



Brief | New Underground Market Comes Online Just in Time for the Holidays

B-2023-12-07b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: PII, Phishing, Fraud, Threat Actor Activity

December 7, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were *identified prior to November 27, 2023*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | New Underground Market Comes Online Just in Time for the Holidays

Executive Summary

Threat actors have opened a new underground market known as OLVX Marketplace (olvx[.]cc) that is gaining notoriety just in time for the holidays. This new marketplace claims to sell all the tools necessary to commit online fraud, manipulate the very savviest of online shoppers, and make this time of year much less merry and bright. OLVX follows a trend ZeroFox Intelligence has observed relating to multiple underground marketplaces now operating on the clear web, whereas in the past, most would only operate on the deep or dark web (DDW).

On or about July 1, 2023, OLVX came online with legitimate and well-respected threat actors advertising tools such as phishing kits, remote desktop connections, cPanel credentials/access, webshells, SPAM sending systems, stolen data, webmail access, and leads/combo lists. Underground marketplaces, even those hosted on the clear web, sell a myriad of products and services to assist cybercriminals in their day-to-day operations. While some marketplaces specialize in illegal/illicit products such as drugs, counterfeit products, and hacked gift cards, OLVX focuses less on end-user products and more on tools and services to aid cybercriminals in their activities to obtain data, many

of which can be deployed by threat actors looking to capitalize on the busy 2023 holiday retail season.

Discovery

In the fall of 2023, ZeroFox researchers noted an increase in activity on the OLVX marketplace, including items sold and purchasers flocking to the newly created store. Research of the platform and its code indicates OLVX stems from a fork based on leakage of code from a different store, OLUX, in early 2020/late 2021.¹ While the code from the original OLUX marketplace is dated by today's standards, multiple stores have appeared post-leak utilizing improved variants of the initial store code. OLVX utilizes Cloudflare to masquerade its actual web hosting location and enhance accessibility.

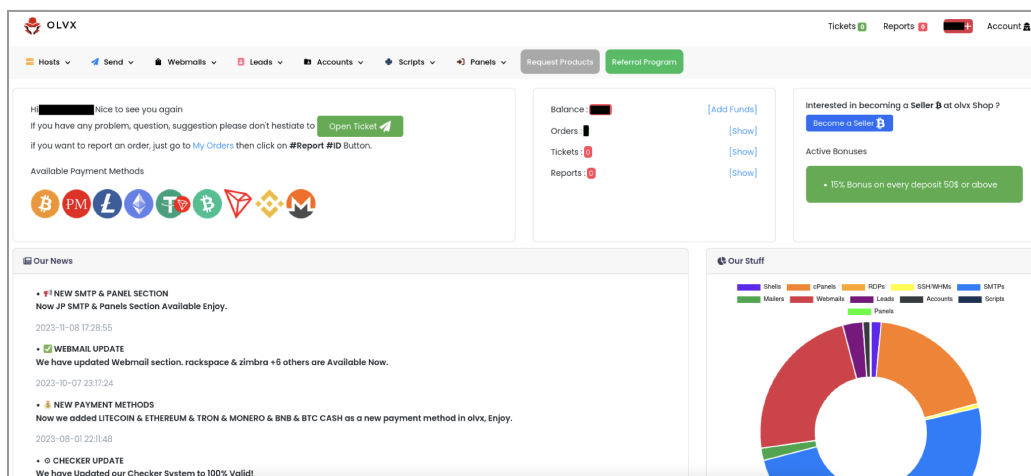


Figure 1. OLVX homepage
Source: ZeroFox Intelligence

Rather than being hosted on the darkweb, the OLVX marketplace is on the open web. Based on an investigation of website coding, the administrators of the OLVX marketplace have implemented multiple methodologies of search engine optimization (SEO) to gain new customers.

