
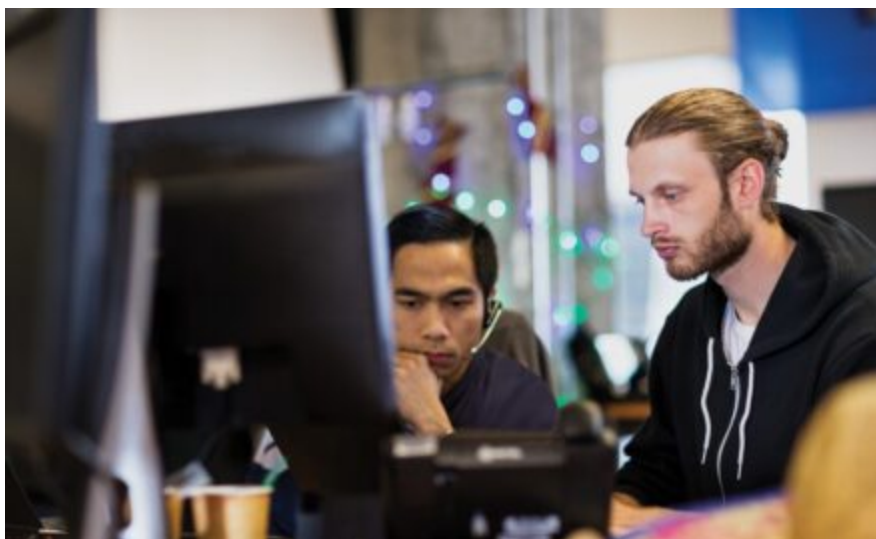


DEV-0196: QuaDream’s “KingsPawn” malware used to target civil society in Europe, North America, the Middle East, and Southeast Asia

 microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/

April 11, 2023



April 2023 update – Microsoft Threat Intelligence has shifted to a new threat actor naming taxonomy aligned around the theme of weather. **DEV-0196** is now tracked as **Carmine Tsunami**.

To learn more about this evolution, how the new taxonomy represents the origin, unique traits, and impact of threat actors, and a complete mapping of threat actor names, read this blog: [Microsoft shifts to a new threat actor naming taxonomy](#).

Microsoft Threat Intelligence analysts assess with high confidence that a threat group tracked by Microsoft as DEV-0196 is linked to an Israel-based private sector offensive actor (PSOA) known as QuaDream. QuaDream reportedly sells a platform they call REIGN to governments for law enforcement purposes. REIGN is a suite of exploits, malware, and infrastructure designed to exfiltrate data from mobile devices.

In this blog, Microsoft analyzes DEV-0196, discusses technical details of the actor’s iOS malware, which we call KingsPawn, and shares both host and network indicators of compromise that can be used to aid in detection.

Over the course of our investigation into DEV-0196, Microsoft collaborated with multiple partners. One of those partners, Citizen Lab of the University of Toronto’s Munk School, identified at least five civil society victims of the DEV-0196 malware that included journalists,

political opposition figures, and a non-government organisation (NGO) worker, in North America, Central Asia, Southeast Asia, Europe, and the Middle East. Furthermore, Citizen Lab was able to identify operator locations for QuaDream systems in the following countries: Bulgaria, Czechia, Hungary, Ghana, Israel, Mexico, Romania, Singapore, United Arab Emirates, and Uzbekistan. Read the Citizen Lab report [here](#).

Microsoft is sharing information about DEV-0196 with our customers, industry partners, and the public to improve collective knowledge of how PSOs operate and raise awareness about how PSOs facilitate the targeting and exploitation of civil society. For more info, read [Standing up for democratic values and protecting stability of cyberspace](#).

DEV-0196: A private-sector offensive actor based in Israel

PSOAs, which Microsoft also refers to as cyber mercenaries, sell hacking tools or services through a variety of business models, including access as a service. In access as a service, the actor sells full end-to-end hacking tools that can be used by the purchaser in cyber operations. The PSOA itself is not involved in any targeting or running of the operations.

Microsoft Threat Intelligence analysts assess with high confidence that DEV-0196 uses this model, selling exploitation services and malware to governments. It's not directly involved in targeting. Microsoft also assesses with high confidence that DEV-0196 is linked to an Israel-based private company called QuaDream. According to the [Israeli Corporations Authority](#), QuaDream, under the Israeli name קוודרים בע"מ, was incorporated in August 2016. The company has no website, and there is little public reporting about the company, with a few notable exceptions.

