RAPID7

INFILTRATE AND ESCALATE: THE 2025 ACCESS BROKERS REPORT

AUTHORS:

Chris Boyd, Lead Threat Researcher

Jeremy Makowski, Sr. Threat Intelligence Researcher

Antony Parks, Threat Intelligence Researcher

Itamar Pinchas, Sr. Threat Intelligence Researcher

Maor Weinberger, Sr. Threat Intelligence Researcher

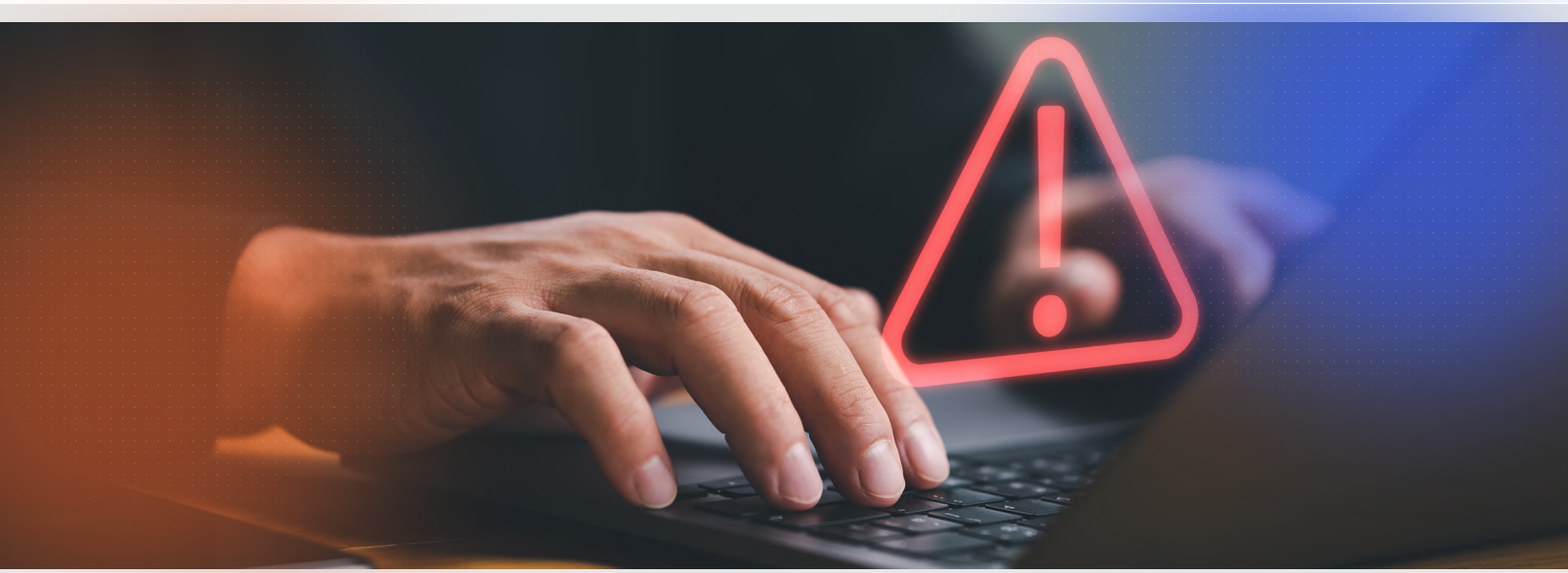
THREAT RESEARCH REPORT

Executive Summary

Network access is the key to both private and organizational systems, and to the information stored upon them. Some of this information is of significant value, and so Initial Access Brokers (IABs) have taken up residence on dark web forums, selling network access to the highest bidders.

These forums, digital bazaars of an endless supply of compromised networks, place unauthorized access directly into the hands of those who most want it. Whether it's a professional threat actor wanting to skip the early-stage hassle of mapping out an Initial Access Vector (IAV), or a newcomer lacking the technical skills to clear the first hurdle, a network of websites is on hand to give them what they need.

Brokers use a variety of tactics to gain a foothold into a network before going on to offer it up for sale. System vulnerabilities, phishing, social engineering, or malware may be used in order to obtain initial access. Pricing may be at least partially based around the time or complexity used to gain access. Low-hanging fruit is ideal for an IAB operation. Weak or absent multi-factor authentication (MFA), exposed and vulnerable devices, reused passwords — anything which means access is compromised so a broker can move on to their next target.



There are several access broker forums on the dark web, and over time these forums change administrative ownership as well as availability. This is especially the case during major law enforcement operations, which involve individual arrests and site takedowns. Regardless, access brokers are a perpetual threat to organizations, and while the platforms they use may change, the insights researchers can gather from them remain valid.

Exploit, BreachForums, and XSS have long been recognized as key hubs within the cybercriminal ecosystem. Rapid7 threat intelligence researchers tracked and analyzed activity within these three forums from July 1 through December 31, 2024, with a primary goal of point-in-time benchmarking and reporting on IAB activity, including TTPs, initial access vectors, pricing strategies, and more.

We chose to analyze these three forums due to their low signal-to-noise ratio and concentration of technically adept threat actors. These forums have served as marketplaces for some of the most trusted and well-connected sellers, often brokers of initial access, data leaks, and exploit kits closely aligned with emerging trends in cybercrime. As such, they provide valuable intelligence for security researchers seeking to analyze market trends, threat actor behavior, and the evolving demand for specific access types. Monitoring activity on these platforms, especially from prolific, reputable brokers, offers a critical perspective into the shifting tactics and priorities within the cybercriminal underground.

The detailed findings of our analysis are shared within this research report, along with further insights into what these findings mean for organizational and security leaders. Also included in this report are a series of recommendations for protecting your business from the one-two punch of IAB compromises.

Key Findings

Our detailed analysis of six months of data from Exploit, XSS, and BreachForums reveals the following key findings:

- The vast majority of access broker sales (71.4%) offer more than just a specific access vector; they also include a level of privilege — and in nearly 10% of those sales, it's a bundle with multiple IAVs and/or privileges.
- The low cost and variety of offerings are an attractive proposition for threat actors of any skill level. The average base price of a sale across all 3 forums is just over $2,700 — with a majority of sales grouping around the $500 to $1,000 range.
- The most popular access vectors offered for sale are equitably observed in Rapid7's incident response data. These are VPN (23.5%) and Domain User (19.9%) access, which are categorized by Rapid7 as valid accounts without sufficient MFA, and RDP (16.7%) — a remote desktop protocol service that the organization left exposed.

The first two findings highlight the diversity of options available for would-be attackers, tied to a business model where initial access to victims is both inexpensive and easy to obtain. The heavy lifting has been addressed by the access broker; all the willing buyer has to do is pay a few hundred dollars to gain immediate access to an already compromised business. In the end, they've gotten into your business for as little as $500 and your business has lost upwards of $5 million (or more).

In the third key finding, we see that compromised accounts are involved in two of the top three most popular access types being sold by brokers. The most popular means of access the broker is selling, VPN, was meant to ensure that only authorized users can access an organization's network; instead, this access management technology is being undermined. Add to that a user account with Admin privileges and you have

In the end, they've gotten into your business for as little as $500 and your business has lost upwards of $5 million (or more).

some real issues on your hands, which is why, for example, we see so many third party service provider breaches in the news.

Other top access vectors on the network edge make it clear that security basics, such as properly enabled MFA and scheduled software updates, are being missed. However, Initial access is only the beginning. Once this is achieved, brokers are intent upon finding ways to pivot within the network so that they can add value to their offer. While the broker's primary goal is always to get in and out as quickly as possible while remaining undetected, any opportunity for SOC teams and their tools to catch them is one to be seized upon.

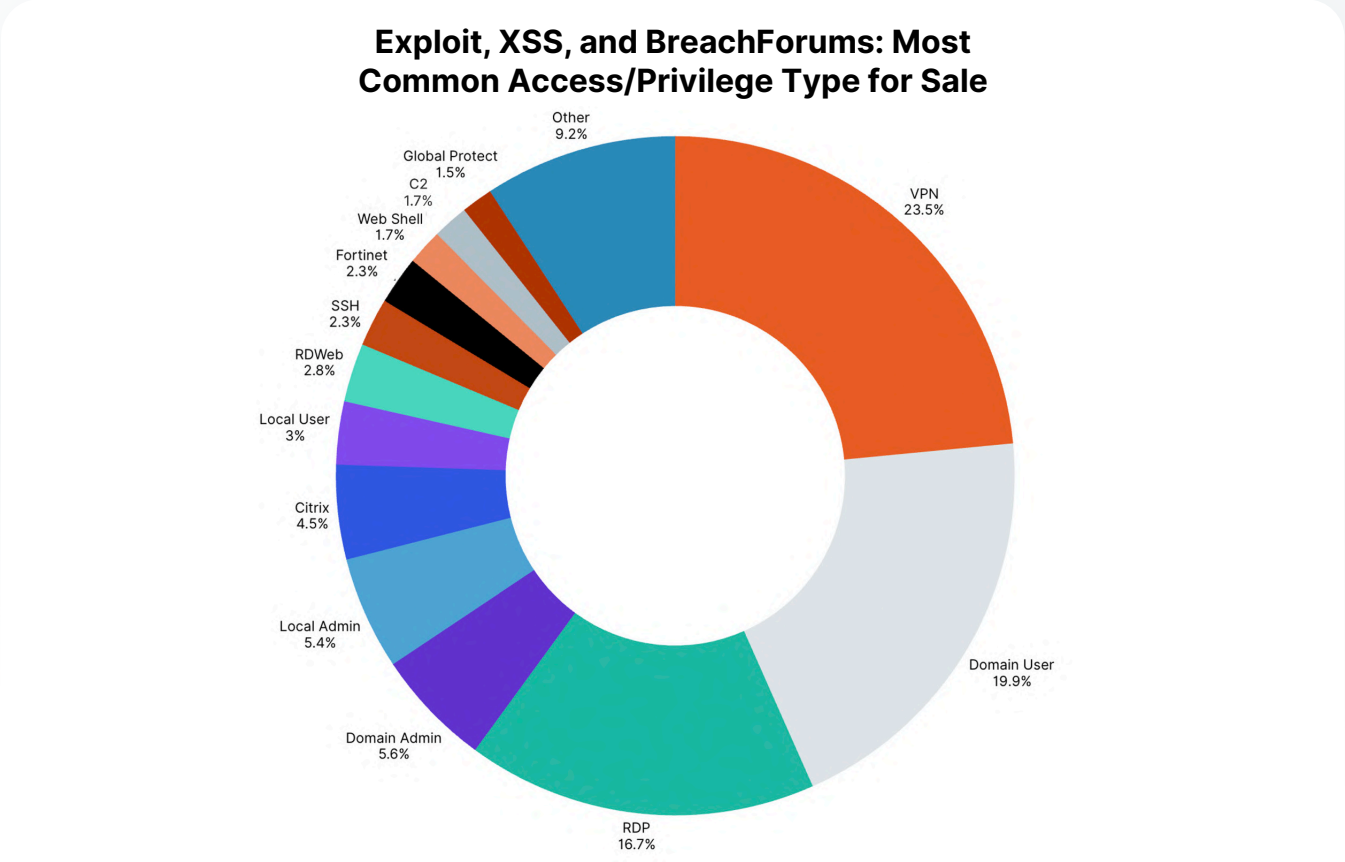
The fact of the matter is, though, once your organization's access is up for sale on a broker forum, you've already been compromised — and to what level, you don't know. Regardless, you're on a path to being further compromised, so understanding how these brokers operate is critical to disrupting the process as early as possible.

