Amnesty International uncovers new hacking campaign linked to mercenary spyware company

6-7 minutes ⋮ 3/29/2023

A sophisticated hacking campaign by a mercenary spyware company targeting Google's Android operating system has been exposed by Amnesty International's Security Lab.

The technical findings were shared with Google's Threat Analysis Group, which focuses on countering government-backed cyberattacks. As a result, Google along with other affected vendors, including Samsung, were able to release security updates protecting billions of Android, Chrome and Linux users from the exploit techniques used in this attack.

Amnesty International is not naming the company while the Security Lab continues to track and investigate its activity. However, the attack showed all the hallmarks of an advanced spyware campaign developed by a commercial cyber-surveillance company and sold to governments hackers to carry out targeted spyware attacks.

> "While it is vital such vulnerabilities are fixed, this is merely a sticking plaster to a global spyware crisis."
>
> *Donncha Ó Cearbhaill, Head of Security Lab, Amnesty International*

"Unscrupulous spyware companies pose a real danger to the privacy and security of everyone. We urge people to ensure they have the latest security updates on their devices," said Donncha Ó Cearbhaill, Head of Amnesty International's Security Lab.

"While it is vital such vulnerabilities are fixed, this is merely a sticking plaster to a global spyware crisis. We urgently need a global moratorium on the sale, transfer, and use of spyware until robust human rights regulatory safeguards are in place, otherwise sophisticated cyberattacks will continue to be used as a tool of repression against activists and journalists."

Amnesty International's Security Lab actively monitors and investigates companies and governments who proliferate and abuse cyber-surveillance technologies which pose a fundamental threat to human rights defenders, journalists, and civil society.

On Monday, in a significant step to address the spyware crisis, US President Biden signed an executive order restricting the government's of use of commercial spyware technology that poses a threat to human rights. The move sends a strong message to other governments to take similar action.

Zero-day attack

The Security Lab's findings allowed Google, in December 2022, to capture a new zero-day exploit chain used to hack Android devices. Zero-day exploits are particularly dangerous as they enable attackers to compromise even fully patched and updated phones, as the vulnerability is unknown to the developer.

The newly discovered spyware campaign has been active since at least 2020 and targeted mobile and desktop devices, including users of Google's Android operating system. The spyware and zero-day exploits were delivered from an extensive network of more than 1000 malicious domains, including domains spoofing media websites in multiple countries.

Amnesty International has published details of the domains and infrastructure it identified as associated with the attack on GitHub to aid civil society in investigating and responding to these attacks.

Google’s Threat Analysis Group found that Android users in the United Arab Emirates were targeted with one-time attack links sent over SMS which, if clicked, would install the spyware on the target’s phone. Human rights defenders in the UAE have long been victimized by spyware tools from cyber-surveillance companies such as NSO Group and Hacking Team over the past decade, including Ahmed Mansoor, who was targeted with spyware from both companies, and subsequently jailed by UAE authorities in response to his human rights work.

Amnesty International’s Security Lab identified additional activity related to this spyware campaign in Indonesia, Belarus, the UAE, and Italy. These countries likely represent only a small subset of the overall attack campaign based on the extensive nature of the wider attack infrastructure.

The Threat Analysis Group was also able to obtain the full Android spyware payload delivered by this attack campaign. The exploit chain used multiple zero-days and other recently patched vulnerabilities able to compromise a fully patched Samsung Android device. These vulnerabilities include a zero-day renderer exploit in Chrome, a sandbox escape in Chrome and a privilege escalation vulnerability in a Mali GPU Kernel Driver. The Mali GPU vulnerability had previously been patched by Arm, but the fix was not included in the latest Samsung firmware available in December 2022. The exploit chain also exploited a zero-day in the Linux kernel to gain root privileges (CVE-2023-0266) on the phone. The final vulnerability would also allow attackers to attack Linux desktop and embedded systems.

Amnesty International continues to work with a growing network of civil society partners to detect and respond to the unique cyber-surveillance threats faced by human rights defenders. This ongoing support includes the sharing of indicators of compromise, forensic methodologies, and the development of forensic tools such as the Mobile Verification Toolkit (MVT) which can be used by civil society to detect targeted spyware threats.

Numerous abuses uncovered by Amnesty International and civil society partners over the past years has shown that the spyware industry poses a critical threat to human rights defenders and civil society around the world. The systemic harms of the growing and unregulated cyber-surveillance extended far beyond the now notorious Pegasus spyware developed by NSO Group.

In the wake of the Pegasus Project, which revealed that spyware had been used to target journalists, human rights defenders and politicians around the world, there is an urgent need for an international moratorium on the development, use, transfer and sale of spyware technologies until there is a global legal framework in place to prevent these abuses and protect human rights in the digital age.