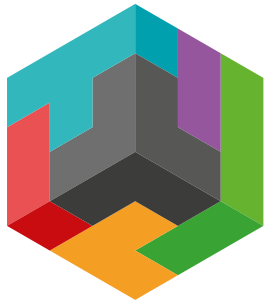


Správa informačních technologií Plzeň

Jak řešíme aplikační ochranu v Plzni

Jakub Bělka – Správa informačních technologií města Plzně

Martin Kylián – F5

F5 HW platformy

A Next-Gen, Fully Automatable Platform

r12000-DS

r10000

r5000

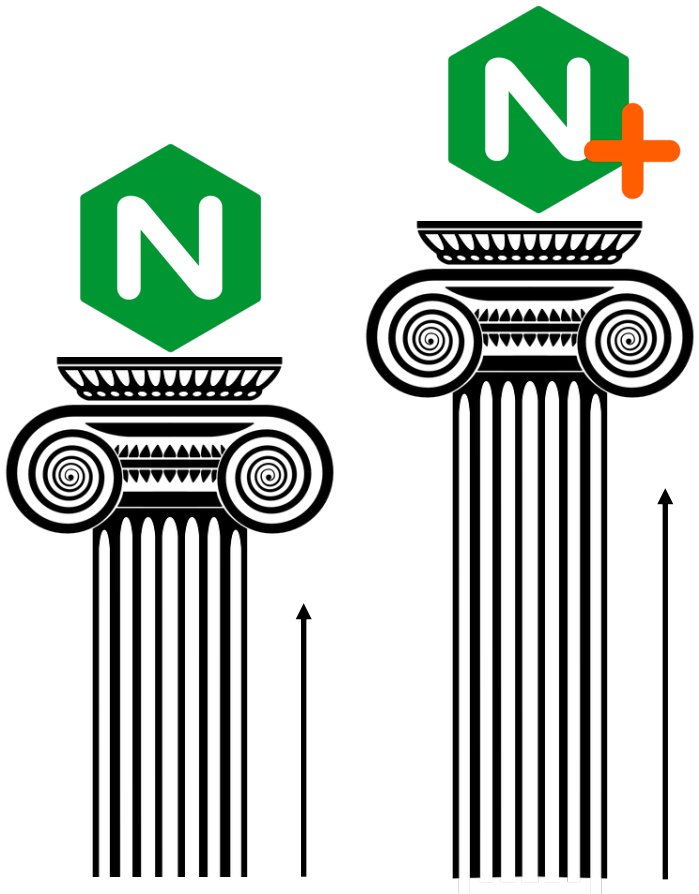
r4000

r2000

VELOS

F5 není jen BIG-IP

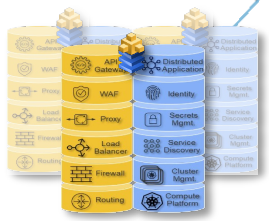
NGINX open source
HTTP2
JSON Logging
Stream Module (TCP… UDP)
Multi Datagram UDP Support
Thread Pools
Dynamic Modules
JavaScript Module for NGINX
ECC Certificate Support
Linux Enhancements



NGINX Plus
All of Core Plus:
+ Authentication
+ High Availability
+ Web App Firewall (NGINX App Protect / DOS)
+ Centralized Management
+ App Performance Analytics
+ K8S Services Discovery
+ API configuration
+ Enterprise-level supports within 30 minutes
+ First-priority CVE response

F5 Distributed Cloud SaaS platforma

Application Delivery Network (ADN)



