



| Brief |

The Underground Economist: Volume 5, Issue 8

B-2025-04-25a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

April 25, 2025

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 (EDT) on April 25, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 8

DragonForce Responds to Criticism Surrounding Ongoing RansomHub Hiatus

On April 19, 2025, actor “lateralmovement” posted on Russian-speaking deep and dark web (DDW) forum RAMP, criticizing the ransomware and digital extortion collective (R&DE) RansomHub, and more specifically the actor “Koley”, who is widely recognized within DDW forums as the face of RansomHub. Public spouts between personalities surrounding reputation are common within these communities and are sometimes done intentionally to confuse law enforcement (LE) entities and researchers investigating these groups.

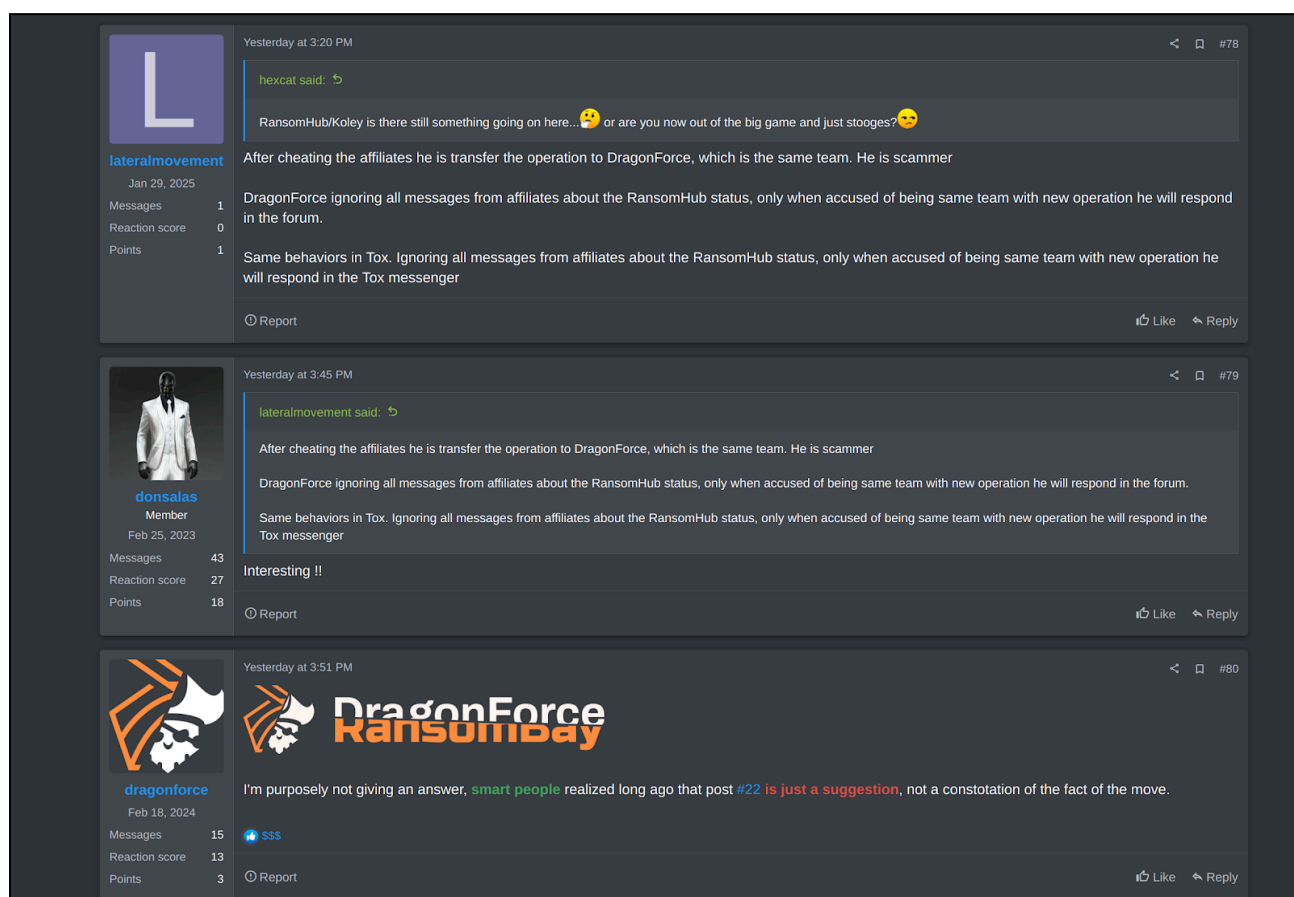
- ZeroFox previously reported on the apparent outage of RansomHub’s dark web victim leak site, which has been offline since April 1, 2025 with no new victims being observed.¹
- Around April 4, 2025, an account associated with DragonForce posted on RAMP claiming that RansomHub “will be up soon”, and that RansomHub had decided to move to DragonForce’s infrastructure.