Exploit, XSS, BreachForums: Combined Data Analysis

In this section, we analyze data from our three target forums to reveal key trends in their marketplace activity. We break down victim revenue, uncover the most popular forms of initial access for sale, and explore how forum sales go from basic access all the way to bundled offerings. We also highlight the combined average base price of Exploit, XSS, and BreachForums, illustrating which offering types buyers are most likely to encounter within the average price range.

Initial access vectors

If your day job is Incident Response, you're likely to be familiar with the most popular forms of access/privilege offered for sale:



As we see in the chart above, VPN leads the pack, appearing in 23.5% of sales across all three forums. Domain User takes second place (19.9%), with RDP not far behind with 16.7% of the overall total. Fourth spot goes to Domain Admin, quite a way behind with 5.5%, and Local Admin sits at 5.4%. These combinations of VPN, RDP, and Domain/Admin User accounts can enable all manner of network exploration, lateral movement, and further escalation into ransomware delivery and data exfiltration.

Making a deal

Delving further into the listings we analyzed, the average combined base sale price for offerings within these forums is $2,726, and the average annual revenue of the victim organization is in the region of $2.232 billion. Along with the type(s) of access available, the broker will often use the victim organization's revenue to further entice the buyer and prove out the value of the asking price. It's important, therefore, to keep in mind that victim revenue numbers are broker-provided based on their own online research, and as such they may not necessarily be accurate.

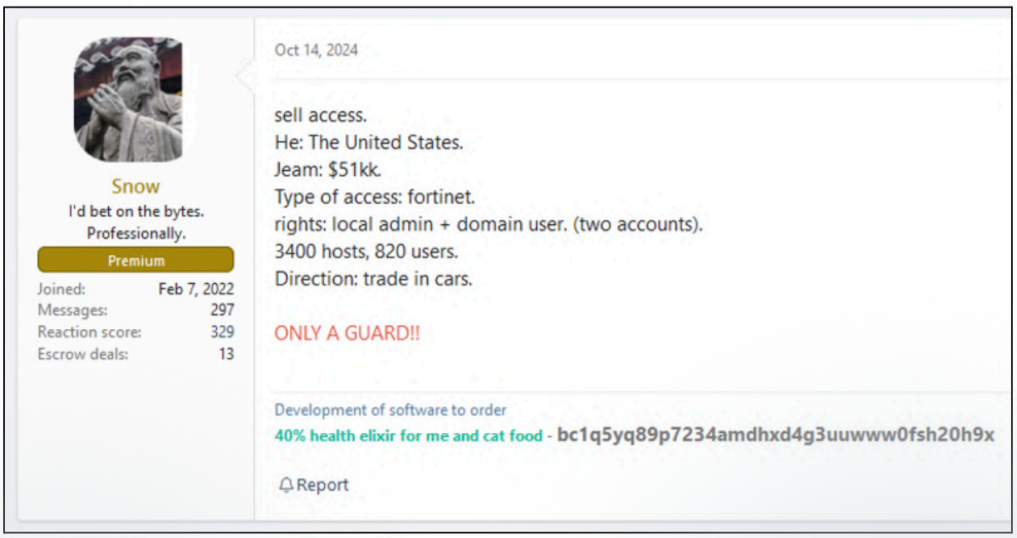
Where individual sales are concerned, pricing across Exploit, XSS, and BreachForums tends to follow a similar pattern, with some outliers — particularly on BreachForums, where at the time, access costs could reach significantly higher totals than the posts made to both XSS and Exploit. We must once again stress that there is never a guarantee that victim revenue provided by a broker is correct; one post in our dataset claims that a victim has "over $1.5T in assets under management," which sits at the upper end of claims a buyer would want to try and verify before making a purchase.

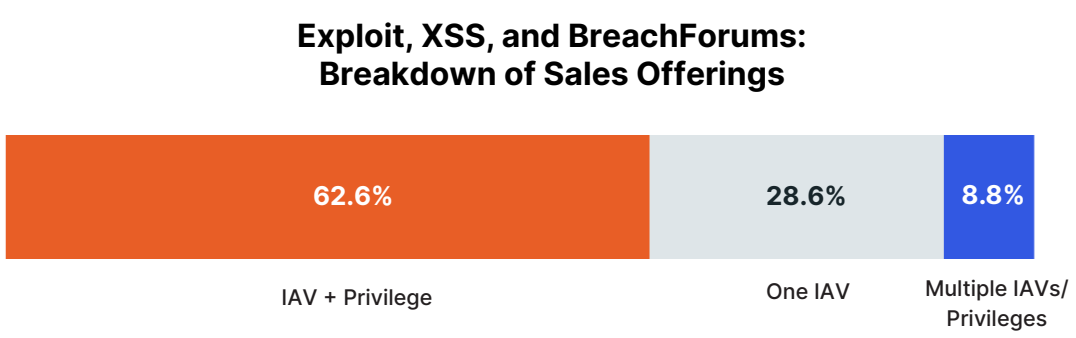
Broker sales in our data broadly fall into one of three types:

1. **A single IAV which permits access to a compromised business (28.6% of the posts Rapid7 examined).** This could be a standalone VPN sale, or standalone RDP access only — no privilege included.

2. **An IAV with one form of privilege included (62.6%).** Brokers can sweeten the deal by including a specific form of privilege, which allows for more rapid traversal of an environment. An example of this would be a sale of RDP with domain user credentials, or perhaps a combination of VPN and an admin account.

3. **Bundle deals, where the sale includes a combination of IAVs and/or privilege types (8.8%).** The seller may be offering multiple routes into a business, several forms of privilege, or a mixture of both. The main aspect of these bundles is that the broker is selling three or more compromised aspects of a business. Perhaps they're selling RDP with RDweb and Domain user, or maybe it's Fortinet with Domain User and Local Admin, like so:





The *best-case* scenario for a compromised business is that the broker "only" has one form of IAV for sale.

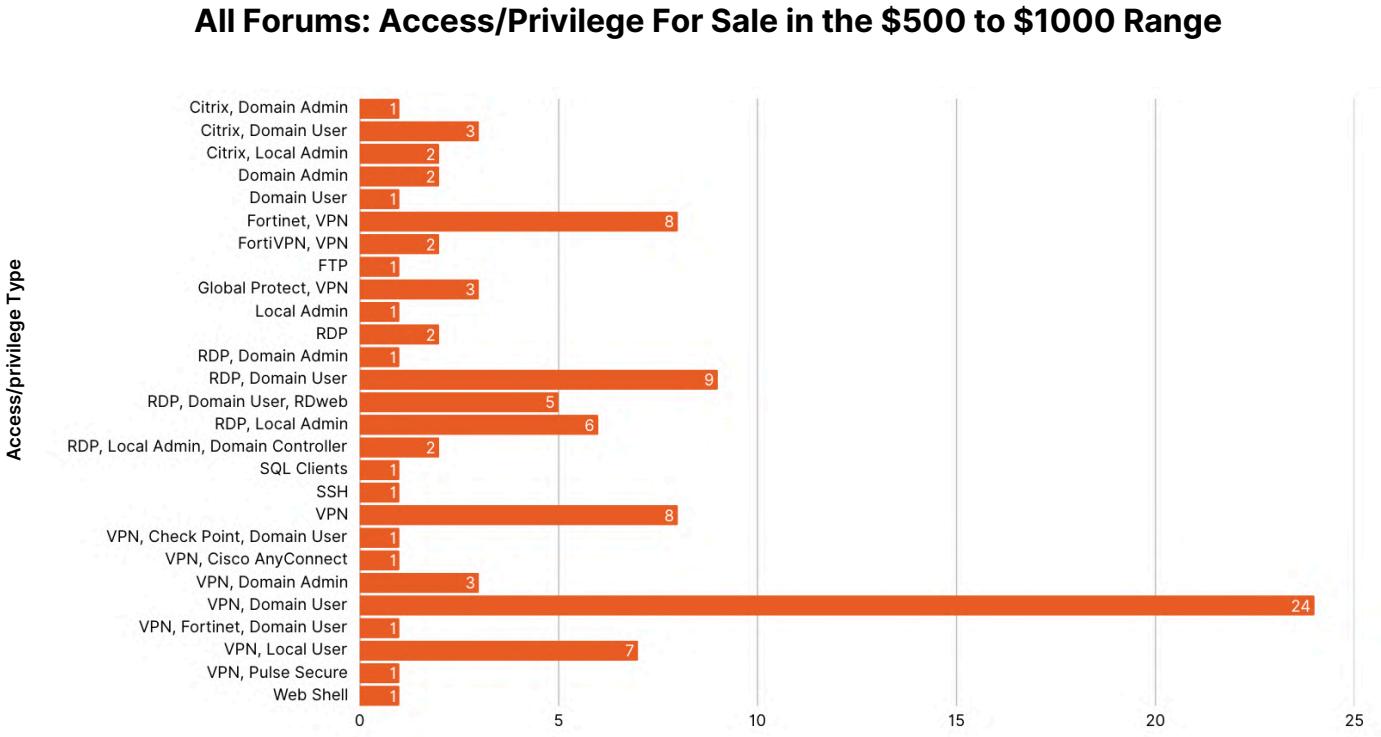
In the worst-case scenario, 71.4% of cases involve a broker potentially gaining significant progress to the victim's network, and taking at least one form of potential privilege under their wing. In this case, victims are in serious trouble *long* before a payment has been made, and that's without considering how long the broker may have lived on the network without detection.

Make no mistake, a business in this predicament is essentially being compromised twice over, by broker and buyer, and at no point has their security solution been able to detect either form of illicit access. All of this, before stopping to consider what, exactly, the broker has stolen for themselves on their way out the door — assuming they ever left.

If your business is compromised by an access broker, you're in bad shape, but if your business has somehow ended up in that 71.4% bucket, threat actors have essentially declared open season.

Popular price points

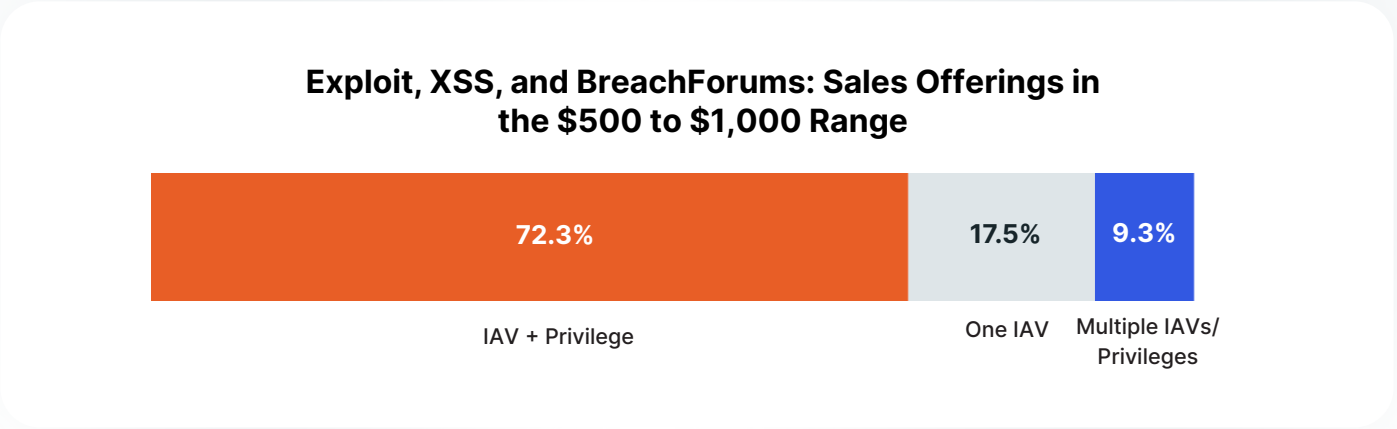
39% of all base pricing from the three forums falls inside the $500 to $1,000 range:



VPN/Domain User is the most popular form of access/privilege by some margin (24.49%), with RDP/Domain User as a standalone offering coming second with 9.18% of the total. At this point, you might not be surprised to learn that the joint third spot goes to VPN, and Fortinet/VPN (both at 8.16% respectively). Overall, 60.2% of everything in the above base price range includes some form of VPN offering — popularity that is reflected time and again in the forum data.