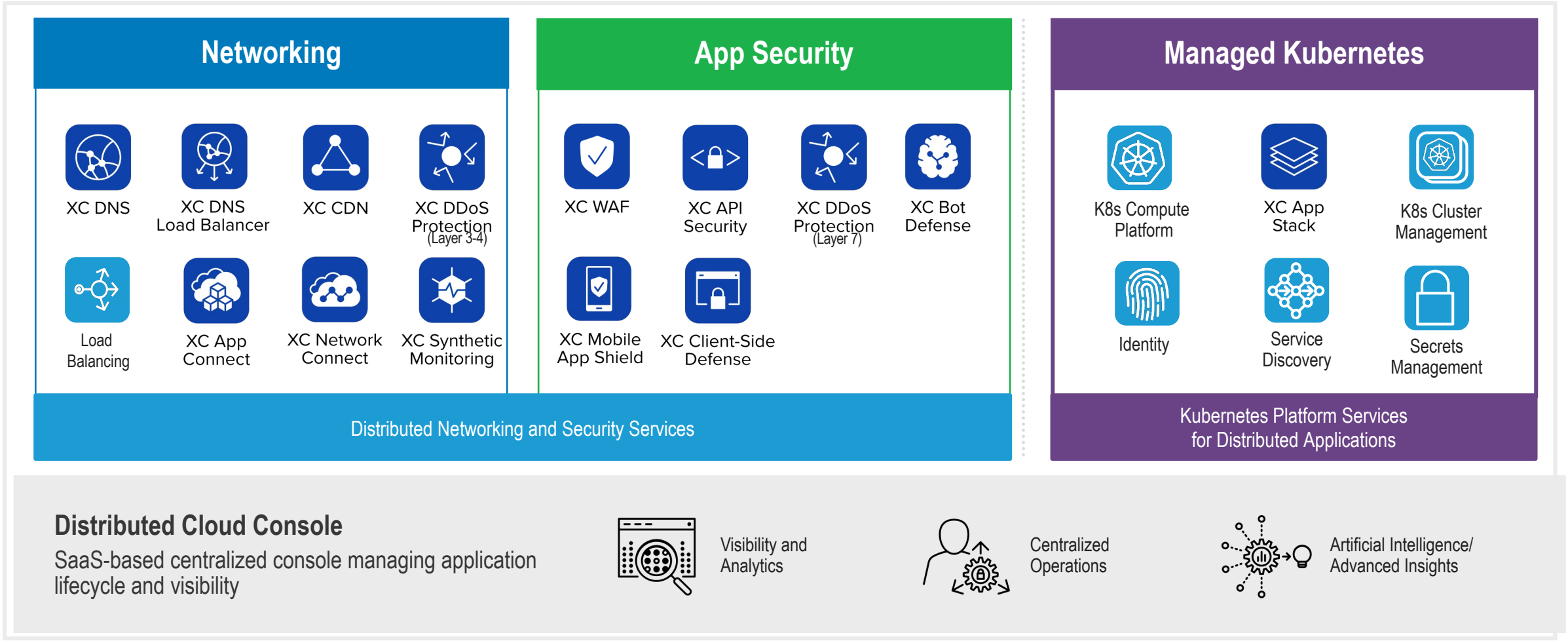
Global Network
Regional Edge [RE]

RE

Legend

- Network Only
- RE Services
- Private Peering (ASN 35280)
- Partner Peering

F5 Distributed Cloud - klíčové vlastnosti



Představení

- Správa informačních technologií města Plzně (SITMP) se stará o infrastrukturu a podporu organizací v rámci Plzeňského kraje.
  Vyvíjí přes 100 vlastních webových aplikací, které provozuje na vlastní infrastruktuře, kde zajišťuje jejich bezpečnost a dostupnost.

  - 100+ spravovaných organizací
  - 100+ vyvíjených webových aplikací
  - 6000+ spravovaných uživatelských stanic
  - 20 000+ uživatelských identit

Obsah prezentace

- Provoz a zabezpečení webových aplikací se stávají kritickou součástí poskytovaných služeb. Vzhledem k jejich počtu a různorodosti na základě organizací jsme se chtěli podělit o své zkušenosti.
- Použité technologie:
  F5 – Load balancer, WAF, Identity proxy a Zero trust
  Kubernetes – Běhové prostředí, Limitace zdrojů, Automatické škálování, HA
  Terraform – Automatizace
  ArgoCD – GitOps
  GITlab – Zdroj pravdy

Běhové prostředí

Běhové prostředí

- Jako hlavní běhové prostředí pro webové aplikace slouží Kubernetes. Jsou aplikace, pro které je nutné stále udržovat zastaralé technologie jako IIS, ale ty už jsou na ústupu. Celé prostředí Kubernetu včetně konfigurace je nasazováno deklarativně. Řekneme počet node s verzí Kubernetes a zbytek se vytvoří sám. To samé platí při přidávání dalších node nebo zdrojů či konfigurace.

```
"node1" = {
  ip          = "0.0.0.1",
  mask        = "/24"
  num_cpus    = 8
  memory      = 16384
  disks       = local.disks
  datastore_id = data.vsphere_datastore.i.id
  host_id     = data.vsphere_host.e.id
  ovf_url     = "https://cloud-images.ubuntu.com/jammy/current/jammy-server-cloudimg-amd64.ova"
}
```

```
"5" = {
  "gitlab_project_id" = 010,
  "name"              = "uzasny-projekt",
  "environment"       = "dev",
  "limits"            = local.default_limits,
},
```

