V březnu na sebe upozornil malware AsyncRAT, útočníci jeho prostřednictvím spustí i DDoS útok

19.4.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Nejvíce detekovaným škodlivým kódem pro operační systém Windows v Česku byl v březnu opět spyware Agent Tesla, přestože počet jeho detekcí oproti předchozímu období poklesl. Doplnil ho opět spyware Formbook. Ani jeden ze zástupců spywaru, který patří mezi největší rizika pro naše přihlašovací údaje, však necílil přímo na Česko. Na předních místech pravidelné statistiky se v březnu objevil také trojský kůň AsyncRAT. Uživatelé stáhnou tento malware většinou ve formě škodlivého programu, který může přes server útočníků posléze stahovat celou řadu doplňkových pluginů s různými škodlivými funkcemi. Ty mohou útočníkům napomáhat v krádeži našich údajů, monitorování našeho chování na internetu nebo jim pomoct s dalšími útočnými kampaněmi, například s útoky typu DDoS. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Zatímco spyware Agent Tesla v březnu utlumil svou aktivitu, spyware Formbook se nadále objevuje ve zhruba stejném objemu zachycených případů. V březnu se pak na předních místech statistiky nově objevil trojský kůň AsyncRAT.

„Spyware Agent Tesla se v březnu neobjevil v žádné větší útočné kampani a ani přílohy s názvy v češtině tentokrát nebyly výrazněji zastoupeny – v zachycených detekcích nejčastěji vidíme, že se útočníci stále snaží uživatele zmást přílohami s názvy poptávka nebo děkovný dopis. Jedná se však o případy, se kterými se mohli čeští uživatelé setkat již v minulých měsících. Spyware Formbook se objevil ve velké kampani z 11. března, ale i v jeho případě byly česky přeložené názvy příloh pouze ojedinělým jevem," shrnuje vývoj kybernetických hrozeb na platformě Windows v Česku Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Trojský kůň AsyncRAT je po malwaru Rescoms z minulého měsíce dalším novým škodlivým kódem na předních místech statistiky kyberhrozeb v Česku. Jedná se o běžného trojského koně typu RAT, tzv. Remote Access Trojan. Jakmile se jednou dostane do systému, umožní útočníkům nad ním získat vzdálenou kontrolu. Jeho zdrojové kódy jsou veřejně dostupné na internetu a každý si je tak může stáhnout a upravit si škodlivý kód pro své účely. Proto má tento malware řadu různých variant s různými funkcemi – pro krádeže citlivých údajů, monitorování našeho chování nebo zneužití našeho počítače k dalším útokům," dodává Jirkal.

Spyware Agent Tesla se v březnu nejčastěji objevoval v příloze „RFQ_C3682402292141.exe", v menším počtu také v přílohách „Poptavka 00413_pdf.exe" nebo „děkovný dopis.docx.exe". Spyware Formbook se nejčastěji ukrýval v příloze s názvem „RFQ RT1120 #10324.exe". Ani trojský kůň AsyncRAT se neobjevil v příloze s názvem v češtině – nejčastěji jsme na něj mohli narazit v příloze „BL109533.exe".

Trojský kůň AsyncRAT funguje v podobě základního programu, kterým útočníci infikují systém oběti. Program je pak závislý na serverech útočníků, z nichž stahuje moduly (pluginy) s různými funkcemi. Útočníci tak mohou stále vyvíjet nové funckionality a na dálku přes své servery je poskytovat základnímu škodlivému programu ke stažení.

„Trojský kůň AsyncRAT je nebezpečný právě rozsahem možných funkcí, které mohou útočníci

průběžně vyvíjet a svůj útok tak přizpůsobovat, aniž by museli znovu vymýšlet cesty, jak dostat škodlivý kód k uživatelům. Jednotlivé funkcionality se poté instalují prostřednictvím různých pluginů. Mezi základní funkce patří například vzdálené monitorování a zaznamenávání obrazovky našeho zařízení, nahrávání pomocí webkamery, manipulace se soubory, zaznamenávání stisků kláves na klávesnici nebo krádež hesel a souborů cookies z prohlížečů Chrome či Firefox," vysvětluje Jirkal.

Dále mohou pluginy trojského koně AsyncRAT obsahovat i pokročilé funkce pro komplexnější typy útoků. Mezi ně patří například spuštění .NET kódu, možnost těžit kryptoměnu XMR (Monero) nebo tzv. seedování torrentů, tedy šíření torrentu s účelem udržet ho dostupný ke stažení. Jednou z dostupných funkcí je ale také možnost spustit útok typu DDoS, který je například v posledním roce velmi častým typem útoku na veřejné instituce v České republice.

S ohledem na skutečnost, že se trojský kůň AsyncRAT šíří podobně jako spyware přílohami e-mailů, bezpečnostní specialisté uživatelům doporučují opatrně zacházet s příchozími e-mailovými zprávami. Obzvláště na pozoru by se měli mít před těmi, které přijdou bez předchozí komunikace z neznámé adresy a budou obsahovat jen strohé nebo žádné další informace. V takových e-mailech bychom nikdy neměli otevírat přiložené přílohy ani klikat na odkazy.

„Před pokročilejšími škodlivými kódy může uživatele a uživatelky vždy nejspolehlivěji ochránit především bezpečnostní software. Dnešní digitální komunikace je již tak všudypřítomná a probíhá v takovém objemu, že například zaměstnancům firem, kteří denně pracují s desítkami e-mailů obsahujícími různá obchodní potvrzení, se může bohužel stát, že jeden nebezpečný e-mail přehlédnou a domněle neškodnou přílohu otevřou. Dostatečně varovná by měla být i ta skutečnost, že trojského koně AsyncRAT stačí stáhnout do počítače jen jednou. Díky dodatečným pluginům pak mohou útočníci zahájit celou řadu škodlivých činností nebo zneužít váš počítač k dalším útokům až po nějaké době a na dálku. Obezřetnost je tak více než na místě," dodává Jirkal z ESETu.

Moderní bezpečnostní program nabízí uživatelům kromě klasické antivirové ochrany i celou řadu pokročilých funkcí a nástrojů. Chrání počítač nejen v reálném čase i před nejnovějšími hrozbami, ale může obsahovat i virtuální privátní síť VPN nebo správce hesel, specializovaný program, který hesla uchovává v zašifrované podobě a účinně je tak chrání před spywarem a password stealery.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

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 řešení od 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.

http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-breznu-na-sebe-upozornil-malware-asyncrat-utocnici-jeho-prostrednictvim-spusti-i-ddos-utok