KEYS TO THE KINGDOM

How Compromised Corporate Emails Have Become the Most Attractive Attack Vector for Cybercriminals

KELA

Keys to the Kingdom: How Compromised Corporate Emails Have Become the Most Attractive Attack Vector for Cybercriminals

KELA Cybercrime Intelligence Center

Contents

Key findings 2
Introduction 3
The goal: Email account takeover 3
Cracking 4
Stealing 4
Stuffing 4
Buying 5
Threat actors selling email access to corporations 5
Automated shops offering corporate credentials 10
Alternative shops and Telegram channels 20
From corporate email to cyberattacks 22
Monetizing email access through phishing 23
Monetizing email access through BEC 25
Monetizing email access through malware 28
Awareness is key 29

Key findings

- The evolution and servitization (paying for a service instead of buying the equipment) of the cybercrime ecosystem enable threat actors to easily acquire corporate webmail. Popular dedicated webmail sale shops include xLeet, Odin, Lufix, and Xmina.
- KELA's analysis shows that the largest shop offering webmail access is XLeet, with an average price of USD 25 for a single webmail. Office 365 is the most attractive email hosting provider on these marketplaces.
- Threat actors aim to gain easy profits from compromised emails. The dedicated shops allow cybercriminals to sell hundreds of compromised corporate emails. That eases the process for threat actors that look for the ideal victim based on different categories such as sectors and countries.
- Once the webmails are purchased, actors can monetize them to steal money and increase their profit in phishing, business email compromise (BEC), and malware attacks.
- Phishing is a common attack vector for threat actors and state-sponsored espionage actors like advanced persistent threats (APTs) that may use automated webmail shops for purchasing corporate credentials.
- Malware is also commonly used by actors that aim to gain high profits from compromised email accounts. Used for social engineering as an initial step in information stealing trojans and ransomware infections, those attacks help attackers steal money and receive high ransom payments from the victims.

Introduction

Threat actors are constantly looking for new monetization opportunities in the cybercrime ecosystem, trying to put their hands on sensitive corporate data and leverage that for their profit. Such compromised data on cybercrime forums can include databases, source code, internal documents, as well access to services such as corporate email credentials. Once credentials are obtained, unauthorized actors can view the content of organizational accounts, as well as send emails from the compromised accounts, which appear legitimate but contain phishing campaigns.

Threat actors now have new marketplaces and shops, which enable them to easily buy corporate email accounts for their attacks. Webmail refers to an email that is sent via a web browser and web-based interface of different business email providers; a user can access a corporate email as long as he is connected to the internet. Regular email clients can be accessed through desktop programs. KELA noticed that actors selling email access via these dedicated, automated shops offer hundreds of thousands of corporate email credentials for sale. In this analysis, KELA takes a closer look at the scope of shops such as XLeet, Odin, Xmina, and Lufix that are easing processes for cybercriminals. This report shows how actors could obtain access and monetize it through several attack vectors, which include phishing, BEC, and malware attacks.

The goal: Email account takeover

People rely on email for almost every single daily activity, both personal and professional. As a result, corporate email accounts have become a valuable target for cybercriminals who aim to gain access to corporate emails and steal sensitive corporate information.

Cybercriminals use a variety of methods to hack into corporate email accounts. The following are among the most common:

Cracking

This method uses brute force or dictionary attacks that aim to reveal users' passwords. A brute -force attack uses trial and error to guess user login, while a dictionary attack uses a wordlist to crack a password-protected security system.

Stealing

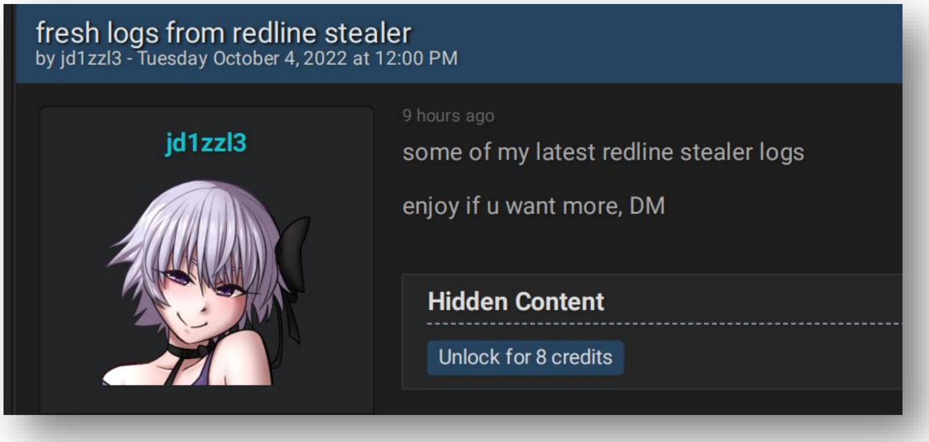
This method gains credentials directly from the user through malware or phishing campaigns. One common type of malware is info-stealing trojans that infect machines to harvest credentials including usernames and passwords. The stolen data and browser-saved information (known as "logs") originate from devices infected by information-stealing malware (referred to as "bots"). Commodity information stealers such as Redline, Raccoon, Mars, and Vidar are widely available for purchase on cybercrime forums. Cybercriminals can also use social-engineering tactics to steal credentials directly from the user.

Stuffing

Threat actors use data leaked from other data breaches to reuse credentials that enable them to log in to other, unrelated corporate services. Many different databases are published in the cybercrime ecosystem, from data leaked on ransomware & data leak sites, to dumps aggregated from multiple data breaches. Leaked data can include employees' and clients' emails and passwords and other person ally identifiable information. Threat actors use this valuable information to conduct other malicious activities. There are different forums that offer stolen database exchanges, like BreachForums, where cybercriminals can sell, trade, or share corporate databases.

Buying

Criminals can also simply buy corporate email credentials or logs that were compromised by other cybercriminals. Automated botnet marketplaces such as RussianMarket, TwoEasy, and Genesis allow actors to access various resources using the stolen credentials. Emails can also be offered directly on the forums, giving actors options for accessing sensitive corporate data — without having to have technical knowledge and skills.



fresh logs from redline stealer
by jd1zzl3 - Tuesday October 4, 2022 at 12:00 PM

jd1zzl3

9 hours ago

some of my latest redline stealer logs

enjoy if u want more, DM

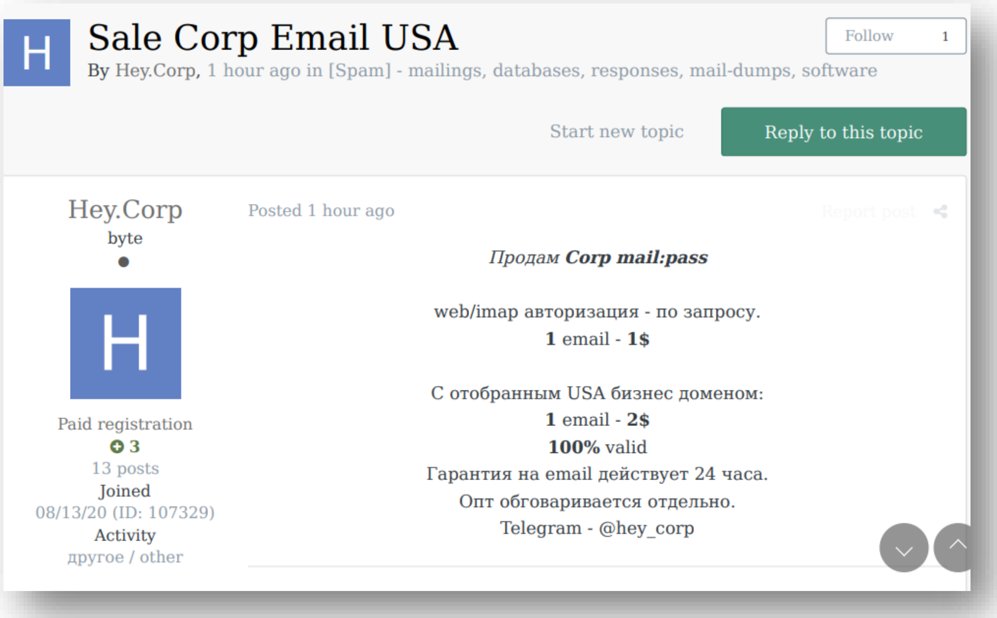
Hidden Content

A threat actor offers logs (web-browser information) harvested from Redline malware.

Threat actors selling email access to corporations

Over the past few years, KELA has been monitoring cybercrime forums that offer different types of access to organizations for sale, including email accounts. Actors describe multiple vectors under the word “access” — from server access to credentials to corporate email and other services and tools such as CMS, CRM, WordPress, and more. The recent rise of shops offering corporate email credentials led KELA to focus on how threat actors can steal or compromise emails.

That corporate email access is in demand among cybercriminals can be illustrated by recent activity on cybercrime forums. On February 22, 2022, a threat actor was selling different corporate emails from US companies. The actor claimed that all of them were valid and that a potential buyer could log in without two-factor authentication. Each individual email was offered for sale for USD 2.



Sale Corp Email USA

By Hey.Corp, 1 hour ago in [Spam] - mailings, databases, responses, mail-dumps, software

Hey.Corp
byte

Paid registration
3
13 posts
Joined
08/13/20 (ID: 107329)
Activity
другое / other

Posted 1 hour ago

*Продам **Corp mail:pass***

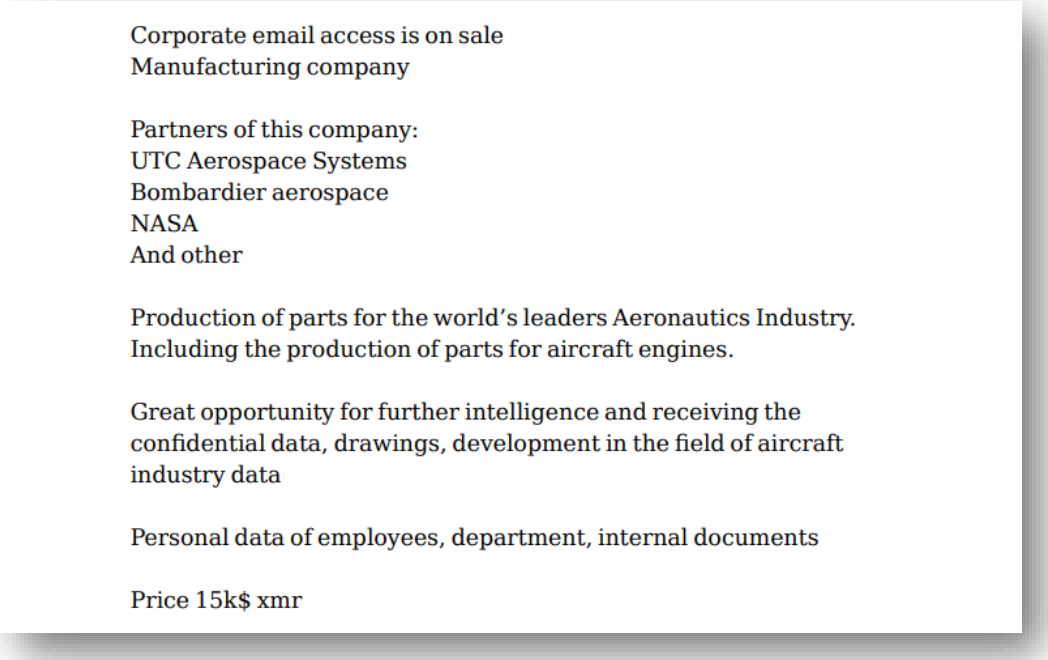
web/imap авторизация - по запросу.
1 email - **1$**

С отобранным USA бизнес доменом:
1 email - **2$**
100% valid
Гарантия на email действует 24 часа.
Опт обговаривается отдельно.
Telegram - @hey_corp

Actor offering email access to US-based companies.

Access to government emails is also regularly sold in underground forums. On July 14, 2022, an actor offered access to a Turkish minister's email and on the same day, he claimed that the access had been sold. On July 31, 2022, KELA observed an actor selling email access to police forces based in South Asia. Each email was offered for sale for USD 80. Recently, the actor leaksmart (also known as Shadowhacker) was selling email access to US governmental entities.

Ransomware representatives are also involved in selling email accesses. On November 22, 2022, the operators of Everest ransomware were selling email access to a Canada-based aerospace manufacturing company. The access was offered for sale for USD 15,000.