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: system-kubeclarity
  namespace: argocd
spec:
  destination:
    namespace: kubeclarity
    server: https://kubernetes.default.svc
  project: default
  source:
    repoURL: https://openclarity.github.io/kubeclarity
    chart: kubeclarity
    targetRevision: 2.23.1
    helm:
      releaseName: kubeclarity
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
    syncOptions:
    - CreateNamespace=true
```

Ochrana aplikací F5 BIG-IP

- F5 slouží jako centrální bod a ochrana všech provozovaných aplikací a to jak těch moderních tak těch starších.
  V rámci F5 využíváme modulů LTM, APM, AWAF.

LTM - Load balancing, SSL offload, manipulace s komunikací

APM - Autentizační proxy, Zero trust

AWAF - Webový aplikační firewall, BOT / DOS protection

- Modul LTM využíváme pro load balancing, manipulaci komunikace a SSL offload.

Load balancing - Přidávání nových členů clusteru do poolu

Manipulace komunikace - Odebírání nežádoucích hlaviček, změna obsahu http/https

```
when HTTP_RESPONSE {
    if { [HTTP::header exists "X-Powered-By"] } {
        HTTP::header remove X-Powered-By
    }
}
```

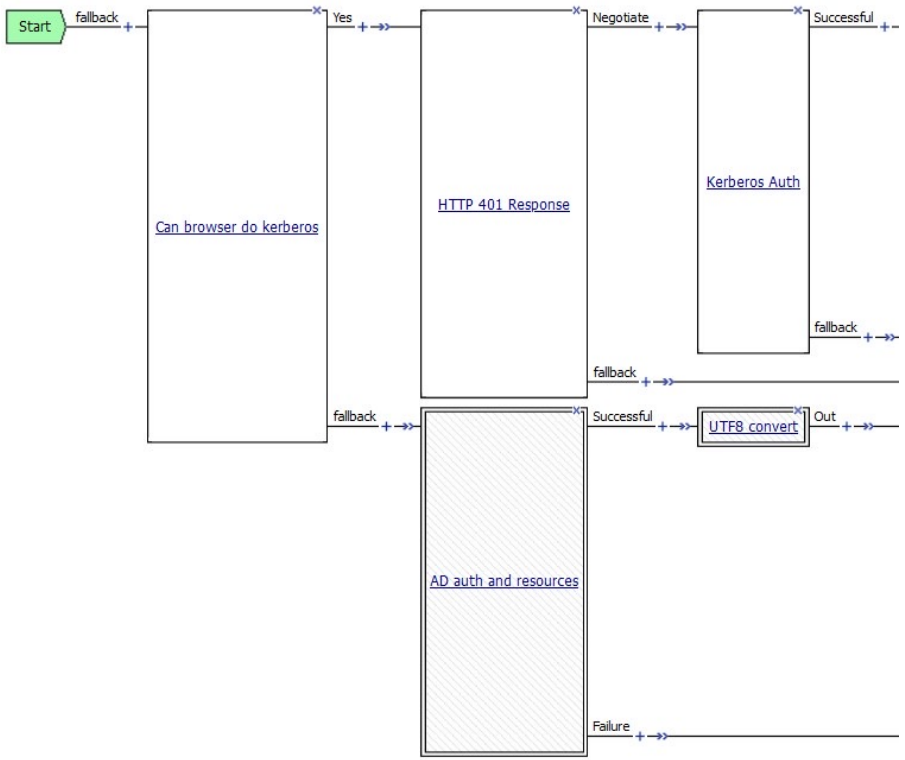
SSL Offload - Deklarované generování a obměna certifikátů

