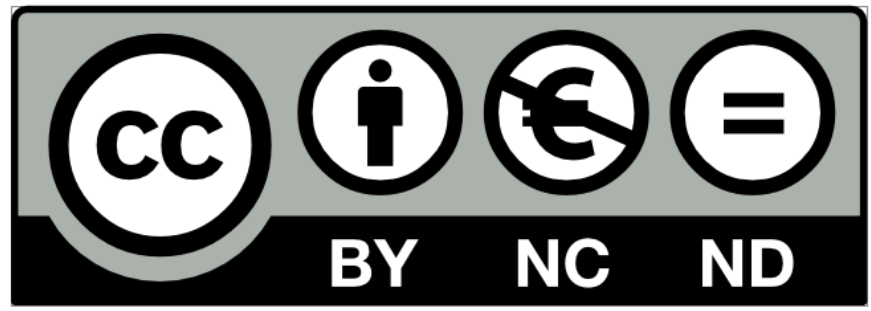
Yksittäisten tiedostojen virustarkistukset netissä

Peruskäyttäjälle.net

Ohjeen versio 30.5.2021



- ➔ Peruskäyttäjälle.netin Creative Commons-esittely (https://peruskayttajalle.net/tietoja.php#cc)
- ➔ Lisätietoa Creative Commonsista suomeksi (https://creativecommons.fi/)

Sisällysluettelo

1 Johdanto

On olemassa verkkopalveluita, joissa voi tarkistaa yksittäisiä tiedostoja haittaohjelmien varalta. Tämä on hyvä vaihtoehto silloin, jos olet esimerkiksi ladannut netistä jonkin ohjelman, jonka turvallisuudesta et ole varma. Tällöin on hyvä saada useampi mielipide asiasta.

Virustarkistuksen voi tehdä lähes mille tahansa tiedostolle, ei ainoastaan ohjelmille. Tarkistettaville tiedostoille on yleensä määritelty enimmäiskoko, joka voi ylittyä joidenkin ohjelmatiedostojen kohdalla.

Tämän kaltaiset verkkopalvelut eivät korvaa tietokoneelle asennettua virustorjuntaa tai muita tietoturvaohjelmia. Ne ovat ainoastaan lisä tietoturvaan. Yksikään verkkopalvelu ei ole myöskään erehtymätön.

Joskus virustarkistuksissa tulee vääriä hälytyksiä, joista käytetään englanninkielistä nimitystä ”false positive”. Jos tarkistettava tiedosto saa vain yhden osuman, kyse voi olla väärästä hälytyksestä.

Tiettävästi verkkopalvelut käyttävät tiedostoja tarkistaessaan ainakin eri virustorjuntaohjelmistojen tunnisteita haittaohjelmista. Jos jotakin haittaohjelmaa ei ole vielä tunnistettu, ei sitä voida myöskään havaita.

Tässä ohjeessa käsitellään kahden eri verkkopalvelun käyttöä. Käsiteltävät verkkopalvelut ovat:

- Jotti (https://virusscan.jotti.org/)
- VirusTotal (https://www.virustotal.com/)

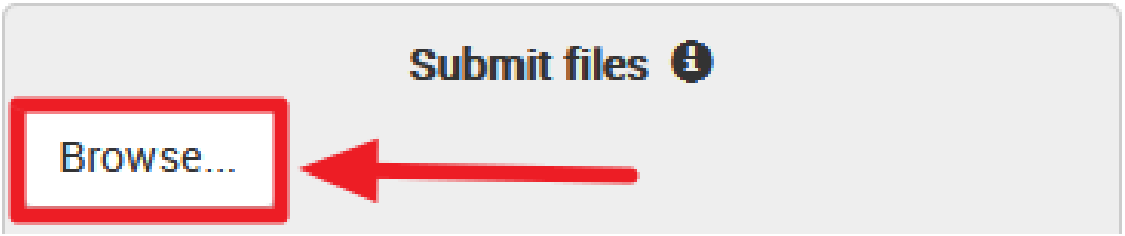
Verkkopalveluista VirusTotalilla voi tarkistaa myös nettisivustojen luotettavuutta. Olen kirjoittanut nettisivustojen maineen ja luotettavuuden arvioimisesta ohjeen Nettisivustojen luotettavuuden arviointi (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php), jossa on käsitelty myös VirusTotalin käyttöä nettisivustojen luotettavuuden arviointiin.

