Analýza Windows 10: Ve svém principu jde o pouhý terminál na sběr informací o uživateli, jeho prstech, očích a hlasu!

Redakce přináší exkluzivní poznatky od našeho administrátora o nejnovějším operačním systému Windows 10 z dílny Microsoftu. Předpokládáme, že po přečtení článku se již budete dívat jinak na svůj počítač, a to pokaždé, když ho zapnete.

S příchodem Windows 10 jsem se rozhodl podrobit tento operační systém několika testům a s výsledky mého zkoumání bych vás nyní rád seznámil. Nasbírané poznatky mohou být pro někoho alarmující, ale přiznám se, že v době mobilních platforem, Androidu a iOS, už nijak překvapivé, alespoň pro mně. Operační systém Windows 10 je ve své podstatě více koncový terminál, než operační systém, protože mnoho procesů a funkcí tohoto systému je přímo nebo nepřímo závislých na vzdálených serverech a databázích společnosti Microsoft a Windows 10 je první operační systém od Microsoftu, který část funkcí svého rozšířeného operačního jádra umístil vzdáleně na své servery.

Co se děje pod prsty?

Windows 10 provádí kolekci všech textů zadaných z klávesnice. Texty se ukládají do dočasných souborů a 1x za 30 minut se odesílají na následující servery:

oca.telemetry.microsoft.com.nsatc.net
pre.footprintpredict.com
reports.wes.df.telemetry.microsoft.com

Přenos je šifrovaný a měl by být anonymní. Nelze však vyloučit, že přenos obsahuje anebo může volitelně obsahovat identifikátory vašeho stroje či vaší osoby. Telemetrický server sbírá informace o vaší poloze v síti, IP a geografické poloze. Footprintpredict předává vaše vstupy z klávesnice vyhledávači Bing od Microsoftu. To je chytré řešení. Pokud např. píšete do chatu o dovolené, Windows 10 pošlou vaše texty odchycené z klávesnice Bingu a vy, když druhý den přijdete na Bing, uvidíte na hlavní stránce vyhledávače nabídky na penziony a hotely na Istrii, protože včera jste na Windows 10 psali „v šifrovaném chatovacím programu“ kamarádovi, že jedete na Istrii. Takže váš „tajný“ rozhovor s kamarádem zná Bing se vším všudy. A když spolu mluvíte přes kryptovanou SIP komunikaci, hlasový port Cortana odposlechne všechno, co řeknete, ale o tom až později v tomto článku. Microsoft tak není marketingově odkázán jen na vstupy uživatele v prohlížeči Edge, ale může zachytávat textové vstupy z klávesnice v jakékoli aplikaci běžící na Windows 10. To znamená náskok před Googlem pro Microsoft.

Jistě teď tušíte, o co se jedná. I když si nainstalujete na Windows 10 šifrovací program pro komunikaci s někým po internetu, díky sběru informací z klávesnice (key logging) si může Microsoft přečíst, co jste psali. Nelze zřejmě zachytit, co vám píše druhá strana v kryptované komunikaci, ale minimálně jednostranné zachycení komunikace je velmi vážná věc.

Třetí server má opět na starosti telemetriku stroje, nové Windows 10 se chovají velmi podobně jako Android, kdy většina operací na úrovni operačního systému obsahuje telemetrické hooks, tzn. záchytné body, které se vztahují k nějaké informaci o uživateli. Pokud např. napíšu do prohlížeče Edge jakékoliv telefonní číslo, do cca. 5 minut se postupně odesílají informace o čísle na tyto telemetrické servery Microsoftu:

vortex.data.microsoft.com
vortex-win.data.microsoft.com
telecommand.telemetry.microsoft.com
telecommand.telemetry.microsoft.com.nsatc.net
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
sqm.telemetry.microsoft.com
sqm.telemetry.microsoft.com.nsatc.net

