AMNESTY
INTERNATIONAL

Englisches Original: https://www.amnesty.org/en/latest/news/2023/07/spain-lack-of-cooperation-from-israel-on-pegasus-spyware-firm-highlights-impunity/

NEWS

29. März 2023

Amnesty International deckt neue Hacking-Kampagne auf, die zu gewerblicher Spionagesoftware-Firma führt

Durch Amnesty Internationals Security Lab wurde eine ausgeklügelte Hacking-Kampagne einer kommerziellen Spionagesoftwarefirma aufgedeckt, die das Google Betriebssystem Android ins Visier genommen hatte.

Die technischen Erkenntnisse teilte Amnesty International mit der Bedrohungsanalysegruppe von Google, deren Hauptaufgabe in der Bekämpfung von regierungsgestützten Cyberangriffen besteht. Daraus folgte, dass Google und andere betroffene Anbieter wie Samsung in der Lage waren, Sicherheitsupdates zu veröffentlichen, durch die Milliarden von Android-, Chrome- und Linux-Nutzer vor den Exploit-Techniken geschützt werden konnten, die für diesen Angriff eingesetzt wurden.

Solange das Security Lab die Aktivitäten der betroffenen Softwarespionage-Firma weiter nachverfolgt und untersucht, wird Amnesty International den Namen des Unternehmens nicht bekannt geben. Der Angriff weist jedoch alle typischen Kennzeichen einer erweiterten Spionage-Kampagne auf, die von einer kommerziellen Cyberüberwachungsfirma entwickelt und an von Regierungen beauftragte Hacker verkauft wurde, um gezielte Spionageangriffe durchzuführen.

Es ist zwar überaus wichtig, solche Sicherheitslücken zu schließen, doch angesichts einer globalen Spionagesoftwarekrise kann dies kaum mehr bedeuten als eine Behandlung der Symptome.

Donncha Ó Cearbhaill, Amnesty International

„Skrupellose Spionagesoftwarefirmem stellen ein echtes Risiko für die Privatsphäre und Sicherheit aller dar. Wir rufen die Menschen dringend auf, dafür Sorge zu tragen, dass sie immer die neusten Sicherheitsupdates auf ihren Geräten haben“, sagte Donncha Ó Cearbhaill, Leiterin des Security Lab von Amnesty International.

*„Es ist zwar äußerst wichtig, solche Schwachstellen zu beheben, doch angesichts einer weltweiten Spionagesoftwarekrise kann dies kaum mehr bedeuten als eine Behandlung der Symptome. Wir brauchen dringend ein weltweites Moratorium gegen den Verkauf, Transfer und Einsatz von Spionagesoftware, bis wirkungsvolle menschenrechtliche Schutzmechanismen eingerichtet sind. Andernfalls werden die hochentwickelten Cyberangriffe weiter als Repressionswerkzeug gegen Aktivist*innen und Journalist*innen zum Einsatz kommen.“*

Unternehmen und Regierungen, die Cyber-Überwachungstechnologien, die eine fundamentale Bedrohung für Menschenrechtsverteidiger*innen, Journalist*innen und für die Zivilgesellschaft darstellen, verbreiten und missbrauchen, werden proaktiv von Amnesty Internationals Security Lab beobachtet und untersucht.

Einen bedeutenden Schritt zur Bewältigung der Spionagesoftwarekrise unternahm am Montag US-Präsident Biden. Er unterzeichnete eine Präsidentenverfügung, durch die der Regierungseinsatz von kommerziellen Spionagetechnologien, die eine Bedrohung für die Menschenrechte darstellen, deutlich eingeschränkt wird. In dieser Maßnahme liegt auch die deutliche Botschaft an andere Regierungen, dass sie ähnliche Schritte ergreifen sollten.

ZERO-DAY ATTACKEN

Die Erkenntnisse des Security Lab ermöglichten Google im Dezember 2022 eine neue Zero-Day-Exploit-Kette abzufangen, die benutzt wurde, um Android -Geräte auszulesen. Zero-Day-Exploits sind besonders gefährlich. Sie versetzen den Angreifer in die Lage, selbst vollständig gepatchte und aktualisierte Telefone zu befallen, weil die Sicherheitslücke den Software-Entwicklern der Hersteller nicht bewusst ist.

Die neu entdeckte Spionagesoftware-Kampagne war schon mindestens seit dem Jahr 2020 aktiv und hatte es auf Nutzer von Mobil- und Desktopgeräten abgesehen, inklusive der Nutzer des Google Betriebssystems Android. Die Spionagesoftware und die Zero-Day-Exploits waren über ein ausgedehntes Netzwerk von mehr als 1.000 schädlichen Internetdomains verbreitet worden und hatten die Webseiten von Medienunternehmen in etlichen Ländern imitiert.

