Core Infrastructure Protection from Distributed Denial-of-Service (DDoS) Attacks

Uldis Lībietis

Tet Chief information security officer

Corporate structure

Republic of Latvia **51%**

49% Telia Company

Citrus Solutions

T2T

Helio Media

Baltic Computer Academy

Data Experts

35% Overkill Ventures

Brand structure

Tet

Technology Brand

Tet Data Centres:
Cloud Services
Virtual Platforms

IT Solutions, IT audit

Tet SOC

Tet GDPR Consultations

Electricity

Technology

Tet Internet for business

Tet IT security

Entertainment Brand

Helio Media
Contents (360TV, STV, Broadcasts)
Advertisements

Local Content

Baltic eSports League

HyperTown RIX, TLL

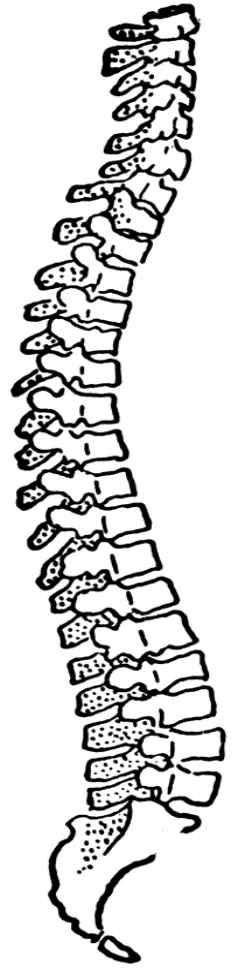
Helio iTV

Helio vTV

Shortcut

Internet for Entertainment

Tet is a **Backbone of Latvian internet** with more than 54% of internet connections

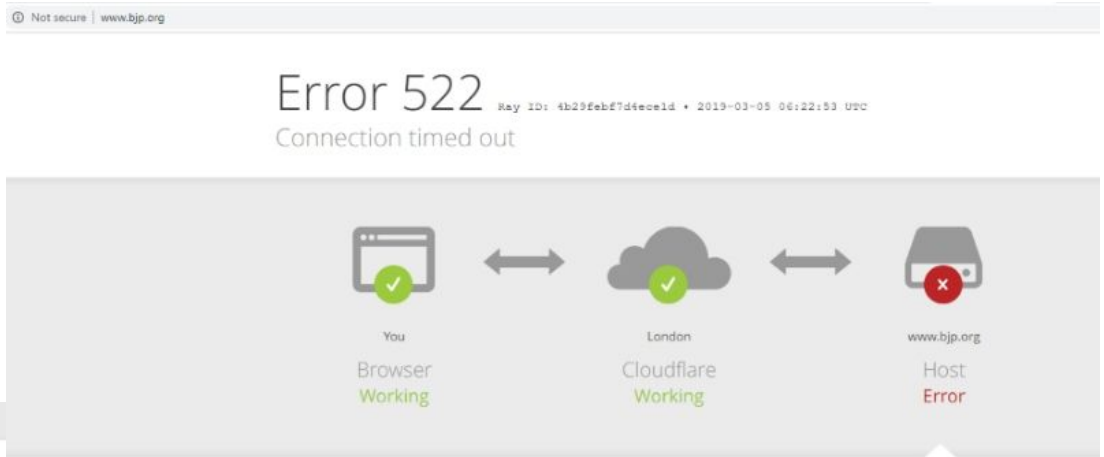


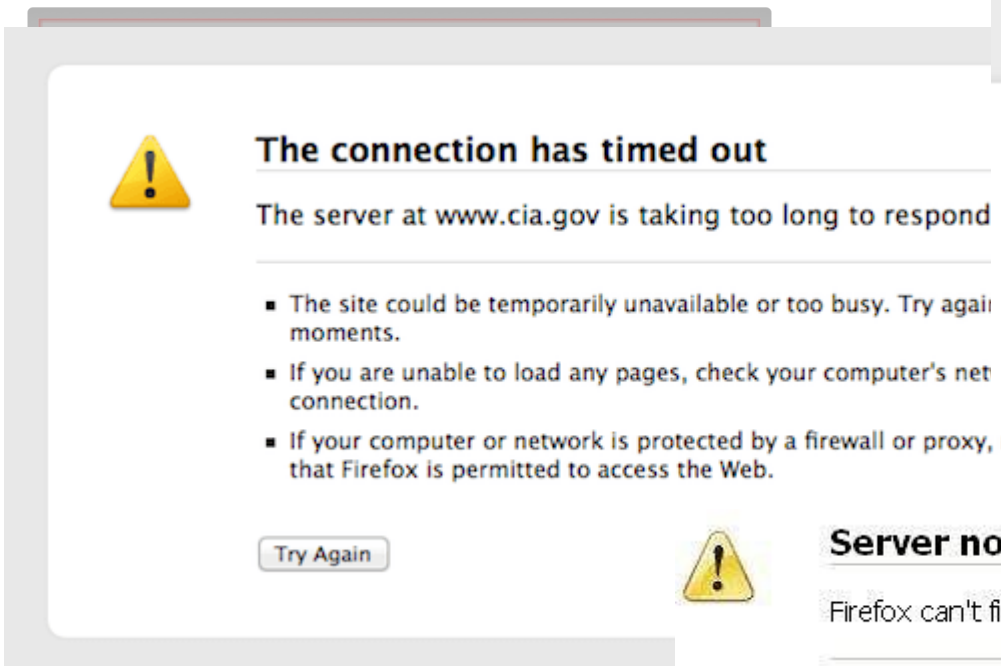
Western Europe and CEE telecommunication market matrix

