**Check Point Research ja CyberInt löysivät haavoittuvuuden peliyhtiö Electronic Artin Origin-palvelualustasta**

*Heikkouksien ketju altisti yli 300 miljoonaa peliharrastajaa kautta maailman pelitilin kaappaukselle ja identiteettivarkaudelle.*

**SAN CARLOS, CALIF. & TEL AVIV – 26.6.2019 –** Yritysten tietoturvaan erikoistuneen [Check Point® Software Technologies Ltd:n](https://www.checkpoint.com/) tutkimustoiminnasta vastaava osasto, Check Point Research, ja digitaalisen kuluttajaliiketoiminnan tarpeita palveleva tietoturvayhtiö [CyberInt](http://www.cyberint.com) ovat tunnistaneet haavoittuvuuksien ketjun Origin-palvelualustassa, jonka on kehittänyt tietokone- ja videopeliyhtiö Electronic Arts (EA). Haavoittuvuuksien kautta olisi voinut ottaa haltuun pelaajan tilin ja kaapata hänen identiteettinsä. Myös pelien ja pelirahan ostaminen uhrin luottokorttitietojen avulla olisi ollut mahdollista.

EA on maailman toiseksi suurin peliyhtiö, joka tunnetaan etenkin urheilupeleistään. Sen pelejä ovat *FIFA, Madden NFL, NBA Live, UFC, The Sims, Battlefield, Command and Conquer* ja *Medal of Honor*. Pelit hyödyntävät Origin-asiakaspalvelusovellusta, jonka avulla pelaajat voivat ostaa ja pelata EA:n pelejä PC:llä ja mobiililaitteella. Origin mahdollistaa esimerkiksi profiilin hallinnan, verkostoitumisen chatin kautta ja yhteispelaamisen. Se sisältää myös yhteisöintegraation esimerkiksi [Facebook](https://en.wikipedia.org/wiki/Facebook)in, [Xbox Live](https://en.wikipedia.org/wiki/Xbox_Live)n, [PlayStation Network](https://en.wikipedia.org/wiki/PlayStation_Network)in ja [Nintendo Network](https://en.wikipedia.org/wiki/Nintendo_Network)in kanssa.

CyberIntin ja Check Pointin tutkijat ilmoittivat haavoittuvuuksista EA:lle alan vakiintuneiden käytäntöjen mukaisesti, mikä mahdollisti niiden paikkaamisen ja päivityksen julkaisemisen.

”Pelaajien turvallisuus on meille ensisijainen tavoite, joten käynnistimme toimet raportoitujen ongelmien korjaamiseksi heti saatuamme raportin CyberIntin ja Check Pointin löydöksistä”, vahvisti Electronic Artsin pelien ja pelialustan tietoturvasta vastaava johtaja **Adrian Stone**.

Mahdollinen hyökkääjä olisi päässyt tilitietoihin hyödyntämällä hylättyjä aliverkkotunnuksia (subdomaineja) ja EA Gamesin käyttämiä kirjautumistunnisteita (access tokens) sekä sisäänkirjautumisprosessiin rakennettuja OAuth Single Sign-On (SSO)- ja TRUST-mekanismeja. Niiden avulla Origin-tiliä on mahdollista käyttää esimerkiksi Facebook- tai Google-käyttäjätunnuksen ja salasanan avulla. Uhrin olisi pitänyt vain klikata hyökkääjän lähettämää linkkiä, joka olisi tullut aidosta, mutta hylätystä ja kaapatusta EA:n osoitteesta.

”EA:n Origin-alusta on valtavan suosittu, ja jos se olisi jätetty paikkaamatta, viat olisivat mahdollistaneet miljoonien käyttäjätilien kaappaamisen ja hyödyntämisen. Löysimme aikaisemmin samantyyppisiä haavoittuvuuksia Epic Gamesin [Fortnite-pelialustasta](https://research.checkpoint.com/hacking-fortnite/). Molemmat tapaukset osoittavat, miten alttiita verkko- ja pilvisovellukset ovat hyökkäyksille ja tietomurroille. Tällaiset pilvessä toimivat sovellukset ovat entistä useammin hakkereiden hyökkäyskohteina, koska ne sisältävät suuria määriä pelaajien henkilötietoja ja usein myös luottokorttitiedot”, sanoi Check Pointin haavoittuvuuksien tutkimuksesta vastaava johtaja (Head of Products Vulnerability Research) **Oded Vanunu**.

