

December 2021

# Threat Report on the Surveillance-for-Hire Industry

*December 16, 2021*

*By Mike Dvilyanski, Head of Cyber Espionage Investigations,  
David Agranovich, Director, Threat Disruption, and  
Nathaniel Gleicher, Head of Security Policy*

## Summary

- The global surveillance-for-hire industry targets people to collect intelligence, manipulate and compromise their devices and accounts across the internet.
- While these “cyber mercenaries” often claim that their services only target criminals and terrorists, our months-long investigation concluded that targeting is in fact indiscriminate and includes journalists, dissidents, critics of authoritarian regimes, families of opposition members and human rights activists.
- We disabled seven entities who targeted people across the internet in over 100 countries; shared our findings with security researchers, other platforms and policymakers; issued Cease and Desist warnings; and also alerted people who we believe were targeted to help them strengthen the security of their accounts.

This report is the result of our months-long investigation and disruption of seven entities providing surveillance-for-hire services to target people across the internet, including journalists and human rights activists. It outlines the actions we took against them and includes our research into what we call the “surveillance chain” — phases of attack we’ve observed over the course of our threat intelligence research. Our hope is to contribute to the broader understanding of the harms this industry represents worldwide and call on the democratic governments to take further steps to help protect people and impose oversight on the sellers of ubiquitous spyware.

## What is surveillance-for-hire and how does it work?

In recent months, there has been an increased focus on NSO, the company behind the Pegasus spyware (i.e. software used to enable surveillance) that we [enforced against and sued](#) in 2019. However, it’s important to realize that NSO is only one piece of a much broader global cyber mercenary ecosystem. As part of a separate effort, today, we are sharing our findings about seven entities that engaged in surveillance activity and we will continue to take action against others as we find them.

The global surveillance-for-hire industry targets people across the internet to collect intelligence, manipulate them into revealing information and compromise their devices and accounts. While cyber mercenaries often claim that their services and surveillanceware are intended to focus on criminals and terrorists, our investigation found they in fact regularly targeted journalists, dissidents, critics of authoritarian regimes, families of opposition and human rights activists around the world. These companies are part of a sprawling industry that provides intrusive software tools and surveillance services indiscriminately to any customer — regardless of who they target or the human rights abuses they might enable.

This ecosystem works to provide powerful capabilities to its clients against victims who in most cases have no way of knowing they are being targeted. In a sense, this industry “democratizes” these threats, making them available to government and non-government groups that otherwise wouldn’t have these capabilities to cause harm. They in effect exponentially increase the supply of threat actors in the world.

We observed three phases of targeting activity by these commercial players that make up their “surveillance chain”: *Reconnaissance*, *Engagement*, and *Exploitation*. Each phase informs the next and often they repeat in cycles. While some of these entities specialize in one particular stage of surveillance, others support the entire chain from start to finish. Although public debate so far has mainly focused on the *exploitation* phase, it’s critical to disrupt the entire lifecycle of the attack because the earlier stages enable the later ones. If we can collectively tackle this threat earlier in the surveillance chain, it would help stop the harm before it gets to its final, most serious stage of compromising people’s devices and accounts.

Here are more details and TTPs (the tactics, techniques, and procedures) characteristic for each attack chain stage.

### ***Reconnaissance***

This first stage of the surveillance chain is typically the least visible to the targets, who are silently profiled by cyber mercenaries on behalf of their clients, often using software to automate data collection from across the internet. Firms selling these capabilities typically market themselves as “web intelligence services” to enable collection, retention, analysis and searchability — both targeted and at scale.

Usually, these services and apps are designed to pull information about targets from all available online records. They typically scrape and store data from public websites such as blogs, social media, knowledge management platforms like Wikipedia and Wikidata, news media, forums and “dark web” sites. Surveillanceware often provides the benefit of obfuscating the origin of the activity through unattributable infrastructure.

One of the primary means of collecting information on social media is the use of fake accounts. These inauthentic assets can be used to search and view people’s profiles, Friends, Likes and other publicly available information, join Groups and Events, and follow or friend targets. They are typically managed by the service provider for its clients, or operated by the customers themselves through software provided by the surveillance-for-hire firm. The level of sophistication of the fake accounts varies considerably across cyber mercenaries and their customers.

