Shane Huntley
Senior Director, Threat Analysis Group
Alphabet

Written Testimony
United States House of Representatives Permanent Select Committee on Intelligence
Hearing Titled "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware"
July 27, 2022

Chairman Schiff, Ranking Member Turner, and esteemed Members of the Committee:

Thank you for the opportunity to appear before the Committee to discuss Google's efforts to protect users from commercial spyware. We appreciate the Committee's efforts to raise awareness about the commercial spyware industry that is thriving and growing, creating risks to Americans and Internet users across the globe.

I. Google's Efforts to Identify and Counter Spyware

A. *Our Expert Teams*

Google has been tracking the activities of commercial spyware vendors for years, and we have been taking critical steps to protect our users. We take the security of our users very seriously, and we have dedicated teams in place to protect against attacks from a wide range of sources. Our Threat Analysis Group, or TAG, is dedicated to protecting users from threats posed by state-sponsored malware attacks and other advanced persistent threats. TAG actively monitors threat actors and the evolution of their tactics and techniques. For example, TAG has been closely tracking and disrupting campaigns targeting individuals and organizations in Ukraine, and frequently publishes reports on Russian threat actors.

We use our research to continuously improve the safety and security of our products and share this intelligence with our industry peers. We also publicly release information about the operations we disrupt, which is available to our government partners and the general public. TAG tracks and proactively counters serious state-sponsored and financially motivated information cyber criminal activities, such as hacking and the use of spyware. And we don't just plug security holes – we work to eliminate entire classes of threats for consumers and businesses whose work depends on the Internet. We are joined in this effort by many other security teams at Google, including Project Zero, our team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world.

B. *Our Ongoing Work*

Google has a long track record combating commercial surveillance tools targeting our users. In 2017, Android – which is owned by Google – was the first mobile platform to warn users about NSO Group's Pegasus spyware. At the time, our Android team released research about a newly discovered family of spyware related to Pegasus that was used in a targeted attack on a small number of Android devices. We observed fewer than three dozen installs of this spyware. We remediated the compromises for these users and implemented controls to protect all Android users.

NSO Group continues to pose risks across the Internet ecosystem. In 2019, we confronted the risks posed by NSO Group again, relying upon NSO Groups's marketing information suggesting that they had a 0-day exploit for Android. Google was able to identify the vulnerability in use and fix the exploit quickly. In December 2021, we released research about novel techniques used by NSO Group to compromise iMessage users. iPhone users could be compromised by receiving a malicious iMessage text, without ever needing to click a malicious link. Short of not using a device, there is no way to prevent exploitation by a zero-click exploit; it's a weapon against which there is no defense. Based on our research and findings, we assessed this to be one of the most technically sophisticated exploits we had ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states.

Although this Committee must be concerned with the exploits of NSO Group, it is not the only entity posing risks to our users. For example, TAG discovered campaigns targeting Armenian users which utilized zero-day vulnerabilities in Chrome and Internet Explorer. We assessed that a surveillance vendor packaged and sold these technologies. Reporting by CitizenLab linked this activity to Candiru, an Israeli spyware vendor. Other reporting from Microsoft has linked this spyware to the compromise of dozens of victims, including political dissidents, human rights activists, journalists, and academics.

Most recently, we reported in May on five zero-day vulnerabilities affecting Chrome and Android which were used to compromise Android users. We assess with high confidence that commercial surveillance company Cytrox packaged these vulnerabilities, and sold the hacking software to at least eight governments. Among other targets, this spyware was used to compromise journalists and opposition politicians. Our reporting is consistent with earlier analysis produced by CitizenLab and Meta.

TAG also recently released information on a segment of attackers we call "hack-for-hire" that focuses on compromising accounts and exfiltrating data as a service. In contrast to commercial surveillance vendors, who we generally observe selling a capability for the end user to operate, hack-for-hire firms conduct attacks themselves. They target a wide range of users and opportunistically take advantage of known security flaws when undertaking their campaigns. In June, we provided examples of the hack-for-hire ecosystem from India, Russia, and the United Arab Emirates.

The growth of commercial spyware vendors and hack-for-hire groups has necessitated growth in TAG to counter these threats. Where once we only needed substreams to focus on threat actors such as China, Russia, and North Korea, TAG now has a dedicated analysis subteam dedicated to commercial vendors and operators.

II. Risks Posed by Commercial Spyware Are Increasing

Our findings underscore the extent to which commercial surveillance vendors have proliferated capabilities historically only used by governments. These vendors operate with deep technical expertise to develop and operationalize exploits. We believe its use is growing, fueled by demand from governments.

Seven of the nine zero-day vulnerabilities our Threat Analysis Group discovered in 2021 were originally developed by commercial providers and sold to and used by state-sponsored actors. TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to state-sponsored actors.

This industry appears to be thriving. In fact, there was recently a large industry conference in Europe, sponsored by many of the commercial spyware vendors we track. This trend should be concerning to the United States and all citizens. These vendors are enabling the proliferation of dangerous hacking tools, arming nation state actors that would not otherwise be able to develop these capabilities in-house. While use of surveillance technologies may be legal under national or international laws, they are found to be used by some state actors for purposes antithetical to democratic values: targeting dissidents, journalists, human rights workers, and opposition party politicians.