The saturation of VPN offerings underscores a preference for stealthy network infiltration, a problem exacerbated by the frequent pairing of additional privileges in many inexpensive sales offerings. Attackers entering by way of an access broker purchase are coming equipped with valid credentials, so they will blend in with expected VPN traffic and have no need to rely on more overt forms of compromise.

The majority of broker offerings (73%) include access and one privilege, with 9.3% offering multiple bundles of access/privilege, and 17.5% a single form of access with no privilege included.



This is how the forums operate as a whole. Next up, we'll look at what makes each individual forum tick, and what the major players get up to when selling their wares.

Individual analysis of Exploit, XSS, and BreachForums

Below is a detailed individual analysis of all three forums, exploring their history, operational methods, and key trends observed during the latter half of 2024. This includes typical illicit offerings, average base price ranges, and popular targeted regions.

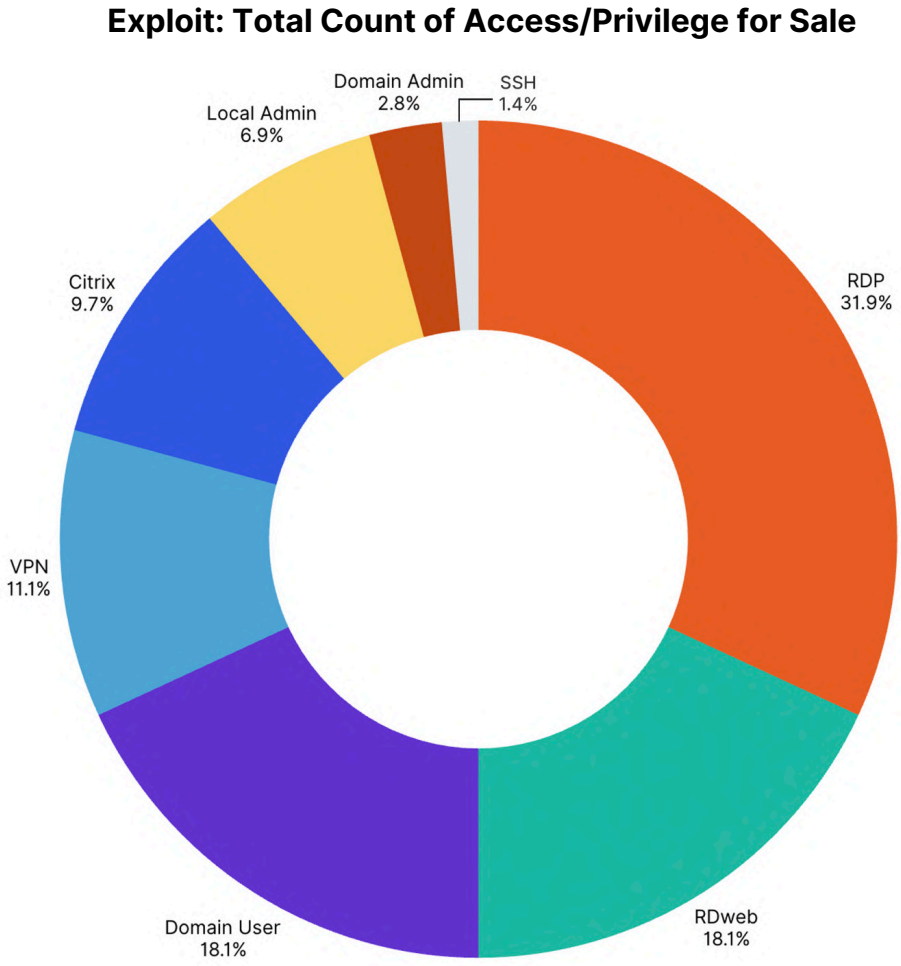
Our analysis also examines pricing strategies of some of the most prolific brokers. We identify their most favored forms of initial access and privilege for sale, which regions they prefer to target, and how their offerings help to shape these underground economies.

Exploit Forum Analysis

Exploit is a long-established (2005) Russian-language underground forum, with numerous sections outside of access brokerage. However, the marketplace is a key draw for many wanting to gain a foothold into networks for reasonable prices. It is particularly active in discussions and transactions involving zero-day vulnerabilities, high-level malware development, and access to compromised networks and infrastructure.

The forum has historically been a go-to marketplace for buying and selling corporate and government-level access. As a result, it attracts the attention of global cybersecurity operations, and intelligence gathered from Exploit often forms the basis of threat actor profiling and cyber defense strategy development.

Unlike more open platforms, Exploit enforces strict vetting processes for membership, including substantial entry fees, proof of past activity, or endorsements from known members. The forum requires a $100 fee to register a new avatar, subject to the approval of the forum admin. Regular users have access to what brokers are posting, and can purchase with or without the escrow service of the forum depending on the transaction and seller.

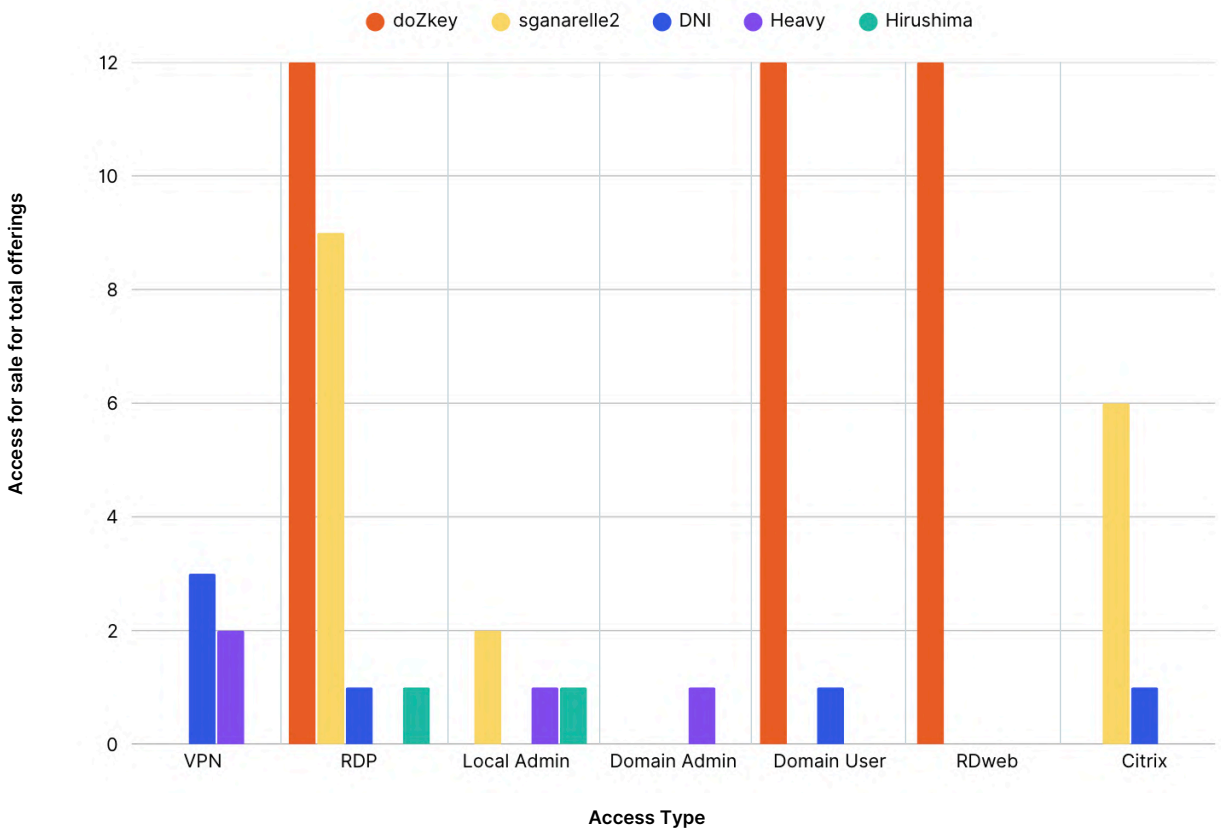


Our H2 2024 data reveals that Exploit offered up 72 forms of initial access/privilege for sale, from a total of 11 brokers. RDP was the most popular form of initial access, comprising 31.9% of everything offered up for sale. RDweb and Domain User were in joint second place (18.1%), with VPN coming in third at 11.1% of the overall total.

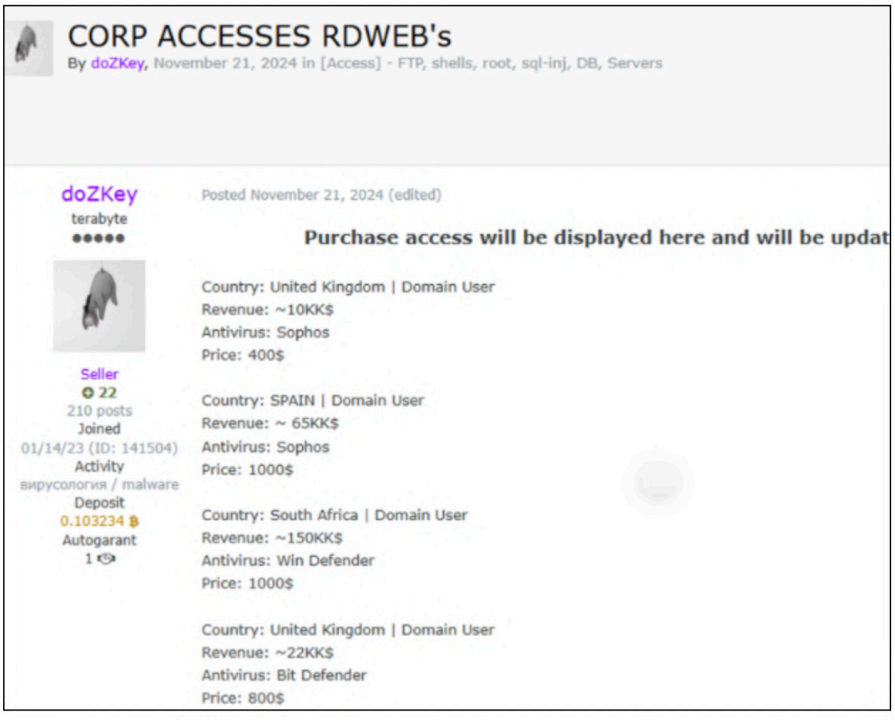
Brokers on Exploit primarily target the US (29%), with a significant drop-off in target nations beyond the top spot — the UK sits at 9%, with both Taiwan and Brazil in third place at 7%.

