Nevlastníte hardware? Tak nevlastníte ani svá data

Šifrovanou komunikaci lze na úrovni hypervizoru odposlouchávat, ukázali experti Bitdefenderu.

BOGDAN BOTEZATU

Odhalení Edwarda Snowdena, týkající se odposlechu uskutečněného NSA a jejich partnerskými agenturami přimělo vlastníky infrastruktur a poskytovatele služeb spolu s běžnými uživateli, aby se ujistili, že se tok dat ukládá v zašifrované formě.

Každou chvíli se zkoumají populární protokoly nebo jejich implementace a nalezené chyby se dříve nebo později opraví. Toto je i případ zranitelností jako Heartbleed nebo Longjam, které podnítily vydávání patchů dosud nevídaným tempem.

Jsou ale firmy – a zároveň i jejich zákazníci – opravdu chráněné, jakmile se těchto chyb začne využívat? Existují nějaké skryté metody, které různé agentury či organizace mohou využít k překonání zabezpečení TLS/SSL?

Koncem května 2016 na konferenci HITB v Amsterdamu ukázal Radu Caragea, člen bezpečnostního týmu Bitdefenderu, že kódovaná komunikace se může v reálném čase dešifrovat za použití techniky, která prakticky nezanechá stopy a je neviditelná pro každého s výjimkou extrémně starostlivých bezpečnostních auditorů.

Co to znamená pro vaši bezpečnost? Tento útok umožní kompromitovanému (nebo dotlačenému k tomu, aby dal přístup třetí straně) poskytovateli cloudových služeb obnovit klíče TLS (Transport Layer Security) užívané k zašifrování veškeré komunikace mezi vaším virtualizovaným serverem a vašimi zákazníky (i v případě, že používáte Perfect Forward Secrecy).

Pokud jste CIO a vaše firma outsourcuje svou virtualizační infrastrukturu třetí straně, předpokládáte, že všechny informace, které proudí mezi vámi a uživateli, byly dešifrované a lze je číst po neomezeně dlouhou dobu.

Nikdo vám neřekne, zda vaše komunikace byla narušená a na jak dlouho to bylo, protože tento postup za sebou nezanechává žádné anomální forenzní důkazy.

Banky, společnosti zabývající se duševním vlastnictvím nebo osobními informacemi, jakož i vládní instituce jsou sektory, které by mohly být těmito chybami velmi ovlivněné.

Základní popis techniky útoku

Nová technika, označovaná jako TeLeScope, byla vyvinutá Bitdefenderem kvůli výzkumným účelům. Umožňuje třetí osobě odposlouchávat komunikaci šifrovanou pomocí TLS mezi koncovým uživatelem a virtualizovanou instancí serveru.

Tato technika je ale účinná pouze u virtualizovaného prostředí, které běží na vrcholu hypervizoru. Tyto infrastruktury jsou v dnešní době velice populární a jsou poskytované giganty, jako jsou Amazon, Google, Microsoft nebo DigitalOcean. Většina z nich souhlasí s tím, že virtualizace je budoucnost, pokud jde o ukládání, přesouvání a zpracování big dat.

Spíše než využívání chyb v protokolu TLS tato nová technika útoku spoléhá na extrahování TLS klíče na úrovni hypervizoru s využitím chytrého snímání paměti.

Zatímco přístup k virtuálním zdrojům virtuálního stroje je něco, co už známe (například přístup k HDD stroji), dešifrování provozu TLS v reálném čase bez zastavení VM v očividném časovém rámci je to, co tu dosud nebylo.

„Objevili jsme tento druh útoku, když jsme zkoumali způsob, jak sledovat škodlivou odchozí aktivitu na naší síti s honeypoty bez nutnosti zásahu do zařízení a bez toho, aby si útočník byl vědom toho, že je sledovaný, uvádí Caragea.

„Po tomto objevu jsme se rozhodli detailně uveřejnit, jak neuspokojivý je stav pasivního monitorování provozu ve virtuálních prostředích v souvislosti se sociálním, ekonomickým a politickým soutěžením. Například nespokojený správce serveru s přístupem k hypervizoru na hostingový server může sledovat, přefiltrovat a zpeněžit všechny informace proudící od a k zákazníkovi: e-mailové adresy, bankovní transakce, chaty, osobní fotografie a další soukromá data," dodává Caragea.

Jak to funguje?

Za normálních okolností pro obnovení klíče z paměti virtuálního stroje je nutné pozastavit applianci a vypsat obsah paměti do souboru. Oba procesy jsou rušivé a vlastníkovi virtuálního stroje (nemluvě o porušení SLA) nápadné.

Výše zmíněný nový přístup Bitdefenderu spočívá v mechanismech živé migrace, přítomných v moderních hypervizorech, které umožňují zúžit potřebný počet stránek paměťového výpisu z celé RAM pouze na ty, jež byly modifikované v průběhu procesu TLS handshake.

„Namísto zastavení stroje (což znatelně zvedne latenci) a plného výpisu paměti, vyvíjíme paměťovou porovnávací techniku využívající tzv. primitives obsažené v technologii hypervizoru," říká Caragea. „Poté, co snížíme velikost výpisu z gigabitů na megabity, není čas potřebný k zapsání i takového množství dat stále zanedbatelný (řádově několik milisekund), ukážeme si tedy dále, jak tento proces dále ‚zamaskovat' v latenci sítě, aniž bude nutné stroj pozastavit."

Jedině vlastnictví infrastruktury

Útok TeLeScope nevyužívá chyb v implementaci protokolu TLS, ani se nepokouší obcházet úrovně implementace šifrování TLS s pomocí tzv. downgrade útoku. Místo toho využívá funkce hypervizoru k přefiltrování klíčů používaných protokolem k dešifrování relace.

Tento koncept odkrývá základní chyby, které se nemohou opravit nebo alespoň zmírnit bez přepsání kryptografických knihoven používaných v současné době. Jediný způsob ochrany je v první řadě zamezení přístupu k hypervizoru – tedy provozovat svůj vlastní hardware uvnitř své infrastruktury.

Další informace o tomto konceptu naleznete na webových stránkách konference HITB. ■

Autor je analytikem ve společnosti Bitdefender.