

How Much is Your Hacked Site Worth? An Overview of Online Shops Selling Access to Compromised Services

Ramuel Gall

Wordfence Senior Threat Analyst

Bachelor of Science in Cybersecurity and Information Assurance

CISSP, GWAPT, CHFI, SSCP, Security+, Pentest+, CySA+, AWS CCP, AWS SAA, AWS CDA

Publication Date: December 20, 2022

© 2022 WORDFENCE ALL RIGHTS RESERVED

Table of Contents

How Much is Your Hacked Site Worth? An Overview of Online Shops Selling Access to Compromised Services	1
Table of Contents	2
Introduction	3
I. Why are "Shops" Proliferating?	3
II. Commonalities Across "Shops"	5
Funding Sources	5
Buyer and Seller Anonymity	6
Verification Functionality	6
Support Ticketing System	7
Stock Status Display	7
III. The "Shops" We Investigated	8
Olux	8
Oxux	9
Hades Shop	10
Omgo	11
Odin	12
AK47	13
IV. Core Products Across the "Shops"	14
RDP Credentials	14
cPanel Credentials	15
Webshell Access	16
Leafmailers and SMTP Accounts	17
Webmail accounts	18
Leads and Combo Lists	20
Scripts and Scam Pages	21
V. Takeaways	23
Customer Base	23
Preventative Measures	23
Appendix	24
Shop domains	24
Olux	24
Oxux/Knockoff Olux Shops (not exhaustive)	24
Hades	24
Omgo	24
Odin	24
AK47	24

Introduction

A key component in the ecosystem used by online criminals, e-commerce sites, colloquially known as “shops,” are geared towards providing a specific range of goods and services frequently used by SEO spammers, scammers, identity thieves, and other small-scale for-profit threat actors. This includes access to hacked servers, websites, and email accounts. In this context, “small-scale” means that we have seen no evidence that the threat actors buying and selling on these shops are closely affiliated with nation-states or APTs, though it is true that the goods and services for sale may occasionally be of use to more skilled attackers for watering-hole attacks, C2 infrastructure, and spear phishing.

Most of these marketplaces are not technically on the dark web, and several of them are clearly indexed and advertise their offerings on search engines. While “pop-up” shops selling hacked accounts on third-party services such as sellpass.io are common, this white paper will focus specifically on standalone e-commerce sites whose core products and services include access to infrastructure used to perform attacks on websites, as well as access to hacked websites and accounts themselves.

The short answer to “how much is a hacked site worth?” is “not much,” though we will go into specific price ranges in a later section.

I. Why are “Shops” Proliferating?

Shops are primarily proliferating thanks to the escrow services they provide that protect buyer and seller. Telegram channels have become a primary communication nexus for cybercriminals¹, and are frequently used to buy and sell malware and leaked or hacked data, but transactions involving illicit goods run a high risk of deception for all parties involved.

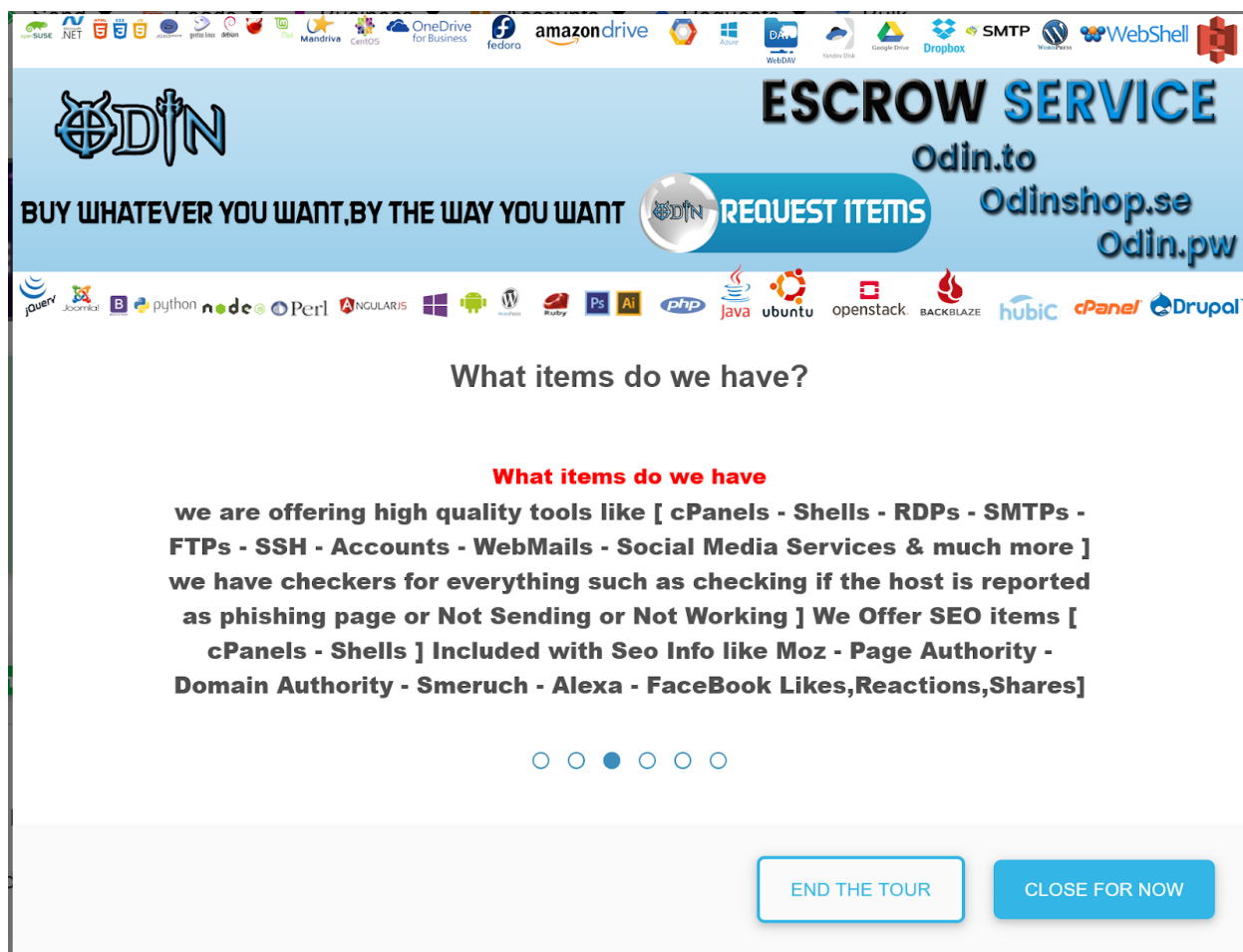
Escrow services, where a trusted third party holds on to payment until goods are delivered, are often necessary to facilitate transactions between actors who make a living out of scams and theft². However, for lower-risk verified goods packaged individually at

¹ “Why cybercriminals are flocking to Telegram,” intel471.com.
<https://intel471.com/blog/why-cybercriminals-are-flocking-to-telegram>.

² Photon Research Team, “Escrow systems on cybercriminal forums: The Good, the Bad and the Ugly,” digitalshadows.com.
<https://www.digitalshadows.com/blog-and-research/escrow-systems-on-cybercriminal-forums/>.

lower unit prices, such as hacked sites or email accounts, it's not quite as practical to involve a live third party for every single transaction.

In addition to these factors, the source code of one of the most popular shops, Olux, has been available for some time³. These factors have led to the proliferation of shops, which act as automated escrow services.



Pictured: The Odin marketplace welcome popup indicating its purpose as an Escrow service

³O. Maksuti, "Olux Shop Script" [source code], github.com.
<https://github.com/omermaksutii/olux>.

