



| Flash |

Mass Access Sale to Retail eCommerce System

F-2024-01-17b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep Dark Web & Criminal Underground

January 17, 2024

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 9:00 AM (EST) on January 17, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Mass Access Sale to Retail eCommerce System

> Key Findings

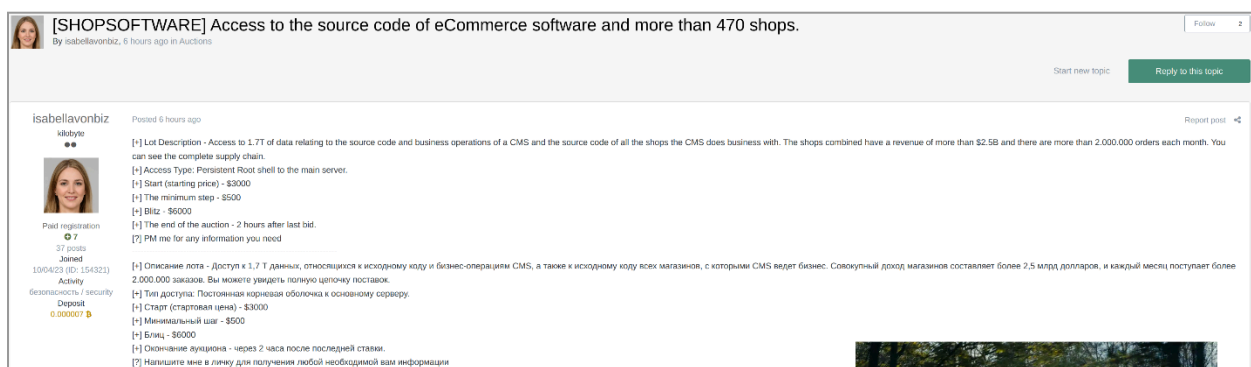
- On January 15, 2024, well-regarded threat actor “isabellavonbiz” announced the sale of the source code, business operations data, and documentation of an unspecified eCommerce Content Management System (CMS) services vendor; as of this writing, the name of the CMS has not been disclosed.
- The entire package was instantly purchased by a highly competent and popular threat actor, with additional intelligence indicating they are buying and potentially hoarding access to as many online shops as possible; this particular package or a variant thereof is no longer for sale.
- The access sale is likely indicative of an impending large-scale attack against the widely-used eCommerce CMS provider and is mostly likely to be part of a broader financially-motivated operation against retail targets.

| Details

On January 15, 2024, well-regarded threat actor “isabellavonbiz” announced the sale of the source code, business operations data, and documentation of an unspecified eCommerce CMS services vendor on the predominantly Russian-language dark web forum exploit[.]in. The actor claimed that the CMS is used by 470 vendors, totalling in

excess of two million orders per month and a combined annual revenue of more than USD 2.5 billion. The package includes:

- The source code of all online retailers with which the CMS has business relationships;
- Approximately 1.7 terabytes of documentation; and
- Persistent root shell to the main server of the CMS. The threat actor claimed that the buyer would be able to observe the entire supply chain.



Exploit[.]in post advertising the CMS data and access sale

Source: ZeroFox Intelligence

The entire package was instantly purchased (or “blitzed”) by guru-level actor “s4l0_” for USD 6,000, leaving no chance for any competition. S4l0_ is a highly competent and popular threat actor, with additional intelligence indicating they are buying and potentially hoarding access to as many online shops as possible.

- In January 2024, ZeroFox observed a mass access sale featuring access to nearly a dozen U.S. WooCommerce online retailers.
- S4l0_ blitzed this deal as well, an hour after its announcement.

The access sale is likely indicative of an impending large-scale attack against the widely-used eCommerce CMS provider and may be part of a broader operation against retail targets. Since the start of 2024, ZeroFox has observed a continued high frequency of mass access sales targeting online retailers.

- Given the highly-specific targeting, it is likely the threat actor will seek to initiate a criminal financial scheme.
- This is most likely to take the form of a large-scale carding operation involving cashing out as many stolen credit and debit cards via the compromised shops' payment processors.
- It is also possible access will be leveraged by or sold to ransomware and digital extortion collectives for mass targeting of retailers.

| Recommendations

- Ensure a thorough understanding of your technology stack and patching schedule, as well as those of operating partners.
- Conduct a thorough assessment of servers and review any relevant activity logs for suspicious behavior.
- Leverage cyber threat intelligence to inform detection of malware and ransomware and digital extortion threats and their associated tactics, techniques, and procedures (TTPs) and Indicators of Compromise (IOCs).
- Protect endpoint devices with phishing-resistant MFA protocols compliant with FIDO2 or PKI standards.
- Ensure critical data is backed up to secure off-site or cloud servers. Sensitive or proprietary data should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures, and key authorities.

| Appendix A: 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 B: 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%