Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Kauno technologijos universitetas

Kibernetinių atakų kompiuterių tinkle užkardinimo bei įsibrovimo prevencijos paslauga

Paslaugos aprašymas

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

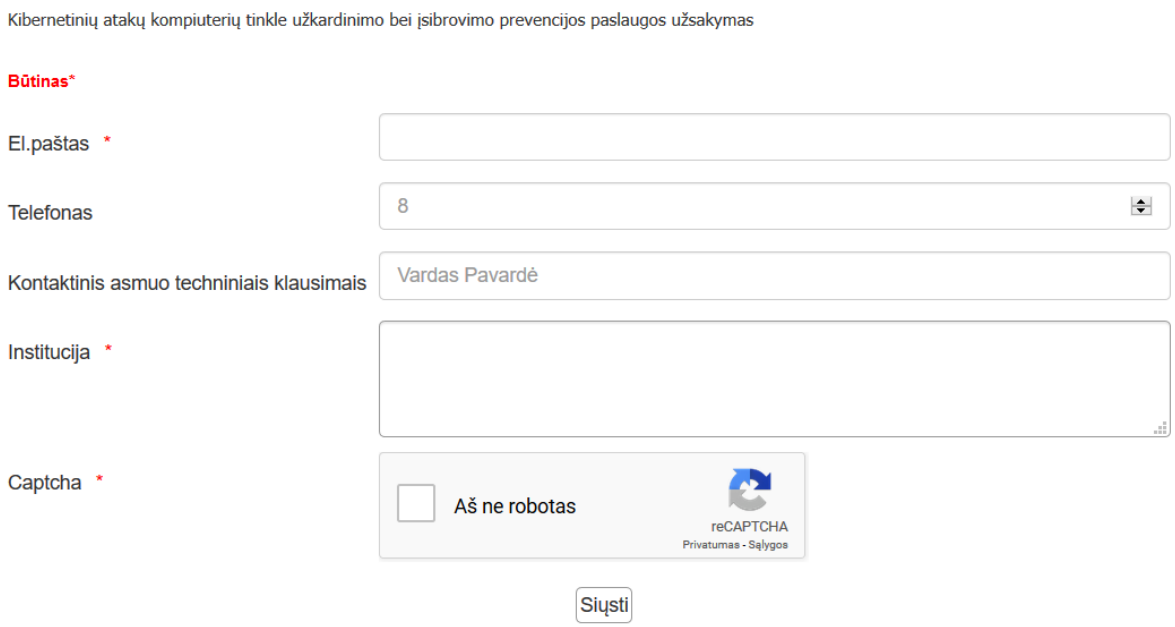
2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Kaunas, 2019 m.

Kibernetinių atakų kompiuterių tinkle užkardinimo bei įsibrovimo prevencijos paslaugos aprašymas

Prisijungimas ir paslaugos valdymas

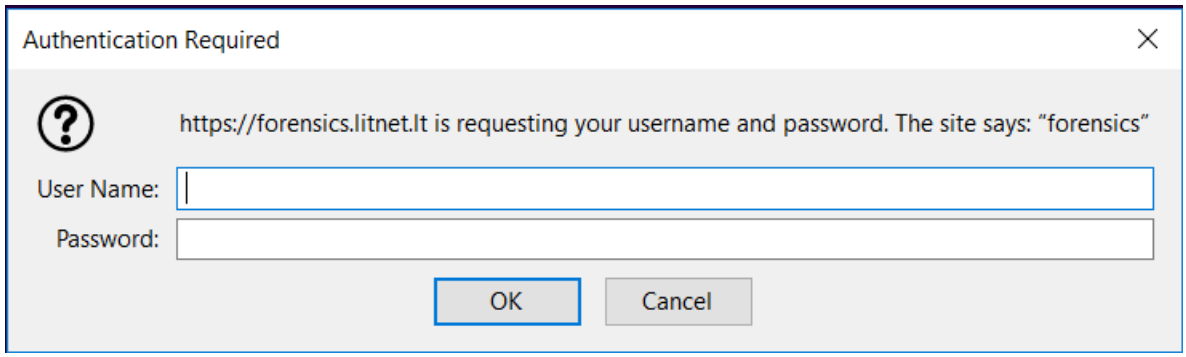
Naršyklės adreso lauke įvedę: https://litnet.lt/lt/component/visforms/?view=visforms&id=6 pradiniame lange gausite paslaugos užsakymo formą, kurią būtina užpildyti resursų tyrimams atlikti paskyrimui (rezervacijai). Norėdami pateikti užsakymą, privalote pilnai užpildyti užklausos formą ir spustelti puslapio apačioje mygtuką „**Siųsti**“. Pateikus šią formą, jūsų užsakymas bus peržiūrėtas artimiausiu metu ir nurodytu kontaktu atsiųsti prisijungimo prie šios paslaugos duomenys.



