2 - 4 October, 2024 / Dublin, Ireland

DARK DEALS: UNVEILING THE UNDERGROUND MARKET OF EXPLOITS

Anna Pavlovskaia & Vladislav Belousov

Kaspersky, Russia

an.pavlovskaia@gmail.com

ABSTRACT

The dark web has emerged as a central hub for malware and exploit sales. This paper explores the complex market dynamics of the dark web and the economy standing behind this business. The pricing of exploits is influenced by many factors such as system criticality, exploit type, number of buyers, uniqueness of the offering, and the reputation of the seller. We also observe the prevalence of fraud and the significant role that escrow services play in facilitating cybercriminal transactions. By shedding light on these issues, the goal of this article is to improve understanding of the illicit marketplace of the dark web.

INTRODUCTION

In the world of cybercrime, the initial penetration of a target's system often determines the success or failure of an attack. The crucial phase of an attack is related to the Initial Access (TA0001) tactic on the MITRE ATT&CK framework, involves gaining access to a target system, and it frequently uses sophisticated exploits to bypass security controls and establish persistence.

According to *Kaspersky* data, in 2023 the most common initial access technique was the exploitation of public-facing applications (42.37% of all cases)[1]. Only a third of these applications were attacked through known vulnerabilities, including those discovered in 2021 and 2022 [1].

Cybercriminals obtain exploits from a wide variety of sources, each of which contributes to the sophisticated chain of their operations. The exploit market is diverse and includes both public and dark web marketplaces.

Publicly available proof-of-concept (PoC) exploits are often shared openly within the cybersecurity community to demonstrate security weaknesses and encourage developers to patch vulnerabilities. These PoCs do not involve financial transactions and are accessible to anyone.

Some researchers discover vulnerabilities and choose to sell them rather than report them. High-value zero-day exploits can be found on official platforms such as *Zerodium*, which buys exploits from researchers at premium prices. *Zerodium*'s deals are typically exclusive, with a focus on acquiring unique, undisclosed vulnerabilities for government and corporate use.

In between are the dark web markets, where exploits of varying sophistication and freshness are bought and sold with relative anonymity. Despite the growth of legitimate bug bounties, it is still easy and profitable to sell zero-day exploits on the black market.

DARK WEB MARKETS ECONOMY

The dark web is a collection of resources that exist for a variety of purposes. These include marketplaces where cybercriminals can trade exploits, giving them a place to buy and sell information about discovered vulnerabilities. The same principles of buying and selling products apply to the dark web markets as they do to traditional markets.

Exploits are a highly profitable product within the dark web markets. However, despite the profitability of these products, there are significant challenges to the sale of such products. The difficulty lies in the complicated nature of demonstrating the effectiveness of an exploit without disclosure of the exploit itself. This dilemma makes fraudulent schemes possible. Sellers may make false claims about exploits or fail to deliver the functionality they promise. As a result, buyers are cautious and sceptical about navigating the murky waters of exploit transactions because of the risk of falling victim to fraud.

This makes buying and selling exploits a complex process with many factors that affect the pricing of exploits and their availability for sale to the public on dark web forums.

Analysis of exploit offers volume

To analyse the state of the dark web exploit market from January 2023 to May 2024, we gathered statistics on messages that related to the buying and selling of exploits. Our sample included messages from international forums and marketplaces on the dark web, as well as from publicly available *Telegram* channels used by cybercriminals.

The distribution of messages is shown in Figure 1. A total of 414 advertisements related to buying and selling of exploits were posted on dark web forums during the observed period[2]. On average, there are approximately 23 exploits offered on a monthly basis.

Proofs of working exploits are not always available, making it challenging to accurately estimate the number of functional exploits on the market. Sellers often provide incomplete or fabricated proof-of-concepts, leaving buyers unsure of the exploit's effectiveness until after the transaction. This lack of verification contributes to the uncertainty and risk inherent in purchasing exploits on the dark web. Consequently, the true number of operational exploits remains difficult to determine, as many advertised exploits may be non-functional or significantly less effective than claimed. This opacity complicates efforts to assess the overall threat landscape and the actual capabilities of cybercriminals operating within these markets.

