INTRINSEC

Innovative by design

Pakistani freelancers building cracking websites for stealer-delivery

Cyber Threat Intelligence

June 2025

@Intrinsec @Intrinsec Blog Website

2025 Intrinsec, Inc. All rights reserved.

Table of contents

1. Key findings

Detailed in this report:

- Information on WhoIs records of cracking websites used to deliver stealer, which have impacted some of our clients. Inside the records, various email addresses link to real identity of Pakistani freelancers specialised in web development and advertising. Reminiscent of how the Cryptbot malware operated, these individuals follow a pay-per-install model for financial gains.
- Nameservers of the domain filescrack[.]com, registered by the same Pakistani individuals, were used since 2021 for more than 300 cracking websites. Additionally, the hosting provider 24xservice, may be used by this network of freelancers to register domains of cracking websites. In fact, the range **185.216.143[.]0/24** hosted by **AS57717 (24xhosting)** is almost full of cracking websites.
- Strategic and geopolitical information on Pakistan's cyber ecosystem, which reveals closer ties with China in recent years, especially in terms of intelligence sharing and emergency response cooperation. Additionally, little can be done to prosecute Pakistani individuals behind these malicious activities as there is no extradition treaty between the US and Pakistan. Servers and domains can be seized but it is only a temporary measure until new ones are rebuilt, just like we observed with Cryptbot.

2. Introduction

Many of our client's employees fall prey to stealer compromises. Their credentials are then leaked or sold on dedicated marketplaces, cybercrime forums and communication channels such as Telegram. Leaked credentials can then be used as initial access to deliver other payloads into corporate networks, such as RATs for espionage purposes or ransomware for data leak. In most cases, these employees were compromised after downloading and executing cracked software. As already explored in previous analysis (see **Following the Sources of Infections Leading to the Deployment of CryptBot**[1]), websites offering cracked software are a commonly known vector of propagation of stealer malware. In this analysis however, we will explore the ecosystem linked to these websites, giving insight into how they are built and by whom. This information sheds light on another aspect of the stealer kill-chain, that starts before the deployment of the malicious payloads and further expands on the segmentation of cybercrime activities. We voluntarily did not analyse the technical kill-chain after a victim downloads a malicious cracking software, as we already previously covered it in various analysis (Cryptbot, Lumma, …)

We discovered a **network of Pakistani freelancers** that build websites related to cracking, potentially for third-party clients, and can also use SEO and Google Ads to promote and reference these websites. As exposed by Google and in our **Cryptbot analysis**[2], Pakistani cybercriminals can be directly involved in cracking website to deliver stealer malware. We could suspect that, mostly in the beginning of their activity, Pakistani freelancers may not be cautious or regardant on the types of projects offered to them. As such, they could accept such opportunities to build their reputation and earn money. Once enough time has passed and they've built their portfolio, they could start institutionalising themselves, just like one freelancer we discovered, who created his own website-building company and is not directly linked to cracking websites since 2021.

[1] https://www.intrinsec.com/cryptbot-hunting-for-initial-access-vector/
[2] https://www.intrinsec.com/wp-content/uploads/2024/12/TLP-CLEAR-CryptBot-Hunting-for-intial-access-vectors.pdf

3. Cracking websites infrastructure

3.1 Suspicious email in WhoIs

Starting from a stealer compromise of one of our clients, we identified that the source of infection was from a website delivering cracked software: "**kmspico[.]io**". This is a well-known vector of stealer-infection, that we identified in various analysis. Pivoting on this domain, we noticed that the hash of the OpenSSH banner exposed on port 22 of the domain's IP address **45.12.1[.]24** (**Virtual Systems LLC**) is also shared by IP address **45.12.1[.]30**, on the same range.

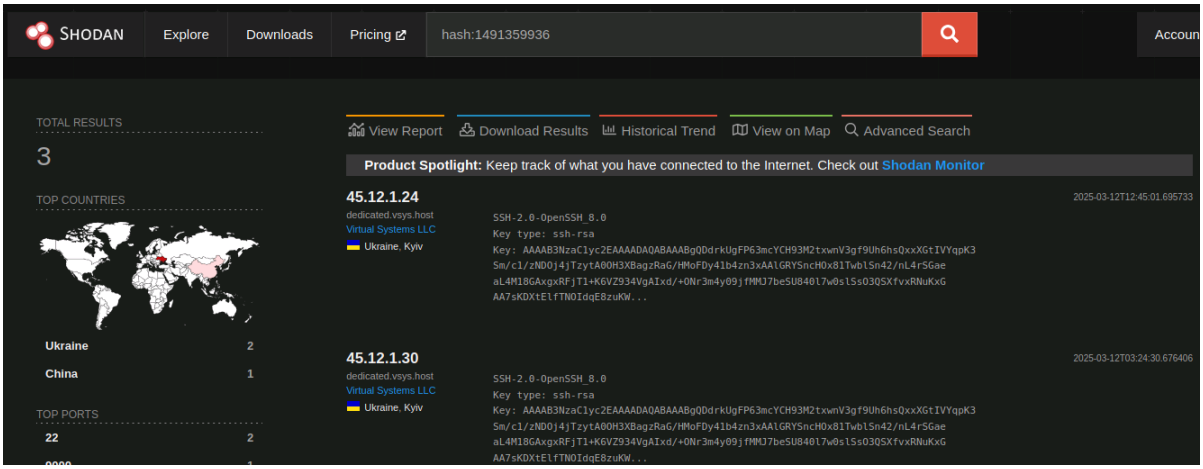

Figure 1: IP addresses exposing the same OpenSSH banner on port 22. Source: https://www.shodan.io/search?query=hash%3A1491359936.

The latter IP address is associated with **multiple domains** that distribute **cracked software**, based on their names and reputation.

URLs (42)

Scanned	Detections	Status	URL
2025-03-09	10 / 96	200	http://vstmania.net/
2025-03-06	6 / 96	200	http://webmail.vstmania.net/
2025-03-05	1 / 96	200	https://45.12.1.30/
2025-02-24	8 / 96	200	http://vstpatch.net/
2025-02-16	3 / 96	200	http://wordoria.online/
2025-03-06	7 / 96	200	https://vstmania.net/
2025-01-09	7 / 96	200	https://vstpatch.net/luminar-crack/
2025-01-08	8 / 96	200	https://vstpatch.net/
2025-01-08	6 / 96	200	https://vstpatch.net/kshmr-essentials/
2025-01-08	8 / 96	200	http://vstpatch.net/fl-studio-crack-2

Figure 2: URLs associated with the IP address 45.12.1[.]30. Source: https://www.virustotal.com/gui/ip-address/45.12.1.30/relations

Searching one of these websites' information, we noticed that it was associated with a nominal email address and with nameservers of **filescrack[.]com**.

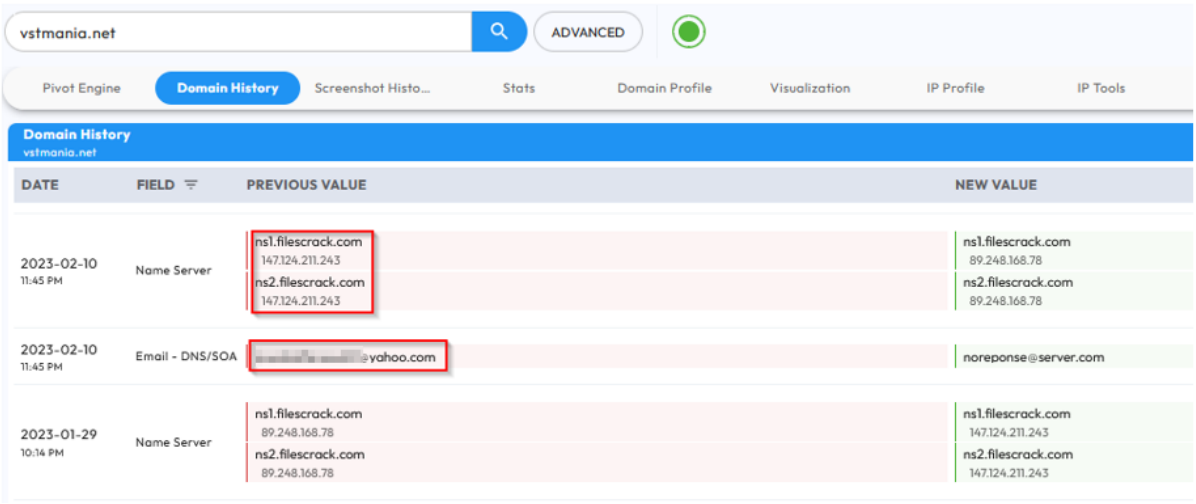

Figure 3: Domain history of vstmania[.]net.

This email address is linked to multiple cracking websites since 2021.

