CLOUDSEC 2023

ENVISION IT

대규모 애플리케이션 디도스 공격과 대응 방법

라드웨어 코리아

Hosted by

TREND MICRO

AGENDA

1. 디도스 공격 동향
2. 라드웨어 클라우드 디도스 솔루션
3. 라드웨어 웹 디도스 솔루션

디도스 공격 동향
DDoS Attack Trends

디도스 공격 동향 (22년~23년)

대용량 디도스 공격

미국 서비스 공급업체 대상의 1.1Tbps 이상의 디도스 공격
유럽 정부 대상의 800Gbps 디도스 공격

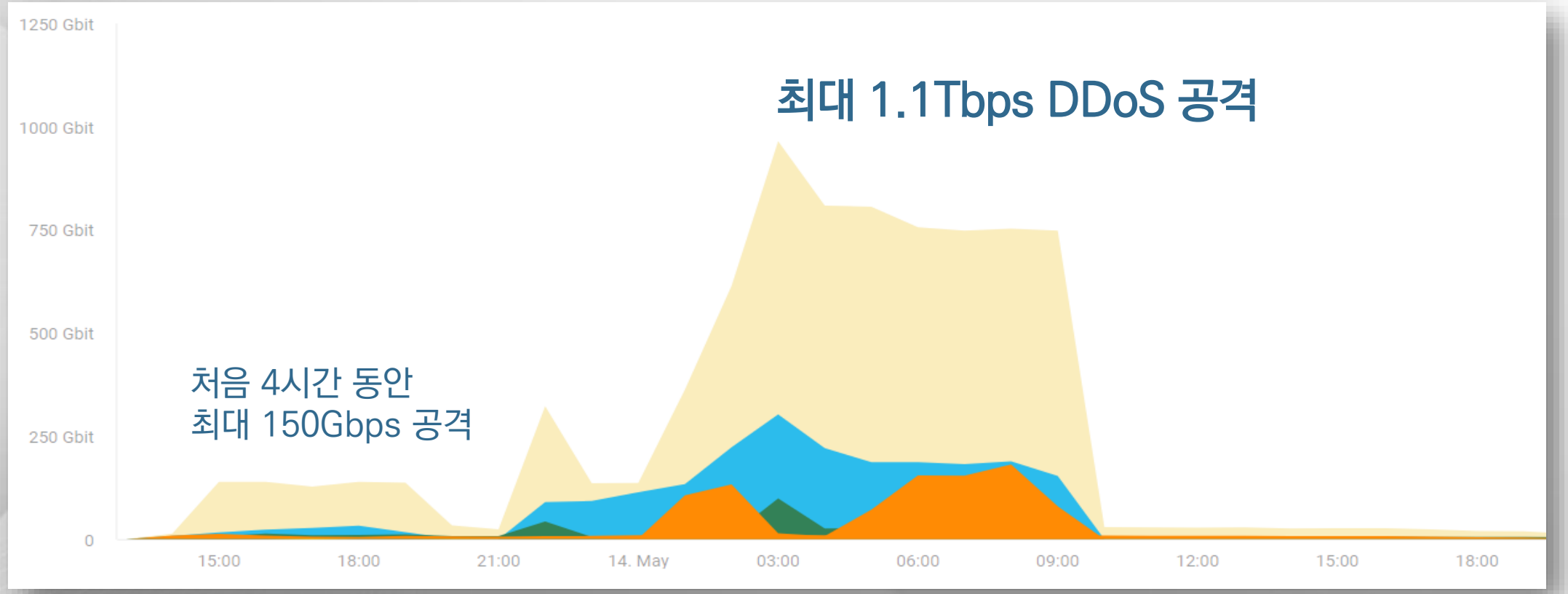
기업/정부 대상 사이버 공격

우크라이나-러시아 사이버 전쟁
기업/국가 대상 사이버 공격 증가
이스라엘 전쟁 – “Iron Swords” 작전

새로운 형태의 디도스 공격

새로운 형태의 Web DDoS 공격
기업/정부 대상의 웹 공격 및 디도스 공격

1Tbps 이상의 대용량 디도스 공격 – 미국 인터넷 서비스 공급업체



- 미국 인터넷 서비스 공급업체 대상의 대용량 디도스 공격 (2022년 5월)
  - 최초 150Gbps, 최대 1.1Tbps 멀티 벡터 공격
  - Network floods, UDP 반사/증폭 공격, 암호화된 HTTPS flood 공격 등

800Gbps 이상의 대용량 디도스 공격 – 유럽 정부 (23년 3월)

