V České republice je používán špionážní software Pegasus. A je používán zcela nelegálně. Důvod je prostý. Žádný z bezpečnostních sborů nemá speciální úpravu zákona, která by umožňovala jeho schválení soudem.

- Pegasus totiž umožňuje převzetí úplné kontroly nad informacemi z mobilního zařízení. Zná všechna Vaše hesla, včetně těch třeba do lékařské dokumentace, do banky, dětem na účty nebo do školních systémů.
- Zaznamenává Vaše setkání u lékaře, nebo diskusi s právníkem. Odposlechne informace obchodního tajemství, know how nebo utajované informace. Dostane se k informacím z minulosti, fotografiím, špicluje ve všech prostorách, které navštívíte, nebo kde necháte svůj telefon. Takže i třeba koupání Vašich malých dětí je součástí záznamu. Povolení soudu k použití tohoto špionážního softwaru může vydat jen soudce, který buď absolutně netuší, o co se jedná a je tak oklamán, nebo není příčetný. Instalaci softwaru dotyčný nepozná. Politici by se tak měli začít strachovat, protože jim v tomto případě žádné šifrovací aplikace nepomohou.
- Pegasus ovládá mikrofon, reproduktor i kameru ještě před zašifrováním. Jejich politické diskuse, jednání, strategie, to vše může být předmětem záznamu a následně i obchodu s informacemi.

V červenci 2021 publikovalo konsorcium (Forbidden Stories) investigativních novinářů ze 17 médií zprávu o tom, že spyware Pegasus je masově nasazován a zdaleka neslouží jen pro sledování teroristů či zločinců obecně, ale byl řadou vlád použit ke špionáži, k potlačování lidských práv a ke sledování opozičních politiků, aktivistů, novinářů, právníků či dokonce některých obětí trestných činů nebo pozůstalých po takových obětech.

Novináři získali databázi 50 tisíc telefonních čísel, u kterých bylo výrazné podezření, že byla terčem odposlechu pomocí software Pegasus. V řadě případů se podařilo potvrdit, že mobilní telefony byly skutečně infikovány tímto software. Toto zjištění vedlo Evropský parlament k zahájení vyšetřování (Polsko, Maďarsko, Řecko). Americká vláda uvalila na NSO Group sankce a zakázala americkým firmám jakoukoliv spolupráci s tímto subjektem (ačkoliv si předtím FBI Pegasus zakoupila, ale údajně nikdy nepoužila).

Francouzský prezident Macron s oblibou používal své dva iPhony pro soukromou komunikaci. Minimálně jeden z těchto telefonů byl nakažen spyware Pegasus, nasazeným na prezidenta marockou tajnou službou.

1. Před malware Pegasus neexistuje účinná obrana. V současnosti není veřejně známa jakákoliv bezpečnostní aktualizace či dodatečný software, který by s jistotou zabránil nákaze zařízení.
Amnesty International poskytuje bezplatně detekční software Mobile Verification Toolkint, který (díky způsobeným skandálům) zjevně funguje a je s určitou mírou pravděpodobnosti schopen detekovat Pegasus a dalších cca 140 různých typů útočného malware. Avšak je to pouze obrana ex post.

2. Kromě software Pegasus a NSO Group jsou na trhu i další obdobné produkty, o kterých je přitom k dispozici jen minimum informací. Jde například o spyware Predator, který je firmou Cytrox vyvíjen v Severní Makedonii, a dle magazínu CHIP jej používá i Spolkový kriminální úřad. Dalším produktem je italský Hermit, vyvíjený firmou RCS Lab.

3. Právní úprava odposlechu je např. v našem trestním řádu zcela zastaralá, a vůbec nekoresponduje se současnými technologickými možnostmi a realitou. § 88 trestního řádu upravuje pouze klasický odposlech telekomunikačního provozu. § 158d odst. 3 upravuje „skrytou prohlídku“, tedy utajený zásah policie do nedotknutelnosti obydlí, do listovního tajemství či zjištění obsahu záznamů, uchovávaných v soukromí pomocí technických prostředků. Ani jedno z těchto ustanovení nepočítá s totálním sledováním člověka pomocí spyware jako je Pegasus.