## ***Engagement***

This second phase of the surveillance chain is typically the most visible to its targets and most critical to spot to prevent compromise. It is aimed at establishing contact with the targets or people close to them in an effort to build trust, solicit information, and trick them into clicking on links or downloading files (to enable the next “exploitation” phase).

To do that, the operators typically rely on social engineering tactics and use fictitious personas to reach out to people via email, phone calls, text messages, or direct messages on social media. These personas are typically tailored to each particular target to seem credible and avoid tipping people off to suspect malicious intent. These efforts are often prolonged and involve creating backstops for fake personas and organizations across multiple internet services so they appear more legitimate and can withstand scrutiny. The social engineering aims can range from obtaining sensitive information desired by the client to targeting the individual with malware to enable full-device digital surveillance. To achieve them, the operators may attempt to direct people to more direct channels like voice or video calls or even in-person meetings.

## ***Exploitation***

The final stage of the surveillance chain manifests as what’s commonly known as “hacking for hire.” Providers may create phishing domains designed to trick targets into giving away their credentials to sensitive accounts like email, social media, financial services, and corporate networks. We’ve seen them spoof the domains of news organizations, telecom providers, banks, and URL-shortening services to deceive their victims.

To enable the delivery of malicious “payload,” the operators may either use their own custom-built exploits or acquire malicious tools from other vendors. The sophistication in tooling varies significantly across this industry, ranging from off-the-shelf malware easily detected by most anti-virus software to single-click or even zero-click exploit links sent to the targets. The ultimate goal is to enable device-level surveillance and monitoring of mobile phones or computers. At that point, depending on the exploit, the attacker can access any data on the target’s phone or computer, including passwords, cookies, access tokens, photos, videos, messages, address books, as well as silently activate the microphone, camera, and geo-location tracking.

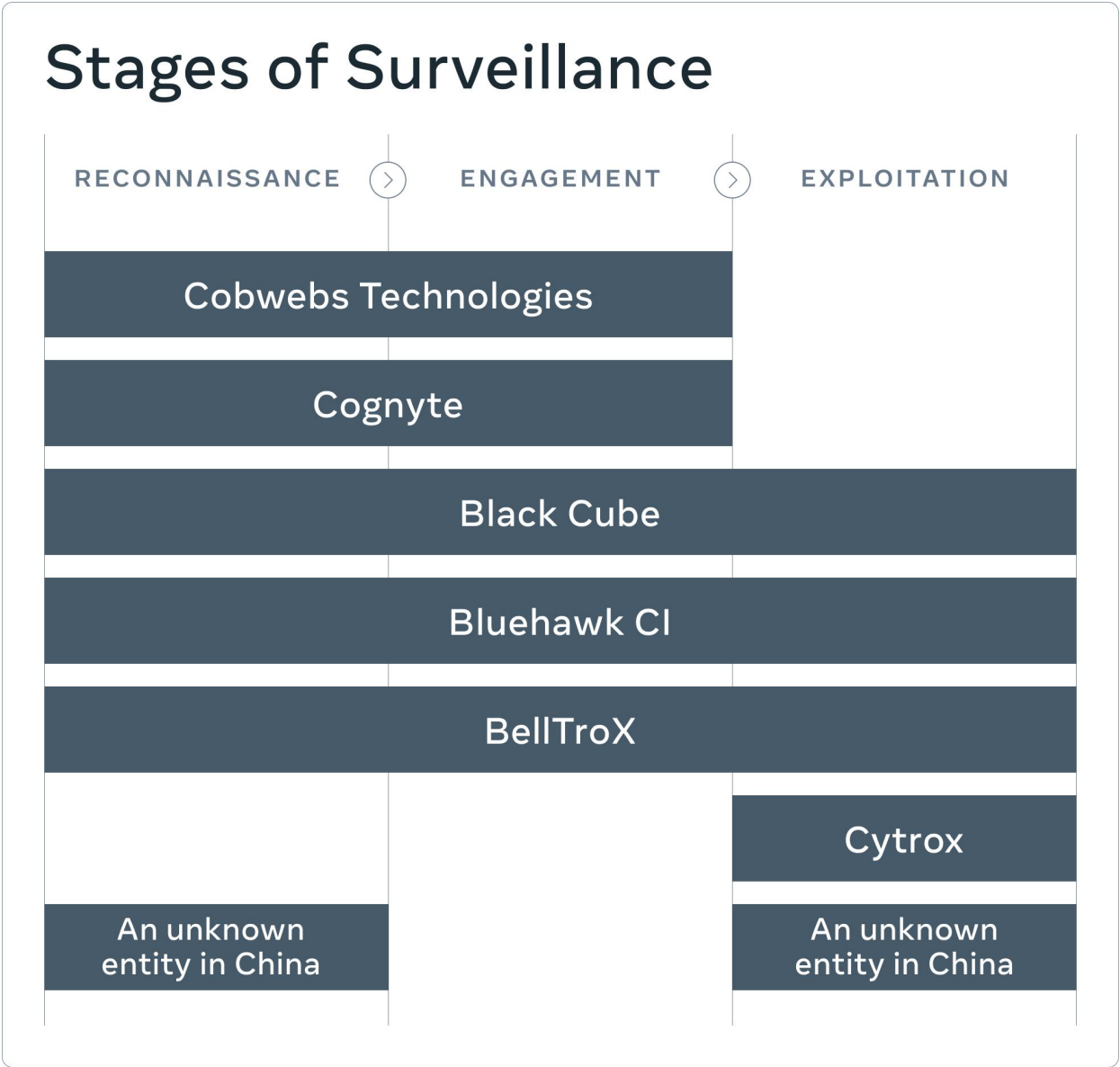
## Our investigative findings and the actions we took

