Hakiranje pomoću umjetne inteligencije

Ovog smo mjeseca ponovo dočekali da trinaesti dan u mjesecu pada u petak. Nije se dogodilo ništa spektakularno, nebo nam se nije sručilo na glavu, ali taj nas datum može potaknuti, makar i ne bili praznovjerni, da se poigramo traženjem rizika koji bi nas mogli izložiti nezgodama na neki drugi datum. Naravno, ovdje nas najviše zanimaju nove tehnologije i načini na koje one obogaćuju društvo, ali istovremeno donose i nove opasnosti.

Pažnju nam je privukla vijest koju prenosi The Washington Post. Događaj je prenesen u anonimiziranom obliku, tako da ne znamo tko su stvarni sudionici. Po svemu sudeći, dogodilo se to negdje u Velikoj Britaniji, u tvrtki koju je osnovala kompanija iz Njemačke. Rukovoditelja engleske tvrtke nazvao je šef roditeljske kompanije i naložio mu da hitno izvrši prijenos 220.000 € na račun treće, neimenovane tvrtke. Kad je prijenos novca obavljen, njemački šef je ponovo nazvao i zahvalio, obećavši da će brzo nadoknaditi isplaćenu sumu. No umjesto toga nazvao je treći put i zatražio da se prebaci dodatni iznos. Kako novac nije nadoknađen, probudila se sumnja i novi transfer nije obavljen. Uskoro se pokazalo da je sve skupa bila prijevara, nalog nije stigao od stvarnog rukovoditelja, već je netko (ili nešto!) vješto imitirao njegov glas, izgovor engleskog s njemačkim akcentom, boju glasa, sve je savršeno odgovaralo. Već pogađate da se nije radilo o čovjeku imitatoru, već je glas rukovoditelja proizveo program umjetne inteligencije. I tako smo dobili novu kategoriju socijalnog inženjeringa, financijsku prijevaru, ili narodski rečeno krađu, koja je izvedena na daljinu, krađom identiteta uz pomoć AI. Pokušaj vraćanja novca nije uspio, jer je već prebačen preko nekoliko računa i izgubio se u bespućima bankarske mreže, završivši u mraku u nekoj poreznoj oazi.

Pisali smo već o tome kako se umjetna inteligencija koristi za stvaranje lažnih video i audio snimaka kojima se može izazvati komične efekte ili kompromitirati neka javna osoba. U takvim se slučajevima radilo o humoru, ili o nekakvoj kampanji za pridobivanje (ne)simpatija javnosti, odnosno birača. U ovom slučaju radi se o čistom kriminalu.

Naša djeca na mobitelu koriste aplikaciju Snapchat koja svojim filterima preobličava snimljene likove i pretvara ih u karikature, likove iz crtića, na primjer zečiće s dugim ušima. Nije teško otići korak dalje, pa zamisliti kako na mobitelu imamo instaliranu AI aplikaciju koja snima glasove (i video) ljudi s kojima komuniciramo i sprema specifičnosti svakoga od njih. Kad se prikupi dovoljno podataka, s pomoću te aplikacije možemo nazivati ljude tako da iz izbornika odaberemo osobu čiji identitet želimo preuzeti. AI će tada preobličiti naš glas (a možda i izgled) u imitaciju odabrane osobe. Mogućnosti socijalnog hakiranja postaju neograničene. No osim zabave i praktičnih šala mogući su i zloslutniji scenariji, koje će kriminalni mozak već znati osmisliti prema svojim potrebama.

Takva aplikacija zasad nije u ponudi na javnom tržištu, ali čini se da je nešto nalik na to već napravljeno, možda se nudi na crnom tržištu.

Znači li to da uskoro nećemo više smjeti vjerovati u identitet sugovornika s kojim komuniciramo? Svako se uspješno društvo zasniva na povjerenju među njegovim članovima. Istovremeno u svakom društvu postoje pojedinci i grupe koji to povjerenje nastoje zloupotrijebiti. Što se toga tiče, u osnovi se ništa nije promijenilo, samo se mijenjaju načini prijevare. Ljudi nenavikli na nove tehnologije praktički se sami nude kao potencijalne žrtve. Zato je važno držati korak sa sve bržim razvojem i biti informiran istovremeno o upotrebi i zloupotrebi svake nove tehnologije.

