DECEMBER 2022

Threat Report on the Surveillance-for-Hire Industry

December 15, 2022

By Mike Dvilyanski, Head of Advanced Threat Investigations
Margarita Franklin, Director of Public Affairs, Security
David Agranovich, Director, Threat Disruption

Meta

TABLE OF CONTENTS

Summary

- Since publishing our first threat report a year ago, we have continued to investigate and take actions against spyware vendors around the world, including in China, Russia, Israel, the United States and India, who targeted people in about 200 countries and territories.
- Our threat research shows that the global surveillance-for-hire industry continues to grow and indiscriminately target people – including journalists, activists, litigants and political opposition – to collect intelligence, manipulate and compromise their devices and accounts across the internet.
- We disabled their accounts, blocked their infrastructure from our platform, shared our findings with security researchers, other platforms and policymakers, issued cease and desist letters demanding that they immediately stop violating activity, and also alerted people who we believe were targeted to help them strengthen the security of their accounts.

Purpose of This Report

We've been investigating and taking action against commercial spyware vendors, the so-called surveillance-for-hire industry, for years. Since publishing our first threat research about this challenge last year, we have taken down more of these entities across our technologies and worked with researchers and our industry partners to tackle this growing challenge from multiple angles.

When we uncover these entities, we take down their accounts, block their online infrastructure and share our findings with security researchers, other platforms and policymakers. We may also issue cease and desist letters demanding that they immediately stop violating activity, and, whenever appropriate, we alert people who we believe were targeted to help them strengthen the security of their accounts.

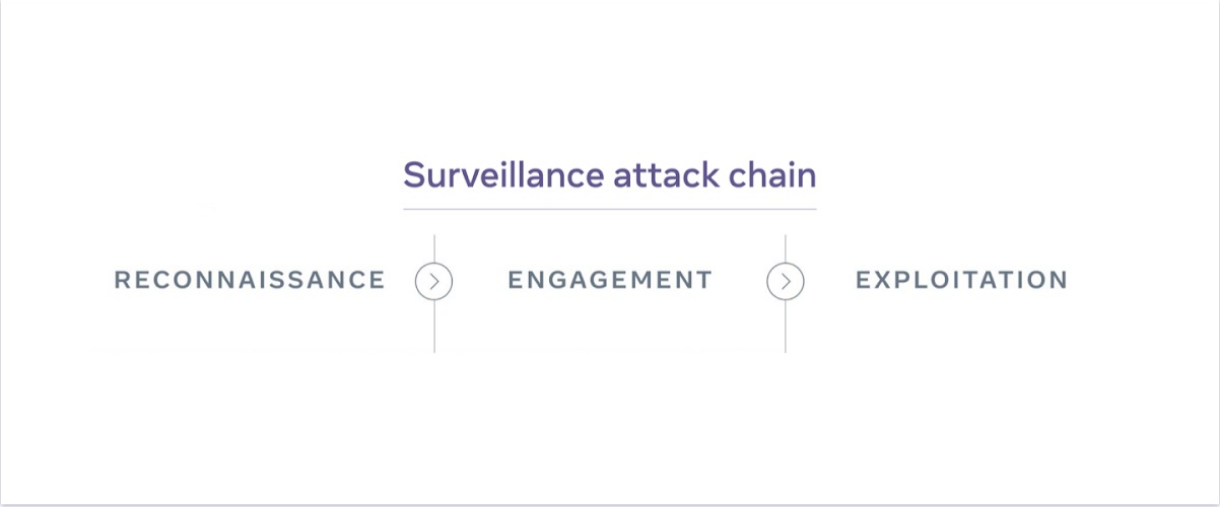
In this report, we're sharing a number of updates. First, we'll walk through the latest trends and tactics that stood out to us in our investigations this year. Second, we'll share our research into one of the entities we recently took down that originated in India and provided hacking-for-hire services to customers around the world. Finally, we'll provide a broad set of recommendations on what levers technology platforms, researchers and policymakers can use to tackle the spyware industry, based in part on the adversarial responses we've seen from the spyware providers we've taken down over the years.

