Fatální: Váš mobilní telefon lze nyní „hacknout“ jediným pípnutím a vy ho neuslyšíte

infokuryr.cz/n/2023/04/13/fatalni-vas-mobilni-telefon-lze-nyni-hacknout-jedinym-pipnutim-a-vy-ho-neuslysite

kuryr 13. dubna 2023

Studie ukazuje, že asistenti od Googlu, Applu, Amazonu a Microsoftu jsou schopni přijímat příkazy přes ultrazvuk. Otvírač dveří pro kybernetické útoky všeho druhu…

Kybernetické útoky se mohou dít také prostřednictvím zvuku, ale toho byste se neměli obávat – nikdy je neuslyšíte. Výzkum profesorů počítačových věd z Texaské univerzity v San Antoniu (UTSA) a University of Colorado (UCCS) vyvinul novou metodu, jak proniknout do dalších zařízení.

Tato metoda s názvem NUIT (Nearly Inaudible Ultrasound Trojan) v podstatě spočívá ve vydávání příkazů hlasovým asistentům od Googlu, Applu, Amazonu nebo Microsoftu pomocí

ultrazvuku. Jakmile přijmou příkazy přes své mikrofony, nezbývá už nic dělat.

„Když hrajete YouTube na chytré televizi, nemá ta chytrá televize reproduktor? Zvuk škodlivých příkazů NUIT se stává neslyšitelným a může také zaútočit na váš telefon a komunikovat s vašimi zařízeními Google Assistant nebo Alexa. Může se to stát i během schůzek Zoom. Pokud někdo aktivuje svůj mikrofon, ***může vyslat útočný signál k hacknutí vašeho telefonu*** *, který je během schůzky vedle vašeho počítače,“ vysvětluje* ***Guenevere Chen*** *, profesorka z UTSA* .

Spolu s doktorandkou UTSA Qi Xia a Shouhuai Xu, lektorem UCCS, byla autorkou studie, která bude podrobně představena na letošním bezpečnostním kongresu USENIX.

Je to proto, že mikrofony zařízení mohou zachytit a reagovat na příchozí příkazy zvuky, které hraničí s ultrazvukem – **konkrétně ve frekvenčním rozsahu 16 kHz až 20 kHz** – něco, co lidské ucho nedokáže. Jak ale **mikrofony v telefonu nebo chytrém reproduktoru uslyší tento zvuk?** Výzkumníci vysvětlují, že tyto audiozáznamy by mohly být zveřejněny na jakékoli webové stránce nebo platformě, včetně YouTube, jako návnada, kterou by někdo mohl kousnout, aniž by si pasti všiml.

Uvedli, že zvuky, které používají k provádění příkazů, jsou dlouhé pouze 0,77 sekundy, což dále komplikuje jejich detekci. Jedinou nevýhodou je, že vyžaduje určitý objem, aby byl útok účinný. Pokud si však myslíte, že poznáte, že jste se stali obětí, protože slyšíte hlas asistenta reagovat na žádost, mýlíte se: příkazy mohou také obsahovat příkaz ztlumit hlas, aby oběť nevěděla, co se děje.

Doposud otestovali 17 zařízení různých značek a téměř ve všech pokusech se jim nepodařilo propašovat pomocí uživatelského rozpoznávání hlasu – nástroje, který umožňuje pouze vám nebo vaší rodině mluvit na dané zařízení. Pouze v případě Applu se jim v tom

podařilo zabránit, pokud nevytvoří umělý, lidský hlas, který je daleko složitější. Předčí však to, čeho se v roce 2017 podařilo skupině výzkumníků z univerzity Zhejiang v Číně, kteří vyvinuli podobný model, ale s řadou omezení snižujících jeho nebezpečnost.

Jak může ultrazvuk otevřít vaše dveře

Hervé Lambert, globální ředitel provozu společnosti Panda Security, zdůrazňuje, že tato technologie „představuje problém pro celý svět domácí automatizace a systémů připojených zařízení“.

„Jeden z nejničivějších scénářů je vidět v hyperpropojených městech, kde někdo může přehrávat hudbu nebo video ultrazvukem, aby dosáhl na mikrofony na ulici,“ poznamenává, než uvede další příklady, jako jsou hotely používající podobné systémy .

„Tohle je fantastický scénář pro okrádání hostů. Můžete mít dobrý systém a pak se s něčím takovým otevřou dveře. To není sci-fi, ale něco, co není příliš složité vzhledem k času a zdrojům,“ varuje.

