



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

Threat Actor Raising Funds For Proposed SS7 Service

New and untested threat actor “cybersec101x” is raising funds for a new service that would potentially provide threat actors with access to a Signaling System No. 7 (SS7) gateway, on the English language Dark Web marketplace “AlphaBay”. The advertised service would allow threat actors to control the SS7 signaling protocols used by most mobile network operators to establish wired/wireless phone calls, SMS messages, number translation, and prepaid billing services.

This access could enable different types of fraud, including:

- SIM-swapping
- Bypassing multi-factor authentication codes sent via SMS

Although the actor does not currently have access to an SS7 entry point, they are still accepting \$5,000 payments to invest in the service. According to the actor, this amount would reserve a one-year license and at least four phones per investor. The actor anticipates their service will launch sometime in the next year.

Based on the actor’s lack of credibility on the marketplace, ZeroFox assesses with moderate confidence that this is a scam intended to defraud would-be investors.

Live SS7 Network Access!! - Premier Service -
Crowdfunding for VIP Access!!



Purchase Listing

[Scroll down for product details, feedback & refund policy.](#)

Sold by **cybersec101x** (0)

Trust Level 1 Vendor Level 1

Sold 0 times since March, 18 2022

	Features		Features
Product Type	Digital	Origin Country	United States
Quantity Left	25	Ships to	Worldwide
Payment	Escrow	Category	Hacking

Shipping/Extra Options:

Default - 1 hour(s) - USD + 0.00 / order

Purchase Price: 5000.00 USD

25.83674895 XMR

Quantity pcs:

1

Proceed to Checkout

♥ Favourite (Alert when Restocked)

‘Breached’ Poised To Replace ‘RaidForums’

In mid-March 2022, well-regarded threat actor and administrator “Pompompurin” launched the fast-growing successor to the English language Deep Web forum “RaidForums”, dubbed “Breached” (AKA “BreachForums”). There have been several attempts to replace “RaidForums” since its closure in late February 2022. This includes “Darknetworld” and “Raidforums2”. However, none of these forums have caught on as quickly as “Breached”.

Although the actor claims this new forum is not affiliated with “RaidForums” in any way, the two share nearly all the same features. The actor is even offering to restore the accounts of old “RaidForums” users, with their reputation scores intact.

Additionally, the forum features a new ransomware section, where threat actors can share detailed leaks about victims or ransomware gangs. Cyberattacks targeting ransomware teams have become increasingly more prevalent on English language Deep and Dark Web forums since the Conti gang announced its support of the Russian invasion of Ukraine in late February 2022.

As a result, ZeroFox researchers note that most of the threat actors who have migrated to “Breached” so far appear to be English speakers with an anti-Russian/pro-Ukrainian stance. This differs somewhat from the more inclusive community associated with the original “RaidForums”.



Original post from
threat actor
“pompompurin”
welcoming users to the
new “Breached” forum

‘Breached’ Poised To Replace ‘RaidForums’ Cont.

Welcome
by pompompurin - Wednesday March 16, 2022 at 06:12 PM

March 16, 2022, 06:12 PM (This post was last modified: March 17, 2022, 08:21 PM by pompompurin.)

[Admin] **pompompurin**



Administrator

ADMINISTRATOR

Posts: 67
Threads: 8
Joined: Mar 2022
Reputation: 1,023



March 16, 2022, 06:12 PM (This post was last modified: March 17, 2022, 08:21 PM by pompompurin.)

Hello, welcome to Breached (Aka "BreachForums")!

I've created this forum as an alternative to RaidForums since it was seized. We are not affiliated with RaidForums in any capacity.

I've waited as long as I am comfortable waiting to see if RaidForums will make a return, but I sadly don't think it will. I've created this forum in part to stop all the stupid people are trying to take the empty spot that RaidForums once filled (for example, <https://darknetworld.com>, Hosted on NameCheap shared hosting 🙄🙄).

If RaidForums does ever return in any official capacity, this forum will be closed and this domain will redirect to it.

You can join the RaidForums Telegram to watch for updates: <https://t.me/+N0H3jueZt-4xYTBk>

This website is a work in progress, expect a lot of bugs // weird glitches. I am aware of 99% of the bugs and I just need a bit of time to work on them all.