Our goal is to contribute to the broader understanding of the harms that this evolving and growing threat represents to people worldwide and call on the democratic governments to take further steps to help protect internet users and impose oversight on the sellers of ubiquitous spyware.

01

Trends & Notable Tactics, Techniques and Procedures (TTPs)

This report is the result of our investigations and disruptions over the course of this year focused on activities by spyware vendors providing surveillance-for-hire services to target people across the internet, including journalists and human rights activists. In our last threat report in 2021, we described what we call the "surveillance chain" — phases of attack we've observed in our threat intelligence research: *Reconnaissance*, *Engagement* and *Exploitation*. Each phase informs the next, and while some of these entities specialize in one particular element of surveillance, others support the entire attack chain.



In addition to expected use of exploits, phishing campaigns and social engineering across the internet that are typical for the surveillance-for-hire industry, here are some notable TTPs we've observed in our latest round of investigations and disruptions in 2022:

USE OF SOCIAL MEDIA TO TEST MALICIOUS CAPABILITIES

We've seen a number of known spyware vendors use fake accounts to test malicious tooling, in an apparent attempt to validate their capabilities to compromise their own test accounts and devices, and then exfiltrate data from them.

For example, we removed a network of about 130 accounts on Facebook and Instagram linked to a known Israeli spyware developer Candiru, co-founded by a former employee of NSO Group, another surveillance-for-hire firm and added to the United States Commerce Department's Entity (trade restriction) List in November 2021. This network sent malicious links between their own fake accounts to test phishing capabilities. According to public research by the Citizen Lab, these malicious links were meant to serve the exploits to future targets and track exploited devices.

We also took down about 250 accounts on Facebook and Instagram linked to another known spyware vendor Quadream, an Israeli-based company founded by former NSO employees. This network engaged in a similar testing activity between their own fake accounts, targeting Android and iOS devices in what we assess to be an attempt to test capabilities to exfiltrate various types of data including messages, images, video and audio files, and geolocation.

In both of these cases, we detected malicious testing activities early and haven't observed targeting of authentic users.

SCRAPING

As a common tactic used as part of the *Reconnaissance phase* (and to later enable *Engagement* and *Exploitation*), we've observed companies that sell these capabilities (and their clients) using fake accounts and software tools to scrape information from social media and other public websites. This first stage of the surveillance chain is typically the least visible to the targets, who are silently profiled by spyware entities on behalf of their clients.

Firms selling these capabilities often market themselves as "web intelligence services" to enable collection, retention, analysis and searchability. In addition to obfuscating the ultimate beneficiaries of spyware services, they also significantly lower the barrier of entry for their customers.

They typically use fake accounts to search and view people's profiles and other publicly available information. They can be managed by the service provider for its clients, or operated by the customers themselves through software provided by the surveillance-for-hire firm.

We removed a number of these firms, including a New York-based company called Social Links, an Israel-based company called Cyber Globes, a Russia-based firm called Avalanche and an unattributed entity in China.

For example, we took down a network of about 230 accounts on Facebook and Instagram linked to CyberGlobes in Israel. It used a combination of fake and likely compromised accounts for targeted scraping on Facebook and Instagram. They also appear to have targeted LinkedIn, Google, Telegram and Twitter.

We also removed more than 100 accounts on Facebook and Instagram linked to Avalanche in Russia, selling access to a platform that enables reconnaissance across the internet. The platform collects data from traditional media, social media networks, and other websites on behalf of its customers inside and outside of Russia. Targeting by this network included Vietnamese activists and environmental activists, politicians, media and NGOs in the US, Nicaragua, Russia and Ukraine.

