ATM jackpotting

alebo bankomat, otras sa!

Útok na bankomat s cieľom zmocniť sa finančnej hotovosti. Útok nevyžaduje fyzický prístup do väčšinou veľmi dobre zabezpečeného priestoru trezoru.

AEC

ATM PC útok

Pri prvom typu útoku sa útočník zameriava na počítač s operačným systémom Windows (ATM PC) a s vlastným softvérovým riešením.

Tento operačný systém je neoddeliteľnou súčasťou bankomatu, podobne ako jeho hardvérové komponenty: dispenser, tlačiareň, pinpad klávesnice, kamery a pod.

Útočník obvykle využije niektorú z konfiguračných chýb, napríklad povolené USB porty alebo nešifrovaný pevný disk a zvýši svoje oprávnenia k tomu, aby mohol zasahovať do nastavení jednotlivých služieb alebo ovplyvňovať možnosti prístupu.

Malware, ktorý útočník do prostredia nasadí, si zaistí cez XFS vrstvu komunikáciu na dispenser, čo mu dovoľuje veľmi často nedostatočný hardening.

Vďaka týmto krokom potom útočník môže prostredníctvom dispensera neoprávnene vyberať hotovosť z trezoru bankomatu, prípadne sa zameria na práve prebiehajúce transakcie a ich presmerovanie na cudzí účet.

Black box zariadenie

Druhý typ útoku sa úplne vyhýba aplikačným bezpečnostným opatreniam nasadeným v ATM PC.

Útočníci pri ňom ATM PC úplne vypnú a pripoja si vlastné black box zariadenie. To môže byť klasický laptop, tablet či Raspberry Pi.

Potom, čo svoj black box pripoja k USB portu bankomatu, môžu priamo odosielať príkazy na výdaj hotovosti z trezoru prostredníctvom dispensera.

Ak nie sú hardvérové periférie zapatchované, umožňujú odpočúvať nešifrovanú komunikáciu medzi operačným systémom a dispenserom bez znalosti patričných kľúčov.

Vďaka tomu sa tento typ útoku stáva veľmi účinným a nebezpečným nástrojom.

Vlastný tím špecializovaný na testy bankomatov

Spoločnosť AEC uskutočnila už celý rad bezpečnostných testov bankomatov. Vyvinuli sme vlastné nástroje a postupy, ako prakticky overiť všetky vyššie popísané scenáre. Vďaka tomu dokážeme upozorniť na slabé miesta v systéme testovaného zariadenia a navrhnúť odporúčania na zvýšenie úrovne zabezpečenia.

Náš tím uskutoční previerku zraniteľností bankomatov behom jedného týždňa. Komplexná analýza zahŕňa spôsoby fyzického prístupu, eskaláciu privilégií, testy operačného systému a aplikácií. Je však možné sústrediť sa iba na penetračné testy infraštruktúry, integračných služieb a manažmentu, reverznú analýzu softvéru, prípadne bezpečnostnú analýzu zdrojového kódu.

www.aec.sk/atm-jackpotting

AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283