

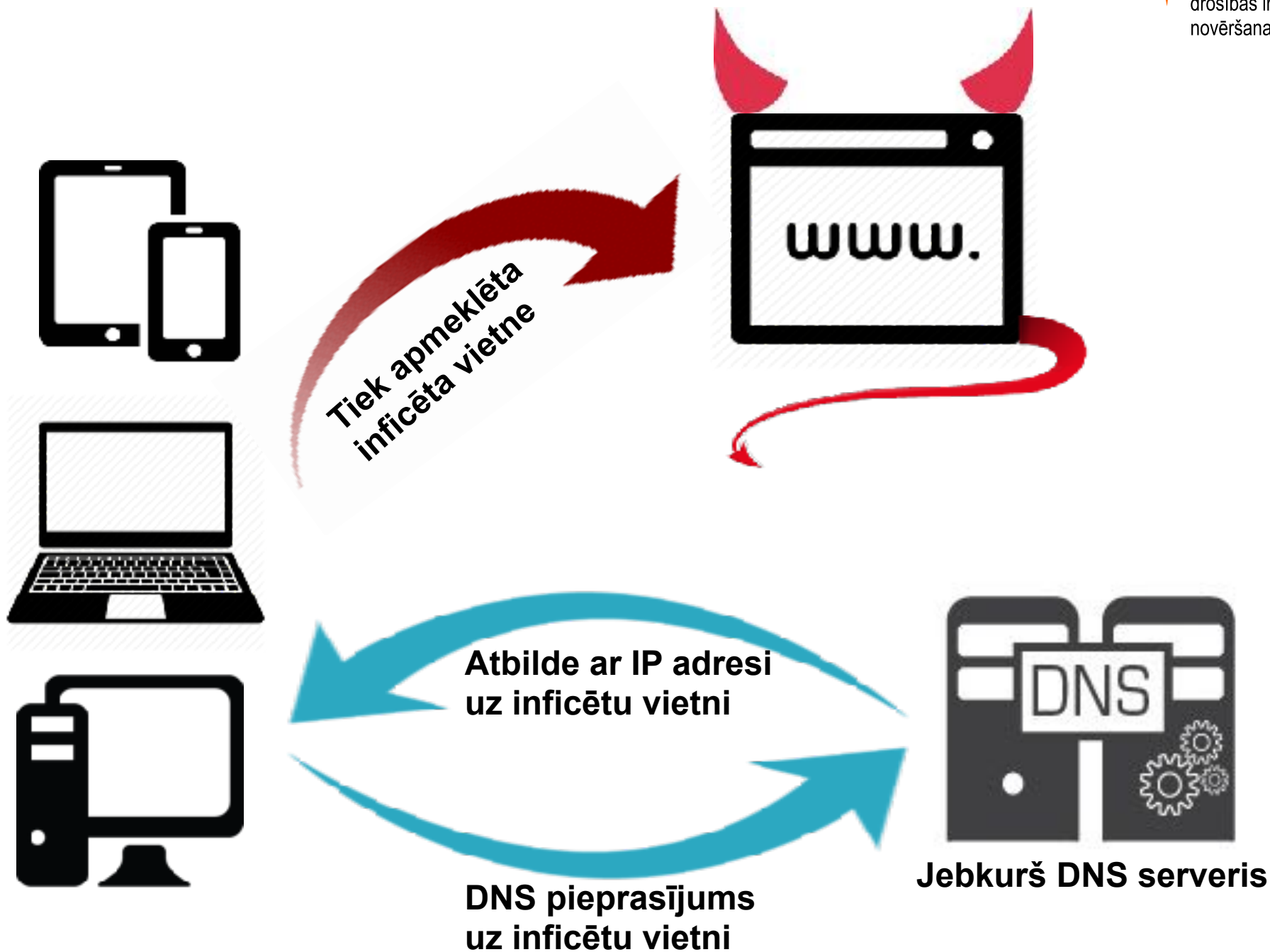


DNS Ugunsgrāvis

Varis Teivāns, CERT.LV

- Plaša mēroga IKT drošības apdraudējumu mazināšana ar viegli ieviešamu, pieejamu un uzticamu servisu
- Aktīva aizsardzība
 - Apturēt infekcijas pirms tās varētu iestāties
- Infekcijas seku ātrāka novēršana
 - Identificēt jau inficētas iekārtas un koordinēt incidenta novēršanu