USE OF LEGITIMATE MARKETING TOOLS

We've found that spyware vendors rely on legitimate marketing tools to support malicious activity. For instance, an Indian firm called CyberRoot Risk Advisory Private, whose activity we detail in the next section, used a marketing tool called Branch to create, manage and track the delivery of phishing links, likely to obfuscate their origin and take advantage of the benefits provided by commercial marketing services. Once clicked on, these links would then redirect people to spoofed domains within this firm's large network of malicious websites. This demonstrates just how important a whole-of-society response is to tackling this growing malicious industry, including through sharing threat indicators so that we can collectively build a fuller picture of these activities across the internet.

CROSS-PLATFORM TARGETING BY THE SPYWARE INDUSTRY

In the vast majority of cases, our investigation showed these firms focus on a wide range of internet services used by their customers' targets. They typically scrape and store data from public websites like blogs, social media, knowledge management platforms like Wikipedia and Wikidata, news media, local forums and "dark web" sites.

As an example, we took down about 3,700 Facebook and Instagram accounts linked to Social Links, a web firm originally based in Moscow, Russia, and now operating in New York in the United States. These accounts were automated to continuously re-scrape Facebook and Instagram, in addition to Social Links also targeting LinkedIn, VKontakte (VK) and Twitter.

INDISCRIMINATE TARGETING OF PEOPLE

While spyware vendors often claim that their services and surveillanceware are intended to focus on criminals and terrorists, our threat research found they in fact regularly targeted

journalists, political 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. 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.

As an example, we found and took down a network of about 900 fake accounts on Instagram and Facebook operated from China. This unattributed entity relied on a wide network of proxies, likely to obfuscate its origin and made basic attempts to make their accounts appear authentic through what appeared to be automated posting and friending activity. Our investigation found this entity's scraping activity to focus on people in Myanmar, India, Taiwan, the United States, and China, including military personnel, pro-democracy activists, government employees, politicians and journalists.

PERSISTENT NATURE OF SPYWARE INDUSTRY

Like with many of the adversarial threats we tackle, spyware vendors are persistent and constantly adapt to avoid detection. In fact, part of our enforcement strategy always includes planning for these networks' attempts to come back to target our systems. Since our last report, many of the entities we removed in 2021 have tried to create new fake accounts and change their tactics, including by updating their software to evade detection and setting up new domains to circumvent our blocking of their infrastructure. We've continued to take action against these attempts.

Another way in which we've seen this threat activity persist is when a company that provides surveillance as a service gets exposed and closes down but its playbook continues to be used — sometimes after a pause — under a new name. This can be, for example, because the same people resume their activity under a new brand, or because former employees of the original spyware vendor take their skills, infrastructure and tooling to a new employer. CyberRoot, an Indian firm, is a good example of such persistence, which we detail in the next section of this report.

02

In focus: CyberRoot

We removed a network of more than 40 accounts on Facebook and Instagram operated by an Indian firm called CyberRoot Risk Advisory Private. Rather than directly sharing malware on our apps, this group's activity manifested primarily in social engineering and phishing, often intended to trick people into giving up their credentials to various online accounts across the internet (e.g. email).