pav. 1 Paslaugos užsakymo forma

1 pav. pavaizduota paslaugos užsakymo forma, kurioje turite įvesti savo elektroninio pašto adresą, telefono numerį, kontaktinį asmenį techniniais klausimais, bei nurodyti instituciją.

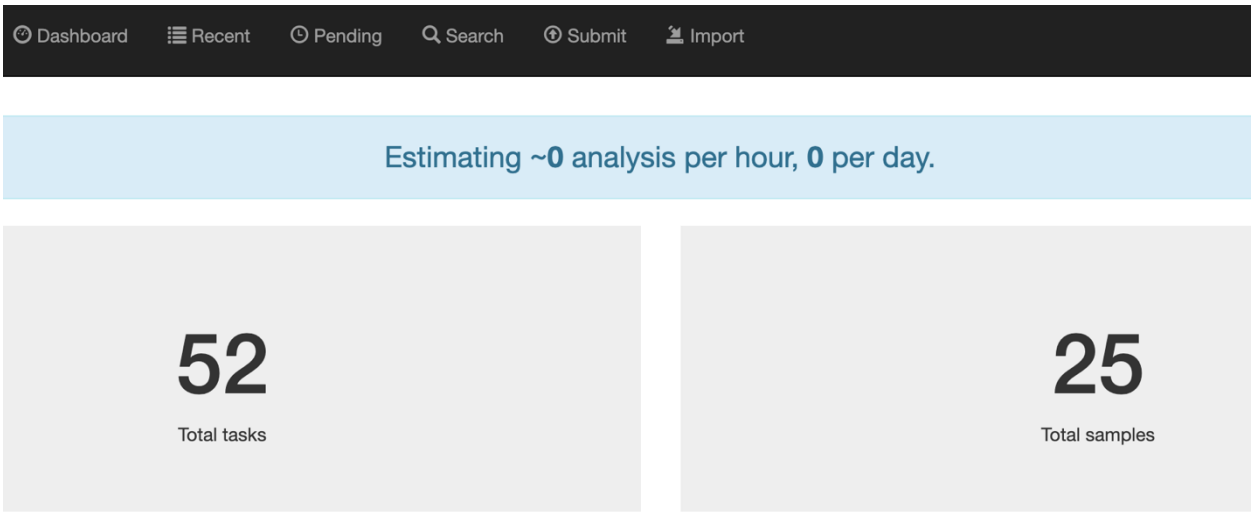
Prisijungimui prie paslaugos naudokite nuorodą: https://forensics.litnet.lt