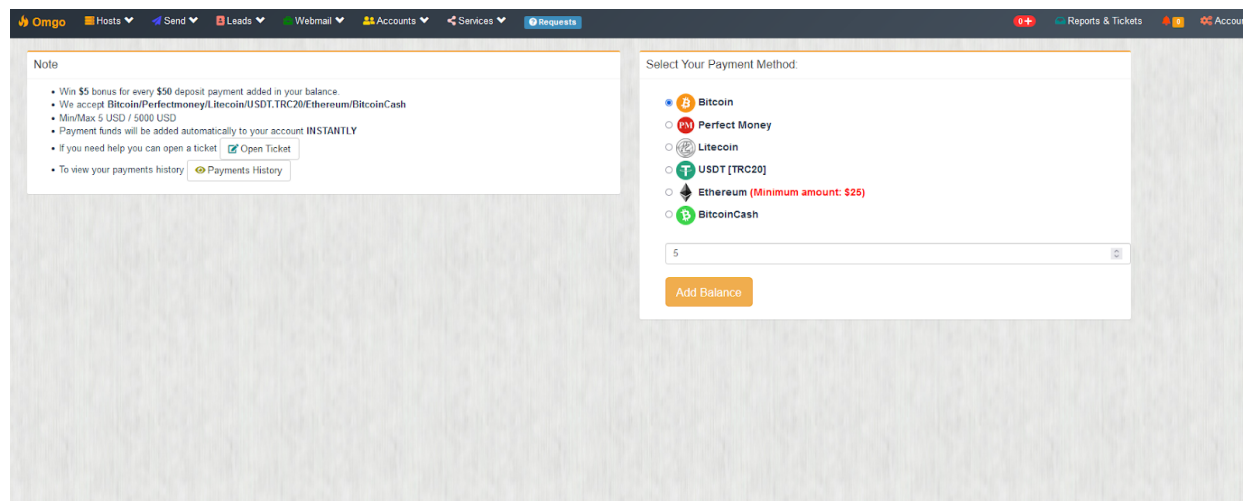
II. Commonalities Across “Shops”

We investigated six different online “shops” for this white paper, though many more exist. Each shop requires registering an account in order to view their products, though no email verification takes place. Nearly every shop we investigated used a CAPTCHA as well as Cloudflare, to hide the server origin, for DDOS mitigation, or both.

It is important to note that not every item for sale was the result of a compromise - in some cases sellers appear to be reselling access to hosting accounts they created, and some shops indicated the source of the product as “Cracked” or “Created”. “Created” hosting or email typically includes a .tk domain, as these can be registered in bulk and are free for the first year. “Created” products are typically less expensive than equivalent “Cracked” products.

Funding Sources


Each shop accepts payments in cryptocurrency, though some also accept other digital payment options such as Perfect Money. Most shops had a maximum deposit amount of \$5,000 USD in a single transaction, which may be intended to help circumvent money-laundering regulations.



Pictured: The Omgo shop's Payment screen, used to add funds

Buyer and Seller Anonymity

Buyers and Sellers on all shops are anonymous and are identified by a number, for example "seller254". Some shops also include seller metrics including total sales and reviews.

DETAILS	SALES	RATING
Seller	Seller254	
Last Login	19/12/2022 03:17:10 am	
Register Date	13/08/2020	
Total Sales	\$ 5539.00	
Total Sold Items	1418	
Average Rating	 (2)	

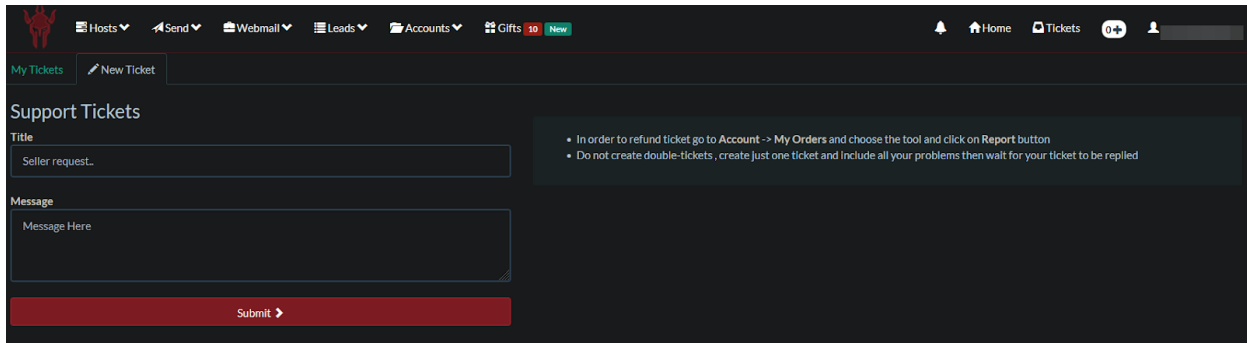
Pictured: Seller Details. Note that this shop provides additional information about the seller including their average rating.

Verification Functionality

Most shops also provide a verification functionality that tests the offered product or service to see if it is still working, for instance, to send an email from a PHP email script known as a leafmailer to the customer's account to verify that it can successfully send mail. We reviewed the headers of an email we received after testing this verification functionality on one of the shops and determined that verification requests are being routed through TOR in order to disguise the shop's origin IP, though the headers did reveal the location of the mailer itself.

Support Ticketing System

Shops typically offer a support ticketing system and a 12 to 24-hour return or replacement warranty.



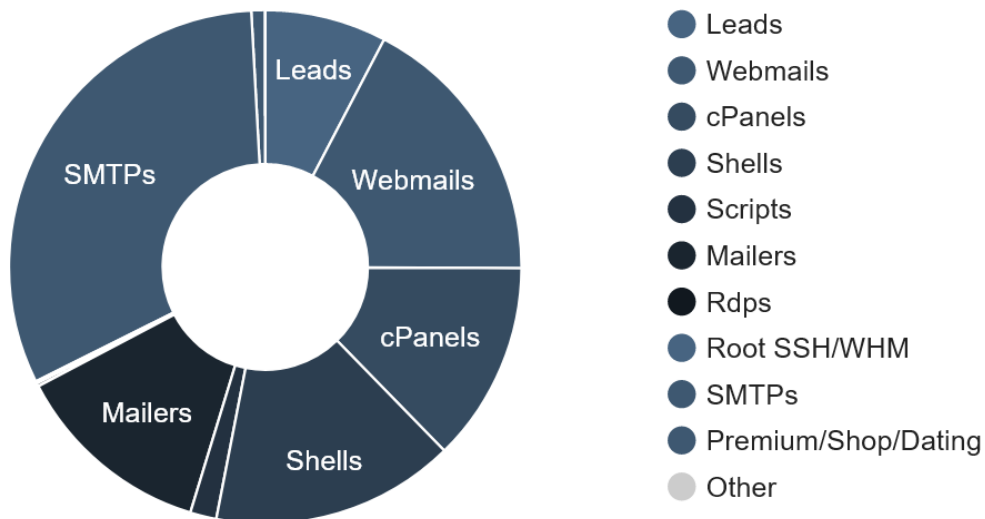
The screenshot shows a web interface for a support ticketing system. At the top, there is a navigation bar with various menu items: Hosts, Send, Webmail, Leads, Accounts, Gifts (with a red '30' badge and a 'New' button), Home, Tickets (with a '0+' badge), and a user profile icon. Below the navigation bar, there is a 'My Tickets' section with a 'New Ticket' button. The main area is titled 'Support Tickets' and contains a form with a 'Title' field (placeholder: 'Seller request...') and a 'Message' field (placeholder: 'Message Here'). A red 'Submit' button is at the bottom of the form. To the right of the form, there is a dark grey box with white text providing instructions: 'In order to refund ticket go to Account -> My Orders and choose the tool and click on Report button' and 'Do not create double-tickets, create just one ticket and Include all your problems then wait for your ticket to be replied'.

Pictured: the Hades Shop support ticket system

Stock Status Display

The number and variety of products in stock varies wildly by shop, and from week to week, indicating a great degree of turnover. For this reason each shop has a stock status display on the dashboard indicating how many of each product it has in stock.

Available Tools !



Pictured: The Stock Status Display on Olux[.]so

III. The “Shops” We Investigated

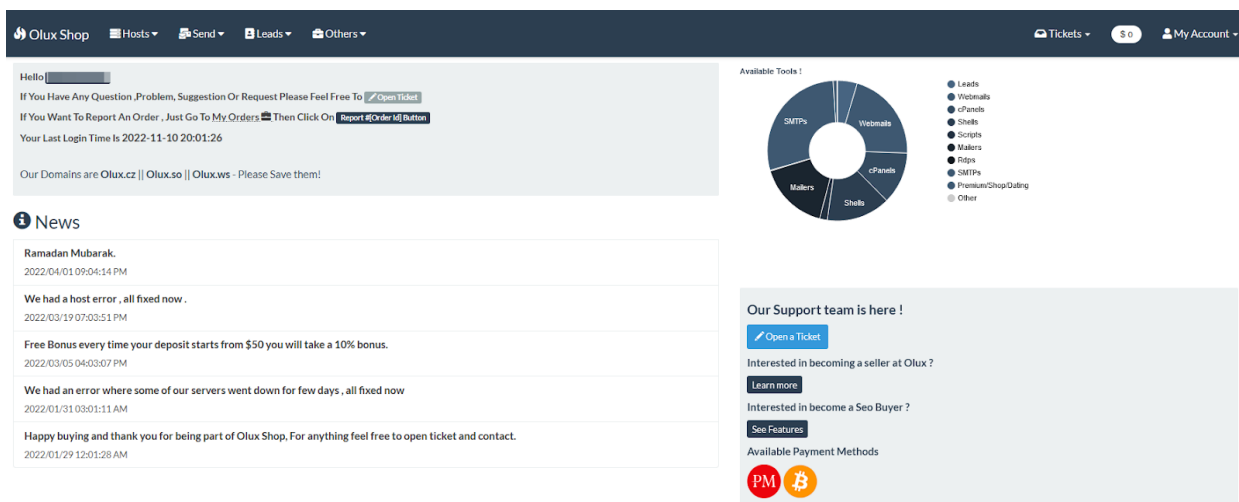
We investigated 6 shops in this overview, please note that this is not an exhaustive list of the ecosystem.