Exploit: Meet the Brokers

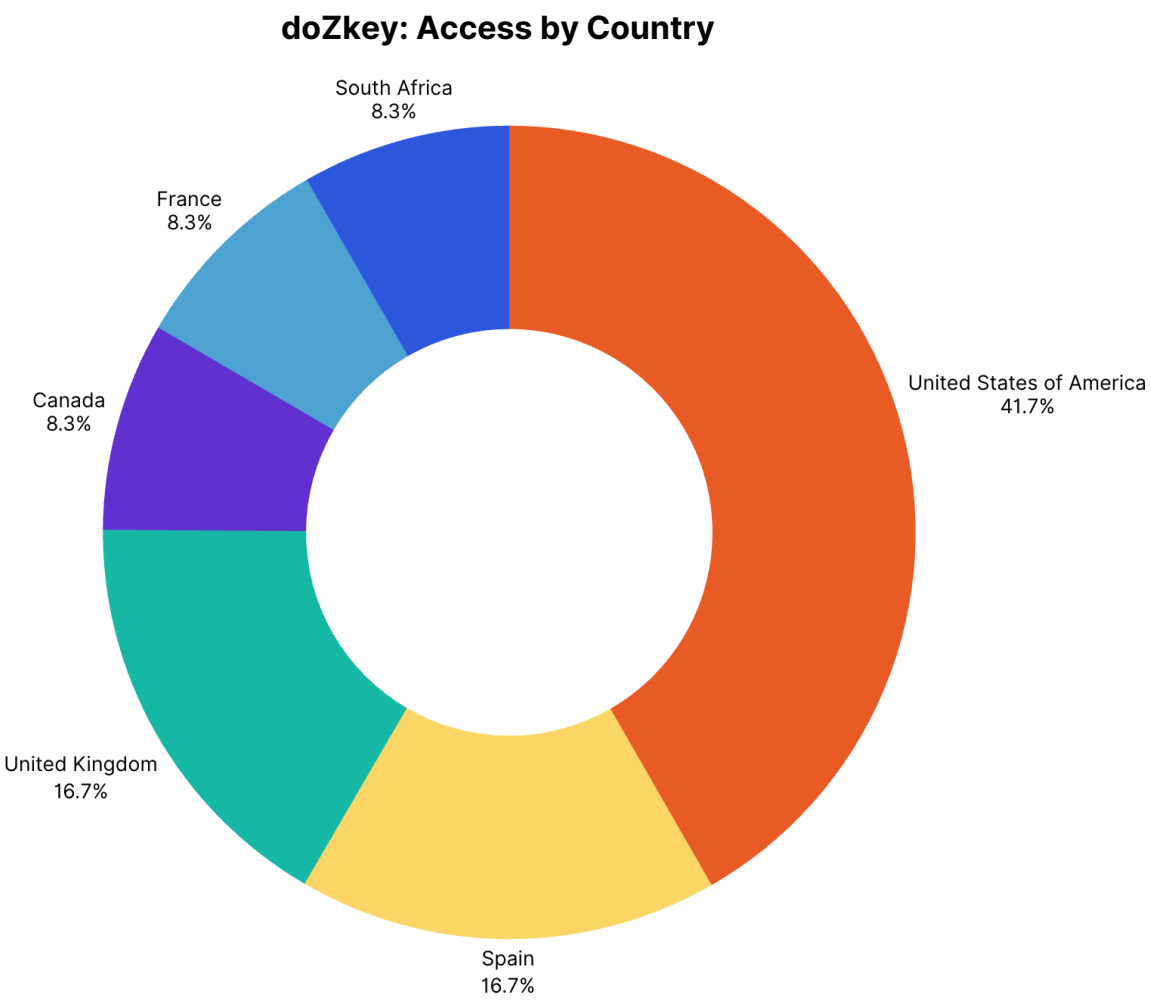
Brokers “doZKey” and “sganarelle2” made up 65.12% of all offerings on the forum, with 27.91% coming from the former and 37.21% of that total posted by the latter. To illustrate how much the broker forum was dominated by doZKey and sganarelle2, here’s the top five brokers measured by their most popular sales offerings for H2 2024:



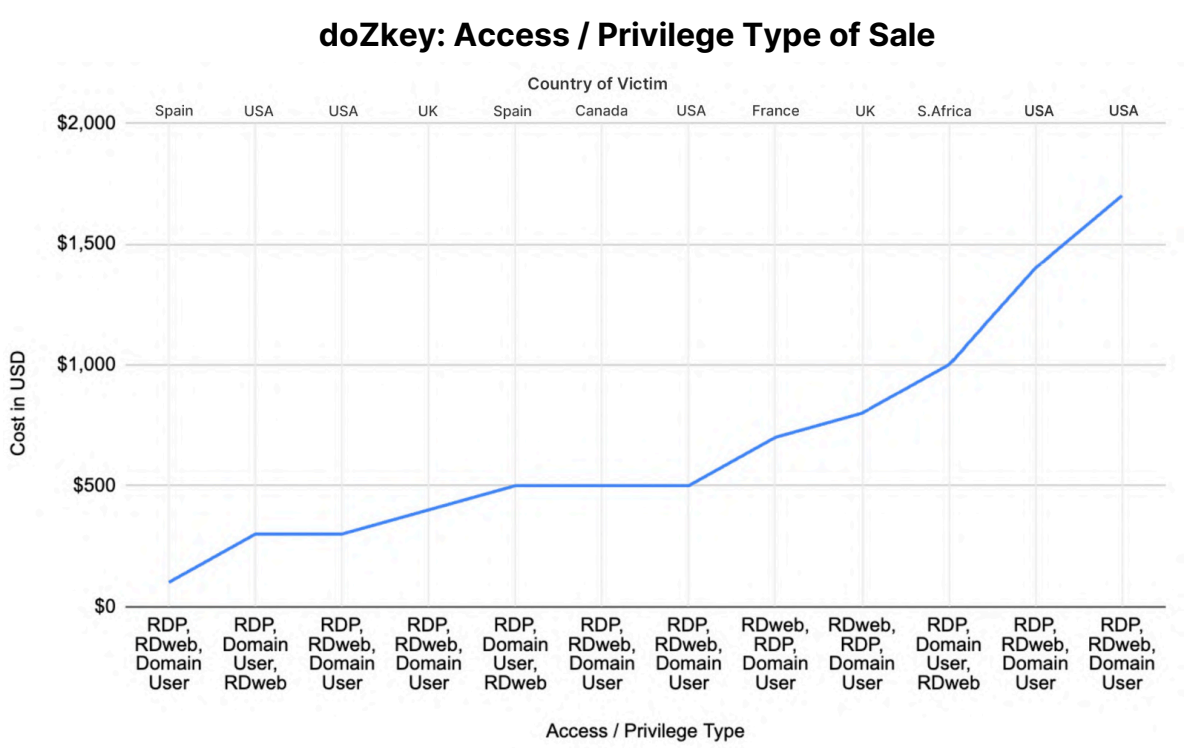
This sales forum is powered almost exclusively by just two users, and RDP, Domain User, and RDweb are mostly overwhelming the other offerings as a result. Below is a typical broker post from doZKey, highlighting types of access, security software, and victim regions:



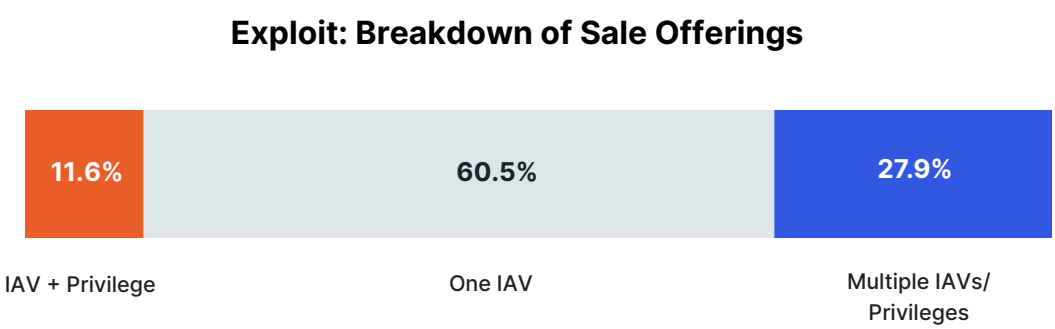
Industry data is not particularly comprehensive across the H2 2024 Exploit forum data. It is only included by brokers in 35% of posts during this time period — and none of this industry information is included in doZKey's posts. 41.7% of doZKey's sales are US businesses, reinforcing that on an individual and group scale, the US is the primary target for sellers no matter which forum they happen to reside upon:



doZKey's pricing ranges from $300 in the US, to $1,700 (also in the US), with an average base price of $800. Everything offered is a combination of RDP, Domain User, and RDweb:

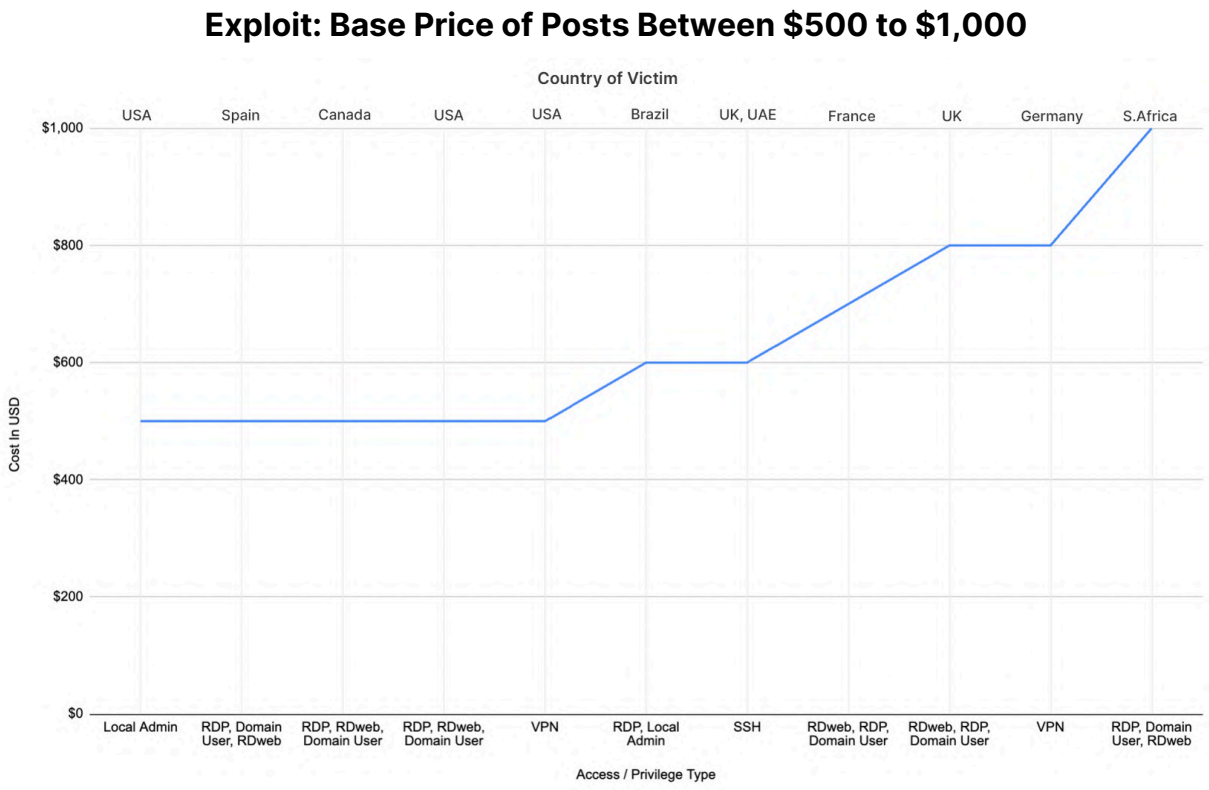


This is a deviation from the Exploit broker user base, where 60.5% of sales are for one access vector only with no explicit administrative privileges included. In fact, multiple IAV/privilege bundles (e.g., sales which include three or more IAVs/privilege types) are popular on Exploit, almost entirely as a result of doZKey's contributions:



Exploit Forum Pricing

Exploit base prices range from $100 to $6,000, with an average of $1,741. A total of 25.58% of base prices are in the $500 to $1,000 range, and 32.56% of base prices are in the $3,000 to $3,500 range. A solitary outlier sale offers RDweb access to an organization with a claimed revenue of between $5 million and $10 million USD, for a base price of $6,000.