[1] The data used in the report is derived from working with organizations that have requested incident response assistance or provided expertise to their internal incident response teams.

[2] The offers included in the sample may be non-unique, because the same offer may be posted on several cybercriminal resources.

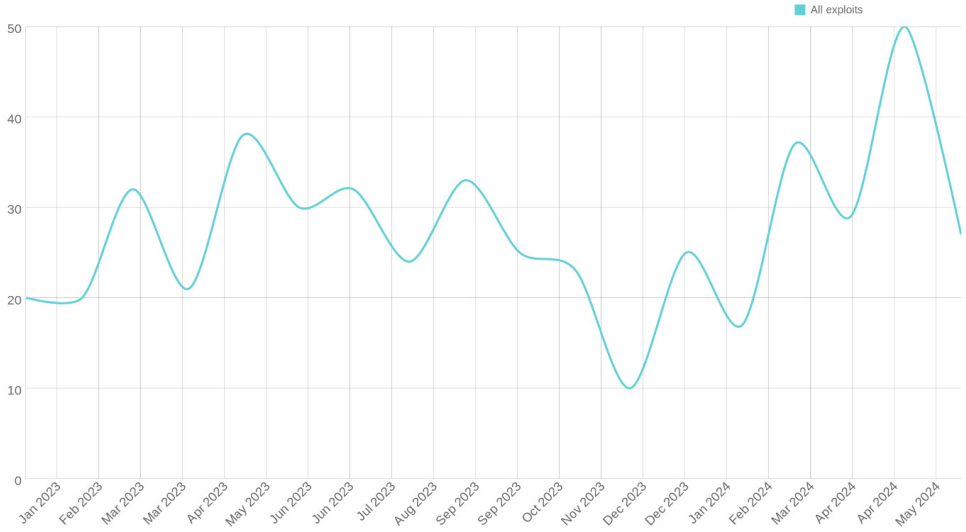


Figure 1: The distribution of messages related to buying and selling of exploits.

Exploit pricing policy

Pricing policies for exploits can vary significantly and are influenced by several key parameters: type of exploit, criticality and prevalence of systems, number of sales, uniqueness of the offer, and reputation of the seller.

Type of exploit

Zero-day exploits are among the most coveted and most expensive. They target undisclosed vulnerabilities that are unknown to software vendors. When a relatively new exploit for a vulnerability is developed, it will initially command high prices due to its novelty and effectiveness before any defences are in place. However, as vendors become aware of the vulnerability and release patches to fix it, and as more users apply these updates, the effectiveness of the exploit diminishes. As a result, demand decreases, leading to a significant decline in its market value.

In contrast, exploits that target known vulnerabilities, especially those with available patches, are less valuable but still useful for attacking systems that have not been updated.

We have analysed the statistics for offers, with a specific focus on zero-day exploit offers to highlight their prevalence and potential impact.