Zvláštní situace nastává, pokud kdekoliv ve Windows 10 napíšete jméno nějakého známého amerického filmu. Windows 10 začnou samy od sebe po určité chvíli hledat na vašem disku ve složce s médii soubory a indexovat je. Indexovaný soubor je poté anonymně odeslán na tyto servery zhruba do 30 minut při nečinnosti počítače, nepodařilo se mi periodu přesně zjistit:

df.telemetry.microsoft.com
reports.wes.df.telemetry.microsoft.com
cs1.wpc.v0cdn.net
vortex-sandbox.data.microsoft.com
pre.footprintpredict.com

Na české filmy to nefunguje, žádná paketová komunikace na internet při psaní českých filmů na klávesnici neproběhla. Tato vlastnost je hodně nebezpečná, protože co se stane, pokud Windows 10 v mediální složce najdou nelegálně ripnutý americký film? Pokud ho pojmenujete na disku jako „seminarka.mkv“, asi ho Windows 10 nenahlásí (Windows 10 zjevně neskenují obsah souboru, pouze ho indexují a odesílají metadata). Je možné, že jde o sběr dat pro pozdější cílené nabídky na nákupy filmů.

Čekáte na fotku do pasu? S Windows 10 ji máte u amerických úřadů zřejmě hned po zapnutí webové kamery

Po první aktivaci Windows 10 a po prvním zapnutí webové kamery se po internetu odešle zhruba 35 MB dat na tyto servery:

oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
vortex-sandbox.data.microsoft.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.net

Operace se provede pouze 1x a nepodařilo se mi ji zatím zopakovat. Je možné, že zasílání dat z web kamery probíhá v delších časových intervalech (dnů nebo týdnů). Nevím, k čemu a proč kamera po svém prvním zapnutí si sahala na internet a odesílala tolik dat. Vzhledem ke dvěma nahoře uvedeným posledním serverům se obávám, že je to nějaká „feature“ ohledně sociálních sítí, že se vaše fotka potom integruje někam, ale opravdu netuším kam a raději ani nedomýšlím. Problém pro hlubší analýzu je v tom, že všechny transfery dat na servery Microsoftu jsou kryptované a není bez nějakého hlubšího reverzního inženýrství možné zjistit, co se vlastně odesílá. Vaše fotografie z web kamery pro účely americké národní bezpečnosti asi není úplně vyloučená varianta. Docela by mně zajímalo vyjádření někoho z Microsoftu, co to má znamenat.

Úplně stejná, ne-li horší, je situace u Androidu, který si veškeré fotografie a vstupy z mobilní kamery může uchovávat na svých serverech a i když nepoužíváte cloudové úložiště Google Disk, určitě není problém na dálku z telefonu fotografie vytáhnout. Operační systém Windows je ale trochu jiná situace. Je to pracovní systém, ve firmách a v kancelářích a takovéto mohutné špehování a sběr dat může být zneužito třeba i k průmyslové špionáži USA proti zemím v Evropě a jiným krajinám.

Řekni mi, kdo jsi a já si tě zapamatuji, kdekoliv tě uslyším!

Největší problém spatřuji v hlasovém portu Windows 10, který je nově vybaven hlasovým asistentem Cortana. Systém reaguje pouze na angličtinu (zatím). Zato však naprosto hrozivě. Hlasové vzorky toho, co řeknete do hlasového portu, jsou okamžitě odesílány na tyto servery Microsoftu:

oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
vortex-sandbox.data.microsoft.com
pre.footprintpredict.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.net
telemetry.appex.bing.net
telemetry.urs.microsoft.com
cs1.wpc.v0cdn.net
statsfe1.ws.microsoft.com

Cortana odesílá data na internet, i když jí ve Windows 10 zakážete (disablujete), což je skandál, který se probírá už i zde, kde se uvádí, že zákaznická podpora Microsoftu uvedla, že i po „vypnutí“ Cortany v nastavení běží Cortana nadále v paměti, což moje analýza potvrzuje. Komunikace opravdu probíhá se servery MS stále. Toto není bug, ale feature ve Windows 10. Potvrzuje to ale mojí domněnku, že hlasový port je zcela oddělen od Cortany a hlasová analýza na Windows 10 probíhá na nižší úrovni operačního systému bez vašeho vědomí, i když Cortanu „odinstalujete“. Podle vzorků hlasu, pokud by se v dostatečném počtu a množství dostaly do rukou např. NSA, by bylo možné identifikovat osobu např. na letištích z odposlechových mikrofonů s přesností převyšující 99% nebo kdekoliv, kde byste se přiblížili k mikrofonu.

