Jaké triky zkoušejí počítačoví piráti

Miloslav Fišer

Nebývale aktivní byly v uplynulém roce počítačoví piráti, kteří šíří především prostřednictvím internetu škodlivé soubory. A první týdny nového roku jasně ukazují, že letos na síti rozhodně bezpečněji nebude.

Antiviry společnosti Kaspersky zachytily v uplynulých 12 měsících o 5,2 procenta více škodlivých souborů než o rok dříve. To v absolutních číslech znamená, že každý den bylo detekováno 360 tisíc nových škodlivých souborů.

„Na tomto růstu se nejvíce podílely trojské koně, tedy škodlivé soubory s nejrůznějšími funkcemi od mazání dat po krádeže osobních informací, a tzv. backdoory – specifický typ trojského koně, díky němuž útočníci můžou napadený počítač vzdáleně ovládat," konstatoval Michal Lukáš, Presales Manager společnosti Kaspersky pro region střední a východní Evropy.

Foto archiv (4x)

Práce a studium z domova

V případě trojských koní byl meziroční nárůst 40,5 procenta, u backdoorů pak 23 procent. „Naopak menší výskyt zaznamenaly Adware soubory – programy, které napadeného bombardují reklamou. Těch bylo v porovnání s rokem 2019 o 35 procent méně," prohlásil Lukáš.

„Většina škodlivých souborů (89,80 procenta) se do napadených počítačů dostala přes soubory Windows PE, což je formát využívaný výhradně operačními systémy Windows. Podíl škodlivého softwaru využívajícího operační systém Android klesl na 13,7 procenta," uvedl bezpečnostní expert.

Podle něj je patrné, že v loňském roce začala spousta lidí studovat a pracovat z domova, většinou na stolních počítačích a noteboocích. „Útočníci se tomu zjevně přizpůsobili a zaměřili se právě na tato zařízení. O 27 procent vzrostl i počet škodlivých skriptů, rozesílaných e-mailem nebo stahovaných z napadených stránek. To rovněž svědčí o tom, že lidé na internetu tráví víc času než dřív a útočníci toho dokážou využít," doplnil Lukáš.

Antivirus jako nutný základ

Bez antiviru nemá běžný uživatel prakticky žádnou šanci si všimnout, že byl jeho přístroj infikován. Každý tablet a chytrý telefon by tak měly být vybaveny bezpečnostním softwarem, který bude všechny hrozby neustále hlídat.

Antivirus by měl být samozřejmostí i na počítačích. Nicméně je dobré podotknout, že nezvané návštěvníky dokážou v počítači nebo mobilu odhalit speciální programy. Jde například o aplikace, které se soustředí pouze na špionážní software a hledání trojských koňů.

Jiné programy zase dokážou v operačním systému nalézt tzv. keyloggery, které jsou schopné zaznamenávat stisk každé klávesy a nasbíraná data odesílat útočníkovi.

Na PC i mobilu by měl být nainstalován vždy jen jeden bezpečnostní program svého druhu. Dva antiviry na disku dokážou udělat pěknou neplechu. Samotný antivirus ale zárukou bezpečí není. Uživatelé by neměli zapomínat na pravidelné stahování všech bezpečnostních záplat, a to pro samotný operační systém i doinstalované programy.

Natočili jsme si vás webkamerou, vydírají podvodníci

Napálit důvěřivce a vytáhnout z nich peníze se snaží v posledních dnech počítačoví piráti prostřednictvím nevyžádaných e-mailů. Uživatelům tvrdí, že z jejich účtu odcizili lechtivá videa, a vyhrožují jejich zveřejněním, pokud jim nebude uhrazeno výkupné. Upozornila na to antivirová společnost Eset.

Podobné phishingové podvody se objevily na českém internetu již v minulosti, aktuálně ale probíhá další masivní kampaň.

„S podobnými e-maily se setkáváme pravidelně a v různých obměnách. Dříve převládaly anglicky psané zprávy, nyní převládají ty s takřka bezchybnou češtinou. Jde ale o masovou spamovou kampaň, kterou můžeme vidět v soukromých i pracovních e-mailových schránkách. Zároveň jde o podvod, neboť žádnou nahrávkou útočník nedisponuje, a proto není důvod žádné výkupné platit," prohlásil expert Esetu Robert Šuman.