QuaDream came to international attention in a [2022 Reuters report](#), which cited a company brochure that described the REIGN platform and a list of capabilities, the report also notably suggested that QuaDream used a zero-click iOS exploit that leveraged the same vulnerability seen in NSO Group's ForcedEntry exploit. An earlier report by Israeli [news outlet Haaretz](#), also citing a QuaDream brochure, revealed that QuaDream did not sell REIGN directly to customers but instead did so through a Cypriot company. Haaretz also reported that Saudi Arabia's government was among QuaDream's clients, as was the government of Ghana. However, Haaretz could not confirm allegations made in the [Ghanian press](#) and [repeated](#) in the Israeli [press](#) that QuaDream employees were among 14 Israeli tech workers from different companies who travelled to Accra, Ghana in 2020 to meet with the incumbent administration three months prior to the presidential election for the purposes of a special project relating to it.

QuaDream was mentioned in a December 2022 report from [Meta](#), which reportedly took down 250 accounts associated with the company. According to the report, Meta observed QuaDream testing its ability to exploit iOS and Android mobile devices with the intent "to

exfiltrate various types of data including messages, images, video and audio files, and geolocation.”

Technical investigation: DEV-0196 malware

Microsoft Threat Intelligence analysts assess with high confidence that the malware, which we call KingsPawn, is developed by DEV-0196 and therefore strongly linked to QuaDream. We assess with medium confidence that the mobile malware we associate with DEV-0196 is part of the system publicly discussed as REIGN.

The captured samples targeted iOS devices, specifically iOS 14, but there were indications that some of the code could also be used on Android devices. Since the malware sample targets iOS 14, some of the techniques used in this sample may no longer work or be relevant on newer iOS versions. However, we assess it's highly likely that DEV-0196 will have updated their malware, targeting newer versions to account for this. Analysis of the malware revealed that it is split into multiple components. The sections below focus on two of those components: a monitor agent and the main malware agent.

Monitor agent

The monitor agent is a native Mach-O file written in Objective-C. It is responsible for reducing the forensic footprint of the malware to prevent detection and hinder investigations. It has multiple techniques to do this, one of which is monitoring various directories, such as */private/var/db/analyticsd/* and */private/var/mobile/Library/Logs/CrashReporter*, for any malware execution artifacts or crash-related files. Once these artifacts or files are identified, the monitor agent deletes them.

The monitor agent is also in charge of managing the various processes and threads spawned on behalf of the malware to avoid artifacts created from unexpected process crashes. The agent uses the *waitpid* function to monitor all child processes that are spawned, and the child process IDs are added to a tracking list. The monitor agent attempts to safely shut down tracked child processes by calling *sigaction* with the SIGTSTP parameter, if *sigaction* returns successfully this means the child process is reachable and a *SIGKILL* command is sent to kill it. This avoids sending a *kill* command to a non-existent PID, which can leave error messages and artifacts behind.

Main agent

The main agent is also a native Mach-O file. However, it is written in Go, a highly portable language, which was likely chosen because it allows compilation across multiple platforms, reducing development effort.

This agent includes capabilities to:

- Get device information (such as iOS version and battery status)
- Wi-Fi information (such as SSID and airplane mode status)
- Cellular information (such as carrier, SIM card data, and phone number)
- Search for and retrieve files
- Use the device camera in the background
- Get device location
- Monitor phone calls
- Access the iOS keychain
- Generate an iCloud time-based one-time password (TOTP)

It achieves some of these functionalities, for example the surreptitious camera use, by leveraging two key binaries, *tccd* and *mediaserverd*, a technique described by [ZecOps](#). The name *tccd* stands for Transparency, Consent, and Control (TCC) Daemon, and the process manages the access permissions for various peripherals such as the camera and microphone. Normally, users are met with a pop-up prompt from the *tccd* process, alerting them that something has requested access to the camera, microphone, or other peripheral, and the user is required to either allow or deny it. In this compromise scenario, the agent injects itself into the *tccd* binary, which allows the agent to spawn both new processes and threads as part of the exploitation process, and also allows it to bypass any *tccd* prompts on the device meaning the user would be unaware of camera compromise. In concert with *tccd*, the agent also provisions itself permission to run in the background via *mediaserverd*. This binary handles the interface that other apps interact with when utilizing the camera. For more details on [iOS process injection](#), *tccd* and other system components, see Jonathan Levin's macOS and iOS internals [books](#) and [blog](#).