Corporate email access is on sale
Manufacturing company

Partners of this company:
UTC Aerospace Systems
Bombardier aerospace
NASA
And other

Production of parts for the world's leaders Aeronautics Industry.
Including the production of parts for aircraft engines.

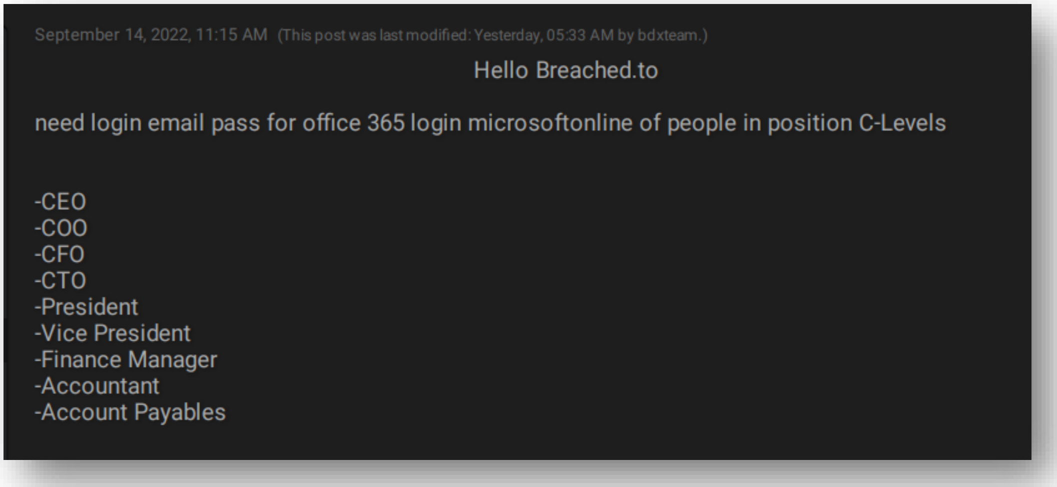
Great opportunity for further intelligence and receiving the confidential data, drawings, development in the field of aircraft industry data

Personal data of employees, department, internal documents

Price 15k$ xmr

Everest is selling email access to a Canada-based aerospace company.

The demand for corporate emails is also high. On September 14, 2022, an actor was looking to buy login details of C-level executives' Microsoft Office emails. The actor detailed the relevant positions that he was interested in, including CEO, COO, CFO, CTO, finance manager, accountant, and more. Based on the essence of these positions, KELA can evaluate that the actor probably aims to carry out BEC attacks by impersonating those people to initiate an urgent wire transfer.



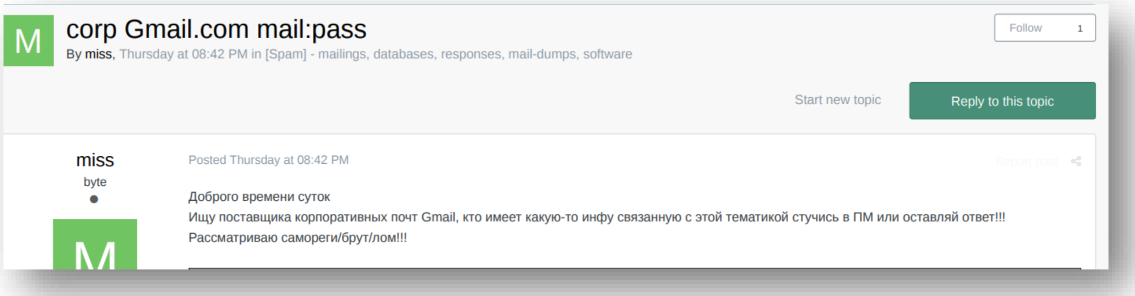
September 14, 2022, 11:15 AM (This post was last modified: Yesterday, 05:33 AM by bdxteam.)

Hello Breached.to

need login email pass for office 365 login microsoftonline of people in position C-Levels

-CEO
-COO
-CFO
-CTO
-President
-Vice President
-Finance Manager
-Accountant
-Account Payables

An actor is willing to buy C-level executives' Microsoft Office email credentials.



corp Gmail.com mail:pass

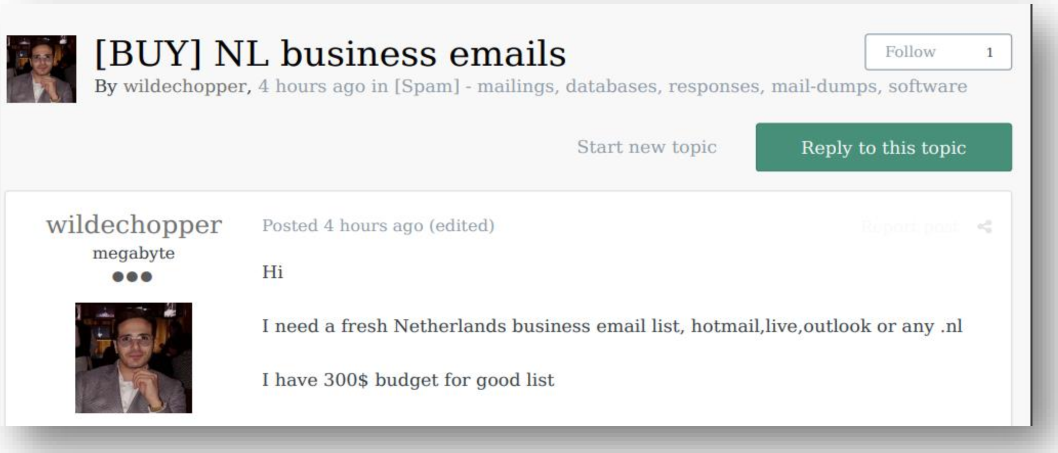
By miss, Thursday at 08:42 PM in [Spam] - mailings, databases, responses, mail-dumps, software

Posted Thursday at 08:42 PM

Доброго времени суток
Ищу поставщика корпоративных почт Gmail, кто имеет какую-то инфу связанную с этой тематикой стучись в ПМ или оставляй ответ!!!
Рассматриваю самореги/брут/лом!!!

An actor is buying Gmail users' business emails.

Threat actors do not only buy corporate email access to a specific company but are also looking for combolists (a text file containing a list of credentials, usually in clear text, aggregated from different data leaks) from specific countries for their attacks. For example, on August 6, 2022, an actor posted that he was interested in combolists of business emails of companies in the Netherlands and that he was willing to pay USD 300; such offers are done on a weekly basis.



[BUY] NL business emails

By wildechopper, 4 hours ago in [Spam] - mailings, databases, responses, mail-dumps, software

wildechopper
megabyte

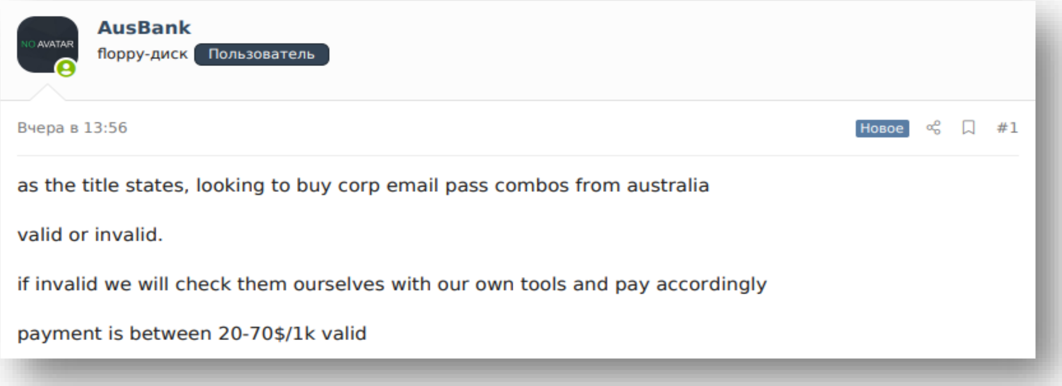
Posted 4 hours ago (edited)

Hi

I need a fresh Netherlands business email list, hotmail,live,outlook or any .nl

I have 300$ budget for good list

A threat actor is interested in Netherlands companies' emails.



AusBank
floppy-диск Пользователь

Вчера в 13:56

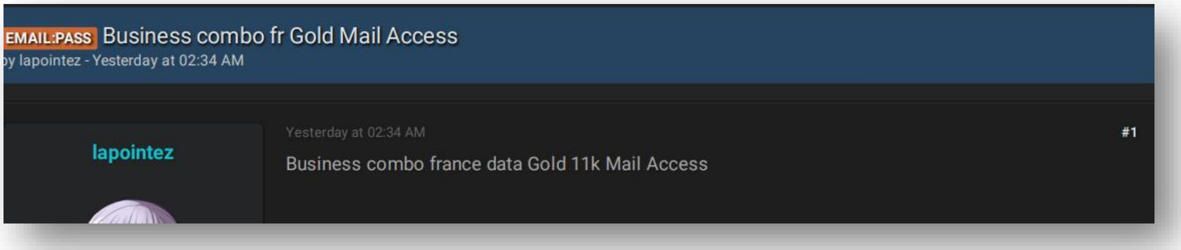
as the title states, looking to buy corp email pass combos from australia

valid or invalid.

if invalid we will check them ourselves with our own tools and pay accordingly

payment is between 20-70$/1k valid

An actor is willing to buy Australian combolists.



EMAIL:PASS Business combo fr Gold Mail Access

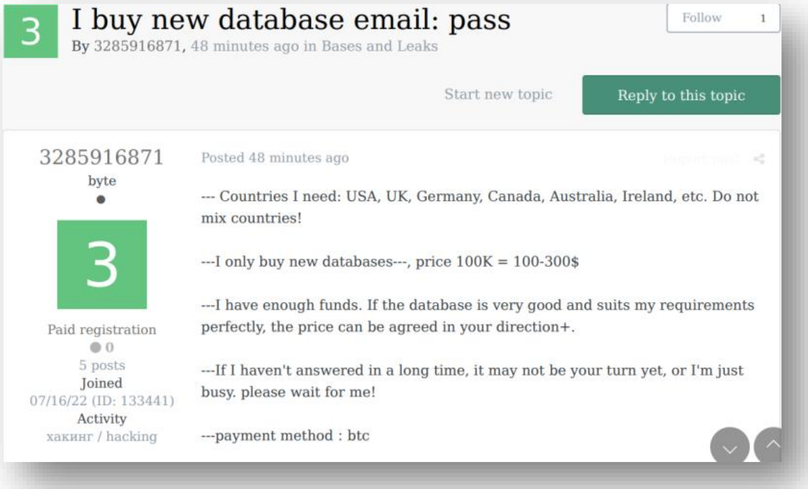
by lapointez - Yesterday at 02:34 AM

lapointez

Yesterday at 02:34 AM

Business combo france data Gold 11k Mail Access

An actor is selling a combolist of French companies.



I buy new database email: pass

By 3285916871, 48 minutes ago in Bases and Leaks

3285916871
byte

Paid registration
● 0
5 posts
Joined
07/16/22 (ID: 133441)
Activity
хакинг / hacking

Posted 48 minutes ago

--- Countries I need: USA, UK, Germany, Canada, Australia, Ireland, etc. Do not mix countries!

---I only buy new databases---, price 100K = 100-300$

---I have enough funds. If the database is very good and suits my requirements perfectly, the price can be agreed in your direction+.

---If I haven't answered in a long time, it may not be your turn yet, or I'm just busy. please wait for me!

---payment method : btc

An actor is seeking combolists from different countries.

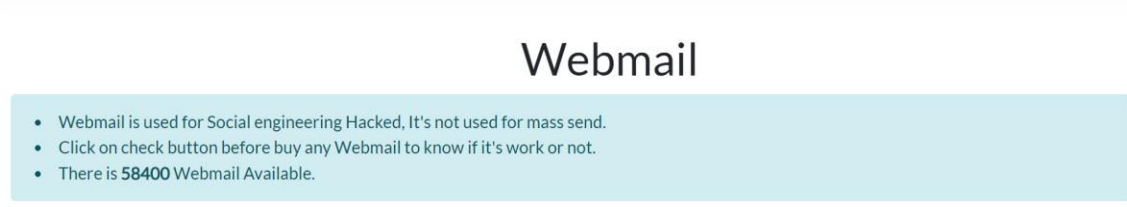
Automated shops offering corporate credentials

For a long time threat actors were forced to look manually for corporate email access on cybercrime forums, finding the relevant sellers and purchasing their relevant goods. Sellers were also required to post their own offers, providing attractive access and combolists for an affordable price.