„Do vašeho přístroje jsme nainstalovali jeden software RAT. Pro tento okamžik je váš e-mailový účet napaden," tvrdí útočníci v e-mailu. Dále se v textu uživatelé dozvědí, že se kvůli napadení zařízení podařilo útočníkům nahrát prostřednictvím předního fotoaparátu video, jak dotyčný majitel telefonu, tabletu nebo počítače masturboval před webkamerou, když sledoval lechtivá videa. Aby toto choulostivé video nezveřejnili, chtějí kyberzločinci zaplatit výkupné ve výši 250 dolarů, tedy bezmála 5500 Kč. Celou částku přitom požadují uhradit ve virtuální měně bitcoin, jejíž transakce nejsou evidovány tak jako například u bankovních převodů. Šance na dopadení pirátů je tedy prakticky nulová.

Podvodné investiční stránky přibývají jako houby po dešti

Rychle rostoucí kurzy kybernetických měn nejsou lhostejné ani počítačovým pirátům, jak upozornili bezpečnostní experti z antivirové společnosti Eset. Ti již zachytili první podvodné investiční stránky, které se snaží uživatele připravit o peníze či osobní data. Falešné weby se přitom nyní množí jako houby po dešti.

V posledních dnech se velice často hovoří o dramatickém nárůstu kurzu bitcoinu, posilují ale i další kyberměny. Celková hodnota trhu s virtuálními mincemi tak ve čtvrtek vůbec poprvé v historii překonala hranici jednoho bilionu dolarů (21,3 bilionu Kč).

A právě rostoucí zájem o virtuální mince láká také počítačové piráty, jejichž cílem jsou tentokrát začínající investoři. Analytici již nyní detekují nárůst bitcoinových podvodů o desítky procent. „Jedná se o takový evergreen podvodů. Detekujeme jej ve více než 20 jazykových mutacích po celém světě. Některé jazykové verze jsou povedenější, některé překlady jsou spíše strojové, nicméně vždy útočníci zneužijí jméno lokálně známé osobnosti," konstatoval Robert Šuman, vedoucí pražského výzkumného oddělení Esetu.

„V Česku takto například zneužívají jména Petra Kellnera, Petra Čecha, Jaromíra Jágra, Jaromíra Soukupa, dále světových inovátorů, jako je Elon Musk či Bill Gates. Na Slovensku jsme zaznamenali podvod s Miroslavem Trnkou, spoluzakladatelem společnosti ESET. Útočníci rychle mění webové stránky i adresy kryptopeněženky. Pro oběti i osobnosti, jejichž jméno je takto zneužité, je velmi složité se bránit," podotkl Šuman.

Zavirovaná videohra pro mobily

Cyberpunk 2077 byl jednou z nejočekávanějších her loňského roku. Přestože jde o titul, který je určen výhradně pro výkonné herní stroje, hrát se dá prostřednictvím cloudových platforem i na chytrých telefonech. Právě toho se ale snaží zneužít počítačoví piráti, kteří již internetem šíří zavirovanou mobilní verzi.

„Zvýšený zájem kyberzločinců o Cyberpunk 2077 je pochopitelný. Herní komunita na tuto hru čekala osm let, takže už před jejím oficiálním vydáním byli uživatelé ochotni stahovat vše, co se této hře podobalo," prohlásil Michal Lukáš, Head of Presales ve společnosti Kaspersky pro region střední a východní Evropy.

Podle něj bezpečnostní experti zachytili kromě prvních podvržených bezplatných verzí tohoto titulu také daleko nebezpečnější variantu – falešnou mobilní verzi Cyberpunku 2077, která šíří vyděračský ransomware. Ten dovede uzamknout celý mobilní telefon a zablokovat uložená data, za jejich zpřístupnění pak útočníci požadují výkupné.

„Dobrou zprávou je, že u falešné mobilní verze zločinci ponechali dešifrovací klíč jako součást trojanu, kterým se šíří. To znamená, že je možné napadené soubory dešifrovat, aniž by bylo nutné zaplatit výkupné. Do budoucna je ale důležité, aby všichni hráči velmi bedlivě sledovali, odkud si stahují hry – zejména pokud je jim nabízena ‚beta' verze na nějaké nové platformě. Hry budou vždy oblíbeným cílem kyberzločinců," dodal Lukáš.

Není ovšem vyloučeno, že u některé z dalších verzí kyberzločinci již tak nepozorní nebudou a falešnou verzi Cyberpunku 2077 budou šířit s nějakým zákeřnějším škodlivým kódem. Uživatelé by tedy měli být velmi obezřetní v tom, co stahují.

