Kybernetičtí zločinci úspěšně vydírají i v Česku

Ze 40 tisíc obětí vyděračů a jejich malware TorrentLocker připadá na Českou republiku 3500 zašifrovaných počítačů. 28 obětí v Česku zaplatilo za šifrovací klíče výkupné.

Bezpečnostní experti ESET prezentovali detailní analýzu rozsáhlého případu internetového zločinu, kdy vyděrači zašifrují soubory na počítači a požadují výkupné za šifrovací klíče. Jde o postupně zdokonalovaný malware TorrentLocker, který od jara 2014 infikoval na 40 tisíc počítačů, převážně v Evropě. Analýza provozu řídících serverů botnetu TorrentLocker umožnila zjistit o této vyděračské kampani detailní informace.

Malware TorrentLocker zašifroval na infikovaných počítačích (resp. na všech jejich připojených diskových jednotkách) přes 525 milionů souborů, za jejichž dešifrování požaduje gang vyděračů výkupné. Výkupné zaplatilo pouze 570 obětí; i tak si vyděrači přišli na v přepočtu víc než 580 tisíc dolarů.

V Česku se obětí TorrentLockeru stalo 3420 počítačů, na nichž bylo zašifrováno 35 milionů souborů. Vyděračům zaplatilo 28 obětí z Česka - v průměru to bylo v přepočtu téměř 22 tisíc korun, celkem 611 tisíc korun.

Analytici ESET zjistili, že zločinci průběžně inovují jak samotný malware, tak metody, jimiž pracují. Například první verze malware používala jednodušší šifrování, které bylo možné obejít. Poté, co některé bezpečnostní firmy prezentovaly službu, která obětem TorrentLockeru jejich soubory zdarma dešifrovala, zločinci přešli na dokonalejší šifrovací metodu CBC (Cipher block chaining). V důsledku toho je zaplatit výkupné opravdu jedinou možností, jak se k zašifrovaným datům dostat. Zdokonalení se dočkala i komunikace o zaplaceném výkupném. Zatímco oběti prvních vln útoků musely informovat vyděrače mailem a mailem také putovaly šifrovací klíče, v další fázi byl tento proces plně automatizován.

TorrentLocker se šíří s využitím elektronické pošty. Oběť dostane email, který obsahuje buď škodlivou přílohu, nebo link na stránku, odkud si má škodlivý kód stáhnout. Záminky jsou ve všech případech podobné: jde o upozornění na údajný balík na cestě, na údajně nezaplacenou fakturu nebo pokutu a podobně.

TorrentLocker je sice funkčně velmi podobný neméně obávanému malware CryptoLocker, ale analytici ESET zjistili, že za ním se vší pravděpodobnosti stojí jiný gang – ten, který má na svědomí úspěšný bankovní malware Hesperbot. Nejen, že hlavními terči byly v obou případech Turecko, Austrálie a Česká republika; tyto škodlivé kódy používají stejné adresy řídících serverů, sdílí části programového kódu a dokonce nejspíš byly zkompilovány na tomtéž počítači.

O společnosti ESET

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software, který drží rekordní počet ocenění a díky němuž může víc než 100 milionů uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy a nabízí firmám i spotřebitelům maximální proaktivní ochranu při minimálních nárocích.

Jedno ze tří evropských výzkumných center ESET pro detekci malware je v Praze. Společnost ESET má celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 180 zemích světa.

ESET software spol. s r.o.
Sídlo a fakturační adresa: Classic 7 Business Park, Jankovcova 1037/49, 170 00 Praha 7, Česká republika
IČ: 26467593 – DIČ: CZ26467593 – číslo účtu: 51-2451350287/0100 – IBAN: CZ46 0100 0000 5124 5135 0287

ESET software spol. s r.o. je zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, oddíl C, vložka 84196
tel.: +420 233 090 260 – fax: +420 233 090 230 – www.eset.cz

Kontakt pro média:

Petr Blažek
petr.blazek@taktiq.com