10
10분간 멀티 벡터 공격

3
3번의 UDP, TCP, GRE 트래픽 피크 발생

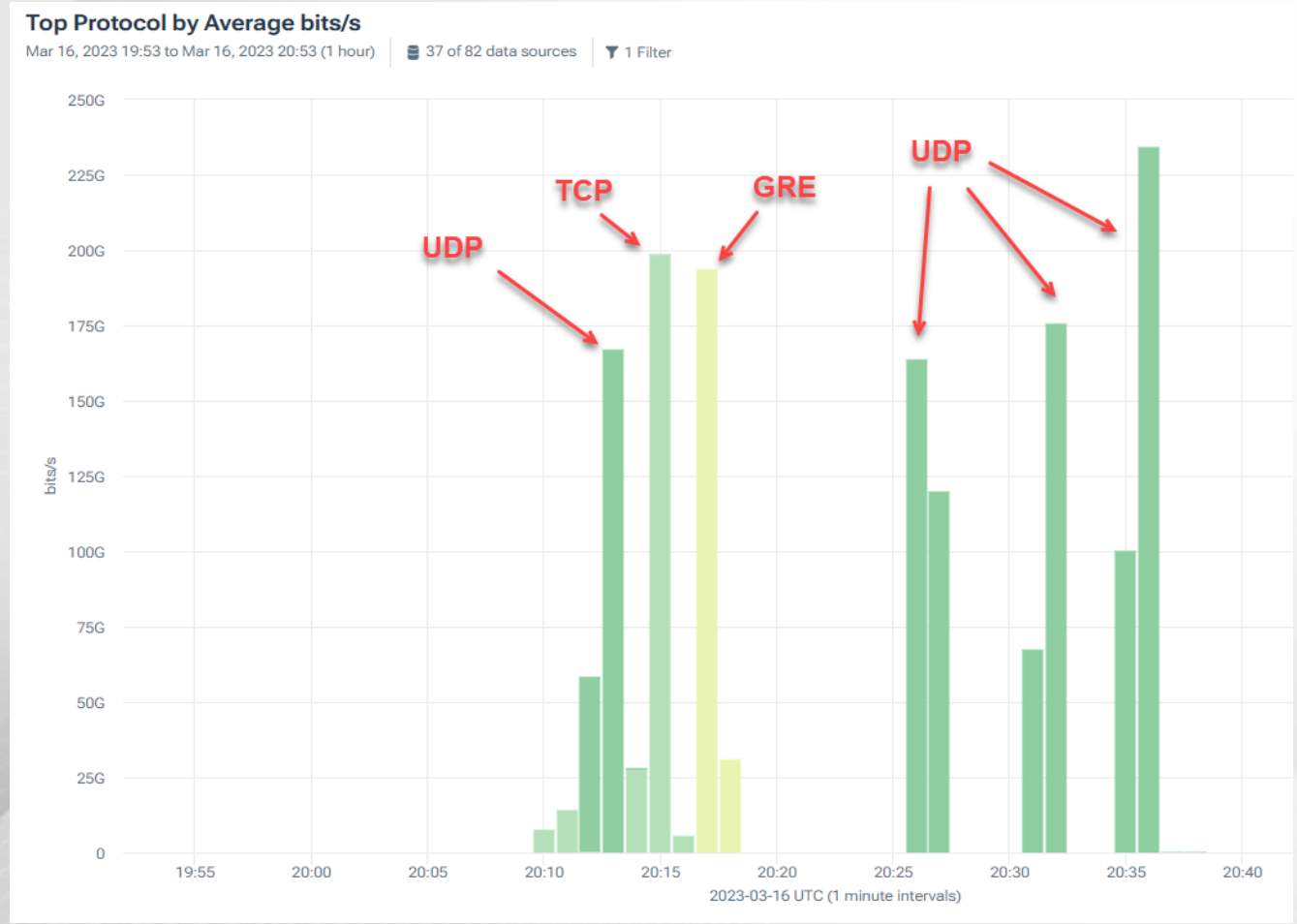
3
3회의 융단폭격 UDP 공격 파도

20K
20,000개의 고유한 소스 IP

780
780Gbps 공격

공격 피크는 780Gbps

800Gbps 이상의 대용량 디도스 공격 – 유럽 정부 (23년 3월)



Protocol	Average Gbits/s	95th Percentile Gbits/s	Max Gbits/s	Last Datapoint Gbits/s
UDP (17)	18.48	164.12	234.61	<0.01
TCP (6)	4.34	7.84	198.41	0.01
GRE (47)	3.82	0.10	193.70	0.00
ESP (50)	<0.01	<0.01	<0.01	<0.01
ICMP (1)	<0.01	<0.01	<0.01	0.00
Total of Top 5	**26.63**	**172.07**	**626.72**	**0.02**

Source Country	Average Unique Src IPs	95th Percentile Unique Src IPs	Max Unique Src IPs	95th Percentile Gbits/s	95th Percentile Kpackets/s	Last Datapoint Unique Src IPs
China (CN)	896	5,834	10,097	35.44	3,744.82	0
United States	217	1,138	1,436	11.32	2,298.40	2
Ukraine (UA)	209	1,064	1,419	8.80	1,431.30	12
Viet Nam (VN)	199	1,064	1,138	15.49	3,180.19	0
Brazil (BR)	194	1,007	1,414	11.13	1,617.54	0
Russian Fede	170	960	1,064	8.09	1,298.84	0
India (IN)	118	652	805	6.36	962.60	0
Japan (JP)	110	585	665	15.11	3,385.70	0

러시아 – 우크라이나 분쟁으로 새로운 사이버 전쟁 시대 도래

친러시아 핵티비스트 그룹

NoName057,
Killnet cluster,
Anonymous Russia,
Passion Group, etc.

우크라이나를 지원하는
국가를 대상으로 공격

클라우드 소싱 봇넷 사용
(정부에서 자금 지원)