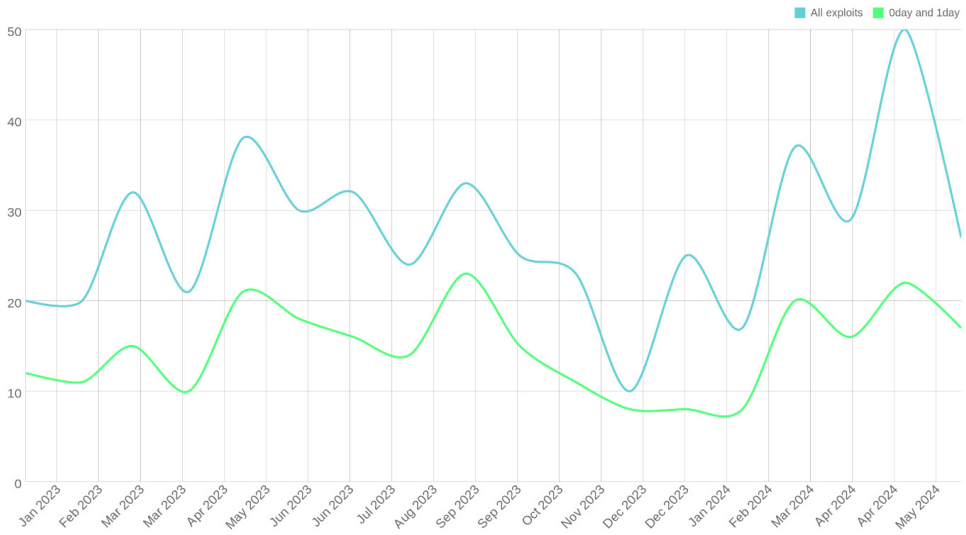


Figure 2: The distribution of messages related to buying and selling of all exploits and zero-day exploits.

The graph in Figure 2 indicates that approximately every second offer is related to a zero-day or 1-day vulnerability. This high proportion is not surprising, as the lack of available security patches for these vulnerabilities makes them highly

valuable. Experienced attackers and Advanced Persistent Threat (APT) groups are willing to pay a premium for these exploits, given their potential to bypass existing security measures and cause significant damage.

Criticality and prevalence of the system

Exploits targeting highly critical systems are particularly valuable due to the significant disruption or damage they can cause. For example, an exploit that compromises a widely used operating system or piece of software can have far-reaching consequences. It is therefore highly sought after.

The ability to infiltrate as many systems as possible, or to affect a single critical system, makes the potential rewards immense.

Number of sales

There are usually two ways to sell exploits: either selling to one buyer only, or to anyone who has an interest in the exploit. Exploits offered on an exclusive or limited basis are generally more expensive due to their scarcity and the greater potential. If an exploit is sold to only one buyer, the likelihood of the related vulnerability being quickly patched is relatively low. Conversely, exploits that are widely sold tend to be less expensive because their widespread use increases the likelihood of detection and subsequent patching by vendors.

Uniqueness of the offer

The dark web market works much like legitimate markets: when many sellers offer a similar exploit, the competition among sellers leads to lower prices. Sellers often emphasize the uniqueness of their exploits to justify higher prices and attract serious buyers.

Reputation of the seller

Experienced sellers with a history of delivering reliable and effective exploits can command higher prices because they're trusted by those buying. These reputable sellers are often preferred because they provide a level of assurance regarding the functionality of the exploit, reducing the risk of scams or ineffective purchases. A seller's reputation is influenced by positive reviews, successful transactions, and a strong track record. Conversely, new or unverified sellers may have difficulty gaining trust and may have to offer lower prices or additional guarantees to attract buyers.

However, in very few cases, the deals are unproven and entirely based on reputation. In most cases, the sale is made in accordance with the established rules of the transaction.

The sellers of exploits typically focus on discovering, developing and selling different types of exploits rather than offering a single exploit. Among the sellers, we discovered a diverse range of operators, including ransomware developers, teams of bug hunters, and even some who have established their own websites for selling exploits.

For some cybercriminals, selling exploits is their main activity, while for others it is a one-time source of income. Figure 3 illustrates the distribution of exploit sales by individual users on the dark web. It reveals that the majority of sellers, accounting for 57%, engage in a single transaction only. This suggests a high turnover rate or a cautious approach to avoid detection and maintain anonymity. In contrast, a small fraction of users, about 7%, sell more than five exploits, indicating a presence of more established sellers who may have built a reputation and trust within the marketplace. This disparity highlights the varied engagement levels among sellers, with most opting for limited activity while a few dominate the market with multiple sales.