¹ [hXXps://lukeleal\[.\]com/research/posts/what-is-anonymousfox/](https://lukeleal[.]com/research/posts/what-is-anonymousfox/)

```
<title>OLVX | Spam Tools | SMTP | SHELL | MAILER | cPanel | FTP | Inbox Sender | Hack Tools | Tools Spam | RDP | SSH | Webmail | Php Mailers | Smtps | Leads | Accounts | Spam Tool | Spam Tools | Fresh SMTP | Fresh Shell | Fresh Mailer | Fresh Sender | Fresh RDP | Fresh SSH | Fresh Webmail | Cracked Webmail | Cracked SSH | Cracked RDP | Scampage 2022 | Fresh Scampages | Fresh Spam Tools | Fresh Hack Tools | Cheap Spam Tools | Spam Paypal Tools | Buy Tools with Crypto | Buy Spam Tools With Crypto | Shell Https | Cpanel Https | Mailer Inbox | Mailer Fresh Inbox | SMTP Inbox | SMTP Fresh Inbox | Cheap SMTP Sender | Shell Fresh Https | Cpanel Fresh Https | RDP Fresh | Leads Fresh 2022 | Fresh Webmail 2022 | Webmail Cheap | Webmail Fresh and Cheap | Leads Fresh For Spam | Combolist fresh | Combolist for Crack | Valid shod | spammer shop | Fresh Cpanel , Fresh Shell, Hacking RDP , Hacking shop , Buy Spamming Tools | Spammer Tools | Inbox Mailer | Buy Tools Spam | Spamming Tools | Rdp Shop | Site To Buy Spamming Tools | Buy Spamm Equipments | Buy Carding Accounts | olux | olux.io | olux shop | olux.to | oluxshop | odin.to | spamtoolz | spam tools shop 2021 | spam tools shop 2022 | zombi bot | heart sender | buyfreshrdp | site to buy smtp | buy hacked rdp | buy hacked webmail | buy hacked account | fresh spam | buy rdp for spamming | buy smtp for spamming | cpanel spam | best site to buy spamming tools | spam mailer | smtp spam | fresh rdp | cpanel for spamming | best cpanel for spamming | Orvx.pw </title>
```

Figure 2. OLVX homepage SEO

Source: ZeroFox Intelligence

This type of SEO and other methodologies to advertise the marketplace via various forums, Telegram, and word of mouth has gained OLVX additional customers in recent months.

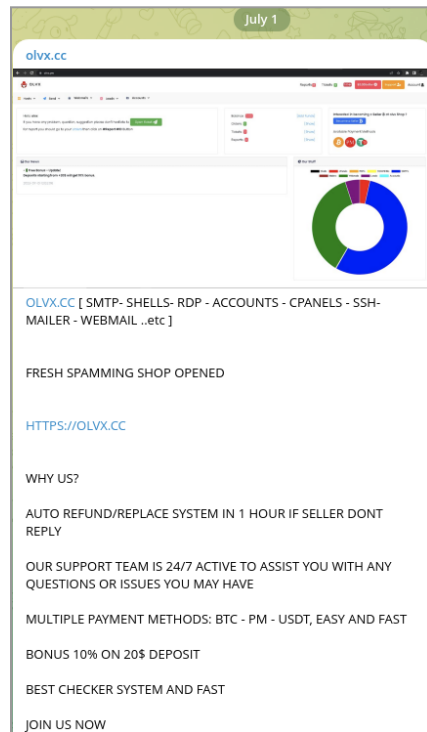


Figure 3. OLVX Telegram group welcome message

Source: ZeroFox Intelligence

Payments and Support

As with many marketplaces, OLVX has implemented numerous tactics to ensure customer service is a priority while serving its illicit customers. OLVX operates a general Telegram channel promoting its new features and the ability to direct-message

operators with any problems. While there are many choices in the illicit marketplace sector, marketplaces that focus on maintaining their customer relationships tend to have a stronger reputation and maintain greater profits.

While the OLVX marketplace offers thousands of individual products across numerous categories, its site administrators maintain relationships with various cybercriminals who create custom toolkits and can obtain specialized files, thereby furthering OLVX’s ability to maintain and attract customers to the platform.