As KELA has already reported, the cybercrime ecosystem has been evolving quickly, focusing on servitization and sales automation. In the same way that dedicated shops appeared for credit cards and logs, new shops and markets for corporate webmails started to appear in 2019, making the work for cybercriminals easier.

Recently KELA added to its security data lake automated shops offering corporate webmails for sale. The list of shops includes **XLeet, Odin, Xmina,** and **Lufix**. The shops offer a wide range of spamming tools from hosting services (cPanels, RDP, and shells), accounts (streaming, VPN, email marketing) and leads (access to email leads and combolists), and also corporate webmails. Many of these shops provide advanced functions, such as “proofs” that webmail access indeed works. These proofs include performing a live check on the email to verify the access or showing a screenshot of the compromised account inbox. KELA’s cybercrime intelligence platform collects this data and allows easy identification of the infected device and username.

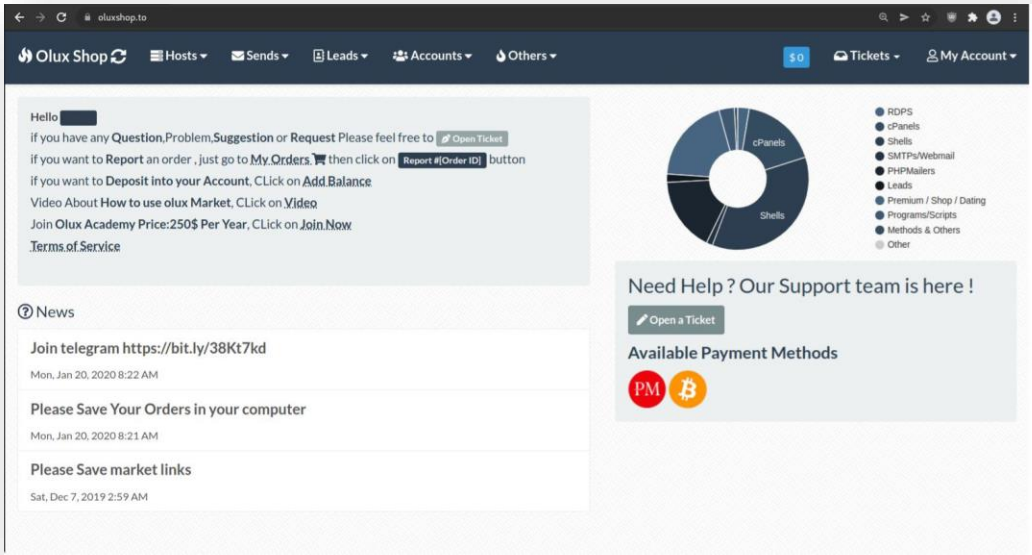
Two markets, XLeet and Odin, explain how webmail is used by cybercriminals, showing the following notice under the webmail section: “Webmail is used for social engineering hacked and not used for mass send.” It likely means that it is a single compromised email account that can be used for social engineering attacks, like BEC, and not like a compromised Simple Mail Transfer Protocol (SMTP) server that is used for sending a large number of messages.



Webmail

- Webmail is used for Social engineering Hacked, It's not used for mass send.
- Click on check button before buy any Webmail to know if it's work or not.
- There is **58400** Webmail Available.

These four shops have similar features and even designs. Some actors claimed that another shop Olux and XLeet use the same source code, while on September 16, 2022, an actor claimed that he was selling Olux/XLeet “script”. On July 13, 2021, an actor was looking for a web developer to create a similar website to XLeet and Olux. XLeet and Odin shops offer the same categories. Therefore, it’s likely that the four shops use similar layout templates and perhaps the same source code.



Hello [redacted]
if you have any **Question**,Problem,**Suggestion** or **Request** Please feel free to Open Ticket
if you want to **Report** an order , just go to My Orders then click on Report #[Order ID] button
if you want to **Deposit into your Account**, CLick on Add Balance
Video About **How to use olux Market**, CLick on Video
Join **Olux Academy Price:250$ Per Year**, CLick on Join Now
Terms of Service

News

Join telegram https://bit.ly/38Kt7kd
Mon, Jan 20, 2020 8:22 AM

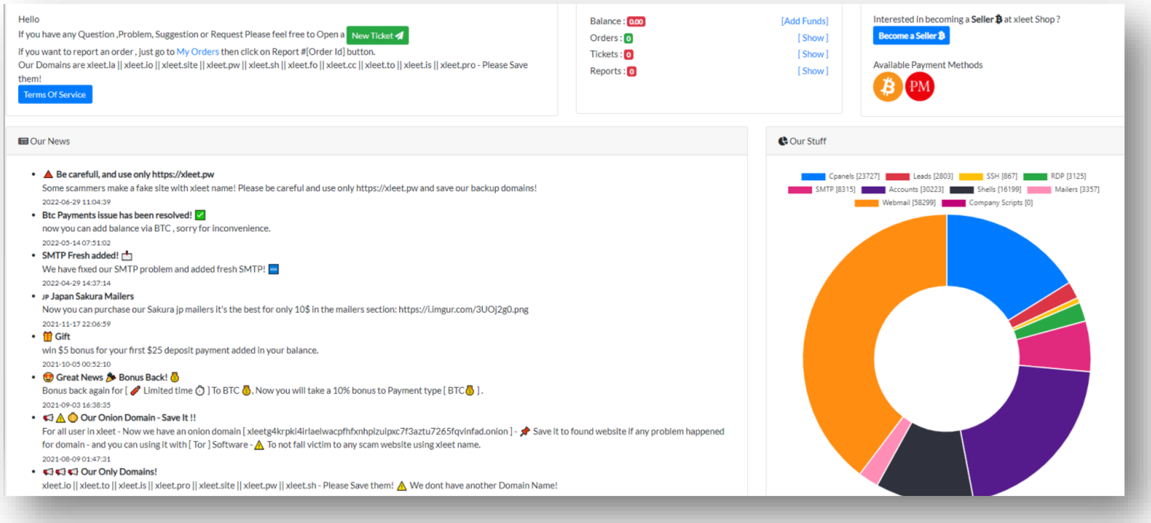
Please Save Your Orders in your computer
Mon, Jan 20, 2020 8:21 AM

Please Save market links
Sat, Dec 7, 2019 2:59 AM

Need Help ? Our Support team is here !

Available Payment Methods

Olux had its source code leaked in 2020.



Hello

If you have any Question ,Problem, Suggestion or Request Please feel free to Open a New Ticket

if you want to report an order , just go to My Orders then click on Report #[Order Id] button.

Our Domains are xleet.la || xleet.io || xleet.site || xleet.pw || xleet.sh || xleet.fo || xleet.cc || xleet.to || xleet.is || xleet.pro - Please Save them!

Terms Of Service

Balance : 0.00 [Add Funds]

Orders : 0 [Show]

Tickets : 0 [Show]

Reports : 0 [Show]

Interested in becoming a **Seller** ₿ at xleet Shop ?

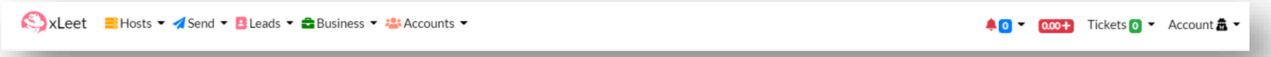
Become a Seller ₿

Available Payment Methods

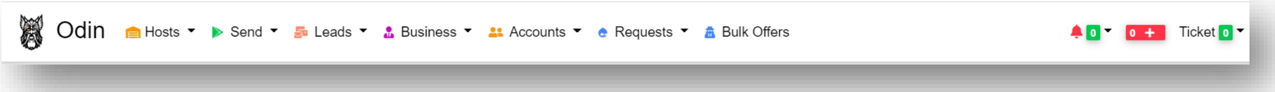
Our News

- ⚠ **Be carefull, and use only https://xleet.pw**
  Some scammers make a fake site with xleet name! Please be careful and use only https://xleet.pw and save our backup domains!
  2022-06-29 11:04:39
- **Btc Payments issue has been resolved!** ✅
  now you can add balance via BTC , sorry for inconvenience.
  2022-05-14 07:51:02
- **SMTP Fresh added!** 📤
  We have fixed our SMTP problem and added fresh SMTP! 🆕
  2022-04-29 14:37:14
- **JP Japan Sakura Mailers**
  Now you can purchase our Sakura jp mailers it's the best for only 10$ in the mailers section: https://i.imgur.com/3UOj2g0.png
  2021-11-17 22:06:59
- 🎁 **Gift**
  win $5 bonus for your first $25 deposit payment added in your balance.
  2021-10-05 00:52:10
- 😍 **Great News** 🎉 **Bonus Back!** 💰
  Bonus back again for [🧨 Limited time ⏱] To BTC 💰, Now you will take a 10% bonus to Payment type [BTC💰].
  2021-09-03 16:38:35
- 📢 ⚠ 🧅 **Our Onion Domain - Save It !!**
  For all user in xleet - Now we have an onion domain [xleetg4krpki4irlaelwacpfhfxnhpizuipxc7f3aztu7265fqvinfad.onion] - 📌 Save it to found website if any problem happened for domain - and you can using it with [Tor] Software - ⚠ To not fall victim to any scam website using xleet name.
  2021-08-09 01:47:31
- 📢 📢 📢 **Our Only Domains!**
  xleet.io || xleet.to || xleet.is || xleet.pro || xleet.site || xleet.pw || xleet.sh - Please Save them! ⚠ We dont have another Domain Name!

XLeet shop has a similar UI to Olux.



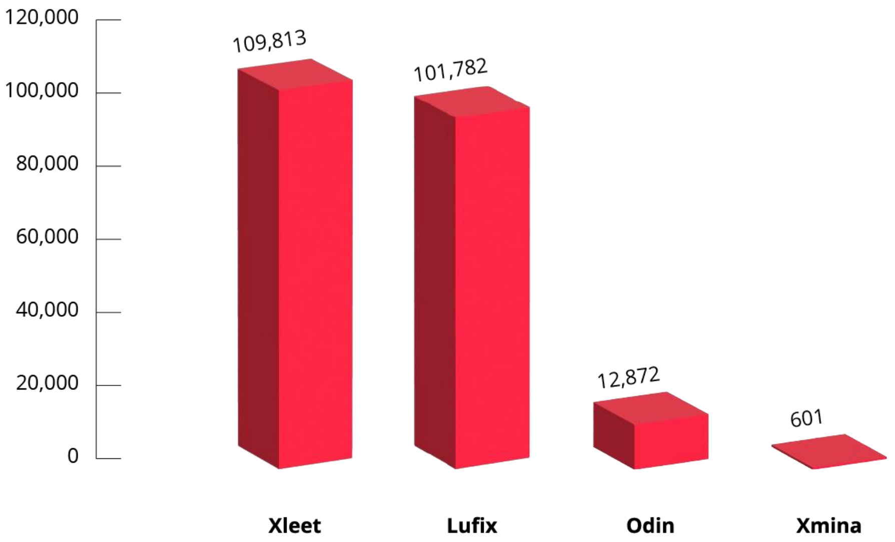
XLeet header.

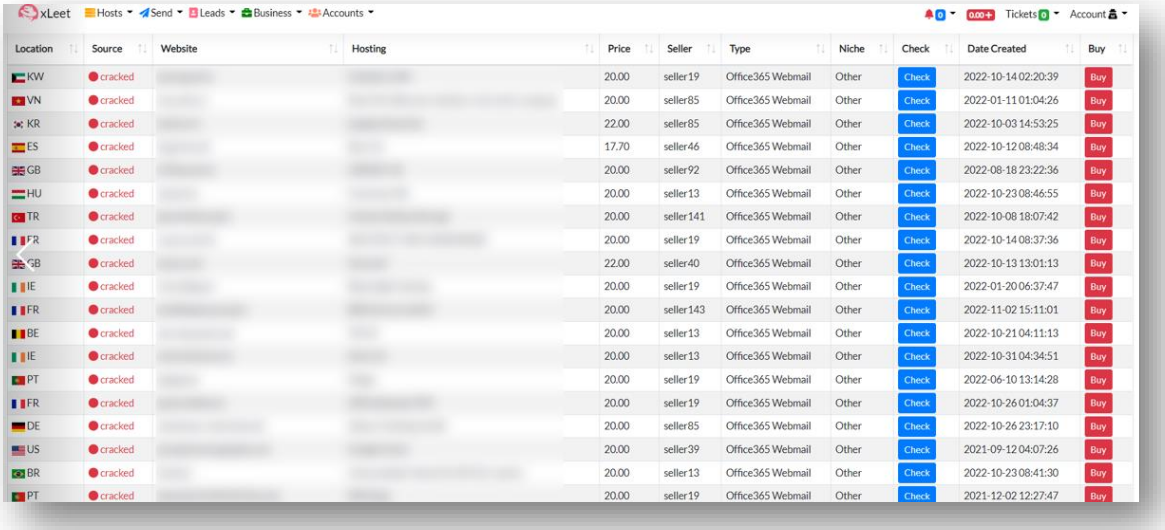


Odin header.