Lateralmovement claimed that RansomHub and the R&DE collective DragonForce are the “same team”, and that Koley is a “scammer”. According to the post, DragonForce is ignoring all messages, both on RAMP and the private messaging platform Tox, from

¹ [hXXps://docs\[.\]google\[.\]com/document/d/1UcEL-vSwdWDHS7DZVDvx5JO6SjvR25w7/edit](https://docs.google.com/document/d/1UcEL-vSwdWDHS7DZVDvx5JO6SjvR25w7/edit)

affiliates seeking information regarding the status of RansomHub-only replying when accused of being the “same team”.

Shortly after the post, DragonForce responded in the same thread, stating that they are purposefully “not giving an answer”, and that “smart people” had already realised that their original post, in response to the ongoing hiatus of RansomHub, was a suggestion that they had merged with DragonForce and not fact.



Lateralmovement's RAMP thread

Source: ZeroFox Intelligence

As of the writing of this report, it remains unclear what caused the cessation of RansomHub. ZeroFox has observed no further activity from RansomHub since April 1, 2025, and affiliates remain seemingly unaware of the collective's current operational status. The recent RAMP comments made by DragonForce, along with lateralmovement's

claims, are likely reflective of attempts by DragonForce to disassociate themselves from the negative accusations leveraged toward RansomHub.

RansomHub is very likely non-operational, posing a significantly reduced threat to global organizations across industries. There is a likely chance that RansomHub will remain non-operational during the coming weeks. DragonForce has exhibited an increased attack tempo in recent weeks, conducting more attacks so far in April 2025 than in any other previous month, though it is unclear whether this is the result of obtaining RansomHub assets.

| Threat Actor Seeks to Buy U.S. Military CAD Files on Exploit

On April 17, 2025, threat actor “M0rk” responded to an April 2024 post made by “Black” in the Russian language dark web forum Exploit. The post advertised the sale of Computer-Aided Design (CAD) files related to U.S. Air Force Academy (USAFA), the U.S. Space Force (USSF), and an unspecified U.S. military base, and is priced at USD 10,000. In M0rk’s response, they enquired as to Black’s preferred communication methods.

- Previously, on February 26, 2025, M0rk posted on Exploit stating that they are seeking databases and email addresses related to government institutions in the U.S., Japan, South Korea, and Taiwan. The post was updated on April 18 to add military and military contractors to the request.
- CAD files are digital files that store 2D or 3D designs, heavily used in industries such as architecture, engineering or manufacturing.

M

Buying database/emails from .GOV
By **M0rk**, February 26 in [Spam] - mailings, databases, responses, mail-dumps, software

M0rk
kilobyte
●●

M

Paid registration
● 0
40 posts
Joined
09/09/24 (ID: 176391)

Posted February 26

Need a lot of databases and emails from the US/Japan/Korea/Taiwan .GOV PM for detail

+ Quote

M0rk Exploit post

Source: ZeroFox Intelligence

E

AutoCAD файлы USAFA, USSF, Military base - USA
By **Elnoir**, April 30, 2024 in [Other] - everything else

Black
kilobyte
●●

E

Paid registration
+ 4
30 posts
Joined
10/31/21 (ID: 121647)
Activity
hacking / hacking
Car warranty


Posted April 30, 2024

I will sell CAD files of the format .dwg .dws .rvt, drawings of schemes, etc., about 2500 files approximately 6 GB
USAFA - United States Air Force Academy
USSF - United States Space Force
\$10k

+ Quote

M0rk
kilobyte
●●

M

Paid registration
● 0

Posted Thursday at 04:36 AM

interested, how can I contact you?

