jamk

Manuaalinen avoimien lähteiden kybe-ruhkatiedustelutehtävä

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Anthony Bäckström

Harjoitus

Maaliskuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto

Tässä tehtävässä on tarkoituksena etsiä internetin avoimista lähteistä. Erilaisia ajankohtaisia kyberuhkia. Tietoa haemme erilaisista uutislähteistä ja artikkeleista sekä virallisista kyberuhkia ylläpitävistä sivustoista.

2 Yksittäisiä kyberuhkia eri lähteistä

Zero Trust: Yleistyvä tietoturvastrategia, jossa oletusarvoisesti ei luoteta mihinkään. Vaatii jatkuvaa varmennusta ja valvontaa, luottaen vähemmän perinteiseen verkon reunaturvallisuuteen. Zero Trust ja ZTNA | Secure Cloud

Tiktok ban: Yhdysvaltain edustajainhuone hyväksyi lainsäädännön, joka voisi pakottaa TikTokin kiinalaisen emoyhtiön ByteDancen myymään sovelluksen. Laki on osa Yhdysvaltain ja Kiinan välisiä teknologisia jännitteitä. What to Know About the TikTok Bill That the House Passed - The New York Times (nytimes.com)

Kyberhyökkäys UnitedHealthcare-yksikköön: Hyökkäys häiritsi reseptien käsittelyä laajasti. Ulkomaisen toimijan epäillään olevan hyökkäyksen takana, mikä korostaa terveydenhuollon tietojen haavoittuvuutta. A Cyberattack on a UnitedHealth Unit Disrupts Prescription Drug Orders – DNyuz

Nobelium-ryhmän kyberhyökkäys: Venäjän tiedusteluryhmä Nobelium hyökkäsi Microsoftin johtajien sähköposteihin. Ryhmä on tunnettu SolarWinds-hyökkäyksestä. Microsoft executive emails hacked by Russian intelligence group (cnbc.com)

Suurin kyberhyökkäys Kyivstaria yritykseen: Ukrainan suurinta mobiilioperaattoria Kyivstaria kohtasi sodan aikana suurin kyberhyökkäys, joka häiritsi palveluita ja ilmahälytysjärjestelmiä.

Hyökkäyksen takana epäillään olevan Venäjä. Ukraine's top mobile operator hit by biggest cyberattack of war | Reuters

AI-kyberhyökkäys: Hongkongilainen yritys menetti 25,6 miljoonaa dollaria ensimmäisessä laatuaan olevassa AI-kyberhyökkäyksessä, jossa huijarit käyttivät deepfake-teknologiaa luodakseen vakuuttavia videokonferenssihahmoja yrityksen talousjohtajasta ja muista työntekijöistä Deepfake scammer walks off with $25 million in first-of-its-kind AI heist | Ars Technica

Silmien skannaus kryptovaluuttaa vastaan: Amerikkalaisyritys Tools for Humanity lanseerasi Worldcoin-kryptovaluutan ja houkutteli ihmisiä skannaamaan silmiensä iirikset palkkioksi. https://www.tivi.fi/uutiset/tv/47c95897-395b-4311-a6f8-7c8caaf3cd43?ref=ampparit:29a5

Lotus Bane: APT-ryhmä Lotus Bane on tunnistettu suorittamaan kyberhyökkäyksiä Vietnamin rahoituslaitoksia vastaan. Ryhmä, jonka toiminta on havaittu alkaen vuodesta 2022, käyttää kehittyneitä tekniikoita, kuten DLL-sivukuormausta ja datan vaihtoa nimettyjen putkien kautta. New APT Group 'Lotus Bane' Behind Recent Attacks on Vietnam's Financial Entities (thehackernews.com)

Avast myi käyttäjiensä selailutietoja: FTC määräsi Avastille 16,5 miljoonan dollarin sakon, koska yritys myi käyttäjiensä selailutietoja mainostajille luvaten samalla estävänsä online-seurannan. Lisäksi Avastilta kielletään selailutietojen myynti tai lisensointi mainostarkoituksiin ja yrityksen on ilmoitettava käyttäjille, joiden tietoja on myyty ilman suostumusta. FTC Slams Avast with $16.5 Million Fine for Selling Users' Browsing Data (thehackernews.com)

Doorbell: Tutkimuksen mukaan useissa internetiin yhdistetyissä ovikellokameroissa on turvallisuuspuute, joka mahdollistaa kameroihin murtautumisen painamalla nappia. Ongelmiin kuuluu laitteiden IP-osoitteiden, kuvien ja Wi-Fi-verkon nimen lähettäminen suojaamattomasti internetin yli. Security | TechCrunch

EU on rikkonut omia tietoturvalakejaan: EU on rikkonut omia tietosuojalakejaan kuuden vuoden ajan käyttäessään Microsoft 365 -pilvipalvelua, toteaa Euroopan tietosuojavaltuutettu. Komission katsotaan laiminlyöneen velvollisuutensa varmistaa palvelun käyttö EU:n tietosuoja-asetusten mukaisesti. https://www.tekniikkatalous.fi/uutiset/tt/648dd8a1-c7ef-4350-8867-fc4a38c42afd?ref=ampparit:64a7

Us Cybersecurity and Infrastructure Security Agency hacked: CISA:n mukaan hakkerit hyödynsivät tunnettuja haavoittuvuuksia kahdessa Ivantin tuotteessa: Ivanti Connect Secure ja Ivanti Policy Secure, molemmat verkkoportit. Ivanti itse oli ironisesti varoittanut haavoittuvuuksien aktiivisesta hyväksikäytöstä, erityisesti Kiinan tukemien hakkerien toimesta, ja CISA oli julkaissut neuvonantonsa haavoittuvuuksista, jotka sisältävät CVE-2023-46805:n, CVE-2024-21887:n ja CVE-2024-21893:n. https://www.cyberdaily.au/security/10301-us-cybersecurity-and-infrastructure-agency-hacked

3 Virallisten tahojen viikkokatsauksia

Kybertuvallisuuskeskuksen viikkokatsaus 11/2024: Sähköpostitunnuksia kalastellaan Dropbox-linkin avulla, Pankkitunnuksia havitellaan ajoneuvorekisteristä, Kyberhyökkäykset siirtyvät pilveen, Haavoittuvuudet. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-112024#68221-0

Vulnerability Summary for Week of March 4, 24: Cybersecurity & Infrastructure Security Agencyn ylläpitämä viikkokatsaus. Josta löytyy kymmenittäin CVSS arvioituja uhkia. Uhkatasoilla High, Medium sekä Low. https://www.cisa.gov/news-events/bulletins/sb24-071

Viikon 11 katsaus: Cyberwatch Finland sivusto pitää viikottaisia ja kuukausittaisia katsauksia. Viikon 11 aiheena oli: EU:n kybersolidaarisuusasetus sai poliittisen hyväksynnän. Sivustolla on hyvin lyhyt video aiheesta. https://www.cyberwatchfinland.fi/post/viikon-11-katsaus

Paloalto Unit 42: Paloalton uhkatieto team: Keskittyy tutkimaan ja analysoimaan erilaisia kyberuhkia. Sivustolta löytyy artikkeleita ja blogeja ajankohtaisista kyberuhkista, niistä tehtyjä analyyseja ja miten niihin voi vastata. https://unit42.paloaltonetworks.com/