2 Jotti

Jotti (https://virusscan.jotti.org/) käyttää virustorjuntaohjelmistojen Linux-versioita, mikä rajoittaa käytettävien virustorjuntaohjelmistojen määrää. Jottissa voi tarkistaa enintään viisi tiedostoa samaan aikaan. Jottin tiedostokoon raja on 250 megatavua, mikä koskee myös tiedostojen yhteiskokoa.

Voit tarkistaa tiedoston Jottissa seuraavasti:

1. Napsauta sivulla kohdassa **Submit files** olevaa **Browse** -painiketta (kuva 1).

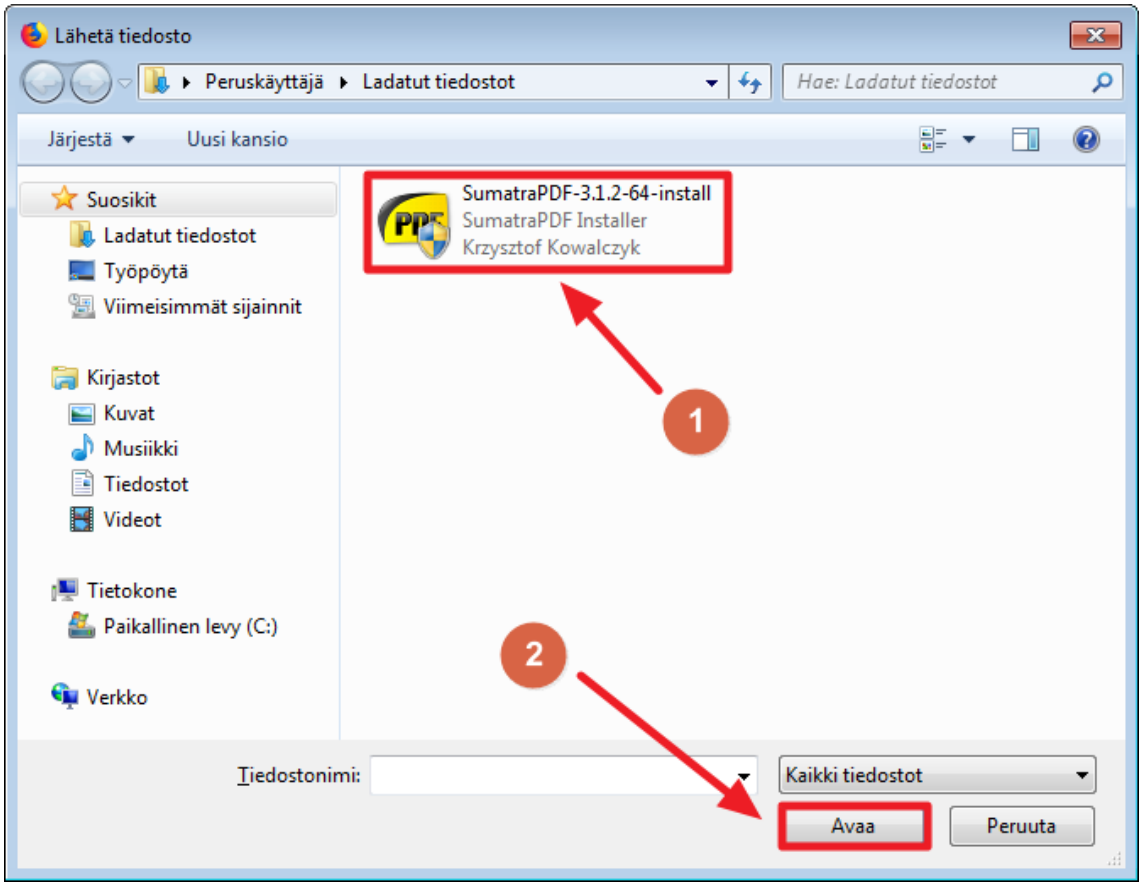


Kuva 1

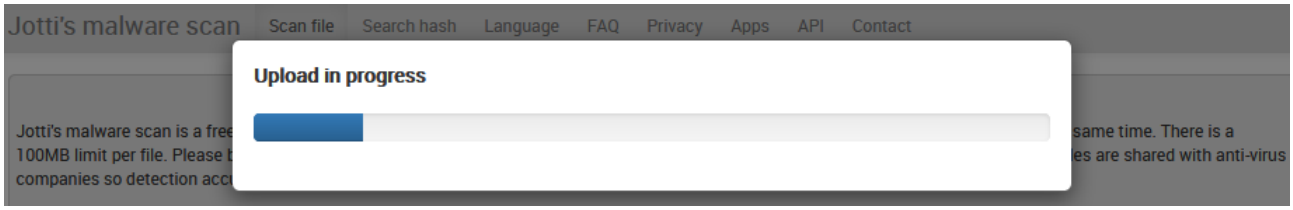
2. Avautuvassa ikkunassa etsi ja valitse enintään viisi tiedostoa. Sen jälkeen napsauta ikkunan alareunan **Avaa** -painiketta. Esimerkissä käytetään tiedostoa *SumatraPDF-3.1.2-64-install* (kuva 2).

3. Jotti lataa valitun tiedoston tai tiedostot verkkopalveluun automaattisesti. Verkkopalvelun sivun päälle avautuu otsikolla **Upload in progress** oleva, valkoisella pohjalla oleva sininen palkki, joka näyttää tiedoston tai tiedostojen verkkopalveluun lähettämisen etenemisen (kuva 3).