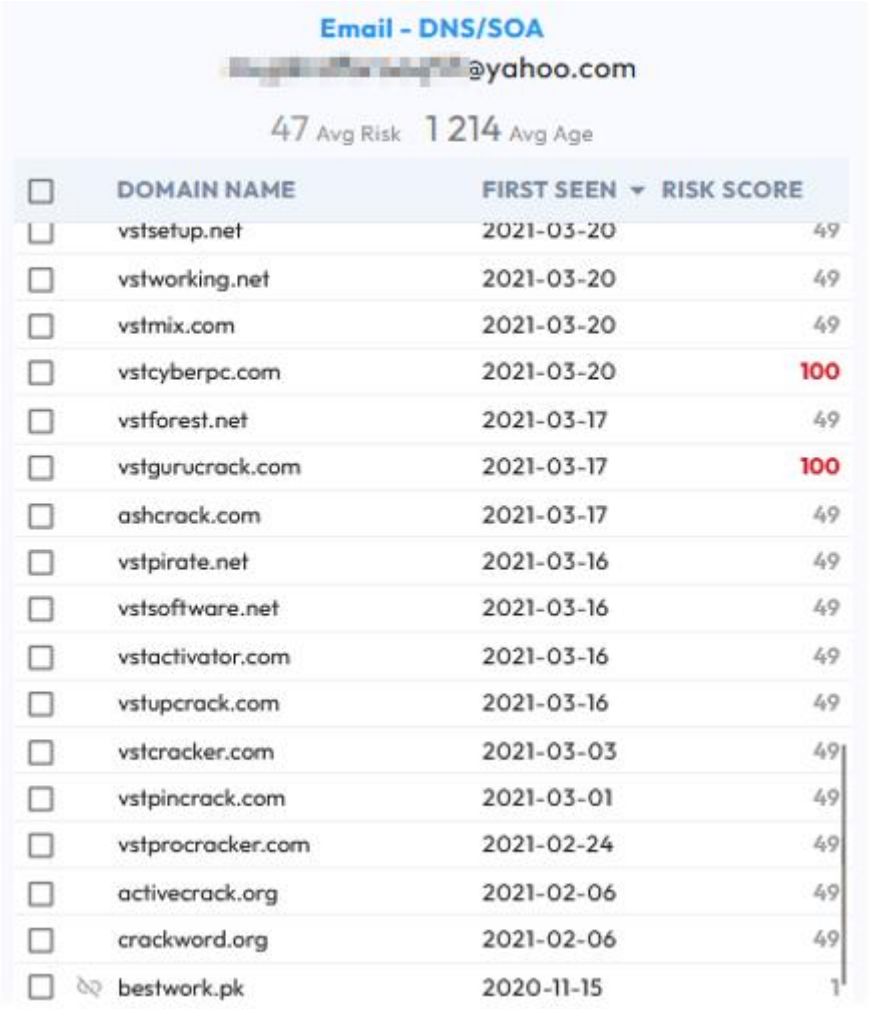

Figure 4: Cracking websites associated with the nominative email address.

3.2 Filescrack nameserver

Among these cracking websites, the domain **filescrack[.]com** is particularly interesting. It is again associated with the same email address.

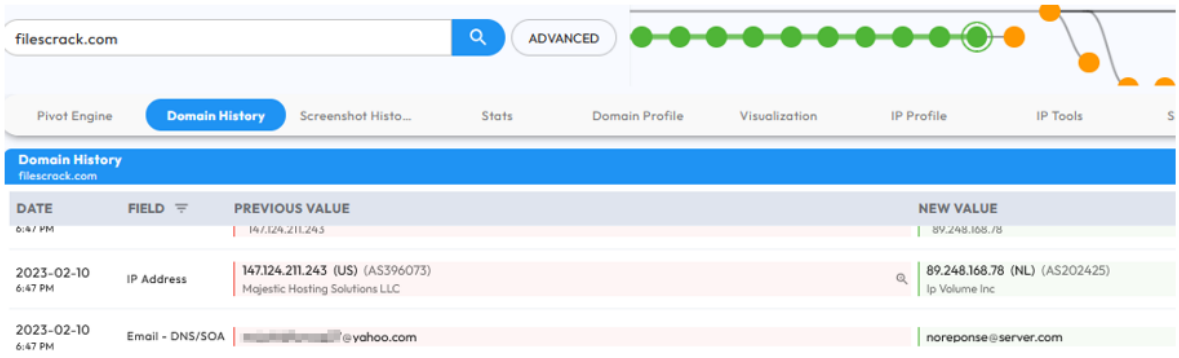

Figure 5: The mail address is associated with filescrack[.]com.

Of interest is the fact that filescrack is used as nameservers. For instance, ns1.filescrack[.]com was linked to **over 300 cracking websites** as of September 2024, and more than 200 as of March 2025.

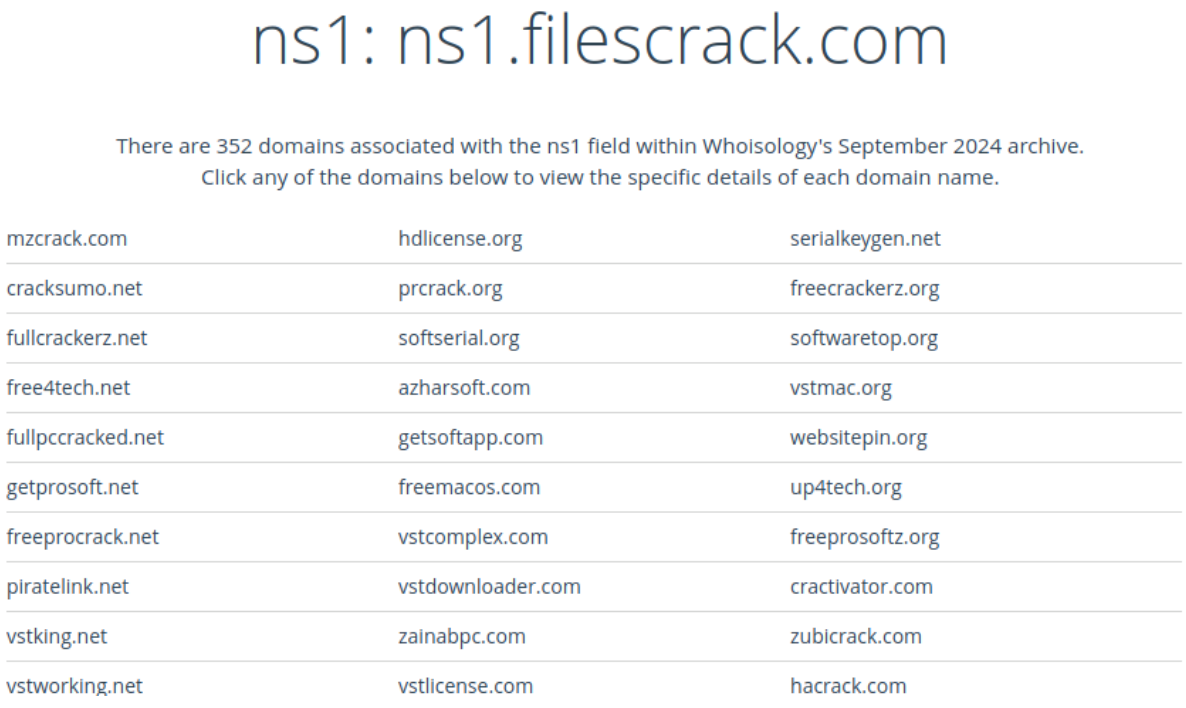

Figure 6: Cracking websites associated with filescrack nameserver. Source: https://whoisology.com/ns1/archive_47/ns1.filescrack.com/1

We see that multiple domains started to be associated with this nameserver since June 2021, which corresponds to the first mentions of the email address in WhoIs of cracking websites.

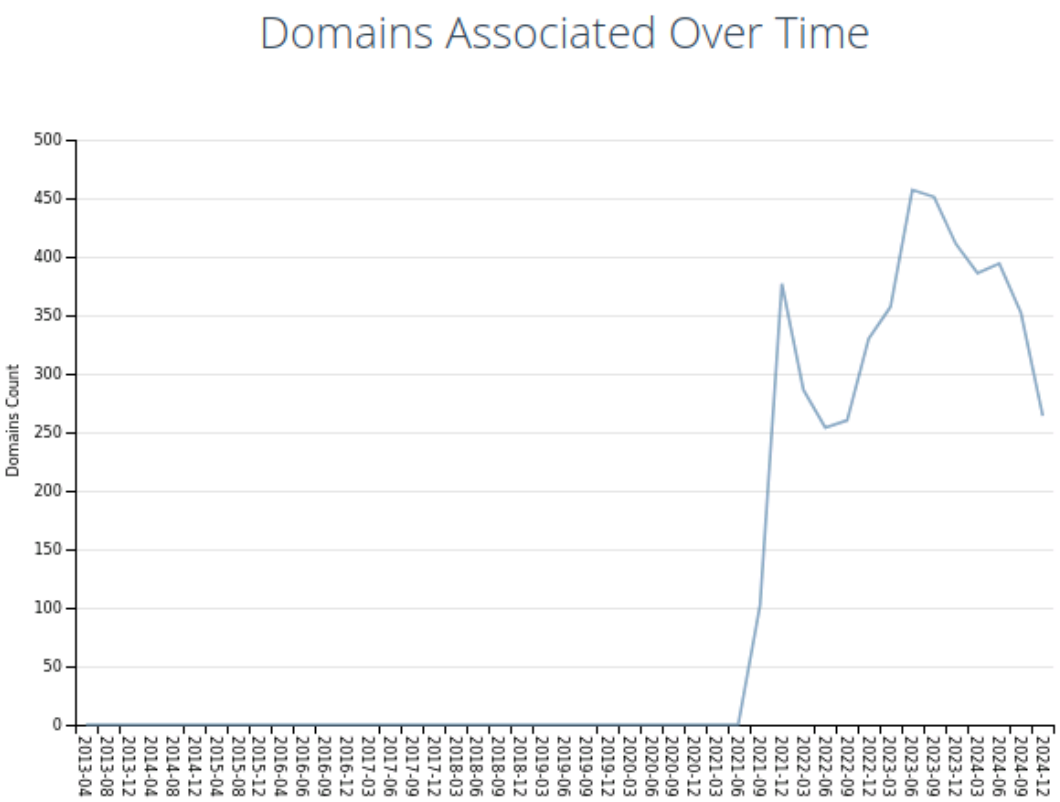

Figure 7: Evolution of domains count on ns1.filescrack[.]com. Source: https://whoisology.com/ns1/archive_47/ns1.filescrack.com/1

On one domain associated with filescrack's nameserver, we noticed that it switched to a nameserver associated with **crackjin[.]net**.