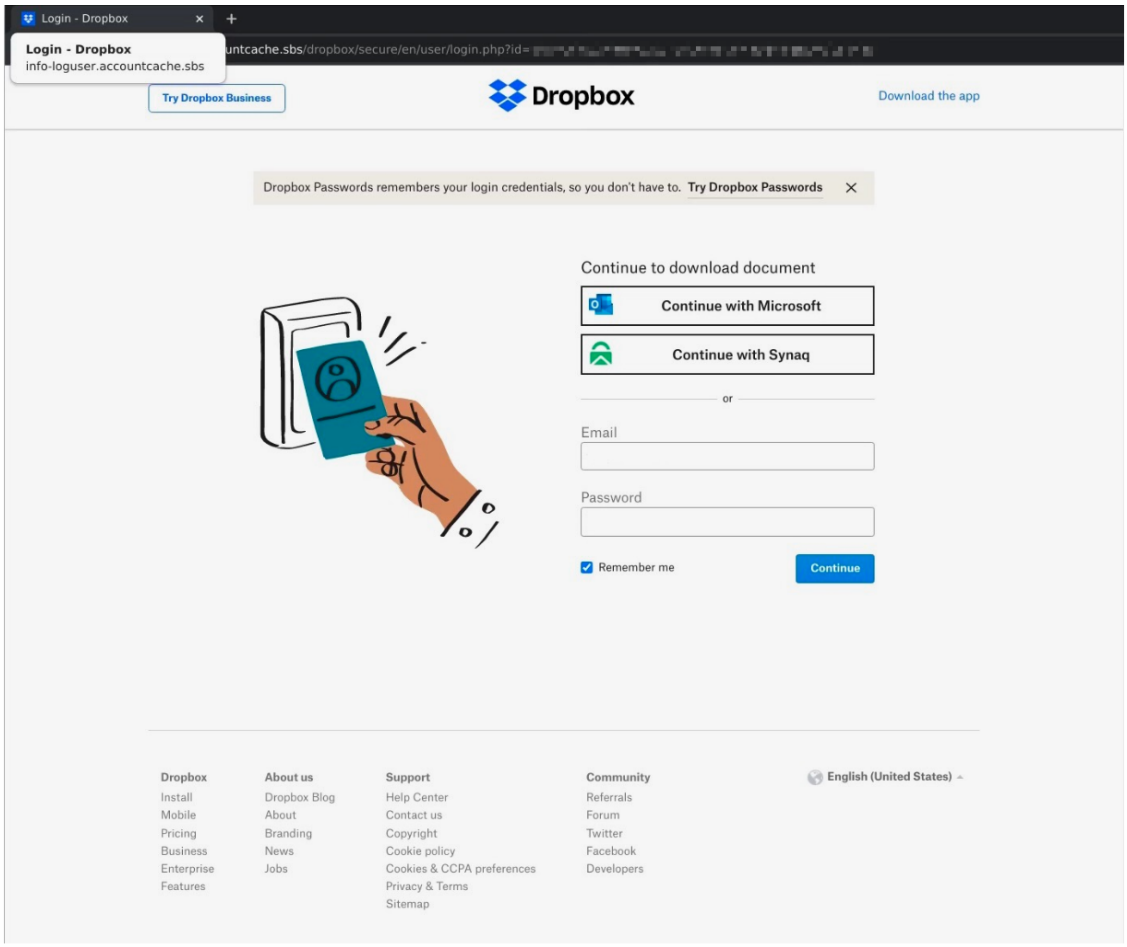
This company used a very similar playbook as another surveillance-for-hire firm we removed in 2021 named BellTroX that appears to have ceased operations on our technologies. According to public reporting, CyberRoot used to support and work with BellTroX in the past, including sharing web infrastructure and even employees.

CyberRoot used fake accounts to create fictitious personas tailored to gain trust with the people they targeted around the world. To appear more credible, these personas impersonated journalists, business executives and media personalities. In some cases, CyberRoot also created accounts that were nearly identical to accounts connected to their targets like their friends and family members, with only slightly changed usernames, likely in an attempt to trick people into engaging.