4. Jos tarkistettavaksi valittua tiedostoa ei ole tarkistettu aiemmin, Jotti tarkistaa tiedoston automaattisesti.

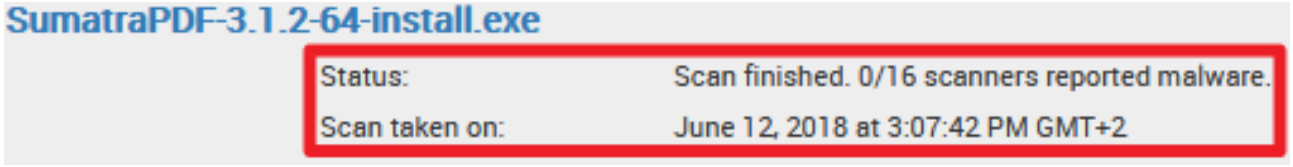


Kuva 2



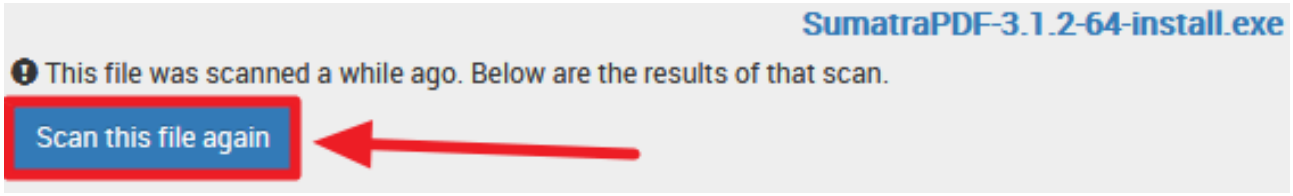
Kuva 3

5. Jos tiedosto on tarkistettu aiemmin, sivun oikeassa reunassa näkyy, kuinka monta osumaa tiedosto on saanut ja milloin se on tarkistettu viimeksi. Esimerkissä tiedosto on saanut nolla osumaa (*0/16*) ja edellinen tarkistus on tehty 12. kesäkuuta 2018 (*June 12, 2018*) (kuva 4). Kuukausien nimet suomeksi ja englanniksi löytyvät luvusta 4.



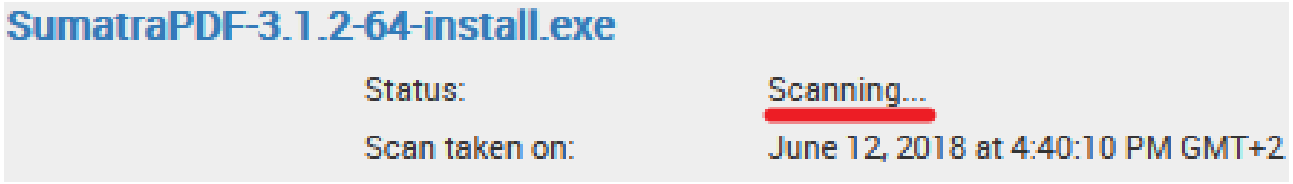
Kuva 4

6. Jos edellisestä tarkistuksesta on kulunut vähintään päivä, kannattaa tiedosto tarkistaa uudelleen napsauttamalla **Scan this file again** -painiketta (kuva 5). Jotti ei anna tarkistaa tiedostoa heti uudelleen, vaan **Scan this file again** -painike on piilotettu. Painike tulee taas näkyviin, kun edellisestä tarkistuksesta on kulunut tietty aika.