Luxusní zboží, nízká cena. Podvodníci číhají na Sbazaru

Na velkých inzertních portálech v různých koutech světa se objevily v posledních dnech podvodné nabídky, ve kterých se zpravidla nabízí drahé zboží za velmi atraktivní cenu. Po Rusku, Litvě a Ázerbájdžánu se kyberzločinci zaměřili také na české uživatele – podvodné nabídky šíří prostřednictvím populárního inzertního portálu Sbazar.cz.

Podvodných inzerátů nalezli analytici z Avast Threat Labs na portálu Sbazar.cz hned několik. Atraktivní cena zboží ale nakonec může uživatele přijít velmi draho. Útočníci se totiž ve skutečnosti snaží z důvěřivců vylákat citlivá osobní data, například i kompletní informace o platební kartě.

Podobné útoky nejsou nijak výjimečné napříč celým internetem. „Na službu Sbazar.cz, stejně jako na jiné internetové služby, zaměří podvodníci čas od času svou pozornost. To se projevuje nabízením údajně cenného a luxusního zboží za nerelevantně nízké ceny," uvedla mluvčí společnosti Seznam.cz Aneta Kapuciánová.

„Našim uživatelům doporučujeme v e-mailech i naší Nápovědě, aby při reakcích na podobné nabídky byli velmi obezřetní. Pokud máme od našich uživatelů nahlášené podvodné jednání na službě, okamžitě daný inzerát a jeho zadavatele prověřujeme a případně blokujeme," konstatovala Kapuciánová.

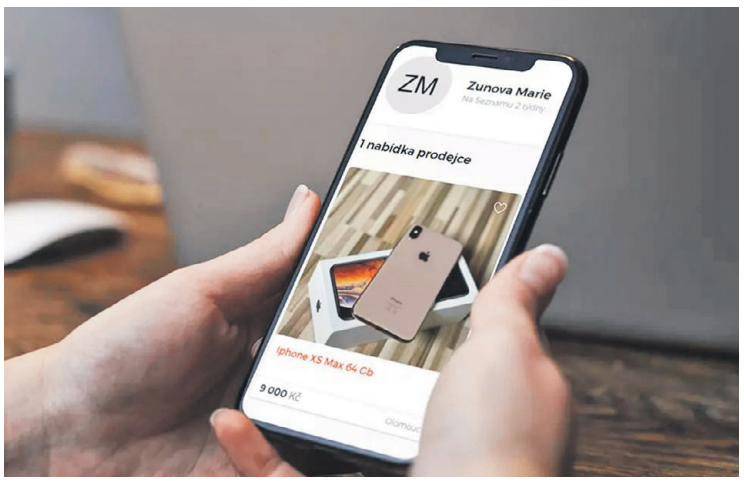

Foto Reuters

Slibují vakcínu, ale důvěřivce oškubou

Řada evropských zemí řeší nedostatek vakcín proti koronaviru. Právě to ale hraje do karet překupníkům, kteří na černém trhu nabízejí vakcíny stále častěji. Za jednu dávku chtějí přitom i 1000 dolarů, což je necelých 21 500 Kč. Upozornila na to kyberbezpečnostní společnost Check Point, jejíž výzkumníci se pokusili vakcínu skutečně objednat.

„Platba proběhla v bitcoinech a výzkumníci poslali prodejci doručovací adresu a požádali o podrobnosti o zásilce. Po několika dnech bez odpovědi prodejce poslal zprávu, že vakcína byla odeslána na uvedenou adresu. O několik dní později byl účet dodavatele nepřekvapivě smazán a zásilka nedorazila," konstatoval Daniel Šafář, bezpečnostní expert Check Pointu.

Někteří dodavatelé mohou sice na darknetu skutečně nabízet pravé vakcíny, ale tento příklad jasně ilustruje, jak se mohou lidé dychtící po očkování snadno nechat napálit. Platbu v bitcoinech ani samotného obchodníka totiž už prakticky není možné dohledat.

Jeden z prodejců, se kterým Check Point komunikoval, údajně tvrdil, že je schopen dodat 10 000 dávek, což by stačilo pro 5000 lidí. Zda by vakcíny skutečně dorazily, ale samozřejmě nikdo neví. „Pokud se něco zdá až příliš dobré, než aby to byla pravda, pak to nejspíš pravda nebude. Když se budete snažit na darknetu koupit nějakou vakcínu a léky, pak výsledkem bude nejspíš jen jediná věc: ztenčí se vaše bankovní konto," varoval bezpečnostní expert.

Check Point doposud odhalil 340 nabídek, což představuje nárůst o 400 % v meziměsíčním srovnání.