



| Brief |

The Underground Economist: Volume 5, Issue 9

B-2025-05-09a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

May 9, 2025

Scope Note

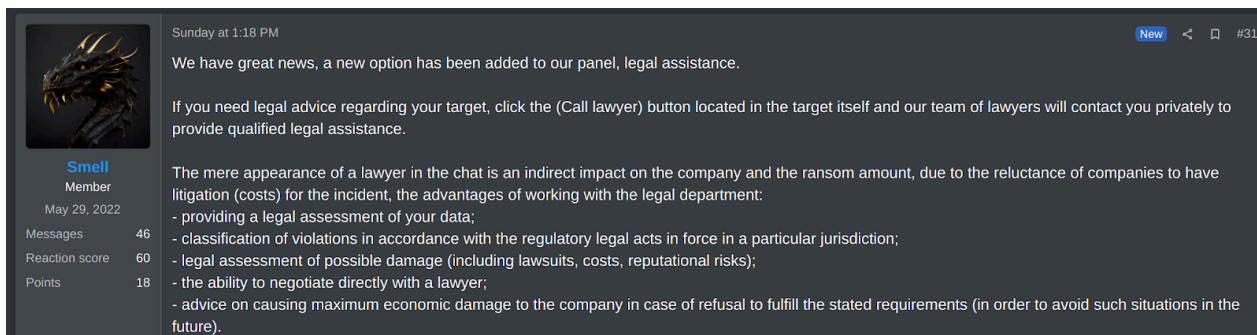
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 May 9, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 5, Issue 9

Qilin Announces New Legal Assistance for Affiliates

On May 4, 2025, threat actor “Smell”, the official spokesperson for the Qilin ransomware collective, posted on Russian-speaking dark web forum RAMP announcing a new “legal assistance” feature now allegedly available to affiliates. Smell claimed that the new offering, available through Qilin’s affiliate panel, includes access to “our team of lawyers” to provide qualified legal assistance on the following:

- Legal assessment of compromised data
- Classification of violations under applicable jurisdictional laws
- Evaluation of potential damages (lawsuits, financial losses, reputational harm)
- Help with direct negotiations with legal advisors
- Strategic advice on maximizing economic damage to non-compliant victims



The screenshot shows a forum post on RAMP by a user named "Smell". The post is dated "Sunday at 1:18 PM" and has a "New" badge. The post content reads: "We have great news, a new option has been added to our panel, legal assistance. If you need legal advice regarding your target, click the (Call lawyer) button located in the target itself and our team of lawyers will contact you privately to provide qualified legal assistance." Below the main text, there is a list of bullet points detailing the benefits of the legal assistance: "The mere appearance of a lawyer in the chat is an indirect impact on the company and the ransom amount, due to the reluctance of companies to have litigation (costs) for the incident, the advantages of working with the legal department: - providing a legal assessment of your data; - classification of violations in accordance with the regulatory legal acts in force in a particular jurisdiction; - legal assessment of possible damage (including lawsuits, costs, reputational risks); - the ability to negotiate directly with a lawyer; - advice on causing maximum economic damage to the company in case of refusal to fulfill the stated requirements (in order to avoid such situations in the future)." On the left side of the post, there is a profile card for "Smell" with a dragon avatar, showing "Member" status, "May 29, 2022" join date, and statistics: "Messages 46", "Reaction score 60", and "Points 18".

