





# Situace.

- Hybridní prostředí

- Nedostatek IT specialistů

- Práce odkudkoliv

- Budeme napadeni?

# Situace.

- Hybridní prostředí

- Nedostatek IT specialistů

- Práce odkudkoliv



**KDY?**



thein.security

Security Operations Center  
(SOC)

*„Rychlá proaktivní detekce  
a reakce jsou naprosto nezbytné,  
pokud chceme čelit moderním  
kybernetickým útokům.  
Rozhodují sekundy, nikoliv  
hodiny nebo dny.“*

MARTIN PÓLRÁN  
CSO

# Hrozby – RIZIKA.

## 1 Pozdní reakce na hrozbu

Útočník se může v prostředí pohybovat dlouhou dobu a nemusí být vůbec odhalen.

## 2 Velké provozní ztráty

Ochromení IT znamená ochromení činnosti firmy.

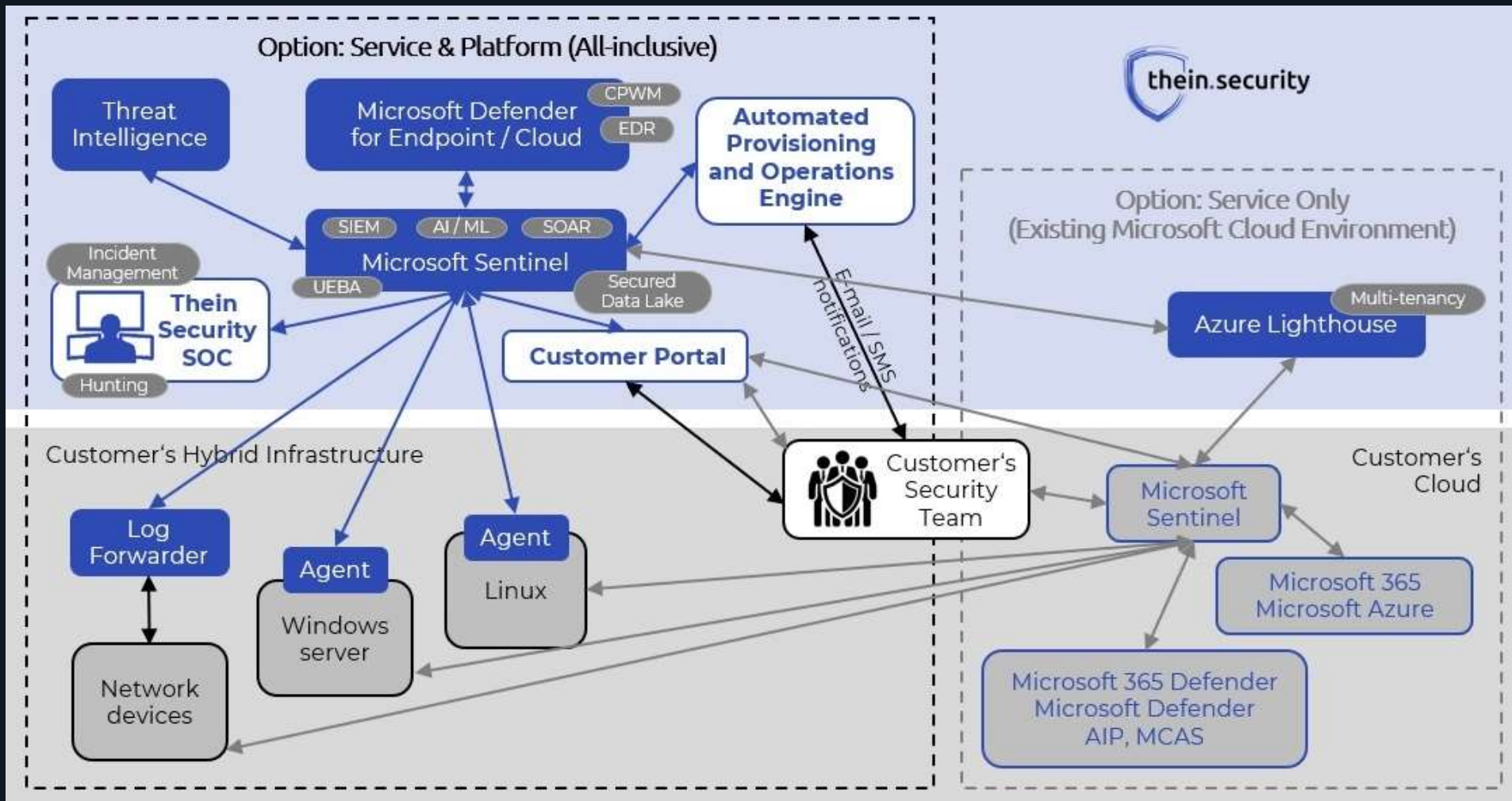
## 3 Únik citlivých dat

Získat data zpět je nákladné a nemusí se to vůbec podařit.

## 4 Dopad na značku a reputaci

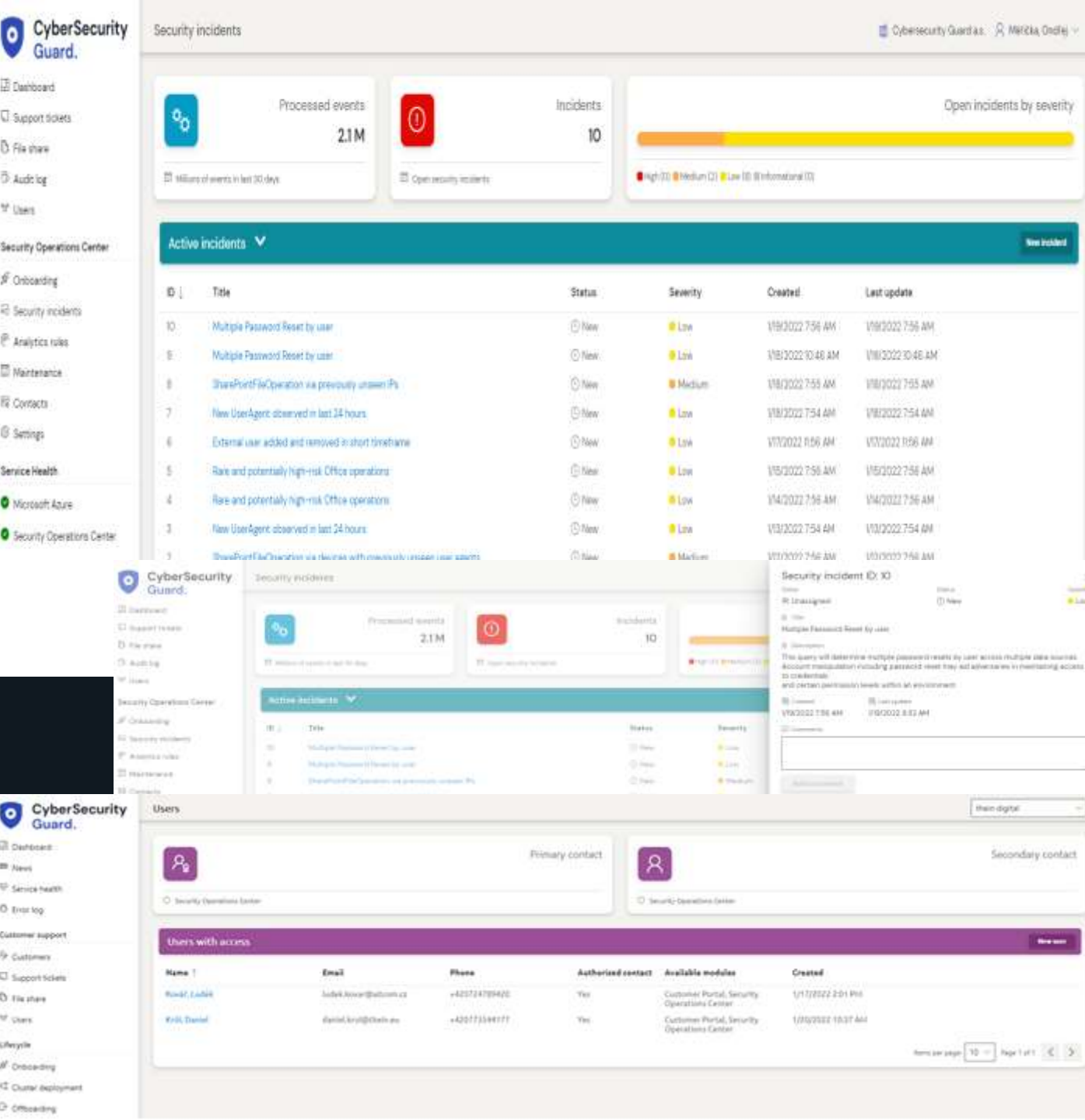
Ztráta dat poškodí image společnosti v očích člen skupiny thein. zákazníků.