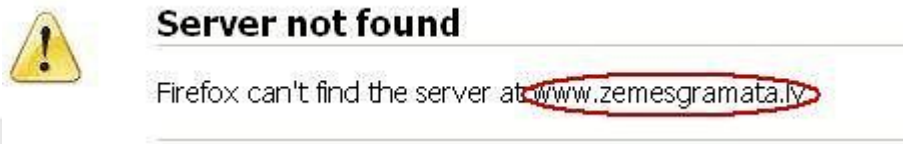
Todays to-do list

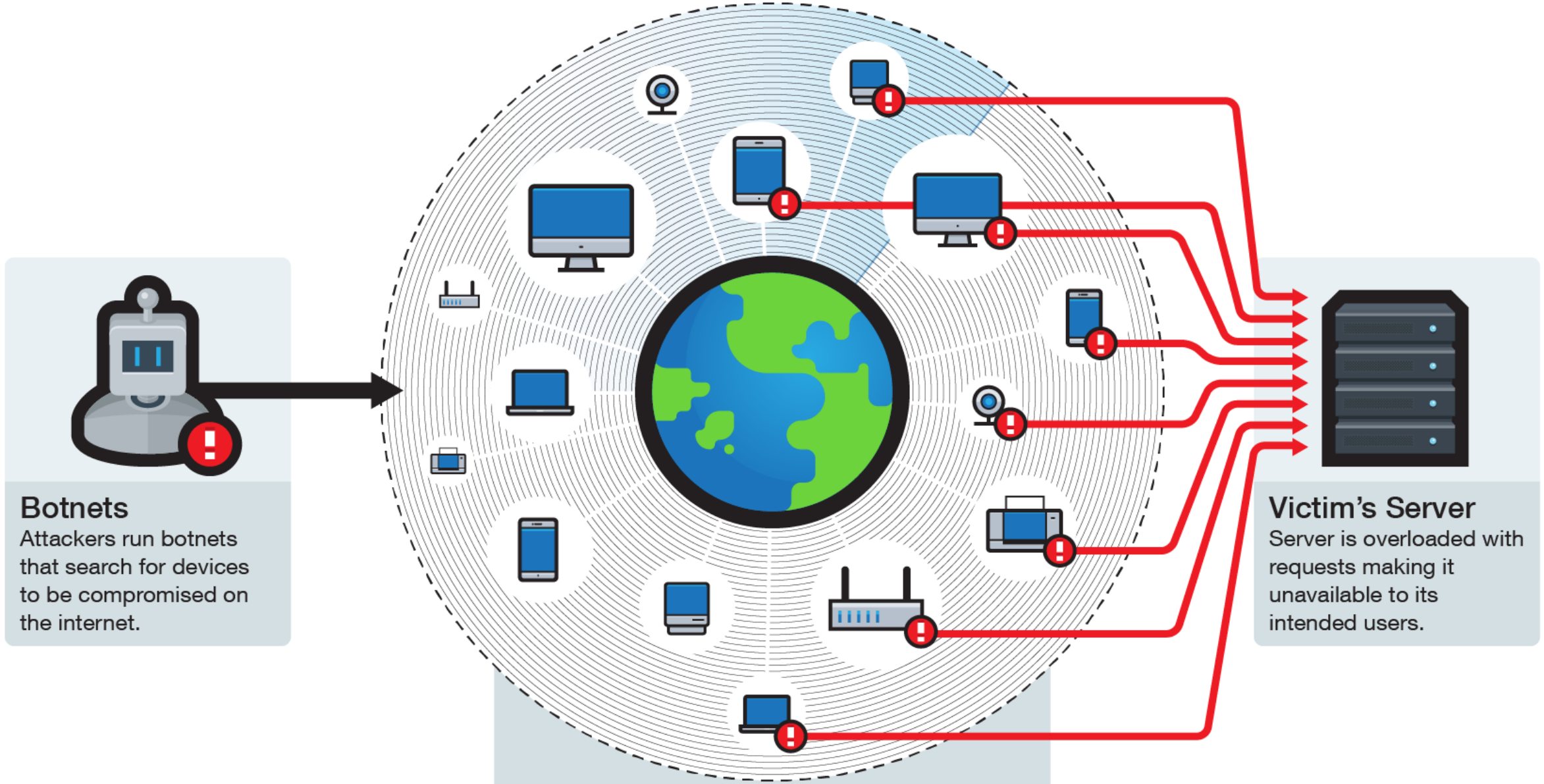
- Overview about last years
- Cybersecurity challenges within ISP
- DDoS is getting smarter
- Our approach
- What to do next

Most of you have seen this









Botnets

Attackers run botnets that search for devices to be compromised on the internet.

