A kiberbűnözés lassan a szoftveripar egyik ágává nő

És olyan károkat okoz, melynek nagysága összemérhető a világ teljes IT-kiadásával – írja Csizmazia Darab István IT-biztonsági szakértő.

Döbbenetes jóslat egy amerikai kutatócégtől, a Cybersecurity Venturestől: 2021-re a kiberbűnözéssel kapcsolatos globális kiadások teljes összege elérheti a 6 ezermilliárd dollárt, miközben 2015-ben még csak 3 ezermilliárd volt. Az összeget érdemes összevetni azzal, hogy a Gartner előrejelzése szerint 2019-re a teljes globális IT-kiadások nem érik el a 4 ezermilliárd dollárt.

Ez a növekedés összefügg a kiberbűnözők stratégiaváltásával. Ma már nem kell szakértelem egy támadás végrehajtásához, mert minden szükséges eszköz megvásárolható hozzá a sötét weben – írja *Csizmazia Darab István* IT-biztonsági szakértő egy ESET-tanulmány kapcsán a blogján. Az alábbiakban az ott megjelent cikk szerkesztett változatát közöljük.

Zombihálózatot tessék!

A kiberbűnözés már 2015-ben is 3 ezermilliárd dollár (860 ezermilliárd forint) kiadást jelentett világszerte, és az előrejelzések szerint ez az összeg 2021-re 6 ezermilliárdra emelkedik. Ez természetesen becslés, és minden olyan költséget tartalmaz, amelyet az incidensek generálnak. Például egy zsarolóvírus esetében nem csak a váltságdíj kifizetését, hanem a számítógépek mentesítésének, újratelepítésének, a biztonsági szabályozás javításának és a szükséges technológiai védelmi beruházásoknak a költségeit is. Emellett forintosítja a termeléskiesés vagy termelékenységcsökkenés okozta veszteséget és a reputációs károkat. Ha becslésről is van szó, arra mindenképpen felhívja a figyelmet, hogy egy IT-biztonsági incidens hatása messze túlmutat az IT-n.

A kiberbűnözők ma már szofisztikált háttérrendszerre, szolgáltatások sorára tudnak támaszkodni támadásaikban. Hogy mi érhető el a sötét weben, arról évek óta próbálnak a biztonsági kutatók pontos képet kapni. A közelmúltban az ESET elemzői is készítettek egy összeállítást a az elérhető termékekről, szolgáltatásokról és azok árairól.

A skála széles. Zsarolóvírusok éppúgy kaphatók, mint bontnetek. Ahogy a legális szoftverek esetében, itt is vannak rendszeres frissítések, technikai támogatás, valamint távoli vezérlő szerverekhez (C&C) való hozzáférés és számos fizetési lehetőség.

A Ranion oldalain például kínálnak mindenféle szolgáltatást és kártevőt. Az oldalon az egyik zsarolóvírus például havi vagy éves előfizetéssel is elérhető – és sajnos egyre alacsonyabb árakon. A legolcsóbb, egy hónapra szóló csomag például alig 120 dollár (körülbelül 33 ezer forint), míg a legdrágább, egy évre szóló előfizetés sem kerül többe 900 dollárnál (cirka 250 ezer forint). Ezek azonban csak az alapszolgáltatás díjai, az árak a külön megvásárolható kiegészítő szolgáltatások fényében akár 1900 dollárig is felmehetnek. Egy másik fizetési modellben a vásárlók magát a kártevőt és a C&C infrastruktúrát ingyen kapják, de a beérkező váltságdíjakból részesedést kér az eladó (így működik a Jokeroo).

Sok múlik az infrastruktúrán

Bármelyik megoldást választják a támadók, a vírusokat terjeszteniük kell, azaz el kell jutniuk áldozatokig, például spamekkel vagy sérülékeny szerve-

reken, RDP-n (Remote Desktop Protocol) keresztül. Ma már erre is számos szolgáltatást vehetnek igénybe. Például van olyan, amely kifejezetten hitelesítő adatokat árusít a világ különböző részein lévő szerverekhez RDP segítségével. Az árak 8–15 dollár között mozognak szerverektől és országoktól függően. Az érdeklődők kereshetnek operációs rendszer szerint, illetve az alapján is, hogy melyik fizetési oldal felhasználóinak van hozzáférése az adott szerverhez.

A „szolgáltató” részletes adatokat ad ilyenkor a szerverekről: a bűnöző például lekérheti a szerverek fizikai helyét, IP-címét, az operációs rendszer verzióját, a feltöltési-letöltési sebességet, sőt még azt is, hogy mikor került bele a „szolgáltató” kínálatába. Így könnyebben dönthet, hogy melyikhez vásárol hozzáférést zsarolóvírus futtatása vagy más, diszkrétebb kártevők, például banki trójai vagy kémprogramok telepítése céljából.

Hasonlóképpen egyre többen foglalkoznak botnetek bérbeadásával spamterjesztésre vagy DDoS támadások végrehajtására. A DDoS támadásnál az árazás a támadás időtartamának, és a botnet által generált forgalom nagyságának a függvénye. Az árak itt is pár tíz dollártól kezdődnek, azaz kisebb támadást már lényegében fillérekből el lehet indítani.

Itt megfigyelhető egy új jelenség: egyre több olyan fiatal jelenik meg a piacon, aki kis botnet hálózatot ad bérbe, főként a Fortnite-hoz hasonló online játékok által használt szerverek támadására. Az ilyen „kézműves” botneteket a közösségi médiában népszerűsítik, és sokszor még arra sem ügyelnek, hogy névtelenek maradjanak.

Bér-adathalászok kora

Szintén egyre általánosabb, hogy különválik az adathalász tevékenység és az adatok felhasználása. A sikeres adathalász támadásokat futtató kiberbűnözők általában nem akarnak újabb kockázatot vállalni azzal, hogy fel is használják az ellopott fiókokat. Ha kisebb is a nyereség, sokkal biztonságosabb, ha a számlákat más bűnözőknek értékesítik.

Az árak itt az elérhető pénzügyi nyereség függvényében alakulnak, például egy hitelkártya adataihoz a hitelkeret 10 százalékáért lehet hozzájutni. A „bértolvajok” legfeljebb ott vállalnak kockázatot, amikor bemutatják referenciaként eszközeiket és azokat a hamis oldalakat, amelyeket az adathalászatra használnak.

Összességében a trend az, hogy egyre kiterjedtebb ez az iparág. Van marketing, amely a termékeket népszerűsíti megfelelő körökben, van ügyfélszolgálat, amely segíti a felhasználókat, a kártevőkhöz jár felhasználói kézikönyv és frissítés – akárcsak a hagyományos IT-üzleteknél.

És az üzlet virágzik is, egyre több a vevő. Az igazi nyereséget azonban ma már egyre kevésbé a támadást végrehajtók teszik zsebre. A nagy üzletet a kiterjedt infrastruktúrával és a jól működő szolgáltatásokkal rendelkező nagy halak realizálják az általuk kínált szoftverek, termékek és szolgáltatások értékesítéséből.

(A szerző az ESET megoldásait forgalmazó Sicontact Kft. munkatársa.)

Erről is hallhat május 9–10-én a jubileumi CIO Hungaryn!

A nagyvállalati IT-biztonság témája is terítékre került 10. CIO Hungary konferencián

Forrás: https://bitport.hu/a-kiberbunozes-lassan-a-szoftveripar-egyik-agava-no

Válogatta: Fonyó Istvánné