Deep and Dark Web 101

netcraft

Introduction:

Cybercriminal forums, illicit marketplaces, and underground communication channels continue to influence the global threat landscape. These spaces, which often operate on the deep or dark web, allow criminals to exchange tools, publish stolen data, sell access, and coordinate attacks while maintaining anonymity. For defenders, understanding how these platforms function is essential because they often reveal the earliest indicators of emerging threats.

This report provides an educational overview of the main types of cybercriminal platforms, how threat actors engage with them, and why continuous monitoring of these ecosystems is critical for organizations. It also explains how Netcraft protects customers by identifying exposed credentials, carding data, domain mentions, and early warning signals that can prevent incidents.

What Are Cybercriminal Forums and Platforms?

Cybercriminal platforms take several forms, each supporting different parts of the underground economy.

- **Forums:** Knowledge sharing, trading, buying and selling illicit goods, recruitment, and collaboration.
- **Marketplaces:** E-commerce style platforms selling illicit goods.
- **Messaging Platforms:** Real-time communication channels with public and private groups, often used similarly to forums and used by groups to announce attacks.
- **Automated Vending Carts (AVCs):** Automated shops for illicit goods such as stolen databases and credentials, often with no user interaction.

Forums:

These are structured much like any other community forum. However, cybercriminals use these discussion-based communities to exchange knowledge with detailed guides, share or sell tools, recruit members to their groups, and advertise general illicit goods and services.

These forums are often split into various sections for tutorials, code sharing, database trading, and selling access to compromised organizations. They often operate on a reputation-based system, where credibility is built through feedback and escrow mechanisms that help facilitate trust between anonymous users. Some notable examples of these forums include the Russian-language cybercriminal forums XSS and Exploit, and English-language cybercriminal forums like Cracked, Nulled, and Leakbase.

Such forums lower the barrier to entry for aspiring cybercriminals, as many tools, scripts, and compromised data can be purchased or downloaded with minimal effort. This allows less experienced individuals to conduct attacks using pre-built resources, without needing to compromise systems or steal data themselves.

In addition, many established forums enforce strict rules governing user behavior. For example, prohibiting activity targeting specific sectors and geography. This is especially true for XSS, where users are not allowed to post data relating to Commonwealth of Independent States (CIS). These rules are actively monitored and enforced by forum staff to maintain stability, reduce unwanted law-enforcement attention, and preserve the forum's reputation among its users.

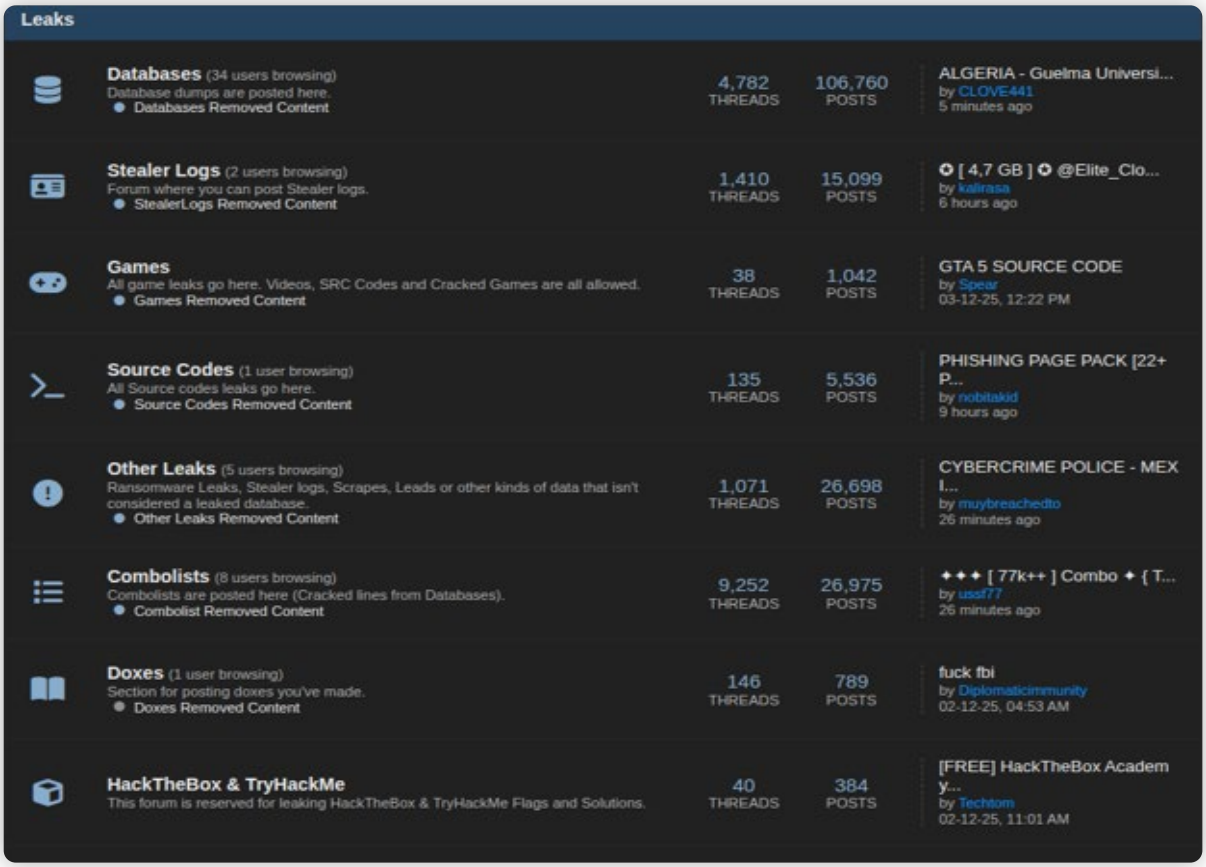
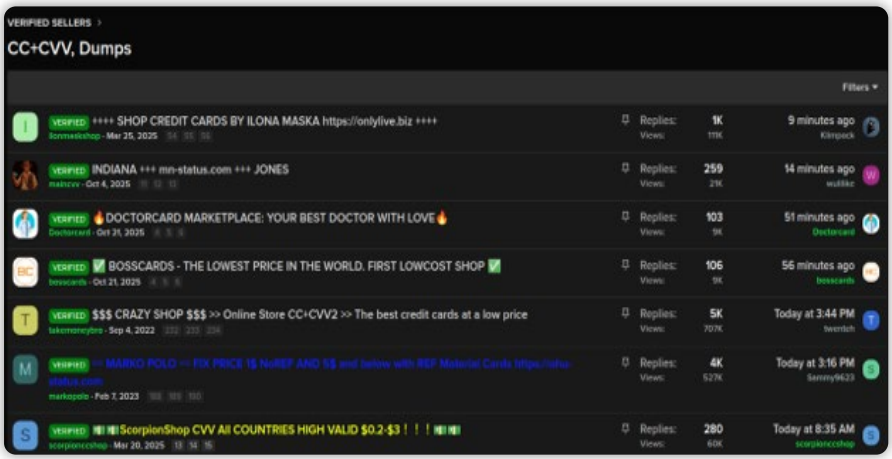


