ALISON

# Európski úradníci nemali zľutovanie. Najvyššia pokuta podľa GDPR dosiahla takmer 200 miliónov eur.

Možno nepoznáte Magecart, ale veľkú časť sveta už zabolelo, čo robia. Magecart je zoskupenie sofistikovaných hekerských skupín, ktoré stojí za najväčšími hekerskými akciami uplynulých rokov od British Airways po Ticketmaster. Vo všetkých prípadoch bolo jediným cieľom získať čísla kreditných kariet, a preto ho odborníci označili za webový ekvivalent bankomatového skimeru.

Ničivá sila kódu Magecart sa v júli ukázala v plnom svetle, keď následne na smernicu GDPR dostala letecká spoločnosť British Airways pokutu viac 183 miliónov GBP za zanedbanie ochrany svojej webovej infraštruktúry. Útok Magecart v roku 2018 viedol k odcudzeniu osobných údajov približne pol milióna zákazníkov spoločnosti. Pokuta, ktorú dostala letecká spoločnosť, prevýšila tú za dátový únik hotelovej siete Marriot a spoločnosti Google. Dnes už tieto bezpečnostné incidenty slúžia ako učebnicový príklad kybernetickej bezpečnosti.

Do mája 2018 bola maximálna pokuta za porušenie ochrany osobných údajov v pomeroch Spojeného kráľovstva 500-tisíc GBP, takže prvá „veľká“ pokuta udelená podľa smernice GDPR pre Marriot bola dvestonásobne vyššia ako táto hranica.

Predstavitelia veľkých spoločností formálne vyjadrili podporu tejto aktivite európskych úradníkov, ale ako sa objavilo v niektorých vyhláseniach, „súcitíme s tými, ktorých postihol taký masívny externý kybernetický útok. Navyše, keď nikto zo zákazníkov British Airways nebol doteraz finančne poškodený.“

Vďaka nedostatočnej bezpečnostnej prevencii sa totiž zoskupeniu Magecart podarilo zaútočiť len za posledných pár mesiacov na 17-tisíc domén. Medzi postihnutých patrí aj dvetisíc najväčších spoločností na svete vrátane internetového obchodu Amazon.

Bezpečnostná firma RiskIQ opísala spôsob, akým hekeri Magecart nazerajú na úložiská v cloudovom systéme Amazon S3 (tzv. kýbliky – buckets). Úložiská obsahujú nielen dáta, ale aj ďalšie podprogramy na prevádzku webových stránok, pričom niektoré sú nesprávne nakonfigurované. V prípade málo zabezpečených sekvencií ktokoľvek s prístupom k účtu Amazon Web Services dokáže nielen čítať obsah, ale do úložiska aj zapisovať. V prípade internetových obchodov tak hekeri vkladajú kód, ktorý kradne čísla kreditných kariet.

Keď hekeri narazia na nezabezpečené úložisko S3, hľadajú na ňom akékoľvek súbory s JavaScriptom. Nastavenia umožňujú komukoľvek do súboru doplniť nový kód, takže útočníci len prilepia svoj malvér Magecart k súboru a prepíšu pôvodný skript na úložisku.

ALISON

V máji Magecart zmenil taktiku.  Kým predchádzajúce útoky boli jasne zacielené, skupiny patriace do Magecartu tentoraz išli metódou čo najširšieho pokrytia. Rozhodili siete a pozmenili kódy veľkého počtu webových stránok vrátane aj tých, ktoré nepredávajú tovar na internete. Počítali s tým, že sa im tento prístup oplatí a „odchytia“ dosť webov, ktoré zhromažďujú dáta z platobných kariet.

V súčasnosti sa všetci hromadne snažia zistiť, ktoré buckety S3 boli nesprávne nakonfigurované. Digitálne kartové skimmery Megacart sa objavujú doslova všade.

Útoky zaznamenalo do konca júla 17-tisíc domén a ich počet stále rastie. Mnohé z napadnutých webov však nerealizujú žiadne transakcie s kreditnými kartami, takže kód Magecart sa nedokáže uplatniť. Tiež sa nevie, koľko úložísk S3 bolo reálne napadnutých, pretože viacero domén môže využívať rovnaké úložisko. Bezpečnostné firmy upozorňujú administrátorov napadnutých webov, hľadajú ďalšie obete a svoj čas si vyžiadajú aj príslušné úpravy backendu.