Suur äri: põrandaalusel turul on müügil üle 70 000 hõivatud serveri

8 aastat tagasi Autor: AM

Kes veel kasutab teie servereid? Selgub, et üsna paljudel serveriomanikel ongi teisi fantoomkasutajaid. Kaspersky Lab paljastas massilise põrandaaluse turu, kus on müügis üle 70 000 häkkerite hõivatud serveri.

Kaspersky Lab´i asjatundjad uurisid ülemaailmset netifoorumit, kus küberkurjategijatel on võimalus osta ja müüa juurdepääsu häkitud serveritele vaid kuue dollari eest serveri kohta. Veebiturul xDedic, mida nähtavasti juhib venekeelne grupeering, on praegu müügis 70 624 sissehäkitud kaugarvuti protokolliga (RDP) serverit.

Paljud serverid teenindavad populaarseid kasutajalehekülgi ja teenuseid või võimaldavad neile juurdepääsu. Mõnedele neist on paigaldatud tarkvara otsepostitusteks, finantsaruandluseks ja kassaterminalide (POS) kasutamiseks. Neid aga võidakse kasutada rünneteks omanike infrastruktuuridele või stardiplatsina massilisemate rünnakute korraldamiseks, samal ajal kui nende omanikel, sealhulgas valitsusasutustel, korporatsioonidel ja ülikoolidel ei ole praktiliselt ettekujutustki sellest, mis nende serverites toimub.

xDedic on jõuline näide uut tüüpi kriminaalsest küberturust: see on hästi organiseeritud ja toetatud ning pakub igaühele – algajatest küberkurjategijatest kuni pakihalduse süsteemi (APT) kasutavate grupeeringuteni – kiiret, odavat ja hõlpsat ligipääsu legitiimsele organisatsioonilisele infrastruktuurile. See grupeering püüab oma kuritegusid korda saata nii märkamatult, kui võimalik.

Üks Euroopa internetiteenuse pakkuja (ISP) teatas Kaspersky Lab´ile xDedic´i olemasolust. Mõlemad firmad tegid koostööd, et selgitada välja, kuidas see netifoorumis käiv äri toimib. Protsess aga on väga lihtne ja põhjalikult läbi mõeldud: häkkerid murravad serveritesse sisse, kasutades tihtipeale maksimaalselt koos kõiki vahendeid (nn jõhkra jõu ründeid) ning edastavad arvestuslikud andmed xDedic´i turule. Seejärel kontrollitakse häkitud serverite RDP konfiguratsiooni, mälu, tarkvara, ajalugu ja palju muud – kõike seda, mille vastu kliendid võivad enne ostmist huvi tunda. Pärast seda lisatakse andmed üha kasvavasse netiandmebaasi, mille abil on võimalik saada ligipääs järgmistele serveritele:

- valitsusvõrkudele, korporatsioonidele ja ülikoolidele kuuluvad serverid;
- serverid, mis on ette nähtud juurdepääsuks teatud veebilehekülgedele ja teenustele (või nende haldamiseks), sealhulgas mängudele, totalisaatoritele, tutvumislehekülgedele, internetikauplustele, internetipankadele ja tasustamissüsteemidele, mobiilsideoperaatorite võrkudele, internetiteenuste pakkujatele ja veebilehitsejatele;
- serverid eelnevalt paigaldatud tarkvaraga, mis võimaldab lihtsustada rünnete toimepanemist, sealhulgas otsepostitussüsteemid, finantsprogrammid ja kassaterminalidele (POS) ettenähtud tarkvara;
- ligipääsu kõigile serveritele toetatakse paljude häkkeri- ja süsteemitööriistadega.

Kõigest 6 dollari eest serveri kohta võivad kõik xDedic´i foorumi liikmed saada ligipääsu serveri kõigile andmetele, samuti kasutada seda platvormina edasisteks kuritahtlikeks rünneteks. Sel eesmärgil võidakse kasutada muu hulgas sihtrünnakuid, kahjurtarkvara, hajutatud teenusetõkestamise ründeid (DDoS), andmepüüki, sotsiaalset manipuleerimist ja ründeid reklaamiprogrammidele.

Serverite seaduslikud omanikud – autoriteetsed organisatsioonid, sealhulgas valitsusvõrgud, korporatsioonid ja ülikoolid – tihtipeale ei teagi, et nende IT-infrastruktuuri on sisse murtud. Lisaks sellele võivad kurjategijad kohe, kui häkkimiskampaania on lõpetatud, juurdepääsu serverile uuesti müüki panna ning kogu protsess algab siis uuesti.

xDedic´i turg avati tõenäoliselt äriks 2014. aasta paiku ja on kasvatanud oma populaarsust oluliselt 2015. aasta keskpaigast alates. 2016. aasta mais olid 416 eri müüjat pannud seal müüki 70 624 serverit 173 riigist. Nende tegevuse tagajärjel enim kannatanud kümme riiki on Brasiilia, Hiina, Venemaa, India, Hispaania, Itaalia, Prantsusmaa, Austraalia, Lõuna-Aafrika ja Malaisia.

xDedic´i foorumi taga seisev, tõenäoliselt venekeelne grupeering kinnitab, et annab ainult kasutada äriplatvormi ning tal ei ole müüjatega mingeid sidemeid ega suhteid.

„xDedic kinnitab veel kord, et küberkuritegevus kui teenus laieneb seda mööda, kuidas lisanduvad ärikeskkonnad ja müügiplatvormid. Niisuguse teenuse olemasolu lihtsustab enneolematult lihtsalt kõigil – alates väheste oskustega kurjategijatest kuni APT süsteemi kasutavatest grupeeringuteni, kellel on toetus terve riigi ulatuses – osaleda võimalikes purustavates rünnetes nii, et see oleks odav, kiire ja efektiivne. Lõpuks langevad ohvriteks mitte ainult tarbijad või organisatsioonid, kellele niisugused ründed on suunatud, vaid ka mitte midagi kahtlustavad serveriomanikud. Nad ei ole tõenäoliselt üldsegi kursis sellega, et nende servereid kasutatakse ikka ja jälle nende teadmata mitmesugusteks rünneteks, mida pannakse toime otse nende nina all," ütles Kaspersky Lab´i globaaluuringute ja analüüsi grupi juht Costin Raiu.

Kaspersky Lab soovitab organisatsioonidele serveriturule sattumise vältimiseks järgmist:

- Võtke kasutusele usaldusväärne lahendus arvutijulgeoleku tagamiseks, kaitstes oma IT-infrastruktuuri kõikehõlmavalt ja mitmel tasandil.
- Nõudke turvaliste salasõnade kui serveri autentimisprotsessi osa kasutamist.
- Hoidke kõigi paranduste tegemist pidevalt kontrolli all.
- Korraldage regulaarselt IT-infrastruktuuri auditeid.
- Mõelge sellele, et investeerida ohtude analüüsiteenustesse, mille pakkujad hoiavad organisatsiooni kursis tekkivate ohtudega, selgitavad kriminaalõigust ja aitavad hinnata riskitaset.

Lähemalt saab xDedic´ist lugeda leheküljelt Securelist.com.

- Uudised

- Turvalisus

Pilt