Internet

Devices with low security are infected and transformed into botnets to launch DDos attack.

Victim's Server

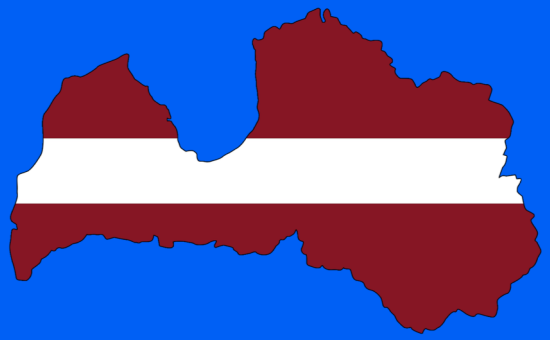
Server is overloaded with requests making it unavailable to its intended users.

Image Source: TrendMicro

Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	**1** Concurrent +	**1** Concurrent +	**1** Concurrent +	**1** Concurrent +
300 seconds boot time	**600** seconds boot time	**1200** seconds boot time	**1800** seconds boot time	**3600** seconds boot time
125Gbps total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity
Resolvers & Tools	**Resolvers** & Tools	**Resolvers** & Tools	**Resolvers** & Tools	**Resolvers** & Tools
24/7 Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

Examples from Latvia



Government institutions

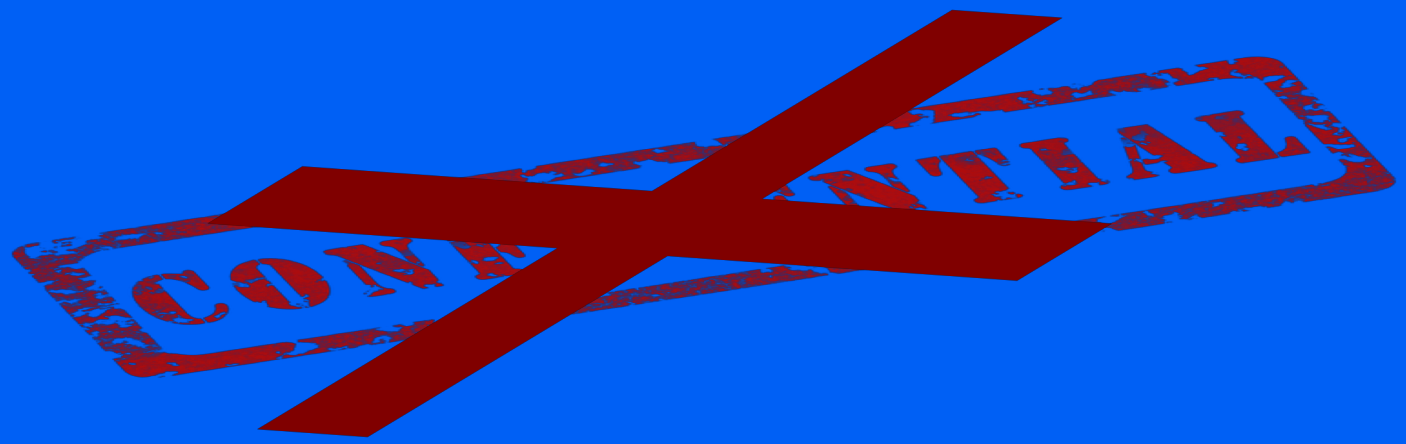
Critical services

News portals

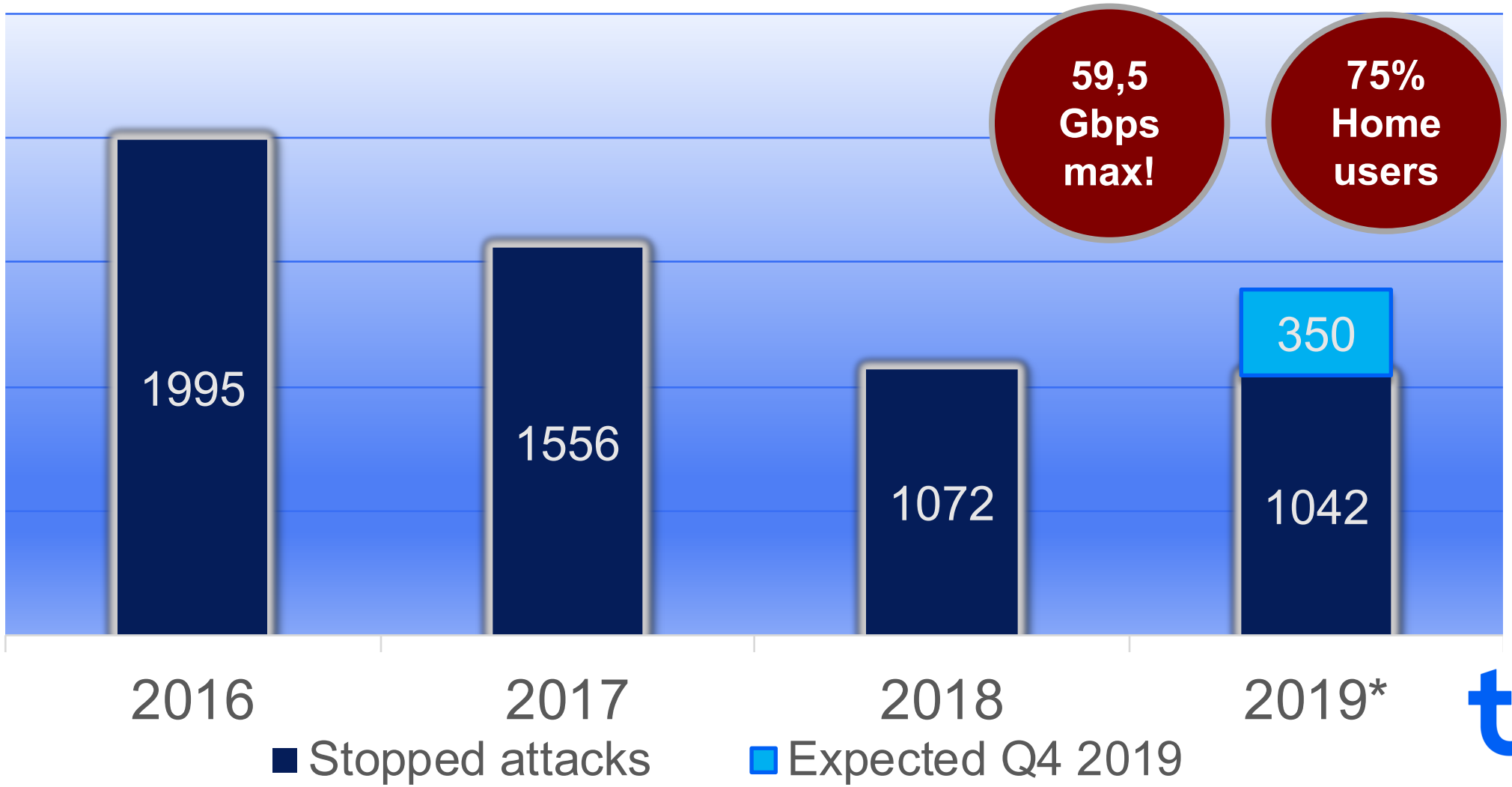
Mass services

Private Enterprises

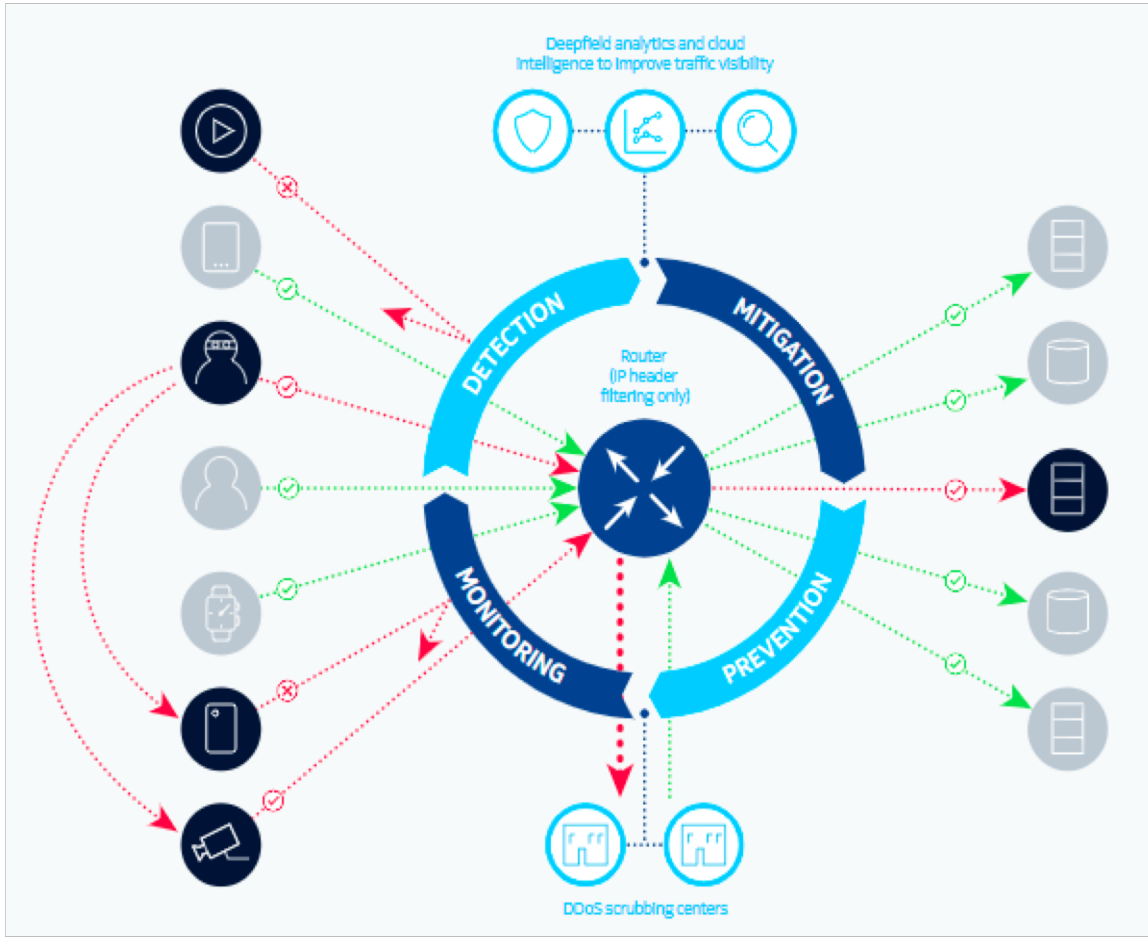
What about Tet?



