Kyberrikolliset hyödyntävät MM-kisahuumaa - Check Point havaitsi huijareiden tempun

*Huijausviestin uhri lataa MM-otteluohjelman ja tulosluettelon kylkiäisenä laitteelleen haittaohjelman.*

**Espoo, 19. toukokuuta 2018.** Tietoturvayhtiö Check Point Software Technologiesin tutkijat ovat tunnistaneet jalkapallon MM-kisoihin liittyvän sähköpostikampanjan, jossa hyväuskoinen uhri lataa laitteelleen MM-otteluohjelman ja tulosluettelon mukana haittaohjelman.

Kun liite avataan, koneelle latautuu myös ohjelma nimeltä DownloaderGuide. Se tunnetaan haittaohjelmien lataajana, jonka kautta hakkeri voi syöttää uhrin laitteelle esimerkiksi mainoksia välittävän haittaohjelman tai verkkoselaimen toimintaa seuraavan lisäosan.

Check Pointin havaintojen mukaan kampanjaan liittyy useita erilaisia sähköpostitse lähetettäviä liitetiedostoa. Kaikilla viesteillä on sama otsikko: "World\_Cup\_2018\_Schedule\_and\_Scoresheet\_ V1.##\_CB-DL-Manager".

Kampanja havaittiin ensimmäisen kerran 30. toukokuuta. Viestien määrä oli huipussaan 5. kesäkuuta, mutta viime viikolla kampanja sai uutta vauhtia kisojen alkamisesta.

”Jalkapallon MM-kisojen kaltaiset tapahtumat, jotka kiinnostavat suurta yleisöä, ovat verkkorikollisten mielestä loistava tilaisuus käynnistää uusia kampanjoita. Kisahypetys voi johtaa huomion herpaantumiseen työpaikoilla, jolloin parhaat käytännöt unohtuvat ja sähköpostien liitteitä avataan harkitsemattomasti. Yritysten ja organisaatioiden olisikin hyvä muistuttaa henkilöstöä tarkkaavaisuudesta myös kisojen aikana”, sanoo Check Pointin tietoturvatutkijoiden kansainvälistä tiimiä johtava **Maya Horowitz.**

"Tämän lisäksi työpaikoilla tulisi ryhtyä toimiin sen varmistamiseksi, etteivät kalasteluviestit ylipäätään pääse henkilöstön postilaatikoihin asti. Monikerroksinen verkkoturvallisuusstrategia suojaa sekä vakiintuneilta haittaohjelmaperheitä hyödyntäviltä tietoverkkohyökkäyksiltä että uusilta uhilta ja estää niiden leviämisen verkon kautta”, Horowitz jatkaa.

**Lisää huijauksia tulossa - Suojaudu näin!**

Check Point ennakoi, että huijauskampanjoja ja urkintahyökkäyksiä koetaan MM-kisojen jatkuessa lisää. Niiltä voi suojautua näin:

• **Pidä ohjelmistot päivitettyinä**. Varmista, että laitteiden käyttöjärjestelmät, tietoturvaohjelmistot, sovellukset ja verkkoselaimet on päivitetty uusimpiin versioihin, koska päivitetyt ohjelmistot tarjoavat tehokkaan suojan haittaohjelmilta, viruksilta ja muilta uhilta.

**• Varo väärennettyjä verkkosivustoja.** Aikaisempien kansainvälisten yleisötapahtumien kokemuksista tiedetään, että kyberrikollisten laatimat väärennetyt verkkosivustot voivat kattaa kaiken mahdollisen yleisöä kiinnostavan lippujen ja oheistavaran myynnistä uutisiin ja otteluiden suoratoistoon asti. Sivusto voi näyttää viralliselta, mutta sen tehtävä on levittää haittaohjelmia tai urkkia uhrien tietoja.

**• Varo tuntemattomilta lähettäjiltä tulevia sähköposteja**. Kyberrikollisten lähettämissä sähköposteissa voidaan tarjota alennuksia tai houkutella arvontaan, jonka palkintona on ottelulippuja. Viestien hyperlinkit tai liitetiedostot lataavat haittaohjelmia koneille tai yrittävät varastaa henkilötietoja.

• **Varo julkisia WiFi-yhteyksiä**. Kun otteluja on päivän mittaan useita, moni houkuttuu katsomaan niitä matkan varrella julkisten, avoimien WiFi-yhteyksien kautta. Julkiset WiFi-verkot ovat kuitenkin hakkereille helppoja kohteita, ja niiden kautta on mahdollista esimerkiksi siepata sähköposteja ja salasanoja sekä ladata uhrin mobiililaitteelle haittaohjelmia.

--

**Teksti ja liitteenä oleva kuva ovat vapaasti käytettävissänne**.

Kuvatekstiehdotus:

Kun sähköpostiviestissä houkutellaan osallistumaan arvontaan, jossa on palkintoina MM-kisalippuja, kannattaa todennäköisesti jättää klikkaamatta.

**Lisätiedot ja haastattelupyynnöt:**

Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, [ramira@checkpoint.com](mailto:ramira@checkpoint.com)

OSG Viestintä, Maija Rauha, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065

**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>

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on maailman suurin tietoverkkojen kyberturvallisuuteen keskittynyt yhtiö. Se tarjoaa alan johtavia ratkaisuja ja suojelee asiakkaitaan kyberhyökkäyksiltä vertaansa vaille olevalla haittaohjelmien, kiristysohjelmien ja muiden tietoturvan uhkien kiinnijäämisprosentilla. Check Pointin kattava tietoturva-arkkitehtuuri suojaa niin yrityksen verkot, pilvipalvelut kuin mobiililaitteetkin, ja myös sen hallintajärjestelmä on kattava ja intuitiivinen. Check Point huolehtii yli 100 000 yrityksen ja yhteisön tietoturvatarpeista organisaation koosta riippumatta.