Olux

The Olux shop is one of the most popular marketplaces of the past few years, and forks of its laravel source code appear to power each of the other shops mentioned in this white paper. While the Olux shop source code was “leaked” by another threat actor in late 2021, we were also able to find older versions of it online, indicating that it has been publicly available for some time. Unlike the other shops we surveyed, the “test” functionality on the Olux shop appears to use encryption rather than simply passing in the ID of the product being offered, indicating ongoing development.

At the time of publication, Olux was stocked with thousands of mailer accounts, webshells, and cPanel accounts. The Olux shop uses a number of domain names for redundancy in case any one domain is suspended. Additionally, as this was the only shop we investigated that was not protected by Cloudflare, we were able to find several additional shops with different branding hosted on the same server, including spyxe[.]to and xleet[.]ws, though we did not investigate these in depth.

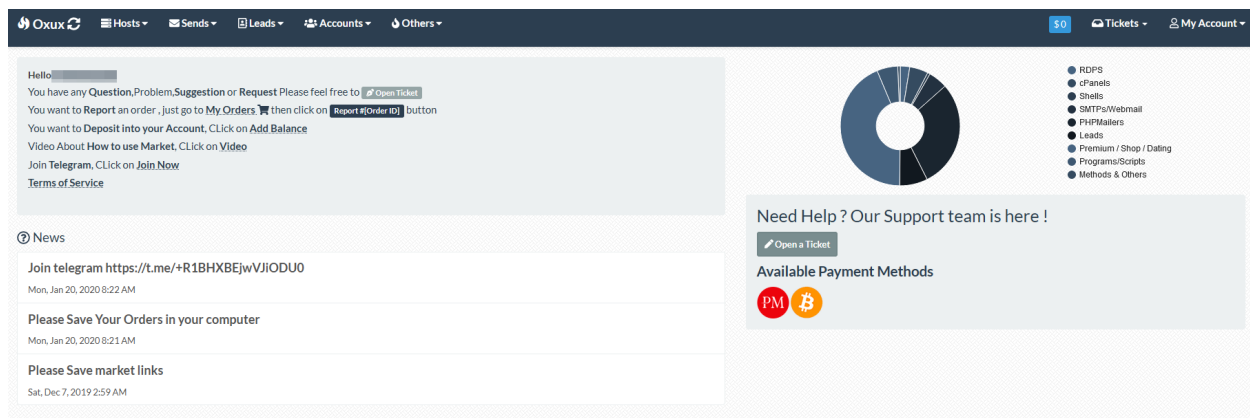
Of particular note is the fact that the Olux shop has started offering Credit Card information (referred to as “fullz”) as well as Bank Accounts for sale, which may attract additional attention from law enforcement. None of the other shops we investigated offer fullz at this time.



Pictured: The Olux Dashboard

Oxux

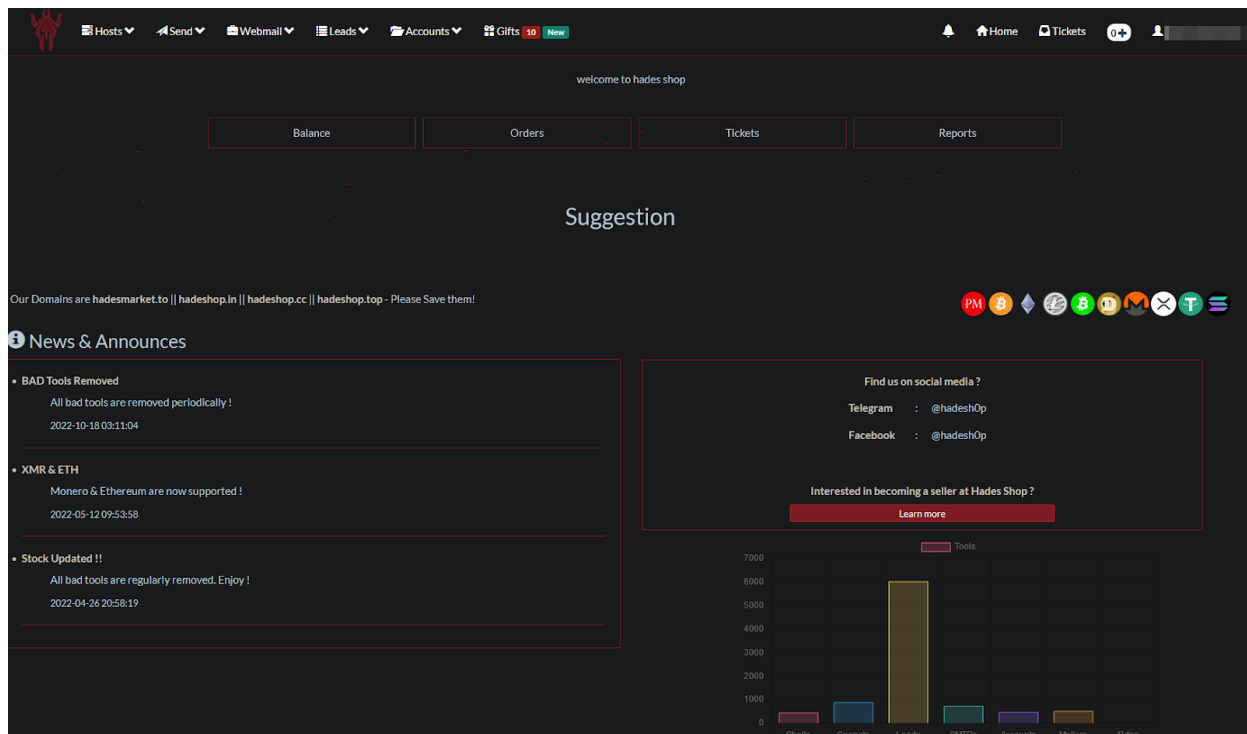
A number of similar-sounding domains capitalizing on the Olux brand, such as “Oxux”, also appear to be hosting functional shops, though these typically lack many of the features of the official Olux shop. The Oxux shop was the first shop we encountered in this investigation and appears to be actively in use. At the time of publication, it was stocked with several hundred RDP accounts, more than any other shop. While we only investigated this particular Olux knockoff, a number of other knockoff, fake, or abandoned Olux-adjacent shops appear to exist, many in various states of disrepair.



Pictured: The Oxux Dashboard

Hades Shop

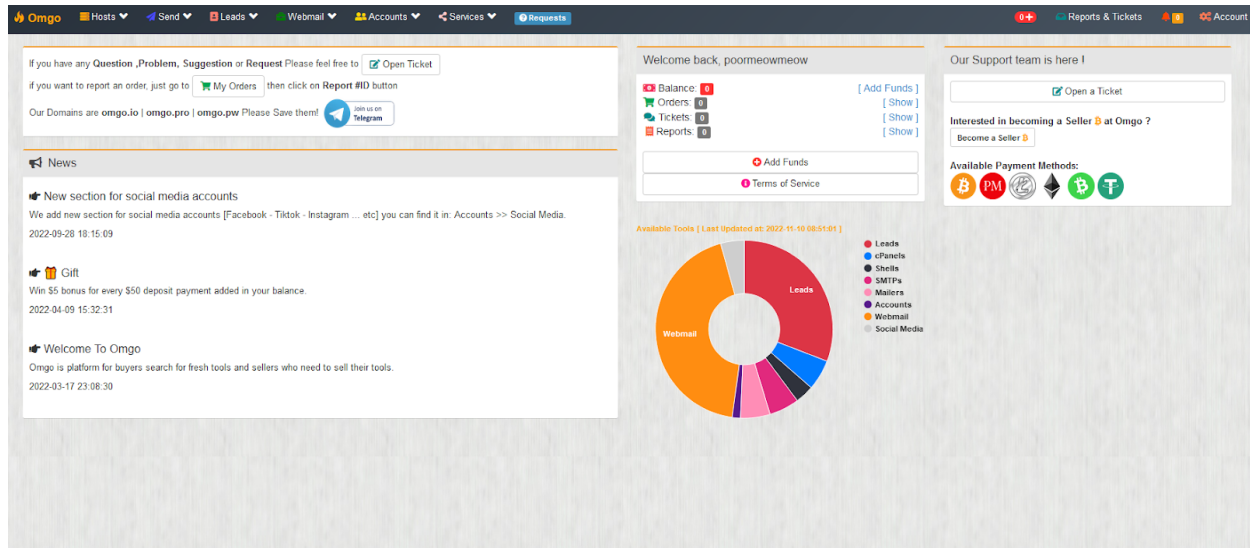
The Hades Shop was one of the more full-featured shops we investigated, including features such as SEO and alexa rank checking for cPanel offerings, and even going as far as to offer promotional giveaway items on depositing funds. Its primary offering at the time of publication was a few thousand email leads and combo lists. Like the Olux shop, the Hades Shop uses a number of domain names for redundancy.



