ALISON

Aj ten najlepšie zabezpečený mobil vedia hacknúť muži zákona. Takto.

- Čo všetko sa dá stiahnuť z vášho mobilu
- Forenzné nástroje novej generácie
- Európa nespí
- Digitálna stopa je užitočná z rôznych dôvodov

Klub naivných používateľov

Odtlačky prstov, rozpoznávanie tváre či šifrovanie. To všetko sú pomerne známe spôsoby na zabezpečenie ochrany mobilných zariadení a najmä informácií v nich. Všetci sa spoliehame na spoľahlivosť a maximálnu odolnosť týchto bezpečnostných prvkov. A nespoliehame sa na to len my, bežní smrteľníci, ale aj osoby s kriminálnym pozadím. Avšak podľa najnovších zistení to nemusí byť tak celkom pravda a ani oni si nemusia byť ich bezpečnosťou úplne istí.

Najnovšia správa výskumnej neziskovej organizácie *Upturn* sa sústredila na analýzu prostredia v Spojených štátoch a priniesla fascinujúce správy z prostredia forenzných špecialistov. Odhaľuje, ako americká polícia získava prístup k údajom z mobilných telefónov podozrivých osôb.

Okno do duše

Muži zákona za oceánom to riešili pomerne jednoducho – obrátili sa na digitálne forenzné firmy špecializované na získavanie prístupu k šifrovaným dátam a k ich následnému sťahovaniu. Autori správy tvrdia, že vo všetkých 50 štátoch uzavreli zmluvy s dodávateľmi ako napríklad *Cellebrite a AccessData,* ktoré im umožnia prístup a kopírovanie údajov z uzamknutých telefónov.

Výkonná technológia umožňuje polícii získať kompletné kópie údajov z mobilného telefónu – všetky e-maily, texty, fotografie, informácie o polohe, údaje z aplikácií a ďalšie. Následne ich môžu extrahovať, analyzovať a použiť. Vzhľadom na množstvo citlivých informácií uložených v dnešných smartfónoch jeden z autorov odbornej štúdie hovorí, že tieto nástroje poskytujú „okno do duše“. A to naozaj v tomto prípade nie je nič poetické.

Miliónové investície

V inventári orgánov činných v trestnom konaní v USA pribudli forenzné nástroje pre mobilné zariadenia (*MDFTs – Mobile device forensic tools*) v hodnote desiatok miliónov amerických dolárov.

Forenzné nástroje pre mobilné zariadenia majú tri kľúčové vlastnosti:

- umožňujú extrakciu veľkého množstva informácií z mobilných telefónov,
- organizujú extrahované údaje v ľahko navigovateľnom formáte, aby mohli byť efektívnejšie analyzované a preskúmané,

- pomáhajú obchádzať väčšinu bezpečnostných prvkov s cieľom kopírovať údaje.

Organizácia Upturn odhaduje, že v rokoch 2015 až 2019 použila americká polícia forenzné nástroje mobilných zariadení pri vyšetrovaní takmer 50-tisíc prípadov. Autori správy tvrdia, že nástroje poskytujú informácie o životoch ľudí ďaleko nad rámec akéhokoľvek vyšetrovania a len málo policajných oddelení obmedzuje spôsob a čas ich použitia.

Európa hľadá riešenia

Aj zločin podlieha globalizácii a Európska únia je nútená zdieľať skúsenosti, zjednotiť sily a v neposlednom rade aj rozpočty, ktoré v prípade kybernetickej bezpečnosti stále rastú.

Mobilné telefóny sú pre orgány na presadzovanie zákona jedinečnou výzvou, pretože:

- 85 percent vyšetrovania trestných činov predstavujú mobilné dáta,
- 65 percent občanov EÚ uprednostňuje prístup k internetu pomocou smartfónov (2017),
- 85 percent všetkých fotografií nasnímaných v EÚ je fotených smartfónmi (2017).

Mobilné telefóny sa v porovnaní s inými zariadeniami analyzujú odlišne, čo znamená, že vyšetrovanie si vyžaduje samostatný forenzný proces. A práve to bol dôvod na spustenie projektu FORMOBILE v máji 2019.

FORMOBILE je projekt EÚ pozostávajúci z devätnástich európskych organizácií, ktorý sa zameriava na vytvorenie komplexného reťazca mobilného forenzného vyšetrovania určeného na zlepšenie digitálnej bezpečnosti a ochrany v EÚ.

Práce na projekte financovanom Európskou komisiou majú trvať tri roky a cieľom je vyvíjať nové nástroje a technológie na získavanie mobilných dát, vyvíjať nové štandardy forenznej vedy a vytvárať programy školení pre nové štandardy.

Digitálna stopa si vás aj tak nájde

V minulosti by sme za stopu považovali odtlačok topánky na zemi alebo všetkým dobre známe odtlačky prstov. Dnes je už všetkým používateľom internetu a mobilných zariadení jasné, že stopy, ktoré za sebou zanechávame v digitálnom svete sú úplne iné.

Áno, v danom prípade hovoríme o tzv. digitálnych stopách. Jednoducho povedané, sú to všetky dáta, údaje či informácie, ktoré za sebou zanechávame pri používaní internetu a mobilných aplikácií. A využití digitálnych stôp je hneď niekoľko.

Digitálna stopa pomáha napríklad v cielení reklamy na potenciálnych zákazníkov, a je teda skvelým nástrojom marketingu. Bohužiaľ sa mnoho ráz stáva aj nástrojom na sledovanie osôb. Ruku na srdce, kto si na internete neskúšal nájsť aspoň základné informácie o známych osobnostiach. A v

neposlednom rade sa digitálna stopa stáva dôkazovým materiálom pri riešení prípadov trestnej činnosti. Mobilné zariadenie je vaším majetkom, ale dôkazový materiál v ňom už tak úplne nie.

Zdroje

https://www.wired.com/story/how-police-crack-locked-phones-extract-information/

https://www.upturn.org/reports/2020/mass-extraction/

https://formobile-project.eu/project#.objectives_scroll