DDoS on Tet core infrastructure



- **Rate limit** access lists on BGP level
- **Advanced IPS/IDS** on enterprise level
- **Full Flow investigation** on application level
- **NBA, AI, ML** for advanced automation



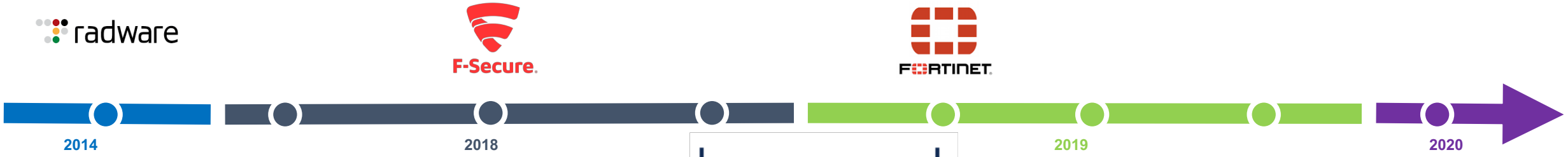
Tet Cybersecurity Services in progress

DDoS Protection
Oct (2014)

Lattelecom Endpoint Protection
May (2018)

Virtual FW and UTM (**SD-WAN**)
Jul (2019)

SOC as Service
(Oct 2019)



Vulnerability Management Services
Jan (2018)

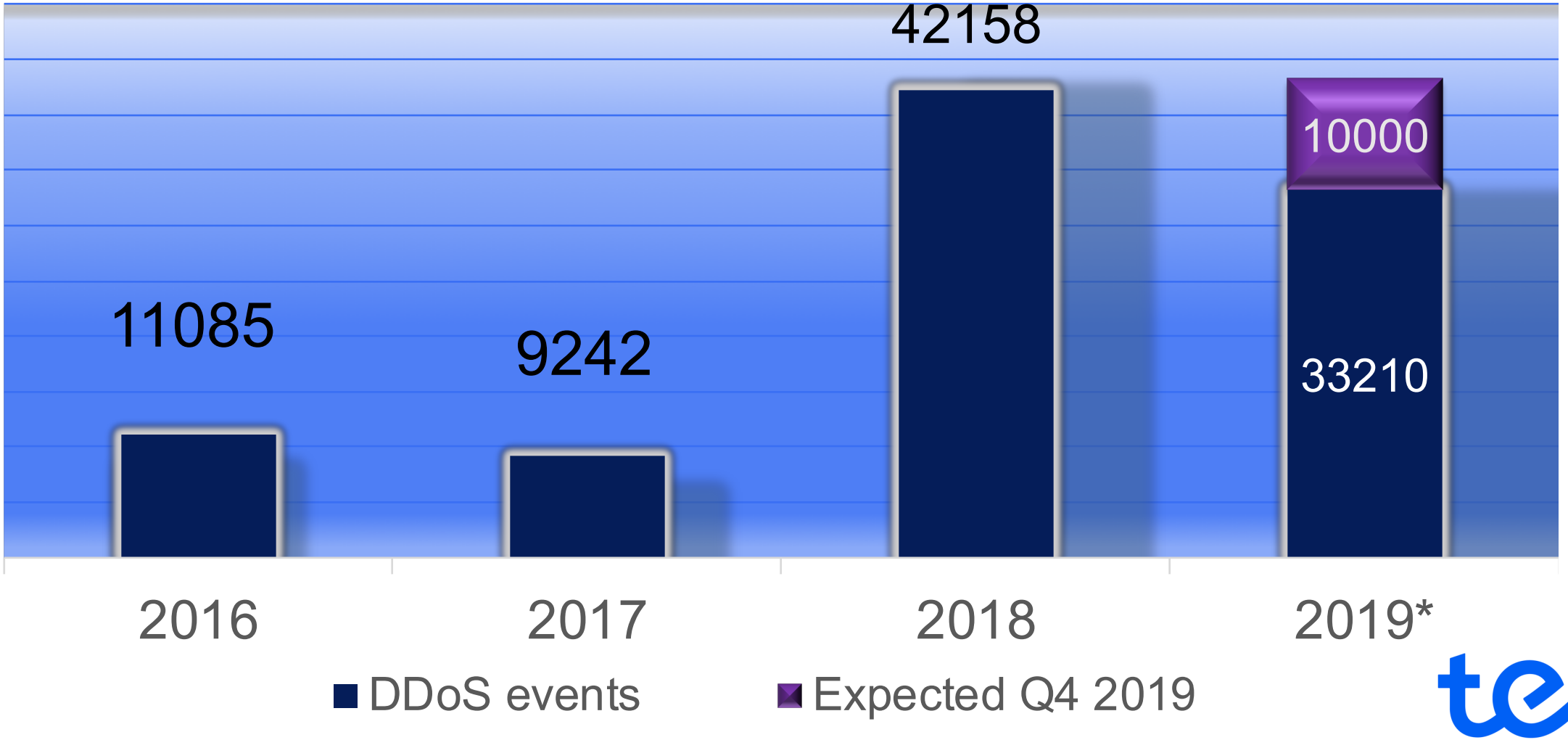
IT/GDPR Audit
Jan (2018)