The techniques used in the main agent include a [PMAP](#) bypass, an [Apple Mobile File Integrity \(AMFI\)](#) bypass, and a [sandbox](#) escape. PMAP is one of the mechanisms that works with the Page Protection Layer ([PPL](#)) to prevent unsigned code from running on iOS devices. AMFI is a protection mechanism comprised of multiple components including a kernel extension, *AppleFileMobileIntegrity.kext*, as well as userland daemon, *amfid*. The [sandbox](#) limits access to system resources and user data via an entitlements system. Although PMAP, PPL, AMFI, and the sandbox have been hardened over the years, advanced attackers attempt to circumvent these protection mechanisms in order to [run unsigned code](#).

The agent also creates [a secure channel](#) for [XPC](#) messaging by creating a nested app extension called *fud.appex*. XPC messaging allows the agent to query various system binaries for sensitive device information, such as location details. Although there is a legitimate binary called *fud* on iOS devices that is part of the Mobile Accessory updater service, *fud.appex* is not part of a legitimate Apple service. The agent creates the malicious app extension inside the folder `/private/var/db/com.apple.xpc.roleaccountd.staging/PlugIns/`. The primary reason for performing XPC messaging from within this application extension is to establish a covert channel that enables the agent to avoid being monitored. This nested directory technique means that the XPC service is registered such a way that it is only visible

to the app extension itself, so any external monitoring by other applications and system processes is far more difficult. Upon unhooking and restoring *tccd* to its original state, the entire *Plugins* folder is removed to further hide any artifacts of its existence.

In their [blog](#), Citizen Lab discusses the presence of likely malicious calendar events on devices compromised by DEV-0196's malware, so another notable function of the main agent is that it contains specific code to remove events from the device's calendar. The agent searches all calendar events from two years prior to the current time and up to the furthest possible allowed future time, removing any events that are tied to a given email address as the "organizer". The agent also removes the email address from the *idstatuscache.plist*, which is a database containing records of the first contact of the device with other iCloud accounts. This list would contain the email address that sent the malicious calendar invitation, as well as a time stamp of the original interaction, such as when the invite was received.

There is additional functionality within the agent to cover its tracks by removing artifacts of location monitoring from the *locationd* process' records. To first query locations from *locationd*, the agent must register a client that communicates with *locationd* via XPC messaging. The *locationd* process then stores a record of these connections in */private/var/root/Library/Caches/locationd/clients.plist*. The malicious agent searches for items in the client *plist* that have a suffix of *subridged*, and then removes them, which indicates that the name of their location monitoring client likely ends in that word. This is another example of malicious activity attempting to masquerade as benign system processes, since *subridged* is the name of a legitimate Apple binary, a part of the SoftwareUpdateBridge Framework.

Technical investigation: DEV-0196 infrastructure

Microsoft developed unique network detections that could be used to fingerprint DEV-0196's infrastructure on the internet. The group heavily utilized domain registrars and inexpensive cloud hosting providers that accepted cryptocurrency as payment. They tended to only use a single domain per IP address and domains were very rarely reused across multiple IP addresses. Many of the observed domains were deployed using free [Let's Encrypt](#) SSL certificates, while others used self-signed certificates designed to blend in with normal Kubernetes deployments.

We have included network-based indicators at the end of this post for detection purposes. Often, threat actors employ domains that carry country-specific TLDs or themes that align with the location of intended targets. Notably, our list of DEV-0196 domains includes domains strongly associated with some countries that Citizen Lab has identified as locations of victims, countries where QuaDream platforms were operating, or both. To be clear, the identification of victims of the malware in a country doesn't necessarily mean that an entity in that country is a DEV-0196 customer, as international targeting is common.