# High level architektura



Díky cloud-native platformě založené na Microsoft technologiích a díky námi vyvinutým komponentám monitorujeme čistě cloudové i hybridní IT infrastruktury.

S minimálními implementačními náklady a rychlým nasazením.



# Cybersecurity Guard portál

1 Zákaznický portál

2 Incidenty

3 Reporty

4 Smluvní podmínky

# Čím se lišíme.



- **Vytěžujeme Vaše technologie a investice do Microsoft technologií**
- **Pokrýváme hybridní prostředí, cloud native technologie**
- **Dohled a řešení incidentů 24 / 7 / 365**
- **Změna bezpečnostní situace – řízení bezpečnosti.**
- **Thein Soc tým pracuje pro Vás**



# Naši mezinárodní partneři.



# Temná strana DDoS -

## DDoS vydírání a trojitá hrozba

*"DDoS vás zasáhne, už to není otázka jestli-  
nebo kdy- ale **jak** na vás zaútočí"*

---

Alexander Tomik, Sales Engineer Central Eastern Europe

[Alexander.Tomik@netscout.com](mailto:Alexander.Tomik@netscout.com)

Oldřich Gosman, Security Operation Center

[oldrich.gosman@thein.eu](mailto:oldrich.gosman@thein.eu)

# V roce 2021 zasáhlo svět téměř než 10 milionů DDoS útoků – a za jakou cenu?

**Vybrané aktuality, hrozby a doporučení**

**Úpoutání na další vlnu vyčerpávací kampaně**

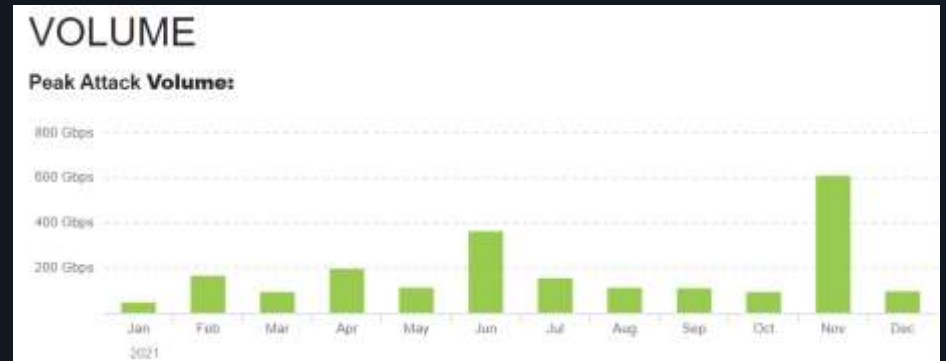
Upozorňujeme na další vlnu vyčerpávací kampaně, která cílí na veřejný i privátní sektor. Útočník se vydává za kybernetickou skupinu s názvem Fancy Lazarus (také známá pod názvem Lazarus Group, Armada, Calcutta). Měla pod vlivem síťového DDoS útoků požaduje zaplacení výkupného v bitcoinech. Po nezaplacení výkupného v daném termínu útok začne a požadovaná částka se každý den oem postupně zvyšuje. DDoS útoky vyvolává...

16.06.2021

**Ukončení činnosti ransomwaru Avaddon**

11. června došlo k ukončení činnosti ransomwaru Avaddon, který mimo jiné napadl i české instituce. Zprávu oznámil server Bleeping Computer poté, co anonymně obdržel dešifrovací klíč a potvrzil jeho validitu. Větš operátorů Avaddon byl následně vypnut a aktuálně je nedostupný. Důvod ukončení není v současné době známý, stejně ovšem o ojedinělý případ, dešifrovací klíč v rukou zveřejnil například operátor ransomwaru TrickCrypt...