Figure 1: HackForums homepage

Underground Marketplaces:

Marketplaces operate much like traditional e-commerce platforms but focus exclusively on illicit digital goods and services. Vendors advertise products such as stolen credentials, malware, fake documents, or exploit kits, where buyers use cryptocurrency payments to complete transactions.

These platforms often feature product listings, vendor ratings, and customer reviews, giving them a surprisingly polished commercial structure. Transactions are also typically mediated via escrow services that hold payment until the buyer confirms delivery, helping reduce scams, while maintaining credibility within the criminal community.



These marketplaces cater to a wide variety of individuals, from individual threat actors seeking quick access to data, to organized groups buying large volumes of stolen information or custom tools.

Automated Vending Carts (AVCs)

AVCs often operate as fully automated shops that sell stolen data without requiring interaction between the buyer and the seller. These types of shops are typically fast, simple, and highly scalable, which makes them attractive to both low skilled and experienced attackers who want immediate access to compromised information.

Buyers can browse inventory by specific criteria and purchase through cryptocurrency payments. AVCs frequently list infostealer logs, compromised credentials for online accounts, browser cookies, access to compromised hosting panels, and even remote access credentials to corporate systems.

Due to the automation, these shops can distribute thousands of compromised accounts, turning stolen data into an easily accessible commodity. In addition, because there is little to no interaction between buyers and sellers, many AVCs do not require user accounts at all, or they allow entirely public access.

This lack of identifiable user activity makes it far more difficult to determine who is purchasing the data and who is operating the shop, which significantly complicates attribution and investigative efforts. A notable example of an AVC is Russian Market, which hosts stolen credentials obtained via infostealers, and sold for as little as $2 to $10 per log pack.

Messaging Platforms:

Messaging platforms such as Telegram and Discord have become very popular in the cybercriminal community because they combine real time communication, and large group capacity. The anonymity features and channel model of Telegram make it attractive. Threat actors can create public broadcast channels, private groups, or invite only rooms to advertise goods, share stolen data, or coordinate activity while retaining a degree of privacy. For example, hacktivist collectives, such as Killnet and NoName057(16) use Telegram channels to announce operations, recruit members and other groups, and coordinate Distributed-Denial-of-Service (DDoS) campaigns, allowing them to publicly claim responsibility.