Prevention and detection

Preventing exploitation of mobile devices by advanced actors who potentially have zero-click exploits is difficult. There are also significant challenges in detecting an attack on mobile devices, both during and after the compromise. This section discusses some methods for minimizing the risk of malicious actors compromising mobile devices, and then provides some indicators of compromise we associate with DEV-0196 activity.

Basic cyber hygiene is important in helping prevent mobile device compromise. Specific best practices include keeping the device's software updated to the latest version, enabling automatic software updates if available, using anti-malware software, and being vigilant about not clicking links in any unexpected or suspicious messages.

If you believe you may be targeted by advanced attackers and use an iOS device, we recommend enabling Lockdown Mode. Lockdown Mode offers enhanced security for iOS devices by reducing the attack surface available to threat actors.

Sentinel detections

Microsoft Sentinel customers can use the TI Mapping analytic to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here:
<https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy>.

In addition, customers can access the shared indicators in a structured format via GitHub so that they can be integrated into custom analytics and other queries:
<https://github.com/microsoft/mstic/blob/master/RapidReleaseTI/Indicators.csv>.

Indicators of compromise (IOCs)

Host-based indicators

These host-based indicators are indicative of DEV-0196 activity; however, they shouldn't be used solely as attribution since other actors may also use the same or similar TTPs.

The file existing, or process activity from,
/private/var/db/com.apple.xpc.roleaccountd.staging/subbridged

The file existing, or process activity from, *com.apple.avcapture*

The folder */private/var/db/com.apple.xpc.roleaccountd.staging/PlugIns/fud.appex/* existing, or having activity detected from the folder.

Network indicators

Based on the results of our C2 investigation, Microsoft Threat Intelligence associate the following domains with DEV-0196 activity. The dates the domains were first detected as likely in use is given, along with the last seen active date.

| Domain | First active | Last active |
|------------------------|---------------------|--------------------|
| fosterunch[.]com | 2022-05-30 | CURRENT |
| womnbling[.]com | 2022-05-30 | CURRENT |
| zebra-arts[.]com | 2022-05-31 | CURRENT |
| pennywines[.]com | 2022-08-19 | CURRENT |
| choccoline[.]com | 2022-08-19 | CURRENT |
| lateparties[.]com | 2022-09-15 | CURRENT |
| foundrycolletive[.]com | 2022-11-07 | CURRENT |
| jungelfruitime[.]com | 2022-11-09 | CURRENT |
| gameboysess[.]com | 2022-11-09 | CURRENT |
| healthcovid19[.]com | 2022-11-10 | CURRENT |
| codingstudies[.]com | 2022-11-16 | CURRENT |
| hoteluxurysm[.]com | 2022-11-18 | CURRENT |
| newz-globe[.]com | 2022-11-23 | CURRENT |
| hotalsextra[.]com | 2022-11-23 | CURRENT |
| nordmanetime[.]com | 2022-11-23 | CURRENT |
| fullaniimal[.]com | 2022-11-23 | CURRENT |
| wikipedoptions[.]com | 2022-11-23 | CURRENT |
| redanddred[.]com | 2022-11-23 | CURRENT |
| whiteandpiink[.]com | 2022-12-02 | CURRENT |
| agronomdoc[.]com | 2022-12-02 | CURRENT |
| nutureheus[.]com | 2022-12-02 | CURRENT |
| timeeforsports[.]com | 2022-12-15 | CURRENT |

| | | |
|-----------------------|------------|---------|
| treeroots[.]com | 2022-12-15 | CURRENT |
| unitedyears[.]com | 2022-12-15 | CURRENT |
| eccocredit[.]com | 2022-12-16 | CURRENT |
| ecologitics[.]com | 2022-12-19 | CURRENT |
| climatestews[.]com | 2022-12-19 | CURRENT |
| aqualizas[.]com | 2022-12-19 | CURRENT |
| bgnews-bg[.]com | 2022-12-20 | CURRENT |
| mikontravels[.]com | 2022-12-23 | CURRENT |
| e-gaming[.]online | 2022-12-23 | CURRENT |
| transformaition[.]com | 2022-12-23 | CURRENT |
| betterstime[.]com | 2022-12-23 | CURRENT |
| goshopeerz[.]com | 2022-12-23 | CURRENT |
| countshops[.]com | 2022-12-23 | CURRENT |
| inneture[.]com | 2022-12-23 | CURRENT |
| shoppingeos[.]com | 2022-12-23 | CURRENT |
| mwww[.]ro | 2023-01-05 | CURRENT |
| rentalproct[.]com | 2023-01-05 | CURRENT |
| bcarental[.]com | 2023-01-05 | CURRENT |
| kikocruise[.]com | 2023-01-05 | CURRENT |
| elvacream[.]com | 2023-01-10 | CURRENT |
| pachadesert[.]com | 2023-01-12 | CURRENT |
| razzodev[.]com | 2023-02-06 | CURRENT |
| wombatcash[.]com | 2023-02-06 | CURRENT |
| globepayinfo[.]com | 2023-02-06 | CURRENT |
| job4uhunt[.]com | 2023-02-08 | CURRENT |
| ctbgameson[.]com | 2023-02-08 | CURRENT |