Sales in the $500 to $1,000 range come from 5 specific brokers, with 64% of all RDP posts in this selection coming from the ever-present doZKey and sganarelle2. The two VPN offerings belong to “DNI” at price points of $500 and $800, another broker sitting in the top 5 posters for this forum.

Sales in the $3,000 to $3,500 range were a near-even split between six instances of Citrix, and eight sales of RDP, all from one of the most prolific brokers on Exploit, sganarelle2.

XSS Forum Analysis

The second of our Russian-language-based forums and originally known as DaMaGeLaB, this site has been in operation since 2004, rebranding as XSS in 2018 after the arrest of one of its administrators. In 2021, the site famously announced a ban on ransomware ads after the Colonial Pipeline compromise turned up the heat on ransomware groups and promotion generally.

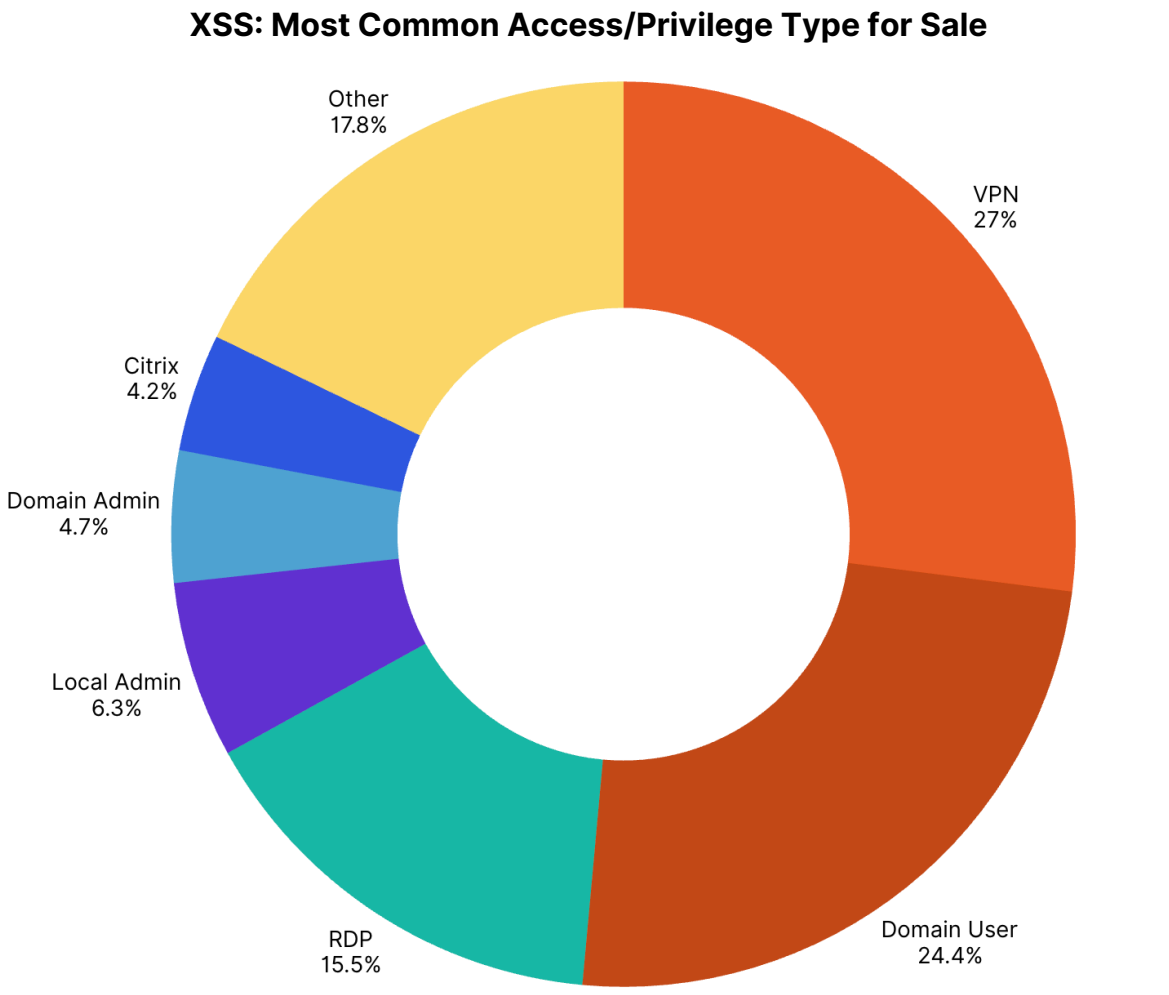
The most recent takedown of the XSS site occurred shortly after the July 22, 2025 arrest of a person believed to be its administrator. At the time of this writing, the forum has yet to make a convincing comeback.

As with Exploit, XSS contained the usual sections you’d expect to see (i.e., malware, reversing, security discussion) alongside the more restricted broker sections. The forum has been known to host a wide range of illicit digital activities, including the trade of malware, botnets, stolen credentials, and compromised RDP/VPN access. The forum also serves as a central hub for cybercriminals, threat actors, and affiliates to buy, sell, and exchange knowledge on exploiting security vulnerabilities and monetizing breached systems.

Despite its criminal nature, XSS maintained a strict code of conduct among members, often banning users

for scams or violations of internal rules. It operated on the clearnet and often required vetted registration, sometimes involving invite codes or proof of reputation from other forums. Due to its activity, XSS has been heavily monitored by cybersecurity researchers and intelligence agencies worldwide.

The XSS forum was free to register (no fees or recommendations), but registration was still subject to authorization from the forum admin. At the time of takedown, brokers published freely on the forum, making their posts accessible to everyone. Purchasing access or services was done with or without



Analyzing our 6-month data sample, XSS offered up 381 forms of initial access/privilege for sale, from a total of 13 brokers. VPN was the most popular form of initial access vector, comprising 27% of all sales on offer. Domain User came second, being present in 24% of sales, with RDP accounting for 15.5% of the overall total. As with Exploit forum, there is something of a notable drop after third and fourth place.

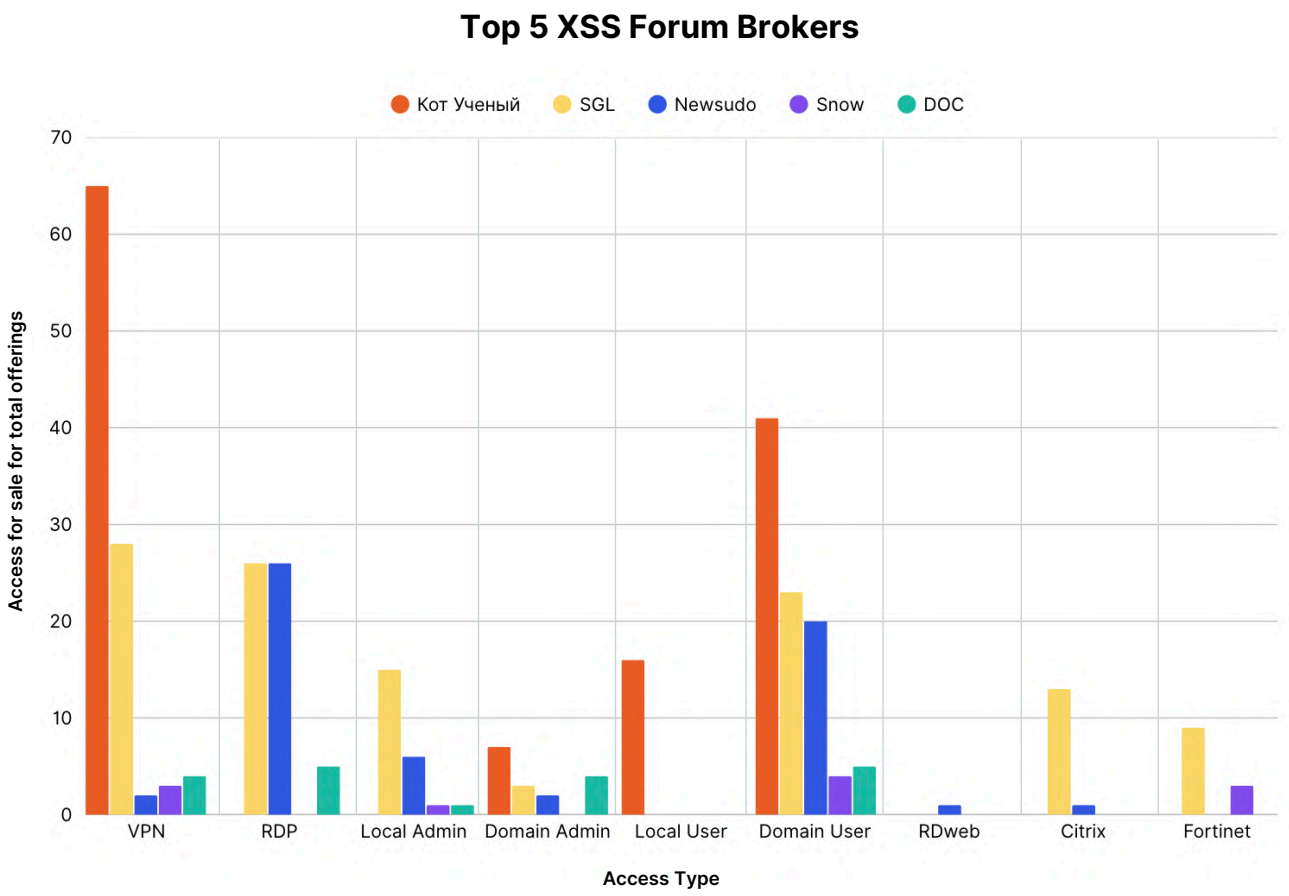
Speaking of “just like Exploit”: brokers on XSS primarily targeted the US (27.7%), with the UK in second place (6.9%), and India in third with 4.8% of all sales offered.

XSS base prices ranged from $100 to $10,000, with an average base price of $1,059. There are a number of outliers across the sales offered; at the very top of the scale, there was AWS/server access for a US-based financial services company, and Domain Admin for another US-based engineering organization, priced at $9,500 and $10,000, respectively.

XSS: Meet the Brokers

As with Exploit, a small number of brokers make a large contribution to the sales postings. Brokers “SGL” and “Кот Ученый” were responsible for 71% of everything available in our 6-month sample, with 37% of that coming from SGL. Кот Ученый was not far behind, responsible for 34% of all initial access/privilege posted.