Pictured: The Hades shop dashboard

Omgo

The Omgo shop is also one of the more full-featured shops, and provides prospective buyers the full domain name as well as SEO information about cPannels for sale. It was one of the most fully-stocked shops we visited, offering tens of thousands of individual hacked webmail accounts and several thousand cPanel accounts, shells, and leafmailers. Like the other shops, Omgo uses multiple domains for redundancy.



Pictured: The Omgo shop dashboard

Odin

The Odin shop seems to be one of the most actively developed shops we investigated and is promoting itself heavily. It had the largest stock of cPanels for sale, more than 10,000 at the time of writing, and actively advertises that its webshells are intended for black-hat SEO.

Odin

Hosts Send Leads Business Accounts Requests Bulk Offers

UNZIP-SEND-SEO

MAILERS 1\$

GOOGLE ADS

BALANCE 0 [Add Funds]

ORDERS 0 [Show]

TICKETS 0 [Show]

REPORTS 0 [Show]

Welcome poormeowmeow

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
odinshop.io || odin.pw || odinshop.se || odin.pm || Tor Mirror odinshoy3y5c6ejn3ktyggxmq5sy5eldremz353z6ucdugdcad onon ||
- Please Save them!

[TERMS OF SERVICE](#)

Invite Users

<https://odinshop.io/?referral=17796> [COPY](#) Total Bonus :- Total Referrals :- 0

Our News

[NEWS BUYER](#) 2022/08/24 08:56:08
are currently working to improve the checkers in all sections ,, stay tuned good things are coming.

[ACTION](#) 2022/08/02 09:30:54

V.I.P Bulk Offers

Latest Added Tools Latest Sold Tools

Latest 10 Sold Tools

Seller417 Sold cpanel To Buyer15241, 2022-11-10 17:12:57
Seller376 Sold cpanel To Buyer15241, 2022-11-10 16:54:33
Seller376 Sold cpanel To Buyer15241, 2022-11-10 16:53:27
Seller376 Sold cpanel To Buyer15241, 2022-11-10 16:53:14
Seller376 Sold cpanel To Buyer15241, 2022-11-10 16:49:09
Seller254 Sold cpanel To Buyer15241, 2022-11-10 16:48:38
Seller376 Sold cpanel To Buyer17786, 2022-11-10 16:45:15
Seller376 Sold cpanel To Buyer17786, 2022-11-10 16:44:13

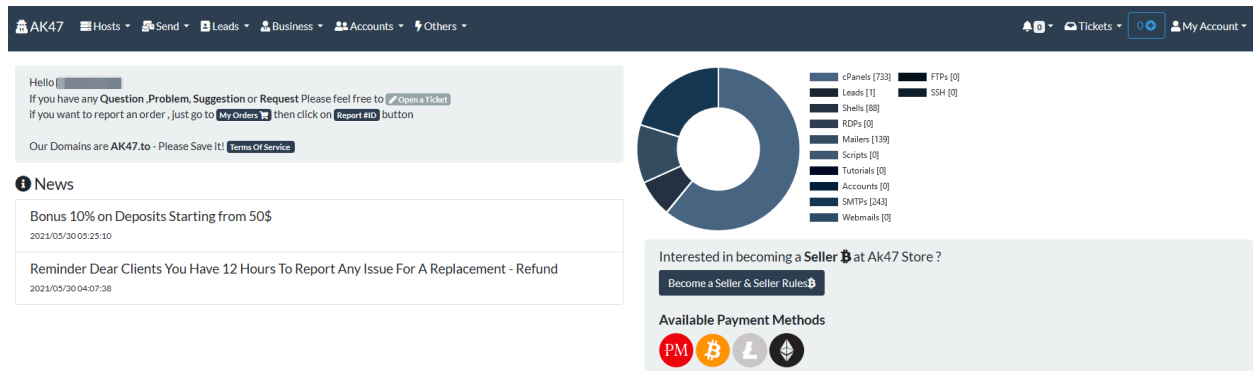
Latest Sellers Offers Latest Buyers Requests

Latest 10 Added Sellers Offers [Send mes...](#)

Pictured: the Odin shop dashboard

AK47

The AK47 shop was the least active shop we investigated and the most limited and similar in functionality to the original Olux/Oxux shop, with a few hundred cPanels for sale and very few other offerings.



Pictured: the AK47 shop dashboard

IV. Core Products Across the “Shops”

RDP Credentials

A core offering of nearly all the shops we investigated is Remote Desktop Protocol (RDP) credentials for Windows Servers, hosted on Microsoft Azure, DigitalOcean, AWS, or another cloud platform. These provide a remote Windows Desktop from which to conduct attacks and are typically used as an additional layer of anonymity in order to actually run the scripts used to send out mass-exploitation and credential stuffing attacks, as well as to bulk-manage exploited sites using tools such as the F-Automatical script. These provide key functionality and it is likely that many of the sellers on the shop sites themselves are using these to compromise and manage their cPanel, webshell, and leafmailer offerings.

Pricing appears to be in the \$3.50 to \$15 USD range, depending on the access level being sold and the amount of RAM the server is provisioned with.

Oxux

Hosts

Sends

Leads

Accounts

Others

\$0

Tickets

My Account

Country

Windows Type

Access

Detected Hosting

Seller

ALL

ALL

ALL

ALL

Filter

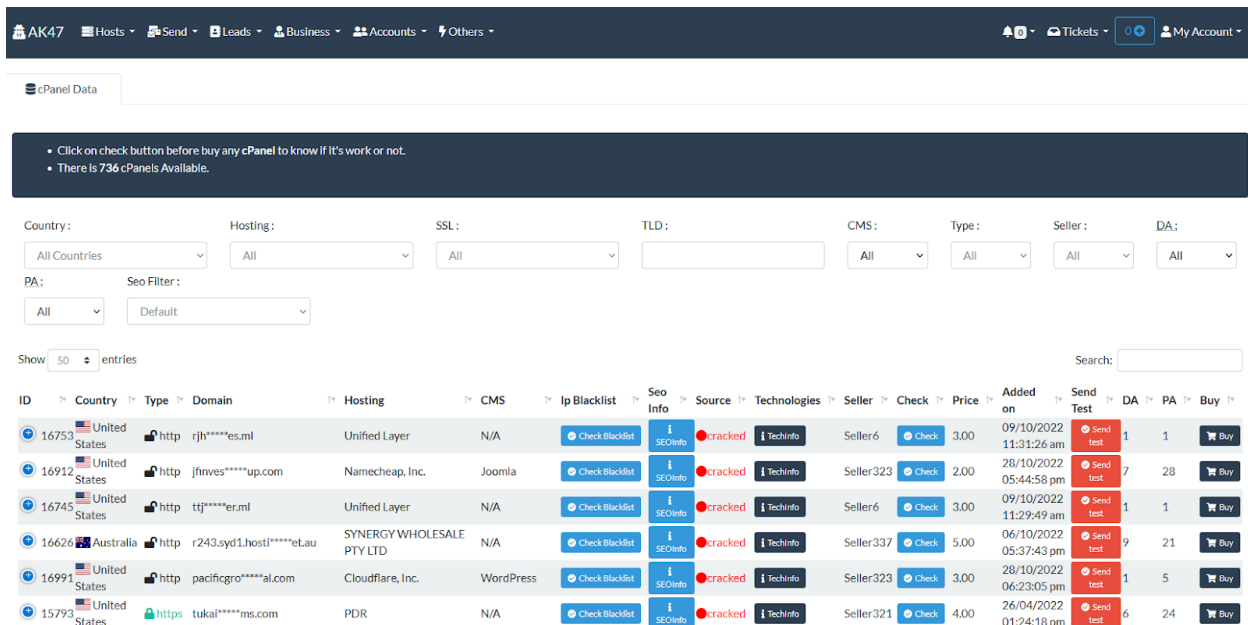
Country	Windows	RAM	ACCESS	USER	Detect Hosting	Seller	Price	Added on	Buy
United States	2012	4GB	User	s2***	AWS EC2	seller25	\$4.5	2022/11/10 11:24:54 AM	
United States	2012	4GB	User	s4***	AWS EC2	seller25	\$4.5	2022/11/10 11:24:48 AM	
United States	2012	4GB	User	s5***	AWS EC2	seller25	\$4.5	2022/11/10 11:24:45 AM	
United States	2012	4GB	User	s5***	AWS EC2	seller25	\$4.5	2022/11/10 11:24:34 AM	
United States	2012	4GB	User	s4***	AWS EC2	seller25	\$4.5	2022/11/10 11:24:31 AM	
United States	2012	4GB	User	s3***	AWS EC2	seller25	\$4.5	2022/11/10 11:24:28 AM	
United States	2022	16 GB	admin	ad***	Microsoft Azure Cloud	seller28	\$10	2022/11/10 08:46:07 AM	
United States	2022	16 GB	admin	ad***	Microsoft Azure Cloud	seller28	\$10	2022/11/10 08:45:02 AM	
United States	2022	16 GB	admin	ad***	Microsoft Azure Cloud	seller28	\$10	2022/11/10 08:43:54 AM	
United States	2022	16 GB	admin	ad***	Microsoft Azure Cloud	seller28	\$10	2022/11/10 08:43:01 AM	
United States	2022	16 GB	admin	ad***	Microsoft Azure Cloud	seller28	\$10	2022/11/10 08:42:01 AM	
United States	2022	16 GB	admin	ad***	Microsoft Azure Cloud	seller28	\$10	2022/11/10 08:41:29 AM	