Vulnerability and Penetration Services
Nov (2018)

SIEM as Service
Jun (2019)

Next gen DDoS Protection
Q1 (2020)

DDoS events per year



UK Police Arrest Suspect Behind Mirai Malware Deutsche Telekom

By **Catalin Cimpanu** February 23, 20

Technology

Extortionist Arrested In US For Hitting Sites With DDoS Attacks

By AJ Dellinger
07/31/17 AT 2:39 PM

Authorities in the United States arrested a man last week who has been charged with launching distributed denial of service, or DDoS, attacks and making threats against a number of major targets.

The man in custody is Kamyar Jahanrakhshan, an Iranian-born man who launched a number of attacks designed to interrupt the service and threaten the operations of a number of new publications and websites including Leagle.com, the Sydney Morning Herald, the Canadian Broadcasting Corporation (CBC) and Metro News Canada.

Read: *Mirai Botnet: Hacker Admits To DDoS Attack Against Deutsche Telekom*

PCWorld
FROM IDG

Privacy

Home / Hacking

NEWS

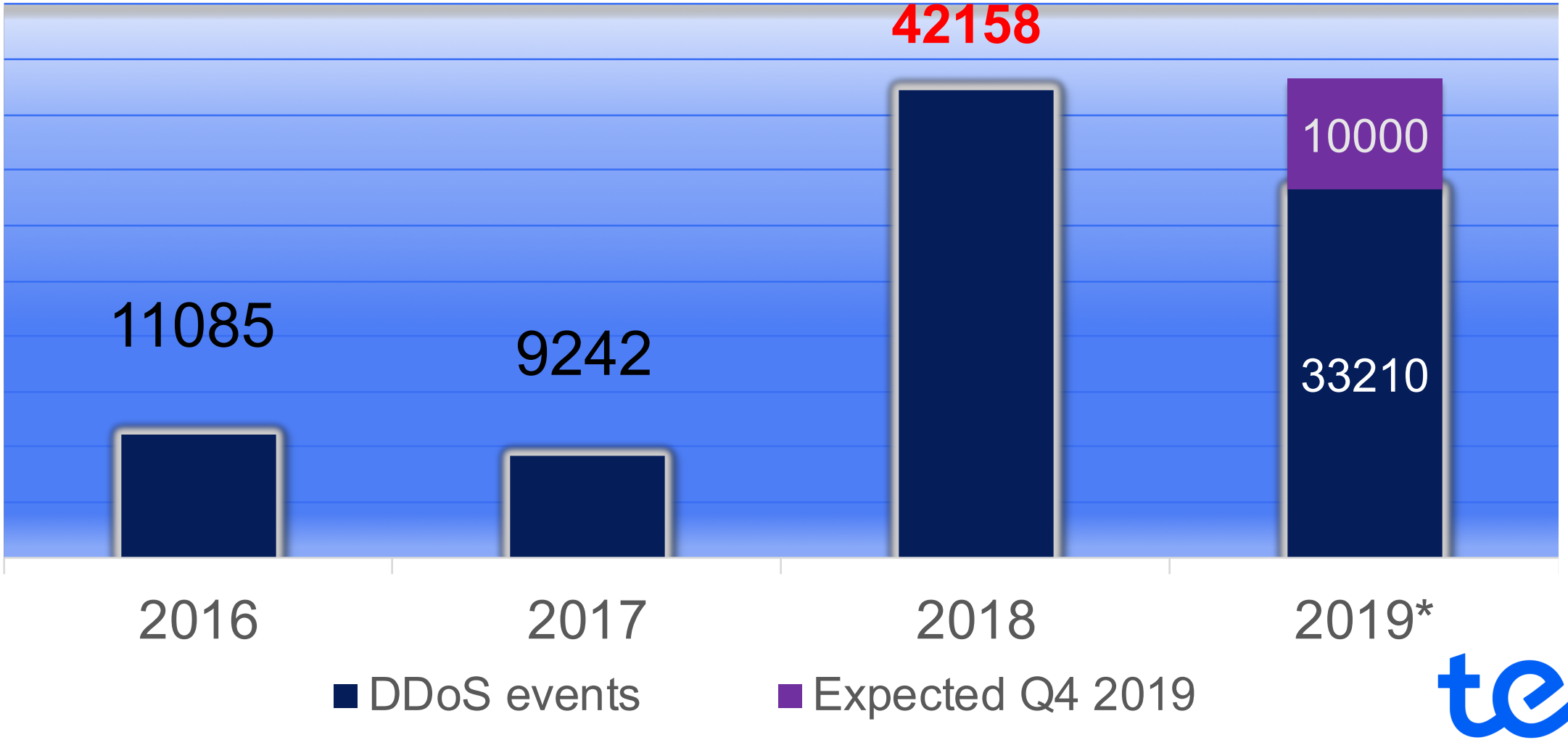
Dozens arrested in international DDoS-for-hire crackdown