RAMP post by Smell on May 4, 2025

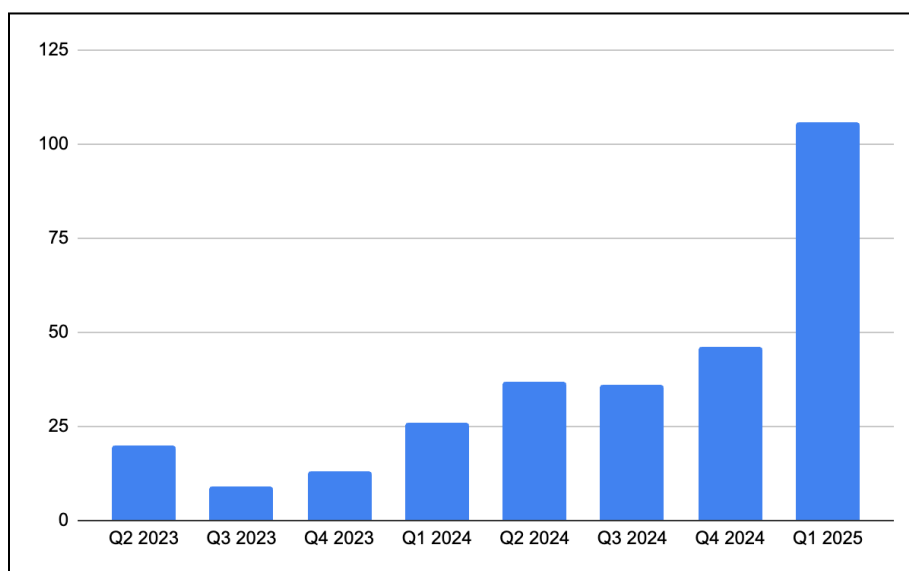
Source: ZeroFox Intelligence

Later on the same day, Smell posted on RAMP stating that they will introduce additional features in the “near future” for its affiliates, including 1 TB of storage space, a tool for spamming corporate emails, a tool for spamming phone numbers, and their own “staff of journalists.”

- “Journalists” is likely an umbrella term for persons trained in media, public relations (PR), and/or journalism.

Notably, the journalists would allegedly work in conjunction with the legal team by drafting content for leak blogs and playing a role in media manipulation and negotiation tactics.

- Qilin is a Russian-speaking ransomware-as-a-service (RaaS) collective first observed by ZeroFox in July 2022.
- ZeroFox has observed a steady increase in ransomware attacks by Qilin over the past two years. The collective claimed responsibility for 20 attacks in Q2 2023 (1.87 percent of all attacks); this number increased significantly to 106 attacks in Q1 2025 (5.38 percent of all attacks), making Qilin the fourth most active collective in Q1 2025.



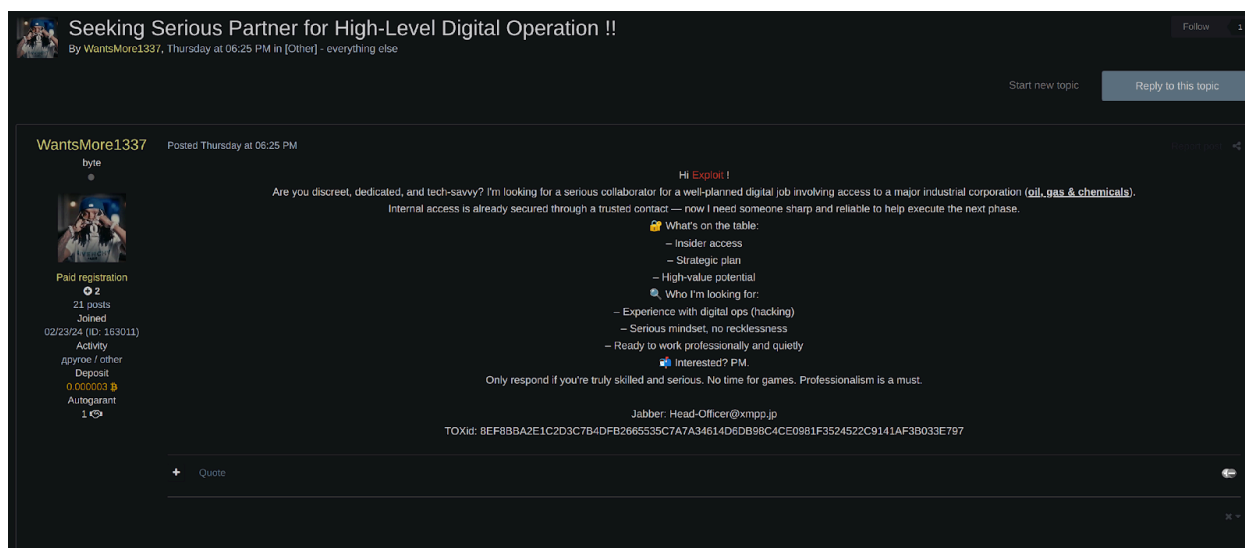
Ransomware attacks by Qilin

Source: ZeroFox Intelligence

This announcement reflects an emerging professionalization trend within ransomware collectives. The integration of legal and journalist services into ransomware operations demonstrates a strategic shift in how ransomware collectives seek to enhance coercion, credibility, and operational efficiency. Providing qualified legal assistance to affiliates will very likely increase threat actor leverage against victims by deploying in-depth knowledge of local, national, and international policies or laws like the European Union's General Data Protection Regulation (GDPR). The proposed integration of both legal assistance and journalist/media/PR services is very likely an attempt by Qilin to attract more affiliates and gain more market share in the ransomware space.

