ALISON

Útočilo sa rýchlo a zbesilo. A ako ďalej v kyberbezpečnosti?

***** Kybernetické útoky pribúdajú z hľadiska vektorov, čísel aj vzhľadom na ich vplyv *** Toto nás môže dostihnúť budúci rok *** Nová kategorizácia hrozieb pre Európu**

Svet je v ostatnom roku svedkom zlepšovania techník a taktík kybernetických zločincov. Neboja sa útokov na akýkoľvek cieľ a nemajú žiadne morálne zábrany. Útoky na zdravotnícke zariadenia to len potvrdzujú. Každých 11 sekúnd sa vo svete udeje ransomvérový útok.

Ofenzívne operácie budú vyžívať technológie

Štáty na seba útočia kyberneticky a už sa tým ani netaja. Jedným z úspešných modelov je aj vytvorenie startupovej spoločnosti v sieti krycích alebo existujúcich technologických spoločností. Spoločnosti sú následne zapojené do operácií riadených a kontrolovaných ministerstvami alebo spravodajskými službami.

Aj štáty použijú sociálne médiá ako zbraň

Kybernetickým zločincom neunikla popularita sociálnych médií. Naopak. Zameriavali sa na zamestnancov firiem, ktorým posielali zaujímavé pracovné ponuky. Priame správy tak jednoducho používali na ovládnutie účtov ich používateľov.

Cielenie na jednotlivcov sa kybernetickým zločincom osvedčilo natoľko, že odborníci predpokladajú využitie tohto vektora útoku špionážnymi skupinami aj inými aktérmi hrozieb, ktorí sa snažia infiltrovať do organizácií.

Nebezpečné a čoraz vyššie výkupné

Ransomvér zostáva jednou z najvplyvnejších kybernetických hrozieb. Počet útokov vo svete za covidové obdobie vzrástol o štyristo percent. Odborníci odhadujú, že škody do konca roku 2021 dosiahnu 21 miliárd dolárov. Takmer polovica výkupného bola platená v bitcoinoch, keďže táto mena garantuje útočníkom najväčšiu anonymitu. V roku 2022 sa očakáva, že počty skupín kybernetického zločinu budú rásť.

Vojna o ramsomvérové tróny

Služba ransomware as a service (RaaS) umožnila vykonávať útoky aj menej kvalifikovaným aktérom hrozieb. Moc sa presunie „od tých, ktorí kontrolujú ransomvér, do rúk tých, ktorí kontrolujú siete obetí“. Služba RaaS urýchlila vybudovanie nového biznisového modelu vo svete kybernetického zločinu. Zatiaľ čo spočiatku kontrolovali situáciu vývojári ransomvéru, trh sa rozrástol. Menej kvalifikovaní aktéri hrozieb podporujú kúpou ransomvéru vybraných vývojárov, ktorí získavajú čoraz väčšie zisky.

ALISON

Zero-day zraniteľnosti viac ako kedykoľvek

Rok 2021 bol takmer šokujúci, pokiaľ ide o počet zero-day zraniteľností zneužitých kybernetickými zločincami. Nájdených a hlásených bolo 66 zero-day zraniteľností, čo je takmer dvojnásobok celkového počtu za rok 2020 a viac ako v ktoromkoľvek inom zaznamenanom roku.

Pozornosť bezpečnostných expertov sa preto sústreďuje najmä na zraniteľnosti najrozšírenejších operačných systémov a platforiem. A dobrá správa pre profesionálnych hackerov – odmeny v bug bounty programoch sú čoraz vyššie.

Rozhrania sú vždy citlivé

Aktéri hrozieb pozorne monitorujú firemné trendy a štatistiky a hľadajú nové služby alebo aplikácie, ktoré by mohli zneužiť. To sa vzťahuje najmä na cloudové aplikácie a API rozhrania. Dosah a popularita z nich robia lukratívne ciele. Práve zabezpečenie API zabraňuje škodlivým útokom na rozhrania alebo ich zneužitiu.