”Pelistudioihin kohdistetut hyökkäykset ovat houkuttelevia hakkereille myös sen takia, että epärehellisin keinoin hankittuja pelihyödykkeitä voi myydä verkon ja darknetin markkinapaikoilla,“ kommentoi CyberInt Technologiesin perustaja ja strateginen johtaja **Itay Yanovski**. ”CyberInt havainnoi jatkuvasti ja automatisoidusti verkkoa hyökkäysten ensimerkkien varalta. Ilmoitamme aina löydöksistämme, kuten äskeisestä [TA505](https://finance.yahoo.com/news/cyberint-reports-ta505-threat-actors-163000014.html):sta, muille alan toimijoille riittävän tehokkaiden turvatoimien käynnistämistä varten”, hän jatkoi.

Check Point ja CyberInt suosittelevat vahvasti käyttämään kaksivaiheista tunnistautumista ja lataamaan pelejä vain niiden virallisilta verkkosivuilta. Vanhempien tulisi huolehtia siitä, että lapset tuntevat verkon vaarat ja ymmärtävät, että kyberrikolliset ovat valmiita lähes mihin tahansa päästäkseen käsiksi pelaajien tietoihin. Check Point ja CyberInt kannustavat peliharrastajia olemaan jatkuvasti valppaina saadessaan tuntemattomista lähteistä lähetettyjä linkkejä.

Haavoittuvuuden tekninen analyysi on käytettävissä Check Point Researchin [blogissa täällä](https://research.checkpoint.com/ea-games-vulnerability).

Check Pointin ja CyberIntin video näyttää havainnollisesti, miten tilin kaappaus tapahtuu. Video löytyy [täältä.](https://www.youtube.com/watch?v=M1aSni70Sq0&feature=youtu.bee)

**Seuraa Check Point Researchia:**

Blogi: <https://research.checkpoint.com/>

Twitter: <https://twitter.com/_cpresearch_>

**Seuraa Check Pointia:**  
Twitter: <http://www.twitter.com/checkpointsw>  
Facebook: <https://www.facebook.com/checkpointsoftware>  
Blogi: [http://blog.checkpoint.com](http://blog.checkpoint.com/)  
YouTube: <http://www.youtube.com/user/CPGlobal>  
LinkedIn: <https://www.linkedin.com/company/check-point-software-technologies>

**Seuraa CyberInt Researchia:**

Blogi: <https://blog.cyberint.com/>

YouTube: <https://www.youtube.com/channel/UCzlxztuatw1FGKSnptjpx9Q/featured>

LinkedIn: <https://linkedin.com/company/cyberint>

Twitter: <https://twitter.com/cyber_int>

**Check Point Research**

Check Point Research huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvahteisöllä on käytettävissään paras mahdollinen tieto kyberturvallisuuden riskeistä. Tutkijaryhmä kerää ja analysoi ThreatCloud-verkkopalvelun tallentamat maailmanlaajuiset kyberhyökkäystiedot, jotta hakkerit pysyvät kurissa ja kaikki Check Pointin tuotteet pystytään päivittämään uusimmilla suojauksilla. Tutkijaryhmä koostuu yli 100 analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvayhtiöiden ja viranomaisten kanssa.

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

**CyberInt**

CyberInt ([www.cyberint.com](http://www.cyberint.com/)) tekee kyberturvallisuudesta liiketoiminnan mahdollistajan kohdistetulla uhkien havaitsemisella ja lieventämisellä. CyberInt tarjoaa alan ainoan alustan, jossa yhdistyvät kyberasiantuntemus ja syvällinen liiketoiminnan ymmärtäminen ja joka tuottaa tietoa ja toimenpiteitä, jotka turvaavat sitä, mikä on yrityksille kaikkein tärkeintä: liiketoiminnan tavoitteita, asiakkaita, työntekijöitä ja brändiä.