4. Ačkoliv je tvrzeno, že nasazení spyware Pegasus má sloužit pro prosazování práva, je důkazní použitelnost čehokoliv získaného pomocí tohoto software sporná, možná žádná. Je tomu tak proto, že tento spyware zcela ovládne vaše zařízení, a reálně umožňuje cokoliv ve vašich dokumentech nepozorovaně upravit, vložit tam zcela nový soubor atd. Kvalifikovaný advokát bude schopen před soudem úspěšně napadnout použitelnost čehokoliv, co bylo získáno těmito prostředky.

5. Hrozba ztráty státního monopolu na odposlechy. Pegasus je jen software, k odposlechu náhle není zapotřebí infrastruktura státu či telekomunikačního operátora.Odposlech je zde realizován ve spolupráci se zahraniční softwarovou firmou.

6. Hrozba ztráty možnosti reálné kontroly bezpečnostních složek. Je zcela představitelná situace, kdy bezpečnostní složka bude kontrolnímu orgánu tvrdit, že Pegasus ani nevlastní, natož aby jej použila, a přitom si jeho použití dohodne s jinou, třeba i zahraniční bezpečnostní složkou.

7. Hrozba úniku do soukromého sektoru. Jak jsem výše popsali, již produkty italské firmy Hacking Team byly používány některý bankami. Pegasus je nasazován v daleko širším měřítku i v řadě zemí, které zcela jistě tento kybernetický odposlech outsourcovaly na soukromé subjekty z důvodu nedostatku vlastních odborníků. Jde jen o „software“, takže možnost odcizení, zkopírování atd. je reálně možná.

Následující informace vychází z přednášky odborníka bezpečnostní laboratoře Amnesty International Etienne Mayniera, kterou prezentoval v červnu 2022 na bezpečnostní konferenci v Rennes.

- Poslední identifikované vzorky kódu spyware Pegasus pocházejí z roku 2016 (iOS) a 2017 (Android). Následně firma NSO Group s cílem zabránit odhalení spyware Pegasus změnila způsob jeho instalace na napadené zařízení. Pegasus monitoruje stav mobilního telefonu, a jakmile ztratí spojení s řídícími servery, nebo detekuje pokus o jailbreak, sám se odinstaluje. Stejně tak po uskutečněném odposlechu je spyware odinstalován tak, aby po sobě nezanechal stopy vlastního kódu. Pro klasické antivirové firmy tak není detekovatelný, protože není k dispozici aktuální vzorek.
- Do roku 2019 Pegasus spoléhal na infekci pomocí odkazů v SMS. Následně však došlo k výraznému rozšíření vektorů útoku, které jsou založeny na zranitelnosti některých aplikací – např. WhatsApp, iMessage, Apple Photo, Apple Music a dalších. Sledovaná osoba tak již nemusí pro nákazu zařízení kliknout na jakýkoliv odkaz, k nakažení telefonu dojde zcela automaticky bez možnosti obrany.
- **Pegasus zřejmě „nepřežije“ ani restart telefonu, ale opětovná nákaza je tak snadná, že je sledování stále možné, a naopak riziko odhalení je o to nižší.**
- **V Maroku Amnesty International zaznamenala dva případy, ze kterých vyplývá podezření, že k nákaze telefonu může dojít i použitím „falešné“ mobilní buňky, tzv. IMSI Catcher, v ČR známý pod názvem Agáta. K nákaze telefonu tak postačí pouze to, že se tento připojí do mobilní sítě.**

Česká republika není uvedena na seznamu zemí, ve kterých byl Pegasus prokazatelně používán. Avšak v prosinci 2021, tedy již po propuknutí skandálu Pegasus, byla firma NSO Group hlavním sponzorem bezpečnostní konference ISS World Europe v Praze.
Je tak zjevné, že české bezpečnostní složky mají vazby na NSO Group a je otázkou, co vše zde bylo v zákulisí konference dojednáno a zobchodováno.