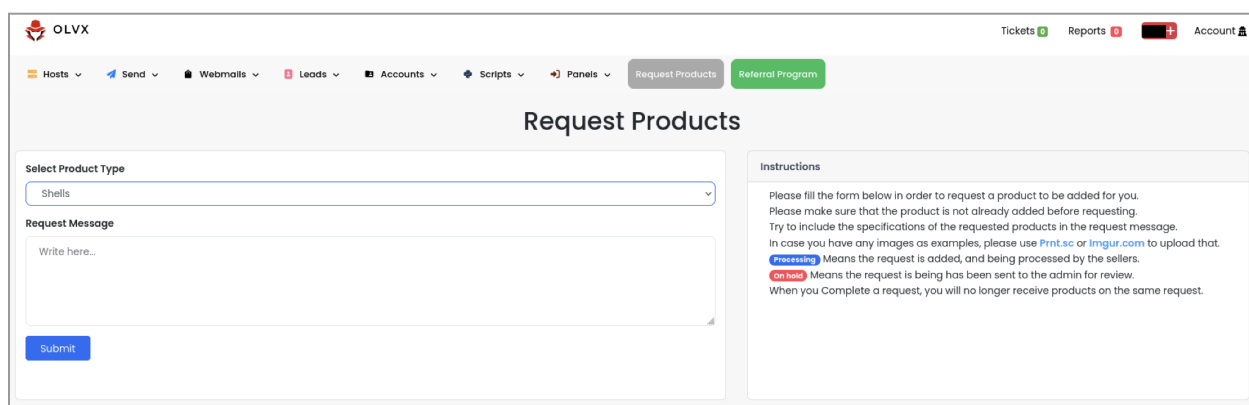


Figure 4. OLVX custom request page
Source: ZeroFox Intelligence

While numerous underground marketplaces offer an escrow service to enhance the privacy and security of transactions, OLVX has opted to offer a direct payment service via cryptocurrency instead.



Figure 5. OLVX payment methods
Source: ZeroFox Intelligence

OLVX has implemented a common method of payment via cryptocurrency, but—rather than allow customers to pay directly for each transaction separately—the marketplace requires customers to transfer funds to the platform and maintain a balance. This is

often seen in other illicit marketplaces, as it increases sales/profitability. When a customer no longer has sufficient funds to process a transaction, they are instructed to “top-off” their account via a time-limited anonymized crypto address.

Items Sold on OLVX Marketplace

Shells

When a malicious actor compromises a legitimate website, it is part of general tactics, techniques, and procedures (TTPs) to establish persistence on the web server. One mechanism of establishing persistence is the uploading of a webshell, which provides the malicious actor with a backdoor to maintain access to website content. While some webshells allow the user to upload the site to one of their choosing, OLVX provides access to existing *hacked* shells via various hosting providers worldwide. Price points are very low, with some under USD 5 among the hundreds of shells listed for sale. The marketplace has the functionality to verify authenticity and connection to shells prior to the customer making the purchase.

ID	Country	SSL	TLD	DA	PA	Server OS	Hosting	Alexa Rank	SEO Info	Price	Seller	Added on	Check Send	Check ZIP	Check	Buy
908	US	HTTPS	.com	0	0	Linux - PHP 7.4.33	Jumpline INC	N/A	N/A	3.00	seller87	2023-11-17 11:36:46	Check Send	Check ZIP	Check	Buy
336	US	HTTP	.com.br	0	0	Linux - PHP 7.3.33	Network Solutions, LLC	N/A	N/A	5.00	seller28	2023-10-05 20:51:19	Check Send	Check ZIP	Check	Buy
1052	FR	HTTP	.com	0	0	Linux - PHP 7.2.34	OVH SAS	N/A	N/A	3.00	seller87	2023-11-19 12:35:14	Check Send	Check ZIP	Check	Buy
434	US	HTTPS	.qa	0	0	Linux - PHP 7.3.33	Unified Layer	N/A	N/A	2.00	seller87	2023-10-16 09:36:27	Check Send	Check ZIP	Check	Buy
611	US	HTTPS	.com	0	0	Linux - PHP 7.4.33	Godaddy.com, LLC	N/A	N/A	3.00	seller87	2023-10-25 07:08:05	Check Send	Check ZIP	Check	Buy

Figure 6. OLVX Shells for sale
Source: ZeroFox Intelligence

cPanels

As of November 2023, OLVX has over 6,000 cPanels listed for sale. The marketplace does not sell cPanel interfaces directly; rather, it provides access to an active cPanel (presumably hacked), allowing the malicious actor to manipulate it to their liking. Upon investigation of products sold within the marketplace, ZeroFox noted that sellers compromise a website and sell access to it individually (via shell, cPanel, etc.) rather than as a bulk purchase, allowing them greater profitability from a single compromised website. To enhance customer service, the OLVX buyers have the ability to view information such as country, top-level domain, hosting provider, and rankings—in addition to verification that the cPanel access is still active—prior to purchase. Pricing is relatively low (generally under \$10 USD).