Cyber Operation Leveraging Insider Access Partnership

On May 1, 2025, the threat actor "WantsMore1337" posted on the dark web forum Exploit seeking a partner to collaborate with on an unspecified operation leveraging insider access to an unnamed, major industrial corporation in the oil, gas, and chemical sector. The actor alleges the internal access has already been secured through a "trusted contact."



WantsMore1337's original post on Exploit

Source: ZeroFox Intelligence

According to the post, WantsMore1337's outlined intent for a potential partner is executing a next phase of the operation. The actor claims to offer a potential partner a

strategic plan, insider access, and high value potential. The post, similar in nature to a company's hiring advertisements, outlines desired qualifications and skills such as:

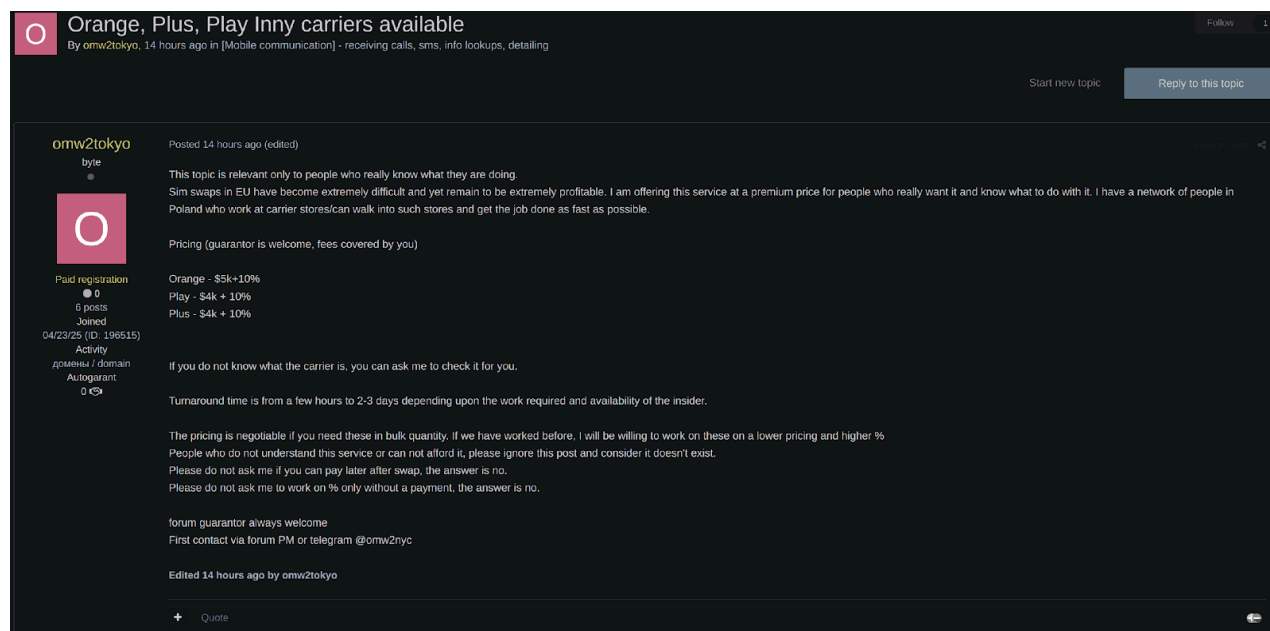
- Experience with digital operations, including hacking
- A serious and cautious approach
- Willingness to work professionally and discreetly

WantsMore1337 is an established actor on the Exploit forum first observed on February 23, 2024. Since joining, the actor has maintained a relatively good reputation on the forum, likely contributing to their perceived legitimacy. ZeroFox has not observed evidence to substantiate the actor's claims but cannot disqualify WantsMore1337 as a credible actor at this time. WantsMore1337 did not specify the nature or the extent of the alleged network access, but there is a roughly even chance that it pertains to an insider access. Successfully exploited, such access could lead to the deployment of malware, digital extortion, industrial espionage, or data theft.