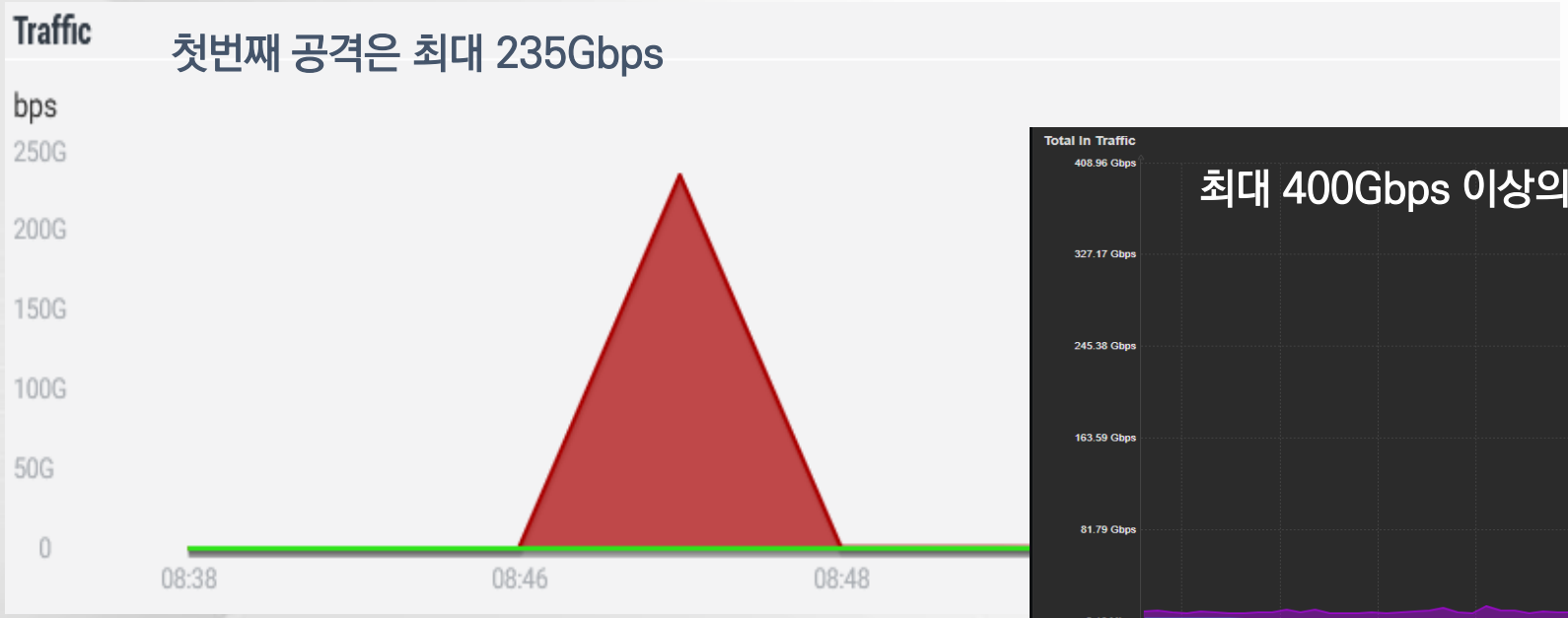
양국의 갈등은 사이버 전쟁으로 확대

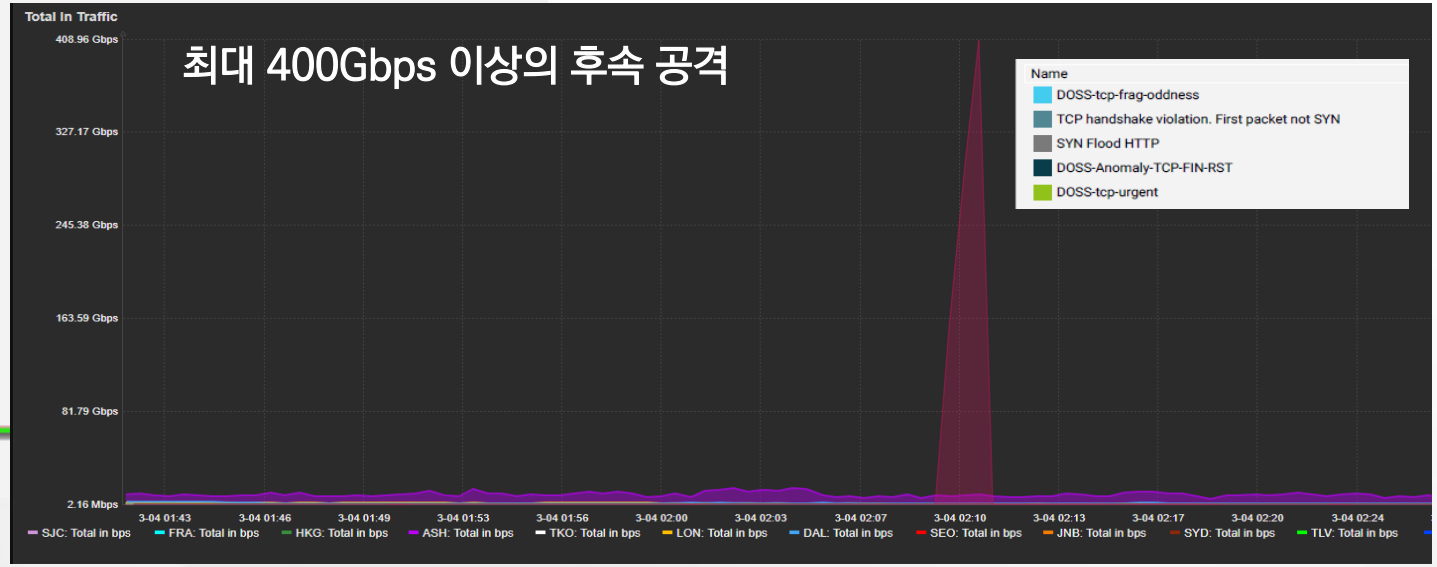
종교적 동기를 가진 그룹

Anonymous Sudan,
Mysterious Team
Bangladesh,
DragonForce
Malaysia, etc

무슬림을 모욕한 것으로
추정되는 대상에 대한
사이버 공격

러시아 – 우크라이나 사이버 전쟁





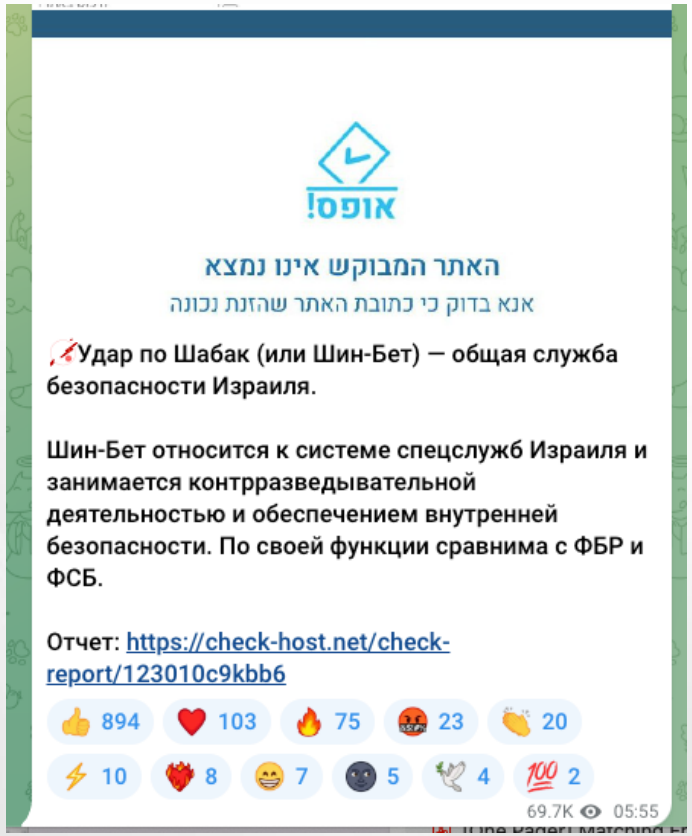
- 전쟁 발생 전후로 우크라이나 정부의 주요 자원이 공격 목표
- 한 달 동안 여러 번 반복되는 100Gbps-400Gbps 디도스 공격
- 멀티 벡터 공격 (네트워크 플러드, UDP 반사/증폭 및 암호화 HTTPs 플러드 공격 등) 을 사용