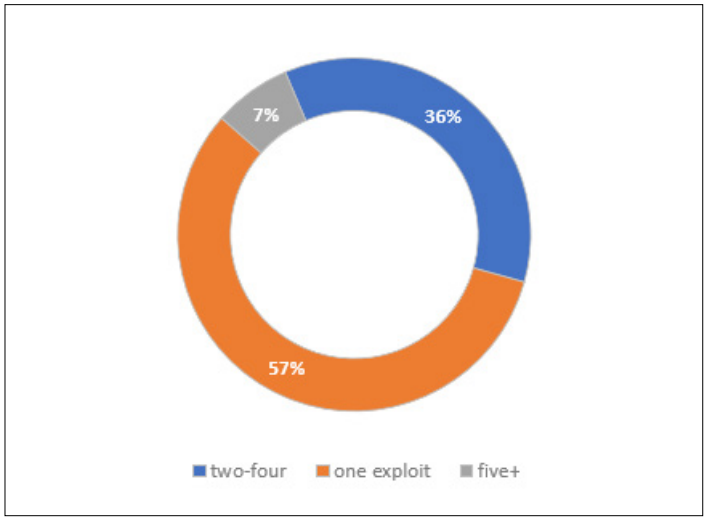


Figure 3: Statistics on sellers by numbers of offers.

Deals regulations

The dark web is an environment where trust is in short supply, both for the seller and the buyer. The buyer may not pay for a service or goods, the seller may take the money and be on his way. For this reason, escrow services (or 'guarantors') have a critical role to play in the facilitation of transactions. These agents act as neutral third parties, holding the buyer's payment until the seller delivers the promised product or service.

The escrow service may be specially organized and supported by a dark web platform, or such services may be provided by a third party who is not interested in the results of the arrangement (also a member of the cybercrime community) [2].

The majority of advertisements offering exploits only accept escrow agents for deals.

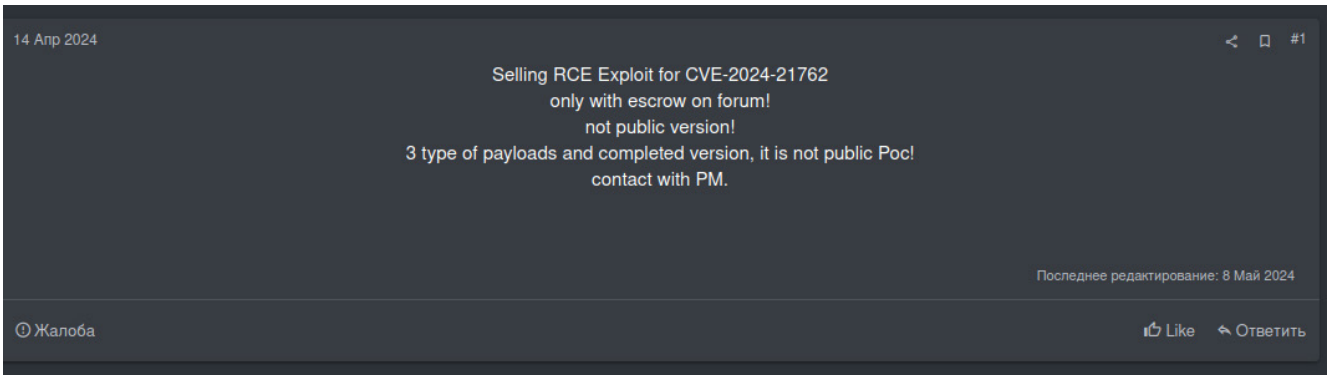


Figure 4: An example of an advertisement where only the escrow agent is accepted.

Exploits are rarely sold without an escrow service and proof from the seller, except in exceptional circumstances. Such cases are usually only possible if the seller has an excellent reputation. Otherwise, these deals tend to arouse suspicion among members of cybercriminal forums and damage the seller's credibility within the community.

Translation:
All sold to an anonymous buyer on an honest-to-goodness basis with no escrow.
You can keep the topic open

Figure 5: Comment that the exploit was sold without escrow.

Exploit cost analysis

For more accurate pricing, it is essential to examine the offerings based on the type of exploit. Exploits can be classified into several categories based on their target. Enterprise-focused exploits are designed to penetrate corporate networks, business applications, and enterprise-level software solutions. Exploits targeting ordinary users typically focus on consumer software, such as web browsers, email clients, and popular applications. Lastly, physical-level device exploits target hardware components, such as IoT devices, routers, and other network infrastructure.

