Opening Statement
Shane Huntley

Oct 26, 2022

Chairman Lenaers, and esteemed Members of the Committee:

Good morning, my name is Shane Huntley and I am the director of Google's Threat Analysis Group or TAG . TAG is the team inside Google that analyzes and counters serious threats to Google and our users including government backed attackers, serious cybercriminal enterprises and information operations. TAG is only one part of Google's large investment in making the internet more secure. We work with many other teams within the company, including Project Zero.

Thank you very much for inviting me to appear before you today. I appreciate this opportunity to explain to the Committee how the commercial spyware industry is unfortunately thriving, creating risks to Europeans and Internet users across the globe.

The business model of commercial spyware vendors is to make money by providing comprehensive and sophisticated cyber espionage capabilities to foreign governments including both the exploits to gain control of a device and the spyware software itself which can collect all kinds of personal information.

While these vendors claim to vet their customers and usage carefully and with the promise that their work is used to target criminals and terrorists what we have observed is consistent with others' reporting, that again and again these tools are found to be used by governments for purposes antithetical to democratic values: targeting dissidents, journalists, human rights workers and political opponents.

NSO Group is the most prominent actor offering commercial spyware often delivered via sophisticated exploits, and with others we have been working for years to counter this threat and mitigate their damage.

In 2017, Google's Android was the first mobile platform to warn users about NSO Group's Pegasus spyware. At the time, our Android team released research about this spyware that was used in a targeted attack on a small number of Android devices. We notified the users, remediated the compromises and implemented controls to protect all Android users. In 2019 we quickly fixed a vulnerability in Android discovered by examining some leaked marketing information from NSO.

In December 2021 our Project Zero team published research about novel techniques used by NSO Group to compromise iMessage users. This was a zero-click exploit, meaning iPhone users could be compromised by receiving a malicious iMessage text, without ever needing to click a malicious link. We assessed this to be one of the most technically sophisticated exploits we had ever seen.

NSO is not the only actor in this space. TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors. We have publicly taken action to discover and counter exploits and malware produced by Equus, Cytrox, Candiru and RCS Labs and countering these threat actors is becoming a bigger part of our work. In 2021, we identified nine zero-day vulnerabilities used by government actors, and seven of them were originally developed by commercial surveillance vendors.

The proliferation of commercial hacking tools is making the Internet less safe and threatening our digital society and national security.

That's why Google is working collaboratively with civil society groups like the University of Toronto's Citizen Lab and industry peers at companies like Apple to counter threat actors through actions like working to patch vulnerabilities and proactively warning users about attempts to infiltrate their accounts.

"We're also active in this debate in Europe. Only yesterday, our President of Global Affairs and Chief Legal Officer Kent Walker was in Brussels where he discussed these issues with chair Lenaers, commissioner Jourova (pronounced Your-ova) and civil society representatives

XXX

In addition to our direct work to counter these threats, we also work to develop and deploy industry-leading security features and protections to protect our users across our products. This includes specific programs targeted for high risk users and sites such as the Advanced Protection Program and Project Shield which is defending the sites of over 200 news and humanitarian organisations in Ukraine from online attacks . Our EU policy team is at your disposal if you wish to learn more about any of those initiatives.

We appreciate the Committee's focus on this issue, and welcome EU efforts to counter threats from foreign commercial spyware.

We also urge the European Union to lead a diplomatic effort to work with the governments of the countries who harbor problematic vendors, and those who employ these tools, to build support for measures that limit harms caused by this industry. While we continue to fight these threats on a technical level, the providers of these capabilities operate openly in democratic countries.

Thank you for convening this important hearing. Google is committed to leading the industry in detecting and disrupting the threats posed by commercial spyware, and I look forward to answering the Committee's questions.