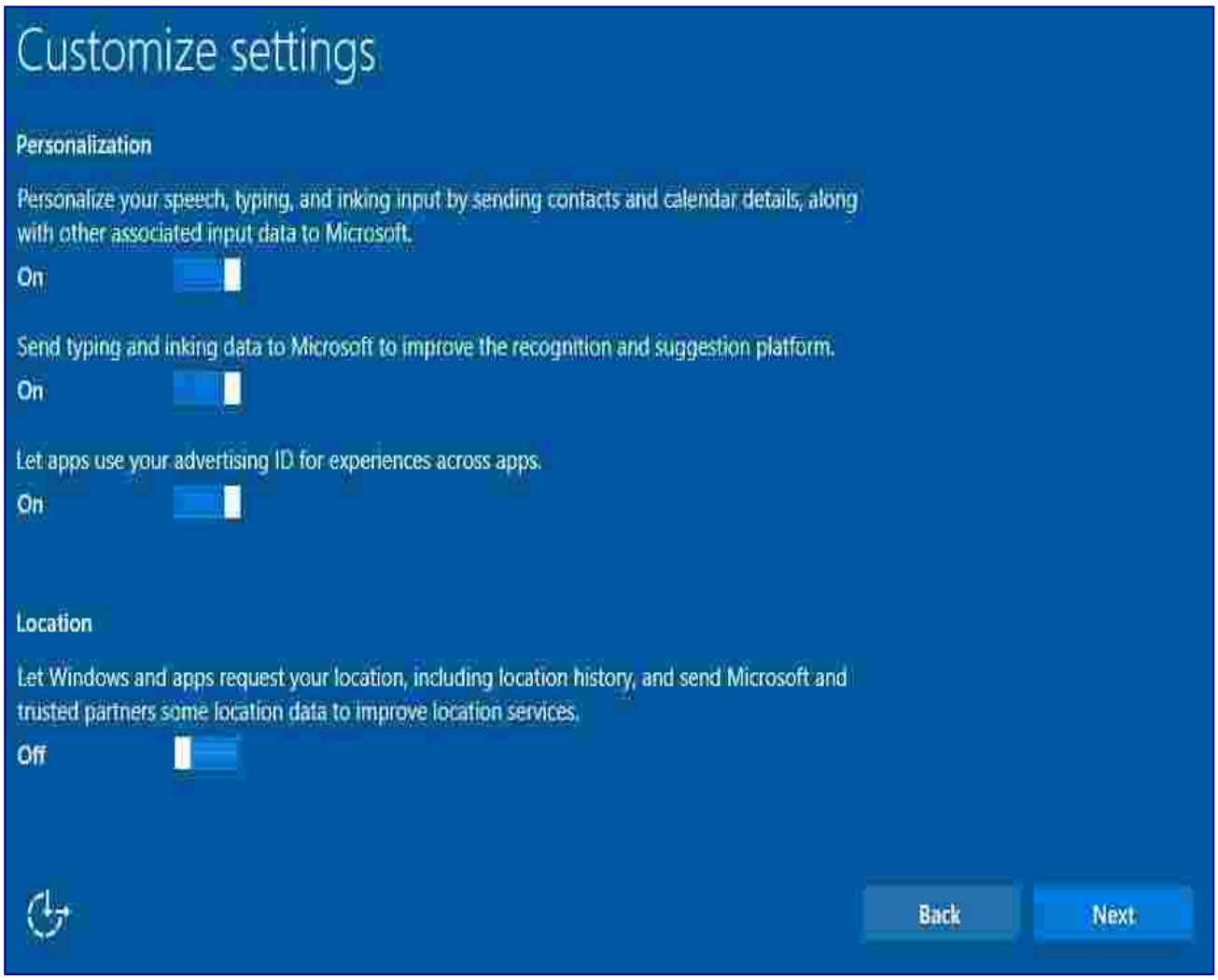
Zajímavé je odesílání dat z hlasového portu. Cortana převádí hlas nejprve na texty. Ty se odesílají na servery:

pre.footprintpredict.com
reports.wes.df.telemetry.microsoft.com
df.telemetry.microsoft.com

