



| **Flash** |

"Spyboy": EDR Bypass Claims Spark Mixed Reactions

F-2023-05-31a

Classification: TLP:GREEN

Criticality: Low

Intelligence Requirements: Dark and Deep Web

May 31, 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 07:00 AM (EDT) on May 31, 2023*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | "Spyboy": EDR Bypass Claims Spark Mixed Reactions

› Key Findings

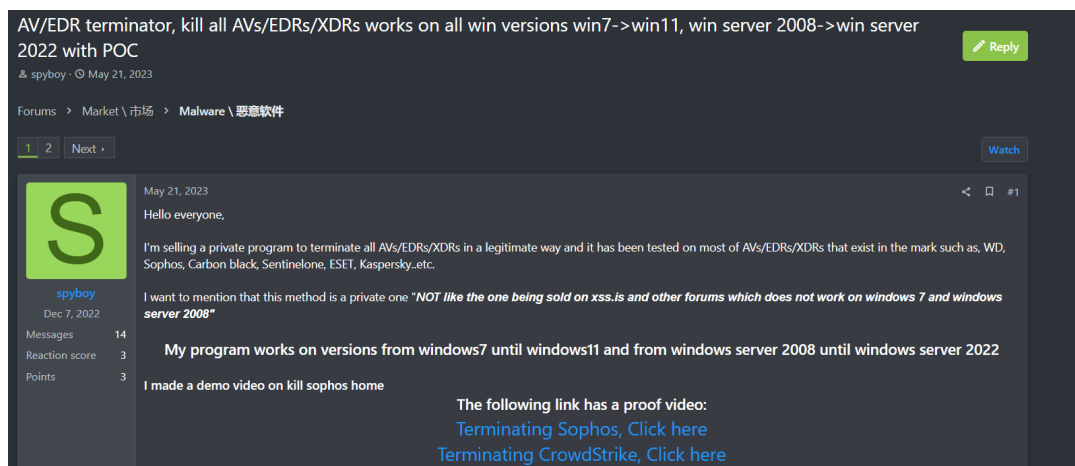
- Threat actor "spyboy" is advertising and selling an Antivirus (AV) and Endpoint Detection and Response (EDR) killer, asserting that it can bypass and disable a wide range of the most prominent AV and EDR solutions on the market.
- Reactions from reputable underground actors regarding spyboy's claims have been mixed, with some actors defending the assertions made while others raising doubts about their validity. ZeroFox has not independently validated or verified the claims made by spyboy.
- Despite skepticism, the discussions and offerings surrounding EDR bypass techniques continue to evolve in underground communities, indicating a dynamic landscape in the realm of cyber threats and defenses.

| Analyst Commentary

A threat actor known as "spyboy" is promoting and selling an AV/EDR killer in Russian-language deep and dark web (DDW) forum RAMP, claiming it bypasses and disables prominent AV and EDR solutions. Spyboy's claims have sparked diverse

reactions from reputable underground actors, with some defending and others questioning the validity of the claims. Spyboy is a relatively new member on RAMP with a positively trending reputation and has agreed to escrow, which is typically seen as a positive indicator of legitimacy within these communities.

- A Russian-speaking actor named "bratva" criticized spyboy's post, suggesting that similar methods are already publicly available at no cost on other platforms such as [github\[.\]com/ZeroMemoryEx/Blackout](https://github.com/ZeroMemoryEx/Blackout) and [redops\[.\]at/blog/a-story-about-tampering-edrs](https://redops[at]blog/a-story-about-tampering-edrs). Additionally, bratva alleged that spyboy might be a security researcher.
- On the other hand, a respected English-speaking threat actor countered these claims, stating that software capable of terminating EDRs is unlikely to be publicly accessible. This underscores the ongoing debate within the threat actor community regarding the credibility of spyboy's claims.



AV/EDR killer advert posted by spyboy on RAMP

Source: ZeroFox Intelligence Internal Collections

Spyboy has a history of discussing EDR bypass on DDW forums and posted an article on [xss\[.\]is](https://xss[.]is) as early as June 2022 supposedly teaching actors how to bypass EDRs—including CrowdStrike's. The post was largely met with skepticism, with multiple actors claiming the article guide does not work.

ZeroFox notes that the underground discussions regarding EDR show an increasing trend in anti-EDR tactics since at least the fall of 2022. In October 2022, very well-regarded threat actors on Russian-language deep and dark web forums Exploit[.]in and xss[.]is began advertising an EDR bypass, naming CrowdStrike specifically—in one case reasserting the method was still effective on May 23, 2023.

- In early October 2022, one of the most well-regarded threat actors and penetration testing specialists on Exploit[.]in, "Lord1," claimed to have developed a fully undetectable (FUD) payload that would bypass all EDR systems associated with Cylance, Sentinel, CrowdStrike, and Carbon.
- On March 25, 2023, a well-regarded forum actor updated an earlier obfuscation services thread to claim they can now bypass CrowdStrike EDR; there have been no public comments on the thread confirming or disconfirming if this tool works.
- On March 29, 2023, very well-regarded and longtime xss[.]is forum actor "rlz" alleged that an EDR bypass tool they developed still works and guaranteed successful bypass or the buyer will get their money back.

ZeroFox Intelligence will continue to monitor the developing conversation around spyboy's claims, particularly relating to the actor's credibility and the efficacy of the purported EDR killer. Given that discussions and offerings surrounding EDR bypass techniques continue to evolve in underground communities, ZeroFox recommends ensuring defensive systems are updated with the latest detections.

Appendix: 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.