16.06.2021



## CZECH REPUBLIC DDOS SUMMARY

2021

### Highlights:

Attacks:	32.3 k
Peak Volume:	612 Gbps
Peak Speed:	84.5 Mpps
Peak Duration:	6 days (5 days, 16 hours)
Top Attack Types:	Total Traffic
	UDP
	IPv4



### Top Source Countries:



### Sources

Iran (Islamic Republic Of)	2,321	9.7 %
United States	1,944	8.1 %
Viet Nam	1,293	5.4 %
Italy	1,174	4.9 %
Latvia	1,120	4.7 %

ПРАЙС

Цена	Скорость	Скорость	Скорость
\$3/д	\$6/мес	\$10/мес	\$12/мес
1 атака	1 атака	1 атака	1 атака
120 секунд атака	300 секунд атака	600 секунд атака	1200 секунд атака
210000 Тп	210000 Тп	210000 Тп	210000 Тп
Layer 3: SYN, UDP, DNS, NTP, ICMP	Layer 3: SYN, UDP, DNS, NTP, ICMP	Layer 3: SYN, UDP, DNS, NTP, ICMP	Layer 3: SYN, UDP, DNS, NTP, ICMP
Layer 7: GET, POST	Layer 7: GET, POST	Layer 7: GET, POST	Layer 7: GET, POST
Купить	Купить	Купить	Купить

# DDoS Extortion & Triple Threat (Ransomware + data theft + DDoS)

## DDoS Extortion (aka RDDoS)

### THE TRIPLE THREAT

3 High-profile DDoS Extortion Campaigns operating simultaneously



Ačkoli DDoS vydírání není nové, objevují se vysoce profilované kampaně DDoS vyděračských útoků.

- **Lazarus Bear Armada (LBA)**
- **Fancy Lazarus**
- **REvil ransomware group**

Zdá se, že útočníci nyní považují DDoS útoky za zločinné snahy samy o sobě - na rozdíl od jednoho pilíře trojitých vyděračských útoků - což znamená, že je třeba očekávat zkušenější kampaně vydírání DDoS, protože sofistikované skupiny ransomwaru tuto taktiku ovládají.

## Ransomware Gangs

And while DDoS extortion runs rampant, Ransomware gangs continue to assimilate DDoS into their toolkit



AvosLocker



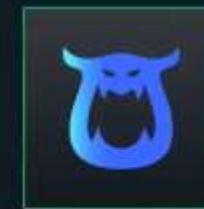
Suncrypt



BlackCat



Avaddon



REvil

Ve zprávě 1H 2021 Threat Intelligence jsme záznamenali že několik různých skupin provádějících operace ransomwaru se také přesunulo na území útoku DDoS, aby vyvinuly větší tlak na oběti, aby zaplatily požadované výkupné.

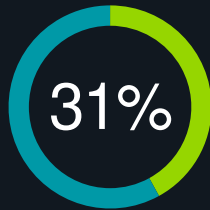
Pro tuto zprávu vytvořila Palo Alto, partner Threat Intelligence, souhrn ransomwarových gangů, které také používají DDoS k vydírání obětí, aby zaplatily výkupné.

Z výsledků zprávy je patrné, že následující skupiny používají DDoS jako součást svých operací.



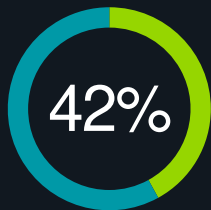
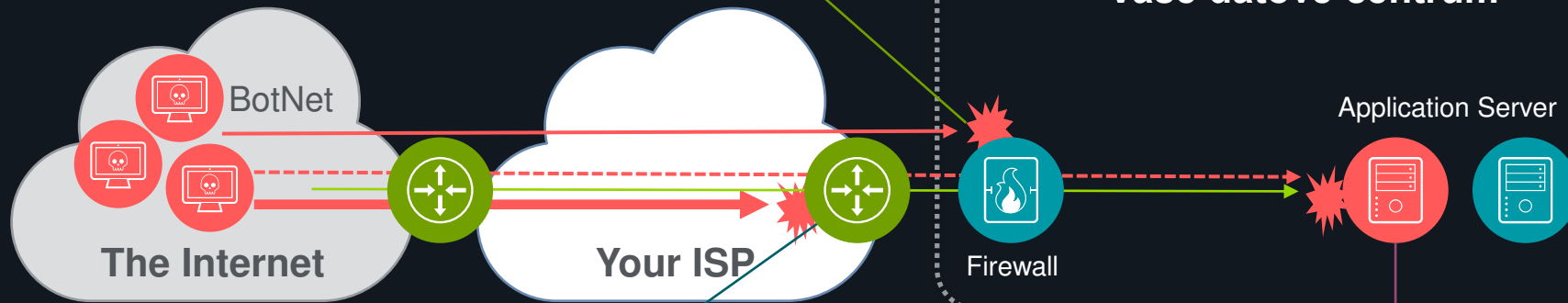
# Nejnovější trendy DDoS útoků - Složitost

