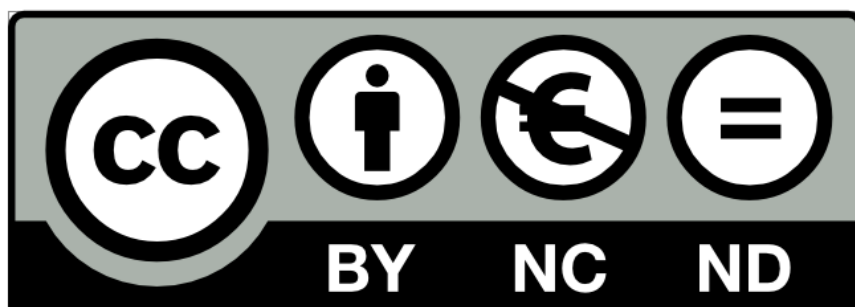


Yksittäisten tiedos- tojen virustarkistuk- set netissä

Peruskäyttäjälle.net

Ohjeen versio 28.11.2017



Tämä teos on lisensoitu **Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen** -lisenssillä. Tarkastele lisenssiä osoitteessa <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.fi>

Voit jakaa tätä teosta, kunhan mainitset selkeästi sen alkuperäksi ja tekijäksi [Peruskäyttäjälle.net](https://peruskayttajalle.net) -sivuston.

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



Sisällysluettelo

1	Johdanto.....	3
2	Jotti.....	4
3	VirusTotal	8
4	Aikojen ja kuukausien nimet englanti–suomi	13



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 ohjelmätiedostojen 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 väärää hälytyksiä, joista käytetään englanninkielistä nimitystä ”false positive”. Jos tarkistettava tiedosto saa vain yhden osuman, kyse voi olla väärästä hälytyksestä.

Tietyvästi 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/) (<https://virusscan.jotti.org/>)
- [VirusTotal](https://www.virustotal.com/) (<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_luotettavuuden_arviointi) (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuuden_arviointi), jossa on käsitelty myös VirusTotalin käyttöä nettisivustojen luotettavuuden arviointiin.

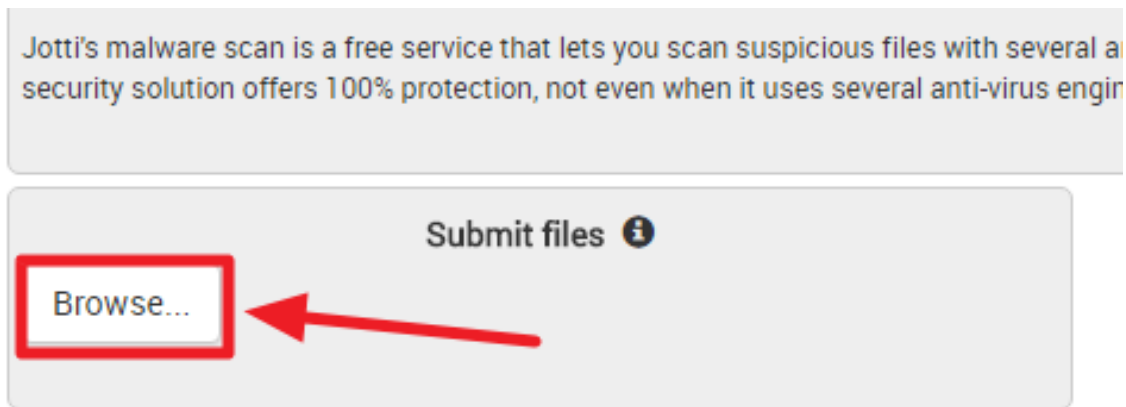


2 Jotti

[Jotti \(https://virusscan.jotti.org/\)](https://virusscan.jotti.org/) käyttää virustorjuntaohjelmistojen Linux-versioita, mikä vähentää käytettävien virustorjuntaohjelmistojen määrän tätä kirjoitettaessa 20:een. Jotissa voi tarkistaa enintään viisi tiedostoa samaan aikaan. Jottin tiedostokoon raja on 100 megatavua.

Voit tarkistaa tiedoston Jotissa seuraavasti:

