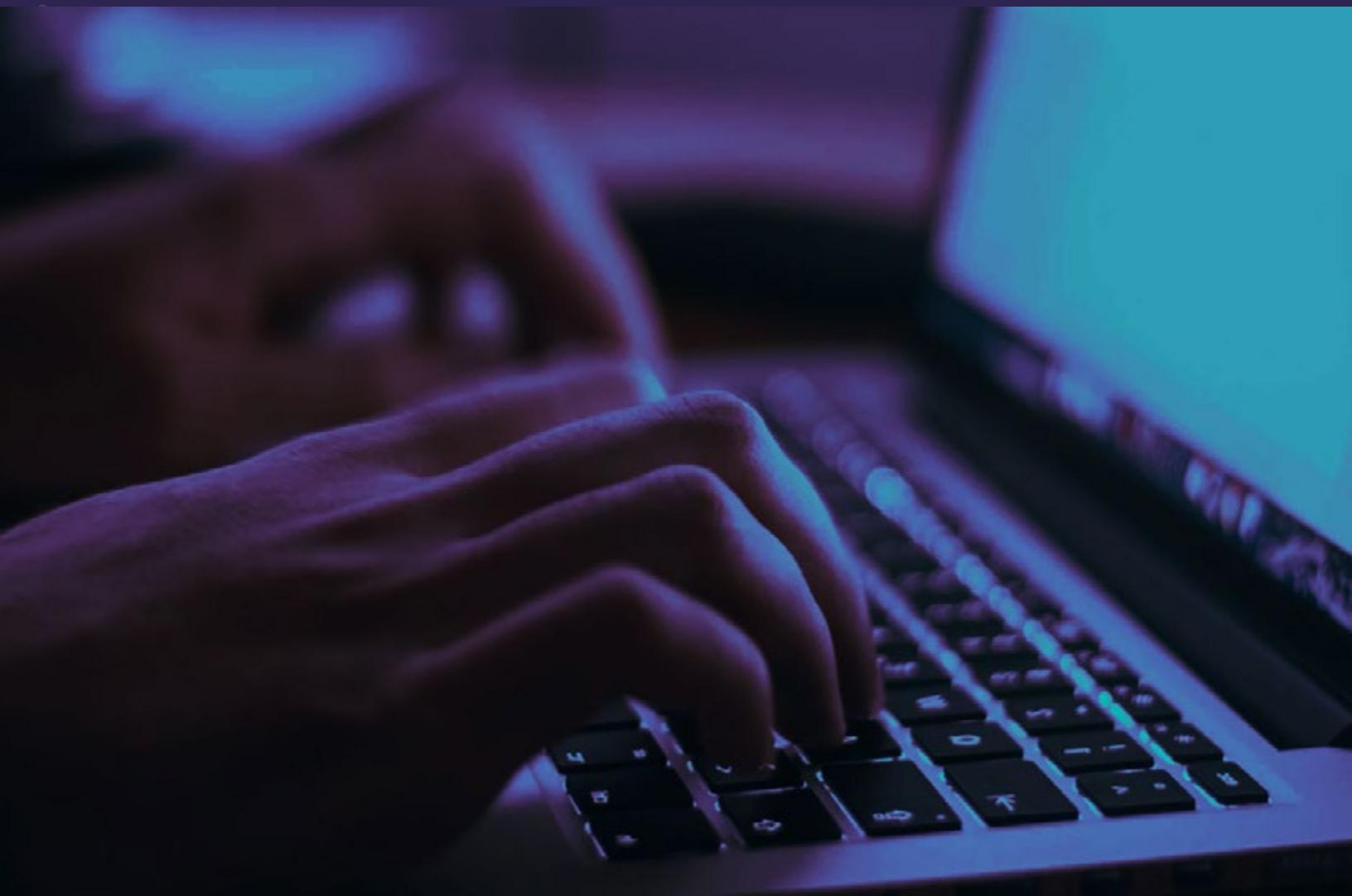


The Modern Cybercriminal Forum

An Enduring Model



Authors: Digital Shadows Photon Research Team

digital shadows

Executive Summary

Some threat actors would have noticed when Torum entered the cybercriminal scene in 2017, but not a lot of them used the new forum. It wasn't until the disappearance of the popular KickAss forum two years later that threat actors started scanning the horizon for an alternative and joined Torum. By October 2019, Torum's membership numbers had shot up to 43,559—a 639-percent gain in just eight months—and the number of posts on the forum had skyrocketed from 6,096 to 61,395.

Cybercriminal forums continue to thrive despite law-enforcement takedowns and the emergence of more efficient and ostensibly secure alternatives. The Photon Research Team took a deep-dive into the cybercriminal underground to investigate the persistence of forums, uncovering several reasons they remain attractive amid appealing alternatives. Our research findings, as documented in this paper, cover some revealing insights:

- As new forums continue to appear and forum membership numbers keep growing, **users have frequently expressed reluctance to move to other platforms for their communication and trading needs.** They see drawbacks in alternative technologies, despite the purported security and efficiency they offer.
- **Many forums boast a long history and respected pedigree, which is hugely appealing to cybercriminals.** The venerable forums tend to attract skilled threat actors and act as repositories of cybercriminal information.
- It can be difficult for threat actors to judge who they're dealing with on a messaging app or Automated Vending Cart (AVC). But **forum reputation systems and users' post histories provide threat actors with valuable indications as to the credibility of other cybercriminals.**
- **Forums' arbitration and escrow systems ensure fair deals and consequences for failed transactions.** It's hard to deny the appeal of this feature when one cybercriminal wants to make a deal with another.
- Not only do they offer a space to communicate and trade, **forums also give users a valuable advertising space and opportunity to reach a wide userbase.**
- **The benefits of a supportive and knowledgeable community are valued by members of a forum,** who give and receive advice, and learn from each other's mistakes.
- **Many threat actors have concerns about the security of alternative technologies,** but continue to have faith in the anonymity and security offered by trusted forums.

Table of Contents

Executive Summary.....	1
Introduction.....	2
Undeniable appeal: Evidence that forums are still popular	3
Out with the old.....	3
...In with the new	6
Strength in numbers: The ever-growing member/post count	7
Playing it safe, resisting alternatives	11
Why forums are still winning the popularity contest	15
Longevity breeds respect	15
Trust issues	18
“Free” advertising	20
The ease of arbitration	22
Sense of community	25
Airing doubts about alternative technologies	27
The future of forums: Is there an end to the trend?	30

Introduction

Forums are among the earliest and most basic Internet communication technologies. They date back to the early 1970s¹ and most experts agree that threat actors set up the first cybercriminal forums in the late 1990s.² By 2001, a carding forum called CarderPlanet had created an established model for forums that almost all future platforms would emulate.³ Today cybercriminals use forums to ask for advice and discuss the latest techniques and developments. Vendors are another avid userbase, selling offerings including access to internal systems, website accounts, databases, credentials, tools, malware, credit-card details, and cybercrime tutorials.

Since forums' inception, many other communication and trading technologies have cropped up, offering improved efficiency, convenience, and security—compared with the clunky thread-and-post model forums use. There are messaging services and encrypted applications like Telegram, Wickr, and Discord, plus decentralized technologies like blockchain DNS, i2P, and BitTorrent. Automatic trading platforms, such as marketplaces and AVCs, have also taken root in the landscape.

Alongside the emergence of those technologies, forums have proven a risky—and outdated—arena for threat actors. They're frequently disrupted by security services in many jurisdictions, and they often vanish quietly. Many believe the forums Hell and KickAss ceased to function for this reason (in 2015⁴ and 2019⁵, respectively), although this has not been confirmed by authorities. At other times, law-enforcement agencies' successes are publicized in the global media. In September 2019 Belarusian authorities seized the servers of notorious hacking forum Xakfor.⁶ The cybercriminal community is well aware of the authorities' presence on their forums, and that some forums only survive so long because they're valuable for police to gather intelligence and evidence.

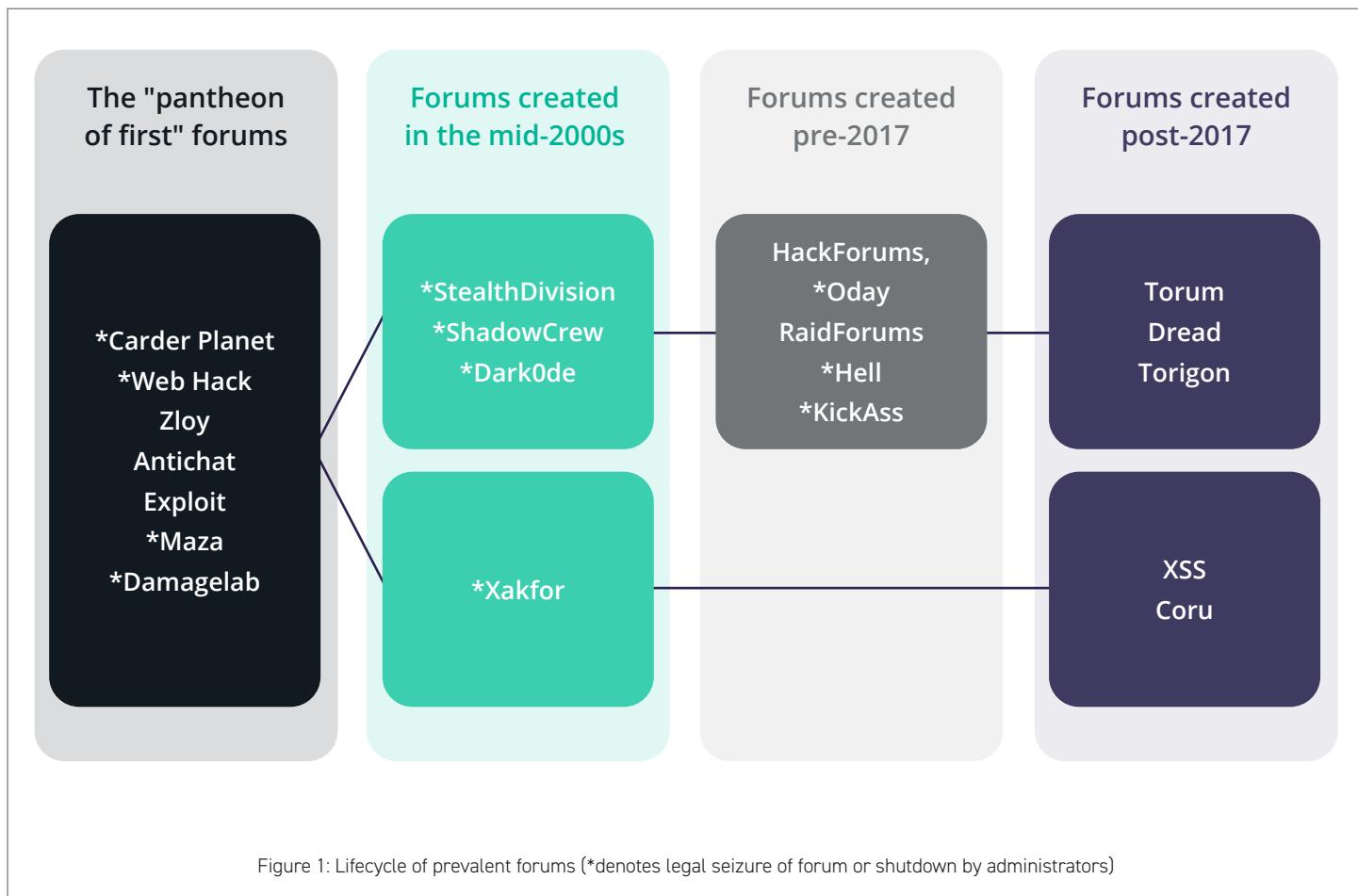
For these reasons, many cyber-security professionals have alluded to forums being doomed to redundancy. With cybercriminals carrying out more transactions and discussions on alternative platforms, you'd expect the need for forums to decrease. It can't be denied that cybercriminals are increasingly using other platforms; the Photon Research Team has even [written](#) about this phenomenon. But the rise of alternative technologies hasn't spelled the end of forums, which seem to be prospering against all odds.

Undeniable appeal: Evidence that forums are still popular

There are several factors supporting the idea that forums are here for the long run. New sites are constantly appearing, membership numbers continue to climb, and users frequently express reluctance to deviate from the traditional forum model. The appearance of new forums is, to a large extent, driven by the need to replace failed ones.

Out with the old...

The English-language cybercrime scene has experienced remarkable instability in recent years, with established forums—and much newer ones—continually vanishing for many varied reasons, some of which we discuss below.



Undeniable appeal: Evidence that forums are still popular

Law enforcement involvement

Takedowns by police or security services have been the reason for the demise of most now-defunct forums. Among them was the prominent Dark0de forum, rendered offline by an FBI-led operation in 2015.⁷ Dark0de had been in operation since 2007 and achieved notoriety among English-speaking cybercriminals for the site's discussion and sale of hacking tools, exploits, breached data, and spamming services. Another casualty was the longstanding Infraud: at its height, a half-billion-dollar operation selling hacking and fraud services, before an international law-enforcement coalition took it down in 2018.⁸



Figure 2: Home page of Infraud after its takedown

Undeniable appeal: Evidence that forums are still popular

Owner/member misconduct

Other forums have perished because of their owners' misconduct. For example, the Photon Research Team has seen sites abandoned by their administrators—0day was a prominent cybercriminal platform that launched in early 2014, but by late 2017 the forum's administrators had apparently forsaken it. Our investigations showed that registration requests went unanswered and the site's Jabber services were down. Rumors circulated that the forum was no longer active: The administrators had left without turning off the lights. At the time of writing, the forum's Tor⁹ URL is no longer accessible, and the clear web URL disappeared several years ago.