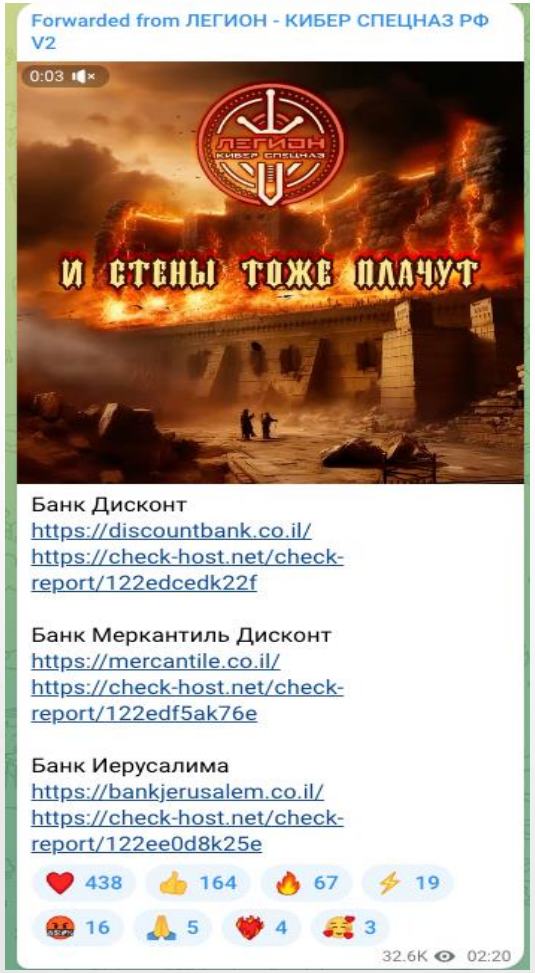
라드웨어는 모든 산업 분야에서 이스라엘을 보호

이스라엘 vs 하마스

'철검(Iron Swords)' 작전

이스라엘 전쟁 – “Iron Swords” 작전





출처 : 킬넷그룹 소속 텔레그램 채널

- **하마스**를 겨냥한 '**철검(Iron Swords)**' 작전이 개시된 이후, 이스라엘 정부와 다양한 조직은 여러 조직으로부터 지속적인 DDoS 공격을 받았고, **Killnet**은 이스라엘을 대상으로 가장 활발하게 활동한 공격자 중 하나였습니다.

이스라엘 전쟁 – “Iron Swords” 작전 – DDoS 공격

공격에 사용 된 공격 벡터 :

- HTTPS Flood
- Network Flood IPv4 UDP
- Network Flood IPv4 UDP-FRAG
- Network Flood IPv4 ICMP
- SYN Flood HTTP
- ICMP-BlackNurse-Attack
- BO-Apache-HTTPD-log-Cookie
- DDOS-APPLE-ARMS-AMP
- DDOS-Mirai-GENUDP-flood
- DDoS-UDP-MEMCACHED-AMP
- DOSS-chargen-reflected
- DOSS-DNS-Ref-L4-Above-3000
- DOSS-UDP-flood-80-Req
- DOSS-UDP-flood-80-Res
- DOSS-UDP-no-data
- TCP Anomalies
- TCP-FIN-ACK Flood
- DOSS-APPLE-ARMS-AMP
- DOSS-Mirai-GENUDP-flood
- DOSS-SSL-ClearText
- DNS Amplification
- DNS Random Sub-Domain

공격 규모 범위 :

- 1.2Gbps – 135Gbps
- 9K RPS – 630K RPS
- 4K QPS – 16K QPS

단일 공격 지속 시간 범위 :

- 2 min – 1443 min

지난 3일 동안 다양한 부분을 대상으로 50건이상의 디도스 공격 발생.

대상은 미디어, 정부 서비스, 중요 인프라 및 금융 서비스 산업

* 이스라엘 공격 대상 목록 :

