ALISON

Ako si plánujú rok hackeri sponzorovaní štátmi? Zdá sa, že bude veľa práce

- Nový rok, nové ciele
- Prémiové štáty a segmenty
- Tretia najsilnejšia ekonomika

Zatiaľ čo akademici vedú diskusie o tom, ako definovať a používať pojem kybernetická vojna, mnoho štátov vrátane USA, Spojeného kráľovstva, Ruska, Indie, Pakistanu, Číny, Izraela, Iránu a Severnej Kórey vlastní aktívne kybernetické kapacity pre útočné a obranné operácie.

Bezpečnostná udalosť roka 2020 a možno aj storočia

Koncoročné udalosti v kybernetickej bezpečnosti boli také závažné a sofistikované, že otriasli piliermi celého biznisu. Začalo sa to, keď FireEye, jedna z najvyhlásenejších bezpečnostných firiem, potvrdila, že rozsiahly decembrový kybernetický útok cielil na informácie o ich klientoch. Menej diplomaticky povedané, išlo o špionáž. Ako spoločnosť uviedla, predpokladá, že takto sofistikovaný útok pochádza od hackerov spozorovaných štátom a v súčasnosti skupinu sleduje pod názvom UNC2452.

Následky útoku pocítili, ako delikátne formulovala zasiahnutá spoločnosť, „vládne, konzultačné, technologické, zdravotnícke, telekomunikačné a ťažobné subjekty v Severnej Amerike, Európe, Ázii a na Strednom východe“.

Vyšetrovatelia však odkryli ešte rozsiahlejšie škody, keď zistili, že útočníci využívali zraniteľnosť v nástroji Orion dovtedy iba málo známej softvérovej firmy *SolarWinds* z amerického štátu Texas. Samotný *SolarWinds* bol cieľom útoku, keďže od marca 2020 využívali štátom podporovaní hackeri spomínanú zraniteľnosť na špehovanie vládnych a obchodných sietí po svete vrátane USA, Spojeného kráľovstva, Izraela a Kanady. Skutočný rozsah tohto útoku zatiaľ nie je známy a ruské oficiálne platformy obvinenia razantne odmietajú.

Nový rok, nové ciele

Ak sa obzrieme za rokom 2020, tak práve tento bol v znamení enormného počtu štátom sponzorovaných hackerských útokov – a v tomto sa ich predpokladá ešte viac. K „tradičným“ cieľom, akými sú vládna komunikácia a kritická infraštruktúra, pribudli nové, ktoré získavajú na dôležitosti každý deň.

Všetky pracoviská, farmaceutické firmy, laboratóriá, mimovládne organizácie a zdravotnícke zariadenia zamerané na výskum a liečbu ochorenia spôsobeného koronavírusom sú ohrozené. Vlastnia informácie vysokej hodnoty so strategickým aj konkurenčným potenciálom. Už v prvej vlne

pandémie zasiahla zdravotníctvo smršť vydierania a incidentov a kybernetickým útokom sa vtedy nevyhli ani slovenské laboratóriá.

Hackerská skupina *Charming Kitten* spájaná s Iránom sa zamerala v apríla na Svetovú zdravotnícku organizáciu, konkrétne na osobné e-mailové účty zamestnancov. Skupina APT32 cielila rozsiahle aktivity z Vietnamu najmä na provinčnú vládu vo Wu-chane.

Štátom sponzorované útoky na výskumný a zdravotnícky sektor budú rásť. Nepriamo to potvrdzujú aj analýzy spoločnosti McKinsey, ktorá očakáva prudký rast výdavkov na kybernetickú bezpečnosť v štyroch kľúčových odvetviach – zdravotníctvo, bankovníctvo a financie, technológie a médiá a verejný a sociálny sektor.

Iránske a čínske hackerské skupiny sa začínajú zameriavať nielen na výskumné spoločnosti, ale aj na ďalšie v zdravotníctve a biotechnológiách. A pravdepodobne budú aj naďalej v čele špionáže zameranej na boj s COVID-19, či už ide o liečbu, alebo aktuálne zdravotnícke dáta. Bezpečnostné zložky Spojených štátov už verejne obvinili obe krajiny, že sa pokúsili nabúrať jednu z globálnych výskumných firiem.

Najvytrvalejší v kybernetickom boji

Spoločnosť FireEye venuje osobitnú pozornosť APT skupinám tzv. pokročilých pretrvávajúcich hrozieb (Advanced Persistent Threaths), ktoré dostávajú úlohy a najmä finančnú podporu od štátu. V spojení so štátom sponzorovanými hackerskými útokmi sa v ich reportoch najčastejšie skloňujú štáty ako Čína, Rusko, Irán, Severná Kórea a dokonca aj Vietnam. Tieto skupiny sa radia medzi najaktívnejšie a najvytrvalejšie z hľadiska hackerských útokov.

Aj dezinformátori majú svoj rebríček

Technologický magazín Wired, ktorý pravidelne zostavuje desiatku najnebezpečnejších osôb na internete (z hľadiska Spojených štátov), do rebríčka za rok 2020 zaradil tri osoby, dve extrémistické platformy a päť hackerských skupín, z toho tri s ruským domicilom (UN2452, GRU Hackers, Berserk Bear).

A tie dve? Iránski hacktivisti z Iran's IRGC Hackers sa masívne prejavili práve počas minuloročných prezidentských volieb a TrickBot má za sebou viacej rokov a významných referencií. Napriek tomu, že toto hackerské zoskupenie utrpelo práve minulý rok stratu likvidáciou svojho servera a útokom na botnetovú sieť, predpokladá sa, že ešte nepovedalo posledné slovo.

Najviac čiernych bodov v hodnotení dostali osobnosti, ktoré sa masívne podieľajú na šírení dezinformácií a konšpiračných teórií. Takže na prvom mieste sa ocitol Donald Trump a hneď za ním Mark Zuckerberg, ktorému odborná redakcia vyčíta, že sa mu sociálna sieť vymkla spod kontroly. Trojicu uzatvára Scott Atlas, odborník neurorádiológie, ktorý spoločne s Donaldom Trumpom

popiera účinok rúšok v boji s pandémiou a, naopak, vyzýva na výrazne neštandardné formy pri jej likvidácii.

Stroj na peniaze

Cybersecurity Ventures očakáva, že celosvetové škody spôsobené kybernetickou kriminalitou budú rásť v nasledujúcich piatich rokoch o 15 percent ročne a do roku 2025 dosiahnu hodnotu 10,5 bilióna amerických dolárov. Táto suma zahŕňa cenu poškodených a ukradnutých dát, peňazí, stratu dobrého mena aj produktivity, forenznú analýzu, autorské práva a náklady na obnovu. Ak sa obzrieme späť, v roku 2015 boli náklady spôsobené kybernetickou kriminalitou na úrovni troch biliónov amerických dolárov.

Ako farbisto uvádza na záver vyššie uvedený autorský kolektív: *Keby sa výkonnosť kybernetickej kriminality merala ako výkonnosť štátnej ekonomiky, kybernetická kriminalita by bola tretia najsilnejšia ekonomika sveta hneď po Spojených štátoch a Číne.*

Zdroje:

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

https://www.fireeye.com/current-threats/apt-groups.html

McKinsey and Company, COVID-19 crisis shifts cybersecurity priorities and budget, July 21, 2020.