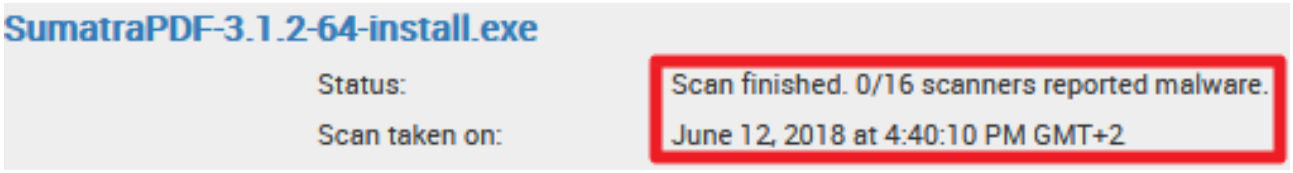
Kuva 5

7. Seuraavaksi virustarkistus käynnistyy. Jos verkkopalvelussa on ruuhkaa, voit joutua odottamaan jonossa jonkin aikaa. Kun tarkistus on käynnissä, lukee otsikon **Status** oikealla puolella teksti *Scanning* (kuva 6).



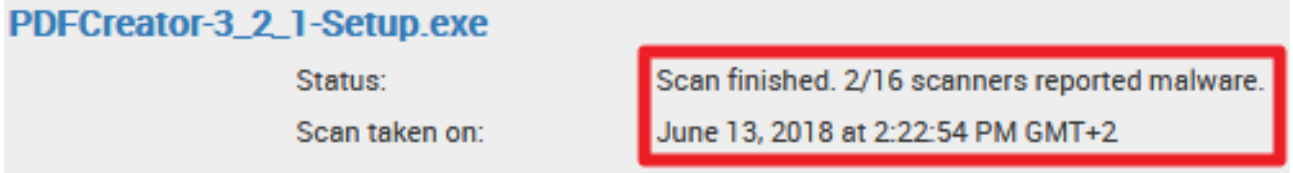
Kuva 6

8. Jos tiedosto on todettu vaarattomaksi, otsikon **Status** oikealla puolella lukee *Scan finished. 0/xx scanners reported malware* (kuva 7).



Kuva 7

9. Jos tiedosto on todettu haitalliseksi, otsikon **Status** oikealla puolella lukee *Scan finished. x/xx scanners reported malware*. Esimerkissä osumia on kaksi (kuva 8).



Kuva 8

10. Alempaa löytyvät tarkemmat tiedot eri virustorjuntaohjelmistojen löytämistä haittaohjelmista. Tiedoista ei välttämättä ole hyötyä asiaan perehtymättömälle, koska tietoturvayhtiöiden haittaohjelmille antamat nimet koostuvat usein erilaisista lyhenteistä, kirjaimista ja numeroista (kuva 9).