주요 언론 매체

A 은행: 가장 큰 은행 중 하나

B 은행: 가장 큰 은행 중 하나

C 은행: 가장 큰 은행 중 하나

공공 서비스 회사

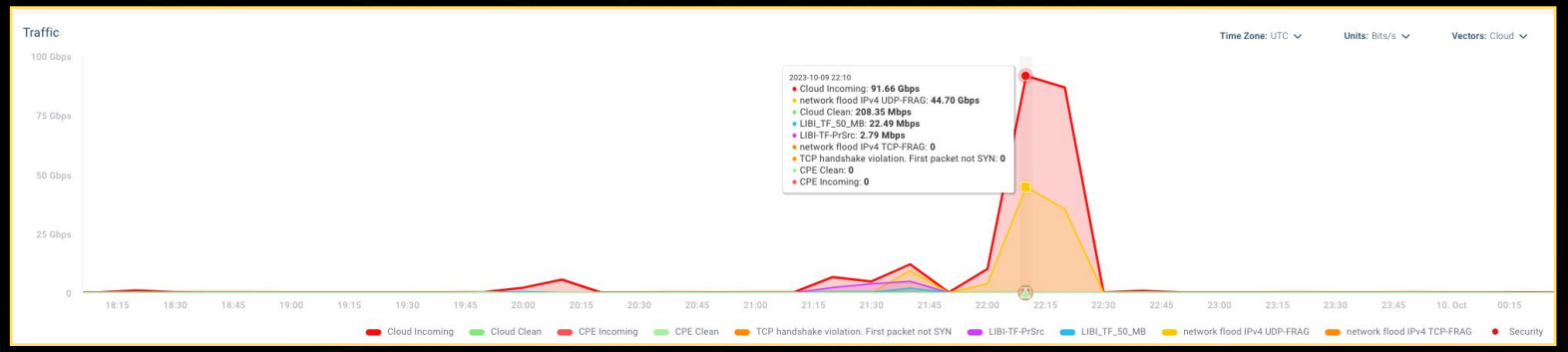
국영 운송 서비스

정부 서비스

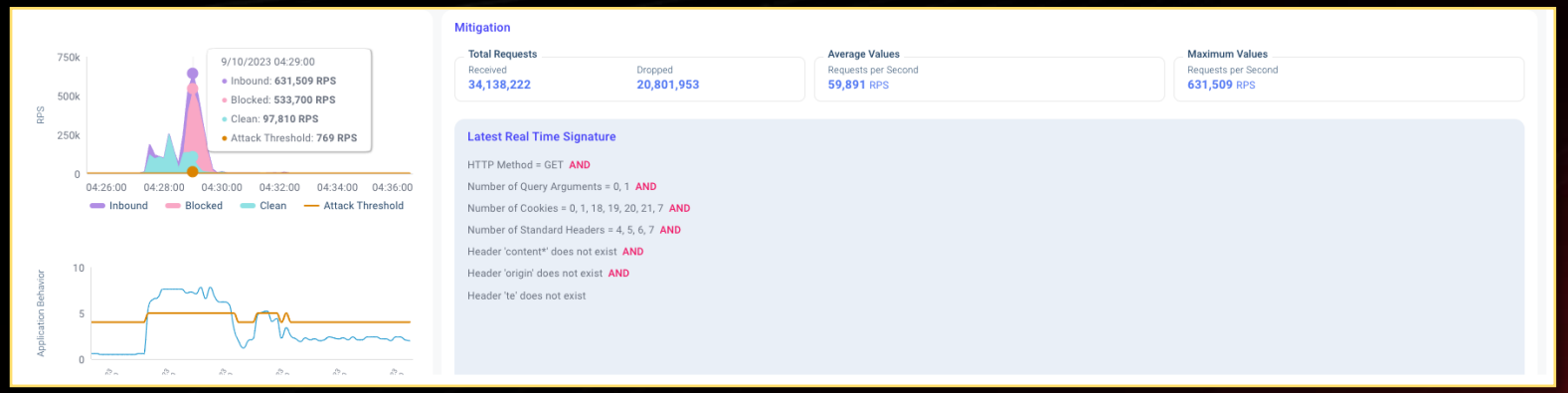
국유 중요 인프라 서비스

출처: Radware 공격 탐지 및 완화 데이터

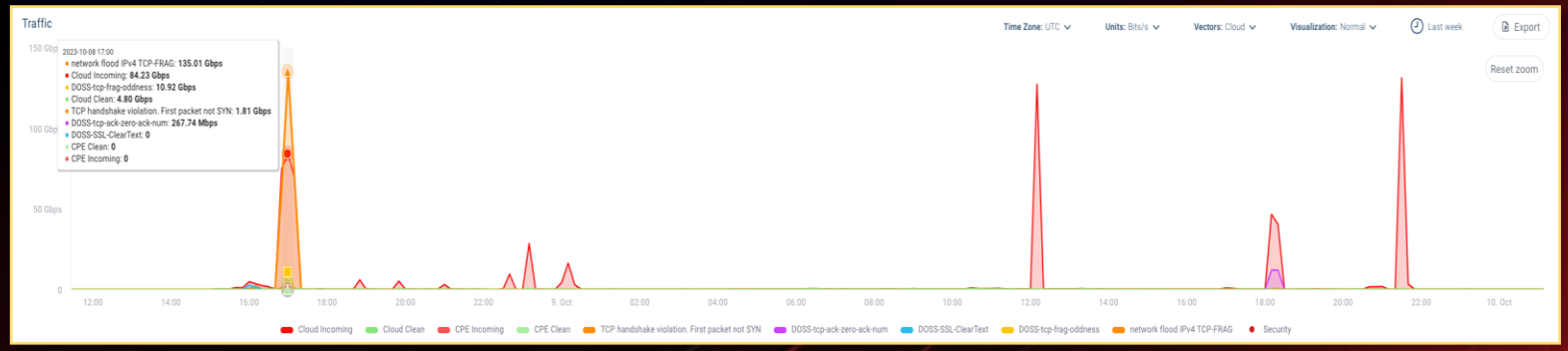
이스라엘 전쟁 – “Iron Swords” 작전 – DDoS 공격



Bank A (금융 서비스):
Network Flood 〉90Gbps
공격 완전 방어 및 서비스 영향 없음

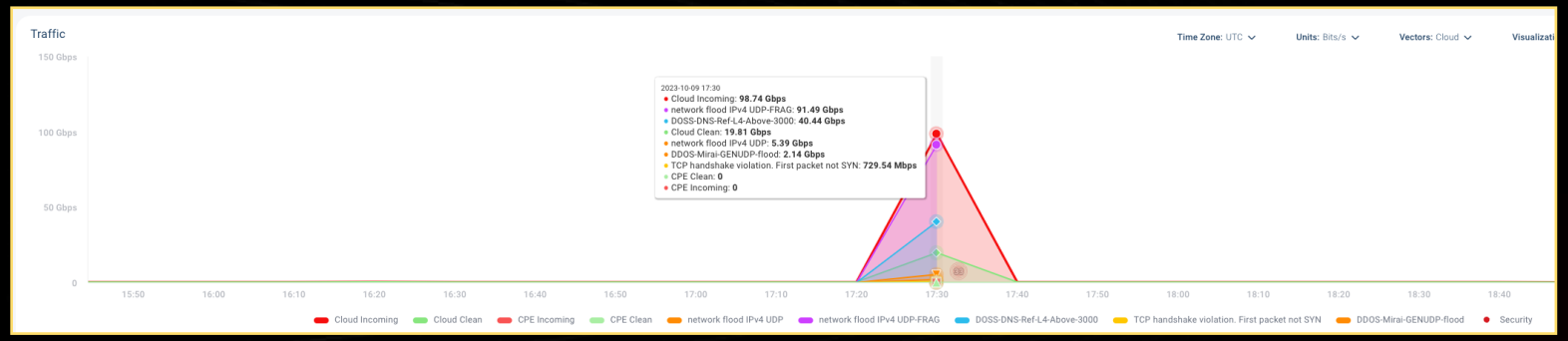


국영 공공 서비스 :
HTTPS Flood 〉650K RPS
공격 완전 방어 및 서비스 영향 없음

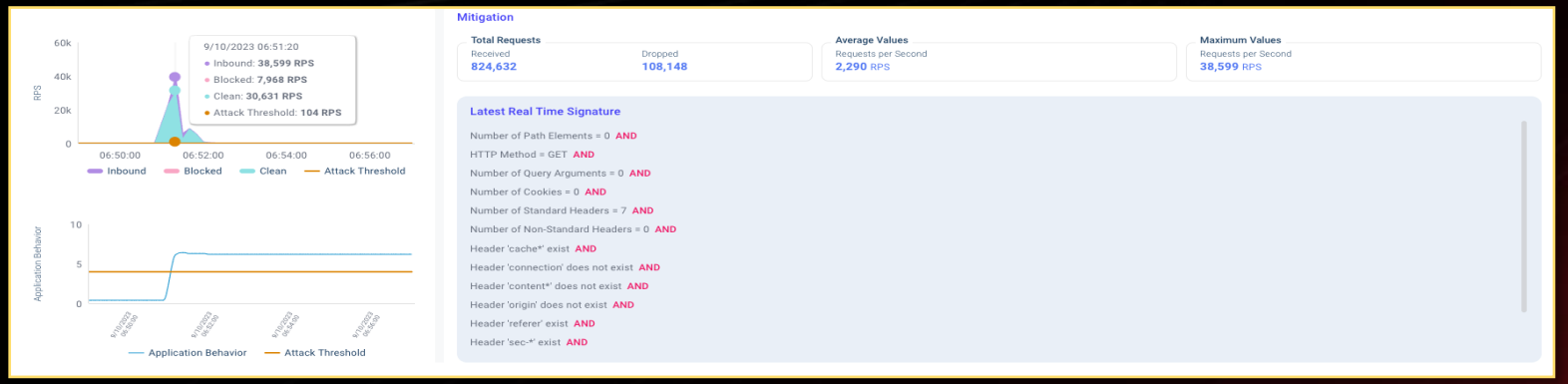


정부 서비스 :
Network Flood 〉135Gbps
공격 완전 방어 및 서비스 영향 없음

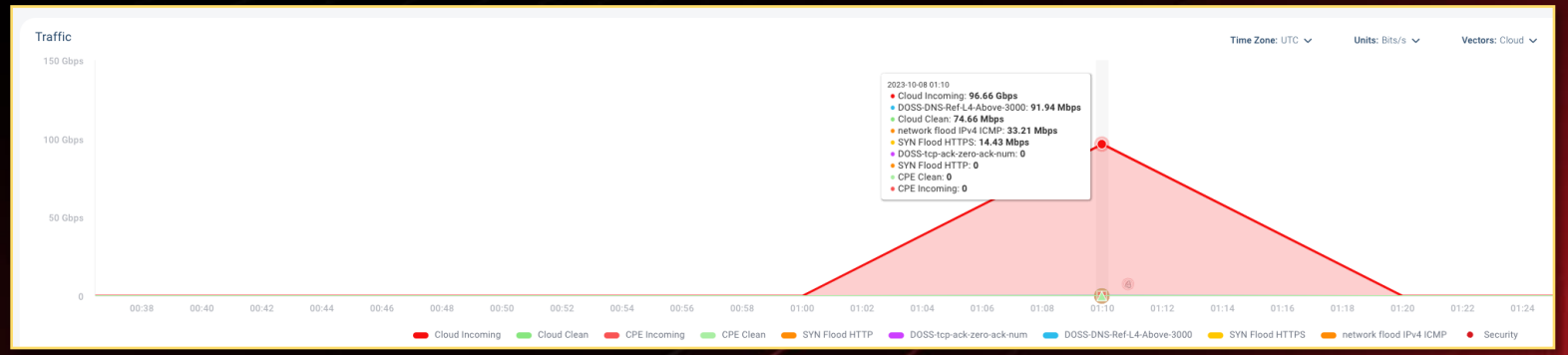
이스라엘 전쟁 – “Iron Swords” 작전 – DDoS 공격



Bank C (금융 서비스) :
Network Flood 〉 96Gbps
공격 완전 방어 및 서비스 영향 없음



국영 교통 서비스 :
HTTPS Flood 〉 35K RPS
공격 완전 방어 및 서비스 영향 없음



국유 중요 인프라 서비스 :
Network Flood 〉 98Gbps
공격 완전 방어 및 서비스 영향 없음

새로운 형태의 디도스 공격 – 이스라엘 철도 회사

공격 피크

L3/4
454
Gbps

L7
159K
RPS

공격 시간

2:35
HOURS MINUTES

공격 레이어

3, 4, 7

공격 차단 엔진

Geo Blocking, BDOS,
UDP Block List, Syn Flood,
Anomalies, Intrusions,
Rate Limit

새로운 형태의 디도스 공격 – Microsoft 365 (23년 6월)

최근 발생한 L7 DDoS 공격에 대한 마이크로소프트의 공식 답변

Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks

MSRC / By MSRC / June 16, 2023 / 3 min read

Summary

Beginning in early June 2023, Microsoft identified surges in traffic against some services that temporarily impacted availability. Microsoft promptly opened an investigation and subsequently began tracking ongoing DDoS activity by the threat actor that Microsoft tracks as Storm-1359.

These attacks likely rely on access to multiple virtual private servers (VPS) in conjunction with rented cloud infrastructure, open proxies, and DDoS tools.

We have seen no evidence that customer data has been accessed or compromised.

This recent DDoS activity targeted layer 7 rather than layer 3 or 4. Microsoft hardened layer 7 protections including tuning Azure Web Application Firewall (WAF) to better protect customers from the impact of similar DDoS attacks. While these tools and techniques are highly effective at mitigating the majority of disruptions, Microsoft consistently reviews the performance of its hardening capabilities and incorporates learnings into refining and improving their effectiveness.

Customers should review the technical details and recommended actions section of this blog to increase the resilience of their environments to help mitigate similar attacks.

Technical Details

Microsoft assessed that Storm-1359 has access to a collection of botnets and tools that could enable the threat actor to launch DDoS attacks from multiple cloud services and open proxy infrastructures. Storm-1359 appears to be focused on disruption and publicity.

Storm-1359 has been observed launching several types of layer 7 DDoS attack traffic:

- **HTTP(S) flood attack** – This attack aims to exhaust the system resources with a high load of SSL/TLS handshakes and HTTP(S) requests processing. In this case, the attacker sends a high load (in the millions) of HTTP(S) requests that are well distributed across the globe from different source IPs. This causes the application backend to run out of compute resources (CPU and memory).
- **Cache bypass** – This attack attempts to bypass the CDN layer and can result in overloading the origin servers. In this case, the attacker sends a series of queries against generated URLs that force the frontend layer to forward all the requests to the origin rather serving from cached contents.
- **Slowloris** – This attack is where the client opens a connection to a web server, requests a resource (e.g., an image), and then fails to acknowledge the download (or accepts it slowly). This forces the web server to keep the connection open and the requested resource in memory.

- DDoS 공격으로 인해 Microsoft 365 서비스 중단 발생
- L3/L4 보다 L7 공격에 집중
- 여러 퍼블릭 클라우드 서비스 및 프록시에 걸쳐 글로벌 봇넷을 기반으로 한 공격

새로운 형태의 디도스 공격 – Microsoft 365 (23년 6월)

Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks

MSRC / By MSRC / June 16, 2023 / 3 min read

Summary

Beginning in early June 2023, Microsoft identified surges in traffic against some services that temporarily impacted availability. Microsoft promptly opened an investigation and subsequently began tracking ongoing DDoS activity by the threat actor that Microsoft tracks as Storm-1359.

These attacks likely rely on access to multiple virtual private servers (VPS) in conjunction with rented cloud infrastructure, open proxies, and DDoS tools.

Recommendations – Layer 7 DDoS Protection Tips

Microsoft recommends customers review the following mitigations to reduce their impact to layer 7 DDoS attacks:

- Use layer 7 protection services such as Azure Web Application Firewall (WAF) (available with Azure Front Door, Azure Application Gateway) to protect web applications.

If using Azure WAF:

- Use the bot protection managed rule set provides protection against known bad bots. For more information, see Configuring bot protection.
- IP addresses and ranges that you identify as malicious should be blocked. For more information, see examples at Create and use custom rules.
- Traffic from outside a defined geographic region, or within a defined region, should be blocked, rate limited or redirected to a static webpage. For more information, examples at Create and use custom rules.
- Create custom WAF rules to automatically block and rate limit HTTP or HTTPS attacks that have known signatures.

series of queries against generated URLs that force the frontend layer to forward all the requests to the origin rather serving from cached contents.

- **Slowloris** – This attack is where the client opens a connection to a web server, requests a resource (e.g., an image), and then fails to acknowledge the download (or accepts it slowly). This forces the web server to keep the connection open and the requested resource in memory.