Kako sa sve većim brojem ljudi komuniciramo preko mreže, a sve manje u četiri oka, morat ćemo usvojiti nove navike i očekivati nove vrste prijevara, kakve do sada nismo poznavali. A to se ne odnosi samo na nas korisnike, već i na društvo u cjelini. Treba pohvaliti objavu primjera neimenovane tvrtke koja je kriminalcima isplatila novac jer nisu prozreli *high tech* prijevaru . Ocijenili su da je važnije upozoriti javnost i prihvatili rizik da time ugroze image tvrtke. Nije poznato da li je to prvi slučaj takve prijevare, ili naprosto prvi koji je prijavljen. U svakom slučaju trebamo se pripremiti za nove pokušaje.

Ne znam da li je normalna praksa da se isplate obavljaju usmenim nalogom, bez papirologije? No tu se radi o privatnim tvrtkama, gdje vlasnik ima veće ovlasti. Svejedno, koliko bi teško bilo nazvati osobu koja je dala nalog i zatražiti još jednom potvrdu? Kako god bilo, bit će potrebno popraviti i sigurnost bankarskih transakcija, uključujući nove načine plaćanja. Bilo bi lijepo da možemo pratiti trag novca i zatražiti povrat prijevarom oduzetih sredstava. No porezne oaze teško ćemo iskorijeniti. Sve dok bogati i moćni imaju interes očuvati ih za svoje potrebe, njima će se koristiti i kriminalci.

Istraživači su otkrili da se može izigrati ograničenje dnevne potrošnje/podizanja gotovine na Visa

kartici. Ograničenje je oblik zaštite: ako se netko dočepa vaše kartice, neće moći potrošiti sve brzo i odjednom. Također saznajemo da lopovi hodaju po gradu noseći uređaj za očitavanje čipa na kreditnim karticama. Čuvajte svoje kartice! Jeste li već kupili RFID novčanik, koji će to spriječiti? Otključavanje automobila na daljinu je komforno, ali lopovi imaju prijemnik koji očita signal, pa mogu otvoriti automobil kad se vi udaljite. Da li vaš ključ šalje uvijek isti signal za otvaranje vrata, ili ih generira nekim algoritmom? Sumnjam da je to itko pitao prodavača automobila, a sumnjam i da oni znaju odgovor na to pitanje. Itd, its. Ukratko, sigurnost se ponekad može popraviti *low tech* metodama, kao što je RFID novčanik, ili otključavanjem automobila na starinski način.

Na blagajnama sve češće vidimo ljude koji plaćaju prislanjanjem mobitela na POS. Još nismo saznali da li su lopovi pronašli način da hakiraju i tu metodu plaćanja. Ali to je samo pitanje vremena.

Ah, da, da ne zaboravimo... Koristite li webmin, ljubazno sučelje za administriranje Linux servera? Otkriven je backdoor koji napadaču omogućava izvršavanje brojnih naredbi na serveru. Procjenjuje se da je na mreži oko milijun servera s instaliranim webminom. Provjerite da li je vaša instalacija ranjiva, pa poslušajte preporuku za prelazak na verziju 1.930. Članak s više informacija potražite na ovoj adresi. [1]

pet, 2019-09-27 14:42 - Aco Dmitrović**Kategorije:** Kolumna [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: hakiranje [3]
umjetna inteligencija [4]
krađa identiteta [5]

Source URL: https://sysportal.carnet.hr/node/1854

Links
[1] https://www.zdnet.com/article/backdoor-found-in-webmin-a-popular-web-based-utility-for-managing-unix-servers/?ftag=COS-05-10aaa0h&utm_campaign=trueAnthem%3A+Trending+Content&utm_content=5d5b706f57819f000168c60c&utm_medium=trueAnthem&utm_source=facebook&fbclid=IwAR0P9BrxyBYrcOeLpQgD-_lQWojEG8-0CFh5zCpjlNaOFvYEY2hSj82eago
[2] https://sysportal.carnet.hr/taxonomy/term/71
[3] https://sysportal.carnet.hr/taxonomy/term/333
[4] https://sysportal.carnet.hr/taxonomy/term/334
[5] https://sysportal.carnet.hr/taxonomy/term/221