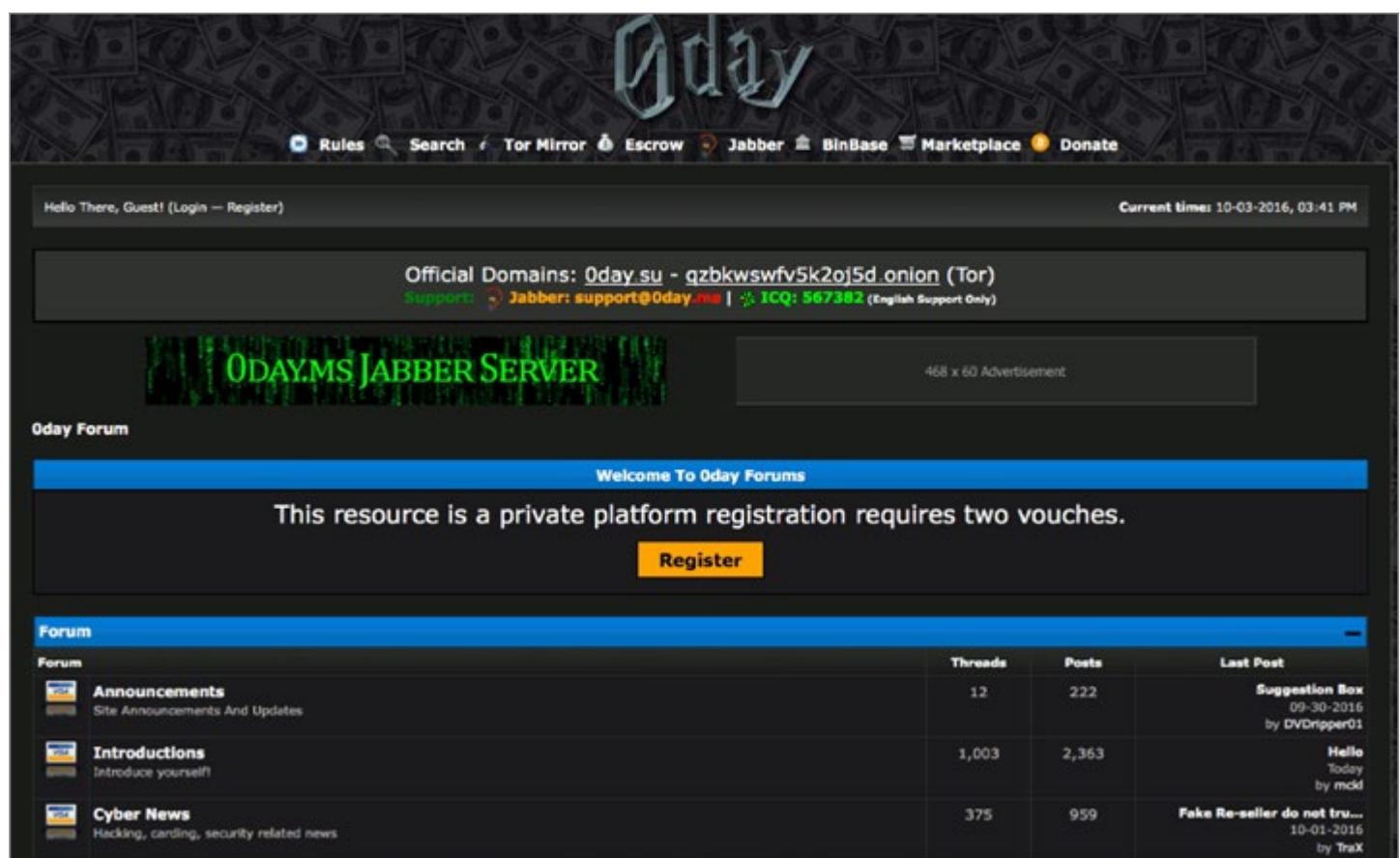


Figure 3: 0day homepage

Sometimes forum members' misconduct can also play a part. That Russian-language forums are much more successful than their English-language counterparts can largely be attributed to the incredible discipline of Russian-language platforms. Strict rules govern what kind of language can be used (profanities are out, grammatically correct Russian is in), which sections will accept new threads, and how forum moderators must be treated (challenging moderators' opinions is definitely out). Such rules guarantee order and ensure that forums can't fragment because members are unlikely to rebel.

Undeniable appeal: *Evidence that forums are still popular*

Poor execution

Then there are the forums that flop because of poor execution on the part of their creators. Torigon was launched by a trio of threat actors in September 2019 with the clear aim of bringing English- and Russian-speaking hackers together to trade malware and exploits on a single platform. But the forum failed to provide translations into Russian for non-English speakers, and neglected to promote the site within the cybercriminal community. The result? A lack of engagement, and failure to reach the target market.



Figure 4: Torigon branding

...In with the new

Despite the considerable unpredictability in the world of English-speaking cybercriminals—when a forum will appear or disappear, whether its members will rebel or law-enforcement action will occur—the overall death of English-speaking forums is not imminent. In fact, the scene is best likened to a game of “whack-a-mole”: No sooner does one forum disappear than another pops up to take its place. In the cybercriminal underground, the appetite for new forums is far from diminishing.

The extraordinary tenacity of the forum model within the English-language cybercriminal community indicates that threat actors still see great value in using these platforms. Starting a new forum requires substantial effort and resources that don’t even guarantee success; even so, we see multiple new sites launch each year. Sometimes forums that have been disrupted by police even attempt to return to the scene, relying on their historic branding to lend them credibility—there have been rumors about the reappearance of Hell (as Hell Reloaded)¹⁰ and Dark0de.¹¹

The appetite for new forums is seen even among Russian-speaking cybercriminals. Although their scene is characterized by the remarkable stability and longevity of forums, sometimes sites do perish...but not always for good. In 2018 a formerly defunct forum, DamageLab, was relaunched as XSS. Owing largely to the pedigree of the experienced team behind the forum, XSS has grown and come to challenge even the most prominent Russian-language platforms. And in March 2019 a new rumor swirled through cybercriminal forums: The coding forum Cult of the Russian Underground (CORU)—missing in action since 2016—would be resurrected. By April 2019 CORU had opened up registration.

Undeniable appeal: Evidence that forums are still popular

Strength in numbers: The ever-growing member/post count

Forum membership numbers and thread/post counts show that the popularity of forums is continuously increasing, despite the advent of alternative technologies like Telegram.



Figure 5: Torum logo

The English-language cybercriminal forum Torum launched in 2017 but didn't gain widespread prominence until 2019, when the suspected law enforcement disruption of KickAss and other smaller forums left English-speaking threat actors looking for an alternative. In February of that year, Torum had 5,898 members, but by October 2019, it had 43,559: **a jump of 639 percent** within eight months. The number of posts increased from 6,096 to 61,395 in the same time span.

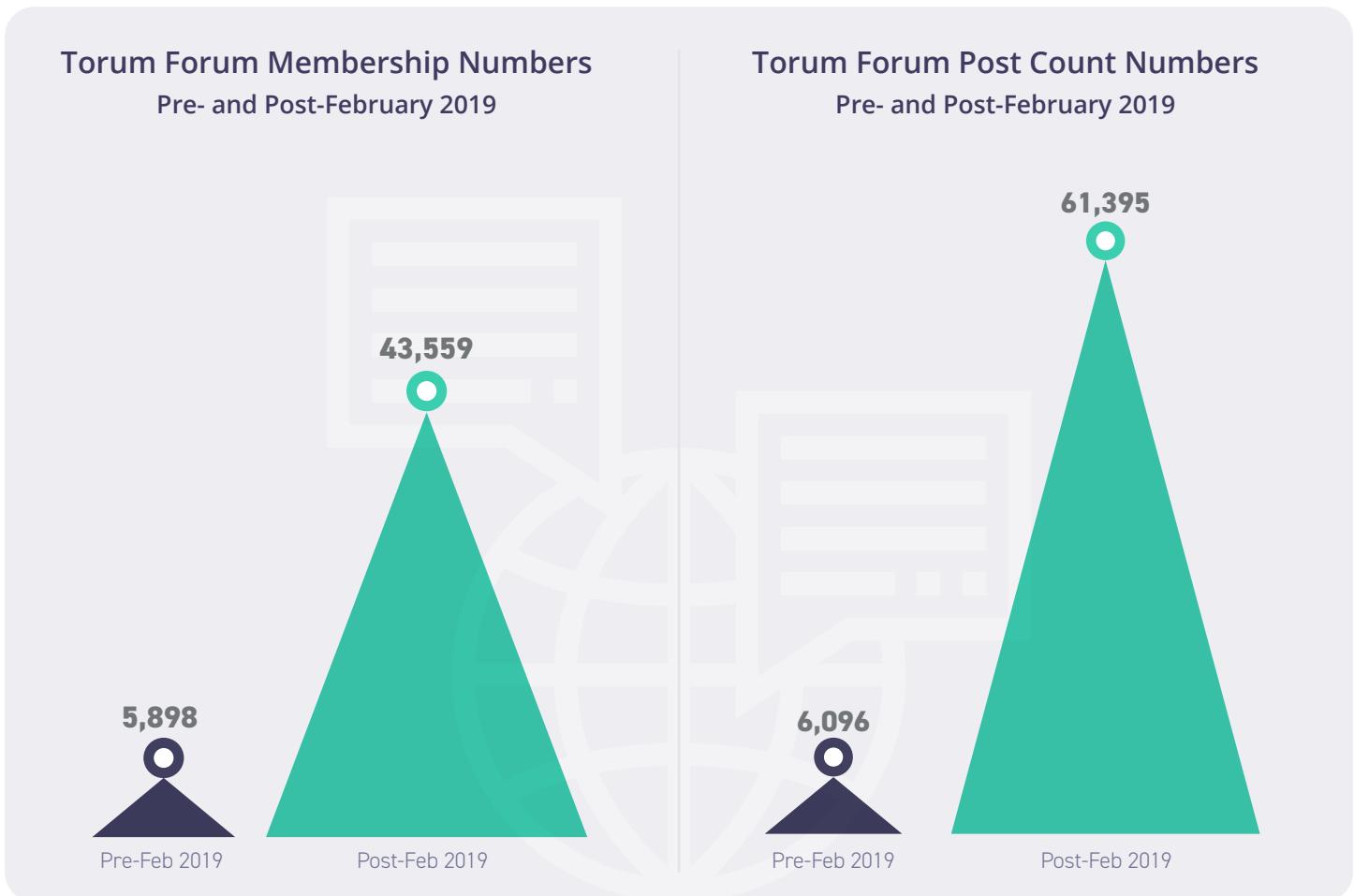


Figure 6: Evidence of growth in membership numbers and post count

Undeniable appeal: Evidence that forums are still popular



Figure 7: Exploit logo

Exploit is one of the most high-profile Russian-language cybercriminal forums. It's operated continuously since 2005, and many threat actors and commentators consider it a platform for some of the most skilled cybercriminals. Despite—or perhaps because of—its longevity and reputation, Exploit has also seen significant growth in membership in recent months. In March 2018 the site had 40,390 registered members. By November 2019, the count was 47,347: a **17.2-percent increase** in an already established forum. A contributing factor may have been the decision to introduce automatic registration in English, to enable non-Russian-speaking users to join more easily. Exploit's post count leapt from 846,020 in March 2018 to 1,012,575 in November 2019.

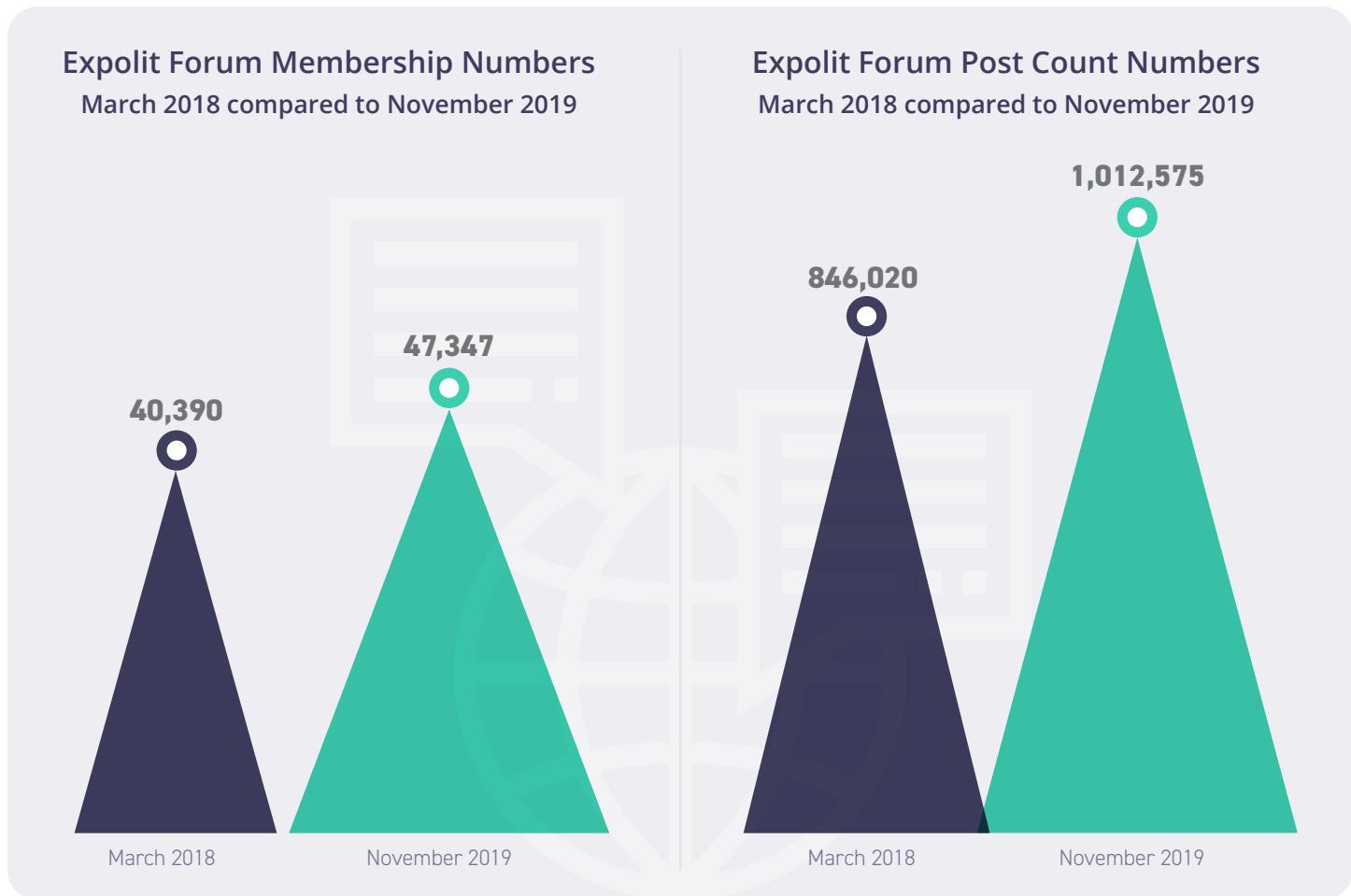


Figure 8: Evidence of growth in membership numbers and post count

Undeniable appeal: *Evidence that forums are still popular*

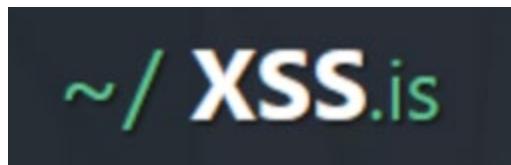


Figure 9: XSS logo

XSS was formerly DamageLab: one of the original Russian-language cybercriminal forums. DamageLab folded after the 2017 arrest of its administrator (see the section “Longevity breeds respect”), but the former administrator of Exploit purchased a partial back-up of XSS in late 2018 and has since built the forum into a thriving and active community, reflected in its growing membership numbers. They've seen an **84-percent increase** between February 2019 (10,344 members) and November 2019 (19,040). And let's not ignore the post count, which grew from 130,040 to 162,470.