MS가 대안으로 권고하는
Azure WAF 기술 조합으로도
L7 DDoS 방어에 실패함

파괴적인 Web DDoS 공격

더 높아진 볼륨 – 울트라 급의 높은 RPS

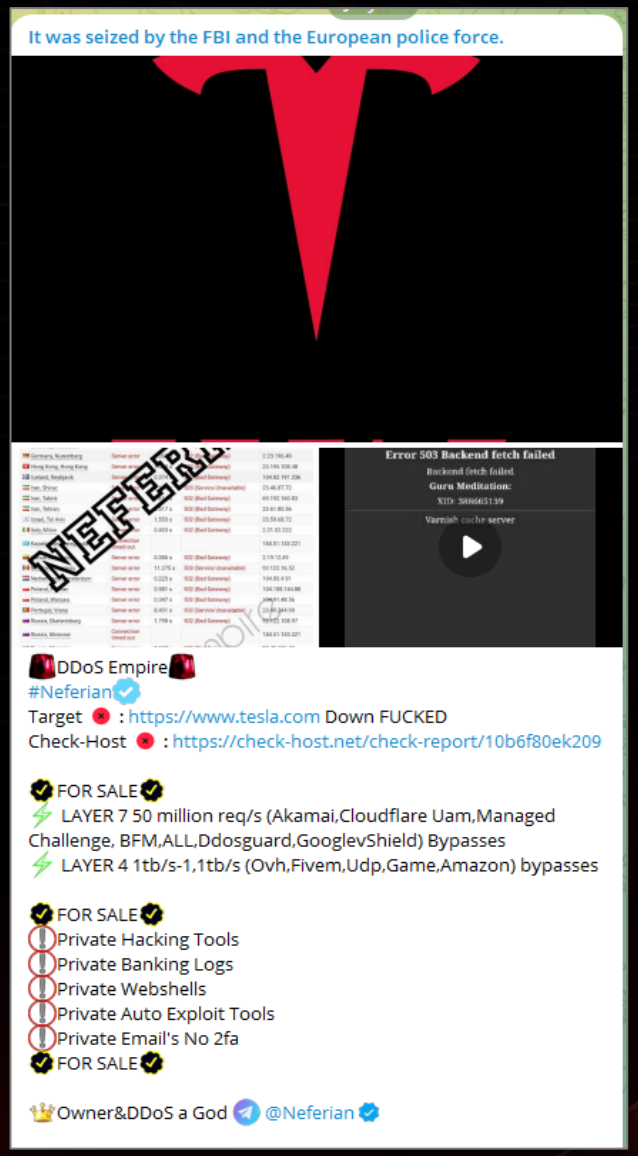
암호화된 공격 트래픽

정상적인 요청 형태를 띰

자동화된 알고리즘 기반의 다양하고 정교한 회피 기술 사용 (무작위 헤더 및 캐쉬 등)

정확한 탐지 및 완화를 위해서는 자동화 된 행동 기반의 탐지/차단 방식이 필요

A사 고객사 피해 사례



Location	Result	Time	Code	IP address
Austria, Vienna	Server error	0.607 s	502 (Bad Gateway)	2.23.196.49
Brazil, Sao Paulo	Server error	0.483 s	502 (Bad Gateway)	23.223.204.49
Bulgaria, Sofia	Connection timed out			2.21.250.215
Czechia, C.Budejovice	Connection timed out			184.51.133.221
Finland, Helsinki	Server error	0.480 s	502 (Bad Gateway)	72.246.168.53
France, Paris	Server error	0.477 s	502 (Bad Gateway)	23.77.166.42
Germany, Frankfurt	Server error	0.619 s	502 (Bad Gateway)	2.23.196.49
Germany, Nuremberg	Server error	0.265 s	502 (Bad Gateway)	2.23.196.49
Hong Kong, Hong Kong	Server error	1.023 s	502 (Bad Gateway)	23.195.108.48
Iceland, Reykjavik	Server error	0.374 s	502 (Bad Gateway)	104.82.191.236
Iran, Shiraz	Server error	0.138 s	503 (Service Unavailable)	23.46.87.72
Iran, Tabriz	Server error	1.614 s	502 (Bad Gateway)	69.192.160.83
Iran, Tehran	Server error	0.517 s	502 (Bad Gateway)	23.61.80.56
Israel, Tel Aviv	Server error	0.553 s	502 (Bad Gateway)	23.59.68.72
Italy, Milan	Server error	0.453 s	502 (Bad Gateway)	2.21.52.222
Kazakhstan, Karaganda	Connection timed out			184.51.133.221
Lithuania, Vilnius	Server error	0.386 s	502 (Bad Gateway)	2.19.12.49
Moldova, Chisinau	Server error	1.275 s	503 (Service Unavailable)	92.122.16.52
Netherlands, Amsterdam	Server error	0.225 s	502 (Bad Gateway)	104.85.4.91
Poland, Poznan	Server error	0.581 s	502 (Bad Gateway)	104.108.144.88
Poland, Warsaw	Server error	0.347 s	502 (Bad Gateway)	104.91.48.56
Portugal, Viana	Server error	0.431 s	503 (Service Unavailable)	23.49.244.99
Russia, Ekaterinburg	Server error	1.798 s	502 (Bad Gateway)	92.122.108.97
Russia, Moscow	Connection timed out			184.51.133.221
Russia, Moscow	Server error	0.558 s	502 (Bad Gateway)	23.45.136.49
Russia, Saint Petersburg	Connection timed out			92.122.108.97
Serbia, Belgrade	Connection timed out			104.96.94.158
Spain, Barcelona	Server error	0.926 s	502 (Bad Gateway)	92.123.32.61
Switzerland, Zurich	Server error	0.297 s	502 (Bad Gateway)	184.86.81.69
Thailand, Bangkok	Server error	0.675 s	502 (Bad Gateway)	104.90.196.51