+ Quote

Black's Exploit post

Source: ZeroFox Intelligence

As of the writing of this report, there have been no public responses to M0rk's Exploit post from February 26, though any communications would likely have taken place privately—as per M0rk's request. M0rk is almost certainly interested in acquiring information related to countries considered geopolitical, military, or ideological adversaries of China.

- Although M0rk's motives are unclear, it is likely that such information would either be used by nation state actors to further strategic agendas or gain insight into oppositional military capabilities.
- There is also a less likely chance that the information would be sold again, to other interested parties.

M0rk's post is likely to garner attention from malicious actors in possession of data sets pertaining to historic or recent network breaches. However, despite joining the Exploit forum in September 2024, and making 40 posts since, M0rk has not yet established a confirmed reputation. This will very likely result in interested sellers exercising increased caution, hindering the acquiring of any such data.

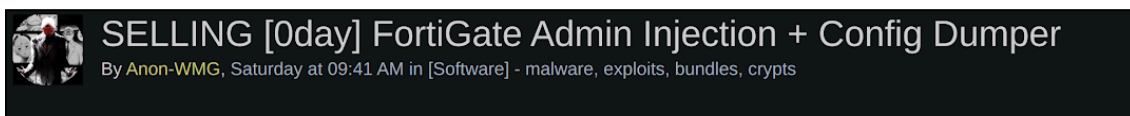
| Remote Code Execution Injection Zero-Day Vulnerability Advertised

On April 12, 2025, the newly registered actor "Anon-WMG" posted in popular Russian-language dark web forum Exploit, advertising an alleged admin injection zero-day vulnerability which targets users of the Fortinet's next generation firewall (NGFW) FortiGate. According to Anon-WMG, the vulnerability allows an attacker to achieve control of vulnerable firewalls without credentials, via remote code execution (RCE).

- Anon-WMG also shared a link to the vulnerabilities shared storage with a proof of concept (PoC) of the weaponized vulnerability; at the time of this writing, this link has expired, which could indicate that there is some controversy around the claims made in the post.

The alleged vulnerability is advertised for a price of USD 6,500, and reportedly has the following features:

- Authentication and access
- Firewall and network address translation (NAT)
- Virtual private network (VPN) and remote access
- Network monitoring
- Certificates and trust



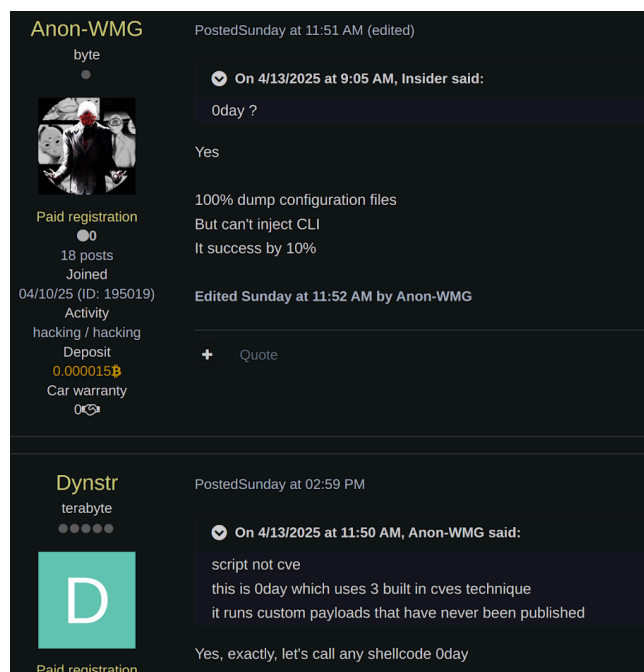
Anon-WMG's Exploit post

Source: Zerofox Intelligence

Anon-WMG joined the Exploit forum on April 10, 2025, and has yet to garner significant credibility within the forum. While the advertisement post generated interest from fellow users, they mostly consisted of speculation surrounding the authenticity of Anon-WMG's claims, with some skeptics suggesting that the alleged vulnerability is unlikely a zero-day.