DNS NS records (18)

Domain	TTL	Last seen
eric.ns.cloudflare.com	21599	2020-12-17 19:14:39 UTC
intel1.socialflag.net	21599	2020-08-29 11:04:30 UTC
intel2.socialflag.net	21599	2020-08-29 11:04:30 UTC
liv.ns.cloudflare.com	21600	2023-09-11 10:23:57 UTC
love.ns.cloudflare.com	21599	2020-12-17 19:14:39 UTC
ns1.bluehost.com	21599	2020-06-09 08:22:09 UTC
ns1.crackjin.net	21600	2024-09-01 13:40:52 UTC
ns1.filescrack.com	86400	2021-07-24 07:50:24 UTC
ns11.filescrack.com	21600	2021-10-07 09:10:57 UTC
ns12.filescrack.com	21600	2021-10-07 09:10:57 UTC

Figure 8: The domain vstmania switched from filescrack to crackjin nameserver. Source: https://www.virustotal.com/gui/domain/vstmania.net/relations

As again, this domain is linked to the previously discovered email address. Interestingly, we can note that the email inside the WhoIs record was changed on 1st March 2023 to another nominative email address.

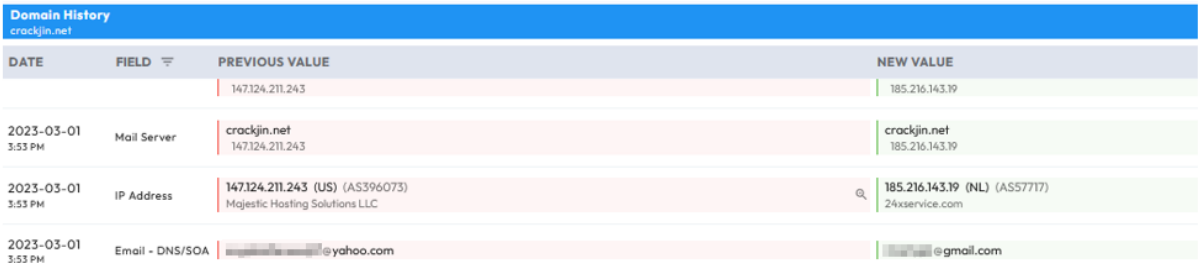

Figure 9: Inside crackjin[.]net WhoIs record, the mail address switched from one identifiable mail address to another.

This email address is also associated with multiple cracking websites.

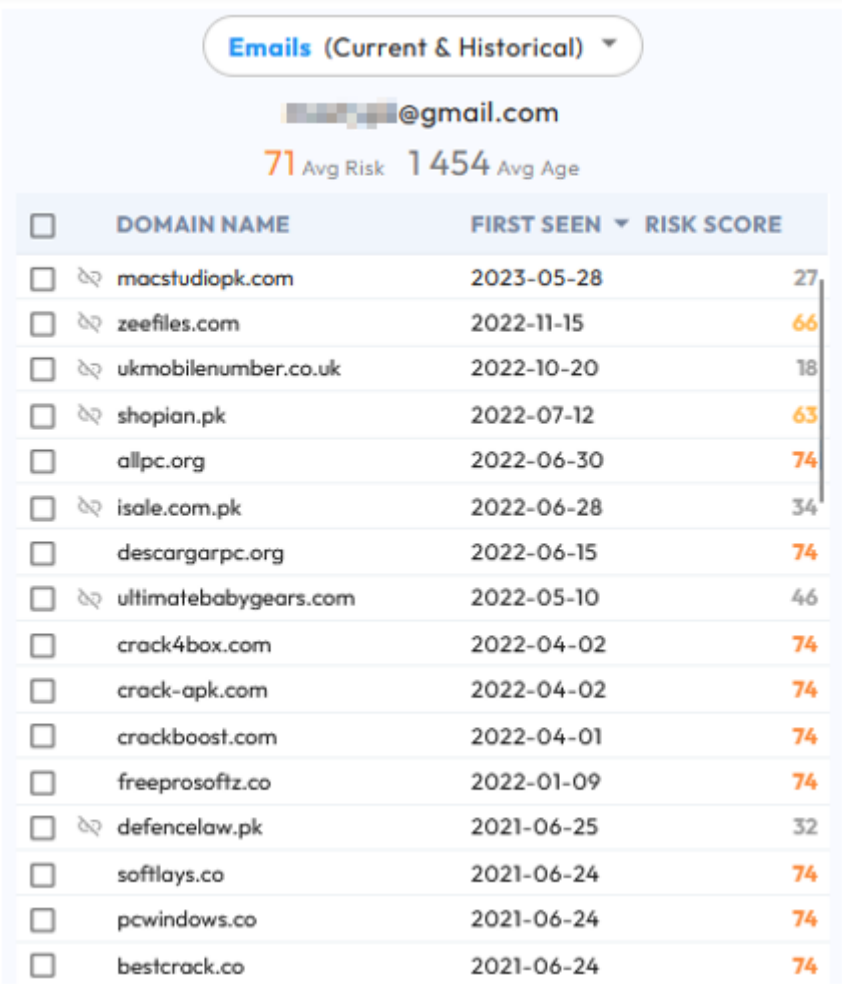

Figure 10: The email address is associated with several cracking websites.

3.3. 24xservice hosting provider

We noticed that many of these cracking websites were linked to the hosting provider **24xservice[.]com**. The website of this hosting provider is also associated with the second email addresses and a third new nominative email address.

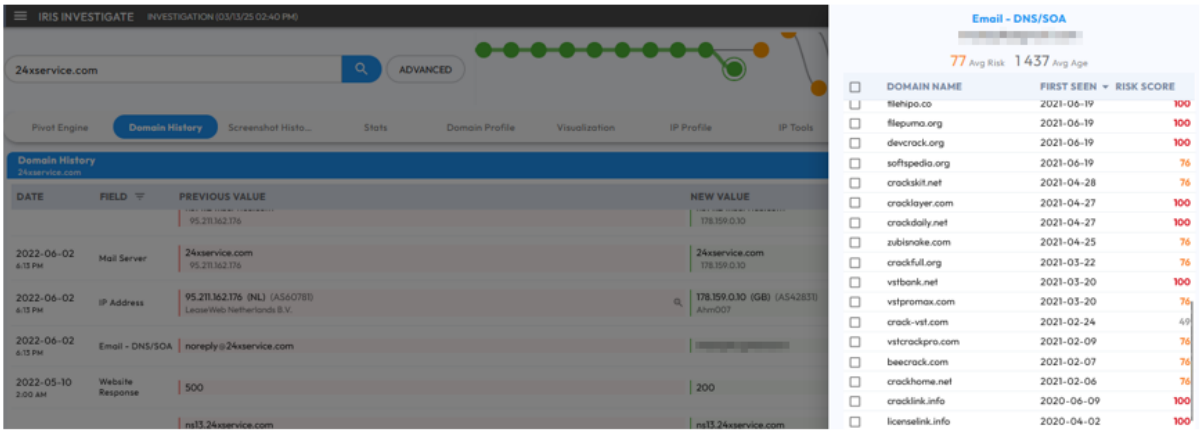

Figure 11: The email address is associated with 24xservice.

24xservice possess the autonomous system **AS57717**, which is peered with Fiberxpress and is located in Lahore, Pakistan. Even though these information can be falsified or usurped, this is another chain linking this infrastructure to Pakistan.

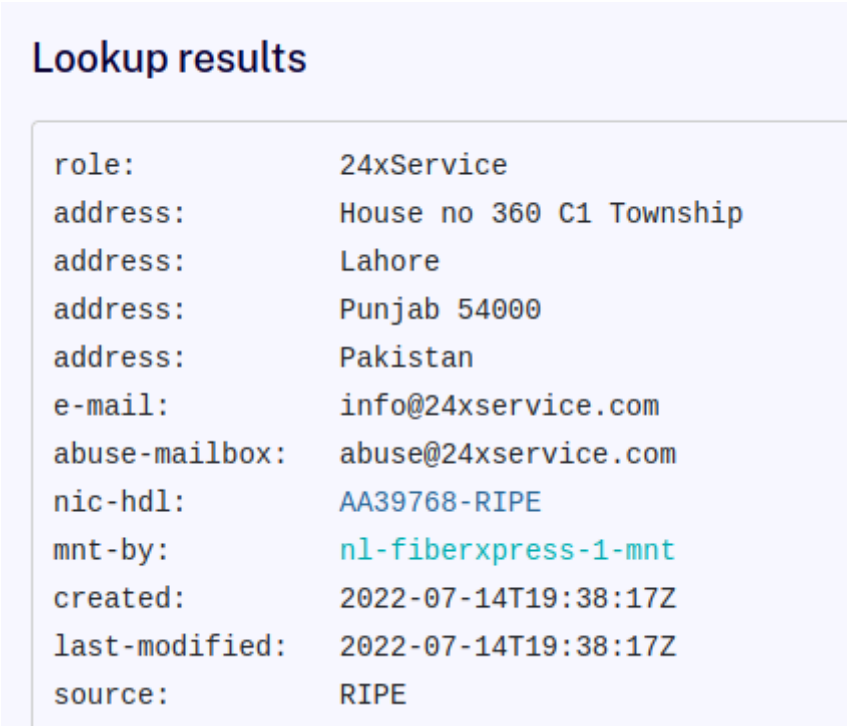

Figure 12: https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=AA39768-RIPE&type=role

Using URLscan, we can notice that websites on the range **185.216.143[.]0/24** hosted by **AS57717** on **24xhosting**, are mostly cracking websites.