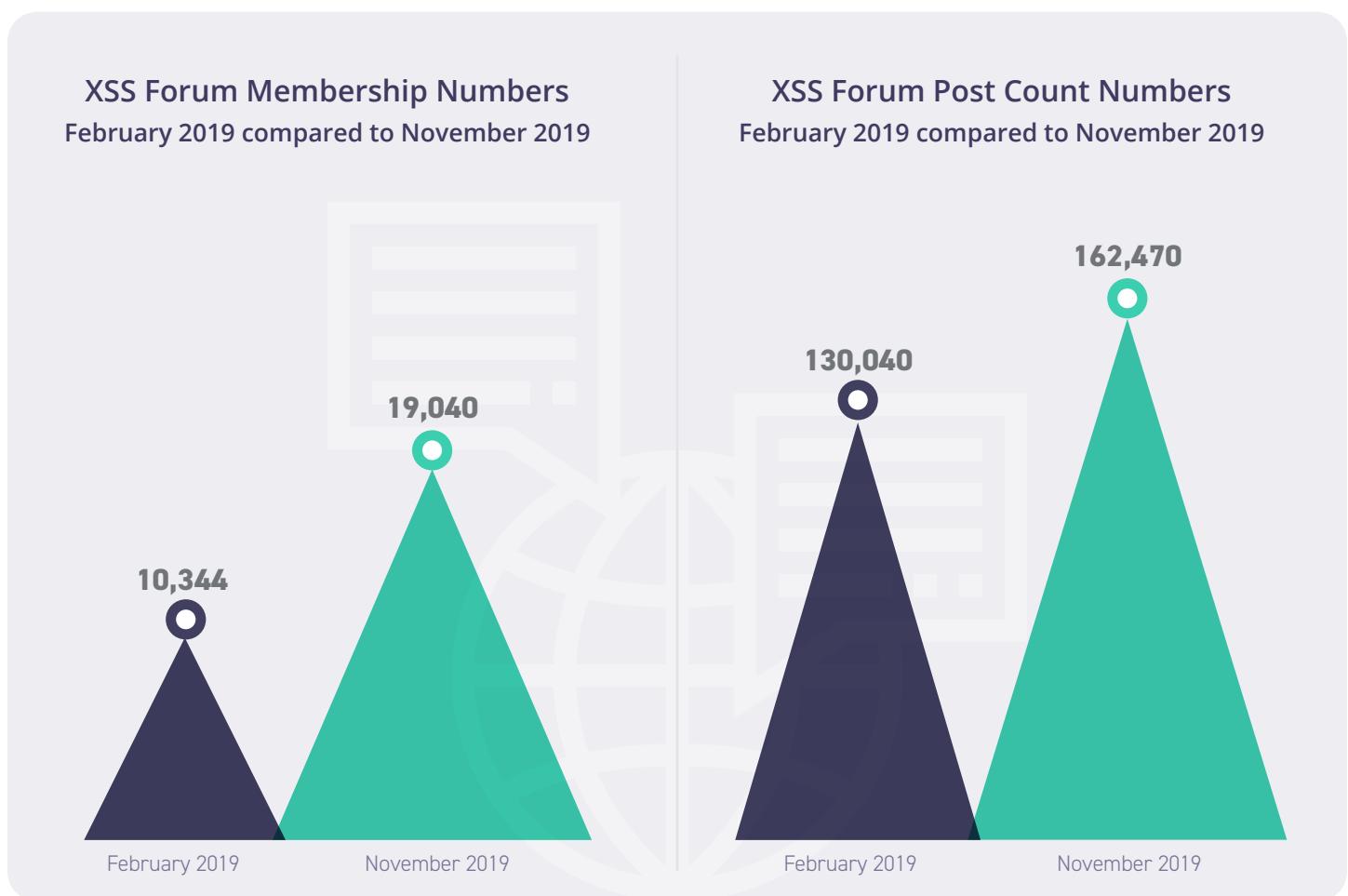


Figure 10: Evidence of growth in membership numbers and post count

Undeniable appeal: Evidence that forums are still popular

Visit numbers also suggest that forums' popularity remains steady. The number of visits to two popular English-language cybercriminal forums, Nulled and Raidforums, has barely diminished since April 2019, according to the visit metrics site SimilarWeb[.]com. Visits to Exploit have increased by over 20,000 in the same period, according to the same site.

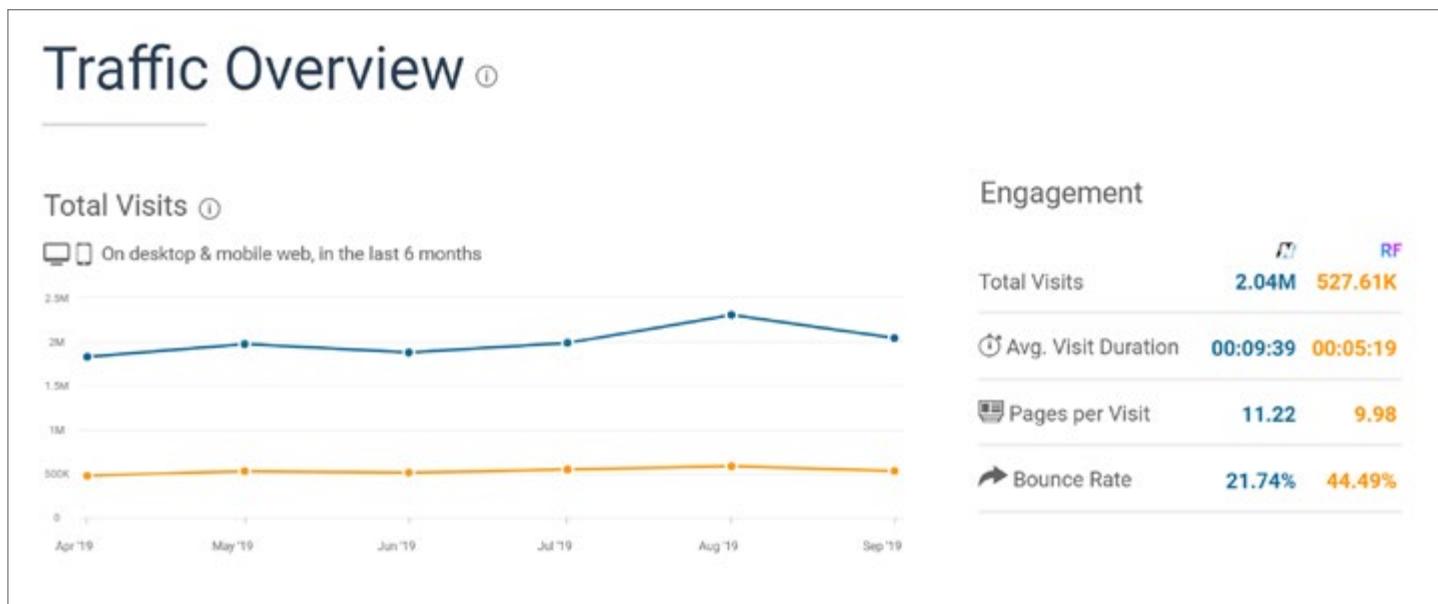


Figure 11: Comparison of Nulled (blue) and Raidforums (yellow) visit figures, past six months (Source: SimilarWeb[.]com)



Figure 12: Exploit visit figures, past six months (Source: SimilarWeb[.]com)

Undeniable appeal: Evidence that forums are still popular

Playing it safe, resisting alternatives

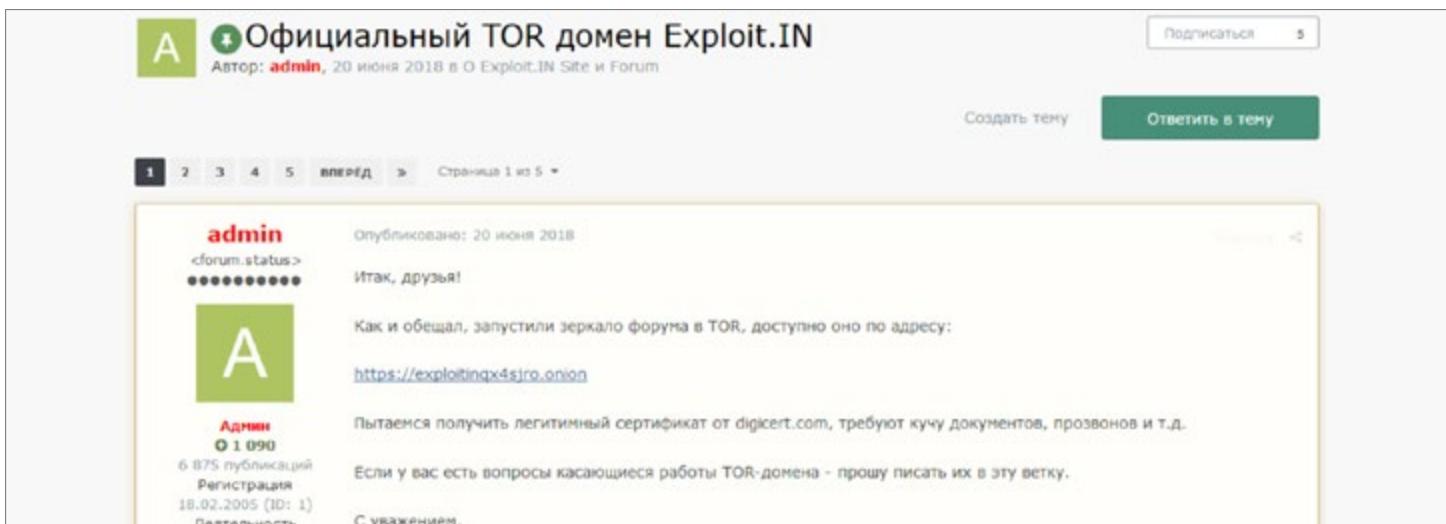
Ways to increase security, efficiency, and profit are common topics of discussion on cybercriminal forums. As such, examples abound of forum users expressing doubts about moving away from the forum model or even, sometimes, about introducing measures to improve forums' functionality and security. Their conservatism stems from trust in the old model, and specific concerns about the newer ones mentioned below.

Messaging applications

In an October 2019 discussion on Torum, one member proposed creating a Telegram or Wickr group for Torum users. Some users supported the idea, but another opined "This is the most stupid idea ever... I think it is against this forums [sic] rules too?" In a separate Torum thread discussing the merits of Telegram, one user stated, "i like Telegram, but I would never send realy [sic] sensitive stuff with that". Their sentiment also extended to other platforms: "one of my real life dealers got busted by writing with WhatsApp!" Even for forum users who have turned to new messaging applications, old habits die hard. We've seen forum users create Discord channels, only to replicate the forum layout or structure with this newer technology.

Tor domains

In June 2018 Exploit introduced a Tor version of the site. But over a year later (October 2019), the Tor version of the forum was still not functioning as expected, and users were complaining about long loading times, complete inaccessibility of the site, and incomplete functionality. Even so, the number of complaints was surprisingly low, considering how long the Tor site had been operating at this suboptimal level. Comments from members revealed that many users hadn't switched to the dark web version of the site—they actually preferred the older, less secure, clear web URL.



The screenshot shows a forum post on the Exploit.IN site. The post is titled 'Официальный TOR домен Exploit.IN' (Official TOR domain for Exploit.IN) and is authored by 'admin' on June 20, 2018. The post content includes a message from 'admin' stating they have launched a mirror of the forum in TOR, with a link provided: <https://exploitingx4sjgo.onion>. The post also mentions that they are trying to get a legitimate certificate from digicert.com, which requires many documents and calls. The post ends with a note for users to ask questions about the TOR domain. The forum interface shows standard navigation elements like a page number (1 of 5), a 'Create topic' button, and a 'Reply to topic' button.

Figure 13: Exploit Tor domain announcement

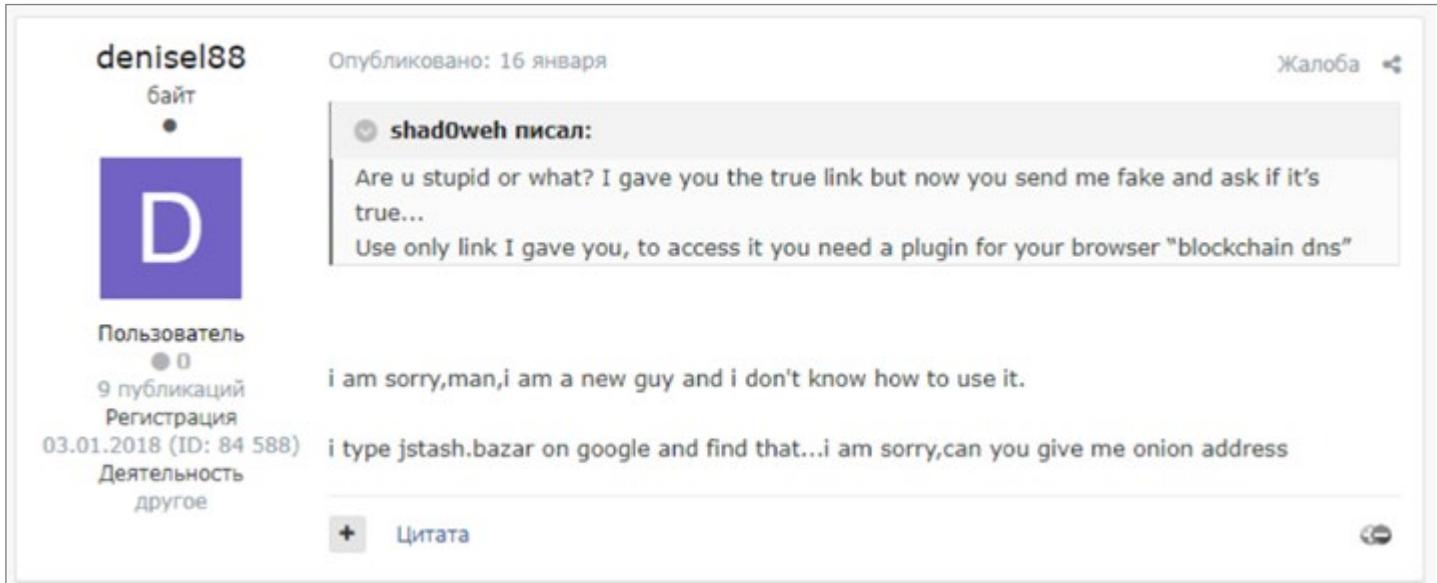
Undeniable appeal: Evidence that forums are still popular

Blockchain DNS

[Blockchain DNS](#) technology, a decentralized system for top-level domains, brings significant security advantages—think bulletproof-hosted platforms and obscured malicious activity. It's also much harder for security services to target blockchain DNS sites because they're not regulated by a central authority in the way conventional DNS sites are. Even in the face of these benefits, almost no reputable cybercriminal platforms have embraced this new development; the AVCs Joker's Stash and Mr Swipe are among the only well-known cybercriminal sites that have.