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

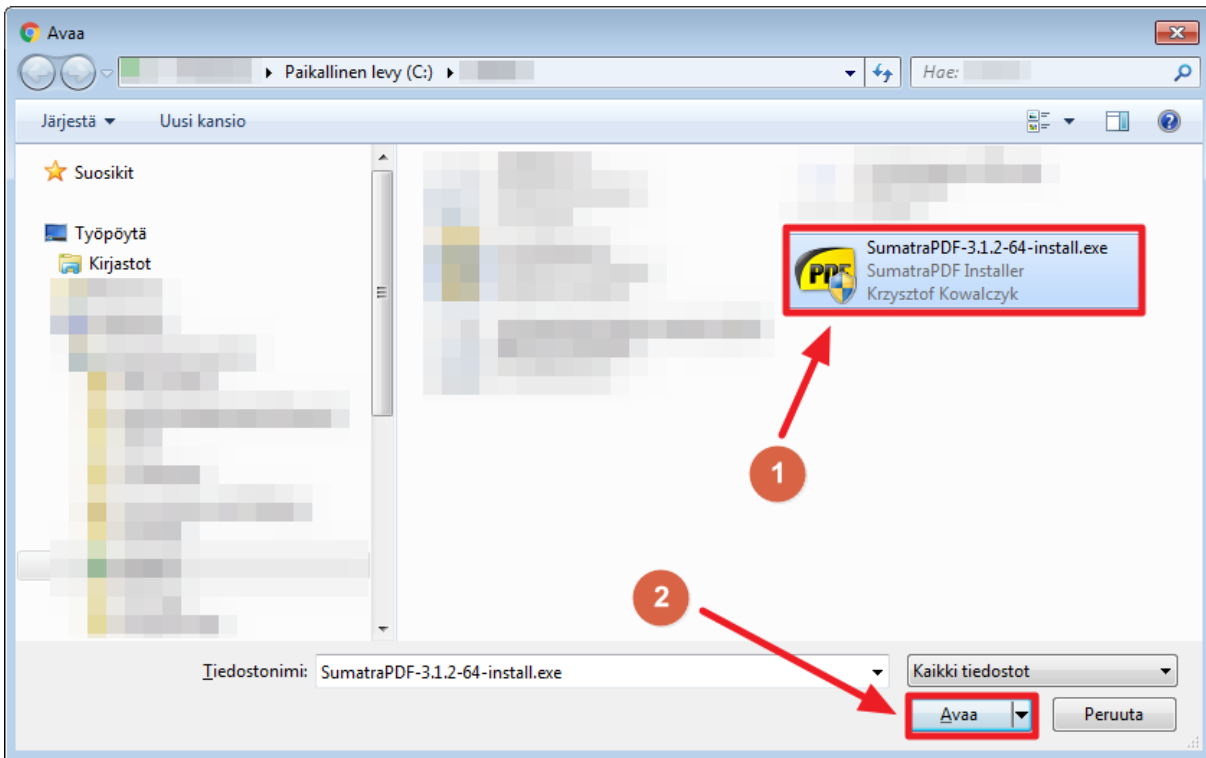


Kuva 1

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.exe* (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.