```
"muj-uzasny-web.cz" = {
  cn = "muj-uzasny-web.cz"
  san = ["www.muj-uzasny-web.cz","www2.muj-uzasny-web.cz"]
}
```

- APM používáme jako autentizační proxy a Zero trust.

Autentizační proxy - SAMLv2 IDP/SP, Kerberos rozhodce, MFA

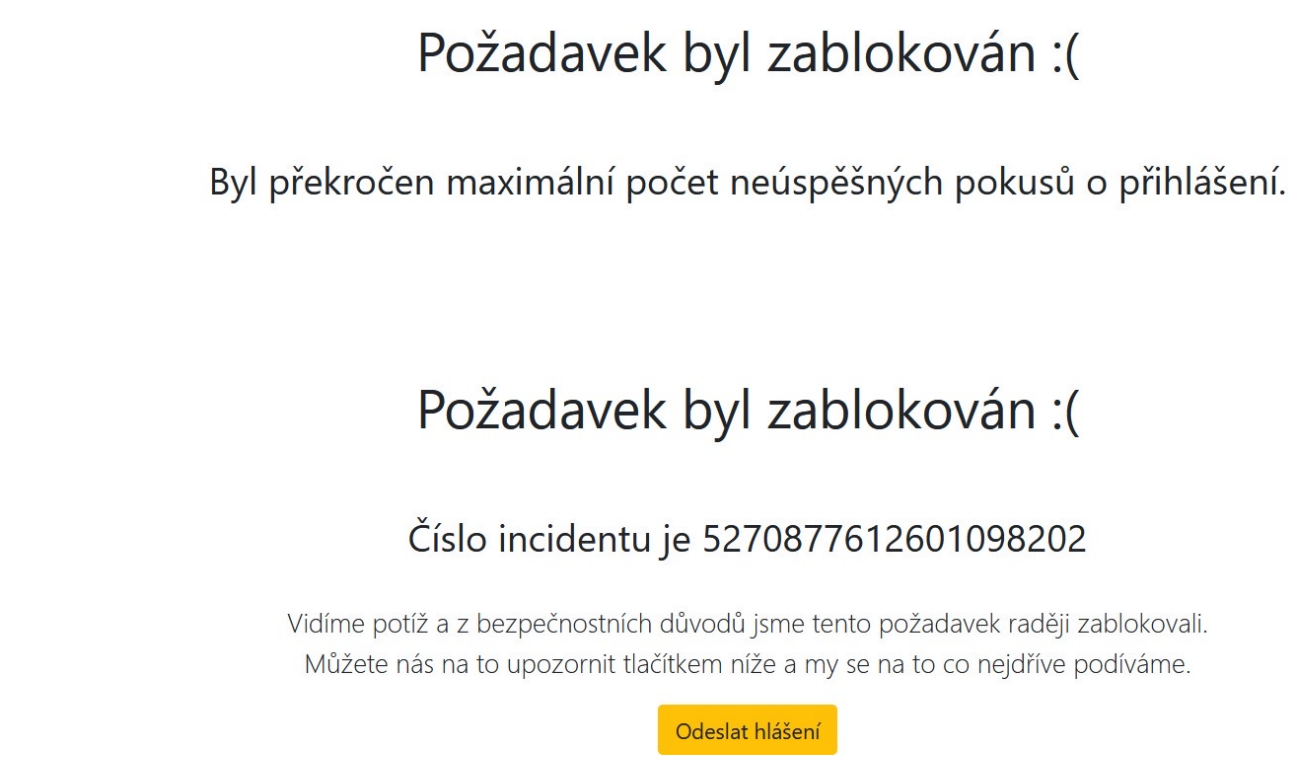
Zero trust – Přístup k citlivým aplikacím, manipulace routovacích domén



- Webový aplikační firewall, BOT/DOS ochrana

Webový aplikační firewall – Učení komunikace, detekce signatur, CI/CD automatizace

BOT/DOS ochrana – mitigace útoků na 7. síťové vrstvě