As a result of our months-long investigation, we took action against seven different surveillance-for-hire entities to disrupt their ability to use their digital infrastructure to abuse social media platforms and enable surveillance of people across the internet. They provided services across all three phases of the surveillance chain that were used to indiscriminately target people. These surveillance providers are based in China, Israel, India, and North Macedonia. They targeted people in over 100 countries around the world on behalf of their clients.

To help disrupt these activities, we blocked related infrastructure, banned these entities from our platform and issued Cease and Desist warnings, putting each of them on notice that their targeting of people has no place on our platform and is against our Community Standards. We also shared our findings with security researchers, other platforms, and policymakers so they too can take appropriate action. We also notified people who we believe were targeted to help them take steps to strengthen the security of their accounts.

The entities behind these surveillance operations are persistent, and we expect them to evolve their tactics. However, our detection systems and threat investigators, as well as other teams in the broader security community keep improving to make it harder for them to remain undetected. We will continue to share our findings when possible so people are aware of the threats we are seeing and can take steps to strengthen the security of their accounts.

*Here is what we found*



**1. Cobwebs Technologies**

Surveillance chain phases: Reconnaissance, Engagement

We removed about 200 accounts which were operated by Cobwebs and its customers worldwide. This firm was founded in Israel with offices in the United States and sells access to its platform that enables reconnaissance across the internet, including Facebook, Instagram, WhatsApp, Twitter, Flickr, public websites and “dark web” sites. In addition to collecting

information about their targets, the accounts used by Cobwebs customers also engaged in social engineering to join closed communities and forums and trick people into revealing personal information.

Our investigation identified customers in Bangladesh, Hong Kong, the United States, New Zealand, Mexico, Saudi Arabia, Poland, and other countries. In addition to targeting related to law enforcement activities, we also observed frequent targeting of activists, opposition politicians and government officials in Hong Kong and Mexico.

## **2. Cognyte**

### **Surveillance chain phases: Reconnaissance, Engagement**

We removed about 100 accounts on Facebook and Instagram which were linked to Cognyte (formerly known as WebintPro) and its customers. This firm is based in Israel and sells access to its platform which enables managing fake accounts across social media platforms including Facebook, Instagram, Twitter, YouTube, and VKontakte (VK), and other websites to social-engineer people and collect data.

Our investigation identified customers in Israel, Serbia, Colombia, Kenya, Morocco, Mexico, Jordan, Thailand, and Indonesia. Their targets included journalists and politicians around the world.