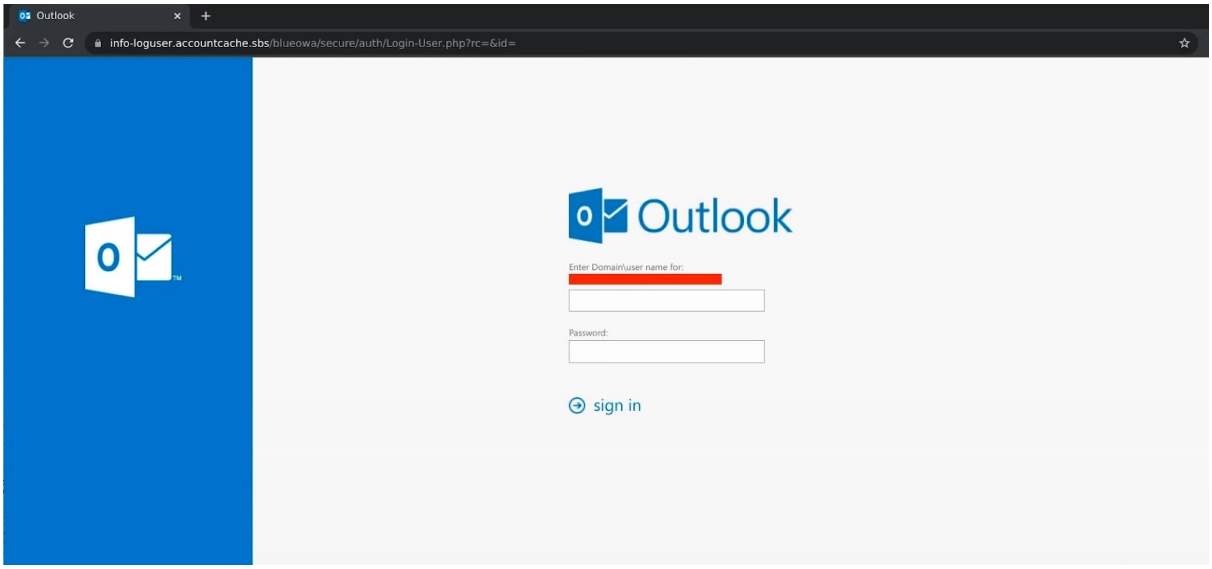
As part of their phishing campaigns, they spoofed domains of major email providers, video conferencing and file sharing tools, including Gmail, Zoom, Facebook, Dropbox, Yahoo, OneDrive and targets' corporate email servers. These domains were used for stealing login credentials to the victims' online accounts on these services.

Our investigation found CyberRoot target people around the world, working in a wide range of industries including cosmetic surgery and law firms in Australia, real-estate and investment companies in Russia, private equity firms and pharmaceutical companies in the US, environmental and anti-corruption activists in Angola, gambling entities in the UK, and mining companies in New Zealand. They were focused on business executives, lawyers, doctors, activists, journalists and members of the clergy in countries like Kazakhstan, Djibouti, Saudi Arabia, South Africa and Iceland. Our investigation corroborates the assessment by investigative journalists at Reuters that this group often targeted people involved in litigation, likely on behalf of law firms.

We blocked this group's domain infrastructure, shared our findings with our industry peers and security researchers, and are sharing threat indicators to help inform further research and detection of this malicious activity across the internet (See Appendix).



The image above is an example of a website where CyberRoot phishing campaigns would direct its targets. In this case, a phishing link contained the domain *dropbox-secure.app[.]link* that the attackers created and configured through a marketing tool called Branch to redirect targets to CyberRoot's phishing infrastructure to trick people into submitting their login credentials. As seen in the browser address bar, the actual phishing content was hosted on the attacker-controlled domain *info-loguser.accountcache[.]sbs.*



This image is another example of a CyberRoot's phishing link containing the domain *instagram-profile.app[.]link*, which only briefly presented a fake Instagram login page. However, perhaps due to a misconfiguration by the attackers, it would then quickly redirect its targets to a fake Microsoft Outlook login page instead. The login page would come with the target's pre-populated email address, likely to make it appear more legitimate.

03

How we protect against spyware

Given the global nature of this threat, no single company can tackle it alone. Similarly, no single lever — be it takedowns or litigation — can solve this threat targeting people and technologies across the world. As part of our ongoing effort to counter spyware vendors and protect people using our services, we rely on a multi-prong approach within the bounds of our platform, which we want to briefly share in this section to help broaden the discussion among different stakeholders — governments, civil society and industry — to help inform our collective defense responses. We're also sharing a more detailed policy paper with additional analysis and proposals.