Similarly, most forums have shied away from using blockchain technology to, for instance, store back-end databases and code to support front-end user interfaces. The Russian-language ProMarket and the English-language L33T both introduced multiple blockchain DNS URLs, but these versions of the forums were down more often than they were functional; the clear web URLs were seen as a much more stable alternative. Add to that perception users' concerns about the public records of blockchain interactions, and you can see why threat actors are reluctant to abandon forums.

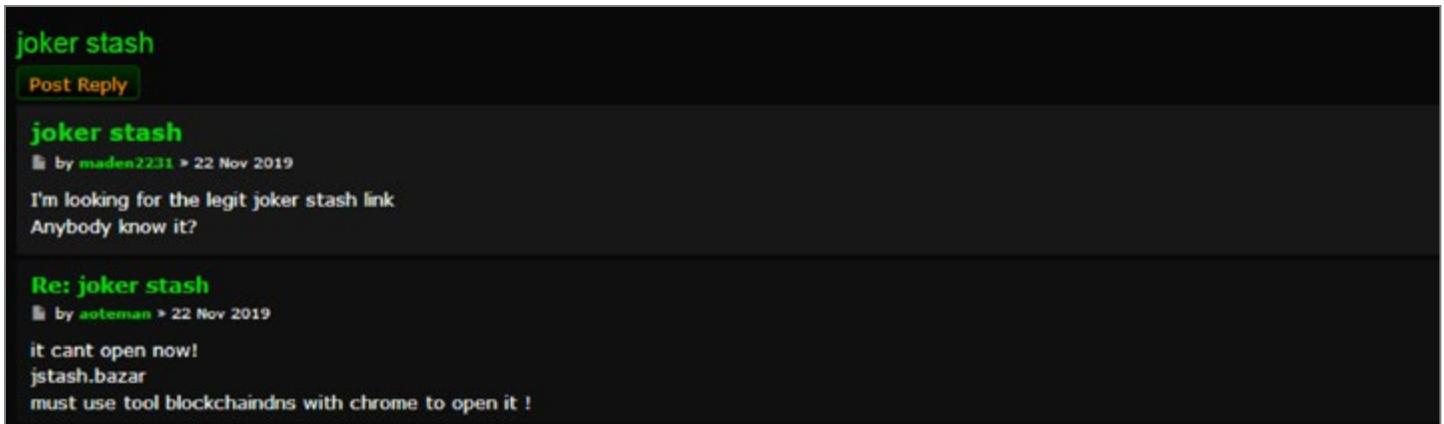
Another factor in threat actors' lukewarm uptake of blockchain technology is the atypical method required to access such sites. Typically, blockchain DNS sites are accessed via Chrome, with a browser extension that enables access to sites with certain URL suffixes. But identifying, downloading, and running the appropriate blockchain DNS extension takes significant skill and knowledge. This much is evident just by scanning the lengthy access instructions provided by Joker's Stash—and by reading the many forum complaints about not gaining access (see Figures 15 and 16).



The screenshot shows a forum post from the 'Joker's Stash' forum. The post is by user 'denisel88' (байт) and was published on January 16. The user 'shad0weh' (shad0weh) has responded, stating: 'Are u stupid or what? I gave you the true link but now you send me fake and ask if it's true... Use only link I gave you, to access it you need a plugin for your browser "blockchain dns"'. The user 'denisel88' has 9 publications and registered on 03.01.2018 (ID: 84 588). The user 'shad0weh' has 0 publications and registered on 03.01.2018 (ID: 84 588). The user 'denisel88' has other activity. The post includes a 'цитата' (quote) button and a reply button.

Figure 14: Exploit user expressing difficulty accessing Joker's Stash via browser plugin

Undeniable appeal: Evidence that forums are still popular



The screenshot shows a forum post on a dark-themed platform. The user 'joker stash' asks for the link to 'Joker's Stash'. Another user, 'auteman', replies that the site can't be opened and provides the URL 'jstash.bazar', noting it must be accessed via 'blockchainDNS' with 'chrome'.

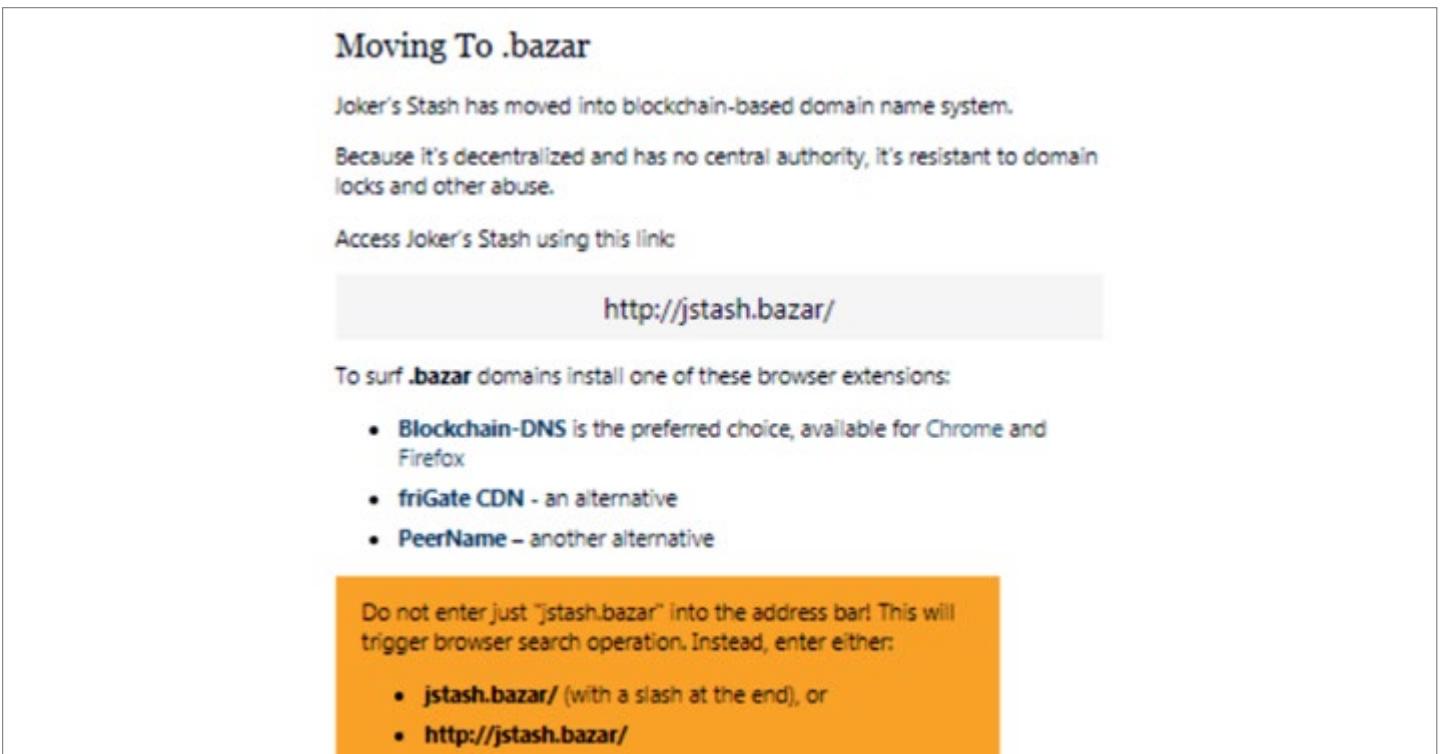
joker stash
Post Reply

joker stash
by [maden2231](#) > 22 Nov 2019
I'm looking for the legit joker stash link
Anybody know it?

Re: joker stash
by [auteman](#) > 22 Nov 2019
it cant open now!
jstash.bazar
must use tool blockchaindns with chrome to open it !

Figure 15: Torum user asking how to access Joker's Stash site

Operational security challenges have also left many threat actors apprehensive when it comes to using blockchain DNS sites. It's not possible to use the extension with a secure browser (such as Tor), meaning the usual "double lock" (secure browser plus VPN) will be lost. Using anything but the latest version of the extension could also expose a user's system details. More-accomplished threat actors would have no problem adapting their usual security posture, but entry-level cybercriminals may balk at such conditions. Uncertain of the benefits this technology presents, many stick with their trusty, accessible cybercriminal forum.



The screenshot shows instructions for accessing the site via blockchain DNS. It includes a note about the site moving to a blockchain-based domain name system, a list of browser extensions for .bazar domains, and a warning about entering the URL directly into the address bar.

Moving To .bazar

Joker's Stash has moved into blockchain-based domain name system.
Because it's decentralized and has no central authority, it's resistant to domain locks and other abuse.

Access Joker's Stash using this link

<http://jstash.bazar/>

To surf .bazar domains install one of these browser extensions:

- [Blockchain-DNS](#) is the preferred choice, available for Chrome and Firefox
- [friGate CDN](#) - an alternative
- [PeerName](#) – another alternative

Do not enter just "jstash.bazar" into the address bar! This will trigger browser search operation. Instead, enter either:

- [jstash.bazar/](#) (with a slash at the end), or
- <http://jstash.bazar/>

Figure 16: Joker's Stash blockchain DNS instructions

Undeniable appeal: Evidence that forums are still popular

AVCs

Using AVCs to efficiently trade credit-card details has been the norm for a number of years, although recent forum discussions suggest that cybercriminals see a downside. In an October 2019 thread on the Russian-language carding forum Omerta, one user advised, “better use a private vendor... all the rest is trash even [sic] joker”, referring to the Joker’s Stash AVC.

The recent [breach of the AVC BriansClub](#), and ensuing surge in attention from the media (and, possibly, law-enforcement bodies), may have led some AVC affiliates (i.e. the suppliers of the stolen credit-card data) to question the risks involved in selling their data to a third-party AVC. Although AVCs offer an alternative to carding forums, they haven’t replaced this method of selling. For credit-card vendors, advertising on cybercriminal forums can mean a bigger profit and greater control over who can view or buy the data.

USA HIGH QUALITY CVV DETAILS - 10 usd per CC

[Post Reply](#)

USA HIGH QUALITY CVV DETAILS - 10 usd per CC

by [cikinaty](#) > 20 Nov 2019

[Report](#) [Quote](#)

PROMO PRICE 10 USD PER CARD ONLY FOR FIRST 10 CUSTOMERS

Data format:

number:expirydate:cvv2:holder:address:city:zip:Email or Phone

For each order free cashout tips.

1. I am selling 100 % live cards with balance on them. The thing you must understand is that many times people think that problem is in their card, not in their skills.

Many cards sold here on Darknet are LIVE with decent amounts on them. People just struggle to card the right way or dont have the right strategy and carding setup for a specific site they are aiming.

And knowing how many beginners are considering themselves to be professionals, nobody is blaming their skills, because its easier to blame cards.

But on the other hand, here also are sold used cards, refurbished, and thats why im coming with this listing, to give you a 100 % working card.

2. I suggest to not go for more than 7-10 % from the balance available in one transaction. 10 % is the maximum limit i recommend, better less. Again, if you are not a beginner, you know that big transactions trigger bank antifraud systems and they cancel your card and call the card holder, especially if cardholder makes online payments very rare. If on card is only 3500 \$ available credit for example, than you can go for a 600-700 \$ transaction which is more than 10 %. But if on cards are 50k \$, a 5000 \$ purchase may kill the card. Hope you get the idea.

WHEN YOU ORDER AND PAY FOR THIS LISTING YOU AGREE TO MY TERMS THAT I AM STATING IN REFUND POLICY

REPLACEMENT POLICY FOR CREDIT CARDS ORDER

WHEN YOU ORDER AND PAY FOR THIS LISTING YOU AGREE TO MY TERMS THAT I AM STATING BELOW

YOU ARE RESPONSIBLE FOR PROPERLY PREPARING YOUR SETUP BEFORE ACCESSING THE ACCOUNT, WHICH CAN INCLUDE A GOOD CLEAN MATCHING SOCKS, RDP/VPS, ANTI DETECT SOFTWARE, ETC. IF YOU ACCESS THE ACCOUNT WITH A PROPERLY PREPARED SETUP YOU WILL BE ABLE TO ACCESS THE ACCOUNT, AND NO SECURITY FLAG WILL TRIGGER.

NO REFUND / REPLACEMENT FOR PHONE VERIFICATION

Figure 17: Forum post selling credit-card details

Why forums are still winning the popularity contest

It's clear that forums aren't giving up the ghost, so what's behind their members' loyalty? The answer lies in several aspects that could apply to even legitimate customer services: a long history and venerable reputation, proof of credibility, guarantees of fair deals. Beyond that, forums also offer an advertising platform and a supportive, knowledgeable community.

Longevity breeds respect

The enduring popularity of forums is, to some extent, driven by their history, especially for Russian-speaking threat actors. Many of the prominent Russian-language cybercriminal forums operating today have a long pedigree. The Photon Research Team spotted a post on XSS that mentioned the "pantheon of the firsts," referring to "the first forums that opened on the Runet¹⁴ in the 2000s," which the post named as Carder Planet, Web Hack, Zloy, Antichat, Exploit, Maza, and DamageLab. The same user said these forums raised "a whole generation of first-class specialists... a whole generation, a whole life, a whole epoch". The reputation of these long-established cybercriminal forums—and the prestige associated with being a forum member—is attractive to many threat actors. Linking to a profile on a hallowed forum is an almost failsafe way to prove your credibility and legitimacy.