Cortana poté odesílá i hlasové vzorky (.wav soubory), ale ne pokaždé. Z měření jsem zjistil, že Cortana má základní slovník instalovaný lokálně u sebe, lze vypozorovat učební algoritmus, Cortana rozlišuje po určité době slova lépe, i komplexní věty a na servery se dotazuje méně často, ale zato ve větších objemech přenosů dat, což je trochu znepokojující.

Zhruba 1x za 15 minut se odesílá (při nečinnosti počítače) souhrn dat o velikosti téměř 80 MB na servery:

oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
vortex-sandbox.data.microsoft.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.net
pre.footprintpredict.com
telemetry.appex.bing.net
telemetry.urs.microsoft.com
cs1.wpc.v0cdn.net



To je příliš velký balík na „metadata“, takže mám důvodné podezření, že se odesílají komprimované hlasové vzorky formátu .wav od uživatele k analýze. Windows 10 se při běžném používání chovají normálně, nemají moc velký traffic do internetu, ale jakmile odejdete od počítače a naběhne spořič, do 15 minut začne podezřele vysoká aktivita odesílání dat. Zde je pro úplnost seznam všech serverů Microsoftu, na které nové Windows 10 „volají“ a předávají data o uživateli:

vortex.data.microsoft.com
vortex-win.data.microsoft.com
telecommand.telemetry.microsoft.com
telecommand.telemetry.microsoft.com.nsatc.net
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
sqm.telemetry.microsoft.com
sqm.telemetry.microsoft.com.nsatc.net
watson.telemetry.microsoft.com
watson.telemetry.microsoft.com.nsatc.net
redir.metaservices.microsoft.com
choice.microsoft.com
choice.microsoft.com.nsatc.net
df.telemetry.microsoft.com
reports.wes.df.telemetry.microsoft.com
wes.df.telemetry.microsoft.com
services.wes.df.telemetry.microsoft.com
sqm.df.telemetry.microsoft.com

telemetry.microsoft.com
watson.ppe.telemetry.microsoft.com
telemetry.appex.bing.net
telemetry.urs.microsoft.com
telemetry.appex.bing.net:443
settings-sandbox.data.microsoft.com
vortex-sandbox.data.microsoft.com
survey.watson.microsoft.com
watson.live.com
watson.microsoft.com
statsfe2.ws.microsoft.com
corpext.msitadfs.glbdns2.microsoft.com
compatexchange.cloudapp.net
cs1.wpc.v0cdn.net
a-0001.a-msedge.net
statsfe2.update.microsoft.com.akadns.net
sls.update.microsoft.com.akadns.net
fe2.update.microsoft.com.akadns.net
diagnostics.support.microsoft.com
corp.sts.microsoft.com
statsfe1.ws.microsoft.com
pre.footprintpredict.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.net
feedback.windows.com
feedback.microsoft-hohm.com
feedback.search.microsoft.com
rad.msn.com
preview.msn.com
ad.doubleclick.net
ads.msn.com
ads1.msads.net
ads1.msn.com
a.ads1.msn.com
a.ads2.msn.com
adnexus.net
adnxs.com
az361816.vo.msecnd.net
az512334.vo.msecnd.net

Seznam serverů je převzat z aplikace Destroy Windows 10 Spying, viz. níže. Při svém testování jsem zachytil živou komunikaci zhruba s polovinou serverů z uvedeného seznamu.