```
when ASM_REQUEST_BLOCKING {
    set asm_support_id [ASM::support_id]
    set asm_violation [ASM::violation details]
    set client_ip [ASM::client_ip]
    HTTP::header remove Content-Length
    set response "......."
    ASM::payload replace 0 [ASM::payload length] ""
    ASM::payload replace 0 0 $response
}
```

F5 DDOS

F5 DDOS

Novinky.cz

Hlavní stránka Stalo se Domácí Volby Zahraniční Válka na Ukrajině Komentáře Krimi Kultura Ekonomika Lifestyle Koktejl

Internet a PC AutoMoto Věda Cestování Historie Podcasty a pořady Sport Kvízy Speciály Počasí TV program Denní tisk Sledované

VÁLKA NA UKRAJINĚ | VÁLKA V IZRAELI | ZBYTEČNÁ VÁLKA

Novinky.cz » Internet a PC » Bezpečnost » Proruští hackeři mají na mušce Prahu, Brno, Ostravu i Plzeň

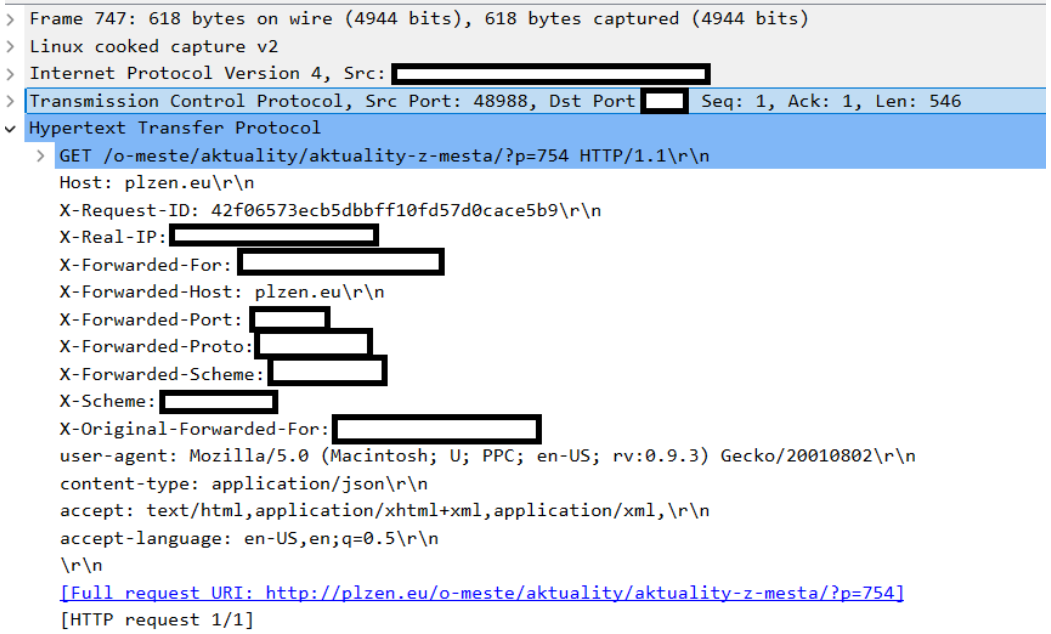
Proruští hackeři mají na mušce Prahu, Brno, Ostravu i Plzeň

Lenka Zoulová, Barbora Růžičková
vybrat autory ke sledování

154

22. 7. 2024, 11:19

Nechvalně známé proruské hackerské hnutí NoName057(16) má na mušce internetové stránky hned několika tuzemských měst. Útočit chtějí hackeři s využitím dobrovolnické platformy DDosia na weby z Prahy, Brna, Ostravy i Plzně. Dokládá to nová konfigurace cílů, proti kterým mají být vedeny DDoS útoky.

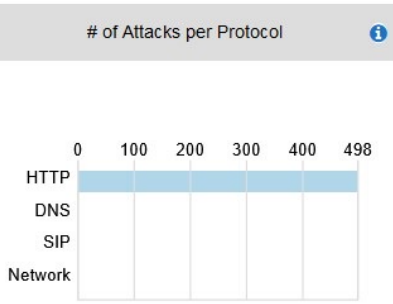