## **3. Black Cube**

### **Surveillance chain phases: Reconnaissance, Engagement, Exploitation**

We removed about 300 Facebook and Instagram accounts linked to Black Cube, an Israeli-based firm with offices in the UK, Israel and Spain. It provides surveillance services that include social engineering and intelligence gathering. Black Cube operated fictitious personas tailored for its targets: some of them posed as graduate students, NGO and human rights workers, and film and TV producers. They would then attempt to set up calls and obtain the target's personal email address, likely for later phishing attacks. Black Cube relied on different tactics to obfuscate its activity, including by performing unrelated activities, likely to drown out malicious targeting in the "noise" of the seemingly innocuous social media behavior.



Our investigation found a wide range of customers, including private individuals, businesses, and law firms around the world. Targeting by Black Cube on behalf of its customers was also widespread geographically and across industries, including the medical, mining, minerals and energy industries. It also included NGOs in Africa, Eastern Europe, and South America, as well as Palestinian activists. They also targeted people in Russia associated with universities, the telecom, high tech, consulting, legal, and financial industries, real estate development and media.

## 4. Bluehawk CI

### Surveillance chain phases: Reconnaissance, Engagement, Exploitation

We removed about 100 Facebook accounts linked to Bluehawk, a firm based in Israel with offices in the UK and the US. We collaborated on this investigation with [The Daily Beast](#) who had identified a subset of this activity leading us to uncover the full cluster and who's behind it earlier this year. Bluehawk sells a wide range of surveillance-for-hire activities that included social engineering, gathering of litigation-related intelligence about people, and managing fake accounts to trick them into installing malware. The individuals behind this firm showed persistence and continued to try to come back to our platform after we took down dozens of their accounts.

These fake accounts posed as journalists working for existing media organizations like La Stampa in Italy and Fox News in the US to trick their targets into giving an on-camera interview. As reported by The Daily Beast, some of these accounts targeted opponents of the UAE emirate Ras Al Khaimah, while others attempted to social-engineer people in Qatar and politicians and businessmen in the Middle East. Most recently, Bluehawk attempted to create accounts claiming to be based in Argentina.

## 5. BellTroX

### Surveillance chain phases: Reconnaissance, Engagement, Exploitation

We removed about 400 Facebook accounts, the vast majority of which were inactive for years, linked to BellTroX and used for reconnaissance, social engineering and to send malicious links. BellTroX is based in India and sells what's known as "hacking for hire" services, which were

reported on by [researchers](#) at the Citizen Lab and [Reuters](#). Its activity on our platform was limited and sporadic between 2013 to 2019, after which it paused. BellTroX operated fake accounts to impersonate a politician and pose as journalists and environmental activists in an attempt to social-engineer its targets to solicit information including their email addresses, likely for phishing attacks at a later stage.

This activity, based on the exact same playbook, re-started in 2021 with a small number of accounts impersonating journalists and media personalities to send phishing links and solicit the targets' email addresses. Among those targeted were lawyers, doctors, activists, and members of the clergy in countries including Australia, Angola, Saudi Arabia, and Iceland.

## 6. Cytrox

### Surveillance chain phases: primarily Exploitation

We removed about 300 accounts on Facebook and Instagram linked to Cytrox. This North Macedonian company develops exploits and sells surveillance tools and malware that enable its clients to compromise iOS and Android devices. In collaboration with the [Citizen Lab](#), we obtained copies of iOS and Android malware for further analysis. As a result, our team at Meta was able to find a vast domain infrastructure that we believe Cytrox used to spoof legitimate news entities in the countries of their interest and mimic legitimate URL-shortening and social media services (see the full domain list in the Appendix). They used these domains as part of their phishing and compromise campaigns. Cytrox and its customers took steps to tailor their attacks for particular targets by only infecting people with malware when they passed certain technical checks, including IP address and device type. If the checks failed, people could be redirected to legitimate news or other websites.

Our investigation identified customers in Egypt, Armenia, Greece, Saudi Arabia, Oman, Colombia, Côte d'Ivoire, Vietnam, the Philippines, and Germany. Targets of Cytrox and its customers included politicians and journalists around the world, including in Egypt and Armenia. Our findings suggest that Cytrox likely provided services to another threat actor known in the security community as [Sphinx](#), which targeted people in Egypt and its neighboring countries.