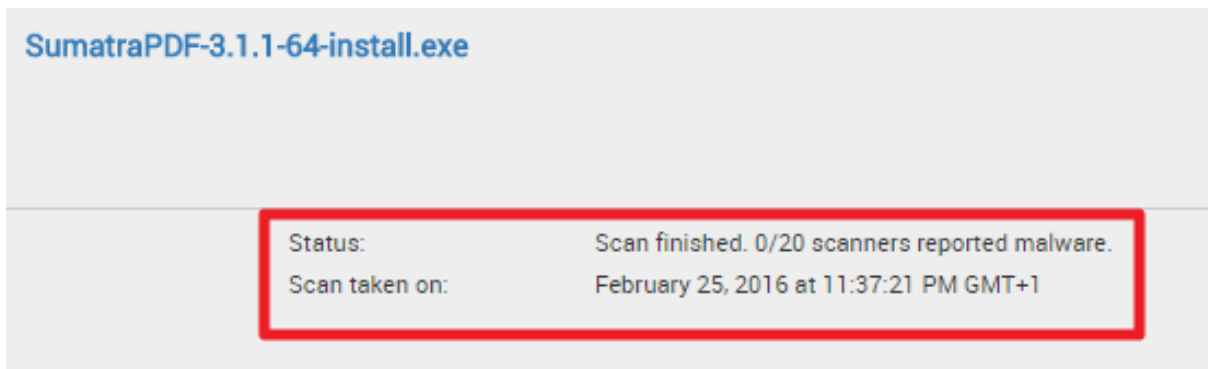
Kuva 2



Kuva 3

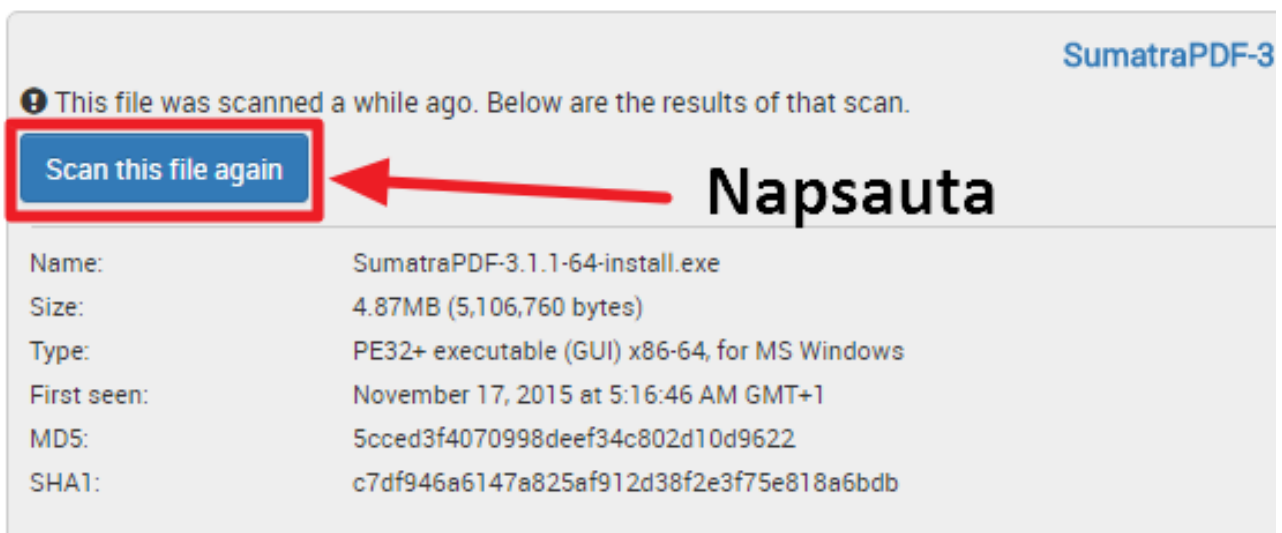
5. Jos tiedosto on tarkistettu aiemmin, sivun oikeassa reunassa näkyy, kuinka monta osumaa tiedosto on saanut ja milloin se on tarkistettu viimeksi. Esimerkissä tiedosto on saanut nolla osumaa ja edellinen tarkistus on tehty 25. helmikuuta 2016 (*February 25, 2016*) (kuva 4). Kuukausien nimet suomeksi ja englanniksi löytyvät luvusta 4.





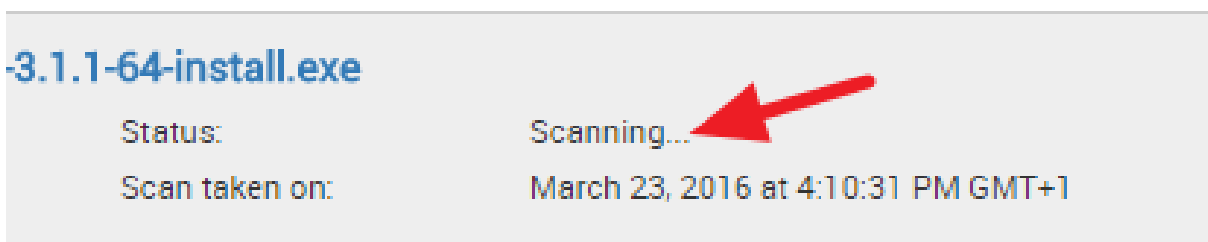
Kuva 4

6. Jos edellisestä tarkistuksesta on kulunut vähintään päivä, kannattaa tiedosto tarkistaa uudelleen napsauttamalla **Scan this file again** -painiketta (kuva 5). Jotta 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

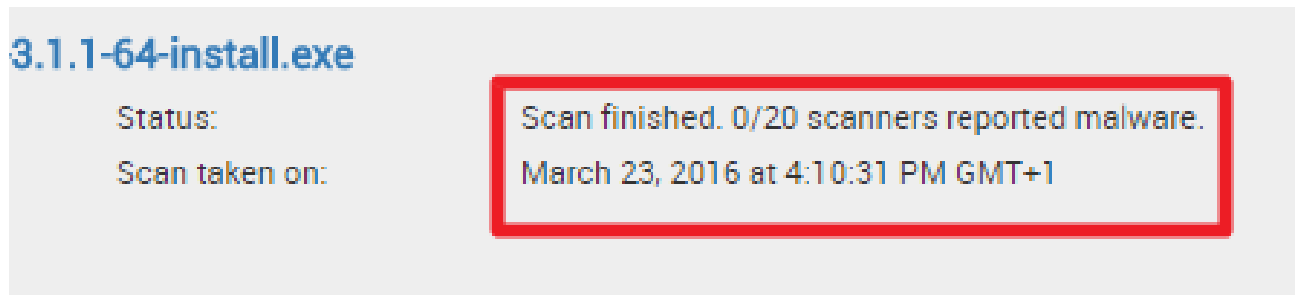
7. Seuraavaksi virustarkistus käynnistyy. Jos verkkopalvelussa on ruuhkaa, voit joutua odottamaan jonossa jonkin aikaa. Kun tarkistus on käynnissä, lukee otsikon **Status** oikealla puolella teksti *Scanning* (kuva 6).