Within the classification of exploits, a closer examination of specific software products commonly targeted by cybercriminals reveals valuable insights. We analysed these offers and statistical data on the average pricing for such products.

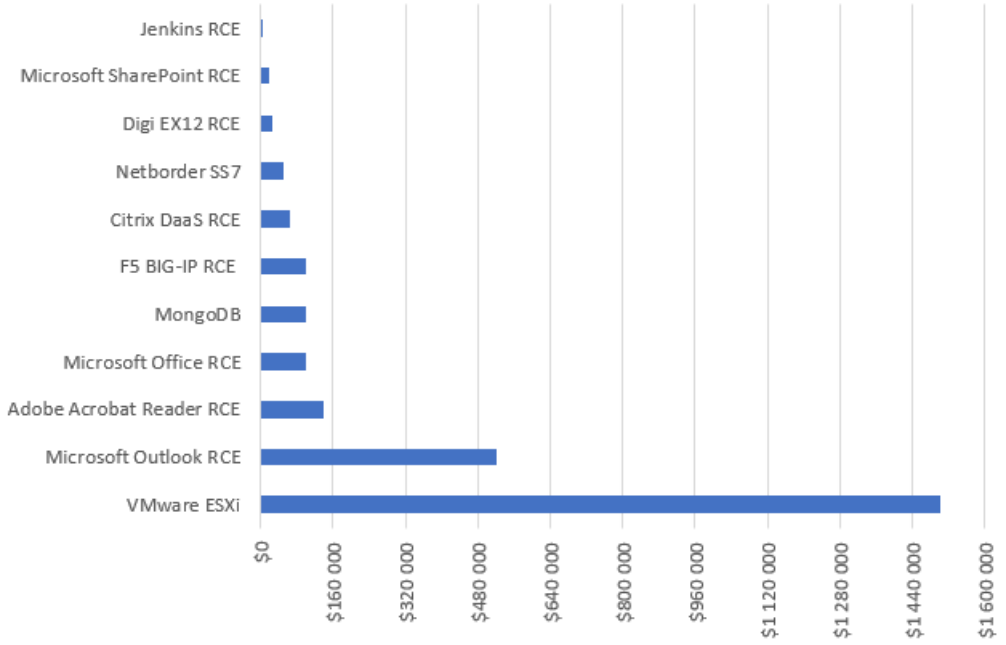


Figure 6: Distribution of exploit price based on software.

It comes as no surprise that the most desirable and expensive exploits often target enterprise-level software.

On 14 May 2024 a new zero-day exploit for *Microsoft Outlook* appeared on a popular dark web forum with a staggering price tag of $1.8 million (previous zero-day exploits for *Microsoft Outlook* were offered for prices ranging from $100 to $300,000[3]). The high price has sparked intense debate in the community and among security experts, who question its value and speculate whether anyone will buy it. However, this *Outlook* exploit is not the most expensive exploit ever seen on the market.

The most expensive exploit recorded in the period analysed targeted the *Magento* open-source e-commerce platform, with a price set at 100 bitcoin (BTC). This high-value exploit was sold exclusively through private message discussions and required the use of an escrow service to facilitate the transaction, ensuring a level of security and trust between the buyer and seller.