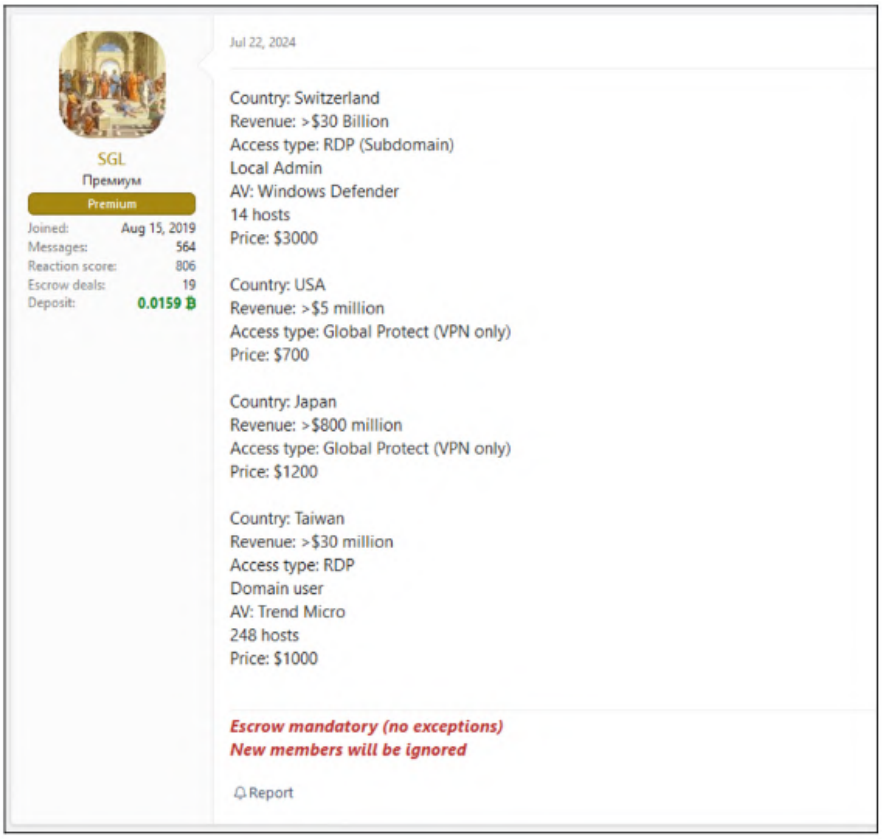
Here are the top five XSS brokers measured by their most popular sales offerings for H2 2024:



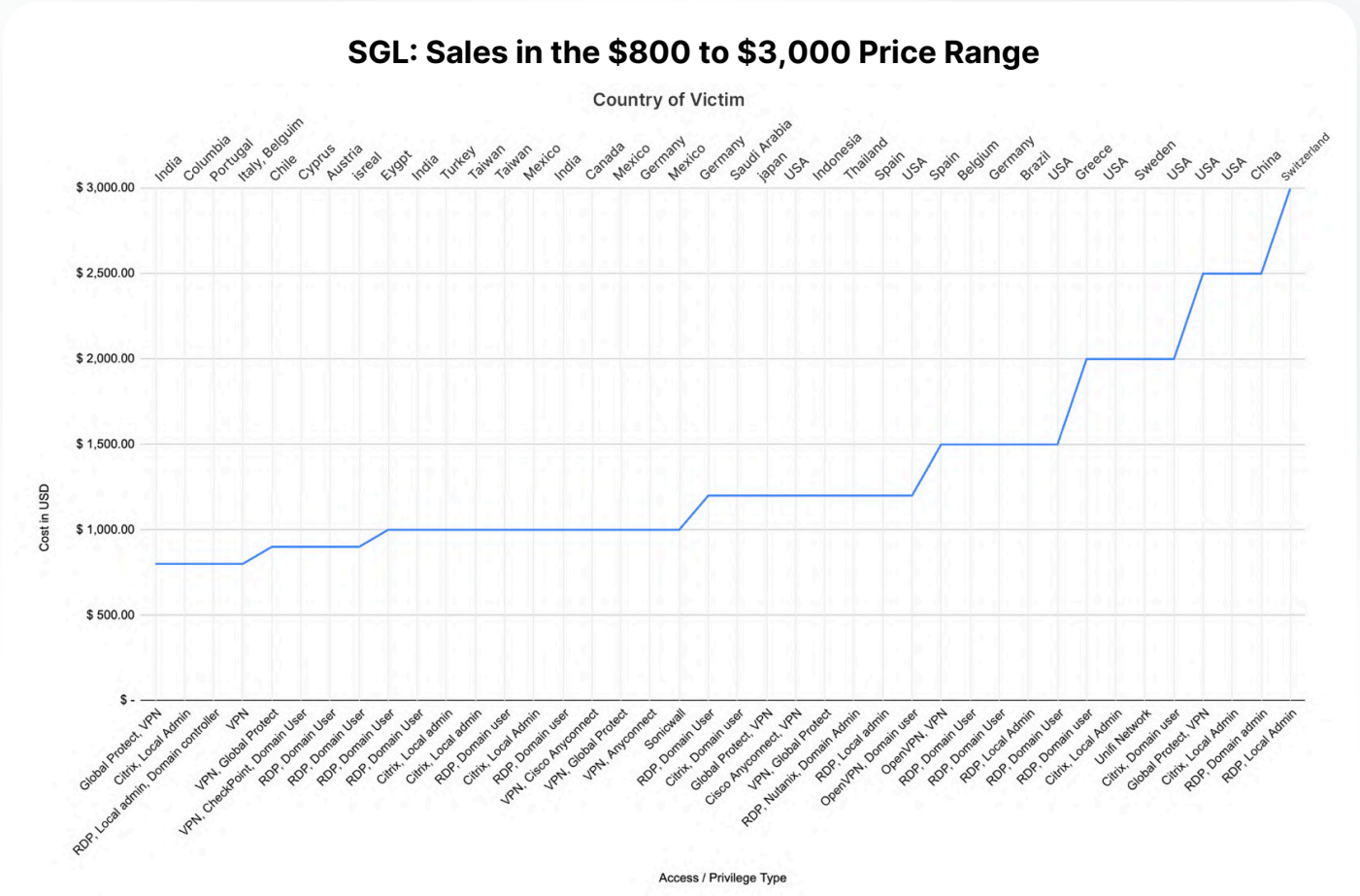
If Exploit’s much smaller sales offering could be considered a boutique, the selection of wares for XSS was more of a department store. Even so, the key areas of focus for the biggest sellers did not dramatically differ; VPN and RDP were still leading the charge, with the only major difference being that Domain User was more in favor across the top three brokers than RDweb.

Victims of SGL were primarily businesses located in the US, with 15% of their posts targeting the region. Кот Ученый’s postings leaned into this to an even greater degree, with 29% of posts targeting US organizations.

SGL’s prices started at $200 for VPN access to a business located in the US, and maxed out at $3,000 for RDP and Local Admin for a compromised business located in Switzerland. SGL had an average base price of $1,037, a few hundred dollars higher than doZKey.



If you were in the market for purchasing access from SGL in the region of $800 to $3,000 — the higher end of the scale where this broker was concerned — then this is what you could expect to see:



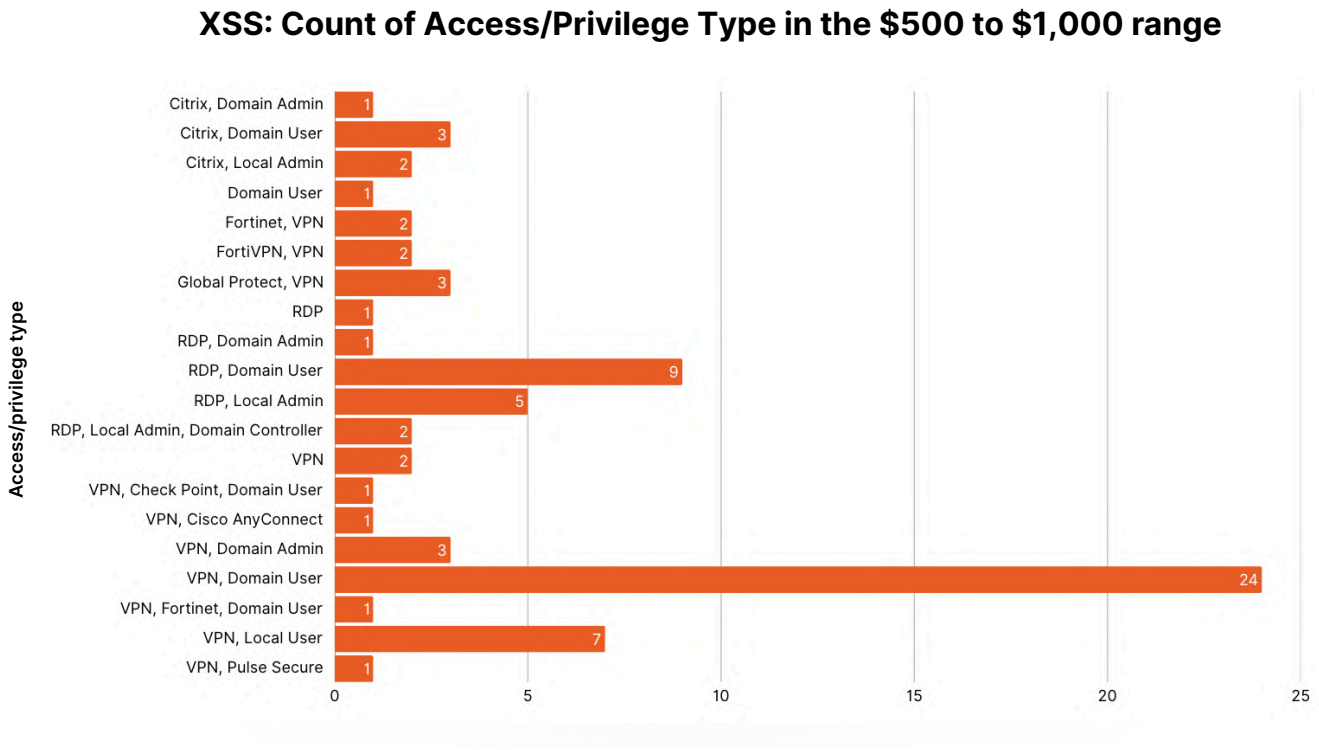
The breakdown was as follows:

- Sales posts focused on the US (17.5%), with Germany, Mexico, and India trailing behind (7.5% each).
- 27.5% of sales sat at the $1,000 price point, with 40% of that total offering RDP/Domain User, and 30% represented by Citrix/Local Admin offerings.
- 30% of sales sat in the $1,500 to $3,000 range. RDP was once again popular no matter the sale price, with just over half of these offerings including various combinations of RDP and Domain User (38.46%), RDP and Local Admin (15.38%), and one single sale of RDP with Domain Admin.

XSS Forum Pricing

XSS forum pricing data highlights a strong showing in the $500 to $1,000 range, with 42% of initial access/privilege for sale falling inside this bracket, and 84% of all sales falling within the $100 to $2,000 range.