pav. 2 Prisijungimo langas prie paslaugos

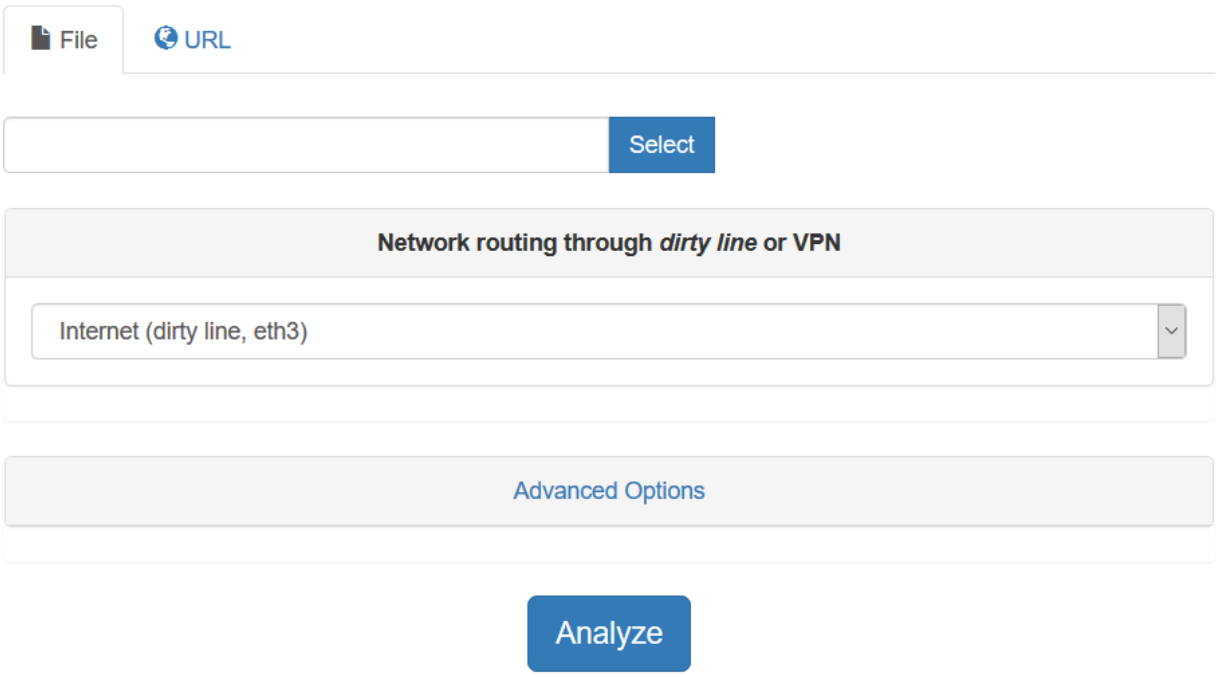
2 pav. pavaizduota prisijungimo prie paslaugos langas, kuriame turite įvesti prisijungimo duomenis atsiųstus į jūsų nurodytą elektroninio pašto dėžutę.

Pagrindiniame paslaugos lange matysite visus savo atliktus tyrimus ir tyrimus atliekamus šiuo metu. Jei jau pateikėte kenkėjišką kodą analizei, taip pat matysite per kiek laiko bus atlikta analizė Jūsų tolimesnei peržiūrai.



pav. 3 Atliktų užduočių skaičius

Norėdami pateikti analizei kenkėjišką kodą paspauskite mygtuką „**Submit**“. Atsiradus meniu punktui, Jūs galite įkelti („**File**“) savo kenkėjišką kodą, kuris gali būti analizuojamas simuliuojant Windows, bei Linux operacines sistemas. Taip pat galite pateikti nuorodą („**URL**“), kuri Jūsų manymu platina kenkėjišką kodą.

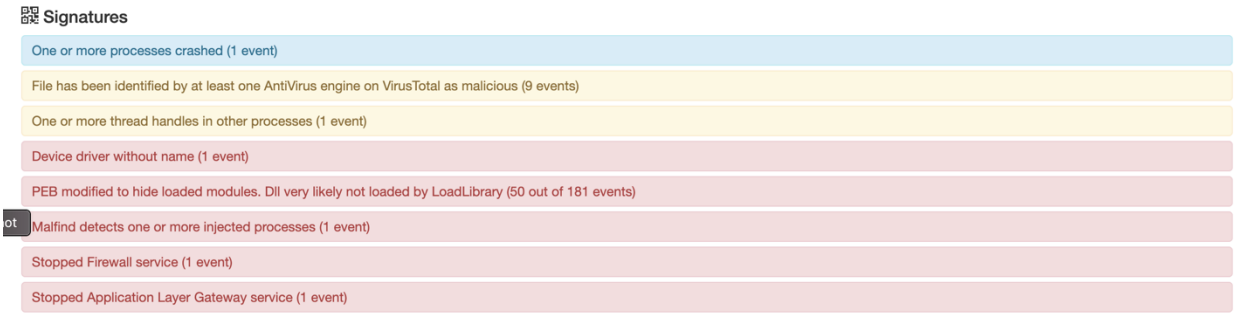


pav. 4. Kenkėjiškos programinės įrangos įkėlimas

4 pav. pavaizduota, kaip atrodo kenkėjiškos programinės įrangos įkėlimas į šią paslaugą. Paspaudus mygtuką „**Select**“ pasirinkite analizei kenkėjišką programinę įrangą ir spauskite mygtuką „**Analyze**“. Galite nelaukti atsakymo, nes tai užtruks tam tikrą laiką. Laiko trukmė priklauso nuo kenkėjiško kodo sudėtingumo. Baigus analizuoti jūsų kenkėjišką kodą (kenkėjišką programinę įrangą) informacija bus patalpina jūsų pagrindiniame tyrimų aplinkos lange (žr. 3 pav.)