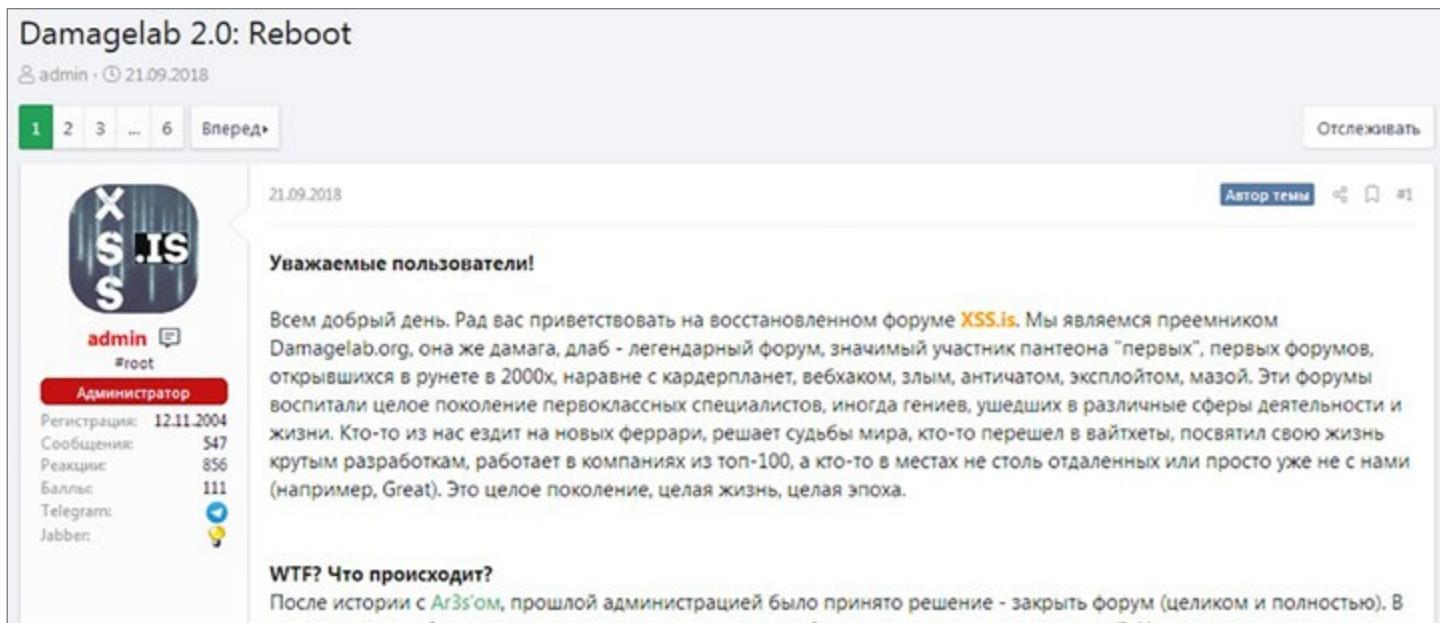
The screenshot shows the XSS homepage with a banner at the top: "For hackers/sellers CC" and "Monetization for your USA CC | Through automated system." Below the banner, there's a section for "UNDERGROUND" with various categories: "Уязвимости web-приложений", "Уязвимости сетей/Wi-Fi/Wardriving", "Malware", "Cracking/Reversing", "Паскаль/Криптари", "IM и Соцсети", and "Франшизы". Each category has a count of posts and messages. To the right, there's a sidebar for "МЫ-ОНЛАЙН" with links to "TOP", "XSS-BIZ", "XSS-IT", "admin@thesecure.biz", and "MarketMS". At the bottom, there's a section for "ПОЛЬЗОВАТЕЛИ ОНЛАЙН".

Figure 18: XSS homepage

In the case of DamageLab, the perceived preeminence of the forum led to one of the most surprising developments in the Russian-language cybercrime landscape in recent years. DamageLab was founded in 2004 and grew to be one of the most prominent Russian-language forums. In December 2017 one of DamageLab's administrators, the Belarusian Sergey Yarets, was arrested in a joint operation of Belarusian, United States, and European police forces for his involvement in the forum and in the Andromeda¹⁵ botnet.¹⁶ Following the arrest of "Ar3s" (Yarets's username on the forum), the remaining DamageLab administration team decided to close the forum entirely to protect the userbase from further investigation by the authorities.

Why forums are still winning the popularity contest

What's unusual is that, almost a year (late 2018), the former administrator of the high-profile Exploit purchased a back-up of DamageLab, dating back to late 2015, and reopened the site. The new administrator vowed that the forum would never again work under its old name because it would be "unsafe, unethical, and bad for karma". They rebranded the site "XSS" and set about restoring, rebuilding, and attracting new members.



The screenshot shows a forum post on the XSS forum. The post is titled "Damagelab 2.0: Reboot" and is dated 21.09.2018. It is made by the user "admin". The post content is as follows:

Уважаемые пользователи!

Всем добрый день. Рад вас приветствовать на восстановленном форуме XSS.is. Мы являемся преемником Damagelab.org, она же дамага, длаб - легендарный форум, значимый участник пантеона "первых", первых форумов, открывшихся в рунете в 2000х, наравне с кардерпланет, вебхаком, злым, античтом, эксплойтом, мазой. Эти форумы воспитали целое поколение первоклассных специалистов, иногда гениев, ушедших в различные сферы деятельности и жизни. Кто-то из нас ездит на новых феррари, решает судьбы мира, кто-то перешел в вайтхеты, посвятил свою жизнь крутым разработкам, работает в компаниях из топ-100, а кто-то в местах не столь отдаленных или просто уже не с нами (например, Great). Это целое поколение, целая жизнь, целая эпоха.

WTF? Что происходит?

После истории с Ar3s'ом, прошлой администрацией было принято решение - закрыть форум (целиком и полностью). В

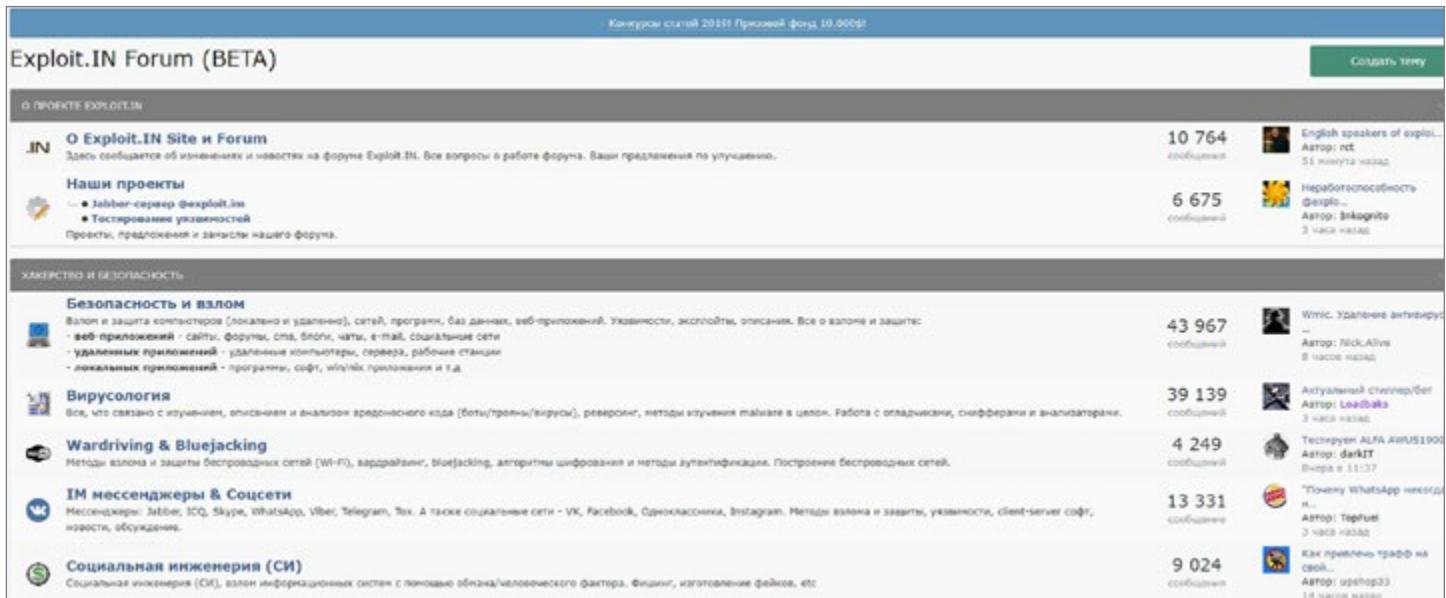
Figure 19: Message announcing reboot of DamageLab

Despite the apparent dangers of operating on a platform associated with an individual known to law-enforcement agencies, the forum has flourished. Membership numbers have grown and the forum now boasts highly skilled threat actors prepared to discuss cutting-edge attack techniques and trade high-value offerings. This success has occurred, in no small part, thanks to the heritage of the forum; many of the older members are still active participants who contribute knowledge and experience.

Even Ar3s, who's now been released from prison (six months in custody meant his fine was waived),¹⁷ holds a legacy role on XSS and has recently been appointed as a moderator of Exploit. And the new XSS administrator used the reputation they acquired as the administrator of Exploit to build trust in their new venture. (This individual has also ridden the coattails of their Exploit success to promote other projects, including a marketplace and a Jabber server.) The prestige and longevity of DamageLab outweighed the potential negative implications of restoring a defunct forum; Ar3s's experiences with the law are often called upon by other forum members and his opinions highly valued.

Promoting a forum by relying on a site's previous reputation has even taken place in the English-language cyber community. The hacking forum Hell, which was taken down in a law-enforcement operation in July 2015, reappeared in early 2016 as Hell Reloaded. One of Hell's original moderators, who created the sequel site, tried to market the new forum and attract new members by relying on the illustrious name of the defunct forum. But many new users remained wary, suspicious that the site was a security services "honeypot". Hell Reloaded is no longer active.¹⁸

Why forums are still winning the popularity contest



The screenshot shows the homepage of Exploit.IN Forum (BETA). At the top, there is a banner for a competition with 10,000€ in prize money. Below the banner, the forum's name is displayed, along with a 'Create topic' button. The main content area is divided into several sections:

- Проекты Exploit.IN**: A section for news and updates about the forum's projects, with 10,764 messages.
- Наши проекты**: A section for forum projects, with 6,675 messages. It includes a link to the 'Jabber-сервер Exploit.IN' and a link to 'Тестирование уязвимостей'.
- Хакерство и взлом**: A section for hacking and cracking, with 43,967 messages. It includes a link to 'Wi-Fi: Удаление антиворус'.
- Вирусология**: A section for viruses and malware, with 39,139 messages. It includes a link to 'Актуальный спиллер/баг'.
- Wardriving & Bluejacking**: A section for wardriving and bluejacking, with 4,249 messages.
- IM мессенджеры & Соцсети**: A section for instant messaging and social networks, with 13,331 messages. It includes a link to 'WhatsApp не работает'.
- Социальная инженерия (СИ)**: A section for social engineering, with 9,024 messages. It includes a link to 'Как прокачать трафик на свой...'.

Figure 20: Homepage of Exploit, which has operated continuously since 2005

A forum like Exploit, which has operated continuously since 2005, attracts users who are aware of the reputation it has built up over many years and the prestige they'll gain as a member, but are also aware of its demonstrable success in surviving threats that have taken down other forums. Forum users who choose Exploit feel safe that time and energy put into building a brand and customer base on the forum will not be wasted.

These forums' extraordinary longevity also means that the sites hold invaluable repositories of cybercrime-related content spanning many years. Exploit, for instance, boasts over a million posts containing discussions, advice, guidance, and recommendations. Sites like Hackforums, which has operated since 2009, are attempting to capitalize on their lifespan and significance of information by promoting themselves as educational resources, rather than simply hacking forums (an approach that may also help deflect unwanted attention from the authorities).

Trust issues

In terms of basic capability, there's very little a threat actor can do on a messaging platform that they can't also achieve on a forum. Several forums have added chat functionalities, enabling users to communicate in groups—as on a messaging platform's public groups or private channels, or in one-to-one conversations. Many forums also promote the privacy of this feature, ruling that forum administrators do not have the ability to read users' private messages.

Why forums are still winning the popularity contest

But there's a major difference between communicating via a messaging service and via a forum: the amount of associated user information. Many messaging services strip away as much data as possible about their users. Often, the only information available is a username, a handle, and maybe an avatar. Some services also allow a short biography. This lack of information is touted as an advantage: Surely, in a world in which staying anonymous is paramount, providing few details to your interlocutor is optimal?

Paradoxically, however, in a world of shadows and anonymity, more information can be the key to success. It's very difficult to judge whether it's safe to trust a username and avatar on a messaging service, especially when you can't see how that user has interacted with other threat actors. Although cybercriminals undoubtedly don't want to reveal any of their real-life, personal information, for successful transactions they need to present details of their online identities. Forums let them build up entire virtual personas.

A forum member considering interacting for the first time with another user will likely be able to see a history of that user's previous forum activity. They can judge their credibility accordingly, considering several factors:

- When did the user join the forum?
- How many posts have they made?
- Do they initiate their own threads or just reply to other members' threads?
- What have they bought? What have they sold?
- How involved are they in "forum life"—do they contribute to community threads? Highlight bugs? Suggest ways the forum can improve?
- How have other forum members reviewed this user's services? Have they reported any problems?

Illogically, trust is even more important in the cybercriminal underground than in everyday life. When there's no information available on an individual's real identity, threat actors can rely only on trust when making decisions. Should they send hundreds of dollars to a vendor in the hope of receiving what they've ordered? Reviewing a user's past activity on a forum can help determine whether they're a credible forum member, an inexperienced threat actor, or—even worse—a scammer, researcher, or law-enforcement official.

Forums promote countless tools and systems that can aid their members in making such assessments. Many English-language cracking forums have "leecher" or "lurker" ratings to highlight users who don't contribute to forum life, resulting in a ban during the frequent member culls. And most forums operate a system for members to award positive or negative reputation points to a user. This can either reflect the results of a transaction or an opinion on the user's contribution to a thread. Negative points can lead to a ban on some forums, so it's in members' interests to try to ensure their score is as high as possible, and they value this opportunity; Exploit removed its reputation system following a site redesign, prompting many users to clamor for its restoration.

Why forums are still winning the popularity contest

Automatic Leecher Banning

Last night I banned 1850 members who had a post counter great than 50 and 0 threads.
From now on we have a task that runs every sunday that will automatically ban members with the following criterium:

- Post Count: Greater than 50
- Thread Count: 0
- Usergroup: 2 (Registered Member)

Those new measures will help to keep the forum clean. It might decrease some statistics (new members per day, new threads per day) but it will also increase the overall quality. Quality beats quantity.

Best regards,
floralN

Figure 21: CrackedTO announcement of leecher banning

There are a host of other ways to boost member trust. Some forums that focus heavily on the sale of goods and services will close a thread temporarily after it begins, so that moderators can verify the vendor's claims. Many forums operate a status system for users with a long tenure and high post count to move up through the ranks of the site; users with a higher rank are automatically afforded greater respect. On some forums, users can only attain a certain rank by being vouched for by other forum members—a sure sign of legitimacy. Still other forums allow users to pay to increase their status, because making such a payment would be undesirable or impossible for some law-enforcement officials, and for individuals looking to just scam other users.