The screenshot shows the OLVX cPanels marketplace interface. At the top, there is a search bar with filters for Hosting, TLD, SSL, Country, Seller, Price Min, and Price Max. Below the search bar, there is a table of listings. Each listing includes an ID, Country, SSL status, TLD, DA, PA, Hosting provider, Alexa Rank, SEO Info, Price, Seller, Added on date, and buttons for Check Send/Upload, Check, and Buy.

ID	Country	SSL	TLD	DA	PA	Hosting	Alexa Rank	SEO Info	Price	Seller	Added on	Check Send/Upload	Check	Buy
1668	US	HTTPS	.club	0	0	Network Solutions, LLC	N/A	N/A	3.00	seller390	2023-09-05 12:17:56	Check Send	Check	Buy
3333	US	HTTPS	.com	0	0	Unified Layer	N/A	N/A	10.00	seller27	2023-10-03 19:58:07	Check Send	Check	Buy
5206	MW	HTTPS	.org	0	0	Inq. Digital Limited	N/A	N/A	6.00	seller63	2023-11-12 12:02:24	Check Send	Check	Buy
3370	NL	HTTPS	.net	0	0	Host Europe GmbH	N/A	N/A	6.00	seller354	2023-10-12 11:08:37	Check Send	Check	Buy
2833	US	HTTPS	.net	0	0	Network Solutions, LLC	N/A	N/A	1.00	seller555	2023-09-24 16:56:54	Check Send	Check	Buy
211	VN	HTTPS	.com	0	0	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	N/A	N/A	3.00	seller4	2023-07-02 16:18:34	Check Send	Check	Buy

Figure 7. OLVX cPanels for sale

Source: ZeroFox Intelligence

Remote Desktop Protocol (RDP) and Secure Shell (SSH) Access

Anonymity during attacks is paramount and a common threat actor TTP. By purchasing RDP or SSH access from potentially compromised legitimate servers, threat actors can further mask their attack source by performing exploits from a server belonging to someone else. RDP and SSH accesses are commonly sold on multiple marketplaces.

OLVX provides access to numerous potentially active servers with compromised RDP credentials. Pricing is under \$10 USD; to further enhance sales, OLVX provides the customer with the ability to verify if credentials are still valid prior to purchase. Pricing is set based on access level and system specifications.

The screenshot shows the OLVX marketplace interface for RDP access. It includes a navigation bar with 'Hosts', 'Send', 'Webmails', 'Leads', 'Accounts', 'Scripts', and 'Panels'. A search bar is present with filters for 'Request Products' and 'Referral Program'. The main section is titled 'RDP' and contains a table of listings. The table has columns for ID, Country, Hosting, Windows, RAM, Access, Username, IP, Price, Seller, Added on, Check, and Buy. The listings are for various countries including Canada, USA, and Australia, with prices ranging from \$6.00 to \$10.00.

ID	Country	Hosting	Windows	RAM	Access	Username	IP	Price	Seller	Added on	Check	Buy
30	CA - Quebec - Montreal	com, Inc.	Windows 2022	4 GB	Admin	Ad*****	3.96.**	6.00	seller853	2023-9-09 15:54:44	Check	Buy
31	CA - Quebec - Montreal	com, Inc.	Windows 2022	4 GB	Admin	Ad*****	99.79.**	6.00	seller853	2023-9-09 16:02:21	Check	Buy
26	US - Ohio - Columbus	com, Inc.	Windows 2022	4 GB	Admin	Ad*****	3.143.**	6.00	seller853	2023-9-09 11:53:46	Check	Buy
29	AU - New South Wales - Sydney	com, Inc.	Windows 2022	8 GB	Admin	Ad*****	3.24.**	9.00	seller853	2023-9-09 15:08:22	Check	Buy
27	US - Virginia - Ashburn	com, Inc.	Windows 2022	8 GB	Admin	Ad*****	18.232.**	10.00	seller853	2023-9-09 12:36:39	Check	Buy
25	US - Ohio - Columbus	com, Inc.	Windows 2022	4 GB	Admin	Ad*****	3.137.**	6.00	seller853	2023-9-09 11:43:20	Check	Buy

Figure 8. RDP access for sale

Source: ZeroFox Intelligence

SMTP Accounts and Mailers

Depending on the campaign goals, it is commonplace for threat actors to send attacks, such as phishing emails to as many victims as possible. As threat actors may get flagged using services such as Gmail or Outlook, they will utilize pre-existing hacked servers to “piggyback” on legitimate SMTP connections to run email campaigns. Mailers (scripts) are also sold to enable the threat actor to run said email campaigns directly from the server. Based on hosting provider and country, mailers and compromised SMTP accounts were less than \$10 USD on the OLVX marketplace, which contains over 1,000 listings.