Pictured: The Oxux marketplace's RDP offerings

cPanel Credentials

cPanel credentials that provide access to a hosting account that includes a domain and webmail are another core product. These credentials effectively grant the buyer full access to any websites hosted under the cPanel. All shops list the TLD, host, and hosting country. Some shops also include the partial or full domain as well as SEO ranking information, traffic to the site, and whether the domain is on a blacklist. We were unable to determine whether any of the webshells or leafmailers for sale were on the same domains as the cPanels, but this would be a trivial way for a seller to make additional money off of a hacked site.

Pricing for cPanel Credentials appears to range from \$2-\$15 USD, with most offerings in the \$7-\$10 USD range.



AK47 Hosts Send Leads Business Accounts Others Tickets My Account

cPanel Data

- Click on check button before buy any cPanel to know if it's work or not.
- There is 736 cPanels Available.

Country: All Countries Hosting: All SSL: All TLD: CMS: All Type: All Seller: All DA: All

PA: All Seo Filter: Default

Show 50 entries Search:

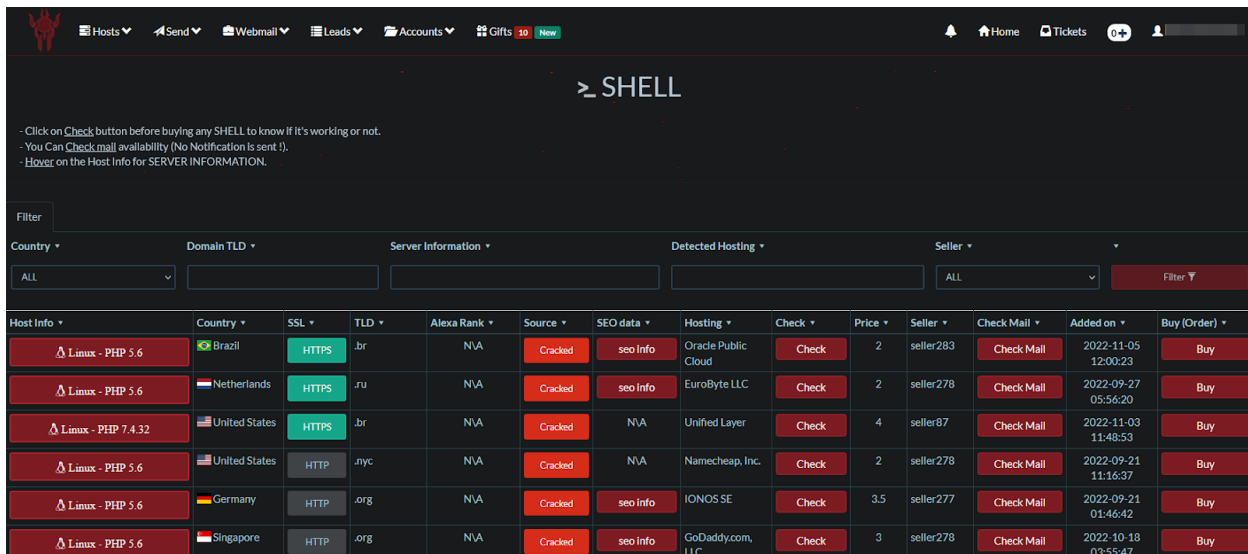
ID	Country	Type	Domain	Hosting	CMS	Ip Blacklist	Seo Info	Source	Technologies	Seller	Check	Price	Added on	Send Test	DA	PA	Buy
16753	United States	http	rjh*****es.ml	Unified Layer	N/A	Check Blacklist	SEOinfo	cracked	Techinfo	Seller6	Check	3.00	09/10/2022 11:31:26 am	Send test	1	1	Buy
16912	United States	http	jfinves*****up.com	Namecheap, Inc.	Joomla	Check Blacklist	SEOinfo	cracked	Techinfo	Seller323	Check	2.00	28/10/2022 05:44:58 pm	Send test	7	28	Buy
16745	United States	http	ttj*****er.ml	Unified Layer	N/A	Check Blacklist	SEOinfo	cracked	Techinfo	Seller6	Check	3.00	09/10/2022 11:29:49 am	Send test	1	1	Buy
16626	Australia	http	r243.syd1.hosti*****eLau	SYNERGY WHOLESALE PTY LTD	N/A	Check Blacklist	SEOinfo	cracked	Techinfo	Seller337	Check	5.00	06/10/2022 05:37:43 pm	Send test	9	21	Buy
16991	United States	http	pacificgro*****al.com	Cloudflare, Inc.	WordPress	Check Blacklist	SEOinfo	cracked	Techinfo	Seller323	Check	3.00	28/10/2022 06:23:05 pm	Send test	1	5	Buy
15793	United States	https	tukai*****ms.com	PDR	N/A	Check Blacklist	SEOinfo	cracked	Techinfo	Seller321	Check	4.00	26/04/2022 01:24:18 am	Send test	6	24	Buy

Pictured: The AK47 Marketplace's cPanel offerings

Webshell Access

The WSO shell in particular has become something of a de facto standard for maintaining persistent access on compromised sites, and provides file manager access and remote code execution capability. Unlike RDPs and cPanels, these are almost always “Cracked”. In many cases purchasing a “Webshell” simply provides the buyer the location of the purchased webshell, though some variants are also password protected.

Pricing for webshells appears to range from \$1-\$6 USD.



The screenshot shows the 'SHELL' section of the Hades Marketplace. At the top, there's a navigation bar with links like Hosts, Send, Webmail, Leads, Accounts, Gifts, and a 'New' badge. Below the navigation bar, the title 'SHELL' is displayed. A note advises users to click on 'Check' before buying and to check mail availability. Below the note, there's a filter section with dropdowns for Country, Domain TLD, Server Information, Detected Hosting, and Seller. The main content is a table listing various webshells for sale.