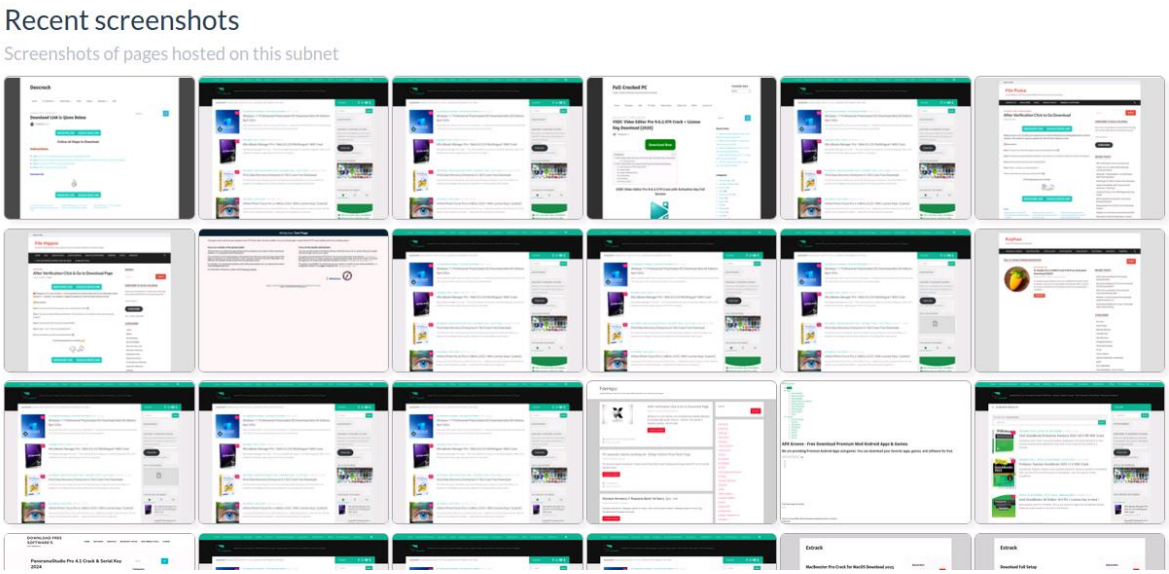

Figure 13: Cracking websites landing page exposed by the range 185.216.143[.0/24. Source: https://urlscan.io/ip/185.216.143.0/24

In fact, checking all the domains hosted on this range, we noticed that it is almost exclusively used for cracking websites, albeit two domains. The complete list of all domains is available in the Indicators of compromise section of this analysis. As we did not identify specific elements pointing that this hosting provider is bulletproof, and as it does not make advertising on cybercrime forums, we suspect that 24xservice belongs to and is used by the Pakistani network we analysed in this report, to host their client's or their own domains which includes cracking websites.

					Rating	
1	sadeempc.com	185.216.143.63	24Xservice.com	Netherlands	# 55,161	
2	vlsoft.net	185.216.143.48	24Xservice.com	Netherlands	# 148,865	
3	pcproductkey.net	185.216.143.29	24Xservice.com	Netherlands	# 297,360	
4	vsthomes.com	185.216.143.19	24Xservice.com	Netherlands	# 407,424	
5	crackedpc.net	185.216.143.48	24Xservice.com	Netherlands	# 410,771	
6	pcserialkey.com	185.216.143.29	24Xservice.com	Netherlands	# 411,701	
7	apxsoftwares.com	185.216.143.48	24Xservice.com	Netherlands	# 474,257	
8	fullcrackedpc.com	185.216.143.82	24Xservice.com	Netherlands	# 476,025	
9	xproductkey.com	185.216.143.48	24Xservice.com	Netherlands	# 480,282	
10	cracxfree.com	185.216.143.121	24Xservice.com	Netherlands	# 544,690	
11	keygenned.com	185.216.143.48	24Xservice.com	Netherlands	# 590,421	

Figure 14: Cracking websites hosted by the range 185.216.143[.]0/24 of 24xservice. Source: https://myip.ms/browse/sites/1/ownerID/1392205/ownerIDii/1392205

4. Network of Pakistani freelancers

4.1 Freelancer web development activity

The email address previously found in multiple WhoIs records of cracking websites, is associated with a real identity as exposed by Epieos.

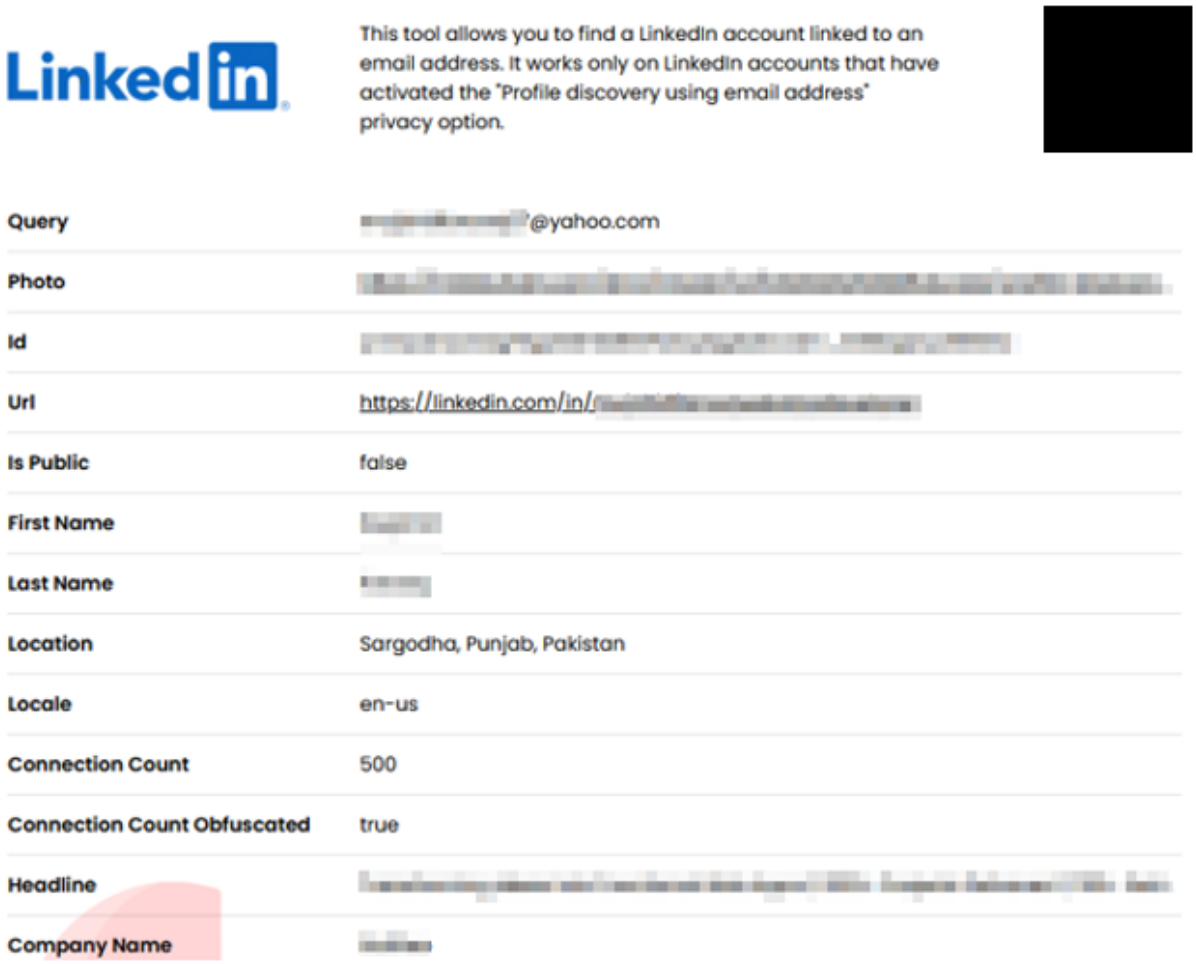

Figure 15: LinkedIn profile associated with the nominative email address.

Additionally, a website named FLCS (Freelancers Community Sargodha) lists IT freelancers in Sargodha, Punjab, Pakistan. On the list, we found the individual whose email was in the WhoIs records previously analysed. We suspect that this individual started his website building activities as a freelance and built those cracking websites, to later turn away from it (around 2023) and operate a "cleaner" online presence and activity.