| | | |
|---------------------------|------------|------------|
| adeptary[.]com | 2023-02-08 | CURRENT |
| hinterfy[.]com | 2023-02-08 | CURRENT |
| biznomex[.]com | 2023-02-08 | CURRENT |
| careerhub4u[.]com | 2023-02-08 | CURRENT |
| furiamoc[.]com | 2023-02-08 | CURRENT |
| motorgamings[.]com | 2023-02-08 | CURRENT |
| aniarchit[.]com | 2023-02-08 | CURRENT |
| skyphotogreen[.]com | 2023-02-26 | CURRENT |
| datacentertime[.]com | 2023-02-26 | CURRENT |
| stylelifees[.]com | 2023-02-26 | CURRENT |
| kidzlande[.]com | 2023-03-01 | CURRENT |
| homelosite[.]com | 2023-03-01 | CURRENT |
| zoolow[.]com | 2023-03-01 | CURRENT |
| studiesutshifts[.]com | 2023-03-01 | CURRENT |
| codingstudies[.]com | 2023-03-08 | CURRENT |
| londonistory[.]com | 2023-03-16 | CURRENT |
| bestteamlife[.]com | 2023-03-16 | CURRENT |
| newsandlocalupdates[.]com | 2023-03-16 | CURRENT |
| youristores[.]com | 2023-03-16 | CURRENT |
| zoolow[.]com | 2023-02-26 | 2023-03-04 |
| kidzlande[.]com | 2023-02-26 | 2023-03-04 |
| homelosite[.]com | 2023-02-26 | 2023-03-04 |
| studiesutshifts[.]com | 2023-02-26 | 2023-03-04 |
| datacentertime[.]com | 2022-11-07 | 2023-02-25 |
| homelosite[.]com | 2022-11-09 | 2023-02-25 |
| zoolow[.]com | 2022-11-10 | 2023-02-25 |

| | | |
|-------------------------|------------|------------|
| kidzlande[.]com | 2022-11-10 | 2023-02-25 |
| studiesutshifts[.]com | 2022-11-10 | 2023-02-25 |
| stylelifees[.]com | 2022-11-11 | 2023-02-25 |
| skyphotogreen[.]com | 2022-11-11 | 2023-02-25 |
| gardenearthis[.]com | 2023-01-11 | 2023-02-25 |
| fullstorelife[.]com | 2023-01-11 | 2023-02-25 |
| incollegely[.]org | 2022-05-24 | 2023-01-20 |
| shoplifys[.]com | 2022-05-26 | 2023-01-20 |
| thetimespress[.]com | 2022-06-24 | 2023-01-20 |
| studyshifts[.]com | 2022-06-24 | 2023-01-20 |
| codinerom[.]com | 2022-07-10 | 2023-01-20 |
| gamingcolonys[.]com | 2022-07-17 | 2023-01-20 |
| kidzalnd[.]org | 2022-07-17 | 2023-01-20 |
| wildhour[.]store | 2022-07-26 | 2023-01-20 |
| wilddog[.]site | 2022-07-26 | 2023-01-20 |
| garilc[.]com | 2022-07-26 | 2023-01-20 |
| runningandbeyond[.]org | 2022-08-04 | 2023-01-20 |
| fullmoongreyparty[.]org | 2022-08-04 | 2023-01-20 |
| greenrunners[.]org | 2022-08-04 | 2023-01-20 |
| sunsandlights[.]com | 2022-08-09 | 2023-01-20 |
| techpowerlight[.]com | 2022-08-16 | 2023-01-20 |
| gamezess[.]com | 2022-08-29 | 2023-01-20 |
| planningly[.]org | 2022-08-29 | 2023-01-20 |
| luxario[.]org | 2022-09-03 | 2023-01-20 |
| vinoneros[.]com | 2022-09-03 | 2023-01-20 |
| i-reality[.]online | 2022-09-07 | 2023-01-20 |