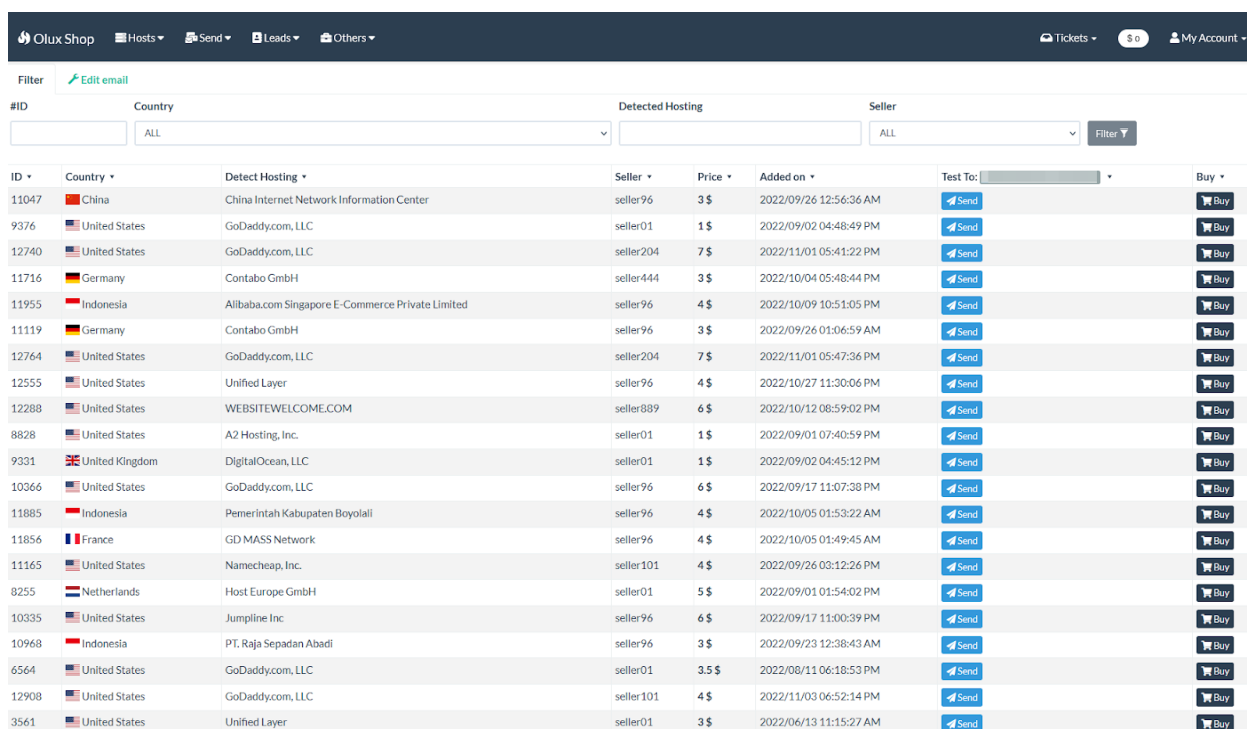
Host Info	Country	SSL	TLD	Alexa Rank	Source	SEO data	Hosting	Check	Price	Seller	Check Mail	Added on	Buy (Order)
Linux - PHP 5.6	Brazil	HTTPS	.br	N/A	Cracked	seo info	Oracle Public Cloud	Check	2	seller283	Check Mail	2022-11-05 12:00:23	Buy
Linux - PHP 5.6	Netherlands	HTTPS	.ru	N/A	Cracked	seo info	EuroByte LLC	Check	2	seller278	Check Mail	2022-09-27 05:56:20	Buy
Linux - PHP 7.4.32	United States	HTTPS	.br	N/A	Cracked	N/A	Unified Layer	Check	4	seller87	Check Mail	2022-11-03 11:48:53	Buy
Linux - PHP 5.6	United States	HTTP	.nyc	N/A	Cracked	N/A	Namecheap, Inc.	Check	2	seller278	Check Mail	2022-09-21 11:16:37	Buy
Linux - PHP 5.6	Germany	HTTP	.org	N/A	Cracked	seo info	IONOS SE	Check	3.5	seller277	Check Mail	2022-09-21 01:46:42	Buy
Linux - PHP 5.6	Singapore	HTTP	.org	N/A	Cracked	seo info	GoDaddy.com, LLC	Check	3	seller278	Check Mail	2022-10-18 03:55:47	Buy

Pictured: Webshells for sale on the Hades Marketplace

Leafmailers and SMTP Accounts

Leafmailers are PHP scripts that run on a webserver and are typically used to send spam or phishing messages and other mass mail. While the leafmailer script itself is legitimate its presence on a site is a very strong indicator of compromise. Pricing for Leafmailers was surprisingly variable, ranging from \$1 to \$55 USD, likely depending on the spam reputation of the compromised site. Leafmailers are typically password protected, since the test functionality frequently discloses the location of the script in the email headers.

“SMTP” access consists of credentials to SMTP email servers and are typically used to send spam or phishing messages and other mass mail. These typically range from \$5-\$10 USD.



ID	Country	Detect Hosting	Seller	Price	Added on	Test To	Buy
11047	China	China Internet Network Information Center	seller96	3 \$	2022/09/26 12:56:36 AM	Send	Buy
9376	United States	GoDaddy.com, LLC	seller01	1 \$	2022/09/02 04:48:49 PM	Send	Buy
12740	United States	GoDaddy.com, LLC	seller204	7 \$	2022/11/01 05:41:22 PM	Send	Buy
11716	Germany	Contabo GmbH	seller444	3 \$	2022/10/04 05:48:44 PM	Send	Buy
11955	Indonesia	Alibaba.com Singapore E-Commerce Private Limited	seller96	4 \$	2022/10/09 10:51:05 PM	Send	Buy
11119	Germany	Contabo GmbH	seller96	3 \$	2022/09/26 01:06:59 AM	Send	Buy
12764	United States	GoDaddy.com, LLC	seller204	7 \$	2022/11/01 05:47:36 PM	Send	Buy
12555	United States	Unified Layer	seller96	4 \$	2022/10/27 11:30:06 PM	Send	Buy
12288	United States	WEBSITEWELCOME.COM	seller889	6 \$	2022/10/12 08:59:02 PM	Send	Buy
8828	United States	A2 Hosting, Inc.	seller01	1 \$	2022/09/01 07:40:59 PM	Send	Buy
9331	United Kingdom	DigitalOcean, LLC	seller01	1 \$	2022/09/02 04:45:12 PM	Send	Buy
10366	United States	GoDaddy.com, LLC	seller96	6 \$	2022/09/17 11:07:38 PM	Send	Buy
11885	Indonesia	Pemerintah Kabupaten Boyolali	seller96	4 \$	2022/10/05 01:53:22 AM	Send	Buy
11856	France	GD MASS Network	seller96	4 \$	2022/10/05 01:49:45 AM	Send	Buy
11165	United States	Namecheap, Inc.	seller101	4 \$	2022/09/26 03:12:26 PM	Send	Buy
8255	Netherlands	Host Europe GmbH	seller01	5 \$	2022/09/01 01:54:02 PM	Send	Buy
10335	United States	Jumpline Inc	seller96	6 \$	2022/09/17 11:00:39 PM	Send	Buy
10968	Indonesia	PT. Raja Sepadan Abadi	seller96	3 \$	2022/09/23 12:38:43 AM	Send	Buy
6564	United States	GoDaddy.com, LLC	seller01	3.5 \$	2022/08/11 06:18:53 PM	Send	Buy
12908	United States	GoDaddy.com, LLC	seller101	4 \$	2022/11/03 06:52:14 PM	Send	Buy
3561	United States	Unified Layer	seller01	3 \$	2022/06/13 11:15:27 AM	Send	Buy

Pictured: Olux shop's Leafmailer offerings. The send verification functionality is visible in this image.

Webmail accounts

“Webmail accounts” are credentials to individual webmail accounts, and are typically intended to facilitate spear phishing, social engineering, and identity theft rather than mass mailing. Some shops broke webmail accounts out into a separate category while others categorized them under email sending or “premium” accounts, which also frequently included accounts to various online gaming and dating services.

In many cases shops will indicate the domain the account is associated with, as well as the email provider. Price varies wildly depending on provider and associated domain, typically between \$2 and \$50 USD, though accounts with additional identifiers or administrative roles might fetch \$125 or more.

Odin

Hosts • Send • Leads • Business • Accounts • Requests • Bulk Offers

🇺🇸 🇬🇧 🇩🇪 🇫🇷 🇮🇹 🇯🇵 🇰🇷 🇸🇪 🇸🇦 🇦🇪 🇩🇪 🇫🇷 🇮🇹 🇯🇵 🇰🇷 🇸🇪 🇸🇦 🇦🇪

🔍

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 2438 Webmail Available.