## 7. An unknown entity in China

### Surveillance chain phases: primarily Reconnaissance, Exploitation

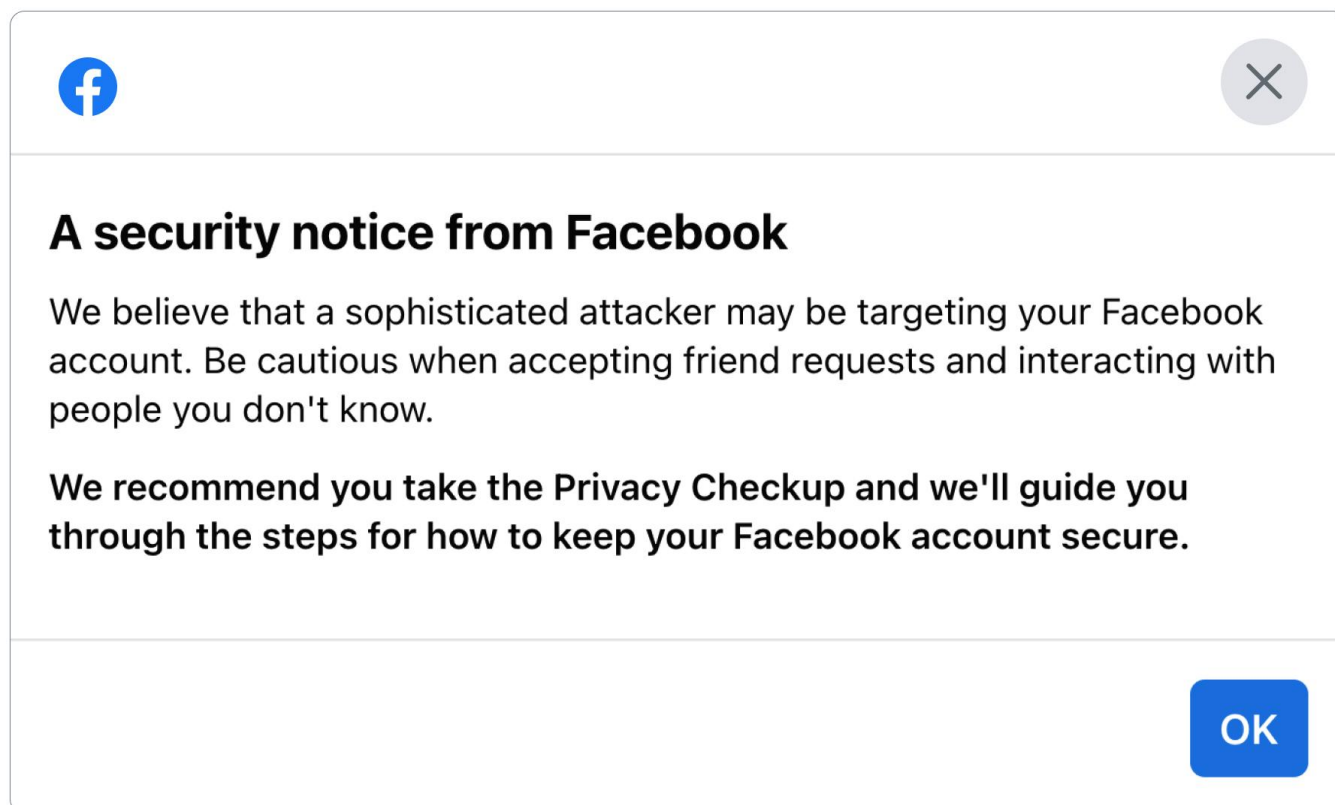
We removed about 100 Facebook and Instagram accounts linked to an unidentified entity in China responsible for developing surveillanceware for Android, iOS, Windows, and also Linux, Mac OS X, and Solaris operating systems. It also engaged in reconnaissance and social engineering activity before delivering malicious payload to its targets. While we haven't been able to attribute this activity to a particular actor, our investigation and analysis of the command-and-control servers behind this surveillance tooling indicate its usage by domestic law enforcement in China.