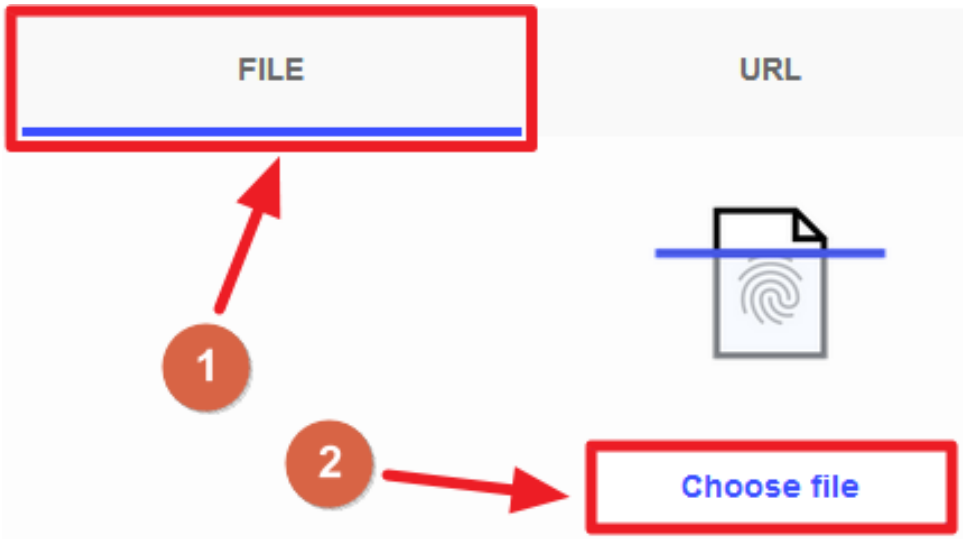
Kuva 9

3 VirusTotal

VirusTotal (https://www.virustotal.com/) käyttää useita kymmeniä eri virustorjuntaohjelmistoja. VirusTotalissa tarkistettavan tiedoston enimmäiskoko on 550 megatavua.

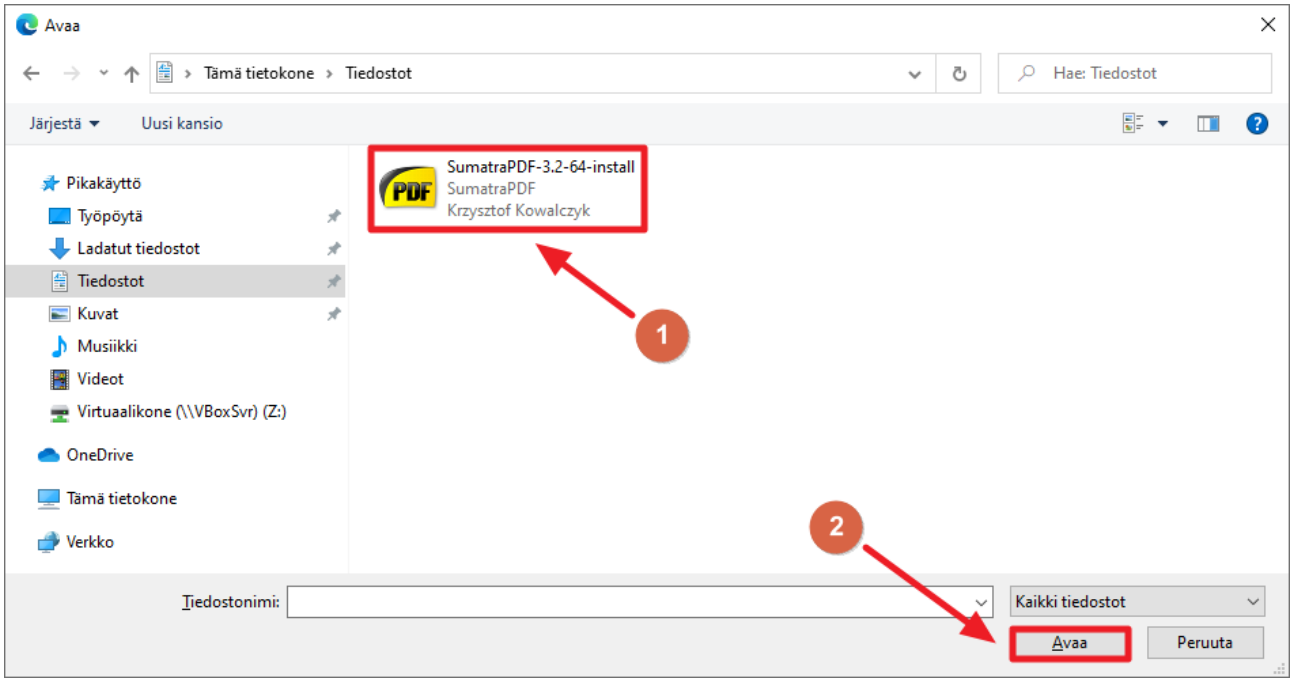
Voit tarkistaa tiedoston VirusTotalissa seuraavasti:

1. Napsauta sivulla **File** -välilehdellä olevaa **Choose file** -painiketta (kuva 10).



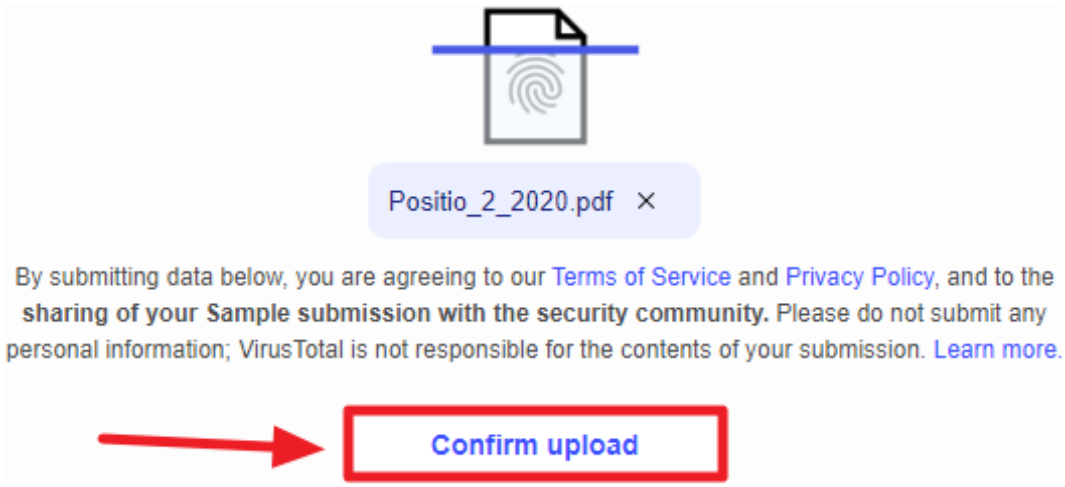
Kuva 10

2. Avautuvassa ikkunassa etsi ja valitse haluamasi tiedosto. Sen jälkeen napsauta ikkunan alareunan **Avaa** -painiketta. Esimerkissä käytetään tiedostoa *SumatraPDF-3.2-64-install* (kuva 11).



Kuva 11

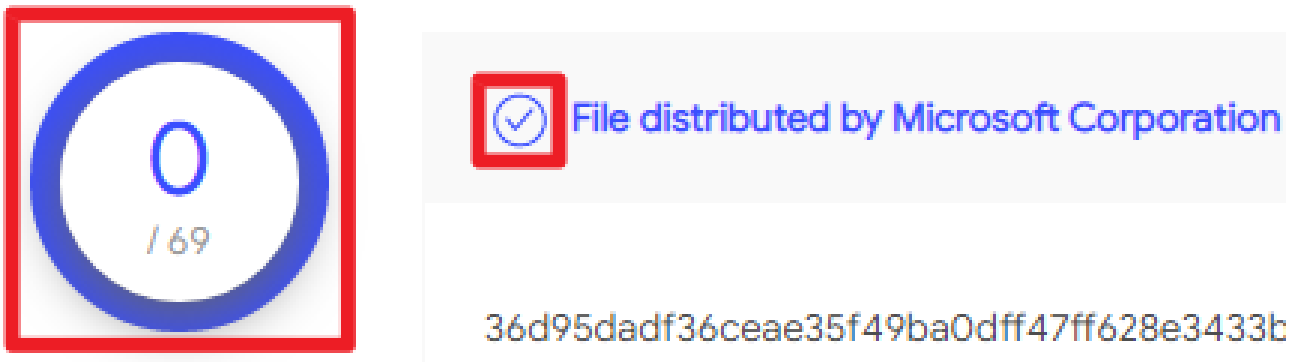
3. Joissakin tapauksissa VirusTotal haluaa vielä erillisen vahvistuksen tiedoston tarkistamiselle yksityisyydensuojan takia, koska kaikki VirusTotaliin ladatut tiedostot ovat julkisesti saatavilla. Näin käy esimerkiksi silloin, kun kyseessä on asiakirja tai PDF-tiedosto. Tällaisessa tapauksessa napsauta **Confirm upload** -painiketta (kuva 12).



Kuva 12

4. Seuraavaksi VirusTotal tarkistaa, onko tiedostoa tarkistettu aikaisemmin. Jos tiedosto on tarkistettu aiemmin ja haittaohjelmia ei ole löytynyt, näkyy sivun yläreunassa vihreä tai sininen ”oikein”-merkki.