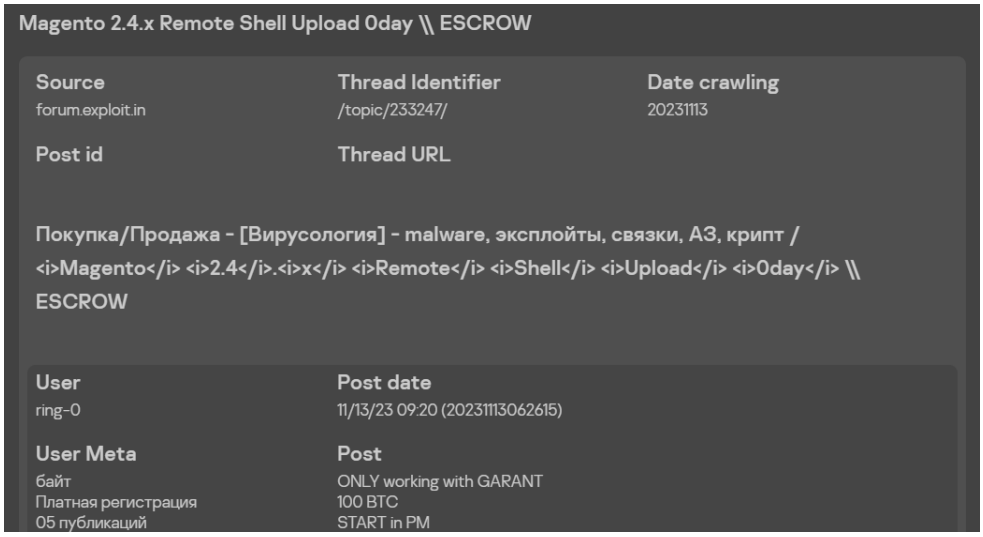


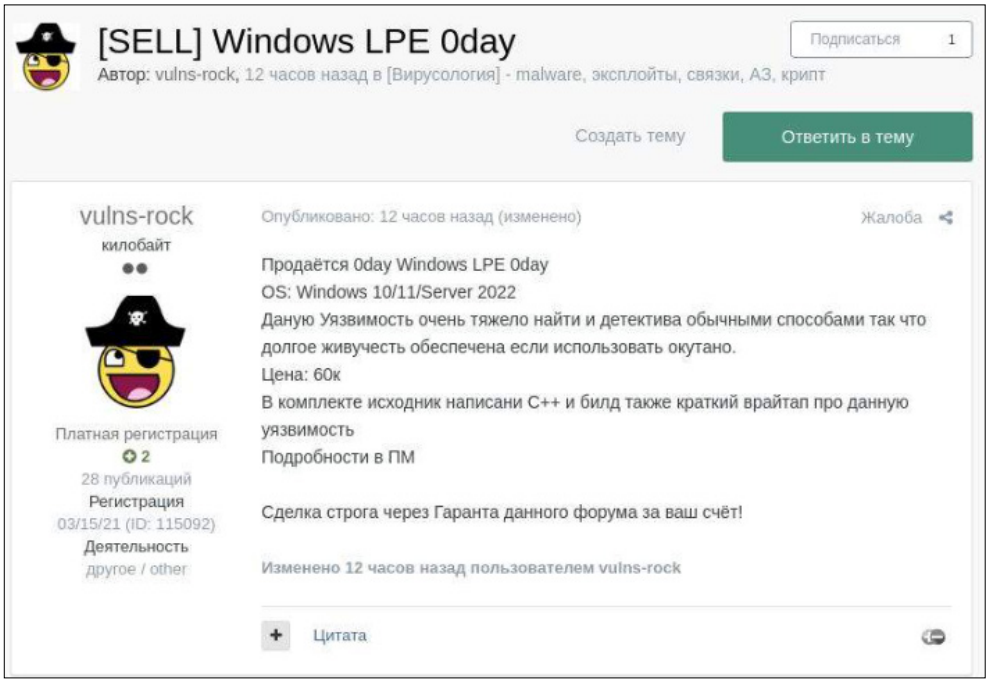
Figure 7: Offer of the Magento exploit (screenshot obtained from internal Kaspersky dark web monitoring system).

Pricing policies and disparities can be observed when examining *Windows* Local Privilege Escalation (LPE) exploit offerings. LPE exploits targeting *Windows* operating systems can vary significantly in terms of their effectiveness, reliability, and potential impact. Factors such as the exploit's compatibility with different *Windows* versions, its ease of use, and the level of access it provides are crucial considerations.

[3] During the research period of January 2023 to May 2024.

The price of zero-day exploits typically ranges $60,000 to $250,000. Meanwhile, 1-day exploits, which target vulnerabilities that have been disclosed but not yet patched, are typically offered at lower prices, ranging from $500 to $10,000.

