E-Bezpečí 2019, 4(1): Page 20-22. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1414

NOVINKA Z UPOINTU OCHRÁNÍ VÁS I VÁŠ POČÍTAČ

Kamil KOPECKÝ

Poradna projektu E-Bezpečí UP v roce 2018 zachytila 15 případů, ve kterých byla webkamera využita k útoku na jiné uživatele internetu. Cílem jsou jak děti, tak i dospělí. Univerzitní informační centrum a obchod UPoint proto zareagoval na zvýšenou obavu o bezpečnost na internetu a zařadil do svého sortimentu posuvnou krytku na webovou kameru, pomocí které uživatel mechanicky reguluje, kdy je možné se skrze kameru „dívat“.

Útoky, jejichž nástrojem se může stát webkamera počítače, mají hned několik podob. Buď využívají tzv. webcam trollingu, nebo k útoku dojde pomocí viru/malware šířeného například prostřednictvím e-mailu.

„Princip webcam trollingu je poměrně jednoduchý - pachatel vyzve v online prostředí vyhlédnutou oběť ke komunikaci prostřednictvím webové kamery. Místo skutečného záznamu však oběť vidí předtočenou videosmyčku. Muži například vidí video atraktivní ženy. Oběť, která uvěří, že skutečně komunikuje s osobou, kterou vidí na webkameře, je následně manipulována. Sofistikovanými způsoby je pak donucena, aby se před webkamerou obnažila,“ vysvětluje Kamil Kopecký, vedoucí Centra prevence rizikové virtuální komunikace PdF, které je garantem projektu E-Bezpečí.

Jak upozorňuje, pachatel vše nahrává a citlivý materiál využívá k útoku - vydírání, sexuálnímu nátlaku a podobně. Oběť, která má strach oznámit situaci policii, pak často platí za to, že se intimní materiály nezveřejní. U dětí může dojít například k vylákání intimních materiálů či přímo k tzv. kybergroomingu.

Podle Martina Kožíška z CZ.NIC se oběťmi útoků s využitím webových kamer nestávají pouze dívky. „Stále častěji jsou to také chlapci, kteří věří, že se v online prostředí seznámí a získají například svého sexuálního partnera. To se samozřejmě může stát, existuje však vysoké riziko, že chlapec komunikuje s internetovým abuzérem.“

Vydírání využívající webové kamery však necílí pouze na děti. Kapitán Pavel Schweiner, vrchní komisař oddělení kybernetické kriminality olomoucké policie a odborný konzultant a lektor projektu E-Bezpečí, připomíná, že se terčem vydírání stávají také významní a úspěšní muži. Ti pak raději vyděrači zaplatí nemalý obnos, než aby došlo ke zveřejnění materiálu, který by je mohl velmi poškodit a poznamenat například jejich kariéru.

„Další možnost, jak lze webkameru zneužít, představují různé druhy virových infekcí, které převezmou kontrolu nad vaší webkamerou a jsou schopny odesílat vaše obrazová data na internet - třeba na e-mail pachatele. To je však poměrně technicky obtížné - útočník či případný virus by musel obejít celou řadu technických zabezpečení, od firewallu přes antiviry a podobně. Není to však nemožné, jak potvrzuje celá řada celebrit, jejichž soukromá fota či krátká videa unikla na internet právě díky virové infekci či přímo hackerskému útoku,“ popisuje další rizika Kamil Kopecký.

Strach z úniku intimních materiálů bývá podle něj také součástí různých hoaxů a podvodných zpráv šířených internetem. „Už v říjnu minulého roku jsem upozorňoval na to, že českým internetem putuje celá řada vyděračských e-mailů označovaných jako tzv. virus RAT (remote access trojan). Ty straší uživatele tím, že neznámý útočník prostřednictvím webové kamery získal přístup k vašim pornografickým materiálům, a pokud nezaplatíte 550 dolarů, budou tyto materiály zveřejněny. A jako důkaz obsahoval e-mail přílohu s těmito ´materiály´. Pokud jste však na přílohu klikli, mohl být váš počítač infikován právě pomocí viru. Samozřejmě k úniku vašich materiálů nedošlo, smyslem zprávy bylo vystrašit a přimět vás k otevření přílohy. Policie ČR v této věci vydala i varování, aby uživatelé v žádném případě žádné částky pachateli neplatili," říká expert z pedagogické fakulty.

Ochránit uživatele by proto mohla i na první pohled nenápadná novinka z UPointu.