The shops allow potential buyers to sort and find emails based on specific characteristics. XLeet is the most mature forum and has been advertised on cybercrime forums since May 2019. Based on the number of credentials offered for sale, XLeet is also the biggest shop.

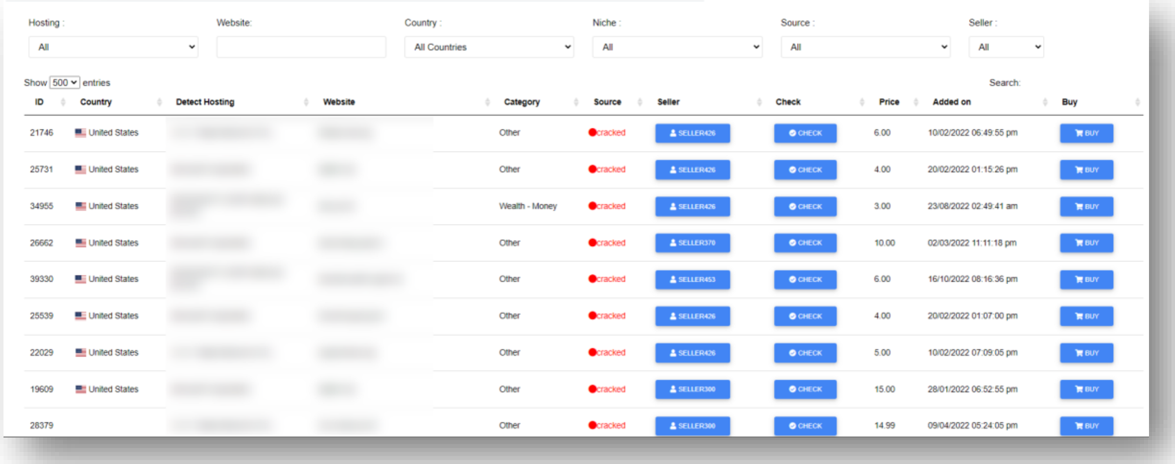
Number of offers per shop





Location	Source	Website	Hosting	Price	Seller	Type	Niche	Check	Date Created	Buy
KW	● cracked	[redacted]	[redacted]	20.00	seller19	Office365 Webmail	Other	Check	2022-10-14 02:20:39	Buy
VN	● cracked	[redacted]	[redacted]	20.00	seller85	Office365 Webmail	Other	Check	2022-01-11 01:04:26	Buy
KR	● cracked	[redacted]	[redacted]	22.00	seller85	Office365 Webmail	Other	Check	2022-10-03 14:53:25	Buy
ES	● cracked	[redacted]	[redacted]	17.70	seller46	Office365 Webmail	Other	Check	2022-10-12 08:48:34	Buy
GB	● cracked	[redacted]	[redacted]	20.00	seller92	Office365 Webmail	Other	Check	2022-08-18 23:22:36	Buy
HU	● cracked	[redacted]	[redacted]	20.00	seller13	Office365 Webmail	Other	Check	2022-10-23 08:46:55	Buy
TR	● cracked	[redacted]	[redacted]	20.00	seller141	Office365 Webmail	Other	Check	2022-10-08 18:07:42	Buy
FR	● cracked	[redacted]	[redacted]	20.00	seller19	Office365 Webmail	Other	Check	2022-10-14 08:37:36	Buy
GB	● cracked	[redacted]	[redacted]	22.00	seller40	Office365 Webmail	Other	Check	2022-10-13 13:01:13	Buy
IE	● cracked	[redacted]	[redacted]	20.00	seller19	Office365 Webmail	Other	Check	2022-01-20 06:37:47	Buy
FR	● cracked	[redacted]	[redacted]	20.00	seller143	Office365 Webmail	Other	Check	2022-11-02 15:11:01	Buy
BE	● cracked	[redacted]	[redacted]	20.00	seller13	Office365 Webmail	Other	Check	2022-10-21 04:11:13	Buy
IE	● cracked	[redacted]	[redacted]	20.00	seller13	Office365 Webmail	Other	Check	2022-10-31 04:34:51	Buy
PT	● cracked	[redacted]	[redacted]	20.00	seller19	Office365 Webmail	Other	Check	2022-06-10 13:14:28	Buy
FR	● cracked	[redacted]	[redacted]	20.00	seller19	Office365 Webmail	Other	Check	2022-10-26 01:04:37	Buy
DE	● cracked	[redacted]	[redacted]	20.00	seller85	Office365 Webmail	Other	Check	2022-10-26 23:17:10	Buy
US	● cracked	[redacted]	[redacted]	20.00	seller39	Office365 Webmail	Other	Check	2021-09-12 04:07:26	Buy
BR	● cracked	[redacted]	[redacted]	20.00	seller13	Office365 Webmail	Other	Check	2022-10-23 08:41:30	Buy
PT	● cracked	[redacted]	[redacted]	20.00	seller19	Office365 Webmail	Other	Check	2021-12-02 12:27:47	Buy

XLeet shop - webmail section



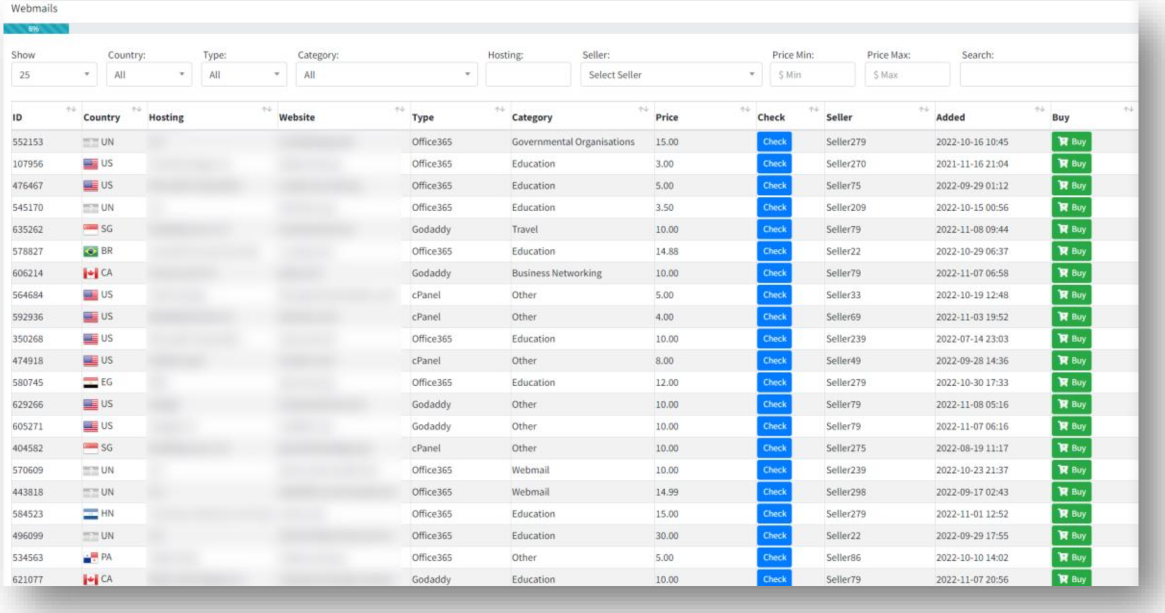
Hosting : All
Website:
Country : All Countries
Niche : All
Source : All
Seller : All

Show 500 entries

Search:

ID	Country	Detect Hosting	Website	Category	Source	Seller	Check	Price	Added on	Buy
21746	United States	[redacted]	[redacted]	Other	●cracked	SELLER426	CHECK	6.00	10/02/2022 06:49:55 pm	BUY
25731	United States	[redacted]	[redacted]	Other	●cracked	SELLER426	CHECK	4.00	20/02/2022 01:15:26 pm	BUY
34955	United States	[redacted]	[redacted]	Wealth - Money	●cracked	SELLER426	CHECK	3.00	23/08/2022 02:49:41 am	BUY
26662	United States	[redacted]	[redacted]	Other	●cracked	SELLER370	CHECK	10.00	02/03/2022 11:11:18 pm	BUY
39330	United States	[redacted]	[redacted]	Other	●cracked	SELLER453	CHECK	6.00	16/10/2022 08:16:36 pm	BUY
25539	United States	[redacted]	[redacted]	Other	●cracked	SELLER426	CHECK	4.00	20/02/2022 01:07:00 pm	BUY
22029	United States	[redacted]	[redacted]	Other	●cracked	SELLER426	CHECK	5.00	10/02/2022 07:09:05 pm	BUY
19609	United States	[redacted]	[redacted]	Other	●cracked	SELLER300	CHECK	15.00	28/01/2022 06:52:55 pm	BUY
28379		[redacted]	[redacted]	Other	●cracked	SELLER300	CHECK	14.99	09/04/2022 05:24:05 pm	BUY

Odin shop webmail section.



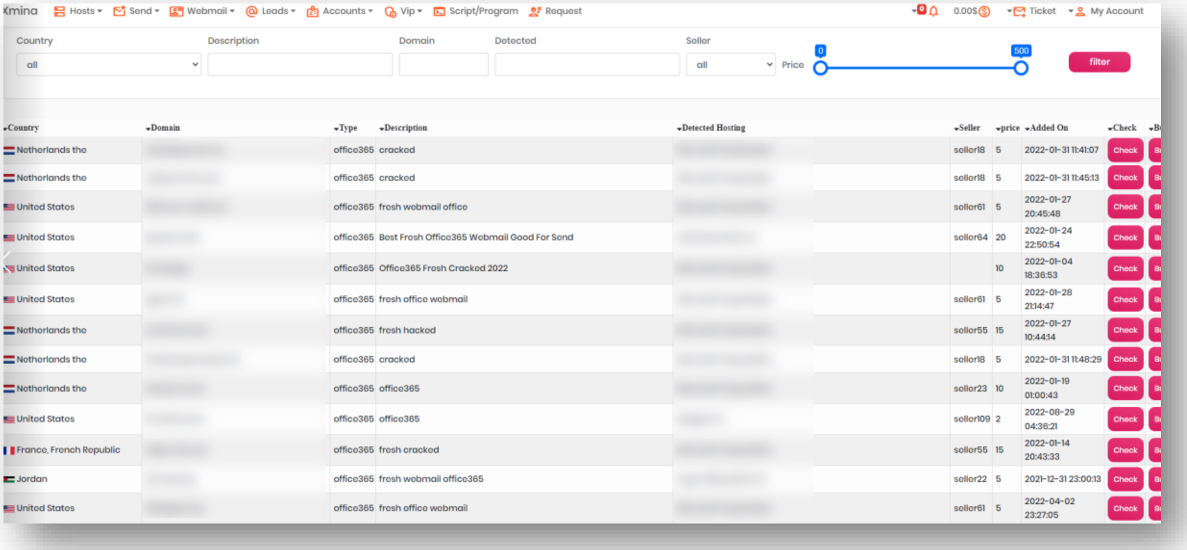
Webmails

6%

Show 25
Country: All
Type: All
Category: All
Hosting:
Seller: Select Seller
Price Min: $ Min
Price Max: $ Max
Search:

ID	Country	Hosting	Website	Type	Category	Price	Check	Seller	Added	Buy
552153	UN	[redacted]	[redacted]	Office365	Governmental Organisations	15.00	Check	Seller279	2022-10-16 10:45	Buy
107956	US	[redacted]	[redacted]	Office365	Education	3.00	Check	Seller270	2021-11-16 21:04	Buy
476467	US	[redacted]	[redacted]	Office365	Education	5.00	Check	Seller75	2022-09-29 01:12	Buy
545170	UN	[redacted]	[redacted]	Office365	Education	3.50	Check	Seller209	2022-10-15 00:56	Buy
635262	SG	[redacted]	[redacted]	Godaddy	Travel	10.00	Check	Seller79	2022-11-08 09:44	Buy
578827	BR	[redacted]	[redacted]	Office365	Education	14.88	Check	Seller22	2022-10-29 06:37	Buy
606214	CA	[redacted]	[redacted]	Godaddy	Business Networking	10.00	Check	Seller79	2022-11-07 06:58	Buy
564684	US	[redacted]	[redacted]	cPanel	Other	5.00	Check	Seller33	2022-10-19 12:48	Buy
592936	US	[redacted]	[redacted]	cPanel	Other	4.00	Check	Seller69	2022-11-03 19:52	Buy
350268	US	[redacted]	[redacted]	Office365	Education	10.00	Check	Seller239	2022-07-14 23:03	Buy
474918	US	[redacted]	[redacted]	cPanel	Other	8.00	Check	Seller49	2022-09-28 14:36	Buy
580745	EG	[redacted]	[redacted]	Office365	Education	12.00	Check	Seller279	2022-10-30 17:33	Buy
629266	US	[redacted]	[redacted]	Godaddy	Other	10.00	Check	Seller79	2022-11-08 05:16	Buy
605271	US	[redacted]	[redacted]	Godaddy	Other	10.00	Check	Seller79	2022-11-07 06:16	Buy
404582	SG	[redacted]	[redacted]	cPanel	Other	10.00	Check	Seller275	2022-08-19 11:17	Buy
570609	UN	[redacted]	[redacted]	Office365	Webmail	10.00	Check	Seller239	2022-10-23 21:37	Buy
443818	UN	[redacted]	[redacted]	Office365	Webmail	14.99	Check	Seller298	2022-09-17 02:43	Buy
584523	HN	[redacted]	[redacted]	Office365	Education	15.00	Check	Seller279	2022-11-01 12:52	Buy
496099	UN	[redacted]	[redacted]	Office365	Education	30.00	Check	Seller22	2022-09-29 17:55	Buy
534563	PA	[redacted]	[redacted]	Office365	Other	5.00	Check	Seller86	2022-10-10 14:02	Buy
621077	CA	[redacted]	[redacted]	Godaddy	Education	10.00	Check	Seller79	2022-11-07 20:56	Buy

Lufix shop webmail section.



Country
all

Description

Domain

Detected

Seller
all

Price 0 500

Country	Domain	Type	Description	Detected Hosting	Seller	price	Added On	Check	B
Netherlands the	[redacted]	office365	cracked	[redacted]	seller18	5	2022-01-31 11:41:07	Check	B
Netherlands the	[redacted]	office365	cracked	[redacted]	seller18	5	2022-01-31 11:45:13	Check	B
United States	[redacted]	office365	fresh webmail office	[redacted]	seller61	5	2022-01-27 20:45:48	Check	B
United States	[redacted]	office365	Best Fresh Office365 Webmail Good For Send	[redacted]	seller64	20	2022-01-24 22:50:54	Check	B
United States	[redacted]	office365	Office365 Fresh Cracked 2022	[redacted]		10	2022-01-04 18:36:53	Check	B
United States	[redacted]	office365	fresh office webmail	[redacted]	seller61	5	2022-01-28 21:14:47	Check	B
Netherlands the	[redacted]	office365	fresh hacked	[redacted]	seller55	15	2022-01-27 10:44:14	Check	B
Netherlands the	[redacted]	office365	cracked	[redacted]	seller18	5	2022-01-31 11:48:29	Check	B
Netherlands the	[redacted]	office365	office365	[redacted]	seller23	10	2022-01-19 01:00:43	Check	B
United States	[redacted]	office365	office365	[redacted]	seller109	2	2022-08-29 04:36:21	Check	B
France, French Republic	[redacted]	office365	fresh cracked	[redacted]	seller55	15	2022-01-14 20:43:33	Check	B
Jordan	[redacted]	office365	fresh webmail office365	[redacted]	seller22	5	2021-12-31 23:00:13	Check	B
United States	[redacted]	office365	fresh office webmail	[redacted]	seller61	5	2022-04-02 23:27:05	Check	B

Xmina shop webmail section.

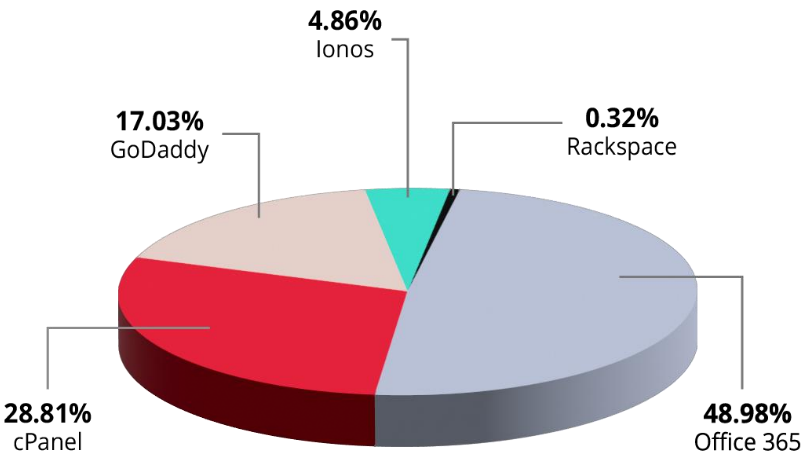
Odin and Lufix have been active since 2020 while Xmina appeared in early 2022. KELA monitored more than **225,000 webmails** listed for sale on the above shops and used this data to define the largest player and find out what metrics of compromised emails are the most important for cybercriminals.

In the researched four markets, the most targeted business email providers were Microsoft 365, GoDaddy, Rackspace, and Ionos. Some of the shops are also listed as a type of access cPanel, which allows accessing webmail using a cPanel interface.

Under the webmail section of all four markets, actors can filter their results by category:

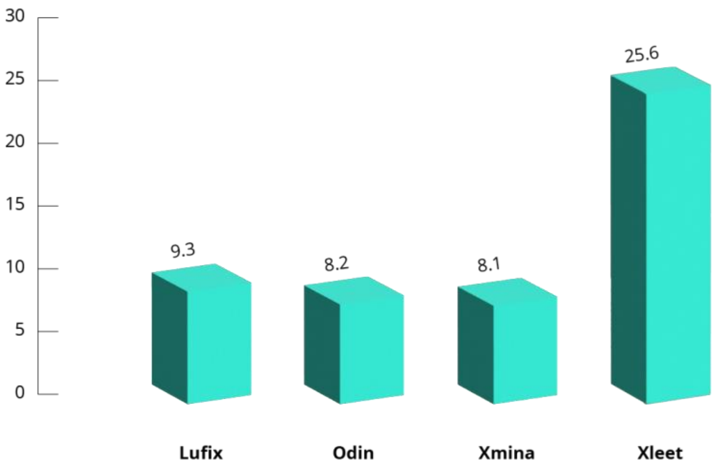
- **Website of the company.**
- **Country.** The US is the most popular location based on the emails advertised on the shops. That's because cybercriminals aim to increase their profit and therefore focus on profitable companies that will be able to pay.
- **Type of business email providers.** The most popular type is Microsoft Office 365, followed by cPanel, Godaddy, Ionos, and Rackspace. Users can access webmail through cPanel's interface via the email accounts category.

Email host providers



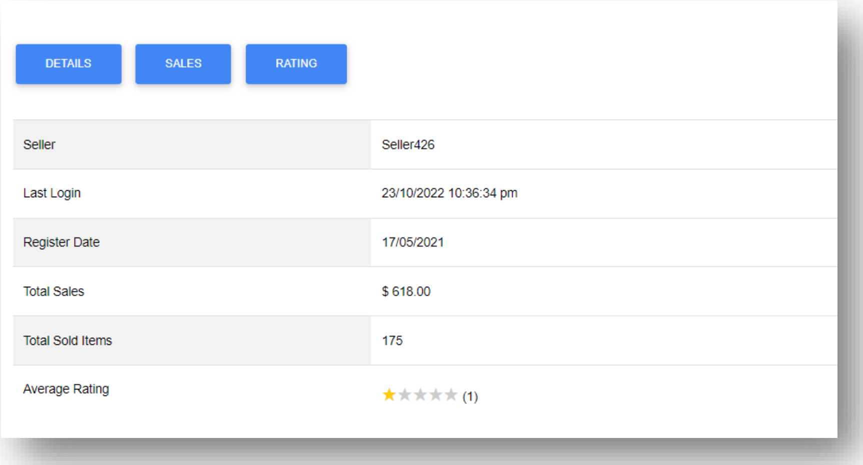
- **Price.** The average price for corporate webmail on Lufix, Odina, and Xmina is USD 8.5. However, the average price on XLeet is more than triple, at USD 25.6.

Average price per market (in USD)



- **Niche.** This is the business sector of the company, also called "Category" on Lufix.

- **Seller.** Sellers are not registered by names but by numbers: seller1, seller2, etc. Odin market provides additional information regarding the sellers. When users click on the "seller" button, they can see the total items sold, total sales, and rating of each seller. It is also possible to see the feedback that users gave to a specific seller.



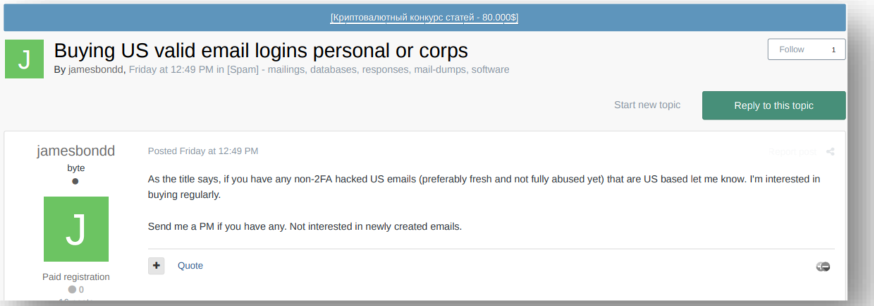
Seller	Seller426
Last Login	23/10/2022 10:36:34 pm
Register Date	17/05/2021
Total Sales	$ 618.00
Total Sold Items	175
Average Rating	★☆☆☆☆ (1)

Odin shop shows the ranking of the sellers.

- **Source.** The source category appears only on XLeet and Odin and shows the method used to obtain those emails. The source category includes three options, including "hacked" (or "cracked"), "logs," or "created." As much as 98% of the emails sold on XLeet were obtained through hacking/cracking.

  Logs refer to the stolen data (including emails and passwords) obtained by information-stealing malware. Threat actors often sell logs on cybercrime forums specifying the details harvested from the user's web browser. The logs are also sold on dedicated markets and offered as bots containing all the browser-saved information regarding compromised accounts that were infected on one computer. On dedicated shops like XLeet, however, the logs category includes only corporate email credentials that were extracted and put on sale.

KELA believes the third category, "created," means that actors created several emails for sale with the same domain name. Such offers are also popular on cybercrime forums.



Buying US valid email logins personal or corps

By jamesbondd, Friday at 12:49 PM in [Spam] - mailings, databases, responses, mail-dumps, software

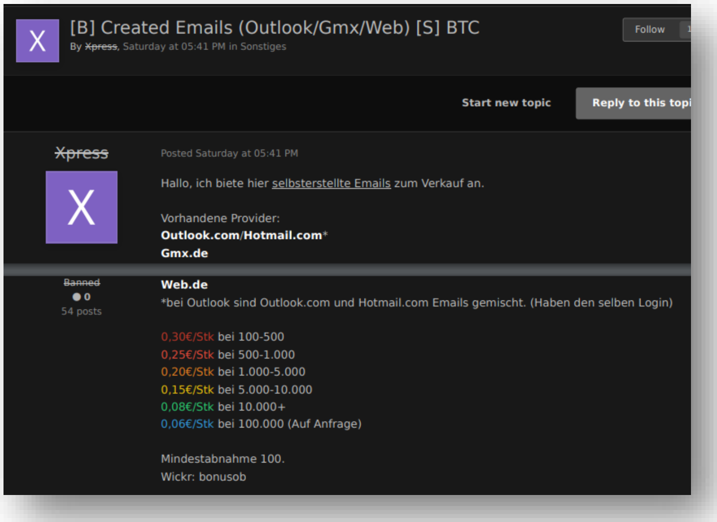
jamesbondd
byte
Paid registration
0

Posted Friday at 12:49 PM

As the title says, if you have any non-2FA hacked US emails (preferably fresh and not fully abused yet) that are US based let me know. I'm interested in buying regularly.