Figure 16: Freelancers listed on the website "Freelancers Community Sargodha". Source: https://flcs.pk/

4.2 Compromised freelancer

Searching for mentions of 24xservice, we found a log of a potential other Pakistani freelancer, indicating he may have used the service. Inside the log, a screenshot made by the stealer shows the freelancer's Skype interface. Using this, we can see that he was a member of a Skype chat named **InstallPP[.]com**, which appears to be a **Pay-per-Install network**. It is mentioned in this tweet[3] as related to **FIN7 and other actors** emulating its modus operandi. The pay-per-install model is also reminiscent of how the **Cryptbot** network operated, as exposed in our analysis and in Google's complaints[4]. Below is a discussion inside a chat named "network ad", where they shared urls of cracking websites and appear to discuss it.

[3] https://x.com/Syndikalist/status/1841889332577378411
[4] https://www.intrinsec.com/cryptbot-hunting-for-initial-access-vector/

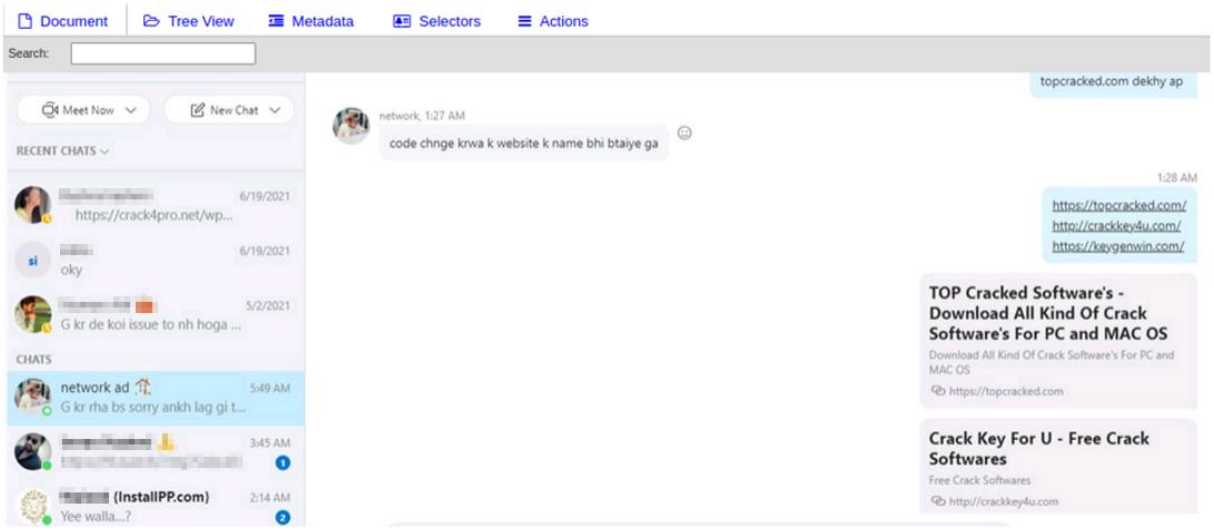

Figure 17: Screenshot collected by a stealer affecting a freelancer, showing his Skype conversation. Source: https://intelx.io/?did=227a9b93-29d2-4a52-a69c-cc4841763d4d

The message in the discussion can be translated from Hindi, as shown below.

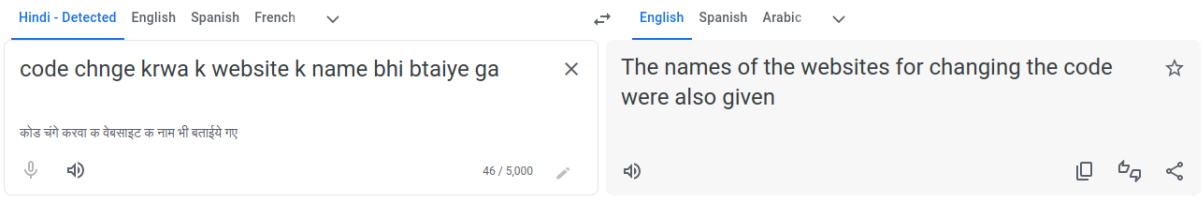

Figure 18: Translation in Hindi of the message visible in the previously mentioned screenshot.

However, in Urdu, the national language of Pakistan (both Urdu and Hindi are standard registers or varieties of Hindustani, with Hindi written in Sanskrit and Urdu in Persian/Arab), the message translates into the following. In both translations, we have the notion that something in the websites need to be changed. It could mean that someone asked them to change the code of the cracking websites evoked in the discussion, or that they themselves noticed something to change.

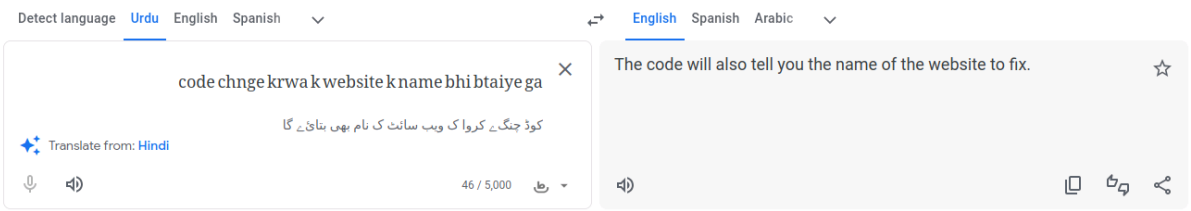

Figure 19: Translation in Urdu of the message visible in the previously mentioned screenshot.

The websites seen in the screenshot (topcracked[.]com, crackkey4u[.]com, keygenwin[.]com, crack4pro[.]net) do not appear to be associated with infrastructures of the previous email addresses. However, these websites used IP addresses from the autonomous system "**Virtual Systems LLC**". Additionally, the IP address **195.66.210.98** was

also associated with **crackjin[.]net in August 2024**, a domain which is linked to the two individual we previously saw on the WhoIs records.

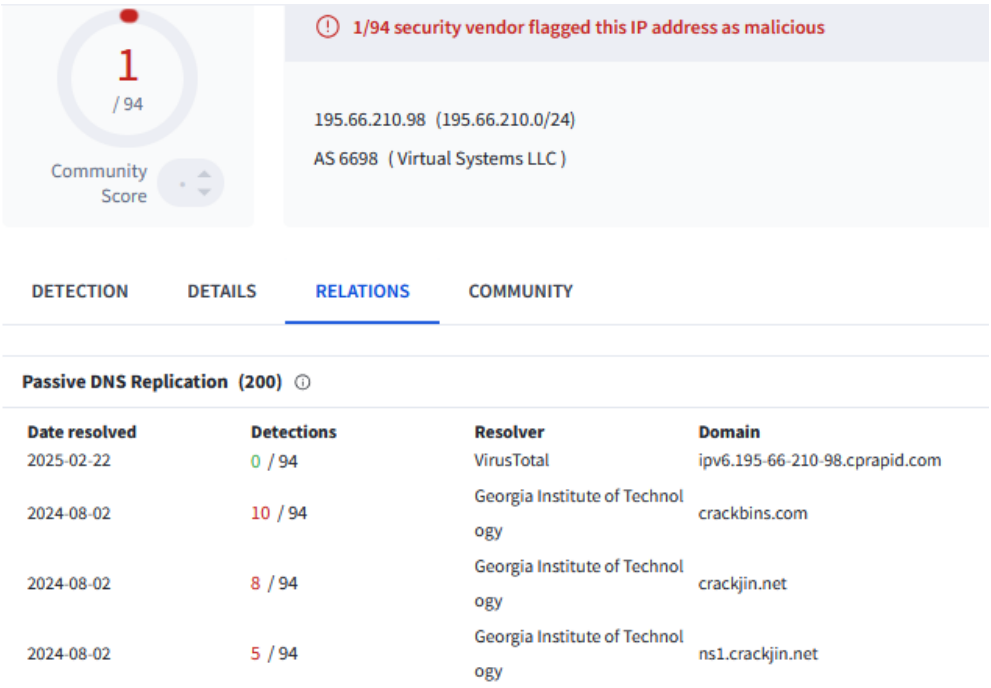

Figure 20: IP address also used by the domain crackjin. Source: https://www.virustotal.com/gui/ip-address/195.66.210.98/relations

4.3 Installpp, pay-per-install service

The website installpp[.]com is now offline, but it appears to have been used as a pay-per-install service. The fact that one potential developer or advertiser of cracking websites was a member of the installpp channel indicates that he could have activated this service on his clients' cracking websites. As exposed below, once a client downloads a "product" from the targeted website and installs it, the member of installpp gets a commission based on the operating system and country of the victim. This type of service can be used for non-malicious installers, but in this case, we suspect that it was employed in the context of cracking websites delivering stealer malware.