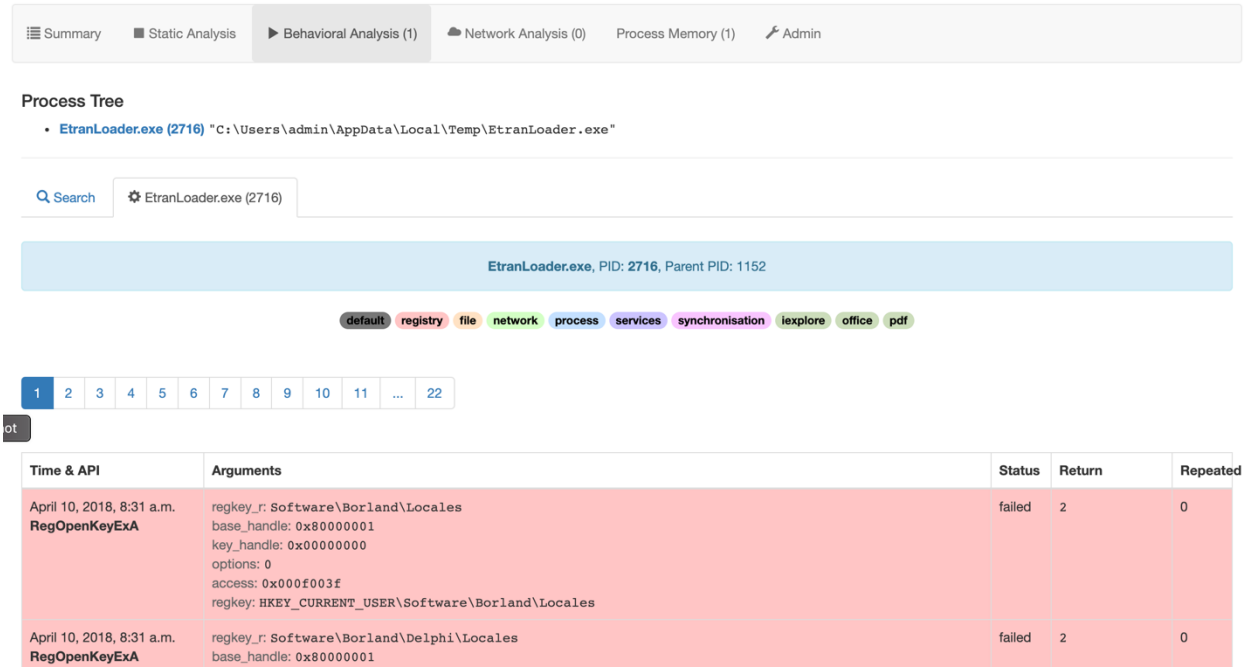
Kenkėjiško kodo analizė

Paslaugos atlikimo metu kenksmingo kodo aptikimas, gali būti suskirstytas į dvi pagrindines kategorijas: anomalijomis pagrįstas aptikimo metodas ir parašu pagrįstas aptikimo metodas. Anomalijomis pagrįstame aptikimo metode naudojamos žinios apie tai, kas yra žinoma kaip tinkamas elgesys ir nusprendžiama ar tikrinama programa yra kenksminga. Specifikacija pagrįstas aptikimas yra specifinis anomalijomis pagrįsto aptikimo metodo tipas. Naudojant specifikacija pagrįstą aptikimo metodą naudojami specifikacijų ar taisyklių rinkiniai, kuriuose yra apibrėžta kas tai yra tinkamas elgesys (atliekamas realus programos paleidimas simuliacinėje Windows ir Linux operacinėje aplinkoje) ir tuomet algoritmų pagalba nusprendžiama ar tikrinama programa yra kenksminga ir jei suteikiamas „parašas“ (žr. 5 pav.).



