



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 užkardavimo bei įsibrovimo prevencijos paslaugos aprašymas

## Prisijungimas ir paslaugos valdymas

Naršyklės adreso lauke įvedę: <https://litnet.lt/lt/component/visforms/?view=visforms&id=6> pradiniam lange gausite paslaugos užsakymo formą, kurią būtina užpildyti resursų tyrimams atlikti paskyrimui (rezervacijai). Norėdami pateikti užsakymą, privalote pilnai užpildyti užklauso 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.

Kibernetinių atakų kompiuterių tinkle užkardavimo bei įsibrovimo prevencijos paslaugos užsakymas

**Būtinas\***


El.paštas \*

Telefonas

Kontaktinis asmuo techniniais klausimais

Institucija \*

Captcha \*

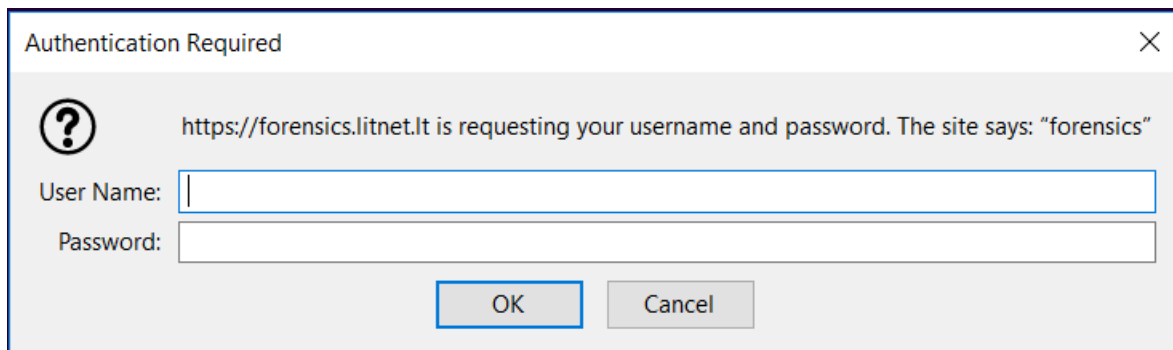
 Aš ne robotas   
reCAPTCHA  
Privatumas - Sąlygos

Siųsti

*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.

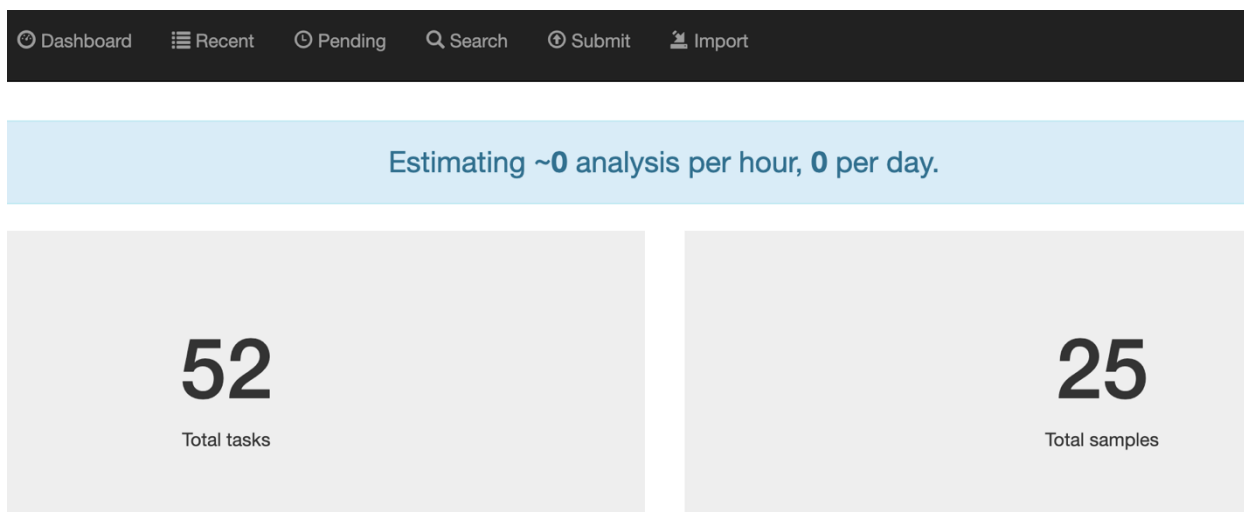
Prisijungimui prie paslaugos naudokite nuorodą: <https://forensics.litnet.lt>