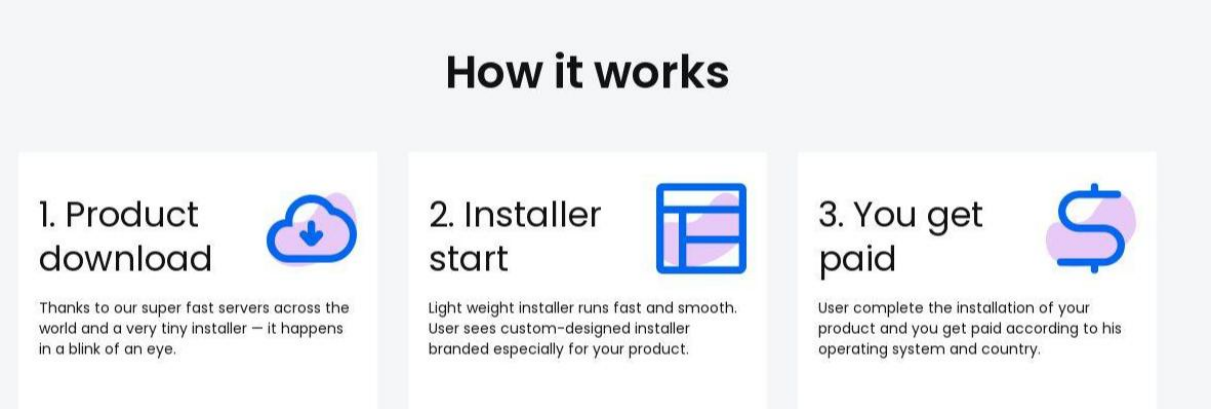

Figure 21: Explanation of the pay-per-install service as exposed on installpp[.]com, using DomainTools' screenshot history.

4.4 Traffic and installs

These types of services are well-known in the cybercrime ecosystem and are referred as "**traffic, installs, seo, spread**". We found many posts on this subject on the cybercrime Exploit and XSS, as well as messaging services like Telegram.

For instance, this post from 30 December 2024, on the Telegram channel "**Traffic – Logs - Malwares - SEO",** references a **website building service to generate automated malware downloads with SEO**.

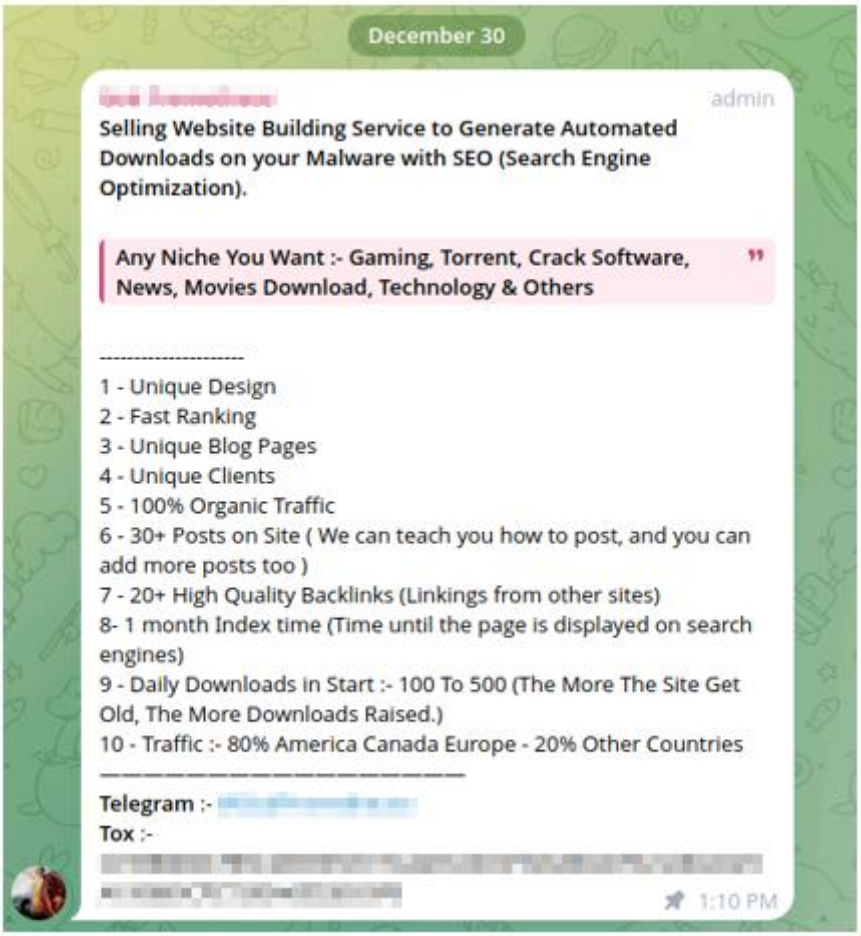

Figure 22: Message advertising website building services for malware delivery. Source: https://t.me/FreshTrafficandLogs/3986

On the Exploit post below from 27 December 2024, a user is selling a website on the theme "PC Crack Software Free Download" with more than 10k visitors per months.

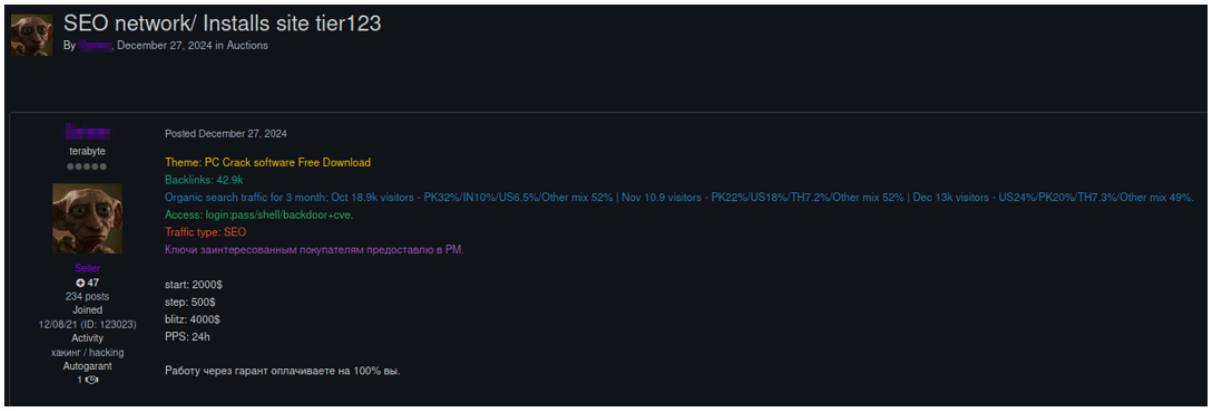

Figure 23: User selling a cracking website for malware delivery.

On this post from 25 January 2025, a user is looking for APK or EXE files to upload on his website for malware delivery. He references Lumma and Rhadamanthys as he can distribute them "easily".

Figure 24: User looking for malicious files to upload on his website.

5. Cybercrime in Pakistan

5.1 Google's complaint against the Cryptbot criminal enterprise

One website found in Google's complaint[5] against the operators of the Cryptbot pay-per-install criminal enterprise was also found in our analysis. However, almost all cracking websites we discovered in this analysis are not linked to the Cryptbot infrastructure we discovered[6]. As such, we can suspect that the infrastructure and criminal enterprise we analysed in this report was not publicly reported on and is different than Cryptbot.

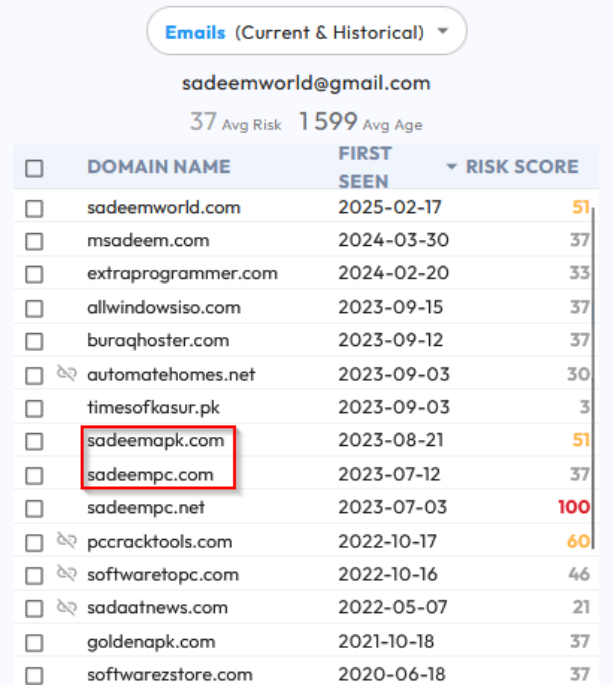

Figure 25:

[5] https://regmedia.co.uk/2023/04/28/handout_google_cryptbot_complaint.pdf

[6] https://www.intrinsec.com/wp-content/uploads/2024/12/TLP-CLEAR-CryptBot-Hunting-for-intial-access-vectors.pdf

5.2 Cybersecurity in Pakistan and cooperation with China

It is also known to host multiple companies, including ones related to **cybercrime activities**, as exposed in this article by KrebsOnSecurity[7] and DomainTools[8] on the phishing cybercrime group "Manipulaters". The American authorities seized websites of the group in the beginning of 2025[9]. However, in the cases of Cryptbot and Manipulaters, only websites have been seized, as there is **no extradition treaty between Pakistan and the United States**. Therefore, the cybercriminals could not be brought to justice.

Pakistan inherited an extradition treaty with the US when it proclaimed its independence from Britain in 1947, as the US and UK signed a treaty in 1932, but in 2020, when questioning the extradition of a Pakistani-American who allegedly planned a bomb attack in New York[10], the Supreme Court of Pakistan questioned the value of a pre-independence agreement and therefore **proclaimed there is no actual extradition treaty with the US**[11].

There is also a possibility that the Pakistani government could be lenient on these types of activities if it does not attack its interests.