Here are the levers we rely on to protect people on our apps against surveillance-for-hire activity:

- **Investigations and threat disruptions:** Our security teams identify and counter adversarial networks that seek to target people on our platform with spyware and other abusive targeting.
- **Technical safeguards against scraping and other abusive activities.** Our dedicated team of more than 100 people includes data scientists, analysts and engineers, and is focused on combating unauthorized scraping across our services, including detecting, blocking and deterring scraping.
- **Public reporting:** We publish our findings and threat indicators to enable our industry peers, researchers, governments and the public to improve our collective understanding of threat actor behavior and to raise costs on spyware vendors who seek to remain clandestine.
- **User alerts and education:** We alert people who we believe were targeted by spyware networks we take down to help them take steps to protect their accounts across our technologies. Our goal is to raise awareness about how these activities may manifest online so that people— particularly among the most targeted groups like journalists, activists, and dissidents — can change their security posture against spyware.
- **Legal action:** We've issued cease and desist letters to entities that violate our terms and policies, putting them on notice that their continued targeting of people who use our apps is not acceptable.

- **Expert briefings and testimony:** We share our analysis and findings into this constantly evolving threat to help ensure that regulation and legislation in this area is informed by expert perspectives.
- **Transparent pathways for legal requests for information by law enforcement:** We maintain authorized channels where government agencies can submit lawful requests for information, rather than resorting to the surveillance-for-hire industry that 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.
- **Cooperation with industry peers.** Where appropriate, we share information with industry peers on surveillance threats. The cross-societal nature of the problem means that no single player can solve this issue on their own, which requires stronger defenses to protect people across the internet.
- **Partnering with civil society.** We work with and welcome broader partnerships with civil society, including security and privacy researchers and digital rights scholars, on joint strategies to protect people from being targeted by spyware.

See our detailed Policy Paper for more information.

Appendix: Threat indicators

Indicators of Compromise related to CyberRoot

Phishing links used by CyberRoot

accounts.app[.]link
cigre-org.app[.]link
drop-box.app[.]link
dropbox-secure.app[.]link
facebook-official.app[.]link
goo-gle-share.app[.]link
helpsupport.app[.]link
instagram-profile.app[.]link
instgrm.app[.]link
jadroo.app[.]link
kamasutra.app[.]link
lnstagram-post.app[.]link
pethub-org.app[.]link
pixel1.app[.]link
profile-auth.app[.]link
y-mail.app[.]link

Phishing infrastructure domains controlled by CyberRoot

accountcache[.]live
accountcache[.]sbs
accountservice[.]sbs
accountservices[.]live
articleverify[.]xyz
awscloudstore[.]online
awsrequest[.]pw
cacheserice[.]pw
cacheservice[.]sbs
cacheservices[.]info
clik[.]sbs
cloudaccount[.]live
cloudsecure[.]live
driveservice[.]live
driveservice[.]online
driveshared[.]live
driveshared[.]online
fileshared[.]pw
loading[.]sbs
mailaccounts[.]co
mailservice[.]pw
mailyaaho[.]pw
mailyhaoo[.]sbs
mailyohoo[.]sbs
microservices[.]live
officalaccount[.]online
officialaccount[.]pw
passive[.]sbs
passiveverify[.]sbs
portalsecure[.]pw
portalsecure[.]pw
portalservice[.]online
portalservice[.]online
redirectserv[.]sbs
requestcache[.]pw
requestprocess[.]info
requestservice[.]live
securedrive[.]live
secureverify[.]live
servercloud[.]live
servicelink[.]sbs
servicelink[.]sbs
servicerequest[.]me
servicesverify[.]live
servicesverify[.]online
session-expired[.]online
sessionaccount[.]live
sessionexpired[.]online
sessionverify[.]live
sharedrive[.]info
sharedrive[.]pw
supportuser[.]pw
useraccount[.]pw
userprofile[.]live
userservice[.]online
webref[.]me