Send me a PM if you have any. Not interested in newly created emails.

An actor is buying "hacked emails."



[B] Created Emails (Outlook/Gmx/Web) [S] BTC

By ~~Xpress~~, Saturday at 05:41 PM in Sonstiges

~~Xpress~~
~~Banned~~
0
54 posts

Posted Saturday at 05:41 PM

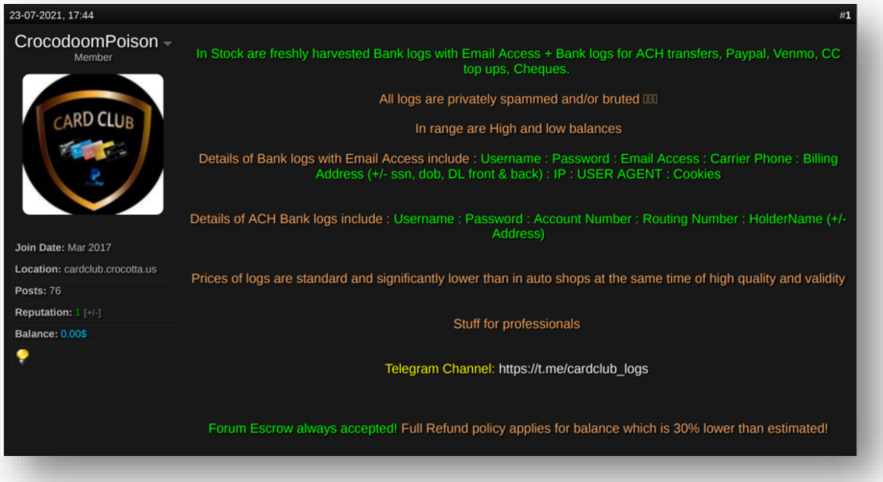
Hallo, ich biete hier selbsterstellte Emails zum Verkauf an.

Vorhandene Provider:
Outlook.com/Hotmail.com*
Gmx.de
Web.de
*bei Outlook sind Outlook.com und Hotmail.com Emails gemischt. (Haben den selben Login)

0,30€/Stk bei 100-500
0,25€/Stk bei 500-1.000
0,20€/Stk bei 1.000-5.000
0,15€/Stk bei 5.000-10.000
0,08€/Stk bei 10.000+
0,06€/Stk bei 100.000 (Auf Anfrage)

Mindestabnahme 100.
Wickr: bonusob

An actor provides "self-created emails" for sale.



23-07-2021, 17:44 #1

CrocodoomPoison
Member

Join Date: Mar 2017
Location: cardclub.crocotta.us
Posts: 76
Reputation: 1 [+/-]
Balance: 0.00$

In Stock are freshly harvested Bank logs with Email Access + Bank logs for ACH transfers, Paypal, Venmo, CC top ups, Cheques.

All logs are privately spammed and/or bruted ▯▯▯

In range are High and low balances

Details of Bank logs with Email Access include : Username : Password : Email Access : Carrier Phone : Billing Address (+/- ssn, dob, DL front & back) : IP : USER AGENT : Cookies

Details of ACH Bank logs include : Username : Password : Account Number : Routing Number : HolderName (+/- Address)

Prices of logs are standard and significantly lower than in auto shops at the same time of high quality and validity

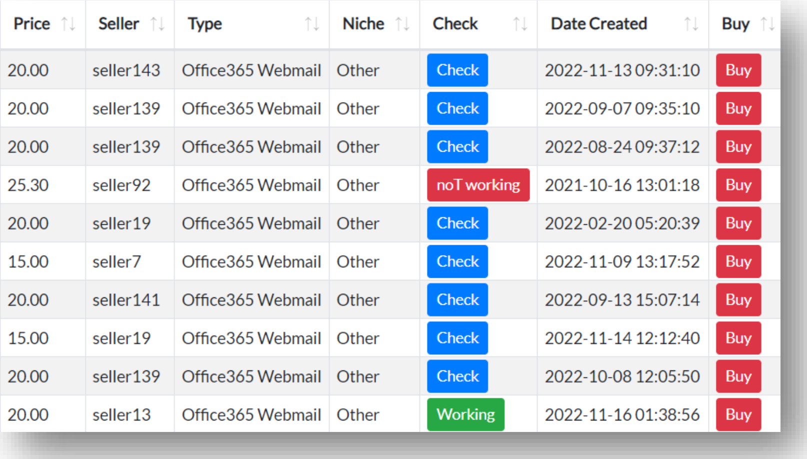
Stuff for professionals

Telegram Channel: https://t.me/cardclub_logs

Forum Escrow always accepted! Full Refund policy applies for balance which is 30% lower than estimated!

An actor is selling bank logs and email access.

- **Checking tools.** There are dedicated checkers that help ensure that stolen email credentials are still valid. Based on cybercrime chatter, there are hundreds of services for checking emails (such as LetsExtract Email Studio Business, Email Checker Pro, SendBlaster Pro, etc). The shops provide a checking service to buyers before they purchase specific webmail. Once an actor is ready to buy an email, they can click the “check” button to see if the credentials work, as shown below.

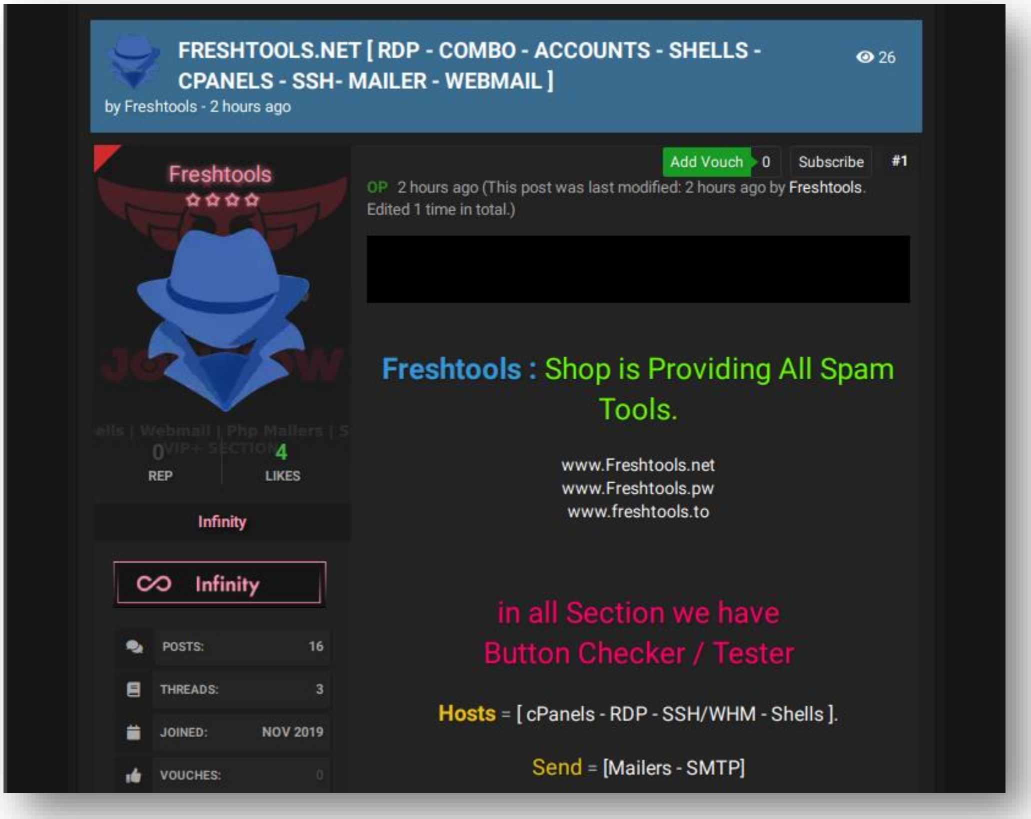


Price ⇅	Seller ⇅	Type ⇅	Niche ⇅	Check ⇅	Date Created ⇅	Buy ⇅
20.00	seller143	Office365 Webmail	Other	Check	2022-11-13 09:31:10	Buy
20.00	seller139	Office365 Webmail	Other	Check	2022-09-07 09:35:10	Buy
20.00	seller139	Office365 Webmail	Other	Check	2022-08-24 09:37:12	Buy
25.30	seller92	Office365 Webmail	Other	noT working	2021-10-16 13:01:18	Buy
20.00	seller19	Office365 Webmail	Other	Check	2022-02-20 05:20:39	Buy
15.00	seller7	Office365 Webmail	Other	Check	2022-11-09 13:17:52	Buy
20.00	seller141	Office365 Webmail	Other	Check	2022-09-13 15:07:14	Buy
15.00	seller19	Office365 Webmail	Other	Check	2022-11-14 12:12:40	Buy
20.00	seller139	Office365 Webmail	Other	Check	2022-10-08 12:05:50	Buy
20.00	seller13	Office365 Webmail	Other	Working	2022-11-16 01:38:56	Buy

Clicking the “check” button” reveals if the webmail is valid or not.

Alternative shops and Telegram channels

As described, automated shops have gained attention among cybercriminals. The re are other, smaller shops that offer similar services — webmails, SMTP, shells, RDPs, cPanel, and others. For instance, the FreshTools shop:



FRESHTOOLS.NET [RDP - COMBO - ACCOUNTS - SHELLS - CPANELS - SSH- MAILER - WEBMAIL]

by Freshtools - 2 hours ago

0 REP | 4 LIKES

Infinity

∞ Infinity

POSTS: 16
THREADS: 3
JOINED: NOV 2019
VOUCHES: 0

OP 2 hours ago (This post was last modified: 2 hours ago by Freshtools. Edited 1 time in total.)

[redacted]

Freshtools : Shop is Providing All Spam Tools.

www.Freshtools.net
www.Freshtools.pw
www.freshtools.to

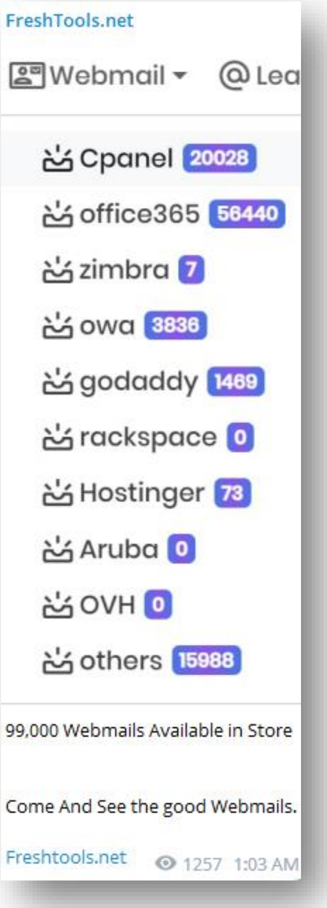
in all Section we have
Button Checker / Tester

Hosts = [cPanels - RDP - SSH/WHM - Shells].

Send = [Mailers - SMTP]

Advertisement of FreshTools on Cracked forum.

The shop also has a Telegram channel, which has more than 1000 subscribers. The common email provider is Office 365, as with other shops monitored by KELA. The admin of the channel releases updates regarding new checkers and webmails added to the shop. The Telegram channel includes a bot feature that allows buyers and sellers to get updates regarding orders, refunds, and more.

