Potvrzujete, že nejste robot? Falešné CAPTCHA šíří nebezpečný malware

1.11.2024 - | PROTEXT

Náš nedávný průzkum prostředí adwaru odhalil, že se tento škodlivý CAPTCHA šíří prostřednictvím různých internetových zdrojů, které nemají s hrami nic společného: stránek pro dospělé, služeb pro sdílení souborů, sázkových platforem, anime a webových aplikací, které vydělávají na návštěvnosti. To svědčí o rozšíření distribuční sítě s cílem oslovit širší okruh obětí. Experti Kaspersky navíc zjistili, že CAPTCHA šíří nejen Lummu, ale také trojského koně Amadey.

Škodlivé CAPTCHA v reklamních sítích

Abyste útočníkům nenaletěli, je důležité porozumět tomu, jak útočníci a jejich distribuční síť fungují. Reklamní síť, která stránky se škodlivou CAPTCHA protlačuje, obsahuje také legitimní, neškodné nabídky. Funguje to následovně: kliknutím kamkoli na stránku pomocí reklamního modulu je uživatel přesměrován na jiné zdroje. Většina přesměrování vede na webové stránky propagující bezpečnostní software, blokátory reklam a podobně – standardní postup pro adware. V některých případech však oběť přistane na stránce se škodlivým CAPTCHA.

Na rozdíl od pravých CAPTCHA určených k ochraně webových stránek před roboty slouží tato napodobenina k propagaci pochybných stránek. Stejně jako v předchozí fázi se oběť ne vždy setká s malwarem. Například CAPTCHA na jedné ze stránek vyzývá návštěvníka k naskenování QR kódu vedoucího na web sázkové kanceláře.

Trojské koně jsou šířeny prostřednictvím CAPTCHA s instrukcemi. Kliknutím na tlačítko Nejsem robot se do schránky zkopíruje řádek powershell.exe -eC bQBzAGgAdABhA<...MAIgA=">>MAIgA= a zobrazí se tzv. ověřovací kroky:

S podobnými pokyny se experti setkali i v jiných formátech než jen CAPTCHA. Například v okně, které je stylizované jako chybová hláška prohlížeče Chrome po neúspěšném načtení stránky. *Útočníci okno vydávají za chybu aktualizace prohlížeče a instruují uživatele, aby kliknul na tlačítko Kopírovat opravu*. Ačkoli se design stránky liší, scénář infekce je totožný se schématem CAPTCHA.

Řádek ze schránky obsahuje příkaz PowerShellu v kódování Base64, který získá přístup k zadané adrese URL a spustí obsah stránky. Uvnitř tohoto obsahu se nachází skrytý skript PowerShell, který nakonec stáhne škodlivý soubor.

Schovaný „dárek“: stealer Lumma

Škodlivý skript prostředí PowerShell nejprve stáhl a spustil archiv s programem Lumma.

Po spuštění spustí 0Setup.exe legitimní nástroj BitLockerToGo.exe, který je obvykle zodpovědný za šifrování a prohlížení obsahu vyměnitelných jednotek pomocí nástroje BitLocker. Tento nástroj umožňuje prohlížet, kopírovat a zapisovat soubory a také měnit různé větve registru – tuto funkci zloděj využívá.

Útočníci, vyzbrojeni nástrojem BitLocker To Go, manipulují s registrem především proto, aby vytvořili větve a klíče, které trojský kůň potřebuje ke své činnosti. Poté Lumma opět pomocí tohoto nástroje vyhledá v zařízení soubory spojené s různými kryptopeněženkami oběti a ukradne je.

Následně útočníci prohlížejí rozšíření prohlížeče související s digitálními peněženkami a kradou z nich data. Následně se trojský kůň pokusí ukrást soubory cookies uložené v různých prohlížečích.

Nakonec malware vyhledá archivy správců hesel, aby ukradl i jejich obsah. V průběhu celého procesu shromažďování dat se trojský kůň snaží opět využít nástroj BitLocker To Go k odeslání ukradených dat na server útočníků. Jakmile malware najde a exfiltruje všechna cenná data, začne navštěvovat stránky různých online obchodů. Účelem je pravděpodobně generování dalších příjmů pro jeho provozovatele zvýšením počtu zobrazení těchto webových stránek, podobně jako u adwaru.

Payload: Amadey Trojan

Stejná kampaň šíří také trojského koně Amadey. Ten je známý od roku 2018 a byl předmětem mnoha bezpečnostních zpráv. Lze říct, že trojský kůň stahuje několik modulů pro krádež přihlašovacích údajů z populárních prohlížečů a různých systémů pro virtuální síťové připojení (VNC). Zjišťuje také adresy kryptopeněženek ve schránce a nahrazuje je těmi, které ovládají útočníci. Jeden z modulů dokáže také pořizovat snímky obrazovky. V některých scénářích Amadey stáhne do zařízení oběti nástroj pro vzdálený přístup Remcos, čímž útočníci získají plný přístup k zařízení.

Statistiky

Od 22. září do 14. října 2024 se s reklamními skripty setkalo více než 140 000 uživatelů. Telemetrické údaje společnosti Kaspersky ukazují, že z těchto 140 000 uživatelů bylo více než 20 000 přesměrováno na infikované stránky, kde se některým z nich zobrazilo falešné oznámení o aktualizaci nebo falešná CAPTCHA. Nejčastěji byli postiženi uživatelé v Brazílii, Španělsku, Itálii a Rusku.

https://www.ceskenoviny.cz/tiskove/zpravy/potvrzujete-ze-nejste-robot-falesne-captcha-siri-nebezpecny-malware/2589852