In some instances, we found this group's malware framework deployed along with facial recognition software developed by a Beijing-based company. At the time of our investigation, access to this framework required not only a username and password but also a SafeNet SuperDog physical hardware key, likely to make sure that only authorized customers who were given that key could use it. Analysis of the malware samples distributed by this entity provided additional insights, indicating that the people behind it were operating on a standard Monday to Friday work schedule with most software builds occurring on Mondays Beijing time.

Our investigation found that malware tools were used to support surveillance against minority groups throughout the Asia-Pacific region, including in the Xinjiang region of China, Myanmar, and Hong Kong.

## Our response to abuse by surveillance-for-hire groups

The "surveillance-for-hire" entities we removed and described in this report violated multiple Community Standards and Terms of Service. Given the severity of their violations, we have banned them from our services. We also alerted around 50,000 people who we believe were targeted by these malicious activities worldwide, using the alert system we [launched](#) in 2015. We recently updated it to provide people with more granular details about the types of targeting and the actor behind it so they can take steps to protect their accounts, depending on the phase of the surveillance attack chain we detect in each case.



The existence and proliferation of these services worldwide raises a number of important questions. While these cyber mercenaries often claim that their services and surveillanceware are meant to focus only on criminals and terrorists, our own investigation, independent [researchers](#), our [industry peers](#) and [governments](#) have [demonstrated](#) that targeting is indeed indiscriminate and includes journalists, dissidents, critics of authoritarian regimes, families of opposition and human rights activists. In fact, for platforms like ours, there is no scalable way to discern the purpose or legitimacy of such targeting. What's more, the use of these third-party services obfuscates who each end customer might be, what's collected and how the information is being used against vulnerable groups. This is why we focus on enforcing against this behavior, regardless of who's behind it or who the target might be.

To support the work of law enforcement, we already have authorized [channels](#) where government agencies can submit lawful requests for information, rather than resorting to the surveillance-for-hire industry which indiscriminately sells these services to anyone willing to pay, including known bad actors. These channels are designed to safeguard due process and we [report](#) the number and the origin of these requests publicly so that people worldwide have the full picture.

We will continue to investigate and enforce against anyone abusing our apps. However, these cyber mercenaries work across many platforms and national boundaries. Their capabilities are used by both nation-states and private enterprises, and effectively lower the barrier to entry for anyone willing to pay. For their targets, it is often impossible to know they are being surveilled across the internet.

Protecting people against this threat requires a collective effort from platforms, policymakers, and civil society to counter the underlying market and its incentive structure. We believe a public discussion about the use of surveillance-for-hire technology is urgently needed to deter the abuse of these capabilities both among those who sell them and those who buy them, anchored in the following principles:

- **Greater transparency & oversight:** There is a need for a robust international oversight that establishes transparency and “know your customer” standards for this market and holds surveillance-for-hire entities to these norms.
- **Industry collaboration:** Surveillance efforts manifest differently on various tech platforms, making industry collaboration critical if we want to fully understand and mitigate them. We stand ready to work with our peers to investigate abuse, share and disrupt surveillance-for-hire threats, including by using legal levers, so we can collectively build deterrence and impose costs on abusive services.
- **Governance & ethics:** We welcome domestic and international efforts to raise accountability through legislation, export controls and regulatory actions. We also encourage broader civil society and regulator-led conversations about the ethics of using these technologies by law enforcement and private companies, as well as creating effective victim protection regimes.

Until recently, these cyber mercenaries rarely faced consequences when their products were used to target vulnerable groups like activists, journalists, and minority groups, and cause serious harm. We’re encouraged to [see](#) our [peers](#) and [governments](#) join the effort we [began](#) in 2019 and draw attention to this threat. For our collective response against abuse to be effective, it is imperative for technology platforms, civil society and democratic governments to raise the costs on this global industry and disincentivize these abusive surveillance-for-hire services. Our hope with this threat report is to contribute to this global effort and help shine the light on this industry.