Figure 8: Offer of the Windows LPE zero-day exploit (screenshot obtained from internal Kaspersky dark web monitoring system).



Translation:

Post message:

For Sale 0-day Windows LPE 0day

OS: Windows 10/11/Server 2022

This vulnerability is very hard to find and detect by normal means so long survivability is ensured if used shrouded.

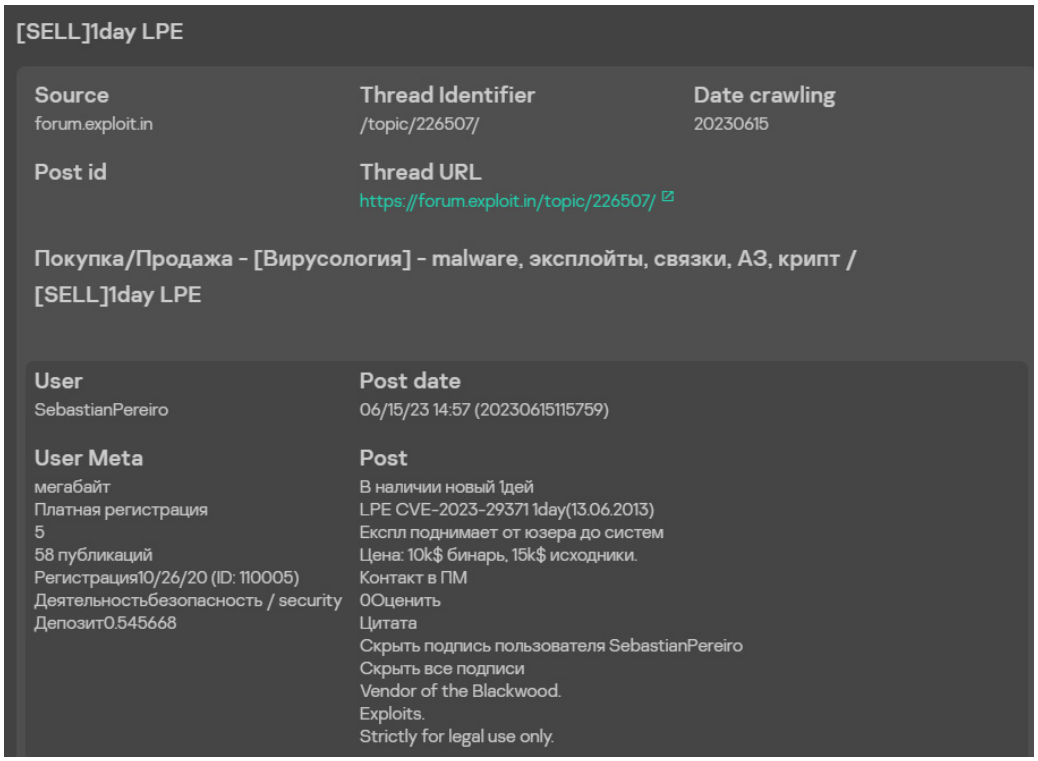
Price: 60k

Included source code written in C++ and build also a brief writeup about this vulnerability.

Details in PM

Deal strictly through the guarantor of this forum at your expense!

Figure 9: Offer of the Windows LPE zero-day exploit.



Translation:

Post message:

New 1day in stock

LPE CVE-2023-29371 1day (06/13/2013)

Exploitation raises from user to systems

Price: 10k$ binary, 15k$ sources

Contact in PM

Figure 10: Offer of the Windows LPE 1-day exploit (screenshot obtained from internal Kaspersky dark web monitoring system).

EXPLOIT SCAMS

Scams involving exploits take various forms, ranging from sellers providing incomplete or non-functional exploits to outright fraudulent transactions where buyers are deceived into paying for non-existent exploits.