 **Fakt: Moderní DDoS útoky jsou složité: tvoří je dynamický multivektor**



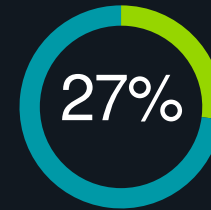
## TCP State-Exhaustion Attacks

- Selhání stavových zařízení (Load Balancers, Firewalls, IPS)
- 2x nárůst (oproti 16 % v předchozím roce)
- U 54 % došlo k selhání



## Volumetric Attacks

- Velké (až 1,7 Tb)
- Saturuje linky
- 91% podniků zažilo nasycení linek



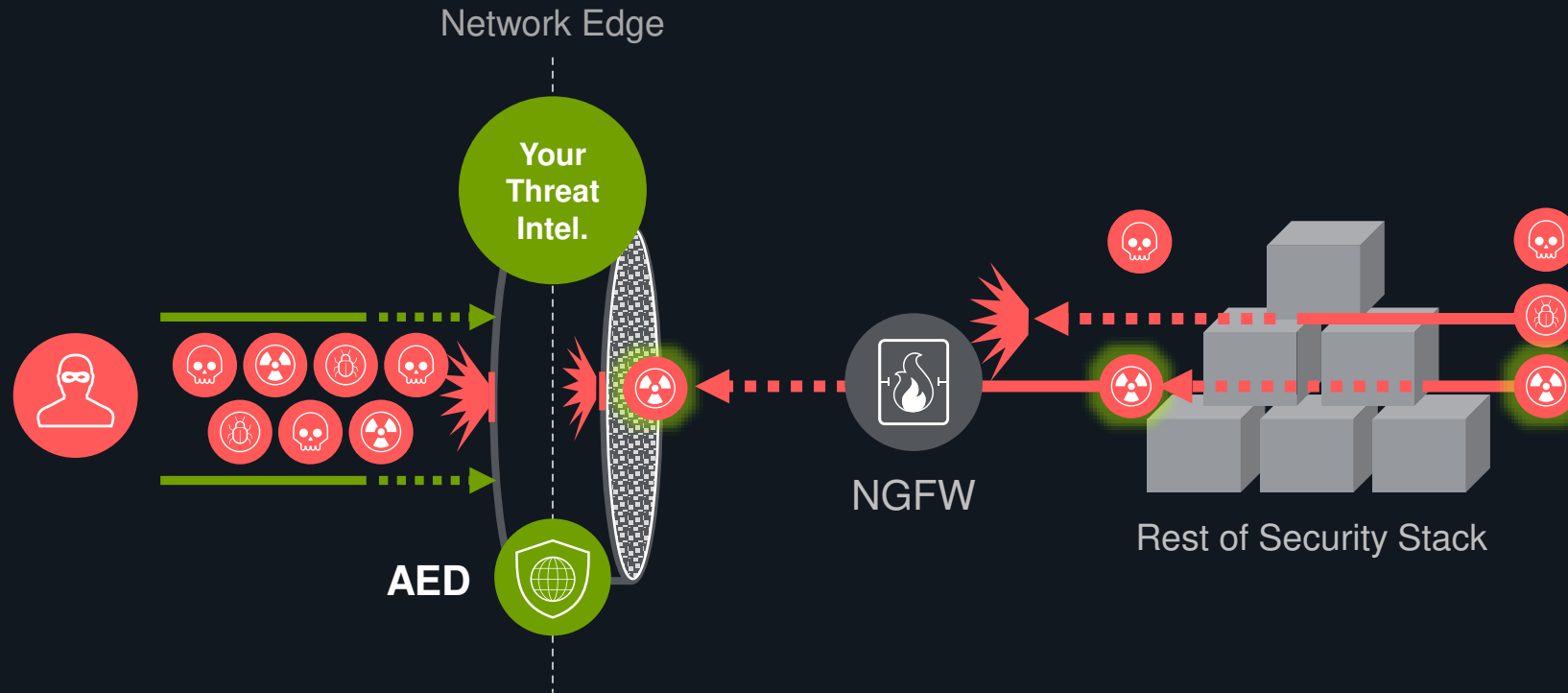
## Application Layer Attacks

- Malé a pomalé, stealth útoky