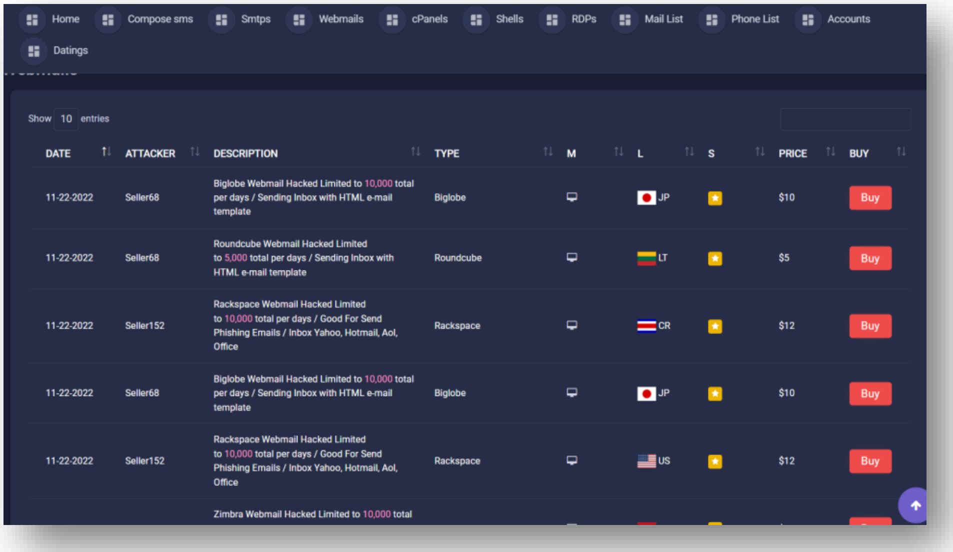


99,000 Webmails Available in Store

Come And See the good Webmails.

FreshTools shop regularly updates the webmail section, adding different email hosting providers.

The actor 0daysec promoted a website called HaxorID, where attackers published information about websites' defacement. The website also offers tools for sale, as well as hacked webmails. The email providers that are offered on the website include Office365, Zimbra, Godaddy, Owa, Hostinger, cPanel, and more. The price for webmail ranged from USD 5 to USD 12. The webmail section includes only 20 emails for sale.



DATE	ATTACKER	DESCRIPTION	TYPE	M	L	S	PRICE	BUY
11-22-2022	Seller68	Biglobe Webmail Hacked Limited to 10,000 total per days / Sending Inbox with HTML e-mail template	Biglobe	🖥	JP	★	$10	Buy
11-22-2022	Seller68	Roundcube Webmail Hacked Limited to 5,000 total per days / Sending Inbox with HTML e-mail template	Roundcube	🖥	LT	★	$5	Buy
11-22-2022	Seller152	Rackspace Webmail Hacked Limited to 10,000 total per days / Good For Send Phishing Emails / Inbox Yahoo, Hotmail, Aol, Office	Rackspace	🖥	CR	★	$12	Buy
11-22-2022	Seller68	Biglobe Webmail Hacked Limited to 10,000 total per days / Sending Inbox with HTML e-mail template	Biglobe	🖥	JP	★	$10	Buy
11-22-2022	Seller152	Rackspace Webmail Hacked Limited to 10,000 total per days / Good For Send Phishing Emails / Inbox Yahoo, Hotmail, Aol, Office	Rackspace	🖥	US	★	$12	Buy
		Zimbra Webmail Hacked Limited to 10,000 total						

HaxorID webmail section.

From corporate email to cyberattacks

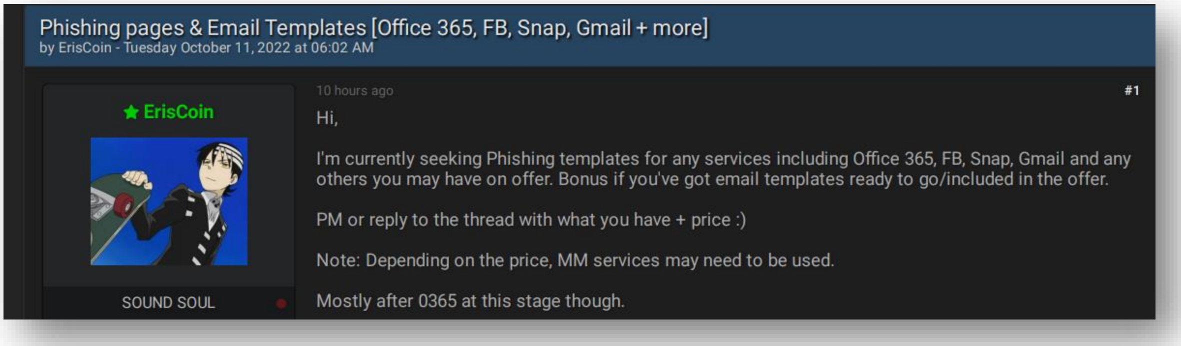
Different stakeholders are engaged in the cybercrime supply chain, aiming to exploit the email vector and gain profit. The sellers use the shops and forums to provide compromised emails. While the buyers monetize the compromised emails and deploy different cyberattacks that will yield high profits. Actors use compromised corporate email addresses for multiple attack types, from phishing to BEC and malware attacks.

The cybercrime chatter suggests that there are different methods to monetize email access. For a low-skilled actor, it's possible to become a part of the supply chain, meaning selling access on cybercrime forums. But shall an actor conduct an attack independently, there are a few possible attack types:

Monetizing email access through phishing

Phishing is a popular type of attack that lures the victim into revealing sensitive information such as passwords and credit card numbers. Phishing attacks are based on social engineering tactics that exploit human error and manipulate individuals' behavior to give up sensitive information to an entity they think they can trust. In this case, having access to a corporate email account abused for distributing phishing messages can benefit an attacker.

There are several tools and tutorials available on the cybercrime underground, further easing the process of phishing attacks, from dedicated templates and phishing pages to phishing kits.



Phishing pages & Email Templates [Office 365, FB, Snap, Gmail + more]
by ErisCoin - Tuesday October 11, 2022 at 06:02 AM

★ ErisCoin

SOUND SOUL

10 hours ago #1

Hi,

I'm currently seeking Phishing templates for any services including Office 365, FB, Snap, Gmail and any others you may have on offer. Bonus if you've got email templates ready to go/included in the offer.

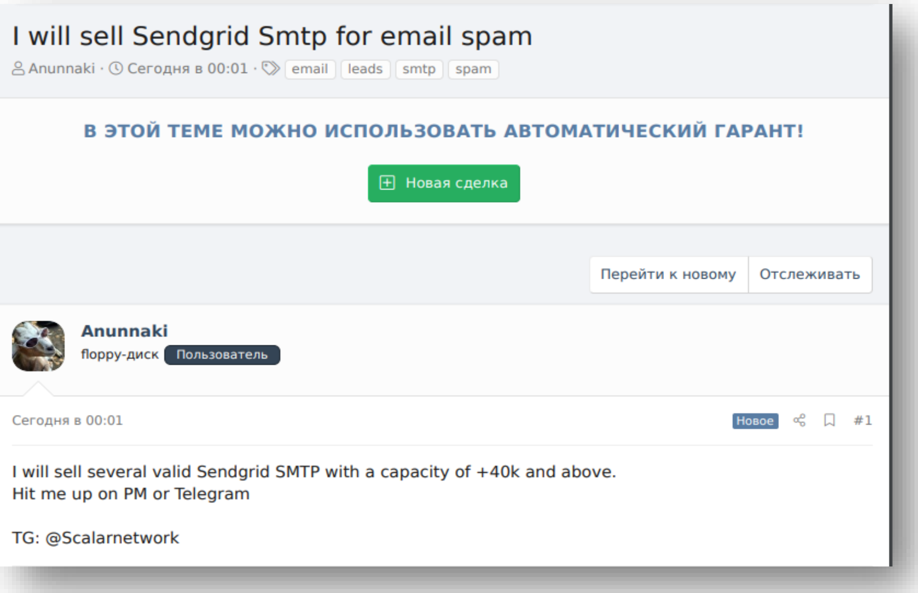
PM or reply to the thread with what you have + price :)

Note: Depending on the price, MM services may need to be used.

Mostly after 0365 at this stage though.

This actor is looking for phishing templates for different services including Office 365.

There are different SMTP services on cybercrime forums that claim to ease the process of phishing attacks. Compromised SMTP servers are used to send emails to recipients with a large number of messages, using the victim's domain, which makes them appear legitimate.



I will sell Sendgrid Smtp for email spam

Anunnaki · Сегодня в 00:01 · email leads smtp spam

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

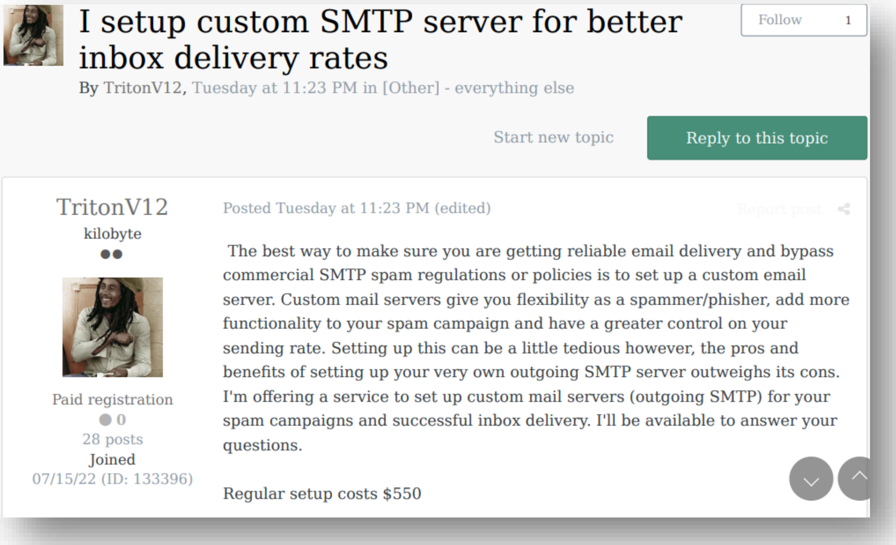
Anunnaki
floppy-диск Пользователь

Сегодня в 00:01 Новое #1

I will sell several valid Sendgrid SMTP with a capacity of +40k and above.
Hit me up on PM or Telegram

TG: @Scalarnetwork

An actor is offering Sendgrid SMTP for email spam.



I setup custom SMTP server for better inbox delivery rates

By TritonV12, Tuesday at 11:23 PM in [Other] - everything else

TritonV12
kilobyte
Paid registration
0
28 posts
Joined
07/15/22 (ID: 133396)

Posted Tuesday at 11:23 PM (edited)

The best way to make sure you are getting reliable email delivery and bypass commercial SMTP spam regulations or policies is to set up a custom email server. Custom mail servers give you flexibility as a spammer/phisher, add more functionality to your spam campaign and have a greater control on your sending rate. Setting up this can be a little tedious however, the pros and benefits of setting up your very own outgoing SMTP server outweighs its cons. I'm offering a service to set up custom mail servers (outgoing SMTP) for your spam campaigns and successful inbox delivery. I'll be available to answer your questions.

Regular setup costs $550

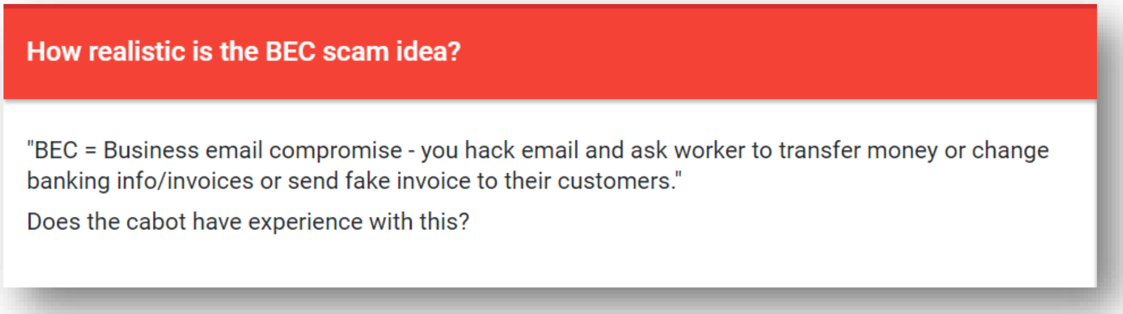
This actor offers an SMTP server for spamming and phishing campaigns.

Combined with legitimate corporate email access bought through the aforementioned auto shops, such tools can significantly ease phishing attacks and attract more non-skilled actors.

Monetizing email access through BEC

Business Email Compromise (BEC), also known as Email Account Compromise (EAC), is an attack that tricks the victim into transferring money to an account or location that the attacker controls. In 2021, the FBI found that the total money stolen in BEC scams far could exceed the losses resulting from ransomware attacks.[1] BEC attacks require less sophisticated technical skills compared to malware attacks and rely more on social engineering techniques. Therefore, their popularity has been growing in the cybercrime ecosystem because they can be extremely profitable.

