Vážené čtenářky, vážení čtenáři,

v uplynulých měsících jsme byli svědky doslova husarského kousku, který se povedl strážcům zákona při mezinárodní akci. Odstřihli totiž Emotet, jeden z největších botnetů na světě. Zda to ale bude trvalé, se teprve uvidí.

Akce se zúčastnili odborníci a policejní orgány z Nizozemska, Německa, Spojených států, Velké Británie, Francie, Litvy, Kanady a Ukrajiny, přičemž mezinárodní činnost koordinovaly Europol a Eurojust, hlavní zatýkání podezřelých se uskutečnilo na Ukrajině.

Emotet je letitá síť nekalých botů (v provozu je už od roku 2014), v posledních měsících ale byla nejčastěji detekovanou skupinou malwaru. Činnost Emotetu začínala s trojanem zaměřeným na krádeže spojené s on-line bankovnictvím, postupem času se ale Emotet vyvinul do platformy malwaru jako služby, kterou používají i jiné zločinecké skupiny pro distribuci vlastního škodlivého kódu nebo pro získání přístupu k infikovaným počítačům.

Emotet provozuje skupina hackerů označovaná jako TA542. Jedním z jejích klíčových klientů jsou například provozovatelé TrickBotu, což je další botnet specializující se na distribuci ransomwaru Ryuk. Sám TrickBot sice po loňské akci, kterou organizoval Microsoft, dostal velkou ránu, ale zcela jej to nepoložilo. Na Emotet spoléhají i tvůrci malwaru Qbot.

Emotet ke své záškodnické činnosti primárně využívá nevyžádané e-maily, které pomocí sociálního inženýrství přimějí uživatele k otevírání dokumentů Wordu se škodlivými makry, nakažených souborů PDF nebo adres URL, které vedou k infikovaným souborům.

Provozovatelé Emotetu podle expertů využívají pokročilé techniky ke zvýšení své šance na úspěšnou kompromitaci, jako třeba threat hijacking, kdy podvržené e-maily představují odpověď na legitimní konverzaci, kterou trojan ukradl z infikovaných počítačů, nebo oslovení příjemců pravým jménem včetně jejich pracovních titulů a názvů společností v předmětu zprávy.

Podle Europolu se infrastruktura Emotetu skládala z několika stovek serverů rozmístěných po celém světě a sloužících různým účelům včetně zvyšování odolnosti botnetu vůči zablokování. Policejní orgány potvrdily strategii, která zahrnovala mj. i získání kontroly nad infrastrukturou Emotetu zevnitř. Informace o infikovaných počítačích, které byly shromážděné během operace, se sdílejí s národními týmy CERT, aby bylo možné identifikovat a kontaktovat oběti.

Podle odborníků je ale otázka, zda se Emotet skutečně podaří plně zablokovat. Tyto skupiny hackerů jsou totiž velmi sofistikované a určitě budou usilovat o nějaký druh obnovy činnosti. Samotný Emotet prý sice nemá žádný vlastní mechanismus obnovy, ale na mnoha infikovaných počítačích bude i nadále nainstalovaný další malware, například Qbot, Trickbot nebo něco jiného – a ty by mohly sloužit jako způsob, jak obnovit infikované boty a stáhnout je zpět pod kontrolu.

Také členové skupiny rozmístění po celém světě mohou zdrojový kód použít k pokusu o opětovné vytvoření botnetu. I když utrpěli velkou finanční ránu, stále se mohou například dohodnout s provozovateli jiných botnetů na spolupráci, která by mohla vyústit v obnovu Emotetu. A pokud se jim to nepovede, jistě se najde celá řada dalších následovníků, kteří se pokusí „díru na trhu" rychle zaplnit.

Takže i když eliminace Emotetu je bezesporu velkým úspěchem vynucování práva, z praktického hlediska může jít jen o dočasné zbrzdění nekalých aktivit hackerů. A s tím je potřeba při stanovení podnikových bezpečnostních strategií nadále počítat.

S přáním příjemně stráveného jara (konečně se světélkem na konci covidového tunelu)

Pavel Louda
vedoucí projektu

Obsah