Tradicionāli DNS pieprasījumi



CERT.LV DNS ugunssmūris



Tiek apmeklēta drošas piezēmēšanās vietne



Drošas piezēmēšanās vietne



Atbilde ar drošas vietnes IP adresi

DNS pieprasījums uz inficētu vietni



CERT.LV DNS RPZ

RPZ zonas transfer



DNS RPZ

NIC.LV DNS rekursīvie serveri ar CERT.LV DNS ugunssmūri

CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija



Tiek apmeklēta
drošas piezēmēšanās
vietne



Drošas
piezēmēšanās
vietne



Atbilde ar drošas
vietnes IP adresi

DNS pieprasījums
uz inficētu vietni

91.198.156.20
2a02:500:4400:400::4

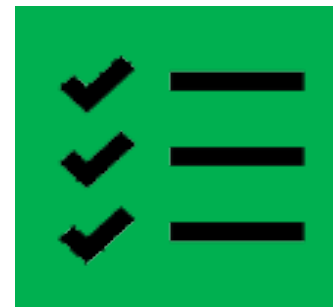
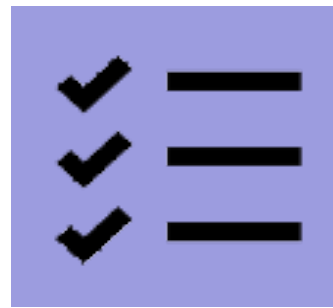


**NIC.LV rekursīvie
DNS serveri**

CERT.LV DNS ugunsmūra zonas

CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija



HIGH-RISK

WEB-MINERS

PHISHING

MALWARE

CERT-SHIELD

**CERT.LV DNS
ugunsmūra
klienti**



DNS RPZ

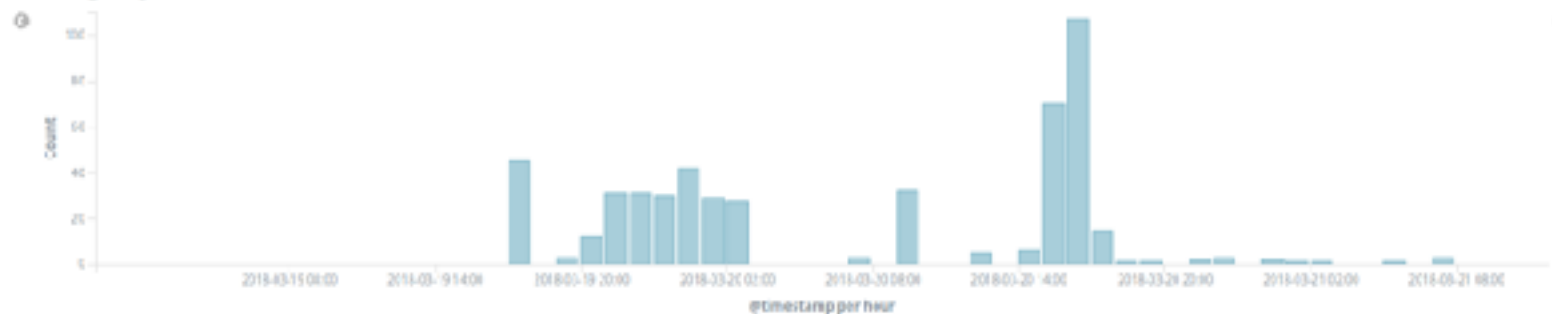
NIC.LV Rekursīvie DNS

Analīze un atgriezeniskā saite

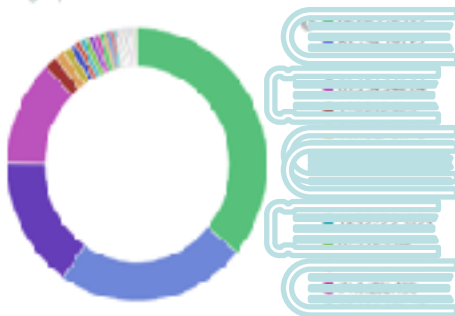
landing-count

Count:
502
Count:

landing-histogram



landing-top-clients



landing-top-verbs



landing-top-requests

request.keyword: Descending	Count
/	387
/favicon.ico	94
/malware.exe	23
/malware	21
/evil.exe	6
/malwarecard	3
/ccw	3
/ccw/commen.cdf	3

landing-top-referrers

referrer.keyword: Descending	Count
-	429
http://testbestest222.lv/	10
http://testbestest200.lv/	9
http://213.145.215.215/malware.exe	5
http://213.145.215.215/malware.exe	5
http://213.145.215.215/malware.exe	5
http://213.145.215.215/malware.exe	5
http://213.145.215.215/malware.exe	5
http://213.145.215.215/malware.exe	5

landing-top-agents

agent.keyword: Descending	Count
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	150
Mozilla/5.0 (11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.146 Safari/537.36	134
Mozilla/5.0 (11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0	68
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) AppleWebKit/604.5.6 (KHTML, like Gecko) Version/11.0.3 Safari/604.5.6	48
Mozilla/5.0 (11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.162 Safari/537.36	39
-	17
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12; rv:58.0) Gecko/20100101 Firefox/58.0	12
Viper(linux)	12
Microsoft-CryptoAPI.1	7
Go-http-client/1.1	3
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.2001.102 Safari/537.36	3
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64)	3
Mozilla/5.0 (2008/03)	3

Kā pieteikties pilnai servisa paketēm?

CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

- **mailto:** cert@cert.lv
- **subject:** CERT.LV DNS firewall
- **body:**
 - Iestādes nosaukums
 - Kontaktpersona



Paldies!

https://www.nic.lv/static/data/NIC_Newsletter_2018Nr6.pdf

Varis Teivāns, CERT.LV