„ ***Pokud jste trochu chytrý a chcete někomu nebo firmě ublížit,*** *můžete to udělat. Potřebujete frekvenční modulátor a musíte být schopni převést příkaz do zvuku.”*

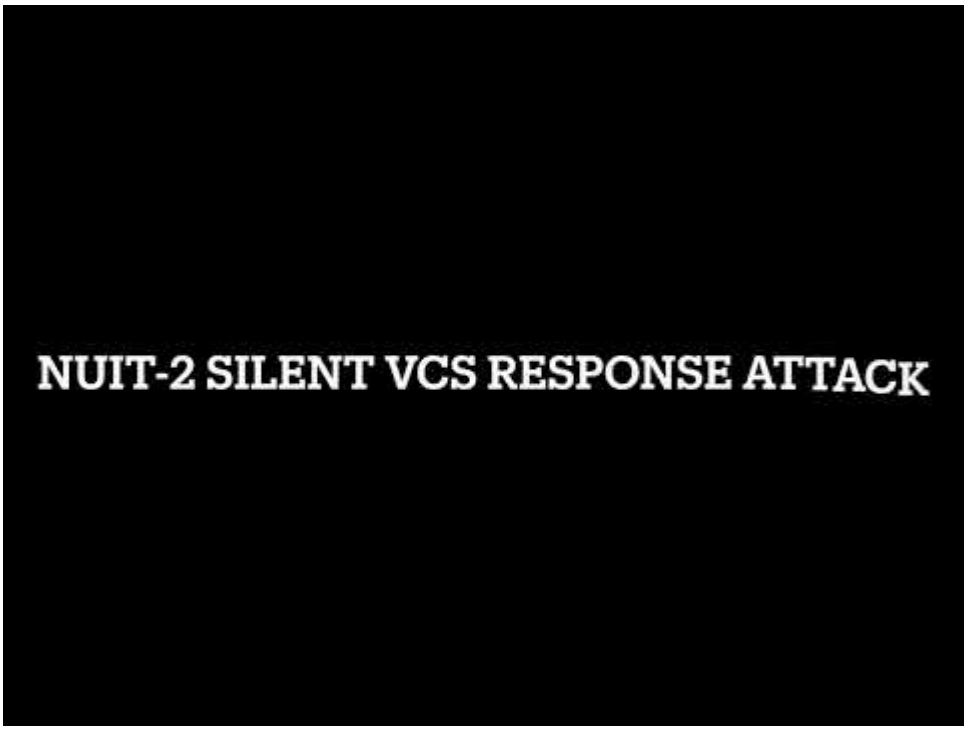
pokračuje specialista, kterého těší, že tento mechanismus byl objeven v rámci univerzitního výzkumu a není výsledkem útoku (zatím nejsou známy žádné útoky tohoto typu ze strany kyberzločinců).

Kromě případu hlášeného na čínské univerzitě nedávno proběhla studie výzkumníků z Korea University School of Cyber Security, kteří našli nástroj, který fungoval podobným způsobem, ale vyžadoval předchozí instalaci malwaru do zařízení. které využívaly ultrazvukové vlny by měly vyzařovat, což také omezovalo účinek, jak uvádí **Bleeping Computer** .

Vývojáři NUIT vyvinuli dvě varianty provádění útoků. V prvním případě je obětí útoku také zařízení přehrávající zvuk – mobilní telefon nebo reproduktor. Sami zveřejnili video, ve kterém ukazují, jak by otevřeli například zámek dveří připojených k internetu.

Watch Video At: https://youtu.be/mg0a9BoWNcQ

Druhou možností je využít zvuků počítače, reproduktoru nebo televize – abychom jmenovali jen několik příkladů – **a vtrhnout do kuchyně jiného zařízení s asistentem, jako je Siri nebo Alexa** . Tímto způsobem lze pozorovat člověka, jak hraje ultrazvuk na svém počítači, a to zase stačí k tomu, aby se malware vplížil do jeho telefonu a otevřel dveře.



Watch Video At: https://youtu.be/mFmS4vvL8ko

To jsou však pouze příklady. Jinými slovy, nejde jen o to, aby jim bylo umožněno používat vaše připojená domácí zařízení doma, ale také o **spouštění všech druhů malwaru na cíli** .

„Existuje tisíc způsobů, jak páchat zlo, protože můžete vytvářet nejrůznější příkazy k instalaci malwaru, a to včetně krádeže dat, hesel, zamykání zařízení, útoků typu denial-of-service…“ říká Lambert z Panda Security.

Autoři studie poskytují také řadu doporučení pro uživatele, která nejsou příliš dalekosáhlá, jako např. B. používání sluchátek místo reproduktorů, ale zaměřují se také přímo na průmysl.

„Nejde jen o problém se softwarem nebo malwarem. Jde o hardwarový útok přes internet. ***Slabé místo spočívá v konstrukci mikrofonu, kterou by výrobce musel opravit,“*** *pokračuje autor.*

To by zahrnovalo řešení, jako je omezení frekvencí v těchto mikrofonech. „Vše, co vyžaduje další konfiguraci, má další náklady. Bezpečnost by měla být středem pozornosti výrobců, ale

dnes si neuvědomuji, že tomu tak je, pokud nejde o citlivou infrastrukturu,“ stěžuje si Lambert.

ZDROJ