Kuva 6

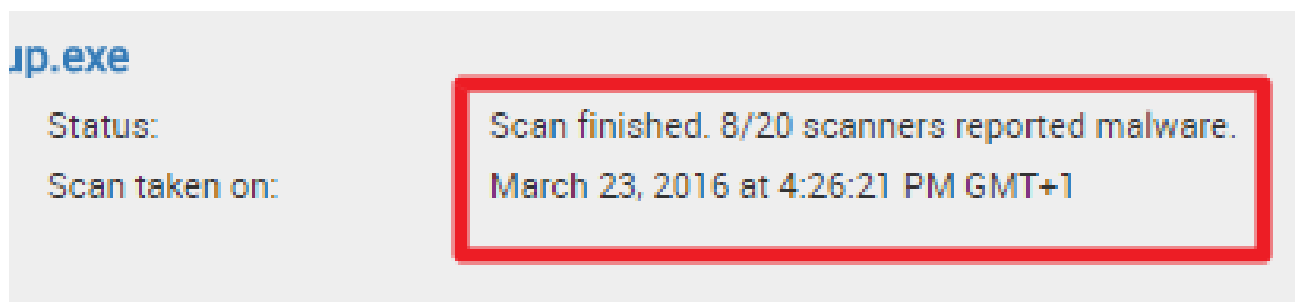


8. Jos tiedosto on todettu vaarattomaksi, otsikon **Status** oikealla puolella lukee *Scan finished. 0/20 scanners reported malware* (kuva 7).



Kuva 7

9. Jos tiedosto on todettu haitalliseksi, otsikon **Status** oikealla puolella lukee *Scan finished. x/20 scanners reported malware*. Esimerkissä osumia on kahdeksan (kuva 8).



Kuva 8

10. Alempaa löytyvät tarkemmat tiedot eri virustorjuntaohjelmistojen löytämistä haittaohjelmista. Tiedoista ei välttämättä ole hyötyä asiaan perehtymättömälle, koska tietoturvahyönteiden haittaohjelmille antamat nimet koostuvat erilaisista lyhenteistä, kirjaimista ja numeroista. Esimerkissä ohjelman asennustiedostosta on löytynyt [OpenCandy](https://en.wikipedia.org/wiki/OpenCandy) (<https://en.wikipedia.org/wiki/OpenCandy>), jonka voi luokitella haittaohjelmaksi (kuva 9).

Ad-Aware	Mar 23, 2016	Found nothing	Arcabit	Mar 23, 2016	Found nothing	avast!	Mar 23, 2016	Found nothing
AVG	Mar 23, 2016	untrusted certificate	AVIRA	Mar 23, 2016	PUA/OpenCandy.Gen	Bitdefender	Mar 23, 2016	Found nothing
ClamAV	Mar 22, 2016	PUA.Win.Packer.Upx-27	Dr.WEB	Mar 23, 2016	Found nothing	eScan	Mar 23, 2016	Found nothing
eSet	Mar 23, 2016	Win32/OpenCandy.A	FORTINET	Mar 23, 2016	Found nothing	F-PROT	Mar 23, 2016	Found nothing
F-Secure	Mar 23, 2016	Found nothing	GDATA	Mar 20, 2016	Found nothing	IKARUS	Mar 23, 2016	PUA.OpenCandy
KASPERSKY	Mar 23, 2016	not-a-virus:AdWare.Win32.OpenCand...	Quick Heal	Mar 21, 2016	Found nothing	SOPHOS	Mar 23, 2016	OpenCandy
TREND MICRO	Mar 22, 2016	Found nothing	VBA32	Mar 23, 2016	AdWare.OpenCandy			

