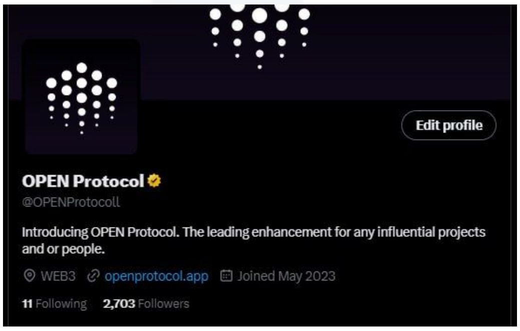
Twitter Gold Badge (Affiliation)
Selling gold ticks from these 2 admin accounts.

OPEN Protocol = $1500 per badge.
GRADIENT = $1750 per badge.

Selling GRADIENT only to HQ customers, not just everyone.
198 4:45 PM



GRADIENT
@GradientHype
Introducing GRADIENT HYPE. The protocol to bring forth your social media presence with expedited designs and targeted advertising.
Media & News Company Web3 gradient.foundation
Joined May 2023
11 Following 20.2K Followers



OPEN Protocol
@OPENProtocoll
Introducing OPEN Protocol. The leading enhancement for any influential projects and or people.
WEB3 openprotocol.app Joined May 2023
11 Following 2,703 Followers

Considering this trend, such Twitter Gold campaigns can be used to spread disinformation, phishing websites to harvest credentials and PII (personally identifiable information), job scams, and crypto scams.

Additionally, such accounts can redirect to websites containing malware or embedded trojans, accidentally downloaded by the masses who trust the X profile spreading such links.

Identifying the TTP

The most common targets are organization's accounts before 2022 that have not been used/ abandoned. The criminals will try to brute force the account. Once it is established that the account belongs to an organization and has dropped (for whatever reason), the criminals will implement a complete account takeover. This is done by changing the recovery email and contact details and replacing them with anonymous or fake logins. Then, this account is converted to gold depending on the ask by buyers.

Secondly, threat actors will gather Twitter-based logins from information stealer malware. These are then validated using configs and brute force methods that will provide a positive response for working accounts. Then, on the advertisement forums and websites, threat actors announce the account for sale, convert it into Twitter gold, and sell it for as low as $800.

Given the above two approaches, the latter is more accessible to implement due to the abundance of logs. For the first method, the threat actors require some technical sophistication.

However, from a buyer's perspective, brute-forced accounts are preferred since malware-infected accounts can be publicly present on cloud shops and don't promise a good service.

Recommendations / Mitigations

How can an organization validate if they are not affected with this?

There are two ways in which organizations can ensure that the Twitter Gold account campaign does not impact them. One is by providing that the dormant accounts are closed if they have been inactive for an extended time period. Secondly, suppose the credentials are stolen from information stealer malware for Twitter corporate accounts. In that case, they need to be alerted and mitigate the compromise with the best password protection practices. Typically, credentials are stolen by malware due to the employees' lack of best security practices. To minimize the risk of being victim to such campaigns, organizations should:

The wide-scale infection of multiple employees by stealer malware also suggests a failure to follow security practices due to the prevalent use of cracked software from malicious websites.

Employees should be trained and educated on workplace cybersecurity practices.
Password policies should be updated, such as replenishing the account passwords regularly.
Employees should be educated against the use of cracked software and its dangers.

Using native password managers should be encouraged instead of saving passwords in web browsers since malware is programmed to steal passwords. Additionally, endpoint security software should be installed on employee devices to detect the presence of malicious software.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

BUSINESS PROPOSITION

With the steep rise in accounts being compromised and advertised daily on the dark web using different methodologies, it is evident that threat actors would not budge from such profit-making businesses anytime soon. Organizations must emphasize the importance of Brand monitoring in cybersecurity strategies to withstand the massive campaigns.

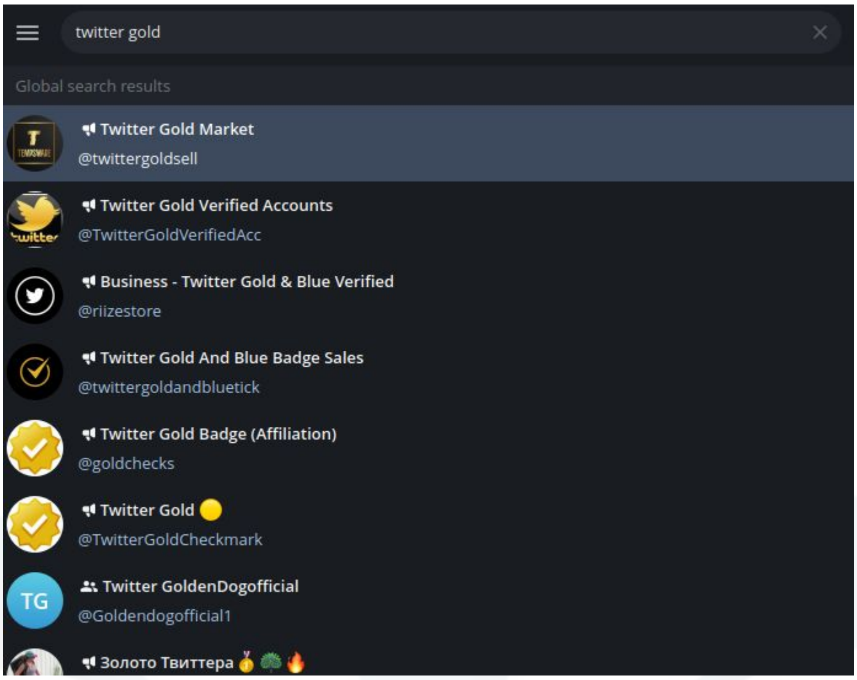
Effective brand monitoring enables businesses to swiftly detect and respond to incidents such as fake profiles, unauthorized product listings, misleading advertisements, and malicious content tarnishing their brand image. These incidents, if left unchecked, can lead to irreparable damage to a company's reputation, financial losses, and erosion of customer loyalty.