In recent years, **Pakistan got closer to China**, both countries joining arms in their rivalry with India. As such, it distanced itself from America. With close cooperations in IT[12] and cybersecurity, such as in **internet connectivity**[13], **intelligence sharing** and **emergency response**[14], traffic coming from Pakistan should be treated carefully.

---

[7] https://krebsonsecurity.com/2025/01/fbi-dutch-police-disrupt-manipulaters-phishing-gang/
[8] https://www.domaintools.com/resources/blog/the-resurgence-of-the-manipulaters-team-breaking-heartsenders/

[9] https://www.justice.gov/usao-sdtx/pr/cybercrime-websites-selling-hacking-tools-transnational-organized-crime-groups-seized

[10] https://tribune.com.pk/story/2267545/pakistan-has-no-actual-extradition-treaty-with-us
[11] https://www.thenews.com.pk/tns/detail/1108003-the-extradition-law
[12] https://www.pta.gov.pk/category/pta-and-huawei-pakistan-sign-mou-to-strengthen-collaboration-in-it-and-telecom-sector-1577608552-2025-01-01
[13] https://www.pakistantoday.com.pk/2024/01/30/pakistan-signs-agreement-with-china-to-become-regional-internet-connectivity-hub/

[14] https://csopakistan.com/pakistan-and-china-strengthen-cybersecurity-cooperation-through-new-mou/

5.3 Cooperation with Russia

As seen earlier in the analysis, one domain (installpp[.]com) was mentioned as related to FIN7-esque landing pages. FIN7 is a Russian intrusion set that was linked to multiple incidents and operations since 2013. Multiple high-ranking members of the operation were sentenced by the United States, but it did not permanently disrupt their operations. Since 2020, FIN7 shifted to a big game hunting approach by using the Revil and Darkside ransomware. A report from Silent Push in 2024, also highlights how FIN7 used thousands of domains for phishing, shell domains as front, and landing pages hosting malware[15].

Overall, Pakistan and Russia also got closer geopolitically in recent years, which translates into cyberspace. In 2024, Russia supported Pakistan's bid to join the BRICS[16], as the country avoided condemning Russia's invasion of Ukraine and the two countries announced cooperation in various domains: defense, cybersecurity, counterterrorism[17]. However, this cooperation is not without frictions. In December 2024, Microsoft reported that the Russian intrusion set Turla, which is linked to the FSB,[18] has infiltrated the infrastructure of the Pakistan-based threat activity cluster SideCopy (Storm-0156) to install backdoors and collect intelligence on targets of interest in South Asia.

[15] https://www.silentpush.com/blog/fin7/#FIN7-shell-domains-morphing-into-phishing-websites
[16] https://apnews.com/article/pakistan-russia-brics-islamabad-bid-2f996195fc650b31243e9d7d91779259
[17] https://thediplomat.com/2024/09/pakistan-and-russias-pivot-to-the-global-south/
[18] https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

6. Conclusion

Based on an analysis from a client's stealer compromise, we shed light into the criminal network and infrastructure leveraged by Pakistani individuals and their clients, to **infect victims worldwide and profit financially**. With this analysis, readers will now have a better understanding of the type of threat actors behind these kill-chains. However, as seen with Google's complaint and in our Cryptbot analysis, **not much can be done to prosecute these individuals**, as Pakistan does not have extradition treaty with the United States and the European Union. Servers can be seized and malware infrastructure dismantled, but this is only a **temporary measure until new ones are rebuilt**. Link with China and Russia also shows that Pakistan is a growing IT country, as can be seen from the **rise of cyber threats**. As such, we can suspect that **Pakistani cybercriminals could target the West more**, either with direct help from the government through funding or involvement in operations, or by being lenient on these types of activities.

7. Actionable content

7.1. Indicators of compromise

Value	Type	Description
Sadeempc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Pcserialkey.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracxfree.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vlsoft.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Pcproductkey.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vsthomes.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedpc.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Apxsoftwares.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fullcrackedpc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Xproductkey.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Keygenned.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Downloadcracker.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Ratondownload.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackbay.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filehorsed.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activatedcrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Goldenapk.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Pcmage.co	Domain-name	Cracking website (hosted by 24xservice[.]com)

Azcrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Hmcrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Axcrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
A2zpc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activatorkey.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Licenselink.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vst4plugins.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Samipc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Azcracked.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Citycrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Licensedkey.co	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracksvst.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filehippos.co	Domain-name	Cracking website (hosted by 24xservice[.]com)
Docrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crack4pro.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackhome.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Spsoftwares.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softwarezstore.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Prosoftz.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Devcrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedactivator.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedexe.com	Domain-name	Cracking website (hosted by 24xservice[.]com)

Piratesfile.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracklicense.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackzip.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Allcracksoft.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Suripc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fullcrackedpc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Installlink.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracked4pc.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Pcmaccrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracklink.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Igetintopc.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crsoftz.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackwin7.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Encrack.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
94fbr.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Click4pc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Procrackedpc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Keykeygen.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Pcsoftz.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filepuma.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softncrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freekeygen.net	Domain-name	Cracking website (hosted by 24xservice[.]com)

Prosvst.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freeactivationkeys.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filecrk.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Up2pc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softspedia.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softwarezpro.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crack4box.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Zainabpc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackme.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freeprosoft.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackdownloader.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Corecrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Allpcsoftwares.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activatorhax.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Mahcrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Serialkeygenpro.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Allpcsoft.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Artcrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softwarecrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Sehrpc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Ahcracks.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Procrack.co	Domain-name	Cracking website (hosted by 24xservice[.]com)

Crackedsofts.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedloader.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filehipo.co	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackproz.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedpro.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Turkycrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackmax.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Hdlicense.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Kmspicoproductkey.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackclue.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Gocrack.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Momopc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Portablecrack.co	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstfine.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Beecrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activatorspatch.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Plugtorrent.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Parrotpc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Ecrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstmac.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Descargarpc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softwaregurucrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)

Wincrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Mzcrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackactivation.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracksumo.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freeprosoftz.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fullcrackerz.co	Domain-name	Cracking website (hosted by 24xservice[.]com)
Provst.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fullkeys.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cractivator.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackpaper.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freeserialkey.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackpatch.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracked4soft.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedios.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Hamapc.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Kalicrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crack4tech.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fullfreecracked.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filespcdownload.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Getprocrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracked4free.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freeproductkey.net	Domain-name	Cracking website (hosted by 24xservice[.]com)

Crackedrules.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Startcrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstcomplex.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstdownloader.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freesoftpc.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackserialkey.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstmacdownload.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Free4pc.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activatorproductkey.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Lulucrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Realproductkeys.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Malacrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackmust.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activationcrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
9to5mac.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Freesoftpc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackbank.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Wazusoft.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Proactivator.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Downloadscrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Extrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracx.net	Domain-name	Cracking website (hosted by 24xservice[.]com)

Cocrack.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracknew.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Systemcrack.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstbank.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Allpc.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cracklayer.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstpromax.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackshome.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activationkeyspro.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fullversionsoft.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackskit.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Serialfull.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstlove.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Softwaresdaily.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Gurucrack.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crack2dl.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Activationskey.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Fbr94.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filehorse.info	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackfullpatch.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Vstlicense.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackxworld.com	Domain-name	Cracking website (hosted by 24xservice[.]com)

Pcfile.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackedfine.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Downloadspatch.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Licenselee.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackkeys4u.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Profreecracks.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Kuyhaa.co	Domain-name	Cracking website (hosted by 24xservice[.]com)
Iactivationkeys.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Patchkey.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Pcvstcrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Chathacrack.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Cloudcracked.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Idmcrackeys.org	Domain-name	Cracking website (hosted by 24xservice[.]com)
Tech-softwares.com	Domain-name	Cracking website (hosted by 24xservice[.]com)
Crackdaily.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Getintopcfree.net	Domain-name	Cracking website (hosted by 24xservice[.]com)
Filescrack.com	Domain-name	Cracking website and nameserver
Crackjin.net	Domain-name	Cracking website and nameserver
plugvst.com	Domain-name	Associated with ns1.filescrack.com
crackword.org	Domain-name	Associated with ns1.filescrack.com
crackfix.org	Domain-name	Associated with ns1.filescrack.com
zamilcrack.com	Domain-name	Associated with ns1.filescrack.com

jincrack.com	Domain-name	Associated with ns1.filescrack.com
freemacos.com	Domain-name	Associated with ns1.filescrack.com
procrackerez.com	Domain-name	Associated with ns1.filescrack.com
lulupc.net	Domain-name	Associated with ns1.filescrack.com
ayeshapc.net	Domain-name	Associated with ns1.filescrack.com
crackedx.net	Domain-name	Associated with ns1.filescrack.com
crackkeygen.net	Domain-name	Associated with ns1.filescrack.com
ganjiswag.net	Domain-name	Associated with ns1.filescrack.com
fullversionpro.net	Domain-name	Associated with ns1.filescrack.com
hacrack.com	Domain-name	Associated with ns1.filescrack.com
installlink.net	Domain-name	Associated with ns1.filescrack.com
securecrack.net	Domain-name	Associated with ns1.filescrack.com
softnkey.net	Domain-name	Associated with ns1.filescrack.com
pcproductkeys.org	Domain-name	Associated with ns1.filescrack.com
soft4mac.org	Domain-name	Associated with ns1.filescrack.com
vstmac.org	Domain-name	Associated with ns1.filescrack.com
vstlicensekey.com	Domain-name	Associated with ns1.filescrack.com
extrack.net	Domain-name	Associated with ns1.filescrack.com
pcsoftnew.net	Domain-name	Associated with ns1.filescrack.com
procrackerz.net	Domain-name	Associated with ns1.filescrack.com
vstmac.net	Domain-name	Associated with ns1.filescrack.com
fullgetpc.com	Domain-name	Associated with ns1.filescrack.com