Lisäksi sivun vasemmassa reunassa, vihreän tai sinisen ympyrän sisällä lukee teksti *0/xx*. Esimerkissä käytössä on 69 virustorjuntaohjelmistoa, jolloin ympyrässä lukee *0/69* (kuva 13).



Kuva 13

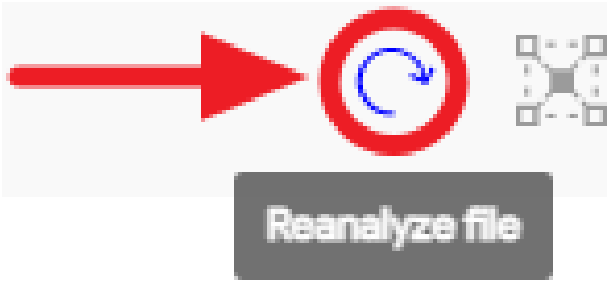
5. Aina kannattaa katsoa, milloin kyseinen tiedosto on tarkistettu viimeksi VirusTotalissa, koska virustorjuntaohjelmistojen tunnisteet päivittyvät jatkuvasti. Tällöin aiemmin tunnistamatta jäänyt haittaohjelma voidaankin tunnistaa. Viimeisimmän tarkistusajankohdan näkee ikkunan oikeasta reunasta.

Aika on muodossa vuosi-kuukausi-päivä ja sen perässä on kellonaika. Esimerkissä tiedosto on tarkistettu viimeksi 24.5.2021, Suomen ajassa kello 1.20,20 (22:20:20 UTC eli koordinoitua yleisaikaa). Lisäksi päivämäärän alla lukee, kauanko edellisestä tarkistuksesta on kulunut aikaa. Esimerkissä aikaa on kulunut 14 tuntia (*14 hours ago*) (kuva 14).

Kuva 14

6. Jos edellisestä tarkistuksesta on kulunut vähintään päivä, kannattaa tiedosto tarkistaa uudelleen. Uudelleentarkistuksen voi tehdä napsauttamalla sivun oikeassa yläreunassa, tarkistusajankohdan lähellä olevaa harmaata painiketta, jossa on ympyrän muotoon taivutettu nuoli.

Kun hiiren osoittimen vie painikkeen päälle, nuoli muuttuu siniseksi ja sen alle ilmestyy teksti *Reanalyze file* (kuva 15).



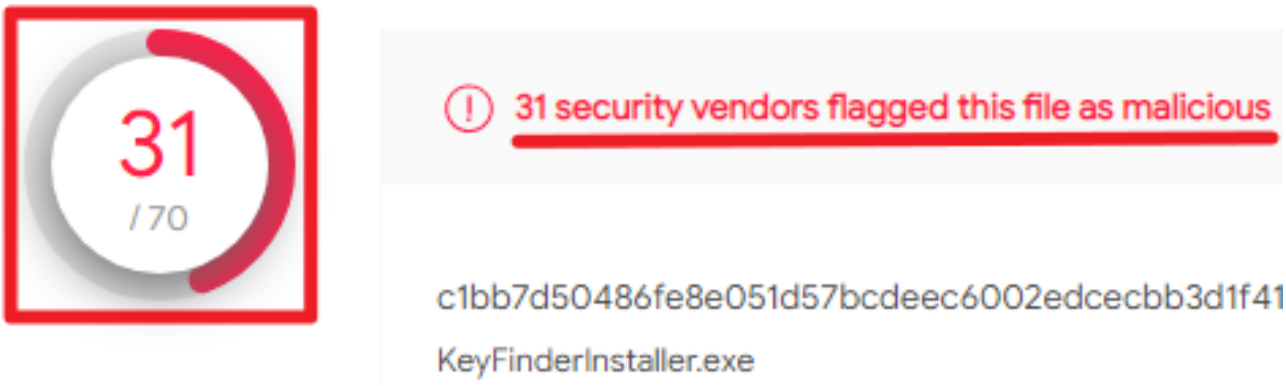
Kuva 15

7. Kun virustarkistus käynnistyy, sivulle ilmestyy teksti *Analyzing*. Samalla sivun vasemmassa reunassa oleva ympyrä muuttuu harmaaksi. Tarkistuksen kesto riippuu tiedoston koosta ja siitä, onko VirusTotalissa ruuhkaa.