The Photon Research Team has found that strict forum rules and conventions also help build a picture of an individual. A user who contributes to forum life and answers other users' questions is more likely to be genuine. Substantive answers and posts also indicate a user's knowledge and experience. Users who only ask, or leave inconsequential replies, are likely to be inexperienced amateurs. Many forums rule that posts must contain meaningful content, and allow negative reputation points to be awarded for so-called empty posts.

Why forums are still winning the popularity contest

“Free” advertising

A good reputation and positive user feedback can also be invaluable to a threat actor marketing goods or services. Whether promoting offerings on other forums or updating existing advertising threads, linking to a high-scoring forum profile or appreciative reviews from other forum users is one of the only ways threat actors can try to convince other members to enter into a transaction. Sometimes they even try to use positive reviews to distract attention from problems they’re experiencing. The founder of the recently established MagBo shells shop, “mrbo”, used a thread containing positive reviews on the Russian-language cybercriminal forum Antichat to promote their site on XSS, despite admitting in the same post that they had been banned from Exploit.

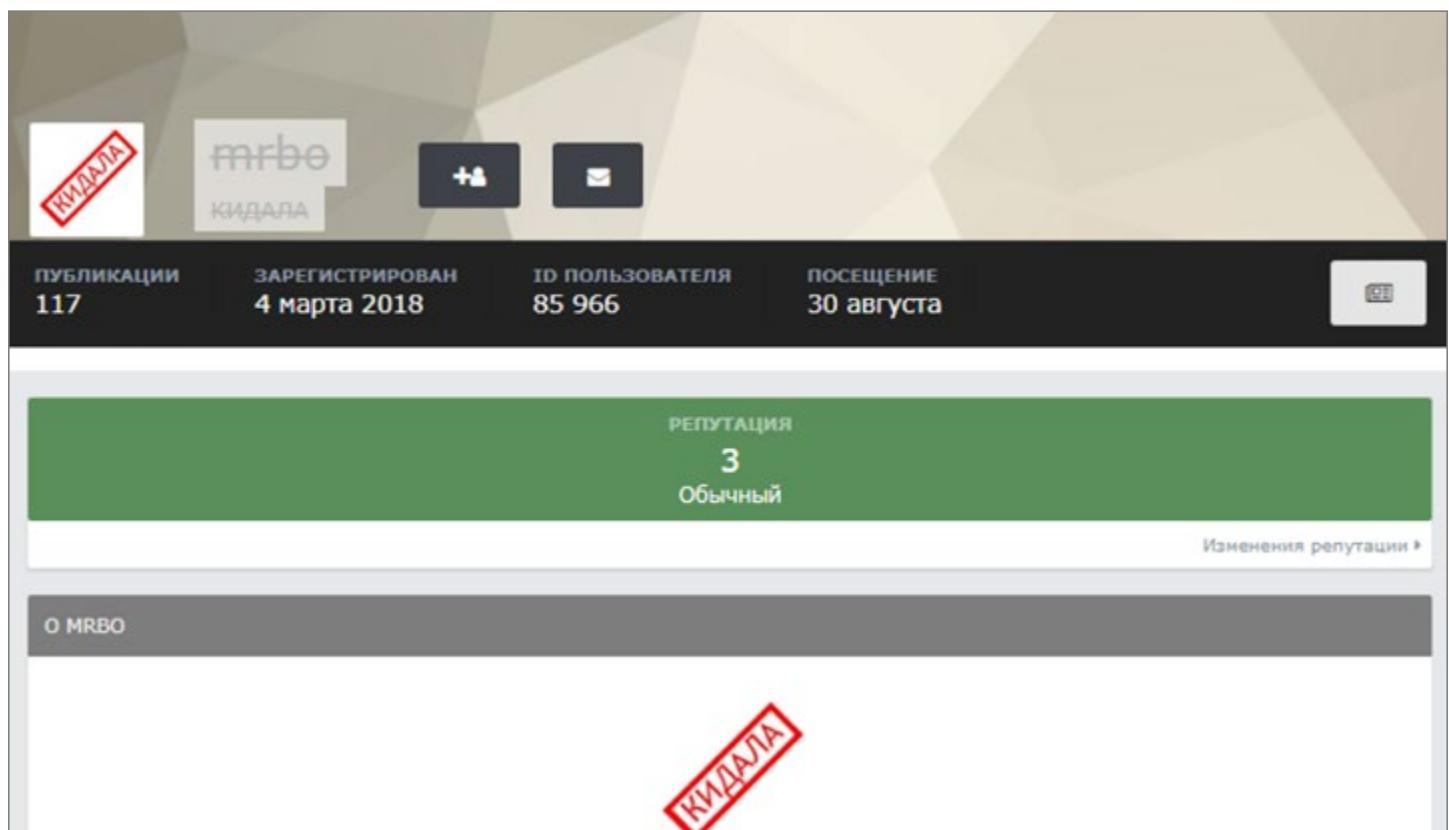


Figure 22: mrbo user profile

Forums’ utility as advertising platforms represents another advantage over alternative technologies. Very few threat actors can operate successfully on alternative platforms alone, finding that forum membership widens the userbase to which they can advertise their goods and services. In a November 2019 discussion on the English-language cracking forum CrackedTO, many users admitted that they had fewer than 50 “friends” on the messaging platform Discord, indicating that the level of exposure on a messaging app is often much lower than on a forum.

Why forums are still winning the popularity contest

It's common for a threat actor to use the same username across discrete forums, establishing a marketing persona, and to extend that "brand" to alternative channels. The prolific travel fraudster "Sergik00", who's offered fraudulent airline tickets and hotel bookings on forums for almost four years, directs interested buyers to their Telegram channels to make orders. We've even seen them work their Telegram handle into custom advertising graphics included in their threads. Crucially, however, Sergik00 has maintained a footprint across a wide variety of cybercriminal forums and included positive customer feedback in their dedicated threads, building their brand across multiple sites.



Figure 23: Sergik00's travel offerings

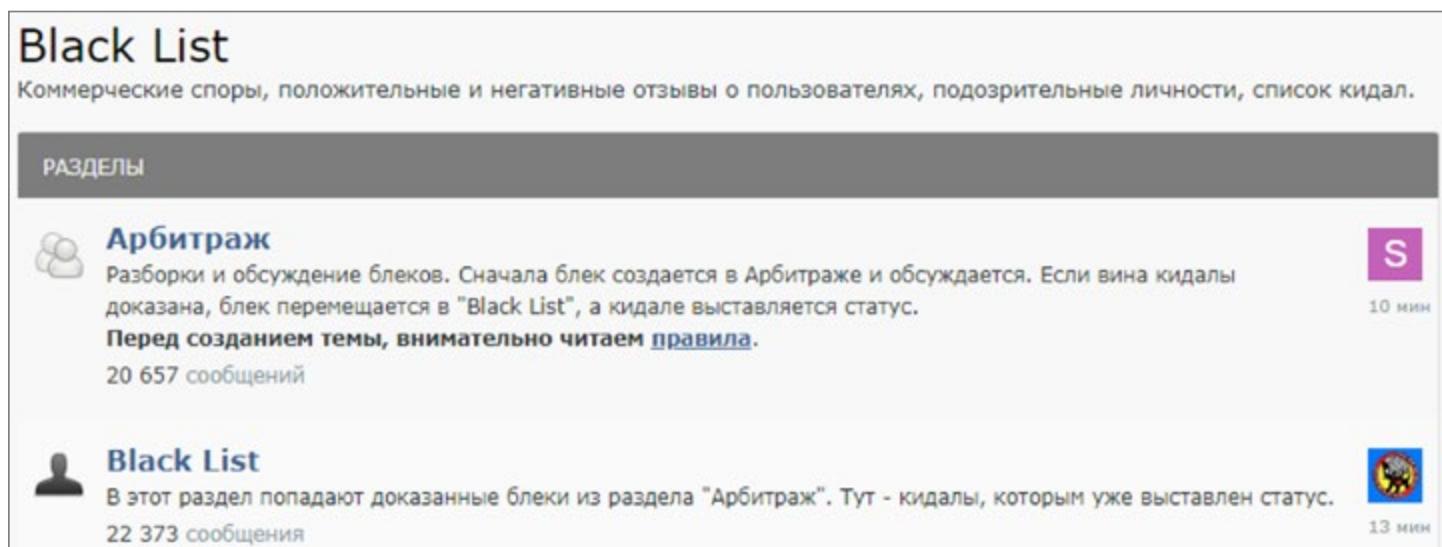
Similarly, the operators of the carding scheme Project13 use Telegram in a variety of ways—with separate European and United States accounts to deal with user orders and a Telegram bot to field user queries. But even with this extensive Telegram infrastructure, they still maintain active advertising threads on numerous Russian-language forums. Even the notorious carding AVC Joker's Stash updates multiple dedicated forum threads each time they upload a large set of new card details to their site.

Why forums are still winning the popularity contest

The ease of arbitration

Another shortcoming cybercriminals see in using alternative platforms is the high risk of falling victim to fraud, and having no recourse if they do. If a threat actor operating exclusively on Discord or Wickr refuses to sell another user a data set after the deal is made, there's not much the buyer—or anyone else—can do about it. The injured party doesn't even have a place to air their anger. But Russian-language cybercriminal forums have built-in justice systems designed to settle disputes, ensure parties stick to the terms of an agreement, and punish wrongdoers.

In general, most forums have a well-used arbitration section, in which users can create threads when they feel deceived by another forum member. Such disputes usually revolve around one party failing to pay the agreed price in a transaction, failing to deliver goods by an agreed deadline, or providing goods that fall short of their description.



The screenshot shows a forum interface with a dark theme. At the top, a banner reads 'Black List' in large white text, with a subtext in Russian: 'Коммерческие споры, положительные и негативные отзывы о пользователях, подозрительные личности, список кидал.' Below this, a dark grey bar contains the word 'РАЗДЕЛЫ' in white. The main content area is divided into two sections: 'Арбитраж' (Arbitration) and 'Black List'.

Арбитраж
A user icon with three people is shown next to the title. The text explains the process: 'Разборки и обсуждение блеков. Сначала блек создается в Арбитраже и обсуждается. Если вина кидалы доказана, блек перемещается в "Black List", а кидале выставляется статус.' Below this, a bold instruction reads: 'Перед созданием темы, внимательно читаем [правила](#)'. The count '20 657 сообщений' (20,657 messages) is displayed.

Black List
A user icon with a person is shown next to the title. The text states: 'В этот раздел попадают доказанные блеки из раздела "Арбитраж". Тут - кидалы, которым уже выставлен статус.' The count '22 373 сообщения' (22,373 messages) is displayed.

Figure 24: Exploit arbitration section

The claimant initiating an arbitration thread should provide all contact details the defendant has used (e.g. Jabber IDs), any other usernames by which they are known, and the logs of one-on-one conversations detailing the full negotiations between the two parties. Forums usually have templates for arbitration claims that participants must use. The forum arbiter can then read through the conversation logs and call upon the defendant to provide their version of events or evidence of their innocence. Other forum members will also supplement the discussion; sometimes these users have also been wronged by the defendant, but sometimes they're contributing out of a sense of community spirit.

Eventually the forum arbiter comes to a decision, usually giving the defendant a chance to pay back any money owed, if they're judged to be guilty. If the defendant fails to make this payment, or if their crimes are considered too egregious, the forum arbiter will ban them from the site. The defendant's name will then be placed on a blacklist as a warning to other forum members not to interact with their username. Resolved arbitration cases

Why forums are still winning the popularity contest

in which the defendant was not banned are also kept as “public” record. This means forum users considering transacting with an unfamiliar vendor can see any arbitration cases involving that vendor.

On some forums, the justice system is even more involved. Verified, a high-profile Russian-language cybercriminal forum specializing in carding, runs a compensation system whereby wronged parties can recoup some of their losses. The user who scammed them may have deposited funds with Verified, and their victim/s can apply to receive those funds. In most cases, guilty defendants have more than one victim; once all users have made claims against them, a member of the forum team steps in to dole out funds proportionally, according to the users’ claims. In most cases, the wronged parties are owed much more than the funds deposited by the fraudster in the forum, but at least they receive some form of compensation.



Компенсация				
Создать новую тему		Темы раздела: Компенсация		
Объявление: Правила раздела / Section rules		07.08.2005		
Тема / Автор		Последнее сообщение	Ответов	Просмотров
Cinderella - компенсация с депозита hound_1		28.10.2019 17:05 от INC. ⚡	1	82
bigresseller - компенсация с депозита KV777		17.10.2019 13:39 от VR_Support ⚡	1	93
Linnman23 - компенсация с депозита васик		15.10.2019 12:10 от VR_Support ⚡	3	161
Vist999 - компенсация с депозита lester567		05.09.2019 16:32 от INC. ⚡	1	153
irnnn - компенсация с депозита John Doe		16.08.2019 18:49 от VR_Support ⚡	2	132
супровбосс - компенсация с депозита		26.07.2019 12:38 от VR_Support ⚡	2	196

Figure 25: Verified compensation section

In one extraordinary example of forum justice, observed on the Russian-language Antichat, a user applied for paid coding work on a project organizing “cryptoattacks”. Despite passing the interview tests and being promised work and payment by the project organizer, the user never received any funds. When complaining about this injustice on the forum, the user explained that they needed the money to pay for their father’s cancer medication. Other forum members also claimed to have been deceived by the project organizer, and shared their own correspondence. Ultimately, the Antichat administrators banned the project organizer and arranged a “whip around” among forum members, to raise funds for the medical treatment. As a result, the forum transferred USD 700 to the defendant. This kind of help from a supportive community does not exist on platforms other than forums.

Why forums are still winning the popularity contest

16 Feb 2018 #107

Rebz said: ↑

от **scoring0**
BTC: 1J5CX5YUzoD6wZG9X1FPxPiG3jMUNQr2Po

Желательно пишите сюда сколько скинули в \$.

Ушло примерно 700\$ (коллективная сумма).

..: Аудит Безопасности сайта :..

-> Отдельные правила для тех, у кого репутация меньше 5 пунктов

Открылся новый раздел Блокчейн, криптовалюты, смарт-контракты

Veil, scoring0 and crlf like this.

16 Feb 2018 #108

Rebz said: ↑

Ушло примерно 700\$ (не только от меня).

