Malware na vzestupu: Kaspersky letos odhalil 467 000 škodlivých souborů denně

13.12.2024 - | PROTEXT

Primárním cílem kybernetických útoků byl i nadále systém Windows, na který mířilo 93 % všech denně detekovaných dat obsahujících malware. Nebezpečné kódy šířené prostřednictvím různých skriptů a formátů dokumentů MS Office se umístily mezi třemi nejčastějšími hrozbami, což představuje 6 % všech denně detekovaných škodlivých souborů.

Detekční systémy společnosti Kaspersky odhalily mezi roky 2023 a 2024 výrazný 19% nárůst malwaru pro Windows. Nejrozšířenějším typem malwaru zůstávají trojské koně – škodlivé programy, které se vydávají za legitimní software –, jejichž nárůst v tomto období činil 33 %. Dvaapůlkrát (o 150 %) se zvýšilo také používání tzv. dropperů – trojských koní, které jsou navrženy tak, aby do počítače nebo telefonu oběti přenesly nepozorovaně jiný malware.

„Počet nových hrozeb každoročně roste, protože útočníci vyvíjejí stále nový malware, techniky a metody, jak napadat jednotlivce i organizace. Letošní rok nebyl výjimkou. Byly zaznamenány nebezpečné trendy, jako jsou útoky na důvěryhodné vztahy a dodavatelské řetězce, včetně útoků na balíčky s otevřeným zdrojovým kódem (třeba případ XZ, kdy zdánlivě důvěryhodný programátor tajně propašoval do kódu programu „zadní vrátka"). Probíhaly masivní phishingové akce a škodlivé kampaně zaměřené na uživatele sociálních sítí a došlo k nárůstu bankovního malwaru. K vytváření nového malwaru nebo usnadnění phishingových útoků přispělo samozřejmě i používání nástrojů umělé inteligence. V tomto vyvíjejícím se prostředí kybernetických hrozeb se uživatelé, kteří dbají na bezpečnost, neobejdou bez spolehlivých bezpečnostních řešení. Odborníci společnosti Kaspersky se proto neustále věnují boji proti novým a sofistikovaným kybernetickým hrozbám a zajišťují uživatelům bezpečné online prostředí, stejně jako robustní kybernetickou bezpečnost a nejnovější informace o hrozbách pro organizace," komentuje Vladimir Kuskov, vedoucí oddělení výzkumu nástrojů proti malwaru ve společnosti Kaspersky.

Tato zjištění jsou založena na detekcích škodlivých souborů zachycených společností Kaspersky od ledna do října a jsou součástí sborníku Kaspersky Security Bulletin (KSB) – každoroční série předpovědí a analytických zpráv o klíčových změnách ve světě kybernetické bezpečnosti.

Abyste zůstali chráněni, dodržujte následující doporučení.

Individuální uživatelé:

• Nestahujte a neinstalujte aplikace z nedůvěryhodných zdrojů.

• Neklikejte na žádné odkazy z neznámých zdrojů nebo z podezřelé on-line reklamy.

• Používejte vždy dvoufaktorové ověřování, pokud je k dispozici.

• Používejte silná a jedinečná hesla obsahující kombinace malých a velkých písmen, číslic a interpunkčních znamének.

• Používejte spolehlivého správce hesel, abyste si je nemuseli všechna pamatovat.

• Instalujte neprodleně všechny dostupné aktualizace; obsahují opravy kritických bezpečnostních problémů.

• Ignorujte zprávy vyzývající k vypnutí bezpečnostních funkcí kancelářského nebo bezpečnostního softwaru.

• Používejte robustní bezpečnostní řešení, které je vhodné pro váš systém a zařízení, například Kaspersky Premium.

Organizace:

• Dbejte na neustálou aktualizaci softwaru na všech používaných zařízeních, abyste zabránili útočníkům proniknout do vaší sítě zneužitím zranitelných míst.

• Neumožňujte přístup ke službám vzdálené plochy (například RDP) přes veřejné sítě, pokud to není nezbytně nutné, a vždy pro ně používejte silná hesla.

• Používejte řešení, jako je Kaspersky NEXT EDR Expert, pro komplexní přehled o všech koncových bodech ve firemní síti, abyste získali spolehlivou obranu, automatizovali rutinní úkoly EDR a umožnili analytikům rychle vyhledávat, určovat priority, vyšetřovat a neutralizovat komplexní hrozby a útoky typu APT.

• Využívejte nejnovější informace o hrozbách na portálu Threat Intelligence, abyste měli přehled o aktuálních taktikách, technikách a postupech (TTP) používaných aktéry hrozeb.

• Pravidelně zálohujte firemní data. Zálohy by měly být izolovány od normálně používané počítačové sítě. Zajistěte, abyste k nim měli v nouzové situaci rychlý přístup.

Zdroj: Kaspersky

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/malware-na-vzestupu-kaspersky-letos-odhalil-467-000-skodlivych-souboru-denne/2608689