Start Data

Download Link

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
39867	United States	GoDaddy.com, LLC	org	Other	Tracked	SELLER	CHECK	10.00	20/10/2022 12:21:12 am	BUY
41477	United States	GoDaddy.com, LLC	net	Other	Tracked	SELLER	CHECK	10.00	24/10/2022 05:58:13 am	BUY
42835	United States	GoDaddy.com, LLC	net	Other	Tracked	SELLER	CHECK	8.00	26/10/2022 12:00:07 pm	BUY
41002	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	10.00	24/10/2022 05:01:26 am	BUY
41082	United States	GoDaddy.com, LLC	co	Other	Tracked	SELLER	CHECK	10.00	24/10/2022 05:03:29 am	BUY
35616	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	10.00	01/09/2022 11:55:04 am	BUY
35431	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	10.00	01/09/2022 11:39:49 am	BUY
41092	United States	GoDaddy.com, LLC	org	Other	Tracked	SELLER	CHECK	10.00	24/10/2022 05:03:38 am	BUY
42706	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	7.00	26/10/2022 01:07:45 am	BUY
43470	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	8.00	30/10/2022 09:18:30 pm	BUY
41943	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	10.00	24/10/2022 07:04:34 pm	BUY
42060	United States	GoDaddy.com, LLC	net	Other	Tracked	SELLER	CHECK	10.00	24/10/2022 07:09:25 pm	BUY
43626	United States	GoDaddy.com, LLC	com	Other	Tracked	SELLER	CHECK	10.00	31/10/2022 06:31:41 am	BUY

Pictured: GoDaddy Webmail accounts for sale on the Odin shop

Office 365 and GoDaddy webmail accounts are common, and we noticed email addresses at a number of educational and international government subdomains for sale.

Office365 Webmail

- Webmail is used for Social engineering hacked, its not used for mass send.
- By clicking in **Test Send** button an email will be sent from the Office365 Webmail to [redacted]
- There is **21021** Office365 Webmail Available

Top Sellers In This Section

- Seller ID : 30** (77 item)
- Seller ID : 1** (25 item)
- Seller ID : 11** (15 item)

Filters: ID: [input], Hosting: [input], Website: [input], Niche: All, Country: All, Seller: Select Seller, Source: All, Price Min: \$ Min, Price Max: \$ Max, Filter [icon]

[input] Update Testing E-mail

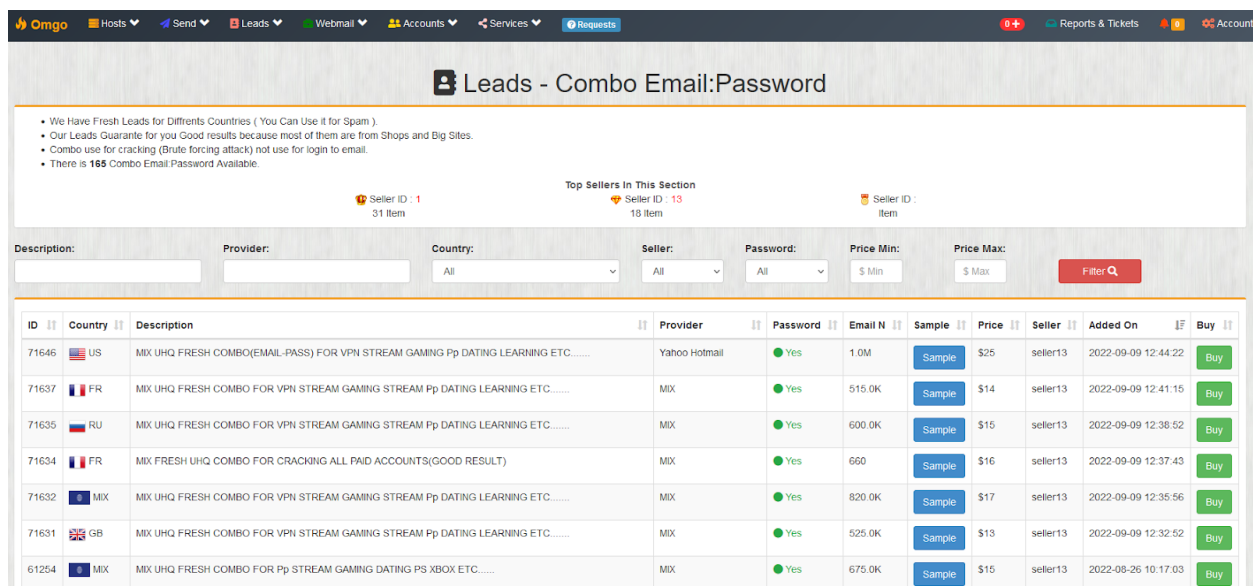
ID	Country	Source	Website	Hosting	Type	Niche	Seller	Price	Check	Added On	Buy
648	MX	Cracked	gov.sa	N/A	Office365 Webmail	Other	seller1	\$15	Test Send	2022-03-18 18:39:17	Buy
35701	MX	Cracked	gov.ph	N/A	Office365 Webmail	Other	seller1	\$10	Test Send	2022-07-16 09:06:05	Buy
84288	MX	Cracked	gov.ph	N/A	Office365 Webmail	Other	seller32	\$6	Test Send	2022-09-22 08:54:55	Buy
35775	MX	Cracked	gov.ph	N/A	Office365 Webmail	Other	seller1	\$10	Test Send	2022-07-16 11:11:04	Buy
87579	MX	Cracked	gov.ph	N/A	Office365 Webmail	Other	seller32	\$6	Test Send	2022-09-30 13:39:09	Buy
44387	MX	Cracked	gov.ph	N/A	Office365 Webmail	Other	seller1	\$10	Test Send	2022-07-26 01:38:48	Buy

Pictured: Office365 accounts for sale on the Omgo shop

Leads and Combo Lists

“Leads” are large lists of email addresses and typically are sold either as standalone email addresses or as “combo” lists. Standalone email lists are intended for spam, phishing, or even traditional marketing purposes, while “combo” lists consist of full sets of leaked credentials to various services. Combo lists are frequently used for the credential stuffing “brute force” attacks blocked by the Wordfence plugin, as attackers are fully aware that most users reuse their passwords and that one set of credentials can grant access to multiple accounts.

Email-only lists are relatively inexpensive and tend to range from \$7-\$20 USD, while “combo” lists tend to start at \$13 and up, with many larger lists in the \$50 price range.



The screenshot shows the Omgo shop interface for "Leads - Combo Email:Password". The page includes a navigation bar with various categories like Hosts, Send, Leads, Webmail, Accounts, Services, and Requests. Below the navigation bar, there's a section titled "Leads - Combo Email:Password" with a list of items for sale. The items are displayed in a table with columns for ID, Country, Description, Provider, Password, Email N, Sample, Price, Seller, Added On, and Buy. The table lists several items, including "MIX UHQ FRESH COMBO(EMAIL-PASS) FOR VPN STREAM GAMING Pp DATING LEARNING ETC....." and "MIX UHQ FRESH COMBO FOR VPN STREAM GAMING STREAM Pp DATING LEARNING ETC.....". Each item has a "Buy" button next to it.