*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.

The image shows a web interface for uploading and analyzing malicious code. At the top, there are two tabs: 'File' and 'URL'. Below them is a text input field and a blue 'Select' button. A section titled 'Network routing through *dirty line* or VPN' contains a dropdown menu with 'Internet (dirty line, eth3)' selected. Below this is an 'Advanced Options' section. At the bottom, there is a large blue 'Analyze' button.

*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.).

## Signatures

One or more processes crashed (1 event)
File has been identified by at least one AntiVirus engine on VirusTotal as malicious (9 events)
One or more thread handles in other processes (1 event)
Device driver without name (1 event)
PEB modified to hide loaded modules. DLL very likely not loaded by LoadLibrary (50 out of 181 events)
Malfind detects one or more injected processes (1 event)
Stopped Firewall service (1 event)
Stopped Application Layer Gateway service (1 event)

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.).


The screenshot shows a behavioral analysis tool interface. At the top, there are tabs for Summary, Static Analysis, Behavioral Analysis (1), Network Analysis (0), Process Memory (1), and Admin. Below the tabs, the "Process Tree" section shows a single entry: "EtranLoader.exe (2716) 'C:\Users\admin\AppData\Local\Temp\EtranLoader.exe'". A search bar contains "EtranLoader.exe (2716)". Below this, a blue bar displays "EtranLoader.exe, PID: 2716, Parent PID: 1152". A row of colored tags includes default, registry, file, network, process, services, synchronisation, iexplore, office, and pdf. A pagination bar shows numbers 1 through 22. Below the pagination bar, a table displays process events.

Time & API	Arguments	Status	Return	Repeated
April 10, 2018, 8:31 a.m. RegOpenKeyExA	regkey_r: Software\Borland\Locales base_handle: 0x80000001 key_handle: 0x00000000 options: 0 access: 0x000f003f regkey: HKEY_CURRENT_USER\Software\Borland\Locales	failed	2	0
April 10, 2018, 8:31 a.m. RegOpenKeyExA	regkey_r: Software\Borland\Delphi\Locales base_handle: 0x80000001	failed	2	0

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.)

 File *RansomKill.exe*

<b>Size</b>	34.0KB	<a href="#">Download</a>	<a href="#">Resubmit sample</a>
<b>Type</b>	PE32 executable (console) Intel 80386, for MS Windows		
<b>MD5</b>	0ae605347a0d45e3f3258c18561fa10b		
<b>SHA1</b>	340d61d01f75f37355c85c8a4c45a192e4a3ee63		
<b>SHA256</b>	3dce34202150d5780afe54f86aa8e252541168dc885274c85d93c0007a527e24		
<b>SHA512</b>	<a href="#">Show SHA512</a>		
<b>CRC32</b>	968A75B9		
<b>ssdeep</b>	None		
<b>Yara</b>	<ul style="list-style-type: none"><li>• anti_dbg - Checks if being debugged</li><li>• without_attachments - Rule to detect the no presence of any attachment</li><li>• without_images - Rule to detect the no presence of any image</li><li>• without_urls - Rule to detect the no presence of any url</li></ul>		

*pav. 7 Informacija apie kenkėjišką kodą*

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

### Score

This file shows numerous signs of malicious behavior.

The score of this file is **4.8 out of 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.