Samozřejmě, že první, co vás napadne, je zakázání komunikace s těmito servery (pomocí zanesení serverů do hosts file a nastavení na 127.0.0.1 na localhost), ale jak jsem si vyzkoušel, po jejich zakázání se Windows 10 začnou chovat podezřele jinak. Vyskakují chybové hlášky, občas se objeví hlášení o „selhání služby“, objevují se problémy se Skypem, kdy není možné udržet stabilní spojení. Problém je i s VPN spojeními, které padají. Ale je možné, že jde jen o nějakou nekompatibilitu a nevyladěnost nového OS. Zřejmě je nutné některé servery nezakazovat a nechat dostupné, aby vše fungovalo, ale neměl jsem čas je analyzovat jeden po druhém, co jejich vypnutí způsobí v delším časovém horizontu ve Windows 10.

Pokud nemáte technické znalosti a nevíte, jak ručně editovat hosts file, můžete použít program Destroy Windows 10 Spying, ke stažení z internetu zde. Upozorňuji, že toto vám nezaručí

anonymitu, protože Windows 10 si v rámci updatů můžou stahovat seznamy dalších serverů microsoftu, resp. Windows 10 si samy mohou zapisovat a měnit nastavení v hosts file, např. při diagnostice Windows, kdy bez upozornění vám Windows vymažou (vykomentují) override nastavení serverů v hosts souboru.

Windows 10 zároveň obcházejí letitou tradici hosts file, protože se na některé klíčové servery Microsoftu připojují natvrdo pomocí IP adres, tzn. bez nutnosti komunikace s DNS servery anebo s hosts souborem, ale nedojde ke stahování třeba updatů. To je zajímavé, že když zakážete v hosts file Windows Update servery, Windows 10 se k nim stejně připojí, ale přímo pomocí IP adres a obejdou tak override v hosts souboru. Ale nedojde ke stažení updatů. V podstatě jde jen o jakési oznámení Microsoftu, že jste si zakázali v hosts file update servery. To je zajímavé chování, jistě ne samoúčelné. Vynulováním komunikace se servery přes hosts file navíc přivodíte nestabilitu některým programům a komponentům. Pokud se rozhodnete Windows 10 používat, použijte tento nástroj jen v případě, že víte, co děláte.

Windows 10 jsou svým charakterem myšlenkovým posunem k terminálové platformě služeb, která o uživateli sbírá informace, aby mu výměnou za to poskytla maximální servis a přizpůsobení se jeho potřebám. Je zde však velmi vysoké riziko zneužití biometrických dat (hlas, oči, obličej) a informací o soukromí, businessu a rodině uživatele. Zachytávání textů z klávesnice dále představuje vysoké riziko pro bezpečnost, kdy hackeři mohou skrze bezpečnostní díry ve Windows 10 v budoucnu zachytávat z Windows 10 vstupní hesla do emailů, bankovnictví atd. Navíc použití kryptovaných nástrojů pozbývá ve Windows 10 smyslu, protože Windows 10 vidí vaše prsty a slyší, co říkáte. Takže kryptovaný chat anebo kryptované SIP volání vám nepomohou.

Možná proto jsou Windows 10 zadarmo?

Pokud by někdo uvažoval velmi zle a zákeřně s cílem špehovat uživatele a občany, nabídl by jim operační systém zdarma, anebo alespoň jeho upgrade zdarma, který je prolezlý šmírovacími programy v samotném základu operačního systému. Windows 10 jsou totiž opravdu zdarma, a to pro všechny majitele předchozích operačních systémů Windows od verze 7. Ale to není Microsoft první s tímto nápadem. S tím už přišel Android od Google před mnoha lety.

Dokud nebudou od Microsoftu k dispozici nějaká vysvětlění, co všechno servery sbírají, není bezpečné Windows 10 instalovat na produkční počítač, ani doma, ani v práci nebo ve firmě. Zcela vyhnout by se tomuto operačnímu systému měli lidé, kteří kryptují data. **Ve své podstatě jsou Windows 10 více analytický systém než operační.** A to představuje značné riziko pro možné zneužití.