Kuva 9

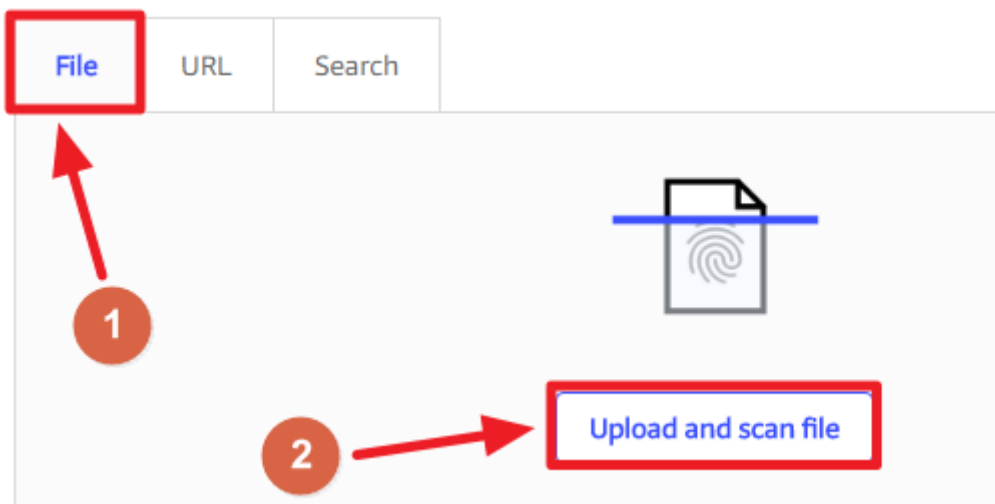


3 VirusTotal

[VirusTotal](https://www.virustotal.com/) (<https://www.virustotal.com/>) käyttää tätä kirjoitettaessa yli 60:tä eri virustorjuntaohjelmistoa. VirusTotalissa tarkistettavan tiedoston enimmäiskoko on 256 megatavua.

Voit tarkistaa tiedoston VirusTotalissa seuraavasti:

1. Napsauta sivulla **File** -välilehdellä olevaa olevaa **Upload and scan file** -painiketta (kuva 10).

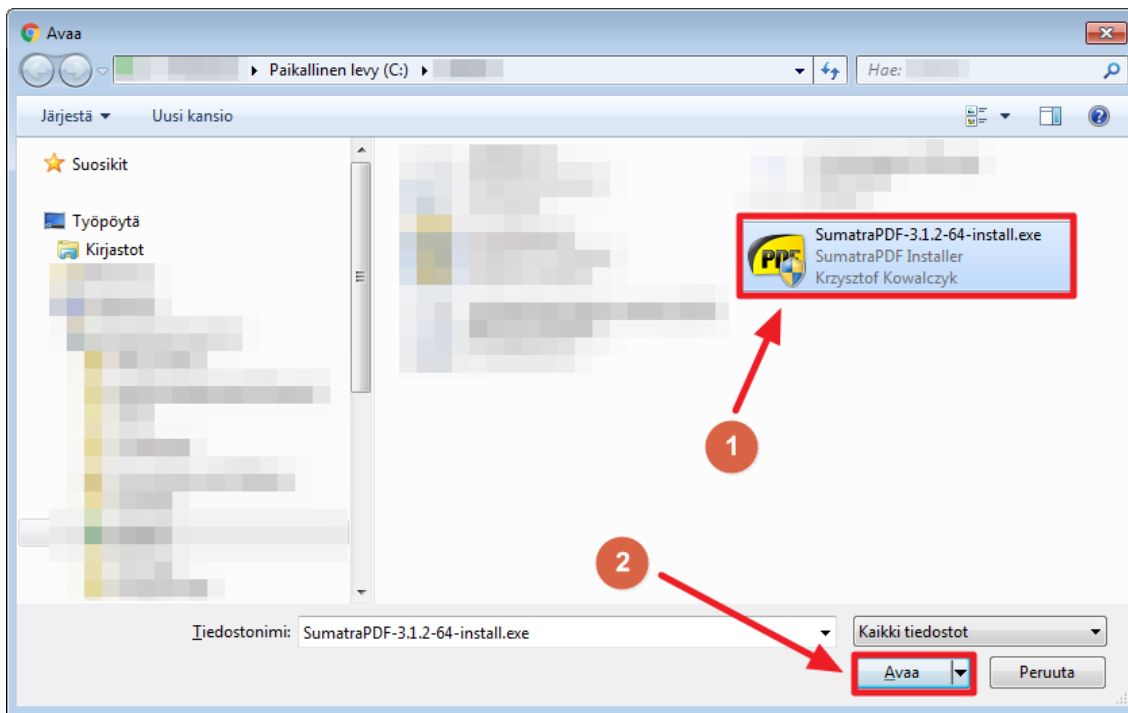


Kuva 10

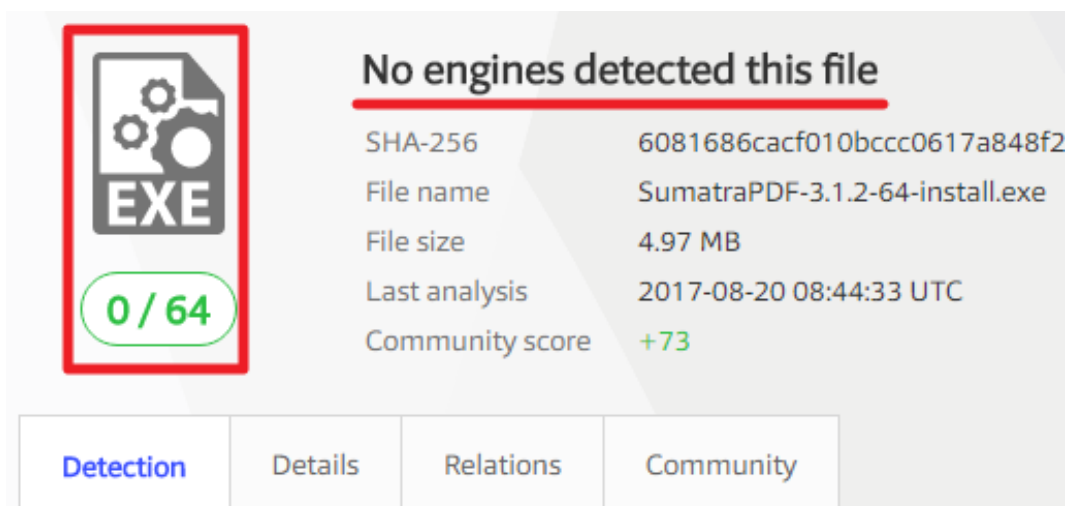
2. Avautuvassa ikkunassa etsi ja valitse haluamasi tiedosto. Sen jälkeen napsauta ikkunan alareunan **Avaa** -painiketta. Esimerkissä käytetään tiedostoa *SumatraPDF-3.1.2-64-install.exe* (kuva 11).