| | | |
|----------------------|------------|------------|
| styleanature[.]com | 2022-09-07 | 2023-01-20 |
| planetosgame[.]com | 2022-12-12 | 2023-01-20 |
| kidsfunland[.]org | 2022-07-29 | 2023-01-19 |
| fullstorelife[.]com | 2022-11-11 | 2023-01-09 |
| localtalk[.]store | 2022-01-26 | 2022-12-20 |
| allplaces[.]online | 2022-01-26 | 2022-12-20 |
| sunclub[.]site | 2022-01-26 | 2022-12-20 |
| thenewsfill[.]com | 2022-05-26 | 2022-12-20 |
| wellnessjane[.]org | 2022-05-26 | 2022-12-20 |
| meehealth[.]org | 2022-05-27 | 2022-12-20 |
| gameizes[.]com | 2022-07-20 | 2022-12-20 |
| playozas[.]com | 2022-07-20 | 2022-12-20 |
| foodyplates[.]com | 2022-07-20 | 2022-12-20 |
| designaroo[.]org | 2022-08-29 | 2022-12-20 |
| designspacing[.]org | 2022-08-29 | 2022-12-20 |
| stockstiming[.]org | 2022-09-01 | 2022-12-20 |
| hoteliqo[.]com | 2022-09-01 | 2022-12-20 |
| projectoid[.]org | 2022-09-01 | 2022-12-20 |
| study-search[.]com | 2022-09-01 | 2022-12-20 |
| tokenberries[.]com | 2022-09-03 | 2022-12-20 |
| recovery-plan[.]org | 2022-09-07 | 2022-12-20 |
| deliverystorz[.]com | 2022-09-07 | 2022-12-20 |
| forestaaa[.]com | 2022-10-04 | 2022-12-20 |
| addictmetui[.]com | 2022-10-20 | 2022-12-20 |
| earthyowantiis[.]com | 2022-10-20 | 2022-12-20 |
| zedforme[.]com | 2022-10-20 | 2022-12-20 |

| | | |
|---------------------|------------|------------|
| forestaaa[.]com | 2022-10-28 | 2022-12-20 |
| navadatetime[.]com | 2022-11-10 | 2022-12-15 |
| careers4ad[.]com | 2022-11-13 | 2022-12-15 |
| gardenearthis[.]com | 2022-11-07 | 2022-12-14 |
| studyreaserch[.]com | 2022-11-09 | 2022-12-14 |
| novinite[.]biz | 2022-08-31 | 2022-12-10 |
| agronomdoc[.]com | 2022-11-16 | 2022-11-28 |
| whiteandpiink[.]com | 2022-11-16 | 2022-11-28 |
| nutreheus[.]com | 2022-11-18 | 2022-11-28 |
| dressuse[.]com | 2022-09-18 | 2022-11-20 |
| iwoodstor[.]xyz | 2022-09-18 | 2022-11-20 |
| teachlearning[.]org | 2022-09-18 | 2022-11-20 |
| subcloud[.]online | 2022-09-21 | 2022-11-20 |
| monvesting[.]com | 2022-09-21 | 2022-11-20 |
| elektrozi[.]com | 2022-09-21 | 2022-11-20 |
| hoteluxurysm[.]com | 2022-11-09 | 2022-11-14 |
| hopsite[.]online | 2022-11-13 | 2022-11-14 |
| bikersrental[.]com | 2022-05-24 | 2022-11-13 |
| takestox[.]com | 2022-05-24 | 2022-11-13 |
| sidelot[.]org | 2022-05-24 | 2022-11-13 |
| powercodings[.]com | 2022-08-21 | 2022-11-13 |
| naturemeter[.]org | 2022-08-21 | 2022-11-13 |
| takebreak[.]jio | 2022-10-12 | 2022-11-13 |
| fullstorelife[.]com | 2022-11-07 | 2022-11-10 |
| noraplant[.]com | 2022-11-09 | 2022-11-09 |
| forestaaa[.]com | 2022-10-04 | 2022-11-07 |