```
> Frame 747: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: [redacted]
> Transmission Control Protocol, Src Port: 48988, Dst Port [redacted] Seq: 1, Ack: 1, Len: 546
v Hypertext Transfer Protocol
  > GET /o-meste/aktuality/aktuality-z-mesta/?p=754 HTTP/1.1\r\n
    Host: plzen.eu\r\n
    X-Request-ID: 42f06573ecb5dbbff10fd57d0cace5b9\r\n
    X-Real-IP: [redacted]
    X-Forwarded-For: [redacted]
    X-Forwarded-Host: plzen.eu\r\n
    X-Forwarded-Port: [redacted]
    X-Forwarded-Proto: [redacted]
    X-Forwarded-Scheme: [redacted]
    X-Scheme: [redacted]
    X-Original-Forwarded-For: [redacted]
    user-agent: Mozilla/5.0 (Macintosh; U; PPC; en-US; rv:0.9.3) Gecko/20010802\r\n
    content-type: application/json\r\n
    accept: text/html,application/xhtml+xml,application/xml,\r\n
    accept-language: en-US,en;q=0.5\r\n
    \r\n
    [Full request URI: http://plzen.eu/o-meste/aktuality/aktuality-z-mesta/?p=754]
    [HTTP request 1/1]
```

```
when HTTP_REQUEST {
        if { ([HTTP::header "Accept"] equals "text/html,application/xhtml+xml,application/xml," ) }{
            drop
            }
}
```

Attacks

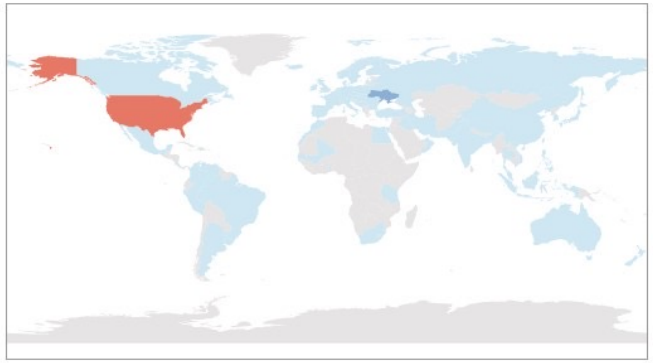
# of Attacks	
Critical	0
High	0
Moderate	0
Low	498



Attack ID	Severity	Vector	Trigger	Virtual Server	Mitigation	Start Time	End Time	Duration	IPs (Conc...	Blocked Tra...
3623...	Low	Application L...	Geo Volumetric ...	/Common/VS_Skol...	Captcha	2024-03-21 23...	2024-03-21 23...	6 minutes	1	11
3623...	Low	Application L...	Geo Volumetric ...	/Common/VS_Skol...	Client Side	2024-03-20 11...	2024-03-20 11...	4 minutes	1	0
3623...	Low	Application L...	Geo Volumetric ...	/Common/VS_Skol...	Client Side	2024-03-15 22...	2024-03-15 22...	4 minutes	1	0
3623...	Low	Application L...	Geo Volumetric ...	/Common/VS_Skol...	Captcha	2024-03-16 12...	2024-03-16 12...	6 minutes	1	0
3623...	Low	Application L...	Geo Volumetric ...	/Common/VS_Skol...	Captcha	2024-03-20 01...	2024-03-20 02...	7 minutes	2	2
3623...	Low	Application L...	Geo Volumetric ...	/Common/VS_Skol...	Captcha	2024-03-20 04...	2024-03-20 05...	17 minutes	1	1

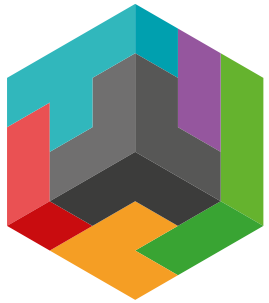
Countries

Source | Destination (Network)



Country	Attacks	Avg TPS	Avg Dropped RPS	Avg Allowed RPS	DNS Packets	SIP Requests
United States	88	0.03	0	0	0	0
Ukraine	48	0.02	0	0	0	0
Sweden	31	0	0	0	0	0
Germany	27	0.03	0	0	0	0
Austria	21	0.01	0	0	0	0
United Kingdom	13	0.01	0	0	0	0
France	6	0.01	0	0	0	0

URL	Virtual Server	DoS Profile	Heavy URL Detection Criterion	Avg Server Latency	Transactions	Latency Histogram
/	VS_k8s.plzen.eu_HTTPS	dos_k8s_prod	Automatic Detection: 09/01/2024 06:42:40 (CEST)	4802.33 ms	504959	



Správa informačních technologií Plzeň

Děkuji za pozornost!

Jakub Bělka – belka@plzen.eu

Martin Kylián – m.kylian@f5.com

www.sitmp.cz