We have also observed proliferation risk from nation state actors attempting to gain access to the exploits of these vendors. Last year, TAG identified an ongoing campaign targeting security researchers working on vulnerability research and development at different companies and organizations. The actors behind this campaign, which we attributed to a government-backed entity based in North Korea, have employed a number of means to target researchers.

In addition to these concerns, there are other reasons why this industry presents a risk more broadly across the Internet. While vulnerability research is an important contributor to online safety when that research is used to improve the security of products, vendors stockpiling zero-day vulnerabilities in secret can pose a severe risk to the Internet when the vendor itself gets compromised. This has happened to multiple spyware vendors over the past ten years, raising the specter that their stockpiles can be released publicly without warning.

The proliferation of commercial hacking tools is a threat to national security, making the Internet less safe and undermining the trust on which a vibrant, inclusive digital society depends. This is why when Google discovers these activities, we not only take steps to protect users, but also disclose that information publicly to raise awareness and help the entire ecosystem, in line with our historical commitment to openness and democratic values.

III. Google's Work To Protect Users

Across all Google products, we incorporate industry-leading security features and protections to keep our users safe. On Search, Google's Safe Browsing is an industry-leading service to identify unsafe websites across the web and notify users and website owners of potential harm. Google Safe Browsing helps protect over four billion devices every day by showing warnings to users when they attempt to navigate to unsafe sites or download harmful files. Safe Browsing also notifies webmasters when their websites are compromised by malicious actors and helps them diagnose and resolve the problem so that their visitors stay safer.

On Gmail, we recommend certain Gmail security precautions to prevent spoofing, phishing, and spam. Spoofers may send forged messages using an organization's real name or domain to subvert authentication measures. We use email authentication to protect against email spoofing, which is when email content is changed to make the message appear from someone or somewhere other than the actual source. And we offer other advanced phishing and malware protection to administrators to better protect their users. By default, Gmail displays warnings and moves untrustworthy emails to the user's spam folder. However administrators can also use advanced security settings to enhance their users' protection against suspicious attachments and scripts from untrusted senders.

For Android, through its entire development lifecycle, we subject the products to a rigorous security program. The Android security process begins early in the development lifecycle, and each major feature of the platform is reviewed by engineering and security resources. We ensure appropriate controls are built into the architecture of the system. During the development stage, Android-created and open source components are subject to vigorous security reviews For users, Android provides safety and control over how apps and third parties can access the data from their devices. For example, users are provided visibility into the permissions requested by each app, and they are able to control those permissions.

We have also built additional tools to prevent successful attacks on devices that run Android once those devices are in users' hands. For example, Google Play Protect, our built-in malware protection for Android, continuously scans devices for potentially harmful applications.

Although our security precautions are robust, security issues can still occur, which is why we created a comprehensive security response process to respond to incidents. Google manages a vulnerability rewards program (VRP), rewarding researchers millions of dollars for their contributions in securing our devices and platforms. We also provide research grants to security researchers to help fund and support the research community. This is all part of a larger strategy to keep Google products and users, as well as the Internet at large more secure. Project Zero is also a critical component of this strategy, pushing transparency and more timely patching of vulnerabilities.

Finally, we also offer the leading tools to protect important civil society actors such as journalists, human rights workers, opposition party politicians, and campaign organizations – in other words, the users who are frequently targeted by surveillance tools. Google developed Project Shield, a free protection against distributed denial of service (DDoS) attacks, to protect news media and human rights organization websites. We recently expanded eligibility to protect Ukraine government organizations, and we are currently protecting over 200 Ukraine websites today. To protect high risk user accounts, we offer the Advanced Protection Program (APP), which is our highest form of account security. APP has a strong track record protecting users – since the program's inception, there are no documented cases of an account compromise via phishing.

IV. Whole of Society Response Necessary to Tackle Spyware

We believe it is time for government, industry and civil society to come together to change the incentive structure which has allowed these technologies to spread in secret. The first step is to understand the scope of the problem. We appreciate the Committee's focus on this issue, and recommend the U.S. Intelligence Community prioritize identifying and analyzing threats from foreign commercial spyware providers as being on par with other major advanced threat actors. The U.S. should also consider ways to foster greater transparency in the marketplace, including setting heightened transparency requirements for the domestic surveillance industry. The U.S. could also set an example to other governments by reviewing and disclosing its own historical use of these tools.

We welcome recent steps taken by the government in applying sanctions to the NSO Group and Candiru, and we believe other governments should consider expanding these restrictions. Additionally, the U.S. government should consider a full ban on Federal procurement of commercial spyware technologies and contemplate imposing further sanctions to limit spyware vendors' ability to operate in the U.S. and receive U.S. investment. The harms from this industry are amply evident by this point, and we believe they outweigh any benefit to continued use.

Finally, we urge the United States to lead a diplomatic effort to work with the governments of the countries who harbor problematic vendors, as well as those who employ these tools, to build support for measures that limit harms caused by this industry. Any one government's ability to meaningfully impact this market is limited; only through a concerted international effort can this serious risk to online safety be mitigated.

Google is investing heavily as a company and as an industry to counter serious threats to our users. In the modern world, we must be able to trust the devices we use every day and ensure that foreign adversaries do not have access to sophisticated exploits. While we continue to fight these threats on a technical level, the providers of these capabilities operate openly in democratic countries. Google is committed to leading the industry in detecting and disrupting these threats.

I thank the Committee for this attention on this critical issue.