The screenshot shows the OLVX marketplace interface for the SMTP Section. It includes a navigation bar with 'Filter' and 'Test Email'. The main section is titled 'SMTP Section' and contains a table of listings. The table has columns for ID, Country, Hosting, Webmail, Type, Limit, Price, Seller, Added on, and Check. The listings are for various countries including USA and France, with prices ranging from \$10.00.

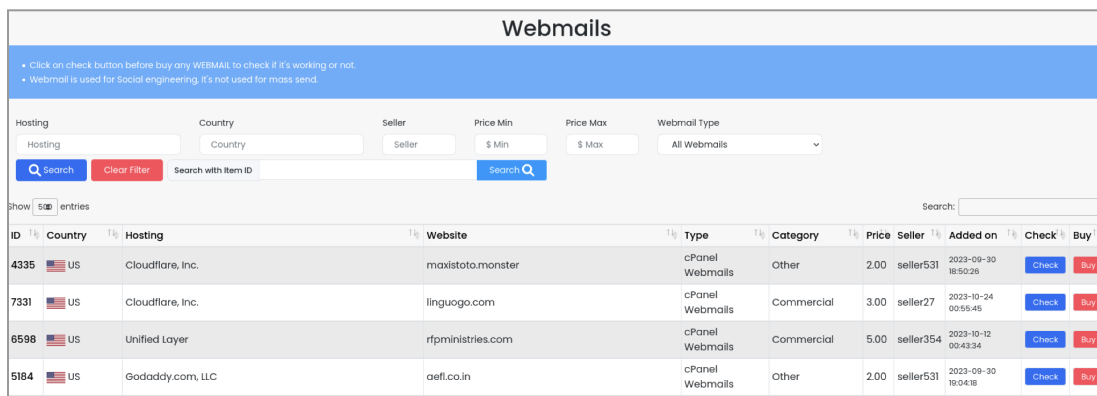
ID	Country	Hosting	Webmail	Type	Limit	Price	Seller	Added on	Check
14893	US	Godaddy.com, LLC	No	Normal	N/A	10.00	seller390	2023-09-21 14:42:24	Check
14890	US	Godaddy.com, LLC	No	Normal	N/A	10.00	seller390	2023-09-21 14:40:59	Check
18533	US	Godaddy.com, LLC	Yes	Normal	N/A	10.00	seller28	2023-10-11 18:13:23	Check
14901	FR	Host Europe GmbH	No	Normal	N/A	10.00	seller390	2023-09-21 14:47:10	Check
14857	US	Input Output Flood LLC	No	Normal	N/A	10.00	seller390	2023-09-21 14:23:01	Check

Figure 9. SMTP access for sale

Source: ZeroFox Intelligence

Webmail Accounts

While many marketplaces, in addition to OLVX, sell combo lists containing compromised email credentials, OLVX provides a more specific service targeting threat actors seeking to perform social engineering attacks. When purchasing a large list/database of thousands of compromised credentials, the threat actor may not have confirmation of the domains captured within the dataset. OLVX offers over 8,000 compromised credentials and provides the threat actor with the ability to search for a specific domain they may need for a social engineering campaign. Based on the nature of selling single-access credentials per transaction, this significantly lowers the cost to just a few dollars.



The screenshot shows the 'Webmails' marketplace interface. At the top, there are instructions: 'Click on check button before buy any WEBMAIL to check if it's working or not.' and 'Webmail is used for Social engineering, it's not used for mass send.' Below this is a search and filter section with fields for 'Hosting', 'Country', 'Seller', 'Price Min', 'Price Max', and 'Webmail Type'. A search bar and a 'Search with Item ID' field are also present. The main content is a table with columns: ID, Country, Hosting, Website, Type, Category, Price, Seller, Added on, Check, and Buy. The table lists four items:

ID	Country	Hosting	Website	Type	Category	Price	Seller	Added on	Check	Buy
4335	US	Cloudflare, Inc.	maxistoto.monster	cPanel Webmails	Other	2.00	seller531	2023-09-30 18:50:28	Check	Buy
7331	US	Cloudflare, Inc.	linguogo.com	cPanel Webmails	Commercial	3.00	seller27	2023-10-24 00:55:45	Check	Buy
6598	US	Unified Layer	rfpministries.com	cPanel Webmails	Commercial	5.00	seller354	2023-10-12 00:43:34	Check	Buy
5184	US	Godaddy.com, LLC	aefl.co.in	cPanel Webmails	Other	2.00	seller531	2023-09-30 19:04:18	Check	Buy

Figure 10. Webmail access for sale

Source: ZeroFox Intelligence

Leads & Combo Lists

As threat actors build out their attack campaign to target as many victims as possible, one vector of gaining source information is via “leads.” These lead files contain a multitude of email addresses and are often sold in bulk, targeting a specific provider. Combo lists contain a plethora of compromised credentials, oftentimes numbering in the millions.² Additionally, ZeroFox observed an 18 percent increase in accounts containing retail/finance compromised credentials, which prior intelligence has revealed is often used by threat actors during the holidays to scam online shoppers. These lists are often used for automated brute force-type attacks. Items available on the OLVX marketplace range in price from \$1-200 USD, depending on database size, target, and country.

² [https://www.zerofox\[.\]com/advisories/20323/\(Breach Disclosure: Combo_2G Combolist\)](https://www.zerofox[.]com/advisories/20323/(Breach%20Disclosure:%20Combo_2G%20Combolist))

ID	Country	Type	Description	Number	Provider	Proof	Price	Seller	Added on	Buy
1059	US	Combo Email:Pass	1.20m Combo List EDU Fresh	1.20m	mix	Show Proof	19.00	seller360	2023-09-18 12:22:04	Buy
266	US	Combo Email:Pass	1.3M PRIVATE UHQ USA CORP BASE COMBOLIST GUARANTEE HITS FRESH	1.3m	mix	Show Proof	20.00	seller360	2023-09-31 11:37:09	Buy
1097	US	Combo Email:Pass	1.4M HQ COMBOLIST CASHOUT TARGET PAYPAL BINANCE COINBASE	1.4m	mix	Show Proof	20.00	seller360	2023-10-01 13:17:52	Buy
1072	US	Combo Email:Pass	1.5M combo Gaming Mixed Domain	1.5m	mix	Show Proof	19.00	seller360	2023-09-19 13:09:29	Buy
1110	US	Combo Email:Pass	1.80M COMBOLIST EDU AZURE AWS G-DRIVE OFFICE 365 & OTHER SITES NEW	1.80	mix	Show Proof	24.00	seller360	2023-10-19 13:22:56	Buy
268	US	Combo Email:Pass	1.90M HQ Private Combolist Shopping Netflix Uplay Steam VPN Spotify	1.90m	mix	Show Proof	24.00	seller360	2023-09-31 11:39:52	Buy

Figure 11. Combo lists for sale
Source: ZeroFox Intelligence

Accounts

In addition to selling combo lists with compromised credentials, OLVX offers a specialized sales area focusing on credentials from specific domains/services. With over 400 active targets for sale ranging from general user accounts to administrator access, there are numerous high-level accounts for threat actors to utilize. Upon investigating items for sale, ZeroFox noted it was commonplace for adult websites to be present, providing a possible social engineering angle for vulnerable individuals. Pricing varied depending on account access and often provided personally identifiable information (PII) in addition to general credentials. To further incentivize purchasing, proof is provided outlining the compromised credential data.

ID	Country	Type	Website	Description	Proof	Price	Seller	Added on	Buy
261	US	Dating	edate.com	eDate (UnPaid) US Premium: 0, Gender: MALE, Age: 33, Country: United States, Location: Holmen, WI, Zip Code: 54836	Show Proof	5.00	seller4	2023-09-26 12:19:49	Buy
308	US	Dating	edate.com	eDate (UnPaid) US Premium: 0, Gender: MALE, Age: 55, Country: United States, Location: Butler, NJ, Zip Code: 07405	Show Proof	5.00	seller4	2023-09-26 13:04:39	Buy
79	US	Dating	OurTime (Paid)	Male / DOB: 8/3/1987 / Age: 50 / Des Plaines, IL / Paid Account / 60016	Show Proof	15.00	seller62	2023-07-03 17:58:48	Buy
367	MIXED	Social Media	Onlyfans.com	Onlyfan Account + CC Use Clean IP + Clean Browser Warranty only good if: incorrect login No cc	Show Proof	1.00	seller714	2023-10-21 05:15:11	Buy