Um die Zivilgesellschaft bei der Untersuchung und Reaktion auf diese Angriffe zu unterstützen, hat Amnesty International diverse Details zu den Domains und Infrastrukturen veröffentlicht, die nachgewiesenermaßen an der Attacke auf GitHub beteiligt waren.

Google‘s Bedrohungsanalysegruppe fand heraus, dass Android-Nutzer aus den Vereinigten Arabischen Emiraten über einen Link für eine Einmal-Attacke angriffen wurden, der beim Anklicken eine Spionagesoftware auf dem Telefon der Zielperson installierte. Schon die letzten zehn Jahre über sind Menschenrechtsverteidiger in den Vereinigten Arabischen Emiraten immer wieder Spionagesoftwaretechnik von Cyber-Überwachungsfirmen wie der NSO-Gruppe und dem Hacking Team zum Opfer gefallen. Einer von ihnen war Ahmed Mansoor. Er wurde mit der Spionagesoftware dieser beiden Firmen ausspioniert und in der Folge von den Behörden der Vereinigten Arabischen Emirate wegen seiner Menschenrechtsarbeit inhaftiert.

In Zusammenhang mit dieser Spionagesoftware-Kampagne konnte Amnesty Internationals Security Lab noch weitere Aktivitäten in Indonesien, Weißrussland, den Vereinigten Arabischen Emiraten und Italien beweisen.

Angesichts der weitreichenden Natur solcher Angriffsstrukturen dürften die genannten Länder aber nur einen kleinen Ausschnitt der insgesamten Spionage-Kampagne abbilden.

Die Bedrohungsanalysegruppe konnte sich auch die gesamten Nutzungsdaten der Android-Spionagesoftware beschaffen. Die Exploit-Kette nutzte etliche unentdeckte Sicherheitslücken und andere kürzlich behobene Schwachstellen aus, durch die sie selbst vollständig gepatchte Android-Geräte von Samsung unter ihre Kontrolle bringen konnte. Zu diesen Schwachstellen zählen auch ein Zero-Day Renderer-Exploit und eine Funktion zur Beendigung einer Sandbox im Google-Browser Chrome und eine Schwachstelle in der Berechtigungserweiterung eines MALI GPU-Kerneltreibers. Die Schwachstelle des MALI-Betriebssystemkerns war zwar kurz zuvor von der Herstellerfirma Arm behoben worden, im letzten Samsung Firmware-Update vom Dezember 2022, war dieses Patch jedoch nicht enthalten. Ebenfalls über eine Zero-Day-Attacke macht sich die Exploit-Kette eine bis dahin unbekannte Sicherheitslücke des Linux-Kernels zunutze, um an privilegierte Zugangsberechtigungen (CVE-2023-0266) für das Telefon zu gelangen. Diese Schwachstelle erlaubte den Angreifern letzten Endes auch Linux-Desktopsysteme und eingebettete Linux-Systeme zu infiltrieren.

Amnesty International setzt die Zusammenarbeit mit einem stetig wachsenden Netzwerk von zivilgesellschaftlichen Partnern weiter fort, um die spezifischen Bedrohungen durch digitale Überwachungswerkzeuge, denen Menschenrechtsverteidiger*innen ausgesetzt sind, aufzudecken und darauf zu reagieren. Die kontinuierliche Unterstützung der zivilgesellschaftlichen Netzwerke durch Amnesty International umfasst auch Hinweise auf Indikatoren für einen möglichen Hacking-Befall, das Teilen von forensischen Methoden und die Entwicklung frei verfügbarer forensischer Instrumente wie das Mobile Verifizierungs-Toolkit (MVT / Mobile Verification Toolkit), mit dem die Zivilgesellschaft gezielte Spionagesoftware-Bedrohungen aufdecken kann.

Die zahlreichen missbräuchlichen Angriffe mit Überwachungssoftware, die Amnesty International und ihre zivilgesellschaftlichen Partner nachweisen konnten, zeigen, dass die Spionagesoftware-Industrie eine massive Bedrohung für Menschenrechtsverteidiger*innen und Zivilgesellschaften auf der ganzen Welt darstellen. Die systematischen Schädigungen durch die stetig anwachsende und unregulierte Cyber-Überwachung gehen weit über die jetzt dafür bekannte, von der NSO-Gruppe entwickelte PEGASUS-Spionagesoftware hinaus.

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.