## Appendix:

### Indicators of Compromise related to Cytrox

2y4nothing[.]xyz	bit-li[.]ws	covid19masks[.]shop
5m5[.]io	bit-ly[.]link	crashonline[.]site
addons[.]news	bit-ly[.]org	cut[.]red
adibjan[.]net	bitlly[.]live	cyber[.]country
adservices[.]gr[.]com	bitlyrs[.]com	danas[.]bid
adultpcz[.]xyz	bitt[.]fi	distedc[.]com
advertsservices[.]com	bity[.]ws	download4you[.]xyz
advfb[.]xyz	bityl[.]me	dragonair[.]xyz
affise[.]app	blacktrail[.]xyz	eagerfox[.]xyz
almasryelyuom[.]com	bmw[.]gr[.]com	ebill[.]cosmote[.]center
alpineai[.]uk	bookjob[.]club	efsyn[.]online
alraeeenews[.]com	browsercheck[.]services	egyqaz[.]com
alraeesnews[.]net	bumabara[.]bid	engine[.]ninja
altsantiri[.]news	burgerprince[.]us	enigmase[.]xyz
amazing[.]lab	businessnews[.]net	enikos[.]news
ancienthistory[.]xyz	canyouc[.]xyz	ereportaz[.]news
android-apps[.]tech	carrefourmistr[.]com	espressonews[.]gr[.]com
api-apple-buy[.]com	cbbc01[.]xyz	etisalategypt[.]tech
api-telecommunication[.]c	celebrnewz[.]xyz	etisalatgreen[.]com
om	cellconn[.]net	ewish[.]cards
applepps[.]com	charmander[.]xyz	fastdownload[.]me
apps-ios[.]net	chatwithme[.]store	fastuploads[.]xyz
aramexegypt[.]com	citroen[.]gr[.]com	fbcb8213450838f7ae251d4
atheere[.]com	ckforward[.]one	519c195138[.]xyz
audit-pvv[.]com	clockupdate[.]com	ferrari[.]gr[.]com
bank-alahly[.]com	cloudstatistics[.]net	ffoxnewz[.]com
bbcsworld[.]com	cloudtimesync[.]com	fimes[.]gr[.]com
bitlinkin[.]xyz	cnn[.]gr[.]com	fireup[.]xyz
bi[.]tly[.]gr[.]com	connectivitycheck[.]live	fisherman[.]engine[.]ninja
bi[.]tly[.]link	connectivitycheck[.]online	flexipagez[.]com
bit-li[.]com	connectivitychecker[.]com	forwardeshoptt[.]com

getsignalapps[.]com	jquery-updater[.]xyz	msas[.]ws
getsignalapps[.]live	kathimerini[.]news	mycoffeeshop[.]shop
getupdatesnow[.]xyz	kinder[.]engine[.]ninja	myfcbk[.]net
goldenscent[.]net	koenigsegg[.]com	mytrips[.]quest
goldenscint[.]com	kohaicorp[.]com	myutbe[.]net
goldescent[.]com	koora-egypt[.]com	mywebsitevpstest[.]xyz
gosokm[.]com	kormoran[.]bid	nabd[.]site
guardian-tt[.]me	kranos[.]gr[.]com	nabde[.]app
guardnews[.]live	lamborghini-s[.]shop	nassosblog[.]gr[.]com
heaven[.]army	landingpg[.]xyz	nemshi-news[.]xyz
heiasjournal[.]com	landingpge[.]xyz	nemshi[.]net
hellasjournal[.]company	leanwithme[.]xyz	networkenterprise[.]net
hellasjournal[.]website	lexpress[.]me	newsbeast[.]gr[.]com
hellottec[.]art	lifestyleshops[.]net	newslive2[.]xyz
hempower[.]shop	limk[.]one	newzeto[.]xyz
hopnope[.]xyz	linkit[.]digital	newzgrou[.]xyz
icloudeu[.]com	linktothisa[.]xyz	niceonase[.]com
icloudflair[.]com	link-m[.]xyz	niceonesa[.]net
iibt[.]xyz	link-protection[.]com	nikjol[.]xyz
ikea-egypt[.]net	liponals[.]store	nissan[.]gr[.]com
ilnk[.]xyz	livingwithbadkidny[.]xyz	novosti[.]bid
in-politics[.]com	llinkedin[.]net	oilgy[.]xyz
infosms-a[.]site	Inkedin[.]org	olexegy[.]com
inservices[.]digital	localegem[.]net	olxeg[.]com
insider[.]gr[.]com	lylink[.]online	omanreal[.]net
instagam[.]click	makeitshort[.]xyz	omeega[.]xyz
instagam[.]in	mifcbook[.]link	onlineservices[.]gr[.]com
instagam[.]photos	md-news-direct[.]com	orangegypt[.]co
instegram[.]co	miniiosapps[.]xyz	orchomenos[.]news
invoker[.]icu	mitube1[.]link	otaupdatesios[.]com
ios-apps[.]store	mlinks[.]ws	paok-24[.]com
iosmnb[.]com	mobnetlink1[.]com	pastepast[.]net
itcgr[.]live	mobnetlink2[.]com	pdfviewer[.]app
itly[.]link	mobnetlink3[.]com	playestore[.]net
itter[.]me	mozillaupdate[.]xyz	pocopoc[.]xyz