3. Seuraavaksi VirusTotal tarkistaa, onko tiedostoa tarkistettu aikaisemmin. Jos tiedosto on tarkistettu aiemmin ja haittaohjelmia ei ole löytynyt, näkyy sivun yläreunassa teksti *No engines detected this file*. Lisäksi sivun vasemmassa reunassa, tiedostotyyppin alla lukee vihreällä teksti *0/xx*.

Esimerkin tiedosto on tyypiltään *EXE* ja käytössä on 64 virustorjuntaohjelmistoa, jolloin tiedostotyyppin alla lukee vihreällä *0/64* (kuva 12).



Kuva 11

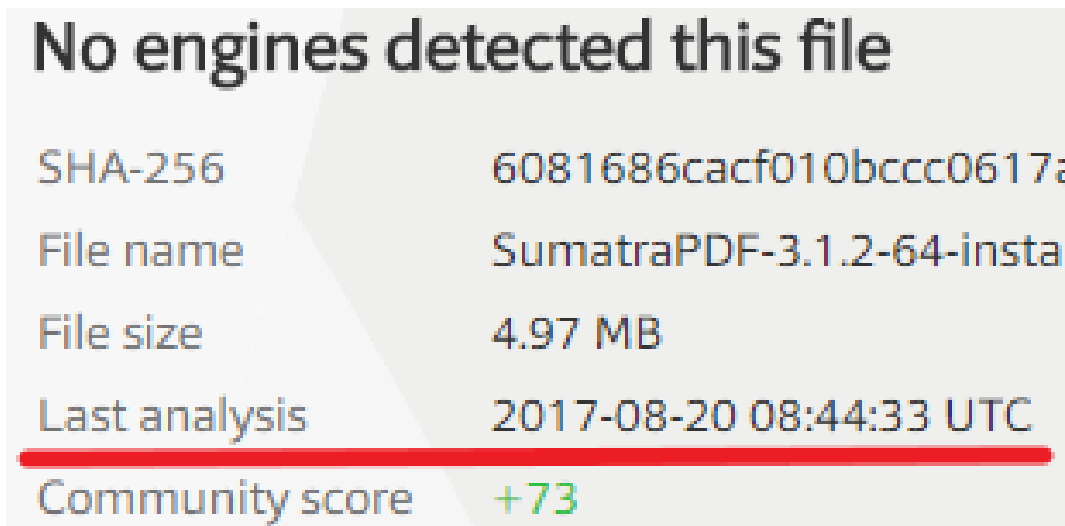


Kuva 12

4. Aina kannattaa katsoa, milloin kyseinen tiedosto on tarkistettu viimeksi VirusTotalissa, koska virustorjuntaohjelmistojen tunnistetut päivittyvät jatkuvasti. Tällöin aiemmin tunnistamatta jäänyt haittaohjelma voidaankin tunnistaa. Viimeisimmän tarkistusajankohdan näkee kohdasta **Last analysis**.

Aika on muodossa vuosi-kuukausi-päivä ja sen perässä on kellonaika. Esimerkissä tiedosto on tarkistettu viimeksi 20.8.2017, Suomen ajassa kello 10.44,33 (08:44:33 UTC eli koordinoitua yleisaikaa) (kuva 13).