8. Jos tiedostosta ei löydy haittaohjelmia, tulos on sama kuin kohdassa 4 ja kuvassa 13.

9. Jos tiedosto on todettu haitalliseksi, näkyy sivun yläreunassa teksti *x security vendors flagged this file as malicious*. Lisäksi sivun vasemmassa reunassa punaisen/harmaan ympyrän sisällä lukee, kuinka moni virustorjuntaohjelmisto on pitänyt tiedostoa haitallisena.

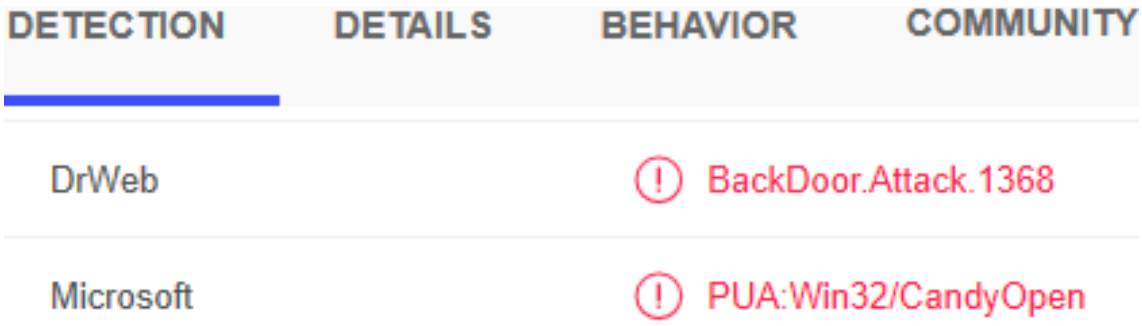
Esimerkissä tiedosto *KeyFinderInstaller.exe* on saanut 31 osumaa (kuva 16).



Kuva 16

10. Alempana sivulla **Detection** -välilehdellä näkyvät ensimmäisenä tiedot virustorjuntaohjelmistoista, jotka pitävät tiedostoa haitallisena. Virustorjuntaohjelmiston nimen jälkeen lukee punaisella tai oranssilla esimerkiksi teksti *Unsafe* tai havaitun haittaohjelman nimi.

Haittaohjelmien nimistä ei ole hyötyä asiaan perehtymättömälle, koska tietoturvayhtiöiden haittaohjelmille antamat nimet koostuvat usein erilaisista lyhenteistä, kirjaimista ja numeroista. Esimerkin kuvaa on rajattu (kuva 18).



Kuva 17

4 Muista yksityisyydensuoja!

Kaikki VirusTotaliin ladattavat tiedostot ovat julkisesti saatavilla. Jotti vastaavasti jakaa palveluun ladattavat tiedostot tietoturvayhtiöiden kanssa. Siksi kumpaankaan palveluun ei kannata ladata mitään arkaluonteisia tiedostoja.

Tiedostojen jakaminen on tarpeellista haittaohjelmien tutkimisen ja niiltä suojautumisen takia. Uusia haittaohjelmia kehitetään jatkuvasti ja näytteet haittaohjelmista ovat tietoturvatutkijoille hyödyllisiä.

5 Aikojen ja kuukausien nimet englanti–suomi

Aikojen nimet englanniksi ja suomeksi

Second	Sekunti
Minute	Minuutti
Hour	Tunti
Day	Päivä
Week	Viikko
Month	Kuukausi
Year	Vuosi

Monikkomuoto englanniksi on sanan perässä oleva *s*-kirjain, esimerkiksi ”päivää” on englanniksi ”days”.

Viikonpäivät

Monday	Maanantai
Tuesday	Tiistai
Wednesday	Keskiviikko
Thursday	Torstai
Friday	Perjantai
Saturday	Lauantai
Sunday	Sunnuntai

Kuukaudet

January	Tammikuu
February	Helmikuu
March	Maaliskuu
April	Huhtikuu
May	Toukokuu
June	Kesäkuu
July	Heinäkuu
August	Elokuu
September	Syyskuu
October	Lokakuu
November	Marraskuu
December	Joulukuu