Anon-WMG responded to these claims by reasserting their claim that it is a zero-day exploit as advertised, with a perfect success rate of exfiltrating configuration files. In the same post however, the actor conceded that the alleged RCE is unable to inject command-line interface (CLI), due to the fact that the success rate for this command execution is just ten percent. This could imply the following:

- Limited execution context: The TCE may be running in a restricted environment, with no access to CLI tools or shells.
- Non-shell execution: Th RCE could execute in a scripting context (Python or PHP, for example), where traditional shell commands are not natively interpreted.
- Output not returned: The RCE may be blind with no output, making it more difficult to confirm successful command injection or requiring additional exfiltration techniques.
- Character filtering: Special characters such as ";" or "&" may be filtered, making payload crafting more difficult.
- Lack of standard binaries: Minimalist environments may lack common binaries such as wget or curl, limiting what can be achieved via CLI.



Responses to Anon-WMG's Exploit post

Source: Zerofox Intelligence

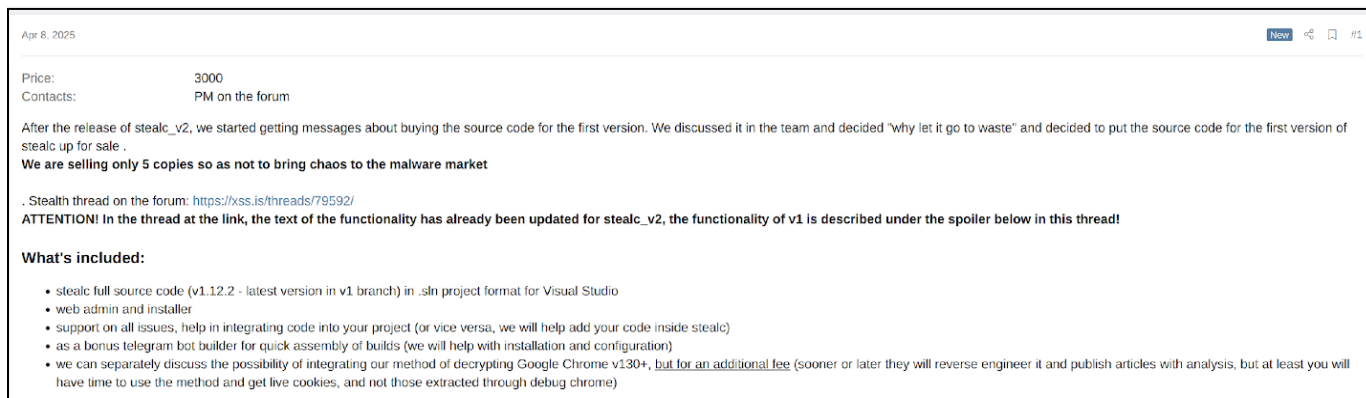
Since the alleged exploit cannot inject CLI, some forum users suggested that this vulnerability is more likely to be a shellcode than a zero-day. Despite this, Anon-WMG claimed that the alleged zero-day leverages three unspecified built-in common vulnerabilities and exposures (CVEs) techniques, running on custom payloads which have never previously been published. Despite considerable skepticism, Anon-WMG offers the use of escrow to make a sale.

| StealC Malware Source Code Advertised for Sale

On April 8, 2025, untested actor, "Plymouth" posted in the Russian-language dark web forum XSS, advertising source code for the StealC information stealer. According to the post, five copies are available for sale at a price of USD 3,000 each.

- StealC is a widely used InfoStealer malware strain, which is currently ranked fourth in terms of popularity within the Russian cybercrime market, with approximately 15 million infected devices recorded since early 2023.

- Plymouth is the self-proclaimed developer and project leader of StealC, which has been operated as a Malware-as-a-Service (MaaS) on Russian-speaking forums since 2023. The service is available via a subscription,



Plymouth's XSS post advertising StealC source code

Source: ZeroFox Intelligence

In the post, Plymouth stated that after StealC v2 was released earlier in 2025, they received messages enquiring about the purchase of source code related to the previous version, v1.12.2. According to an April 15, 2025 post made by Plymouth, three out of five copies had been sold, though it is unclear who the buyers were, what their motives are, and what the final sale price was. There is a likely chance that buyers will seek to resell the source code for profit, or seek to enhance the malware in support of other MaaS projects.

Although ZeroFox has previously observed the sale of malware source code pertaining to out of date versions, the USD 3000 asking price is lower than is usually expected for such a tool. This likely either reflects Plymouth's desire for a quick sale or a wider choice of buyers. It is also very likely that the sale is limited to five buyers only, in an attempt to maintain the reputation of StealC v.2 and avoid market disruption.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%