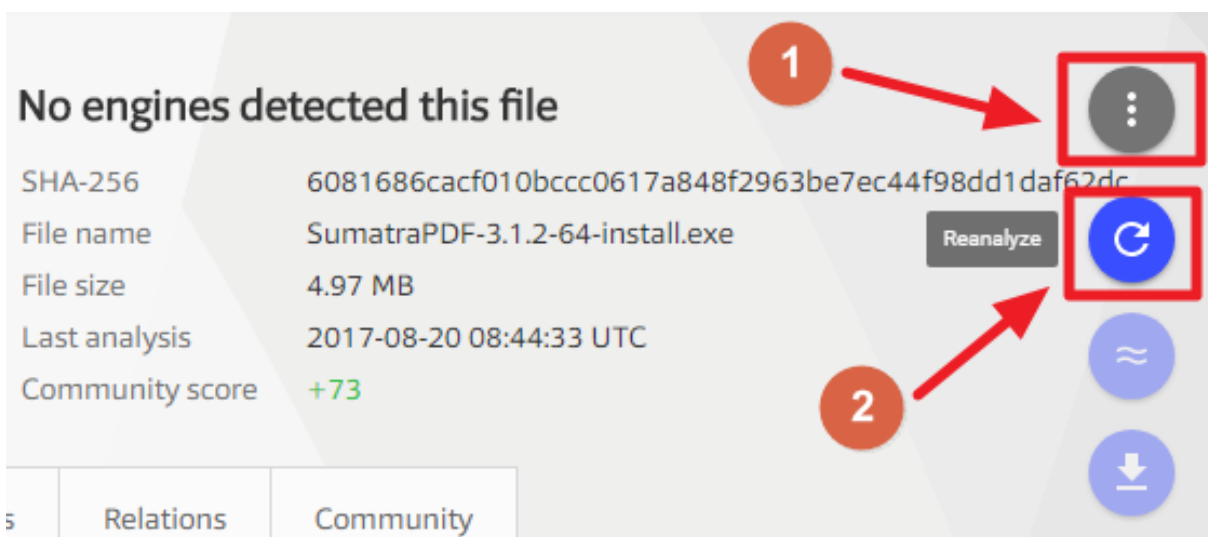




Kuva 13

5. Jos edellisestä tarkistuksesta on kulunut vähintään päivä, kannattaa tiedosto tarkistaa uudelleen. Uudelleentarkistuksen voi tehdä napsauttamalla sivun oikeassa yläreunassa olevaa sinistä painiketta, jossa on kolme pistettä päällekkäin.

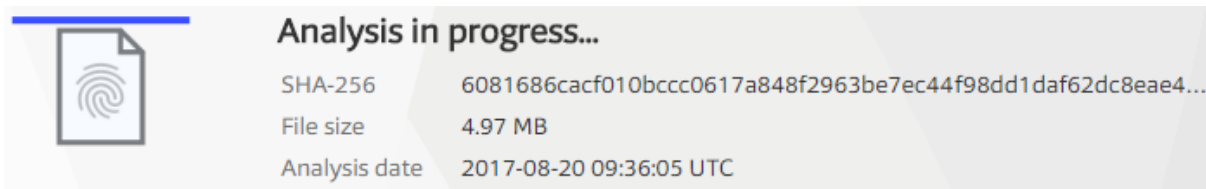
Sen jälkeen napsauta harmaaksi muuttuneen painikkeen alapuolelle ilmestyvää sinistä painiketta, jossa on ympyrän muotoon taivutettu nuoli. Kun hiiren osoittimen vie painikkeen päälle, sen vasemmalle puolelle ilmestyy teksti *Reanalyze* (kuva 14).



Kuva 14

6. Kun virustarkistus käynnistyy, sivulle ilmestyy teksti *Analysis on progress*. Tarkistuksen kesto riippuu tiedoston koosta ja siitä, onko VirusTotalissa ruuhkaa (kuva 15).

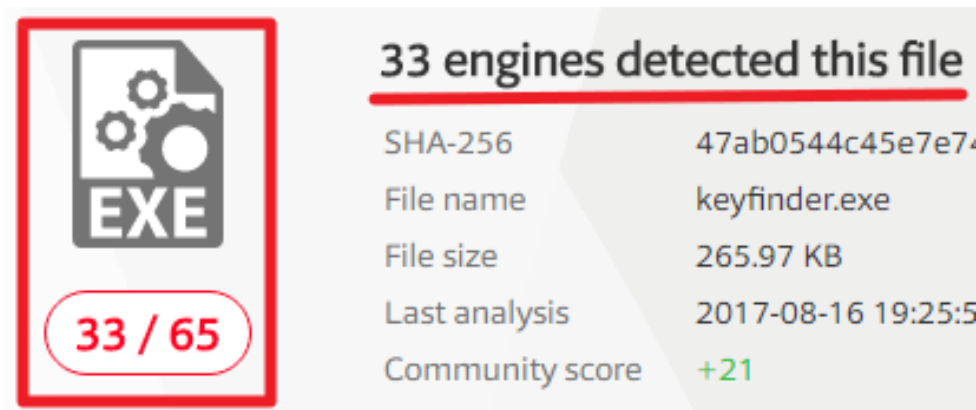
7. Jos tiedostosta ei löydy haittaohjelmia, tulos on sama kuin kohdassa 3 ja kuvassa 12.