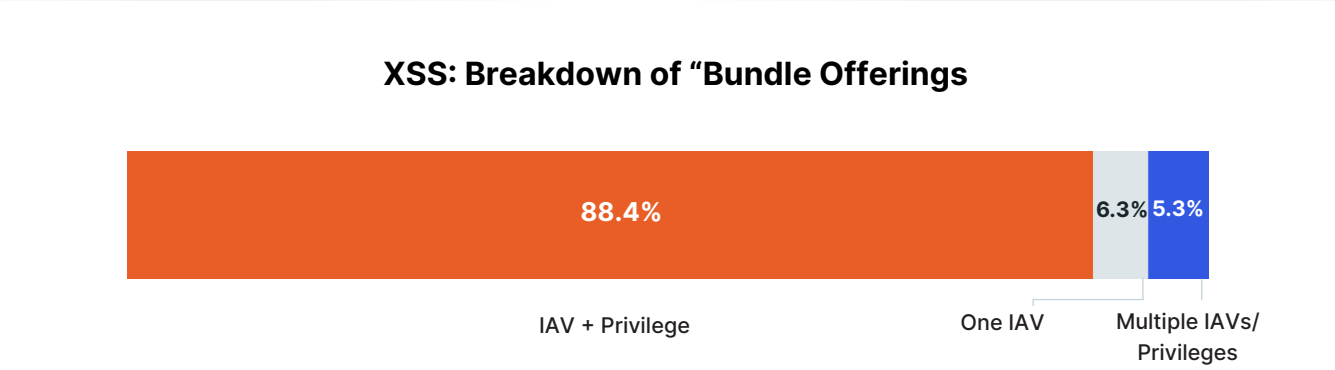
One of these sales was a private message offer — a brief outline of a medical industry compromise, where forum users were invited to send a direct message for more information. As there was no access/privilege type listed, we have removed this entry from the "Count of Access/Privilege Type" chart below.



Here, the humble VPN was king — particularly when paired with Domain User as a means of making further inroads into a compromised network. Even at the lower end of the scale, it was omnipresent, sitting alongside Local User and a variety of products which included Fortinet, Pulse Secure, Cisco AnyConnect, and Global Protect.

Four of the top five forum brokers made an appearance here, with particularly strong showings from SGL (46.8% of posts) and Кот Ученый (43% of posts). To give you an idea of the sheer domination shown by the two top brokers in the $500 to $1,000 range, Newsudo sits in third place with just 6% of posts overall.

As for what kind of bundling is taking place in XSS sales, unlike Exploit, the preference was overwhelmingly for IAV and a privilege (88.4%), with one IAV and no privilege included (6.3%), and multiple IAVs/privileges (5.3%), trailing far behind.



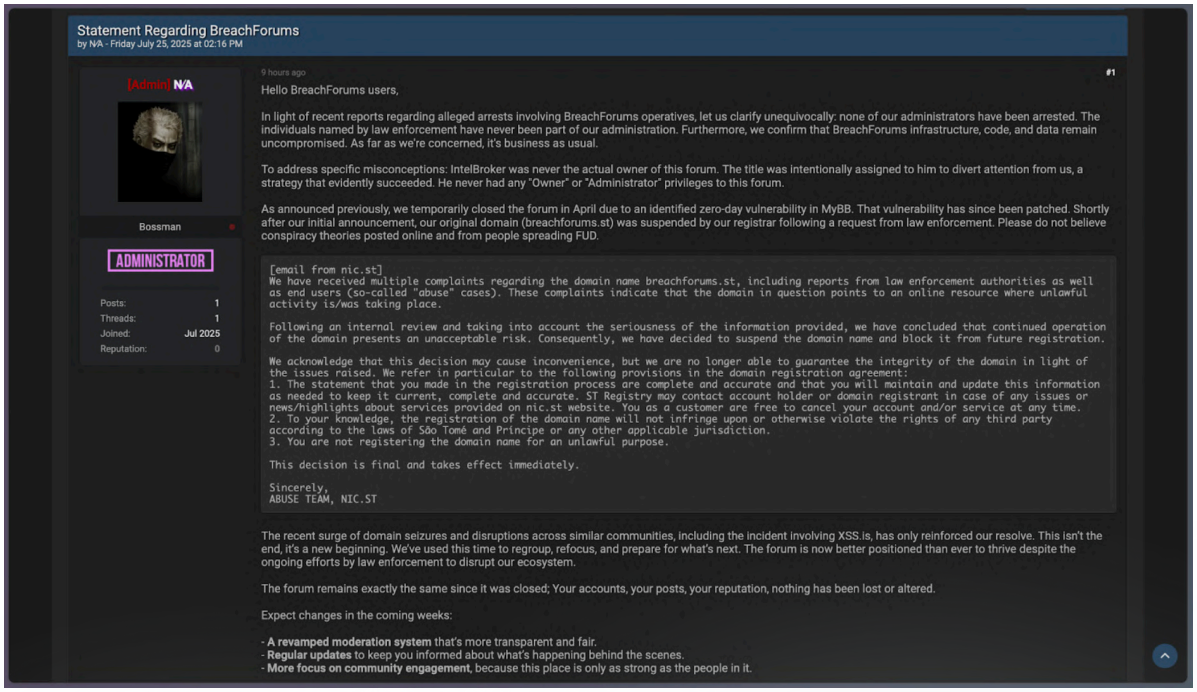
BreachForums Analysis

BreachForums is known for its erratic yet determined history. Arrests, multiple law enforcement takedowns, and several changes of ownership are woven into the site’s history, itself a successor to RaidForums. Registration for the forum has historically been free and subject to administrator approval, like most cybercrime forums.

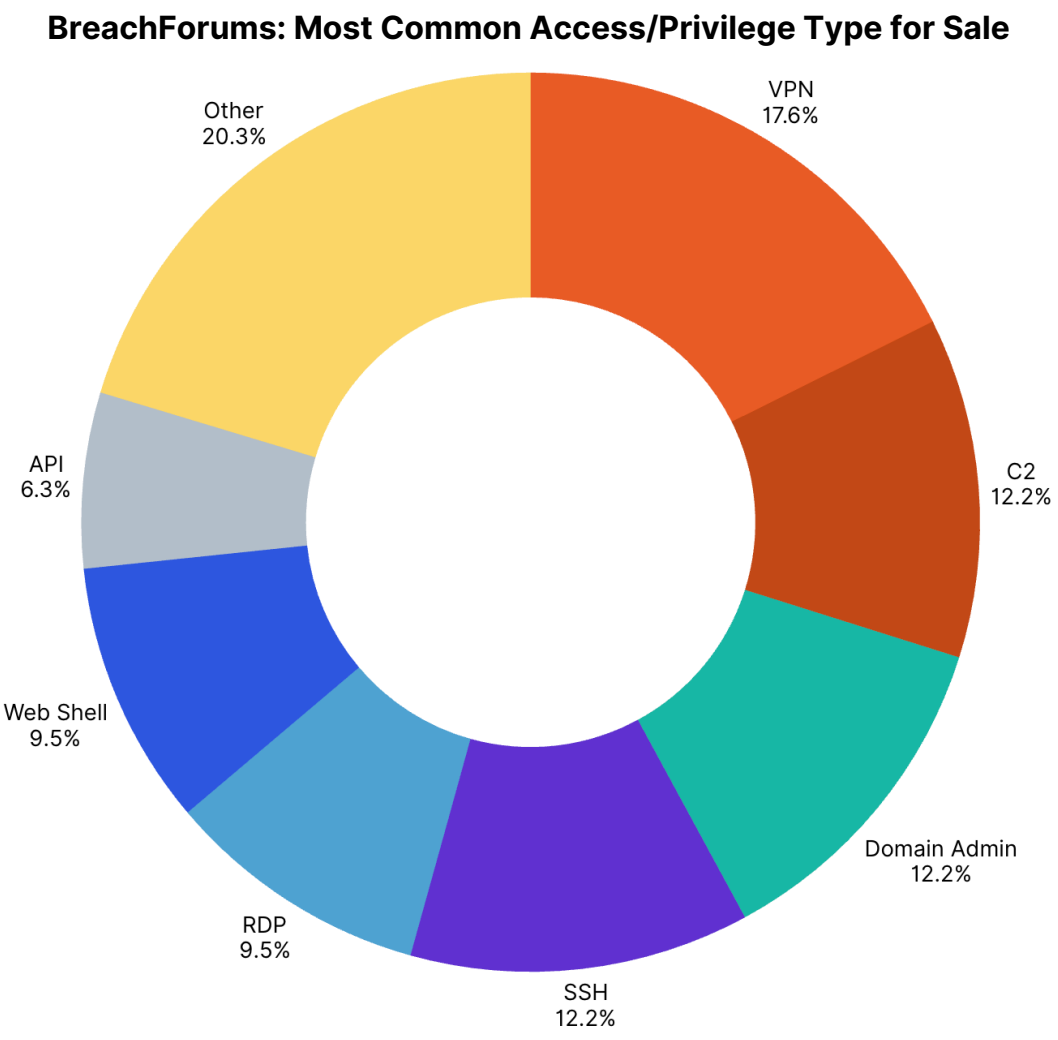
In June 2023, the publicly accessible BreachForums domains were seized by US law enforcement and an FBI seizure banner was put in place. A second incarnation of the site sprang up under a new admin team that same month, operating until May 2024 when law enforcement once again took down the clear-net version of the site, as well as its Onion portal and Telegram. Despite this, the site came back for a third time — again within the same month.

It was during this incarnation that our data was gathered, shortly before the site vanished yet again. At the beginning of 2025, “IntelBroker,” a well-known figure on the site, announced that he was stepping down as the site’s “owner” because he was “very busy IRL.” Having previously claimed to be a Serbian network technician, he was later revealed to be a British national following his February arrest in France.

Around April 15th, the BreachForums site went offline, and there was much speculation surrounding the event that could have triggered the outage. BreachForums didn’t officially resurface until July 25th, at which time the following message was posted:



And with that, it was back to “business as usual.”