Я не знаю как сказать спасибо. Ребзу уже озвучил в пм: починю линуксы(сваяю практически любую настройку, кроме сложных кластеров), чутка смыслу в ИБ. Все, кто скинулся - пишите в пм, я скажу спасибо тем, что умею, если у вас есть необходимость.

scoring0
New Member

Joined: 6 Nov 2017
Messages: 20
Likes Received: 2
Reputations: 0

Figure 26: Announcement of sum sent to user for medical treatment, with subsequent message of thanks

Why forums are still winning the popularity contest

Sense of community

The previous case is just one example of the sense of community spirit that prevails on cybercriminal forums and contributes to their continued persistence. The forum community even celebrates together: Members wish each other a happy birthday or send New Year's greetings, and Exploit even celebrated Halloween.



Figure 27: Exploit Halloween banner

By contrast, messaging services, marketplaces, and AVCs are almost exclusively platforms for buying and selling goods and services, and this doesn't satisfy all users. The Photon Research Team has observed users on CrackedTO bemoaning the transactional nature of Discord, for example. Forums offer a place to conduct transactions but come with the added bonus of the knowledge and skills of an entire userbase, arguably enhancing trading. On a forum a threat actor can open up discussions with specific vendors, to ask for details of other goods the vendor offers, or inquire about the geographies/systems that can be targeted; in a marketplace, that threat actor can only send limited queries about a specific listing. Several well-known marketplaces, including Rapture, Empire, Olympus, and HYDRA, have even run forums alongside their main marketplace offering, to facilitate further discussions and reap the benefits of a forum community.

A good example of cybercriminal forums' community-mindedness lies in the discussions on most major Russian-language forums about law-enforcement activity. In dedicated sections their users discuss the fate of fellow members who've fallen foul of the police or intelligence services, sharing as many details about their story as they can find, so the community can learn from that user's mistakes. Users often post news articles about cybercriminals' arrests, forensically examining the details of the case to work out how they were caught.

For example, a discussion arose on Exploit about the case of hacker Roman Seleznev, who was sentenced to 37 years' imprisonment for credit-card fraud in 2016. One user said Seleznev was aware of Western intelligence agencies' interest in him but chose to travel abroad for a vacation anyway. He was caught "while passing through passport control at an airport in a country without an extradition agreement with the United States", the forum user said. The user also said officials discovered Seleznev's real-life identity because he used the same email address his wife used for social media as a back-up email address that received malware logs. When Exploit users moved on to discuss the danger of Russian-speaking cybercriminals travelling abroad, one forum member remarked darkly, "Russian resorts are better than American prisons."

Even more striking is the propensity of forum members who have had brushes with the law to return to the forum, then share the details of their experience with the community. XSS user "maza-in"—the supposed creator of the "Anubis" banking trojan—was arrested in early 2019, but that didn't mark the end of their forum activity. maza-in's arrest had followed an investigation by an unspecified Russian security force, and in August 2019 XSS users posted links to local news websites in Stavropol, Russia, saying maza-in was due to appear before Stavropol military court with an unnamed accomplice. In October 2019 maza-in reappeared on XSS with a new username (appending "1" to the end of their previous moniker) to provide details about the circumstances of their arrest.

Why forums are still winning the popularity contest

Рассказ об аресте maza-in (от 1го лица)

maza-in1 · 16.10.2019

1 2 3 4 5 Вперед Отслеживать

16.10.2019 Автор темы

NO AVATAR
maza-in1 floppy-диск
Пользователь
Регистрация: 16.10.2019
Сообщения: 5
Реакции: 19
Баллы: 8



Всем привет, сегодня я расскажу о ситуации которая со мной произошла, а точнее как меня арестовали. Буду

Figure 28: maza-in1's post recounting the story of their arrest

maza-in1 wondered whether their “excessive self-confidence” had “destroyed” them, adding that they had been “ruined” by “a careless attitude to security”. They explained that they had registered an email account using a “white” IP address (i.e. legitimate and not shielded by VPN technology) and then used that email address to sign up to Exploit. maza-in1 allegedly had no intention of engaging in cybercrime when they registered on Exploit, so they didn’t consider the security implications of using the email address. maza-in1 stated that their former partner, “cccalypse”, hadn’t been arrested because they were so “paranoid” about monitoring their anonymity.

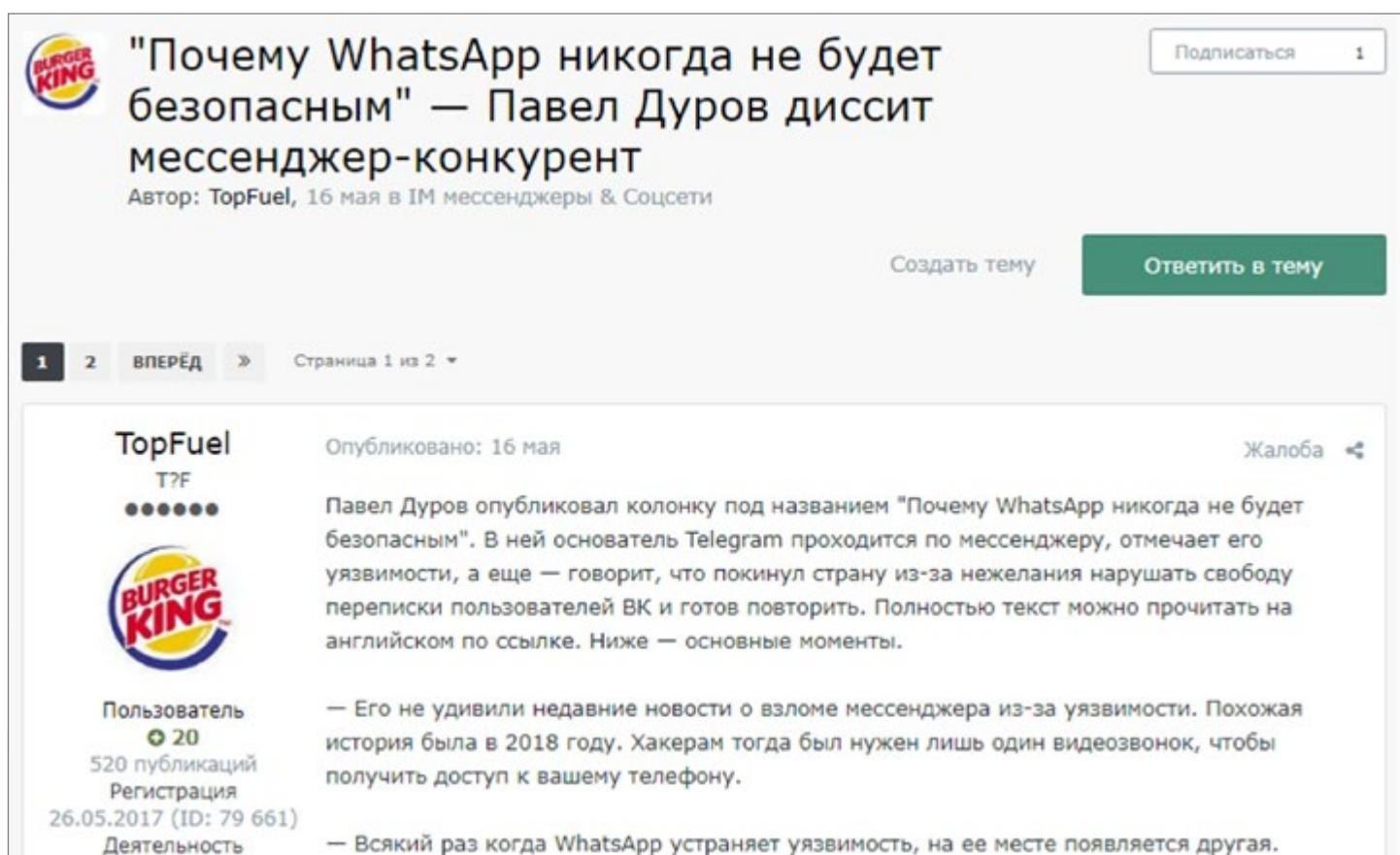
Ultimately maza-in1 was sentenced to 18 months’ imprisonment on probation, confiscation of documents, and a fine of RUB 120,000 (USD 1,872). They claimed that they were “saved” from a harsher sentence for not having targeted countries in the Commonwealth of Independent States and there being no identifiable “injured party”. Although some XSS users were suspicious of maza-in1’s return, the community was generally welcoming, valuing the insight into the criminal justice system and the small mistakes that could lead to capture. Cybercriminals can’t find such continual insight anywhere online except a forum.

Why forums are still winning the popularity contest

Airing doubts about alternative technologies

A key concern for cybercriminals when choosing where and how to operate is security, and how easy it is to maintain absolute anonymity. Relying on new technologies and messaging services for security—no matter how ostensibly secure they are—ineliminately means trusting those platforms' operators not to compromise their users' anonymity, either deliberately or inadvertently.

Consider Telegram, which has come under sustained pressure from the Russian authorities to share the app's encryption keys with the security services. A Moscow court even banned Telegram in April 2018, although Russia-based users continue to use the app via VPNs.²⁰ Telegram creator Pavel Durov left Russia in 2014 following repeated clashes over his other project, the social network VKontakte. Although Durov regularly asserts that he'll never give in to the Russian government's demands, it's possible to imagine circumstances arising that could compel him to agree.



The screenshot shows a forum post from a Russian-speaking community. The post is titled "Почему WhatsApp никогда не будет безопасным" (Why WhatsApp will never be safe) by Pavel Durov, dated May 16, 2018. The post discusses the security of WhatsApp and its founder, Pavel Durov. The post has 1 reply. The user TopFuel, who is a Burger King impersonator, has 2 posts and 520 publications. The post content includes a link to the full article and a summary in Russian. The summary states that Pavel Durov published an article about WhatsApp's lack of security, mentioning vulnerabilities and the 2018 hack. The post ends with a note that WhatsApp fixes one vulnerability only to introduce another.

"Почему WhatsApp никогда не будет безопасным" — Павел Дуров диссит мессенджер-конкурент

Автор: TopFuel, 16 мая в IM мессенджеры & Соцсети

Создать тему Ответить в тему

1 2 ВПЕРЁД Страница 1 из 2

TopFuel Опубликовано: 16 мая Жалоба

Павел Дуров опубликовал колонку под названием "Почему WhatsApp никогда не будет безопасным". В ней основатель Telegram проходится по мессенджеру, отмечает его уязвимости, а еще — говорит, что покинул страну из-за нежелания нарушать свободу переписки пользователей ВК и готов повторить. Полностью текст можно прочитать на английском по ссылке. Ниже — основные моменты.

— Его не удивили недавние новости о взломе мессенджера из-за уязвимости. Похожая история была в 2018 году. Хакерам тогда был нужен лишь один видеозвонок, чтобы получить доступ к вашему телефону.

— Всякий раз когда WhatsApp устраниет уязвимость, на ее месте появляется другая.

Figure 29:: Exploit users discuss WhatsApp

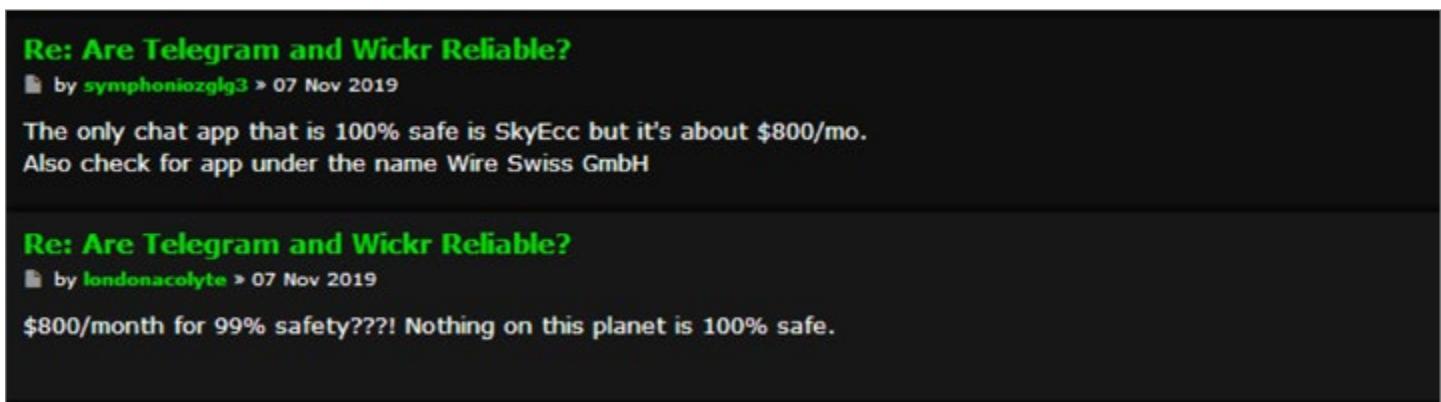
Not only are cybercriminals subject to the behavior of messaging app operators, but services may have vulnerabilities that can put user security at risk. Commercial spyware, such as Pegasus, has [exploited a vulnerability in WhatsApp](#) to infect user devices and intercept communications. The infection was triggered after a WhatsApp call to the target's phone, which allegedly didn't require the user to answer the call. Pegasus can also remove any trace of the infection from the device's communication logs. Users on Exploit have repeatedly

Why forums are still winning the popularity contest

discussed the security of WhatsApp; in one example thread from May 2019, a long discussion was prompted by Pavel Durov's own comments that WhatsApp would "never be safe".

Reflecting on the reliability of messaging apps, a Torum user said (verbatim): "I know peoples that have been busted cause to wickr, snapchat and whatsapp. Telegram has been cracked by feds too a year or two ago (I remember a big seized of terrorist weapons thanks to Telegram)." Another forum user warned on Verified: "don't use whats[app]/viber, the FBI have already downloaded conversations from there. telegram at your own risk."

In general, conversations about operational security and anonymity are common on cybercriminal forums: In the same thread on Torum as mentioned above, another user opined, "The only chat app that is 100% safe is SkyEcc but it's about \$800/mo." In a different thread on a similar topic, a member claimed: "With high level of resources, any centralized messaging service can potentially be compromised. I am not saying it is easy, but it is still a possibility that should be considered."



The image contains two screenshots of forum posts from the Torum platform. The first post, titled 'Re: Are Telegram and Wickr Reliable?' and dated 07 Nov 2019 by 'symphoniozg13', states: 'The only chat app that is 100% safe is SkyEcc but it's about \$800/mo. Also check for app under the name Wire Swiss GmbH'. The second post, also titled 'Re: Are Telegram and Wickr Reliable?' and dated 07 Nov 2019 by 'londonacolyte', states: '\$800/month for 99% safety??!! Nothing on this planet is 100% safe.'

