ALISON

Zero-day útoky? Stále pribúdajú a stále dôležitejší je rozpočet

- **Trh so zero-day zraniteľnosťami naberá na obrátkach**
- **Kto najčastejšie nakupuje**
- **Najväčší svetový bug bounty program**

Zero-day zraniteľnosť sa stáva plnohodnotnou a výhodnou komoditou. Vďaka širokej ponuke na dark webe nakupujú rôzne skupiny, organizácie a dokonca aj štáty. Takto si napríklad už za 10 dolárov kúpite balík škodlivého kódu k populárnemu WordPressu. A za pol milióna by ste mohli skúsiť hacknúť Zoom (ale nie je to overené).

Deň nula

Slabina alebo chyba v softvéri či hardvéri, ktorá bola odhalená, ale ešte nie je opravená, sa označuje ako zero-day zraniteľnosť. Deň odhalenia chyby je zero-day a zvyčajne túto informáciu vydajú špecializované skupiny, ktoré softvér alebo hardvér testujú. Odo dňa nula sa začínajú počítať dni (n), až kým sa na chybu „nasadí záplata“, a z toho vzniká n-dňová zero-day zraniteľnosť, ktorá sa veľmi prísne posudzuje v kvalitatívnom hodnotení.

Útočníci využívajú hluché obdobie pred opravou chyby na zero-day útok, ktorého obeťou sa môže stať ktokoľvek. Ak nie ste obstavaný špičkovou kybernetickou bezpečnosťou, jedinou možnou záchranou pre používateľa je oficiálna oprava alebo aktualizácia.

Častým cieľom hackerov sú internetové prehliadače práve vďaka svojej rozšírenosti a enormnému množstvu používateľov. Phishingové správy zneužívajú zraniteľné miesta v poštových programoch a napádajú systémy, získavajú kontrolu nad infikovaným počítačom a kradnú osobné údaje. Doba ohrozenia môže byť niekoľko dní, ale aj týždňov alebo mesiacov.

Bezpečnostná firma FireEye v roku 2019 zaznamenala viac zero-day zraniteľností ako za predchádzajúce tri roky. Zatiaľ čo v minulosti boli zero-day zraniteľnosti skôr vzácnosťou a ich používanie bolo orientované na veľmi dôležité ciele, v súčasnosti sa stávajú ľahko dostupnými pre rôzne skupiny aktérov.

Zero Day Initiative

Zero Day Initiative (ZDI) vznikla, aby diskrétne informovala o zero-day zraniteľnostiach. Táto formácia firiem a jednotlivcov sama seba označuje ako „najväčší svetový bug bounty program“. Výskumné tímy informujú o odhalených nedostatkoch vlastníkov softvéru či hardvéru diskrétne a za určitú finančnú odmenu. Nezverejňujú sa žiadne technické podrobnosti, pokiaľ nie je vydaná oprava.

Keď sa objaví informácia o zero-day zraniteľnosti, formácia ZID urobí analýzu a označí to signatúrou, čiže vytvorí pravidlo, ktoré sa verejne distribuuje. Pravidlo sa aplikuje na bezpečnostných zariadeniach, a keď príde útok, je blokovaný alebo umiestnený do karantény.

Špeciálne bezpečnostné produkty však dokážu chrániť aj „bezbranný“ softvér a hardvér, ktorý nemá ešte záplaty a aktualizácie. Výhodou je, ak bezpečnostné produkty majú skoršiu identifikáciu zraniteľnosti ako konkurencia, a tak vedia s predstihom chrániť pred zero-day útokmi.

Kto najčastejšie nakupuje na zero-day trhu

Medzinárodná diplomacia pozná označenie „spoločnosti poskytujúce ofenzívne kybernetické služby“. Práve tieto čoraz častejšie nakupujú na trhu zero-day zraniteľností. Vzrástol najmä počet zero-day útokov proti cieľom na Blízkom východe. Špionážna skupina Stealth Falcon a FrutiyArmor sa zameriava na novinárov a aktivistov na Blízkom východe. V roku 2016 využila malvér izraelskej firmy NSO Group, ktorým cielili útoky na novinárov na Blízkom východe. Táto skupina využila v rokoch 2016 až 2019 viac zero-day zraniteľností ako ktokoľvek iný.

Analytici na základe dostupných údajov za rok 2019 zostavili rebríček počtu zero-day útokov, ktoré priradili podľa ich pôvodu krajinám. V prvej trojke sú podľa početnosti Čína, Rusko a USA.

Zaujímavosťou týchto útokov je, že po vydaní opráv softvéru dokážu útočníci rýchlo preskúmať, aké opravy boli vykonané, a v krátkom čase zakomponujú opravenú zraniteľnosť do svojich útokov. Využívajú tak čas pred vydaním ďalšieho softvéru a napadnú čo najviac cieľov.

Hitparáda minulého mesiaca

Najnovším úlovkom odborníkov v spolupráci s Trend Micro Zero Day Initiative je odhalenie piatich zero-day zraniteľností operačného systému Windows. Klasifikáciu vysokým rizikom si vyslúžili štyri z nich a dokonca zraniteľnosti označené CVE-2020-0916, CVE-2020-0915 a CVE-2020-0986 útočník môže zneužiť na získanie vyšších používateľských oprávnení na postihnutom systéme.

Spoločnosť Microsoft bola informovaná o existencii týchto zraniteľností v decembri 2019, avšak termín na vydanie opráv v máji 2020 zmeškala. Varovanie vydala koncom mája aj slovenská vládna kyberbezpečnostná jednotka CSIRT.

Zero-day zraniteľnosti trápia aj aplikáciu Zoom. Kritická zraniteľnosť bola nájdená začiatkom apríla v klientovi aplikácie pre operačný systém Windows a spoločnosť Zoom vydala aktualizáciu. Podľa anonymných zdrojov mala aplikácia Zoom opätovný problém. Hackeri predávali zero-day zraniteľnosti pre oba operačné systémy Windows a macOS. Cena za zraniteľnosť údajne dosahovala sumu 500-tisíc amerických dolárov. Spoločnosť však tvrdí, že sa nenašli žiadne dôkazy, ktoré by tieto informácie potvrdili.

Zdroje:

- https://www.fireeye.com/blog/threat-research/2020/04/zero-day-exploitation-demonstrates-access-to-money-not-skill.html
- https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/security-101-zero-day-vulnerabilities-and-exploits
- https://www.zerodayinitiative.com
- https://www.csirt.gov.sk