Nový cieľ pre hijacking

Kontajnery sú často platformou pre moderné cloudové aplikácie. Sú prenosné, efektívne a modulárne, čím urýchľujú čas potrebný na nasadenie a správu aplikácií. Ak aktéri hrozieb využijú zraniteľnosti, môže to viesť až k hijackingu koncových zdrojov. Takže pojem hijacking, ktorý sa pôvodne používal na označenie únosov, nadobúda v dobe cloudu prenesený význam na ovládnutie infraštruktúry alebo zariadení.

Európa to vidí takto

Agentúra EÚ pre kybernetickú bezpečnosť ENISA identifikovala osem hlavných skupín kybernetických hrozieb, pričom výber vychádzal z ich dôležitosti, popularity a vplyvu počas rokov 2020 a 2021. ENISA zároveň identifikovala trendy v európskom priestore a vytvorila novú kategorizáciu hrozieb.

1. Ransomvér

Hlavná hrozba počas pre európske inštitúcie a firmy počas obdobia apríl 2020 až jún 2021 a mimochodom aj najčastejšia téma v médiách v súvislosti s kauzami kyberbezpečnosti. Koniec je zatiaľ v nedohľadne.

2. Malvér

Štatistická krivka, ktorá už hlásila klesajúci trend, začína stúpať. Aktéri sa uchyľujú k relatívne novým alebo nezvyčajným programovacím jazykom na prenos kódu.

ALISON

3. Cryptojacking

Alebo aj cryptomining attack. Typ kybernetického zločinu, pri ktorom zločinec využíva výpočtové kapacity obete na ťažbu kryptomien bez jej súhlasu, dosiahol v prvom kvartáli roku 2021 rekordné čísla.

4. Hrozby súvisiace s e-mailom

V kampaniach stále dominuje pandémia ochorenia COVID-19. Útoky rafinovane zneužívajú slabé miesta v ľudskej psychike, nemajú technickú podstatu. Aj napriek rastúcej osvete v kybernetickej bezpečnosti hrozba stále pretrváva.

5. Hrozby voči údajom

Hrozba je stále vysoká, keďže prístup k údajom je hlavným cieľom útočníkov. Mať údaje znamená príležitosť na vydieranie, výkupné, ohováranie či dezinformácie.

6. Hrozby voči dostupnosti a integrite

Tu si konštantne zachovávajú miesto v rebríčku hrozieb DDoS a webové útoky, ktoré sa stávajú čoraz brutálnejšie. Sú kvalitne cielené a masívne. Nedostupnosť údajov a služieb sú kritickým faktorom.

7. Dezinformácie a nepravdivé informácie

Táto kategória hrozieb sa v reporte ENISA zjavila prvýkrát. Dezinformačné kampane sú na vzostupe a ťažia z rastu vplyvu sociálnych médií a online komunikácie. Tieto kampane sa často používajú pri hybridných útokoch na zníženie dôvery voči zástancom kybernetickej bezpečnosti či relevantným inštitúciám.

8. Neúmyselné hrozby

Väčšinou sú založené na ľudských chybách a nesprávnej konfigurácii systému. Pandémia a práca z domu zvýšili početnosť aj podiel týchto hrozieb na incidentoch. Neúmyselné hrozby však môžu súvisieť aj s prírodnými katastrofami, ktoré majú dosah na infraštruktúru.

9. Útoky na dodávateľský reťazec

Oblasť, ktorej bude Únia venovať najviac pozornosti vzhľadom na potenciálne likvidačné následky. Pre kybernetických zločincov sú hodnotnými cieľmi najmä poskytovatelia riadených služieb.

Zdroj

Agentúra EÚ pre kybernetickú bezpečnosť ENISA: Threat Landscape 2021, apríl 2020 – júl 2021
McAfee v spolupráci so spoločnosťou FireEye: Predikcie kybernetických hrozieb pre firmy na rok 2022
Cybersecurity Venture: Global Ransomware Damage Cost
MIT Technology Review: 2021 has broken the record for zero-day hacking attacks