pav. 5 Kenkėjiškos programos parašas

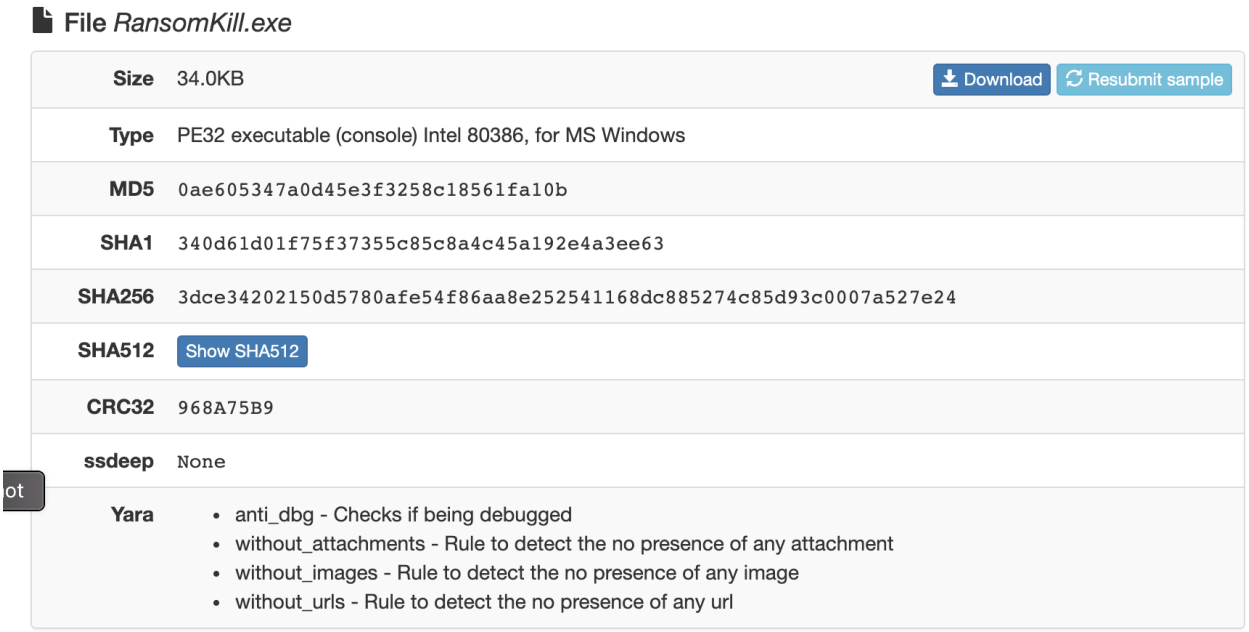
Kenkėjiškas kodas vykdo ataką išnaudodamas taikomosios programos pažeidžiamumus, todėl kenkėjiškos elgsenos nagrinėjimo tyrimams reikalingas tam skirtos aplinkos, turinčios programas su tokio tipo pažeidžiamumais virtualioje aplinkoje. Norint analizuoti įvairias kenkėjiškas programas, yra sukurta universali ir lanksti aplinka. Visa tai reikalauja daug kompiuterinių resursų ir laiko, todėl kai kurie tyrimai gali užtrukti. Taip pat pilnam tyrimui yra atliekama dinaminė analizė. Ji atliekama virtualios aplinkos sistemoje, kadangi ataka vykdoma tiesiogiai sistemoje (žr. 6 pav.).



pav. 6 Kenkėjiško kodo simuliacija ir analizė

Šios virtualios aplinkos sistemos yra inicializuojamos tiek kartų, kiek yra analizuojama atakų vektorių turintis kenkėjiškas kodas ar internetinė nuoroda, kas reiškia jog yra labai efektyviai naudojami tyrėjų turimi ištekliai.

Kenksmingo kodo detektorius (algoritmas) yra įrankis, sudarytas naudojant keletą kenksmingo kodo aptikimo metodų. Kenksmingo kodo detektorius bando apsaugoti sistemą, aptikdamas kenksmingą elgseną ir pateikia informacija apie tiriamą objektą (žr. 7 pav.)



pav. 7 Informacija apie kenkėjišką kodą

ir įvertiną jo riziką (žr. 8 pav.). Rizikai vertinti naudojama skalė nuo 0 iki 10.

pav. 8 Kenkėjiško kodo vertinimas

Detektorius gali būti arba gali nebūti toje pačioje sistemoje, kurią bando simuliuoti kenkėjiško kodo elgsenos aplinka. Detektoriaus veikimas yra pagrįstas aprašytais kenksmingo kodo aptikimo metodais, kurie nulemia aptikimo pajėgumą.

Sėkmingai atlikti tyrimai ir jų ataskaitos visada bus prieinamos jūsų pagrindinėje aplinkoje (žr. 3 pav.). Čia matysite ar paslauga atlikta, skaičių kiek atlikta tyrimų, kiek atliekamų šiuo metu. Sėkmingai baigus tyrimus, bei susipažinus su tyrimu rezultatais galite atsijungti nuo tyrimų aplinkos.