Experti Kaspersky Lab objevili v trojském koni Duqu neznámý programovací jazyk

Společnost žádá programátorskou komunitu o pomoc

Odborníci společnosti Kaspersky Lab zjistili, že část trojského koně Duqu je napsána v neznámém programovacím jazyce. Duqu je propracovaný trojský kůň, za jehož vznikem stojí titíž lidé, kteří vytvořili nechvalně proslulého červa Stuxnet. Duqu slouží primárně jako zadní vrátka do napadeného systému, čímž usnadňuje následné krádeže důvěrných informací. Samotný virus byl poprvé detekován v září 2011, avšak podle údajů společnosti Kaspersky Lab lze působení malwaru spojeného s Duqu vystopovat již v srpnu 2007.

Odborníci antivirové společnosti zaznamenali více než tucet napadení virem Duqu, přičemž většina jeho obětí se nachází v Íránu. Z výsledků analýzy činností napadených společností a povahy informací, na něž se Duqu zaměřil, vyplývá, že hlavním cílem útočníků byla krádež informací o průmyslových řídicích systémech využívaných v řadě různých odvětví a sběr tajných informací o obchodních vztazích mnoha íránských organizací.

Velkou záhadou dosud zůstává, jak trojský kůň Duqu komunikoval se svými řídicími (command and control – C&C) servery po infikaci cílového zařízení. Součást Duqu zajišťující interakci s C&C servery se nachází v Payload DLL. Komplexní analýza výzkumníkům společnosti Kaspersky Lab odhalila, že jedna konkrétní část Payload DLL, která komunikuje výhradně s C&C servery, je napsána v neznámém programovacím jazyce. Výzkumníci tuto neznámou část pojmenovali „Duqu Framework".

Na rozdíl od zbytku viru Duqu není část Duqu Framework napsána v C++ a nebyla kompilována v programu Visual C++ 2008 společnosti Microsoft. Je možné, že tvůrci viru vygenerovali intermediární C kód za použití vlastního systému, ale mohli také použít úplně jiný programovací jazyk. Výzkumníkům společnosti Kaspersky Lab se podařilo potvrdit, že objevený jazyk je objektově orientovaný a sám vykonává soubor činností vhodných pro síťové aplikace.

Jazyk použitý v Duqu Framework je vysoce specializovaný. Umožňuje, aby část Payload DLL fungovala nezávisle na ostatních částech viru Duqu a propojuje ji s dedikovaným C&C serverem několika různými cestami, mimo jiné prostřednictvím Windows HTTP, socketů a proxy serverů. Payload DLL díky speciálnímu jazyku může navíc zpracovávat HTTP požadavky C&C serveru přímo, tajně odesílat kopie ukradených informací z infikovaného zařízení na C&C server a dokonce i šířit škodlivý datový obsah na ostatní zařízení v síti. To umožňuje řízené a utajené šíření infekcí na další počítače. Kompletní popis analýzy a související údaje najdete v blogovém postu na stránce společnosti Kaspersky Lab Securelist.

Společnost Kaspersky Lab se tímto obrací na programátorskou komunitu s žádostí o pomoc a zároveň by ráda vyzvala každého, kdo zná framework, toolkit nebo programovací jazyk schopný generovat podobné instrukce, aby zkontaktoval její odborníky.

O společnosti Kasperky Lab
Kaspersky Lab je největším poskytovatelem antivirových řešení v Evropě. Společnost nabízí jedny z nejúčinnějších bezpečnostních prostředků proti IT hrozbám, které jejím zákazníkům zajišťují ochranu před počítačovými viry, spywarem, crimewarem, hackery, phishingem a spamem. Společnost se řadí mezi čtyři celosvětově nejvýznamnější poskytovatele bezpečnostních řešení pro koncové uživatele. Produkty společnosti se díky vysoce účinné detekci hrozeb a téměř bezkonkurenčně rychlým odezvám na akutní ohrožení řadí mezi špičku na trhu s bezpečnostním software pro domácí uživatele, malé a střední podniky i velké společnosti a mobilní výpočetní technologie. Technologie Kaspersky jsou součástí řady produktů a služeb dodávaných předními poskytovateli IT zabezpečovacích řešení po celém světě.

Více informací o společnosti Kaspersky Lab najdete na www.kaspersky.com. Nejnovější informace o antivirových, antispywarových, antispamových a dalších bezpečnostních řešeních, problémech a trendech naleznete na www.securelist.com.

Pro další informace prosím kontaktujte:
Štěpán Kačena
PR Consultant
Grayling
Tel.: 224 251 555
Mobil: 774 226 127
stepan.kacena@grayling.com