V pětině všech detekovaných případů se v Česku objevil virus Delf.NBX, rizikem je pro neaktualizované počítače

20.12.2023 - Rita Gabrielová, Lucie Mudráková | ESET software

Největší hrozbou pro operační systém Windows v Česku se stal v listopadu virus Delf.NBX, a to v pětině všech zachycených případů škodlivého kódu.

Nezvyklý typ útoku s využitím malwaru, který je v bezpečnostní komunitě převážně dobře zmapovaný, svědčí podle bezpečnostních expertů o tom, že útočníci cílili na země, kde předpokládali nižší úroveň zabezpečení. Škodlivý kód byl detekován po celém světě, kromě České republiky také například v Číně nebo v Egyptě. Spolu s virem Delf.NBX se v listopadu objevil další nezvyklý typ malwaru, a to škodlivý kód Agent.RIK, který se snaží obejít bezpečnostní kontroly. Oba typy škodlivého kódu se šíří podobně jako spyware prostřednictvím e-mailových příloh. Bezpečnostní specialisté upozorňují, že v nebezpečí mohou být především starší počítače s neaktualizovaným operačním systémem a nedostatečnou ochranou. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Do čela pravidelné statistiky pro operační systém Windows v České republice se dostal v listopadu virus Delf.NBX. Virus je typem škodlivého kódu, který napadá jiné programy, infikuje je a vytvoří z nich nositele dalšího škodlivého kódu. Napadený program přitom může v zařízení stále fungovat a uživatelé nemusí útok postřehnout.

„Viry jsou typem malwaru, na který dokáže bezpečnostní komunita již dnes velmi rychle reagovat, proto tento typ škodlivého kódu volí útočníci především v zemích, kde předpokládají horší bezpečnostní prostředí. Kromě Česka, kde se virus objevoval především 13. listopadu, pak útočníci zacílili také na Čínu a Egypt,“ vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Virus Delf.NBX se dokáže šířit prostřednictvím USB disků, zaznamenávat stisky kláves na klávesnici nebo stahovat a šířit další malware – v tomto případě se dokonce jednalo o v Česku dobře známý spyware Agent Tesla. Virus NBX dokáže odcizit informace o počítači a pořídit snímky obrazovky. Spyware Agent Tesla pak ještě jeho útok rozšiřuje o možnost krádeže dat, typicky uživatelských hesel,“ doplňuje Jirkal.

Virus Delf.NBX infikuje soubory s příponami .exe a excelové soubory s příponou .xlsx. Stejně, jako spyware, ho útočníci šířili prostřednictvím e-mailových příloh, a to jmenovitě například přílohami s názvy „Purchase Inquiry.exe“ nebo „OBJEDNÁVKA_ 13.11.23.exe“.

Virus Delf.NBX nebyl v listopadu jedinou novou hrozbou pro operační systém Windows v Česku. Bezpečnostní experti v českém prostředí detekovali také malware Agent.RIK, který se nejvíce šířil prostřednictvím e-mailové přílohy „Request for Quote Al-Farabi Kazakh National University 23-10-2023·pdf.vbs“.

„Malware Agent.RIK již patří k velmi pokročilému typu škodlivého kódu. Šíří se jako příloha s příponou .rar, která obsahuje VBS script pro stahování dalších nástrojů k poměrně složitému spuštění škodlivého kódu. Nejvíce jsme ho pozorovali 6. listopadu a útok doznával ještě následující

dva dny. Tato podoba obálky, ve které se malware šíří k uživatelům, obecně nemá dlouhou životnost a složí pouze k jednorázovému využití,“ říká Jirkal a dodává: *„Při analýze škodlivého kódu jsme zjistili ještě jednu další zajímavost – v názvu e-mailové přílohy, jejímž prostřednictvím se Agent.RIK nejvíce šířil, útočníci použili speciální znak, který připomíná tečku, ale o tečku se nejedná. Tím se útočníci pravděpodobně snaží zmást samotné bezpečnostní programy, které se zaměřují na přípony e-mailových příloh.“*

Kromě nových hrozeb se i v listopadu objevil spyware Agent Tesla, a to tentokrát v pěti procentech případů. Spyware nejvíce útočil 17. listopadu a nejčastěji se ukrýval v e-mailových přílohách s názvy „2354878090658095444717750-044802-sanlccjavap0003-8881.exe“, „INVOICE & AWB #5291760_pdf.exe“ a „Zpusob_platby,jpg.exe“.

Bezpečnostní experti doporučují v případě ochrany před pokročilejšími škodlivými kódy vždy využívat kvalitní bezpečnostní programy a ty pravidelně aktualizovat, stejně jako operační systém celého zařízení. Škodlivý kód typu virus je známý již několik let, největším rizikem je ale pro neaktualizovaná a zastaralá zařízení.

„Na případech v Česku z letošního listopadu můžeme vidět, že útočníci mohou kdykoli zkusit znovu šířit typ malwaru, který je považovaný za dobře zmapovaný a svým způsobem již za zcela vymizelý. I když nepředpokládáme, že by se škodlivý kód mohl v našem prostředí udržet delší dobu, útočníci i přesto mohli uspět v případě špatně zabezpečených uživatelů,“ říká Jirkal z ESETu.

V případě, že bezpečnostní řešení rozpozná nákazu virem v zařízení opakovaně, bezpečnostní specialisté doporučují reinstalovat celý operační systém počítače a zároveň naformátovat všechny USB flash disky, které byly do počítače zapojeny. Kvalitní bezpečnostní řešení může zařízení přítomnosti viru zbavit také, zde však podle expertů záleží na typu použitého bezpečnostního programu.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-petine-vsech-detekovanych-pripadu-se-v-cesku-objevil-virus-delfnbx-rizikem-je-pro-neaktualizo