politika[.]bid	speedymax[.]shop	twitter[.]net
politique-koaci[.]info	sportsnewz[.]site	ube[.]gr[.]com
prmopromo[.]com	sports-mdg[.]xyz	uberegyp[.]cn[.]com
pronews[.]gr[.]com	static-graph[.]com	updates4you[.]xyz
protothema[.]live	stonisi[.]news	updateservice[.]center
proupload[.]xyz	supportset[.]net	updatetime[.]zone
ps1link[.]xyz	suzuki[.]gr[.]com	updatingnews[.]xyz
ps2link[.]xyz	svetovid[.]bid	update[.]xyz
quickupdates[.]xyz	symoty[.]com	url-promo[.]club
qwert[.]xyz	syncservices[.]one	url-tiny[.]app
qwxzy[.]com	synctimestamp[.]com	userservicescheck[.]com
redeitt[.]com	syncupdate[.]site	userservicesforyou[.]com
safelyredirecting[.]com	telecomegy-ads[.]com	utube[.]digital
safelyredirecting[.]digital	telenorconn[.]com	viva[.]gr[.]com
sepenet[.]gr[.]com	tesla-s[.]shop	vodafoneegypt[.]tech
sephoragroup[.]com	teslal[.]shop	vodafoneegypt[.]com
servers-mobile[.]info	teslal[.]xyz	wavekli[.]xyz
serviceupdaterequest[.]com	teslali[.]com	we-site[.]net
m	tgrthsgrgwrthwrtgwr[.]xyz	weathear[.]live
sextape225[.]me	timestamps[.]com	weathernewz[.]xyz
shorten[.]fi	timeupdate[.]xyz	weathersite[.]online
shortenurls[.]me	timeupdateservice[.]com	webaffise[.]com
shortmee[.]one	tiny[.]gr[.]com	wha[.]tsapp[.]me
shortwidgets[.]com	tinylinks[.]live	worldnws[.]xyz
shortxyz[.]com	tinyulrs[.]com	wtc1111[.]com
simetricode[.]uk	tinyurl[.]cloud	wtc2222[.]com
sinai-new[.]com	tiol[.]xyz	wtc3333[.]com
sitepref[.]xyz	tly[.]gr[.]com	xf[.]actor
smsuns[.]com	tly[.]link	xnxx-hub[.]com
snapfire[.]xyz	tovima[.]live	xyvok[.]xyz
sniper[.]pet	trecv[.]xyz	yallakora-egy[.]com
solargoup[.]xyz	trecvf[.]xyz	yo[.]utube[.]digital
solargroup[.]xyz	trkc[.]online	yo[.]utube[.]to
speedy[.]sbs	tsrt[.]xyz	youarefired[.]xyz
speedygonzales[.]xyz	tw[.]itter[.]me	yout[.]ube[.]gr[.]com



youtu-be[.]net  
youtub[.]app  
youtube[.]gr[.]live  
youtube[.]voto  
youtubesyncapi[.]com  
youtubewatch[.]co  
yuom7[.]net  
z2a[.]digital  
z2adigital[.]cloud  
z2digital[.]cloud  
zougla[.]gr[.]com  
zougla[.]news