To add to the above, the deep and dark web are breeding grounds for cybercrime. Thus, by continuously monitoring these clandestine networks, organizations can gain visibility into these hidden corners of the internet and avert potential risks before they materialize into costly incidents.

CloudSEK's Contextual AI engine leverages Cyber Threat Intelligence and Attack Surface Monitoring to proactively shield an organization's employees and customers from a comprehensive spectrum of cyber threats, including phishing attacks, data leaks, dark web exploits, brand impersonation attempts, and infrastructure weaknesses.

Additionally, CloudSEK XVigil continuously scans thousands of deep and dark web sources to identify fraud, targeted threats, and emerging risks.

1] Searching for Twitter Gold brokers on Telegram via OSINT



twitter gold

Global search results

Twitter Gold Market
@twittergoldsell

Twitter Gold Verified Accounts
@TwitterGoldVerifiedAcc

Business - Twitter Gold & Blue Verified
@riizestore

Twitter Gold And Blue Badge Sales
@twittergoldandbluetick

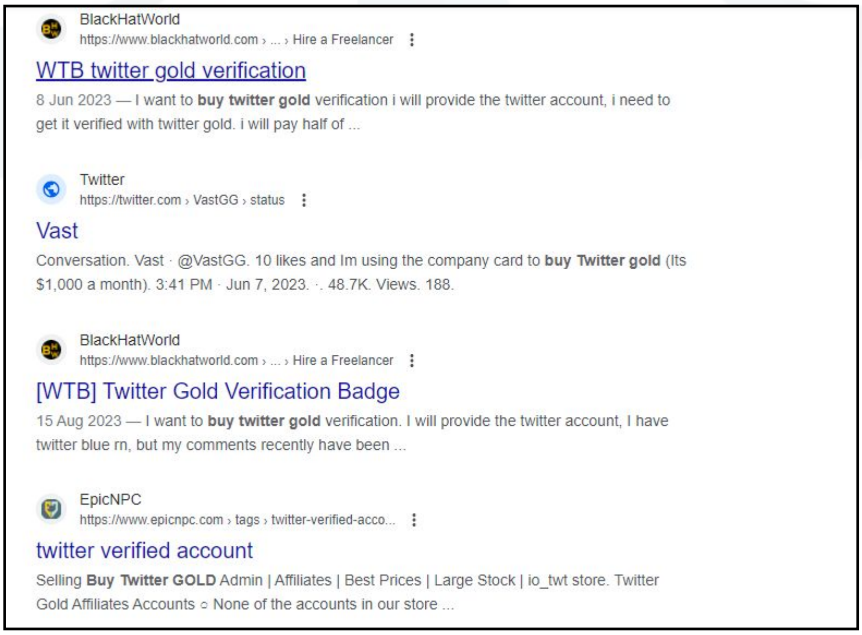
Twitter Gold Badge (Affiliation)
@goldchecks

Twitter Gold 🟡
@TwitterGoldCheckmark

Twitter GoldenDogofficial
@Goldendogofficial1

Золото Твиттера 🥇🦚🔥

[2] Searching for Twitter Gold Brokers via Google Dorking (The indexed pages will be highlighted)



BlackHatWorld
https://www.blackhatworld.com › ... › Hire a Freelancer
WTB twitter gold verification
8 Jun 2023 — I want to **buy twitter gold** verification i will provide the twitter account, i need to get it verified with twitter gold. i will pay half of ...

Twitter
https://twitter.com › VastGG › status
Vast
Conversation. Vast · @VastGG. 10 likes and Im using the company card to **buy Twitter gold** (Its $1,000 a month). 3:41 PM · Jun 7, 2023. ·. 48.7K. Views. 188.

BlackHatWorld
https://www.blackhatworld.com › ... › Hire a Freelancer
[WTB] Twitter Gold Verification Badge
15 Aug 2023 — I want to **buy twitter gold** verification. I will provide the twitter account, I have twitter blue rn, but my comments recently have been ...

EpicNPC
https://www.epicnpc.com › tags › twitter-verified-acco...
twitter verified account
Selling **Buy Twitter GOLD** Admin | Affiliates | Best Prices | Large Stock | io_twt store. Twitter Gold Affiliates Accounts ○ None of the accounts in our store ...

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

CloudSEK

We Predict Cyber Threats

Initial Attack Vector Protection Platform

Founded in **2015**

200+ *CloudSters*

3 Offices
HQ; *Singapore*
R&D: *London, UK*
Bengaluru, India

180+ *Clients Globally*

3 *Products*

We secure some of the Fortune 500 and Unicorns

... And we are backed by eminent investors

Accelerated by

NVIDIA INCEPTION PROGRAM

NETAPP EXCELLERATOR

CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services. We have been featured in several Gartner market guides and are a **qualified AWS partner**. We are the **Highest Rated Security Threat Intelligence company** on Gartner Peer Insights from the Asia Pacific region.

NETAPP EXCELLERATOR BEST GROWTH STRATEGY 2019

ISO 27001

ISO 22301

Gartner Peer Insights. Customer First

DSCI Excellence Awards Security Product Company of the Year 2020

aws PARTNER

NASSCOM Emerge 50 Awards 2020

Highest Rated Security Threat Intelligence Vendor **in Asia Pacific**

Gartner Rated **4.6+** peerinsights

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give context to our customers' digital risks.

CloudSEK

www.cloudsek.com
info@cloudsek.com