Kuva 15

8. Jos tiedosto on todettu haitalliseksi, näkyy sivun yläreunassa teksti *xx engines detected this file*. Lisäksi sivun vasemmassa reunassa, tiedostotyyppin alla lukee punaisella teksti *xx/6x*.

Esimerkissä osumia on 33, jolloin sivun yläreunassa lukee teksti *33 engines detected this file*. Esimerkin tiedosto on tyypiltään *EXE* ja käytössä on 65 virustorjuntaohjelmistoa, jolloin tiedostotyyppin alla lukee punaisella *33/65* (kuva 16).














Kuva 16

9. Alempana sivulta **Detection** -välilehdeltä löytyvät tarkemmat tiedot eri virustorjuntaohjelmistojen löytämistä haittaohjelmista. Tiedoista ei ole hyötyä asiaan perehtymättömälle, koska tietoturvyhtiöiden haittaohjelmille antamat nimet koostuvat erilaisista lyhenteistä, kirjaimista ja numeroista (kuva 17).







10. VirusTotalin rekisteröityneillä käyttäjillä on mahdollisuus äänestää, onko tiedosto vaaraton vai haitallinen. Lisäksi rekisteröityneet käyttäjät voivat kirjoittaa kommentteja. Annetut äänet ja kommentit löytyvät sivun **Community** -välilehdeltä, äänet otsikon **Votes** alta.

Ääniä voidaan antaa tiedoston vaarattomuuden puolesta (teksti *Safe* ja peukalo ylöspäin) tai tiedoston haitallisuudesta (teksti *Unsafe* ja peukalo alaspäin) (kuva 18). Äänten alapuolelta löytyvät kommentit otsikon **Comments** alta. Kommentit on kirjoitettu lähes poikkeuksetta englanniksi (kuva 19).



Detection	Details	Relations	Community 9
AhnLab-V3		 Win-AppCare/WinKeyfinder.272357	
Antiy-AVL		 Trojan[PSWTool]/Win32.RAS	
Avira		 SPR/Tool.agenv	
AVware		 Trojan.Win32.Generic!BT	
Baidu		 Win32.Trojan.WisdomEyes.16070401.9500.9996	
CAT-QuickHeal		 Trojan.IGENERIC	
ClamAV		 Win.Keylogger.Agent-200429	
Comodo		 ApplicUnwnt.Win32.AdWare.Keyfinder.~A	
Cylance		 Unsafe	
Cyren		 W32/FindKey.YLSC-2262	
ESET-NOD32		 a variant of Win32/MagicalJellyBean.A potentially unsafe	

Kuva 17

Detection	Details	Relations	Community 9						
<p>Votes ⓘ</p> <div style="border: 2px solid red; padding: 10px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;"></td> <td style="padding: 0 10px;">Safe</td> <td style="text-align: right; background-color: #27ae60; color: white; border-radius: 15px; padding: 5px 10px;">39</td> </tr> <tr> <td style="text-align: center;"></td> <td style="padding: 0 10px;">Unsafe</td> <td style="text-align: right; background-color: #e74c3c; color: white; border-radius: 15px; padding: 5px 10px;">9</td> </tr> </table> </div>					Safe	39		Unsafe	9
	Safe	39							
	Unsafe	9							

Kuva 18





[PayloadSecurity](#)

📅 2016-01-10

```
submitname:"keyfinder.exe"
vxstream-threatscore:100/100
memurl:"Heuristic match: '' WMI Script - ChangeVLKey.vbs '' This script
changes the product key on the computer (XP SP1) '
*****
ON ERROR RESUME NEXT if Wscript.arguments.count<1 then
Wscrip,Pattern match: http://support.microsoft.com/default.aspx?
scid=kb;en-us;Q328874,Heuristic match:
http://www.magicaljellybean.com,Pattern match:
http://support.microsoft.com/default.aspx?scid=kb;en-
us;Q328874,Heuristic match: mailto:jellybean@magicaljellybean.com"
mutants:"\Sessions\1\BaseNamedObjects\Local\ZonesCounterMutex,\S
essions\1\BaseNamedObjects\Local\ZoneAttributeCacheCounterMutex,
\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex,\Sessi
ons\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex"
source:https://www.hybrid-
analysis.com/sample/47ab0544c45e7e745b2459018b4ca5aa1631602c
d6977a2a0ce73a2f5f454831?environmentId=4
```

Kuva 19

4 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

Kuukaudet

Monday	Maanantai	January	Tammikuu
Tuesday	Tiistai	February	Helmikuu
Wednesday	Keskiviikko	March	Maaliskuu
Thursday	Torstai	April	Huhtikuu
Friday	Perjantai	May	Toukokuu
Saturday	Lauantai	June	Kesäkuu
Sunday	Sunnuntai	July	Heinäkuu
		August	Elokuu
		September	Syyskuu
		October	Lokakuu
		November	Marraskuu
		December	Joulukuu