crack-vst.com	Domain-name	Associated with ns1.filescrack.com
mahapc.net	Domain-name	Associated with ns1.filescrack.com
procrackerez.net	Domain-name	Associated with ns1.filescrack.com
vstprocracker.com	Domain-name	Associated with ns1.filescrack.com
zubicrack.com	Domain-name	Associated with ns1.filescrack.com
shezacrack.com	Domain-name	Associated with ns1.filescrack.com
vstupcrack.com	Domain-name	Associated with ns1.filescrack.com
sdcrack.com	Domain-name	Associated with ns1.filescrack.com
prdownloader.com	Domain-name	Associated with ns1.filescrack.com
seriallink.org	Domain-name	Associated with ns1.filescrack.com
activecrack.org	Domain-name	Associated with ns1.filescrack.com
ashcrack.com	Domain-name	Associated with ns1.filescrack.com
vstapps.net	Domain-name	Associated with ns1.filescrack.com
vstsoft.net	Domain-name	Associated with ns1.filescrack.com
vstmix.com	Domain-name	Associated with ns1.filescrack.com
vstgurucrack.com	Domain-name	Associated with ns1.filescrack.com
alghazalimodelschool.com	Domain-name	Associated with ns1.filescrack.com
vstcracked.org	Domain-name	Associated with ns1.filescrack.com
ayeshapc.org	Domain-name	Associated with ns1.filescrack.com
plugcracked.org	Domain-name	Associated with ns1.filescrack.com
vstmafia.org	Domain-name	Associated with ns1.filescrack.com
pcsoftsfull.org	Domain-name	Associated with ns1.filescrack.com

sampc.info	Domain-name	Associated with ns1.filescrack.com
plugcrack.net	Domain-name	Associated with ns1.filescrack.com
vstsetup.net	Domain-name	Associated with ns1.filescrack.com
azharsoft.com	Domain-name	Associated with ns1.filescrack.com
piratcrack.com	Domain-name	Associated with ns1.filescrack.com
softwaresideas.com	Domain-name	Associated with ns1.filescrack.com
samsoftz.com	Domain-name	Associated with ns1.filescrack.com
pcsoftz.org	Domain-name	Associated with ns1.filescrack.com
softserial.org	Domain-name	Associated with ns1.filescrack.com
leecrack.com	Domain-name	Associated with ns1.filescrack.com
kingcrack.org	Domain-name	Associated with ns1.filescrack.com
softwaresguru.org	Domain-name	Associated with ns1.filescrack.com
plugcrack.org	Domain-name	Associated with ns1.filescrack.com
abdullahpc.org	Domain-name	Associated with ns1.filescrack.com
cracknote.net	Domain-name	Associated with ns1.filescrack.com
vstmafia.net	Domain-name	Associated with ns1.filescrack.com
vstsoftware.net	Domain-name	Associated with ns1.filescrack.com
crackdudu.com	Domain-name	Associated with ns1.filescrack.com
freecrackerz.org	Domain-name	Associated with ns1.filescrack.com
piratecrack.org	Domain-name	Associated with ns1.filescrack.com
getprocrack.net	Domain-name	Associated with ns1.filescrack.com
joincrack.net	Domain-name	Associated with ns1.filescrack.com

softwarelink.net	Domain-name	Associated with ns1.filescrack.com
optimalcrack.com	Domain-name	Associated with ns1.filescrack.com
vstjin.com	Domain-name	Associated with ns1.filescrack.com
pesktop.net	Domain-name	Associated with ns1.filescrack.com
procrackz.net	Domain-name	Associated with ns1.filescrack.com
productcrack.net	Domain-name	Associated with ns1.filescrack.com
cracklee.net	Domain-name	Associated with ns1.filescrack.com
vstforest.net	Domain-name	Associated with ns1.filescrack.com
vstworking.net	Domain-name	Associated with ns1.filescrack.com
soft4mac.net	Domain-name	Associated with ns1.filescrack.com
stcrack.net	Domain-name	Associated with ns1.filescrack.com
crackspro.org	Domain-name	Associated with ns1.filescrack.com
starcrack.org	Domain-name	Associated with ns1.filescrack.com
procrackz.org	Domain-name	Associated with ns1.filescrack.com
mustcrack.com	Domain-name	Associated with ns1.filescrack.com
ghazanfarpc.com	Domain-name	Associated with ns1.filescrack.com
crackactivater.com	Domain-name	Associated with ns1.filescrack.com
softwarelee.org	Domain-name	Associated with ns1.filescrack.com
prodownloader.org	Domain-name	Associated with ns1.filescrack.com
crackdisk.org	Domain-name	Associated with ns1.filescrack.com
softwarespro.org	Domain-name	Associated with ns1.filescrack.com
thiscrack.net	Domain-name	Associated with ns1.filescrack.com

vstcyberpc.com	Domain-name	Associated with ns1.filescrack.com
vstpincrack.com	Domain-name	Associated with ns1.filescrack.com
crackfue.com	Domain-name	Associated with ns1.filescrack.com
crackpatch.net	Domain-name	Associated with ns1.filescrack.com
crackmap.net	Domain-name	Associated with ns1.filescrack.com
crackex.net	Domain-name	Associated with ns1.filescrack.com
vstserial.com	Domain-name	Associated with ns1.filescrack.com
thesecrack.net	Domain-name	Associated with ns1.filescrack.com
vstpirate.net	Domain-name	Associated with ns1.filescrack.com
zippycrack.net	Domain-name	Associated with ns1.filescrack.com
crackapps.org	Domain-name	Associated with ns1.filescrack.com
iamactivator.org	Domain-name	Associated with ns1.filescrack.com
crackking.org	Domain-name	Associated with ns1.filescrack.com
softwarepatch.net	Domain-name	Associated with ns1.filescrack.com
serialsoft.net	Domain-name	Associated with ns1.filescrack.com
thatcrack.net	Domain-name	Associated with ns1.filescrack.com
vstcracker.com	Domain-name	Associated with ns1.filescrack.com
andicrack.com	Domain-name	Associated with ns1.filescrack.com
topcracksofts.com	Domain-name	Associated with ns1.filescrack.com
mailcrack.net	Domain-name	Associated with ns1.filescrack.com
premiumcrack.net	premiumcrack.net	Associated with ns1.filescrack.com
crackboss.net	Domain-name	Associated with ns1.filescrack.com

crackhouses.net	Domain-name	Associated with ns1.filescrack.com
keygencrack.org	Domain-name	Associated with ns1.filescrack.com
cyberspc.org	Domain-name	Associated with ns1.filescrack.com
vstpro.org	Domain-name	Associated with ns1.filescrack.com
smartcrack.org	Domain-name	Associated with ns1.filescrack.com
quickideas.org	Domain-name	Associated with ns1.filescrack.com
vstcrackpro.net	Domain-name	Associated with ns1.filescrack.com
185.216.143.0/24	IP-range	24xservice, used for cracking websites

7.2 Recommendations

- Block the IOCs provided in the "Indicators of compromise" section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to stealer-malware and cracking websites. Intrinsec offers its own CTI feed to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- Regularly train employees to recognize phishing attempts, especially those involving malicious attachments or suspicious links. Conduct internal phishing tests to assess and improve employee awareness.
- Train your employees to not download cracked software and only install programs and updates from official sources. Whenever possible, do not mix personal usage on corporate computers to limit risk of exposure of corporate credentials.
- Use advanced email security gateways to detect and block phishing emails, particularly those containing malicious attachments or links.
- Employ sandboxing solutions to analyse email attachments and URLs before they reach users.
- Enable multi-factor authentication (MFA) for browser-related accounts to mitigate credential theft.
- Set up network monitoring to identify unusual or unauthorized outbound connections, particularly to known Command and Control (C2) servers.

8. Sources

- https://threatfox.abuse.ch/browse/malware/win.eye_pyramid/
- https://www.domaintools.com/resources/blog/the-resurgence-of-the-manipulaters-team-breaking-heartsenders/
- https://www.justice.gov/usao-sdtx/pr/cybercrime-websites-selling-hacking-tools-transnational-organized-crime-groups-seized
- https://x.com/Syndikalist/status/1841889332577378411
- https://www.pta.gov.pk/category/pta-and-huawei-pakistan-sign-mou-to-strengthen-collaboration-in-it-and-telecom-sector-1577608552-2025-01-01
- https://csopakistan.com/pakistan-and-china-strengthen-cybersecurity-cooperation-through-new-mou/
- https://www.pakistantoday.com.pk/2024/01/30/pakistan-signs-agreement-with-china-to-become-regional-internet-connectivity-hub/
- https://cloud.google.com/blog/topics/threat-intelligence/russian-targeting-gov-business/
- https://www.silentpush.com/blog/fin7/#FIN7-shell-domains-morphing-into-phishing-websites