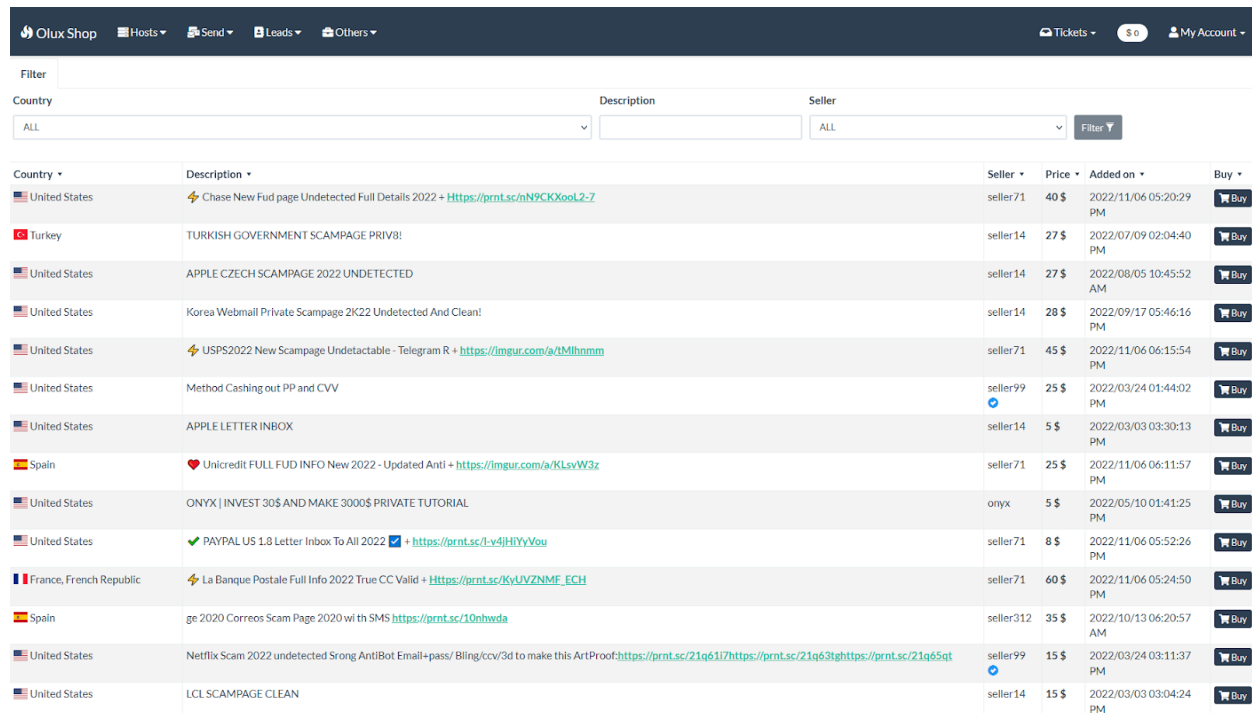
ID	Country	Description	Provider	Password	Email N	Sample	Price	Seller	Added On	Buy
71646	US	MIX UHQ FRESH COMBO(EMAIL-PASS) FOR VPN STREAM GAMING Pp DATING LEARNING ETC.....	Yahoo Hotmail	Yes	1.0M	Sample	\$25	seller13	2022-09-09 12:44:22	Buy
71637	FR	MIX UHQ FRESH COMBO FOR VPN STREAM GAMING STREAM Pp DATING LEARNING ETC.....	MIX	Yes	515.0K	Sample	\$14	seller13	2022-09-09 12:41:15	Buy
71635	RU	MIX UHQ FRESH COMBO FOR VPN STREAM GAMING STREAM Pp DATING LEARNING ETC.....	MIX	Yes	600.0K	Sample	\$15	seller13	2022-09-09 12:38:52	Buy
71634	FR	MIX FRESH UHQ COMBO FOR CRACKING ALL PAID ACCOUNTS(GOOD RESULT)	MIX	Yes	660	Sample	\$16	seller13	2022-09-09 12:37:43	Buy
71632	MIX	MIX UHQ FRESH COMBO FOR VPN STREAM GAMING STREAM Pp DATING LEARNING ETC.....	MIX	Yes	820.0K	Sample	\$17	seller13	2022-09-09 12:35:56	Buy
71631	GB	MIX UHQ FRESH COMBO FOR VPN STREAM GAMING STREAM Pp DATING LEARNING ETC.....	MIX	Yes	525.0K	Sample	\$13	seller13	2022-09-09 12:32:52	Buy
61254	MIX	MIX UHQ FRESH COMBO FOR Pp STREAM GAMING DATING PS XBOX ETC.....	MIX	Yes	675.0K	Sample	\$15	seller13	2022-09-26 10:17:03	Buy

Pictured: Combo lists for sale on the Omgo shop

Scripts and Scam Pages

Most sites also allow sellers to offer exploitation scripts, post-exploitation “checker” and “config” scripts, and “scam pages” (phishing toolkits and email templates) for sale.

The scam page offerings typically include screenshots to show how closely they match up-to-date versions of the service they are imitating and tend to range from \$25-\$100.



The screenshot shows the Olux Shop marketplace interface. At the top, there's a navigation bar with links like 'Olux Shop', 'Hosts', 'Send', 'Leads', 'Others', 'Tickets', a balance of '\$0', and 'My Account'. Below this is a filter section with dropdowns for 'Country' (set to 'ALL'), 'Description', and 'Seller' (set to 'ALL'), along with a 'Filter' button. The main content is a table listing various scam page scripts for sale.

Country	Description	Seller	Price	Added on	Buy
United States	Chase New Fud page Undetected Full Details 2022 + https://prnt.sc/nN9CKXool2-7	seller71	40 \$	2022/11/06 05:20:29 PM	Buy
Turkey	TURKISH GOVERNMENT SCAMPAGE PRIV8!	seller14	27 \$	2022/07/09 02:04:40 PM	Buy
United States	APPLE CZECH SCAMPAGE 2022 UNDETECTED	seller14	27 \$	2022/08/05 10:45:52 AM	Buy
United States	Korea Webmail Private Scampage 2K22 Undetected And Clean!	seller14	28 \$	2022/09/17 05:46:16 PM	Buy
United States	USPS2022 New Scampage Undetectable - Telegram R + https://imgur.com/a/tMlhnmm	seller71	45 \$	2022/11/06 06:15:54 PM	Buy
United States	Method Cashing out PP and CVV	seller99	25 \$	2022/03/24 01:44:02 PM	Buy
United States	APPLE LETTER INBOX	seller14	5 \$	2022/03/03 03:30:13 PM	Buy
Spain	Unicredit FULL FUD INFO New 2022 - Updated Anti + https://imgur.com/a/KLsvW3z	seller71	25 \$	2022/11/06 06:11:57 PM	Buy
United States	ONYX INVEST 30\$ AND MAKE 3000\$ PRIVATE TUTORIAL	onyx	5 \$	2022/05/10 01:41:25 PM	Buy
United States	PAYPAL US 1.8 Letter Inbox To All 2022 + https://prnt.sc/l-v4jHfYV9u	seller71	8 \$	2022/11/06 05:52:26 PM	Buy
France, French Republic	La Banque Postale Full Info 2022 True CC Valid + https://prnt.sc/KyLJVZNMf_ECH	seller71	60 \$	2022/11/06 05:24:50 PM	Buy
Spain	ge 2020 Correos Scam Page 2020 w/ th SMS https://prnt.sc/10nhwda	seller312	35 \$	2022/10/13 06:20:57 AM	Buy
United States	Netflix Scam 2022 undetected Strong AntiBot Email+pass/ Billing/ccv/3d to make this ArtProof: https://prnt.sc/21q61i7 https://prnt.sc/21q63tgh https://prnt.sc/21q65qit	seller99	15 \$	2022/03/24 03:11:37 PM	Buy
United States	LCL SCAMPAGE CLEAN	seller14	15 \$	2022/03/03 03:04:24 PM	Buy

Pictured: the Olux Marketplace Scripts offerings.

The image shows a web browser window with the address bar displaying `/wp-admin/setup-config.php?step=1`. The page features the WordPress logo at the top center. Below the logo, a white box contains the following text and form fields:

Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	<input type="text" value="wordpress"/>	The name of the database you want to use with WordPress.
Username	<input type="text" value="username"/>	Your database username.
Password	<input type="text" value="password"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if localhost doesn't work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

At the bottom of the form is a blue "Submit" button.

Pictured: A fake WordPress installation “scampage” designed to harvest database credentials by replacing the legitimate setup-config.php file.

V. Takeaways

Customer Base

The vast majority of these products and services are geared towards relatively unskilled actors taking advantage of known weaknesses, especially human error. That is, the individuals using these services and purchasing hacked accounts are frequently not writing exploits themselves and are relying primarily on mistakes such as credential reuse and victims falling for phishing scams.

Additionally, most of the goods and services for sale on these sites are instrumental rather than terminal - they're being sold to attackers hoping to use them as tools to turn a profit with extra steps. The vendors on these platforms are, effectively, selling stolen pickaxes during a gold rush. Individual hacked websites and even RDP servers are generally not worth very much, so most attackers will not expend extraordinary effort to gain or maintain access to a given service beyond the functionality provided by the tools they use. This is also why "hacking back" against an attacker is a futile tactic.

The actual techniques vary: some shop customers might use RDPs to perform credential stuffing or web application exploits in the hopes of taking over sites for resale on the very same marketplaces. Others might be engaging in low-effort, low-reward enterprises such as SEO and email spam. The shops do have offerings, such as combolists and individual webmail accounts, that can be useful to attackers taking part in riskier businesses, such as social engineering, carding, and identity theft, but with the exception of Olux shop, do not appear to sell credit cards or other information that might make them a priority target for law enforcement.

Highly skilled attackers do exist and almost certainly purchase products from shops to aid in their goals, but there are far more profitable ways for a skilled attacker to monetize their capabilities than selling access to commodity hosting and email accounts, such as ransomware or "priv8"(non-public, frequently zero-day) exploits.

Preventative Measures

In almost all cases, following security best practices such as using strong unique passwords and 2-factor authentication for every online account, including cPanel accounts, using a Web Application Firewall that blocks against known exploits, ensuring all software remains up to date, and being wary of social engineering attempts is enough to prevent a website from ending up on one of these marketplaces.

Appendix

Shop domains

Olux

Olux[.]cz

Olux[.]so

Olux[.]ws

Oxux/Knockoff Olux Shops (not exhaustive)

Oluxs[.]shop

Olux[.]store

Oxux[.]to

Hades

Hadesmarket[.]to

Hadeshop[.]in

Hadeshop[.]cc

Hadeshop[.]top

Omgo

Omgo[.]io

Omgo[.]pro

Omgo[.]pw

Odin

Odinshop[.]io

Odin[.]pw

Odinshop[.]se

Odin[.]pm

AK47

AK47[.]to