- Zhroucení aplikačních serverů



# Arbor Edge Defense (AED)

První a poslední linie inteligentní, automatizované obrany perimetru



## PRVNÍ OBRANNÁ LINIE

- Příchozí DDoS útoky
- **Nejen volumetrické**
- Sondování / průzkumné / útoky hrubou silou

## POSLEDNÍ OBRANNÁ LINIE

- Zablokuje odchozí komunikaci od ohrožených interních hostů.
- **Nad rámec tradičního DDoS: AIF, 3rd Party IoC**



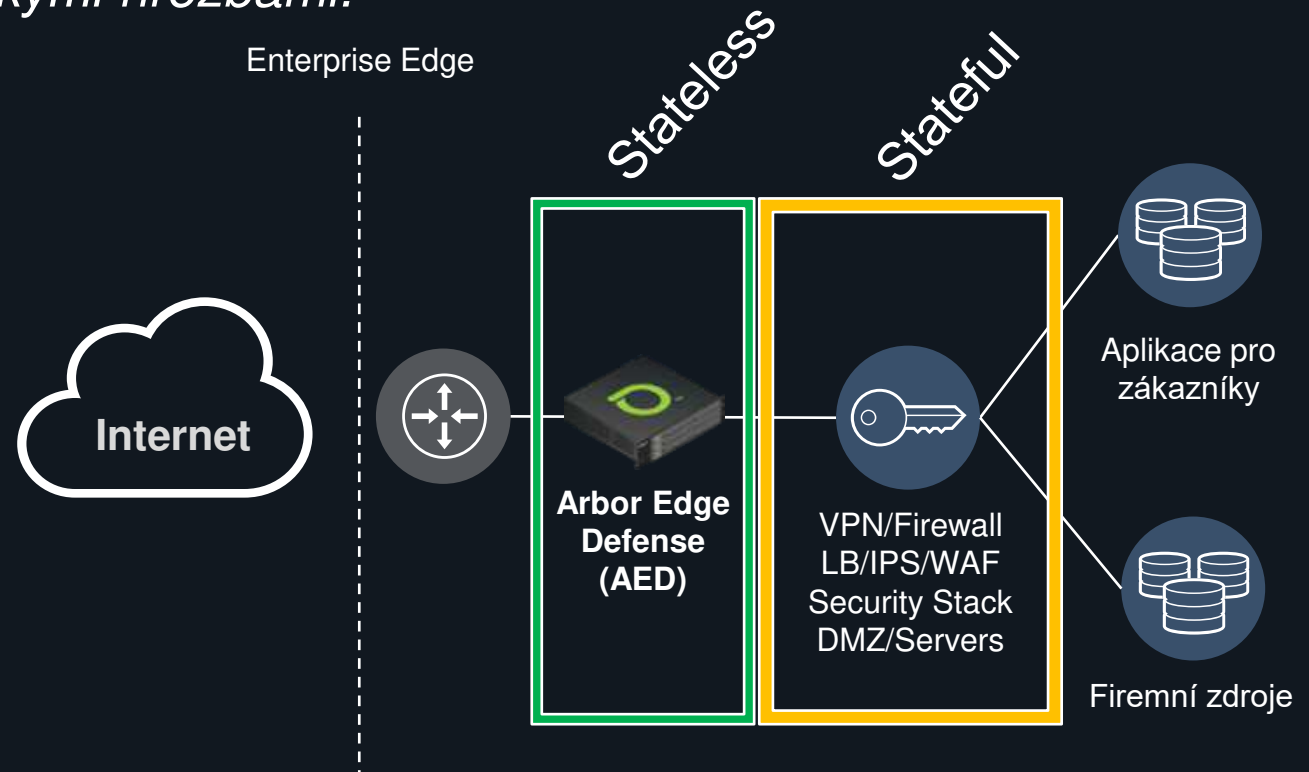
# Uvedení Arbor Edge Defense (AED)