Threat actors consult and share information regarding BEC attacks. The actor arch6661 posted on XSS forum asking who was involved in compromising business email. He probably was looking for a hacker who could conduct BEC attacks and steal money. The actor TESTAROSSA replied that the sum for a BEC scam that he could cash out ranges from USD 20,000 to USD 20 million.



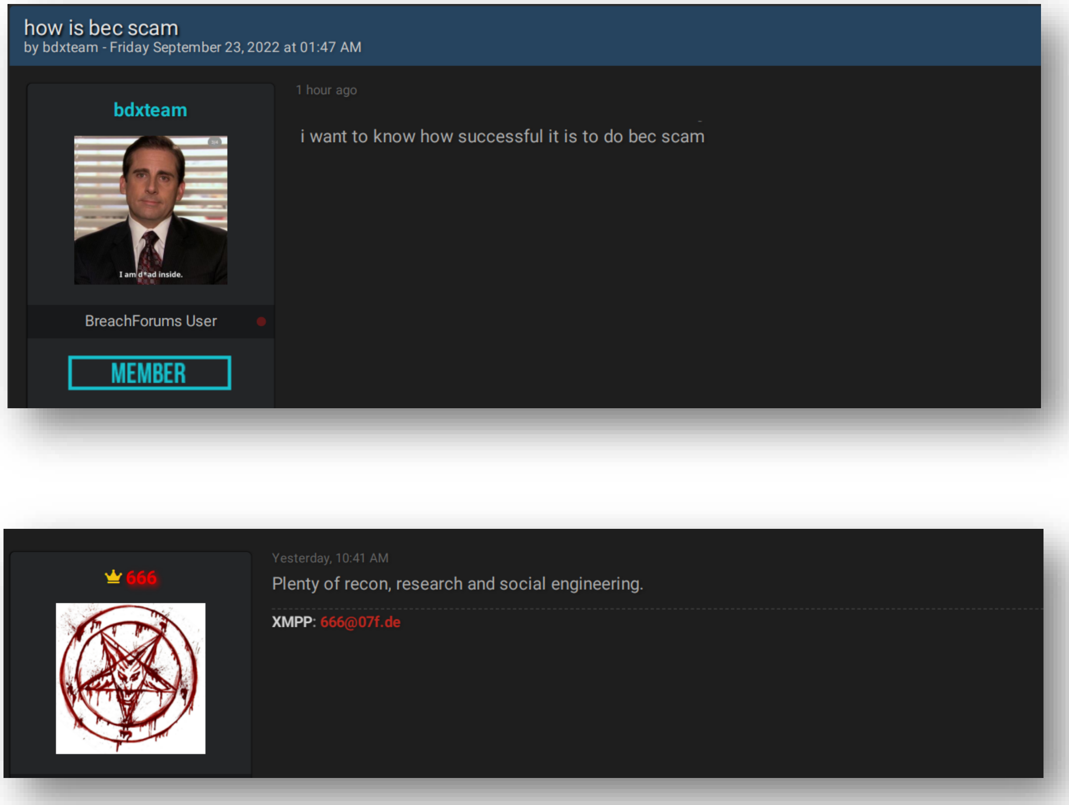
How realistic is the BEC scam idea?

"BEC = Business email compromise - you hack email and ask worker to transfer money or change banking info/invoices or send fake invoice to their customers."

Does the cabot have experience with this?

A threat actor explained the aim of a BEC attack.

[1] The total losses in BEC attacks was USD 2.4 billion, compared with about USD 49 million for ransomware attacks. It's important to note that it's more difficult to track the financial damage of ransomware victims due to the lack of transparency regarding ransomware payments. Moreover, the FBI report was based on the voluntary complaints of just 3,729 victims, in a case where there are certainly many more victims.



how is bec scam
by bdxteam - Friday September 23, 2022 at 01:47 AM

bdxteam

BreachForums User

MEMBER

1 hour ago

i want to know how successful it is to do bec scam

666

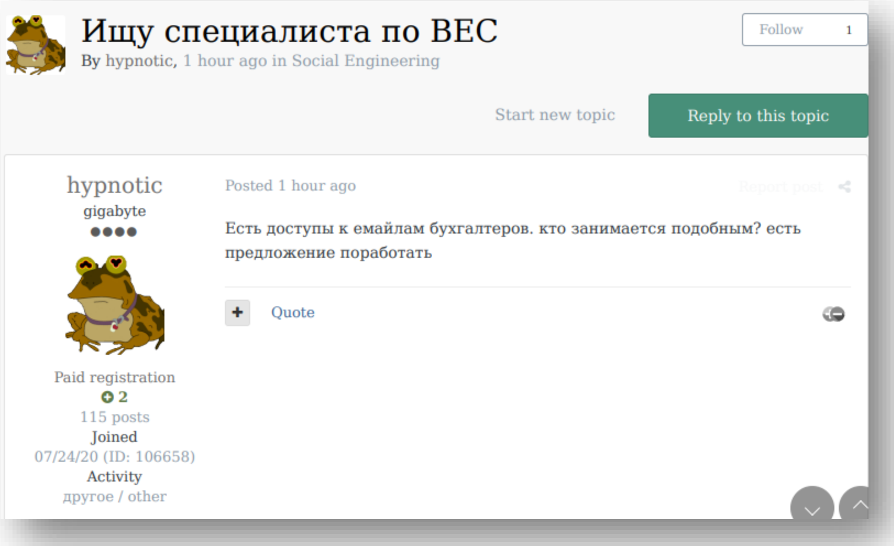
Yesterday, 10:41 AM

Plenty of recon, research and social engineering.

XMPP: 666@07f.de

Actor 666 claimed that a successful BEC attack requires several tactics.

In another example of cooperation between cybercriminals, on July 7, 2022, a threat actor, hypnotic, posted on Exploit that he was looking for a BEC specialist who had accountants' email access. It is likely that hypnotic was interested in targeting email accounts of employees in finance and accounting positions who are authorized to have business credentials and can pay the spoofed bills. The actor LastOneLeft responded that he was working on several finance accounts and had already been able to steal a large amount of money, providing proof of concept screenshots.



Ищу специалиста по BEC

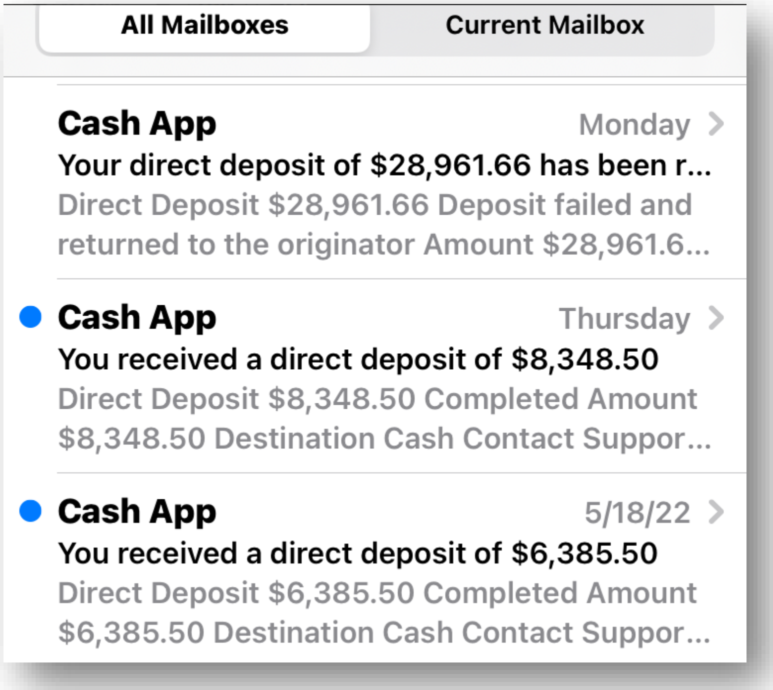
By hypnotic, 1 hour ago in Social Engineering

hypnotic
gigabyte
●●●●
Paid registration
2
115 posts
Joined
07/24/20 (ID: 106658)
Activity
другое / other

Posted 1 hour ago

Есть доступы к емайлам бухгалтеров. кто занимается подобным? есть предложение поработать

An actor is looking for a BEC specialist.



Cash App Monday
Your direct deposit of $28,961.66 has been r...
Direct Deposit $28,961.66 Deposit failed and returned to the originator Amount $28,961.6...

Cash App Thursday
You received a direct deposit of $8,348.50
Direct Deposit $8,348.50 Completed Amount $8,348.50 Destination Cash Contact Suppor...

Cash App 5/18/22
You received a direct deposit of $6,385.50
Direct Deposit $6,385.50 Completed Amount $6,385.50 Destination Cash Contact Suppor...

An actor providing proof of successful BEC scams and the cash he has stolen

A recent BEC campaign targeted CEOs or CFOs of organizations with spear-phishing using adversary-in-the-middle (AiTM) techniques to hack corporate executives' Microsoft 365 accounts, even those protected by multi-factor authentication.

One BEC actor can target thousands of companies, causing losses of millions of dollars. Automated markets can ease the scale of attacks, allowing actors to target dozens of corporate emails. A cybercrime BEC group that targeted more than 50,000 victims is SilverTerrier. Some of its members were arrested in 2021 after scamming thousands of companies globally. According to Interpol, one of the threat actors obtained more than 800,000 potential victim domain credentials on his laptop.

Monetizing email access through malware

Malware attacks involve all types of malicious software, like ransomware, information stealing trojans, spyware, etc. Starting with a compromised email account cybercriminals can also use social engineering attacks as an entry vector to deploy malware on targeted networks, luring a victim into downloading a malicious payload.

Malware installation enables actors to gain easy profits. Threat actors can install info stealing trojan to steal user banking credentials and cash out money from a compromised account. Cybercriminals can also deploy a ransomware attack and demand a ransom payment. Ransomware gangs use extortion tactics to monetize operations faster, threatening the victim that they would publish valuable data if the victim does not pay the ransom.

Threat actors share information regarding different malware campaigns on cybercrime forums. On March 29, 2022, the threat actor digitalninja asked what the best way was to spread malware. The responses showed the value of email access in this supply chain. The threat actor n0nce suggested as one of the methods picking a few specific targets and trying to email them individually.

Last year IKEA suffered a cyberattack that started from compromised IKEA email accounts. The threat actors targeted employees with internal phishing attacks using stolen reply-chain emails. The company warned its employees that the attack came via employees' email accounts as a reply to an ongoing conversation. The email contained malicious documents capable of installing malware on recipients' devices.

Awareness is key

Cybercriminals are constantly looking for new ways to conduct cyberattacks that will generate high sums of money. In February 2022, researchers found that more organizations (78%) suffered email-based ransomware attacks, closely followed by BEC attacks (77%) The findings show that the email vector is favored by cybercriminals, who prefer to manipulate human behavior rather than technical vulnerabilities. It seems that compromised corporate emails are valuable goods that can easily be monetized for several attacks from phishing, BEC, and different malware attacks.

The cybercrime ecosystem focuses on servitization and sales automation. As a result, dedicated shops will flourish. Shops like XLeet, Odin, Xmina, and Lufix offer corporate webmails, and make cybercriminals' lives easier, allowing them to buy a large number of emails at an affordable price, and then targeting dozens of victims.

Organizations should ensure that they continually:

- **Train and educate all employees, customers, and vendors** on safely using their credentials and personal information online. This cyber-training should specifically include how to identify suspicious activities, such as possible scam emails or unusual requests from unauthorized individuals or email addresses. The human factor plays a significant role in an organization's cybersecurity. The larger the organization, the bigger the chance of threats. Therefore, creating such mandatory cybersecurity training across all these organizations would significantly reduce the chances that they would be compromised because of an employee's mistake.
- **Enforce a periodic password change** for all services and platforms among the organization's employees and customers. The password should be different from any other passwords previously or currently utilized by the compromised users.

- **Monitor the cybercrime landscape** to discover new trends and threats. Attackers develop methods to commit scam attacks. Knowing cybercriminals' tactics and being familiar with new cybercrime marketplaces allow companies to address this evolving threat more effectively and decrease financial losses.

KELA's monitoring of different shops uncovered compromised corporate webmails, providing real-time intelligence into cybercrime activities, allowing companies to identify compromised accounts and prevent cyberattacks.

Try KELA's cybercrime intelligence platform for free to uncover threats to your organizaton within minutes