Some features that will be finished by the end of the week on here:

- All official databases from RaidForums put on our own CDN.
- Fully working shoutbox.
- And much more.

I will also be offering people their ranks (VIP, MVP, GOD) back. If you had a rank on RaidForums and you paid via CoinPayments, send me a full copy of the email receipt (Looks like this: <https://z.zz.fo/Poi5Q.png>). I need the full email including the signed message details so I can confirm you indeed bought a rank. If you paid another way at this current point in time I cannot verify if you really had a rank on RaidForums or not, so I cannot offer you your rank back. Apologies. You can either contact me via Telegram or via PMs on here. Please do not contact if you don't have the CoinPayments email to confirm you had a rank.

Edit: If you paid via PayPal, feel free to also contact me (with proof).

Questions? Contact me on Telegram, <https://t.me/paste>

Thanks ❤️

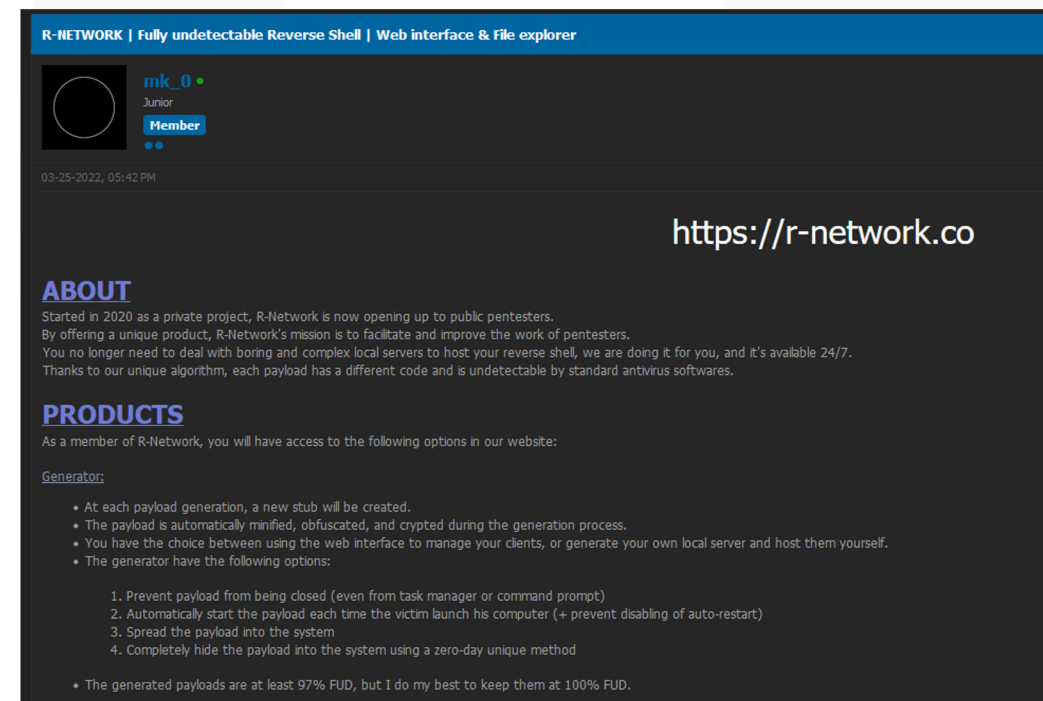
Service Automatically Generates Malicious Payloads To Compromise Targets

New and untested threat actor “mk_0” advertised a service, dubbed “R-Network”, that they claim can automatically generate malicious payloads to compromise target machines, on the English language Dark Web forum “CryptBB”. The actor claims that the randomly generated payloads allow threat actors to establish a reverse shell connection to their targets without being detected by most antivirus products. Once they have gained this initial access, the actor claims that operators can leverage a simple web interface to manage and remotely execute additional code on compromised machines.

According to the actor, the payloads can be customized to perform a variety of different functions, including:

- Deliver malware to a specific target machine
- Prevent the malicious process from being terminated
- Run malware at startup
- Hide malware in memory using an alleged zero-day exploit

The actor did not specify a price for the service.