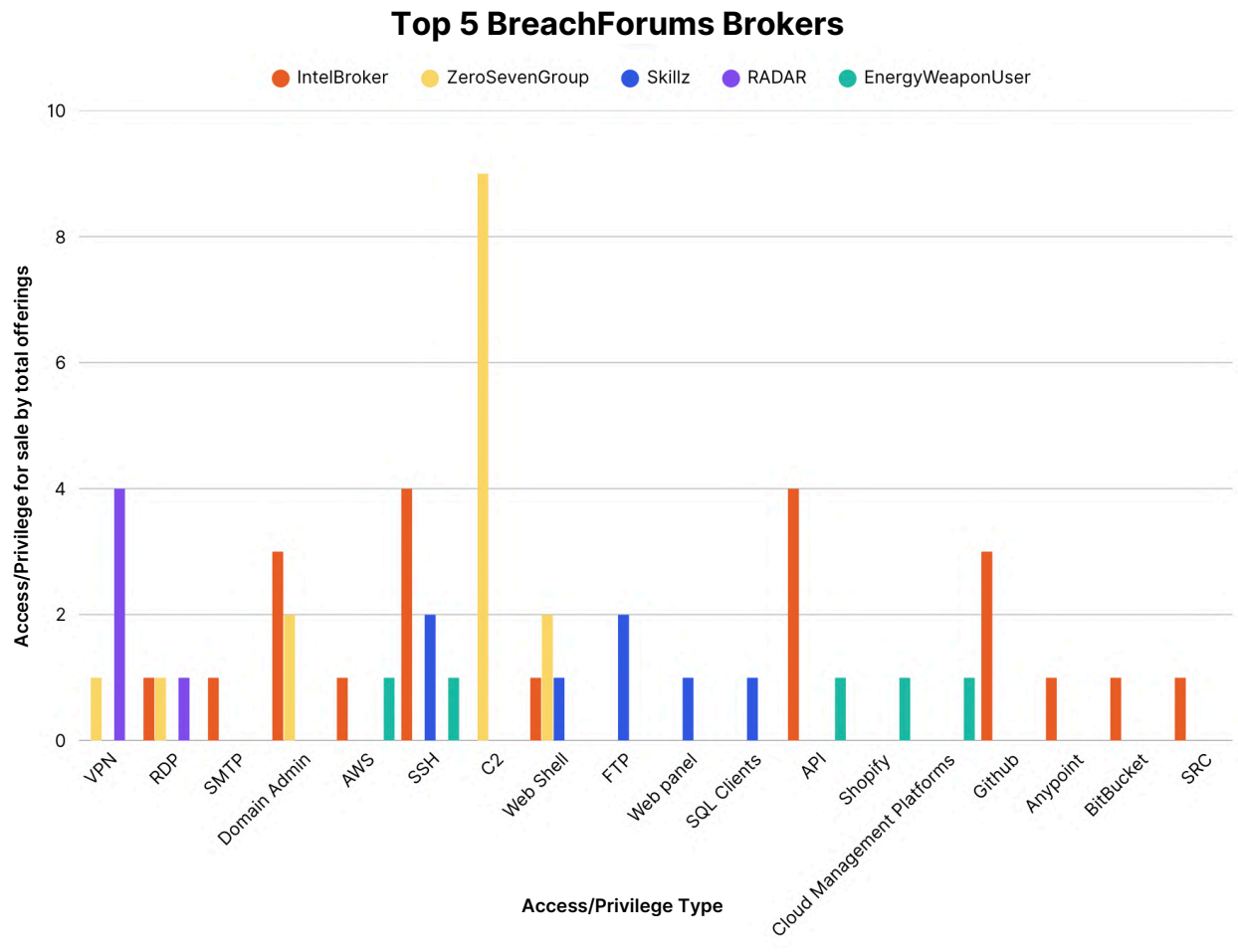
Our H2 2024 data reveals that BreachForums offered up 82 forms of initial access/privilege for sale, from a total of 26 brokers. Just like XSS, VPN was the most popular form of access (17.6%), although there's no real stand out here, unlike on the Exploit and XSS forums.

SSH, Domain Admin, and C2 all take second place with 12.2%, and it's also a tie for third spot with both RDP and Web Shell being present in 9.5% of broker posts.

BreachForums: Meet the Brokers

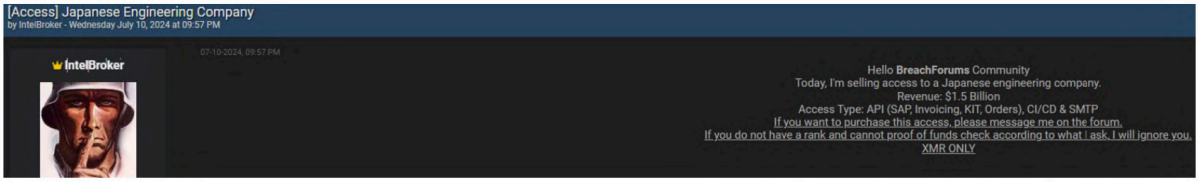
The most prolific poster to BreachForums (with almost 19.05% of all sales) was, in fact, IntelBroker — at least leading up to his "resignation" at the beginning of this year. The only other broker who came close for number of sales was "ZeroSevenGroup"; they dealt almost exclusively in Command and Control (C2), an infrastructure that is very popular with attackers because it allows them to evade detection, exfiltrate data, or deploy additional malware to compromised systems.

The chart below presents the top five BreachForums brokers at the time, along with their most common offerings.



IntelBroker's sales were a mixed bag of standalone Domain Admin, SSH (sometimes combined with API or GitHub, other times as a solo sale), and other rarely seen data points such as AWS or BitBucket. Roughly one-third (33.33%) of IntelBroker's offerings involved SSH, while 25% of his posts included either GitHub or Domain Admin.

Although his pricing on posts ranged from $500 to $40,000 (the latter granting SSH access to a US-based gambling firm), IntelBroker's pricing data is incomplete due to many of his negotiations involving direct messaging.



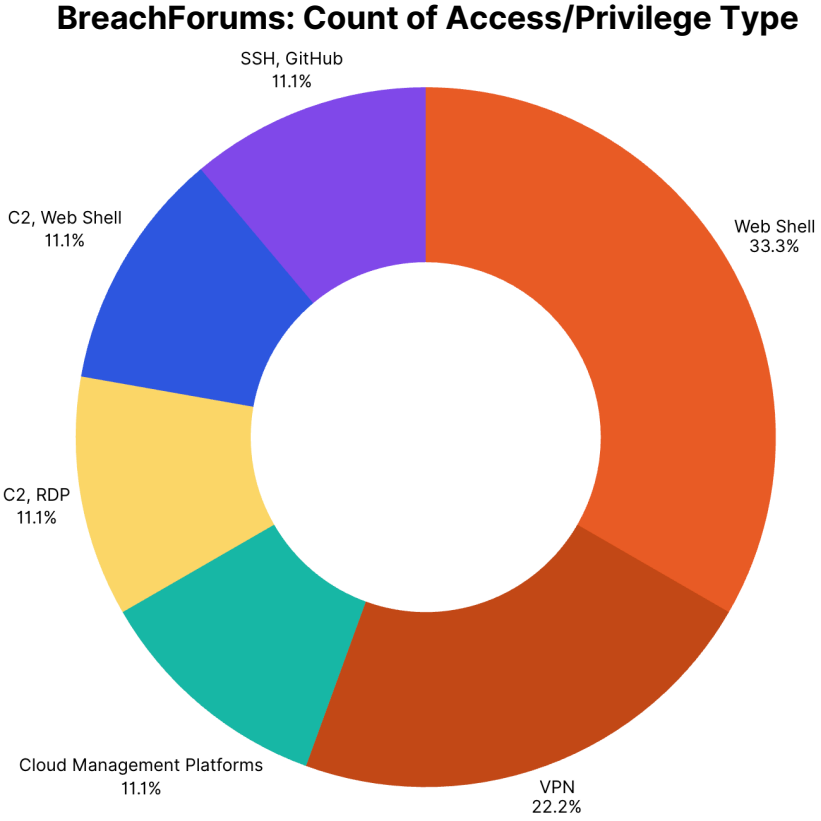
Regions targeted by IntelBroker appear somewhat novel compared to much of what we've covered so far. His most commonly targeted locations were South Korea and Japan (21%), with the US and India in second place (14%), and a selection of nations taking third position (7%) that included Australia, Thailand, and China.

BreachForums: Forum Pricing

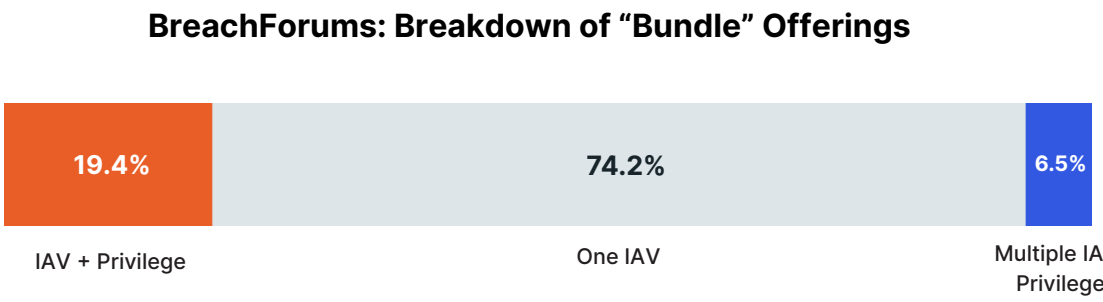
Although BreachForums had a higher volume of broker posts made over H2 2024 than Exploit, 32% of all visible posts did not contain a base price. This means that in terms of the number of posts with a visible base price, Exploit and BreachForums were nearly identical.

On BreachForums, 23% of all base prices posted were in the $500 to $1,000 range, with ZeroSevenGroup making up 30% of all posts, IntelBroker 20%, and several other brokers sitting at 10% — these included Skillz, RADAR, and EnergyWeaponUser from the top 5 brokers list.

What was on offer for $500 to $1,000? Some form of web shell access made up 33.3% of posts, while the ever-present VPN took second spot with 22.2%. Everything else was a mix of several forms of initial access, including C2, RDP, and SSH, as shown below.



For bundled deals, this is how BreachForums operated:



In the graphic above we see that nearly three quarters (74.2%) of the offerings on BreachForums were for a single IAV with no privilege included. An IAV with one form of privilege followed at 19.4%, and bundles of IAVs and privileges sat at a low 6.5%. BreachForums was most closely aligned with Exploit where selling a form of IAV with no privilege included was concerned (60.5%), while XSS overwhelmingly favored sales of an IAV with one privilege included (88.4%).

Recommendations

Leverage Actionable Threat Intelligence: Threat Intelligence and data sharing are important tools in the fight against access brokers. You probably won’t be able to spot your own business on a forum post, but careful analysis of individual broker trends, favored industries, and common forms of software and system access can help you to make an informed decision regarding where brokers’ weak points lie.

Intelligence that can make use of this data and point you toward potentially suspicious user activity can be the difference between weeks or months of a threat actor living off the land, and shutting down an attack before it begins.

Enforce MFA: VPN, RDP, and Domain User accounts being the most popular broker sales offerings highlights that their buyers aren’t kicking SOC doors down — they’re swiping themselves through with a very cheap lanyard. Rapid7’s Q1 2025 Incident Response findings reflect the popularity of these offerings, with valid credentials/no MFA as the IAV accounting for 56% of all incidents Rapid7 observed, and exposed RDP services abused in 44% of observed attacks.

So many devastating attacks begin because no authentication is in place when an employee is phished, or a database filled with insecure passwords is compromised. Strong MFA protocols and enforcement will help to lock down these attacks right out of the gate.

Take a Unified Approach to Exposure Management and Threat Detection: Even when risk is known, it’s often already in play — making fast, contextual response just as critical as prevention. Security teams need to identify illegitimate access quickly, correlate suspicious behavior across users and assets, and shut down attacker movement before damage is done. This involves leveraging AI-powered alert triage to surface stealthy initial access behaviors faster, as well as built-in automation to contain access brokers before they further escalate.

Test Your Defenses: Regular Red Team exercises can help to highlight weak spots in your defenses, which brokers seek to take advantage of. Nothing will grant a greater understanding of your environment than a penetration tester finding exposed entry points or long-abandoned accounts which were never disabled.

Conclusion

Organizations that unwittingly have their network access posted for sale on initial access broker forums have already been victimized once, and they are on their way to being victimized once again when the buyer attacks. The good news is that this isn't the scenario that has to play out, especially given today's technological advancements in the SOC.

Yet initial access brokers are clearly happy to keep selling combinations of VPN, RDP, and Domain and Admin accounts to leverage entry points into networks. They're also very good at gaining access to these evergreen weak spots in the first place, and buyers are likely happy to continue making purchases.

It makes sense, then, to utilize relevant threat intelligence and get a sense of what's making waves on broker forums. There's no time like the present to start making some waves of your own and formulate a plan for tackling the trifecta of peril that is VPN, RDP, and Domain Accounts — before someone else tackles them for you.

ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.