Figure 30: Torum users discuss app safety

If we judge by these frequent conversations, many forum users seem to see an innate disadvantage in messaging apps. This is because the safety of the teams running the app services doesn't depend on the apps remaining secure; on a forum the administrator is, in most jurisdictions, committing a criminal act by running their platform. They have a vested interest in keeping the forum as secure as possible, maintaining their own anonymity and that of their members. Understandably, the teams behind forums take this responsibility seriously.

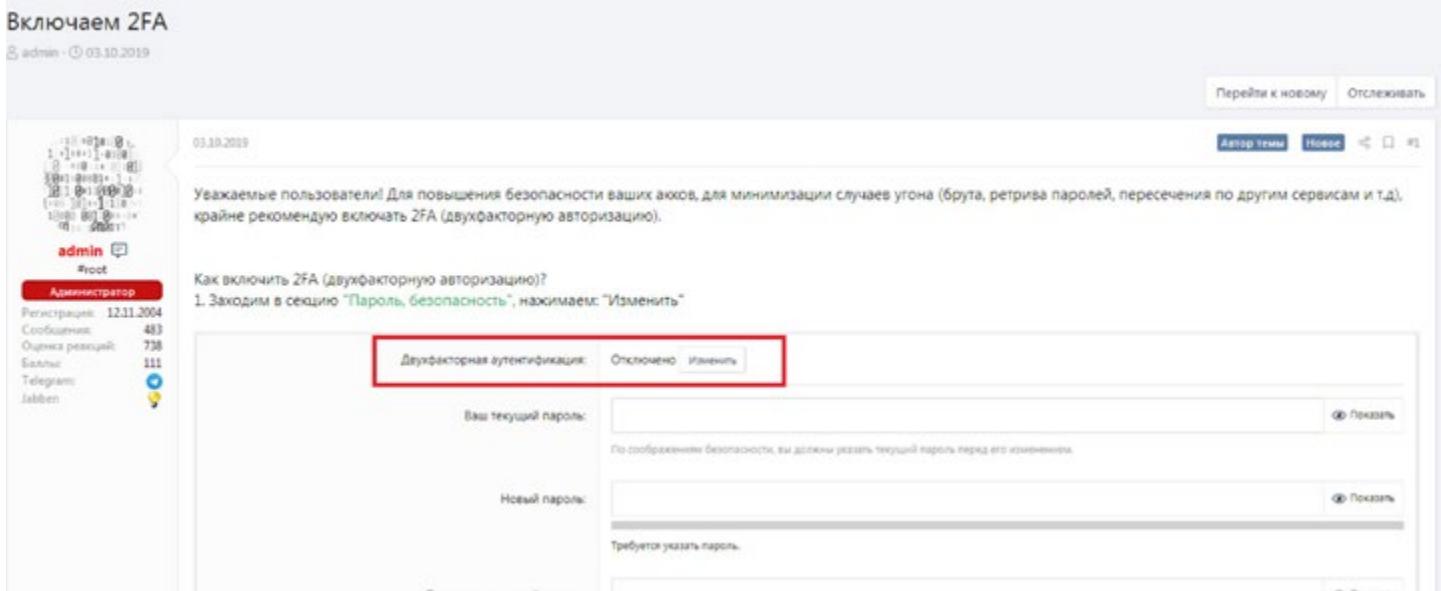
The now-defunct English-language forum KickAss prioritized security to such an extent that forum users were disadvantaged. In late 2018 the administrator removed all time and date stamps from posts, probably to thwart police forces' efforts to collate intelligence for their enquiries. But the side effect is that it also made the forum much more inconvenient for its members to use. The CrackedTO forum also employed this tactic, as did the English-language Carding Forum—which also went so far as to expunge all user IP address information from forum logs (to impede investigations if the log database were seized).

A final downside to using legitimate messaging services is the risk that the companies behind them will not tolerate criminal activity. In one discussion on CrackedTO, users noted that they had been subject to regular bans on Discord for breaking that platform's rules on permitted activities.

The future of forums: Is there an end to the trend?

Despite the age—and ostensible outdatedness—of the forum model and technology, forum administrators show every sign of striving to ensure these platforms remain popular in years to come. They're acknowledging the primary concerns of their users, as described above: security, trust, and anonymity.

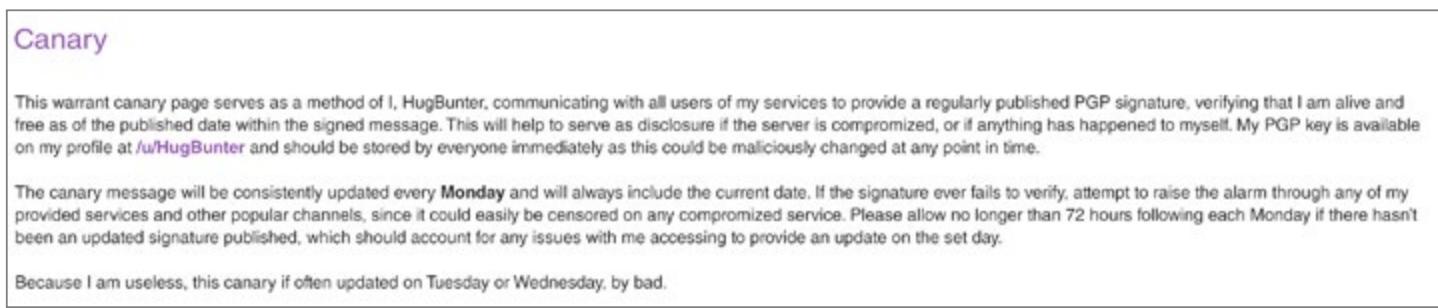
Three major site updates, all recorded in October 2019, demonstrate forums' future-looking stance. Firstly, XSS introduced two-factor authentication (2FA). The forum administrator said the move was intended to increase the security of users' accounts and minimize the risk of such compromises as "brute-force cracking attacks, [unauthorized] password retrieval, and interceptions by other services".



The screenshot shows a forum post titled "Включаем 2FA" (Enabling 2FA) by user "admin" on October 3, 2019. The post contains a message in Russian encouraging users to enable 2FA for better account security. It includes a link to a password change page where the "Two-factor authentication" setting is highlighted with a red box. The page shows fields for the current password and a new password, with a note that the current password must be entered before changing it.

Figure 31: XSS 2FA announcement

Next, the English-language forum Dread introduced a "Canary" feature, aimed at updating forum members of the status of Dread's administrator and their control of the forum. These weekly updates, conducted via a personalized, cryptographically signed message from the administrator, were likely introduced following that individual's September 2019 disappearance from the forum, which threw the community into disarray. The Canary feature demonstrates a clear intent to sustain the credibility of the forum, eliminate the potential for a law-enforcement takeover, and avoid a takeover by someone masquerading as the legitimate administrator.



The screenshot shows a forum post titled "Canary" by user "HugBunter" on October 3, 2019. The post contains a message in English explaining the purpose of the Canary feature: to provide a regularly published PGP signature to verify the administrator's status. It also includes a note about the consistency of the update schedule and the importance of storing the PGP key. The message is framed by a box.

Figure 32: Dread Canary feature announcement

The future of forums: Is there an end to the trend?

Lastly, Verified introduced a free version of registration that allows users limited access to the forum's escrow system. Many forums run escrow services, in which a third-party guarantor ensures that both buyer and seller receive what they expect from a transaction. Making use of this function provides added reassurance to sellers that they are dealing with a credible buyer rather than a scammer, researcher, or security service representative, all of whom would be reluctant to commit funds in this way. Verified offering their escrow system to users for free—rather than requiring a full Verified membership—extends the forum's reach even beyond the bounds of the site.

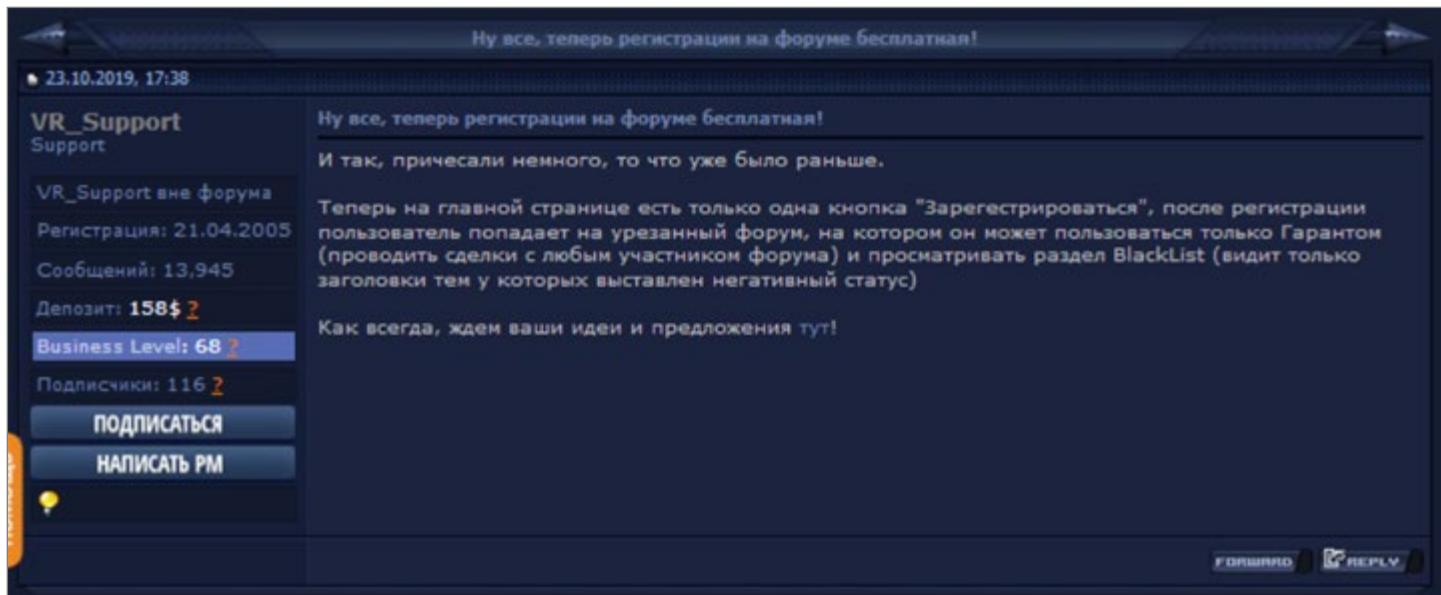


Figure 33: Verified free registration announcement

We've also seen cases of forum users taking it upon themselves to bolster their security, rather than relying on directives from forum administrators. In recent months both English- and Russian-language forum users have started [taking advantage of escrow services when transactions have barely even been initiated](#). Interested buyers usually contact vendors to request more details about their advertisement, such as screenshots of internal system access that prove that the offering is legitimate. But recently many vendors have begun insisting that buyers place money in a forum escrow service before they send any additional details.

The drive to pioneer new features and site improvements, to adapt to a changing security landscape, suggests that the threat actors running cybercriminal forums recognize the necessity to provide value for their users. Even long-established forums see the need to innovate; Exploit recently embarked on an entire site redesign. Forum members themselves take an active role in suggesting improvements or changing the way they use forums. With this continuous push for improvement, and the host of features and benefits simply not obtainable from other types of technologies, it's highly unlikely that cybercriminal forums' popularity will diminish in the coming years. Instead, the symbiotic relationship between alternative technologies and forums—in which the former can't thrive without the latter—will flourish.

Endnotes

¹ https://en.wikipedia.org/wiki/Internet_forum#History

² <https://www.infosecurity-magazine.com/news/bhusa-russia-dark-web-revealed/>

³ <https://www.bbc.co.uk/news/technology-40671091>

⁴ <https://www.hackread.com/hell-is-back-with-hell-reloaded-on-the-dark-web/>

⁵ <https://www.darkowl.com/blog/2019/all-signs-point-to-a-law-enforcement-takedown-of-kickass-forum>

⁶ <https://www.zdnet.com/article/belarusian-police-shut-down-notorious-hacking-forum/>

⁷ <https://www.europol.europa.eu/newsroom/news/cybercriminal-darkode-forum-taken-down-through-global-action>

⁸ <https://www.wired.com/story/infraud-feds-takedown-cybercrime/>

⁹ Tor denotes The Onion Router: a group of cyber networks consisting of a series of virtual tunnels, rather than being directly connected, which can be used as a building block for software developers to create new communication tools with built-in privacy features. A Tor URL ends in ".onion" and can be only used on the Tor browser.

¹⁰ <https://www.hackread.com/hell-is-back-with-hell-reloaded-on-the-dark-web/>

¹¹ <https://roguemedia.co/2019/04/09/infamous-notorious-hacker-forum-known-as-darkode-comes-back-online-under-new-ownership/>

¹² Usually, when a user types a URL into an Internet browser, a computer will query a DNS server for the IP address that corresponds to that URL. The final part of the domain (.com, .de, .uk, .org) is known as a Top Level Domain (TLD) and is controlled by a central authority such as Internet Corporation for Assigned Names and Numbers (ICANN), Nominet or DENIC. Blockchain TLDs – including .bit, .bazar and .coin – are not owned by a single central authority. DNS lookup tables are shared over a peer-to-peer network and use a different technology from traditional DNS requests.

¹³ Bulletproof hosts are service providers whose selling point is allowing customers to conduct any kind of activity with protection against law enforcement

¹⁴ Runet refers to the Russian-speaking Internet

¹⁵ Andromeda, also known as Gamarue, is a malware family used to create a network of infected computers (a botnet). Andromeda's main goal was to distribute other types of malware. The FBI dismantled Andromeda—which has links to 80 malware families—in November 2017; <https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation>

¹⁶ <https://medium.com/@SwiftSafe/infamous-belarusian-hacker-ar3s-behind-massive-andromeda-botnet-released-bf7463cb0703>

¹⁷ <https://www.scanforsecurity.com/news/sergei-yarets-free-revelations-andromeda-botnet-operator-ar3s.html>

¹⁸ <https://news.softpedia.com/news/infamous-hacking-forum-hell-returns-online-raises-questions-of-trust-498482.shtml>

¹⁹ <https://patch.com/washington/seattle/roman-seleznev-sentenced-nearly-30-years-hacking-case>

²⁰ <https://www.theguardian.com/world/2018/apr/13/moscow-court-bans-telegram-messaging-app>

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threat. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight, visit
www.digitalshadows.com

London

Columbus Building, Level 6,
7 Westferry Circus,
London, E14 4HD

+44 (0) 203 393 7001

messages@digitalshadows.com

San Francisco

235 Pine St. Suite 1050,
San Francisco, CA 94104

+1 (888) 889 4143

Dallas

5307 E. Mockingbird Ln.
Suite 200
Dallas, TX 75206

digital shadows 