New Leak Of Sensitive Data Targets Indian Government & Military

The well-regarded threat actor and known intelligence broker “spectre123” shared a link to download a new leak of sensitive data related to the Indian government and military, on the English language Deep Web forum breached[.]co. The actor cited India’s ongoing relationship with Russia and the humanitarian crises in both India and Ukraine as reasons for publishing more than 40 GB of classified data on their website, intelrepository[.]com.

According to the actor, the leaked data contains information from:

- The joint defense secretary
- Ministry of Defense
- Navy

The actor recently returned from a lengthy absence from the underground to disclose leaks related to the Venezuelan Navy, as well as a Russian contractor. The actor expressed anti-Russian/pro-Ukrainian sentiment as their motivation for the leaks, quelling previous rumors that “spectre123” was working with the Russian government.

Indian Government and Military 40 GB worth of defense documents leak

by spectre123 - Sunday March 27, 2022 at 08:31 PM



★ spectre123

V.I.P User

VIP

Posts: 1
Threads: 1
Joined: Mar 2022
Reputation: 0

11 hours ago

Hello everyone,
Today I have leaked 40 gigabytes of important defense data of one of Russia's major allies, India.

Link: <http://intelrepository.com/leaks.htm>

Enjoy.

Confidential/sensitive intel(Updated as of 3/28/2022)

On this section of the site you can find intel(most of which has been paid for by me) which has been leaked to the public for free. In addition to that new leaks will be added at the top of the page.

Indian government and military defence data mega leak

Files download links: https://mega.nz/file/Cy4n0Q4Q#hBqz5-vUyE_B2qyl9uqSYqsOTxtuQeUSGftlXN_TlqU
<https://mega.nz/file/Png0JbID#JFFBmIuWl9pdNaEdbkqm9-j6ntzUZQFq7KpgzYaAesQ>
https://mega.nz/file/BR8V0a1J#hKqLcvHfEbcMJP-jNtf4-5MjVloW_OWVvJvJfP-7IE
<https://mega.nz/file/W6ZCwBDQ#s05knXomwzGa5m7PBfdl3UcqBaBnWN637odklo8sAOU>
https://mega.nz/file/bvRDAKhI#lGA-LW_Vl0U5izTO_LEcvUFVn6hJdooblfqWfs5w1AA
<https://mega.nz/file/nz5gDB4R#OUxIJEZqtOBNEzOFXjt406Qp7Wg9xbfbmxhVqNjepuQ>
<https://mega.nz/file/VJITIS5J#TYlo4swaJfRmaBEusdr7nZSxnfJ5l6ySQlyv3lVmxM>
https://mega.nz/file/MpFDCAgQ#RRKVJWQR9Awb0ln_EtXy_tCaoecHF8y5bEpd8EAUqhQ
https://mega.nz/file/INODSYpJ#UpU_QnAJsPrAGTmrJhLdAQg5vjYVOVFepTUFM0dqt4
<https://mega.nz/file/YRMSDLSb#lCDcYvK4uxbs57Iva554yduDot57s53mrN24l7U8xS4>
https://mega.nz/file/c8ly0TbA#ayPFsr-QsWnx-_7UgCnAH4vkY2OikXGZTeRbWz5-znU

Details: The Indian government has a remarkably twisted propensity towards turning a blind eye to the humanitarian crisis in their own nation and now as well in Ukraine. It continues to do business with Russia and refuses to speak on the war, all in an effort to maintain their shallow political interests. These documents have been released to show that there are consequences for taking such foolish decisions. This 40 gigabytes worth of data, split into 11 parts, includes all kinds of top secret, secret and confidential documents from the following sectors, ALISDA, DGAQA, MSQAA, DRDO, DDP, Joint Defence Secretary India, BSF, MOD and the Indian Navy. They also contain data from multiple defence companies as well and information regarding defence tech, missile systems, employee details, border forces details, internal affairs of the MOD and a multitude of other things. (NOTE: The password for 9th file is: dirmsqaadgaqa.7z and for the 11th file it is: OjharNasikDGAQA.7z)