Figure 12. Accounts for sale
Source: ZeroFox Intelligence

Phish Kits (Scampages)

As phishing continues to be one of the most profitable methods cybercriminals use to compromise victims,³ marketplaces such as OLVX often sell pre-developed phish kits. While marketplaces and the DDW economy will refer to phish kits as Scampages, security-minded researchers are aware this naming convention is only used to minimize keyword searches for legal reasons. Phish kits are sold in ZIP format and often contain secondary applications incorporating anti-cloaking technologies, two-factor authentication (2FA) bypass capabilities, and, at times, the ability to instantly send compromised credentials to a Telegram bot. Over the past two months, OLVX listings of phish kits targeting the retail and finance sector have grown by more than 25 percent, indicating the preparation of a multitude of campaigns being ramped up for the holiday season. Based on an investigation of additional available items, ZeroFox Intelligence observed that more feature-rich kits (2FA bypass, anti-cloaking, etc.) were priced as high as \$150 USD for a single page, while general pages were priced below \$20 USD. To further incentivize sales, proof via screenshot is provided to showcase the quality of the phishing landing page. Available OLVX phish kits for sale target retail, finance, and shipping, in addition to a myriad of other sectors.

ID	Name	Type	Description	Language	Proof	Price	Seller	Buy	Added on
269	CITIZEN BANK V2 Latest PRIV8 SCAMPAGE	Scampages	CITIZEN BANK V2 Latest PRIV8 SCAMPAGE 100% Clean LATEST ANTIBOTS UNDETECTED GOOD DESIGN PREMIUM SCAMPAGE PROOF https://prnt.sc/HC_gmArq5HrR	PHP	Show Proof	19.00	seller616	Buy	2023-10-11 22:34:35
29	Chase Bank	Scampages	Chase Bank Double Card Info Only + Telegram Feature FUD Page 2023	N/A	Show Proof	30.00	seller4	Buy	2023-08-29 14:27:51
271	CITIZEN BANK V4 Latest PRIV8 SCAMPAGE	Scampages	CITIZEN BANK V4 Latest PRIV8 SCAMPAGE 100% Clean LATEST ANTIBOTS UNDETECTED GOOD DESIGN PREMIUM SCAMPAGE PROOF https://prnt.sc/yk-yL5Lo-sl6	PHP	Show Proof	19.00	seller616	Buy	2023-10-11 22:38:42
135	Truist bank	Scampages	New Truist Bank with strong antibot ✓	PHP	Show Proof	50.00	seller431	Buy	2023-09-07 07:24:47
179	KEYBANK PREMIUM SCAMPAGE ✓	Scampages	✓KEYBANK 100% UNDETECTED ScamPage Clean Undetected Strong antibot Premium Scampage ✓	PHP	Show Proof	26.00	seller616	Buy	2023-10-03 14:17:09

Figure 13. Phish kits for sale

Source: ZeroFox Intelligence

Hosting

OLVX is currently utilizing Cloudflare to masquerade its actual hosting location and Simple Carrier LLC (known to host questionable content) to advertise its distributed denial of service (DDoS) protection services.

³ <https://securityintelligence.com/articles/phishing-attack-profitable-stop/>

Conclusion

Marketplaces such as OLVX continue to be popular sources from which cybercriminals purchase the tools they need to conduct targeting campaigns. As the November and December holiday shopping season is the busiest for retailers and consumers, the OLVX marketplace has, accordingly, also been ramping up its supply of items available to cybercriminals. While consumers shop online patronizing legitimate businesses, cybercriminals are busy on OLVX purchasing the supplies they need to target the innocent during the “most wonderful time of the year.”

Recommendations

- Remain alert when shopping online around the holiday season; only make purchases from known, trusted retailers, and avoid clicking any shopping links on social media pages or within unexpected emails.
- Implement secure password policies, with phishing- resistant MFA, complex passwords, and unique credentials. Regularly change credentials and avoid repetition of passwords across various accounts.
- Employ a dark web monitoring strategy, such as having ZeroFox continually monitor for leaked information.

| Appendix A: Indicators of Compromise (IOCs)

IOCs	Description
olvx[.]cc	Primary domain
olvx[.]pw	Alternate domain/SSL certificate
185.196.8[.]146	Hosting IP
AS42624	Hosting ASN

Appendix B: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix C: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%