The arrests targeted buyers of DDoS-for-hire services, which make a profit by shutting down Internet-connected systems

By Michael Kan
U.S. Correspondent, IDG News Service

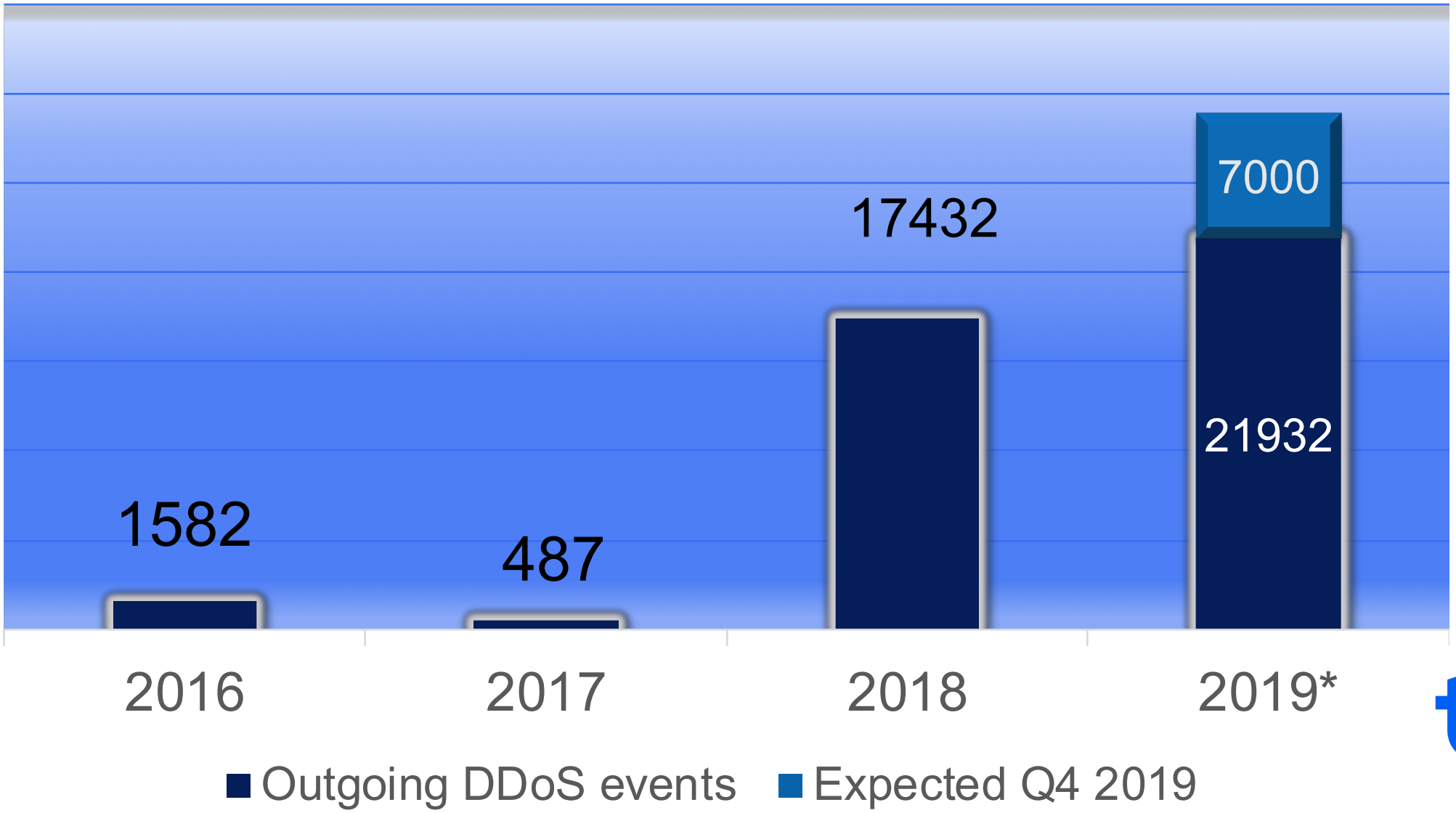
tet

DDoS events per year



What happened in 2018?