| SIM Card Swap Services Target European Mobile Carriers

Around April 30, 2025, an English-speaking threat actor known as "omw2tokyo" advertised subscriber identity module (SIM) card swap services targeting three major European mobile carriers (Orange, Play, and Plus) on the dark web forum Exploit. The actor claims to have connections to a network of insider employees that work at these carriers' retail stores in Poland, which could allow omw2tokyo to bypass traditional security barriers implemented to safeguard customer accounts. In this case, the actor alleges insiders have facilitated omw2tokyo's efficiency at completing SIM swap requests.

- The exact time of the advertisement's publication is unknown, as the actor edited the original post.



omw2tokyo's revised advertisement on Exploit

Source: ZeroFox Intelligence

Omw2tokyo is newly registered on the Exploit forum (first observed on April 23, 2025) with limited user feedback and reputation. The actor has offered transactions via escrow or a middleman service—likely as an attempt to legitimize the service and increase the likelihood of successful sales. At this time, ZeroFox cannot determine the reliability of the service nor the authenticity of the actor's alleged insider access. In omw2tokyo's advertisement, the actor alleges that their SIM card swap services are expected to be complete after a few hours or two to three days, depending on resource availability and bandwidth. Service expectations and pricing schemes are also outlined for various carriers in Poland as follows:

- Orange - USD 5,000
- Play - USD 4,000
- Plus - USD 4,000

The advertisement also specifies that buyers must pay 10 percent of any funds obtained to omw2tokyo.

ZeroFox has observed SIM swapping to be one of the most sought-after underground services in Europe, most likely due to its effectiveness in circumventing multi-factor

authentication (MFA). The increasing trend of insider networks within telecommunication providers highlights the risk insider threats pose to organizations industry-wide. Actors leveraging SIM swapping attacks likely will gain additional personally identifiable information (PII) to further infiltrate personal networks and conduct social engineering attacks, online banking fraud, and business email compromises (BEC).

| Threat Actor Shows Renewed Interest in Taiwan Data

On April 29, 2025, untested threat actor “M0rk” posted an advertisement on Russian-speaking dark web forum xss seeking to recruit “hackers” and purchase Taiwan-related data. ZeroFox has previously reported on M0rk seeking to buy data related to Taiwan on the Exploit forum.

- On February 26, 2025, M0rk posted on Russian-language dark web forum Exploit stating that they are seeking databases and email addresses related to government institutions in the United States, Japan, South Korea, and Taiwan. The post was updated on April 18 to add military and military contractors to the request.
- On April 17, 2025, M0rk responded to an April 2024 post made by “Black” in Exploit advertising the sale of Computer-Aided Design (CAD) files related to the U.S. Air Force Academy (USAFA), the U.S. Space Force (USSF), and an unspecified U.S. military base.

Recruiting hackers/purchasing Taiwan data

M0rk · Yesterday at 9:35 AM

ESCROW AVAILABLE IN THIS THREAD!

New deal



M0rk
HDD-drive
Пользователь
Joined: Sep 14, 2024
Messages: 27
Reaction score: 0

Yesterday at 9:35 AM

Цена: PM with your offer
Контакты: FE822DA74FF22A29D5A8B8F7738A19BFEAFF5DCB5662B5D3B977B7BE9524BF62083E2A3CE39C

Long-term needs

Report

Post by M0rk on April 29, 2025

Source: ZeroFox Intelligence

The actor joined both Exploit and xss in September 2024 and has not garnered any reputation points from other forum members as of writing this report. While reputation points do not solely represent the credibility of an actor, M0rk's lack of any likely does cast doubt about the actor's legitimacy among other users on the forum. The actor has shown a consistent interest in government and military-related data from countries that are frequently perceived as geopolitical or ideological adversaries of China.

It is likely that M0rk is a financially motivated threat actor looking to acquire sensitive data to subsequently sell to interested parties—likely those ideologically aligned with China. It is almost certain that M0rk will continue seeking access to similar data sets on both Exploit and xss in the near future. M0rk's post is also likely to gain engagement via private communication channels from other threat actors in possession of relevant data sets.

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 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 deep and dark web (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%