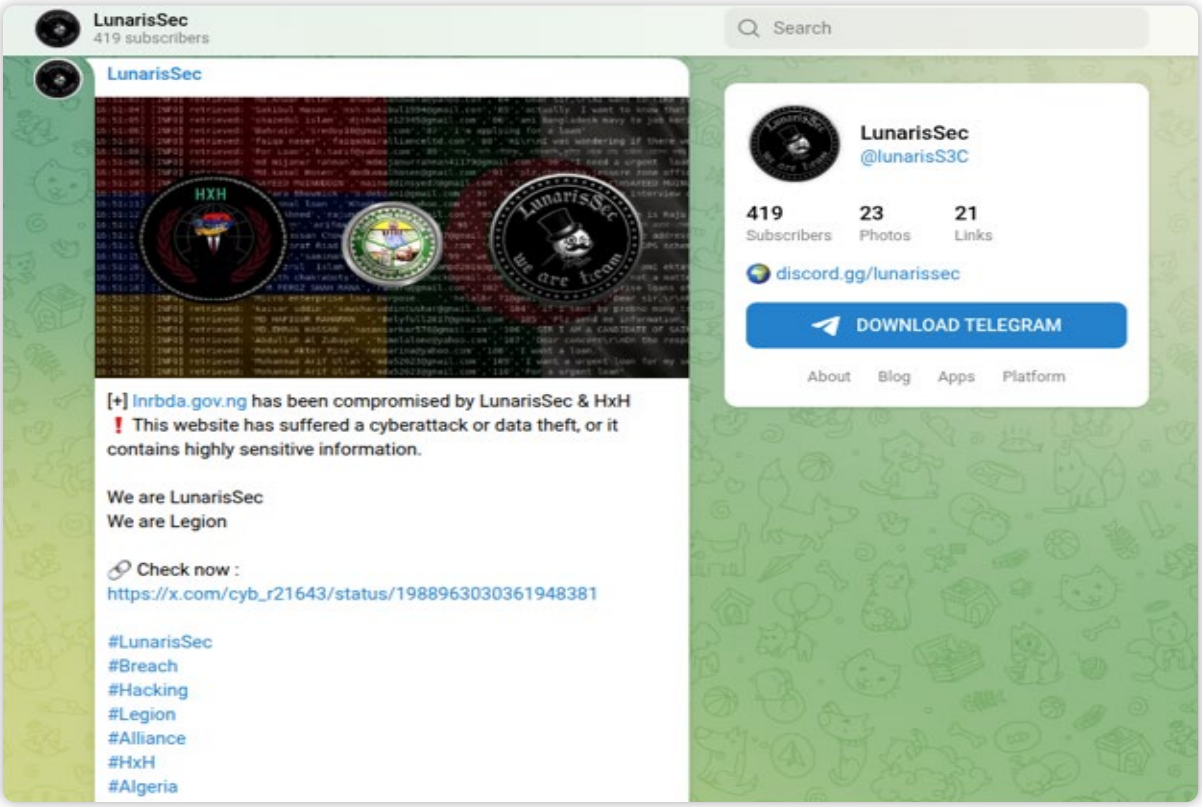


Figure 2: Telegram channel of cybercriminal group claiming responsibility for attacks

Organizations should consider monitoring Telegram as these groups typically will announce their future attacks, giving organizations a heads-up in a sense. Discord, while not as popular as Telegram, allows cybercriminals to create and join servers with segregated channels for different purposes. This includes announcements, sales, recruitment, tutorials, and OPSEC discussions, like cybercriminal forums.

Because these Discord and Telegram channels can be set to private, requiring invite links, they are more difficult to archive and monitor than static web pages. These channels and servers often can be very noisy, with a mix of low-value and high-value signals. For instance, a single server may contain both casual bragging and concrete sales of access or data. This means that defenders monitoring these should focus on signals of intent and impact, meaning mentions of targeted organizations, leaked credentials, advertised access, or calls for mass action, rather than volume alone.

How Netcraft Monitors These Spaces and Protects Customers

Netcraft continuously monitors these cybercriminal platforms, providing customers with early detection of threats that may directly impact customers.

Credential Exposure:

- Leaked credentials
- Stealer logs

Early detection enables organizations to reset credentials before attackers use them, which helps prevent account compromise, lateral movement, and potentially ransomware deployment.

Carding and Financial Data:

- Compromised card information
- Carding community trading activity

Financial organizations can block fraudulent transactions or replace affected cards quickly, reducing financial loss.

Domain and Brand Mentions

- Mentions of domains
- Discussions involving targeted brands
- Access sales linked to customer infrastructure
- Phishing kits impersonating customers
- Leaked internal system information.

Early warnings allow security teams to take action before an attack becomes operational. This includes phishing takedowns, credential resets, and proactive defensive measures.

Why This Monitoring is Critical

Cybercriminal activity often begins long before an attack is launched. Credentials leak before intrusions occur. Domains are discussed before phishing infrastructure is deployed. Access is advertised before exploitation takes place. This intelligence reduces risk by transforming early-stage criminal activity into actionable insights.