In some cases, scammers may even offer exploits that claim to target zero-day vulnerabilities but are actually ineffective or recycled from previously disclosed vulnerabilities. This is why cybercriminals frequently leave comments under exploit posts when they harbour suspicions about the authenticity of the offered exploits. These comments serve as a form of community policing, where individuals within the dark web marketplace scrutinize and evaluate the legitimacy of the posted exploits. Common suspicions may arise due to discrepancies in the seller's claims, lack of sufficient proof-of-concepts, or unusually high prices. By voicing their doubts and concerns publicly, cybercriminals aim to warn others within the community and prevent potential scams or fraudulent transactions.

For example, under a post offering a zero-day for an ICS device a user expresses scepticism regarding the value and legitimacy of the '0day' exploit being discussed. The commenter suggests that the exploit may not truly be a zero-day vulnerability but rather a result of an exposed service or poor configuration, indicating that it may not be as sophisticated or exclusive as claimed. Overall, the commenter raises doubts about the exploit's effectiveness and the rationale behind the high price tag attached to it.

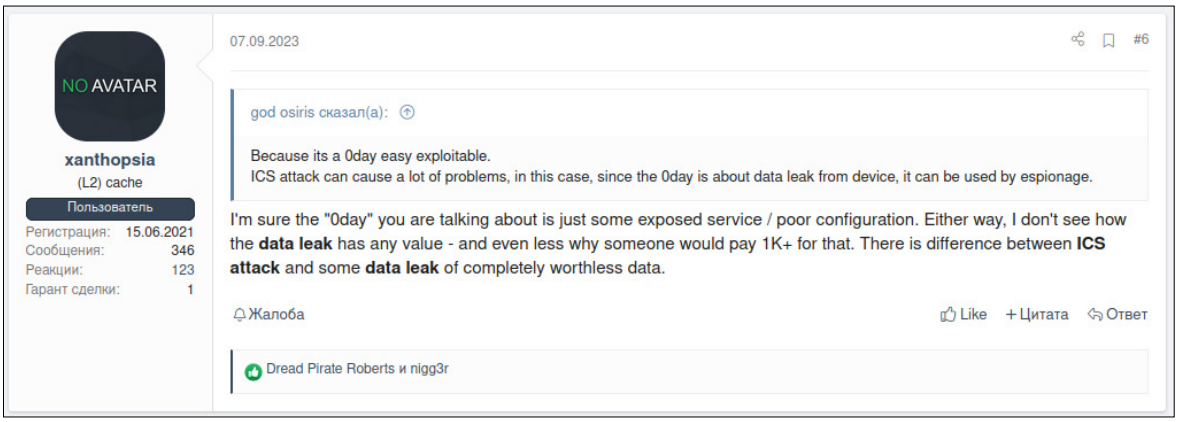


Figure 11: Comment under the offer of a zero-day for an ICS device.

Therefore, these comments play a crucial role in fostering transparency and accountability within the dark web marketplace, helping cybercriminals to mitigate the risks associated with exploit acquisitions.

CONCLUSION

Our study of the economics of exploits on the dark web has shed light on the complex dynamics that shape this underground market. We have delved into the factors influencing exploit pricing, ranging from system criticality and exploit type to the reputation of sellers. Prices are based on the perceived value of the customer and the complexity of each transaction in the dark web exploit economy. Moreover, to ensure trust and security in transactions, deals are often facilitated through escrow services. These intermediaries provide a secure platform where funds are held until both parties fulfil their obligations, minimizing the risk of fraud or disputes. In addition, our analysis has revealed the prevalence of scams and the importance of community policing in verifying the authenticity of exploit offerings.

The dynamic nature of the exploit market reflects the critical role that timely software updates and patches play in mitigating security risks and reducing the profitability of exploiting vulnerabilities, making dark web monitoring and cyber threat intelligence a valuable source of information about potential incidents.

REFERENCES

[1] Kaspersky. Incident response analyst report 2023. 14 May 2024. https://securelist.com/kaspersky-incident-response-report-2023/112504/.

[2] Kholopova, V. Business on the dark web: deals and regulatory mechanisms. SecureList. 15 March 2023. https://securelist.com/dark-web-deals-and-regulations/109034/.