Malware StripedFly má na svědomí už víc než milion obětí, informuje Kaspersky

3.11.2023 - | PROTEXT

V roce 2022 se globální výzkumný a analytický tým (GReAT) společnosti Kaspersky setkal se dvěma neočekávanými detekcemi v procesu WININIT.EXE, které byly vyvolány sekvencemi kódu nalezenými předtím v malwaru Equation.

Příčinou byl StripedFly, jehož aktivity probíhaly nejméně od roku 2017 a účinně se vyhýbaly předchozím analýzám, protože byl dříve nesprávně klasifikován jako těžař kryptoměn. Po komplexním prozkoumání problému se ukázalo, že těžba kryptoměn je pouze součástí mnohem většího celku – komplexního škodlivého víceúčelového frameworku s mnoha doplňky.

Tento malware obsahuje několik modulů, které mu umožňují působit jako pokročilá trvalá hrozba (APT), těžař kryptoměn, a dokonce jako ransomware, což rozšiřuje potenciální motivy útočníků od finančního prospěchu až po špionáž. Je zajímavé, že kryptoměna Monero těžená jedním z modulů dosáhla 9. ledna 2018 své nejvyšší hodnoty 542,33 USD, zatímco v roce 2017 činila asi jen 10 USD. Od roku 2023 si udržuje hodnotu kolem 150 USD. Odborníci společnosti Kaspersky zdůrazňují, že těžební modul je hlavním faktorem, který malwaru umožňuje unikat detekci po delší dobu.

Útočník, který stojí za touto operací, získal rozsáhlé možnosti tajného špehování obětí. Škodlivý software krade a shromažďuje každé dvě hodiny citlivé informace, například přihlašovací údaje k webům a Wi-Fi sítím nebo osobní údaje, jako jsou jméno, adresa, telefonní číslo, zaměstnání a pracovní pozice. Kromě toho může malware na zařízení oběti nepozorovaně pořizovat snímky obrazovky, získat významnou kontrolu nad počítačem, a dokonce nahrávat vstupy z mikrofonu.

Původní přenašeč infekce zůstával neznámý, dokud vyšetřování společnosti Kaspersky neodhalilo, že využívá zranitelnost EternalBlue. Přestože je známá od roku 2017, je stále významná, protože mnoho uživatelů svoje systémy neaktualizovalo. Podle počítadel stažení, dosáhl odhadovaný počet cílů StripedFly více než jednoho milionu obětí po celém světě.

„Na vytvoření tohoto malwarového frameworku bylo vynaloženo opravdu pozoruhodné úsilí a jeho odhalení bylo dost velkým překvapením. Schopnost aktérů hrozeb přizpůsobovat se a vyvíjet další škodlivé aktivity je neustálou výzvou, a proto je pro nás jako výzkumníky tak důležité, abychom se i nadále věnovali odhalování a blokování šíření sofistikovaných kybernetických hrozeb a aby zákazníci nezapomínali na komplexní ochranu,“ říká **Sergey Lozhkin**, hlavní bezpečnostní výzkumník z globálního výzkumného a analytického týmu společnosti Kaspersky.

Abyste se nestali obětí cíleného útoku známého nebo neznámého aktéra hrozeb, doporučují výzkumníci společnosti Kaspersky následující opatření:

http://www.ceskenoviny.cz/tiskove/zpravy/malware-stripedfly-ma-na-svedomi-uz-vic-nez-milion-obeti-informuje-kaspersky/2435798