LV internet users involved in DDoS



Picture source: videogame Honor Night Samurai cover

Typical outgoing DDoS

- Attackers group size — 100
- Traffic from one group — 300 Mbps
- Attack duration, minutes — 1,5
- Task shift between groups — YES

Extreme outgoing DDoS values from Latvia

- Attackers group size — 2000
- Traffic generated — 2,6 Gbps
- Attack duration, minutes — 5
- Multiple attacks a day — YES

Sveiki!

Paldies, ka savā ikdienā izmanto Tet sniegtos pakalpojumus.
Lai saņemtie pakalpojumi vienmēr būtu kvalitatīvi, Tet uztur un seko līdzi tīkla infrastruktūras drošībai, kā arī sadarbojas ar IT drošības incidentu novēršanas institūciju - CERT.LV. Tiklīdz ir konstatēti kādi pārkāpumi vai incidenti, piemēram, datorvīrusa izplatīšanās, lietotājs tiek informēts. Plašāk par drošības prasībām var izlasīt Informācijas tehnoloģiju drošības likumā.

Esam saņēmuši informāciju no CERT.LV, ka Tava lietotā ierīce, iespējams, ir inficēta vai pakļauta ievainojamībai.

Vairāk par infekciju vai ievainojamību var uzzināt šeit:
http://www.esidross.lv/cert-lv-bridinajums/?hash/b965ee90669ee1824ec7567a19828642

Statiskas IP adreses, platjoslas pieslēgumu servisa numuri, kuri izplata infekciju un pārkāpuma datums:

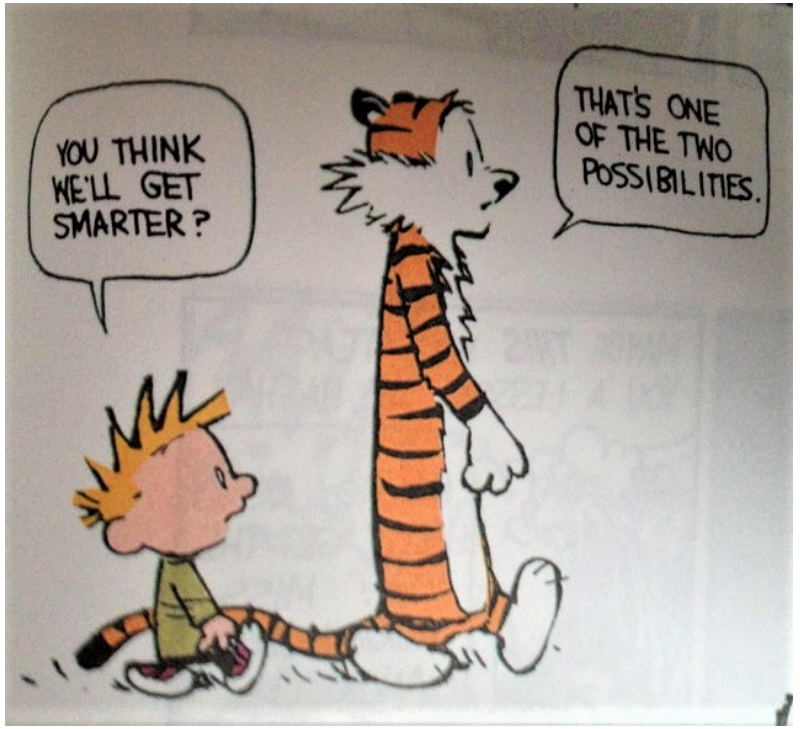
Recent DDoS Attacks Rattle Online Poker Industry

The typical DDoS poker cheating technique targets a specific user

Exchanges for the digital currency Bitcoin have often been the target for attacks

Sometimes with the intention of stealing money directly, other times simply to induce investor panic

Hackers are getting smarter



Challenges for the future

- DDoS still alive and growing
- Smarter attacks
- Local attackers – geo filtering will not work
- IoT expansion – more vulnerable devices
- Industrial security
- AI/ML expansion for better attack planning

In case of attack

- Don’t panic
- Have a communication plan
- Identify attack
- Know your recourses and weaknesses
- Mitigate attack by using anti-DDoS solutions

If you can't do it yourself, hire a partner

We will manage your IT Security

TET Security Operational Center

24/7/365

tet

Tet IT Security

Thank you!

Meet us @

Riga Comm – 10.10.2019

DSS ITSEC – 17.10.2019

Payment Market Conference - 24.10.2019

RIGA COMM 2019

2019 10th ANNIVERSARY DSS ITSEC FOR ITSEC PROFESSIONALS

Latvian member of EPCA Vedicard www.vedicard.eu

tet