Luuuk ukradl za týden půl milionu eur

Londýn, 26. června 2014

Analytici Kaspersky Lab objevili cílený útok na klienty velké evropské banky. Podle záznamů ze serveru využívaného útočníky ukradli kybernetičtí zločinci během jediného týdne více než půl milionu eur (téměř 14 milionů korun). Poprvé experti narazili na kampaň Luuuk na konci letošního ledna při odhalení jeho řídících C&C serverů (comand and control).

Kaspersky Lab také našla záznamy o transakcích, jež obsahovaly informace o tom, jaké sumy z jakých účtů byly odčerpány. Celkem identifikovala 190 obětí, většinu z nich v Itálii a Turecku. Jednotlivé ukradené částky se pohybovaly v rozmezí 1 700 až 39 000 eur.

Dva dny po odhalení C&C serverů týmem Kaspersky Lab odstranili kybernetičtí zločinci veškeré stopy, které by mohly analytiky dovést až k nim. Experti se nicméně domnívají, že se spíše změnila infrastruktura kampaně Luuuk, než že by ji útočníci zcela zastavili. Ihned po objevení útoku Kaspersky Lab kontaktovala bezpečnostní služby a policejní orgány a předala jim své důkazy. Nadále také monitoruje, zda se podobný útok nebude opakovat.

Analytici jsou přesvědčení, že důležitá finanční data byla útočníky získána automaticky a podvodné transakce začaly probíhat ve chvíli, kdy se oběť přihlásila do svého bankovního účtu. Na C&C serverech nezůstaly žádné informace o malwaru využitém v této kampani, nicméně existující varianty malwaru Zeus (Citadel, SpyEye, IceIX, apod.) obsahující k tomu potřebné funkce.

Ukradené peníze byly převedeny na účty podvodníků neobvyklým způsobem. Členové podvodné organizace obdrželi části ukradených částek na speciálně vytvořené účty, z nichž je vybrali pomocí bankomatů. Jedna skupina byla odpovědná za převod částek ve výši 40 až 50 tisíc eur, jiná 15 až 20 tisíc eur a třetí ne více než dvou tisíc.

„Rozdíly v částkách v různých skupinách naznačují různé úrovně důvěry uvnitř gangu. Víme, že jejich členové často své kumpány podvádějí a zatajují částky, které měli vybrat. Šéfové Luuuku se možná snažili těmto ztrátám zabránit tím, že vytvořili různé úrovně důvěry – podle výše částky,“ komentoval strategii zločinců přední analytik Kaspersky Lab Vicente Diaz.

Zabezpečení před Luuukem

Podle důkazů jde pravděpodobně o profesionální zločineckou kampaň. Odcizení peněz z účtu lze zabránit zabezpečovacími technologiemi a sofistikovanými funkcemi antivirových řešení. Kaspersky Lab například vyvinula platformu Kaspersky Fraud Prevention, které finančním organizacím nabízí mnohavrstvou ochranu před podvody.

Více informací o kampani Luuuk si přečtěte na blogu Securelist.com.

O společnosti Kaspersky Lab

Kaspersky Lab je největším soukromě vlastněným poskytovatelem koncových bezpečnostních řešení na světě. Společnost se řadí mezi čtyři největší prodejce bezpečnostních řešení pro koncové uživatele. Již více než 16 let patří Kaspersky Lab mezi přední inovátory v oblasti informačních technologií a poskytuje efektivní digitální bezpečnostní řešení domácím uživatelům, malým a středním firmám i velkým podnikům. Aktuálně společnost registrovaná ve Velké Británii působí v bezmála 200 zemích a oblastech a poskytuje ochranu více než 300 milionům uživatelů. Více informací o společnosti Kaspersky Lab najdete na www.kaspersky.cz.*

**Společnost zařadil na čtvrté místo žebříček „IDC Worldwide Endpoint Security Revenue by Vendor, 2012“. Žebříček vyšel ve zprávě „IDC Worldwide IT Security Products 2013-2017 Forecast and 2012 Vendor Shares – August 2013“ a řadil poskytovatele software podle zisku z prodeje koncových bezpečnostních řešení v roce 2012.*

Pro další informace prosím kontaktujte:

Michal Malysa
PR Consultant
Grayling Czech Republic
Tel.: 224 251 555
Mobil: 775 708 086
michal.malysa@grayling.com
Twitter.com/GraylingCZ