Flash

Spamming Package Targeting the U.S. SSA Advertised on the DDW

F-2026-06-15a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Spamming, Phishing, Deep and Dark Web

June 15, 2026

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 June 15, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Spamming Package Targeting the U.S. SSA Advertised on the DDW

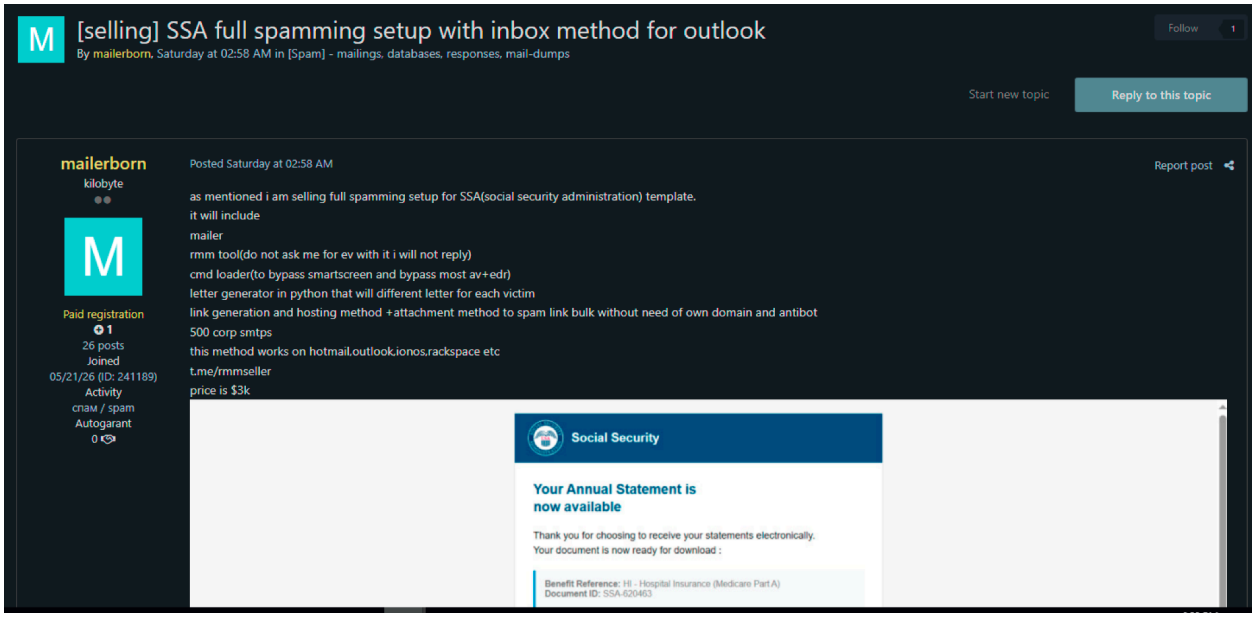
| Key Findings

- On June 6, 2026, untested threat actor "mailerborn" advertised a spam distribution package targeting the U.S. Social Security Administration (SSA) on the predominantly Russian-language deep and dark web (DDW) forum Exploit.
- Mailerborn joined Exploit on May 21, 2026, and has made nearly 30 posts as of reporting but has garnered only one reputation point.
- The claimed features of the package—including a command loader that can evade common security controls, access to about 500 corporate Simple Mail Transfer Protocol (SMTP) servers, and per-recipient email generator—are likely to enhance phishing capabilities.
- Although ZeroFox has previously observed similar spam-related services—including email bombing and SMS spamming tools—on underground forums, this is likely a dedicated offering built around SSA-themed lures.

Details

On June 6, 2026, untested threat actor mailerborn advertised a spam distribution package targeting the U.S. SSA on the predominantly Russian-language DDW forum Exploit. The actor included a link to a Telegram channel, likely to communicate with interested buyers, and listed the package at USD 3,000. As of writing, the post has not received any engagement.

- The actor claims the package does not require a dedicated domain, includes anti-bot protections, and supports a large-scale, Python-based per-recipient email distribution at deployment.
- The package also allegedly provides access to about 500 corporate SMTP servers and includes a command loader designed to evade security controls and a Remote Monitoring and Management (RMM) tool that enables remote monitoring and automation.