| | | |
|--------------------------|------------|------------|
| goodsforuw[.]com | 2022-10-26 | 2022-11-07 |
| stayle[.]co | 2022-10-26 | 2022-11-07 |
| eedloversra[.]online | 2022-10-28 | 2022-11-07 |
| sevensdfe[.]com | 2022-11-03 | 2022-11-07 |
| dsudro[.]com | 2022-11-03 | 2022-11-07 |
| gameboysess[.]com | 2022-11-07 | 2022-11-07 |
| sseamb[.]com | 2022-10-26 | 2022-11-06 |
| healthcovid19[.]com | 2022-11-04 | 2022-11-06 |
| noraplant[.]com | 2022-11-04 | 2022-11-06 |
| fullstorelife[.]com | 2022-11-04 | 2022-11-06 |
| datacentertime[.]com | 2022-11-04 | 2022-11-05 |
| recover-your-body[.]xyz | 2022-01-06 | 2022-11-02 |
| reloadyourbrowser[.]info | 2022-07-05 | 2022-11-02 |
| comeandpet[.]me | 2022-07-05 | 2022-11-02 |
| brushyourteeth[.]online | 2022-07-05 | 2022-11-02 |
| digital-mar[.]com | 2022-08-10 | 2022-11-02 |
| retailmark[.]net | 2022-08-16 | 2022-11-02 |
| dsudro[.]com | 2022-10-04 | 2022-11-02 |
| studysliii[.]com | 2022-10-26 | 2022-11-02 |
| homeigardens[.]com | 2022-09-07 | 2022-10-29 |
| stayle[.]co | 2022-10-20 | 2022-10-24 |
| studysliii[.]com | 2022-10-20 | 2022-10-24 |
| goodsforuw[.]com | 2022-10-20 | 2022-10-24 |
| dsudro[.]com | 2022-10-20 | 2022-10-24 |
| sseamb[.]com | 2022-10-20 | 2022-10-24 |
| sevensdfe[.]com | 2022-10-20 | 2022-10-24 |

| | | |
|------------------------|------------|------------|
| koraliove[.]com | 2022-04-05 | 2022-10-13 |
| topuprr[.]com | 2022-04-05 | 2022-10-13 |
| zeebefg[.]com | 2022-04-05 | 2022-10-12 |
| takebreak[.]jio | 2022-06-21 | 2022-10-11 |
| forestaaa[.]com | 2022-10-03 | 2022-10-03 |
| teachlearning[.]org | 2022-09-18 | 2022-09-18 |
| newsbuiltin[.]online | 2022-09-15 | 2022-09-17 |
| fyfa[.]xyz | 2022-09-15 | 2022-09-17 |
| monvesting[.]com | 2022-07-19 | 2022-09-15 |
| teachlearning[.]org | 2022-07-19 | 2022-09-15 |
| elektrozi[.]com | 2022-07-20 | 2022-09-15 |
| thepila[.]com | 2022-09-15 | 2022-09-15 |
| thegreenlight[.]xyz | 2022-01-11 | 2022-09-14 |
| gosport24[.]com | 2022-01-11 | 2022-09-14 |
| classiccolor[.]live | 2022-01-11 | 2022-09-11 |
| shoeszise[.]xyz | 2022-02-24 | 2022-09-11 |
| cleanitgo[.]info | 2022-02-24 | 2022-09-11 |
| setclass[.]live | 2022-02-24 | 2022-09-11 |
| white-rhino[.]online | 2022-04-14 | 2022-09-11 |
| space-moon[.]com | 2022-04-14 | 2022-09-11 |
| enrollering[.]com | 2022-05-24 | 2022-09-11 |
| newslocalupdates[.]com | 2022-08-19 | 2022-09-11 |
| newsbuiltin[.]online | 2022-09-11 | 2022-09-11 |
| beendos[.]com | 2022-04-14 | 2022-09-10 |
| linestrip[.]online | 2022-07-01 | 2022-09-07 |
| sunnyweek[.]site | 2022-07-01 | 2022-09-07 |