Ochrana podnikového perimetru: První a poslední linie inteligentní, automatizované, bezstavové, perimetrické obrany. Poskytuje bezstavovou ochranu před vyčerpáním stavu a aplikační vrstvou DDoS. Poskytuje viditelnost a kontrolu nad celým připojením k internetu a zároveň využívá inteligenci ATLAS pro pokročilou ochranu před kybernetickými hrozbami.



## Arbor Edge Defense

- Viditelnost paketů na perimetru
- Inline a transparentní pro síť
- Monitorování / detekce / ochrana v reálném čase
- Vyladěno pro podnikovou infrastrukturu
- Profesionální znalosti a zaměření na zákazníka a firemní infrastrukturu
- Chrání dostupnost všech podnikových služeb před sofistikovanými DDoS útoky
- Klíčový bod ochrany perimetru



# Proč NETSCOUT ARBOR?

#1

Lídr v oboru produktů a služeb ochrany před útoky DDoS.

1/3

Objem internetového provozu monitorovaného projektem ATLAS

20

Již řadu let Arbor dodává inovativní technologie a produkty pro zabezpečení a viditelnost sítě



Arbor Networks je součástí NETSCOUT od roku 2015.





# Kontakty pro vás.



Oldřich Gosman

+420 731 241 074

[www.theinsecurity.eu](http://www.theinsecurity.eu)



Alexander Tomík

+43 664 240 92 51


[www.netscout.com](http://www.netscout.com)

**Děkujeme.**

[www.theinsecurity.eu](http://www.theinsecurity.eu)

# The Rise of Server-Class Botnet Armies

## RISE OF SERVER-CLASS BOTNET ARMIES: MERIS, DVINIS, AND GITMIRAI.



Meris had as many as  
**4,800 BOTS**

Contributing to more than  
**4,000 DDOS ATTACKS**

Attack size as high as  
**337 GBPS**

**MERIS BOTNET**

### Meris Botnet Snapshot

First Seen:

June 2021

Current Active Nodes: ~2,000  
Peak Active Nodes: ~4,800  
Attacks to Date: ~4,000  
Maximum Attack Size: ~337 Gbps  
Average Attack Size: ~7 Gbps



increased from  
**3,500**

when we first started  
tracking to more than  
**24,000 BOTS**

Attack size as high as  
**463 GBPS**

**DVINIS BOTNET**

### Dvinis Botnet Snapshot

First Seen:

September 2021

Current Active Nodes: ~24,000  
Peak Active Nodes: ~24,000  
Attacks to Date: ~29,000  
Maximum Attack Size: ~463 Gbps  
Average Attack Size: ~3 Gbps



As many as  
**3,800 NODES**

contributing to more than  
**16,000 BOTS**

Attack size as high as  
**584 GBPS**

**GITMIRAI BOTNET**

### GitMirai Botnet Snapshot

First Seen:

November 2021

Current Active Nodes: ~3,800  
Peak Active Nodes: ~3,800  
Attacks to Date: ~16,000  
Maximum Attack Size: ~514 Gbps  
Average Attack Size: ~5.4 Gbps



✚ Navštivte nás:

• <https://www.netscout.com/arbor-ddos>  
DDoS and Cyber Threat Protection, Network Visibility

• <https://horizon.netscout.com/>  
Cyber Threat Horizon, Realtime mapping of DDoS attacks.

• <https://www.netscout.com/threatreport>  
NETSCOUT Threat Intelligence Report

• <https://www.netscout.com/product/arbor-cloud>  
Arbor Cloud DDoS Protection Services

• <https://www.netscout.com/global-threat-intelligence>  
Cyber Attack Threat Intelligence & Analysis