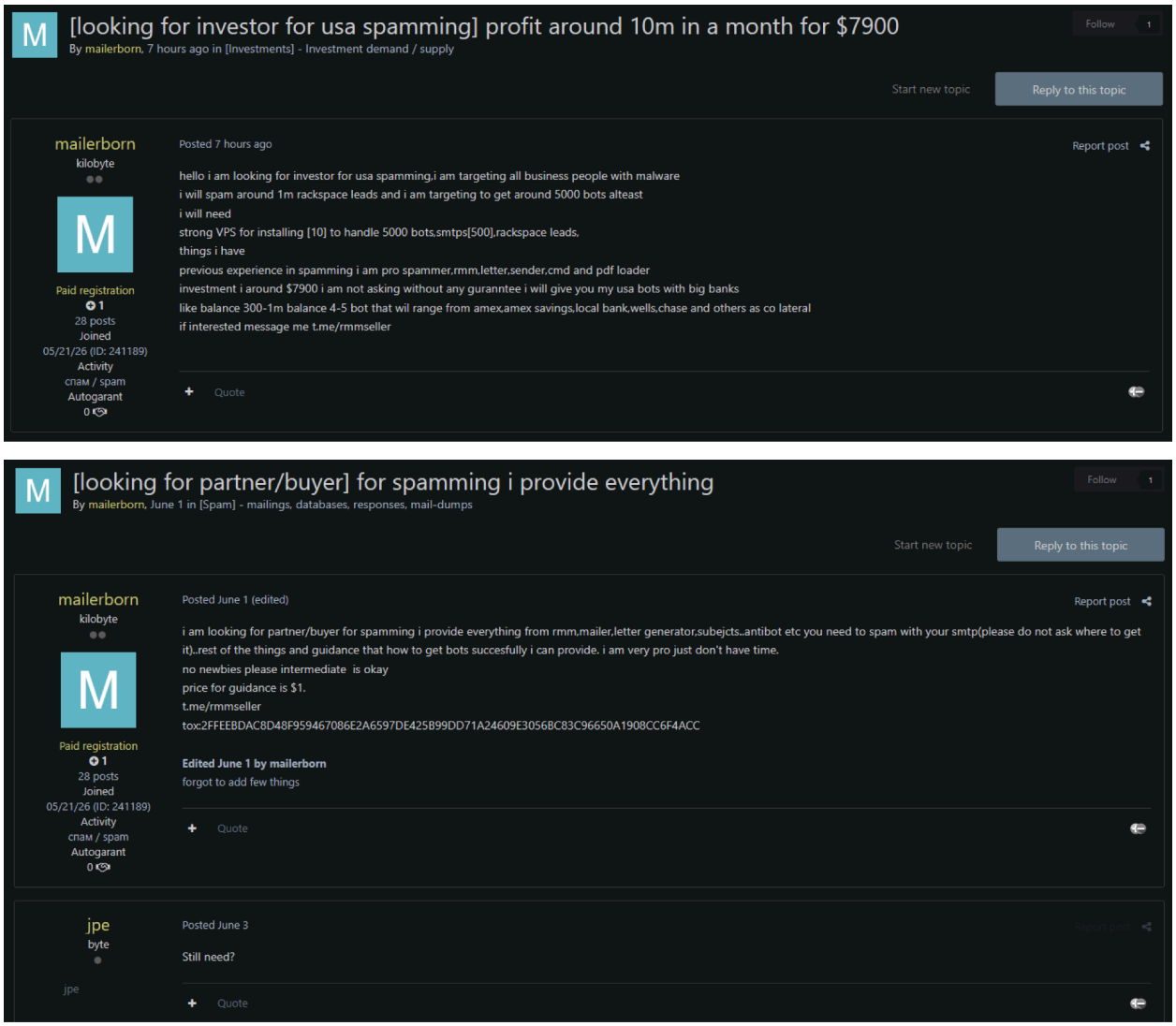


mailerborn's post on Exploit

Source: ZeroFox Intelligence

The actor joined Exploit on May 21, 2026, and has made nearly 30 posts as of reporting but has garnered only one reputation point. The high volume of posts is likely an indication that mailerborn is trying to gain prominence on the dark web forum.

- The actor has previously posted on the forum seeking partners and investors, very likely to orchestrate a large-scale spamming campaign targeting U.S. entities, including banks and government organizations.
- The actor claims to be a "pro-spammer" and has stated they can provide sufficient resources to conduct the campaign, including bots allegedly specifically designed to target banks. The posts likely suggest mailerborn's effort to expand the alleged campaign and scale up its operations.



mailerborn's posts seeking partners and investors for a spamming campaign

Source: ZeroFox Intelligence

The claimed features of the package—including a command loader that can evade common security controls, access to about 500 corporate SMTP servers, and per-recipient email generator—are likely to enhance phishing capabilities. The attacker can send emails through trusted corporate infrastructure using the SMTP servers, while bypassing basic security controls using the command loader.

Although ZeroFox has previously observed similar spam-related services—including email bombing and SMS spamming tools—on underground forums, this is likely a dedicated offering built around SSA-themed lures. The actor's efforts to advertise the tool, seek partners, and attract potential investors likely suggest an interest in expanding operations beyond a single campaign. Additionally, the volume of posts made since joining the forum is likely an attempt to build visibility, attract partners or investors, and gain credibility within the cybercriminal community.

Mailerborn is unproven, has a low reputation on Exploit, and the advertised package remains untested. However, the combination of claimed technical capabilities—such as SMTP server access, antivirus (AV)-evasive command loader, and scalable per-recipient distribution—very likely represents a meaningful increase in phishing potential if the tooling performs as described. ZeroFox assesses that SSA-themed lures are likely inherently effective for social engineering campaigns against broad consumer demographics, given the agency's direct association with financial benefits for millions of U.S. citizens. Mailerborn's concurrent efforts to recruit partners and investors suggest this is not a one-off listing but an attempt to build a durable operation. ZeroFox will continue to monitor mailerborn's activity on Exploit and associated channels for signs of increased credibility, operational escalation, or evidence that the package has been deployed.

| 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%

| Appendix C: ZeroFox Intelligence Threat Actor Reputation Scale

Untested	Moderately Credible	Well-regarded	Prominent
Has garnered no reputation; credibility cannot be determined.	Has made up to 10 transactions; has been active on forum for at least three months.	Has at least 10 transactions; has been active on forum for three months to one year.	One of the most well-known and credible threat actors on the site; long-term, established presence on the forum of more than one year.