* 테슬라

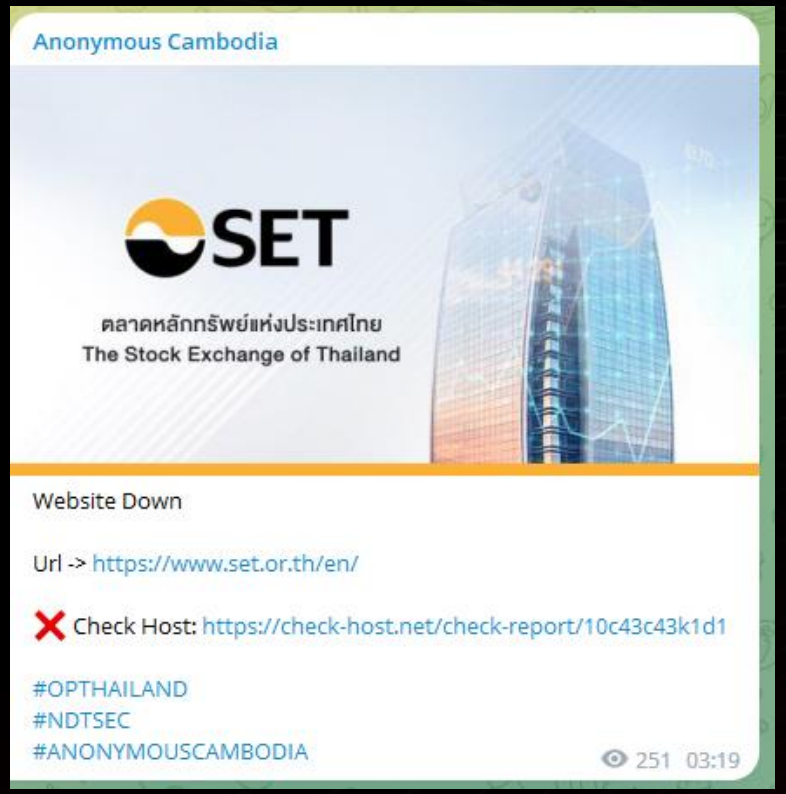
- Website : www.tesla.com
- Country : 미국 (USA)
- Industry :

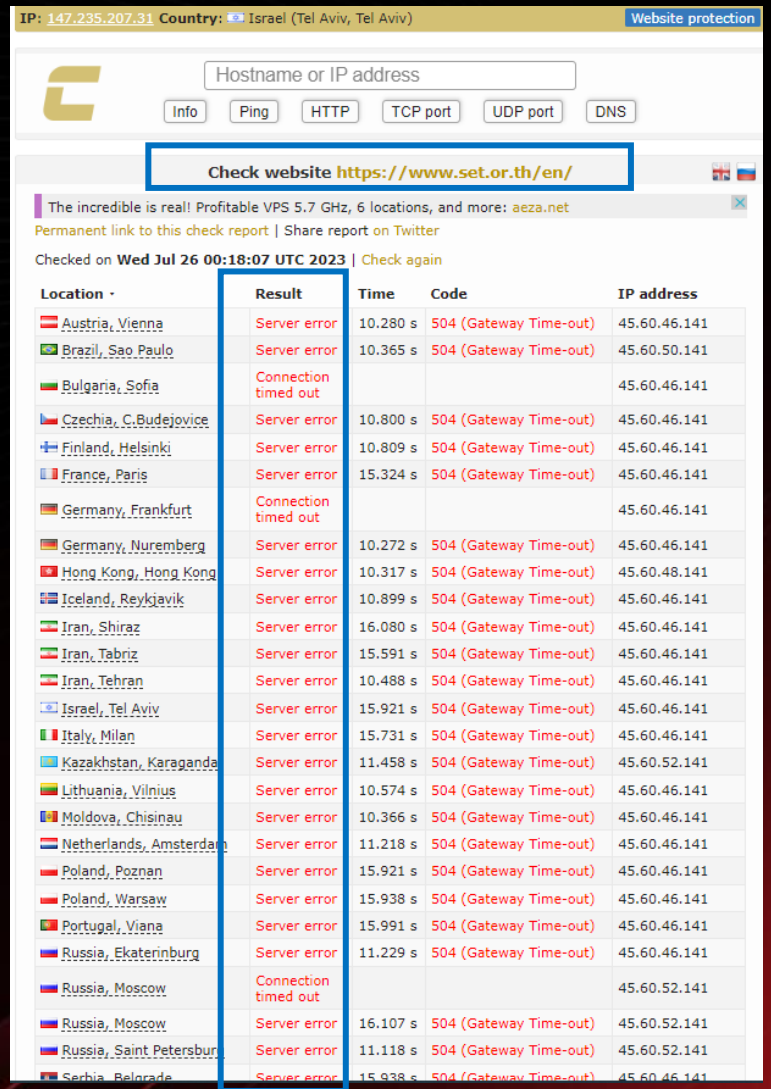
전기 자동차 제조업체 (Electric vehicles manufacturer)

- Telegram Message (DDoS Empire) :

https://t.me/DDoSEmpire/789

I사 고객사 피해 사례



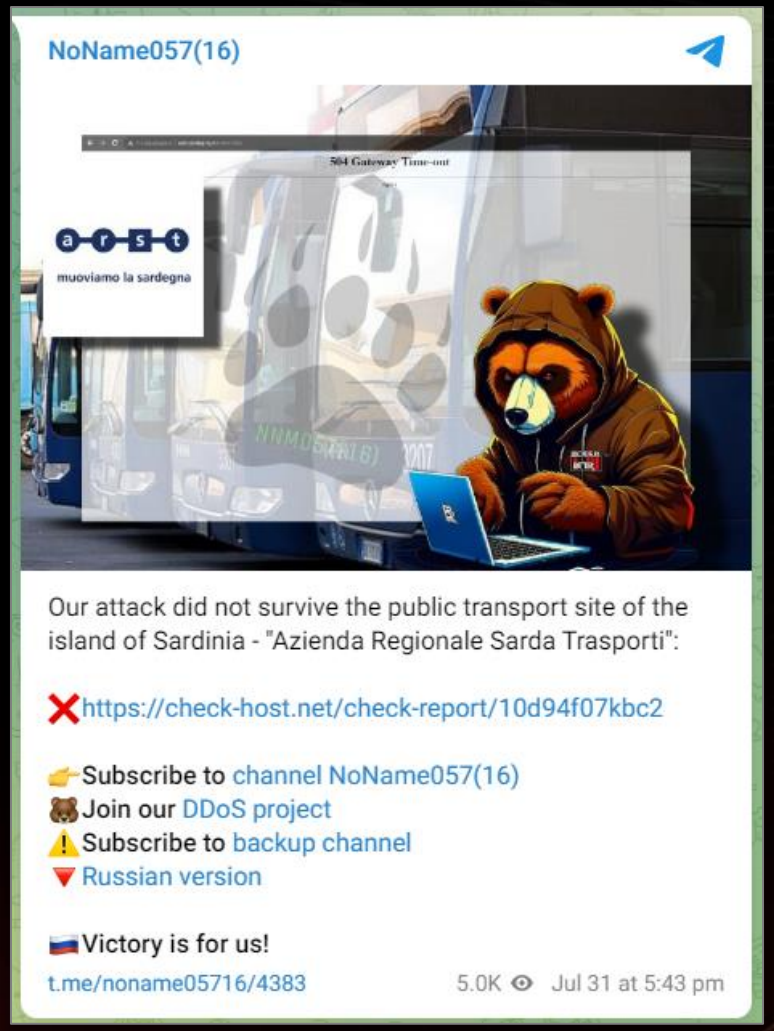


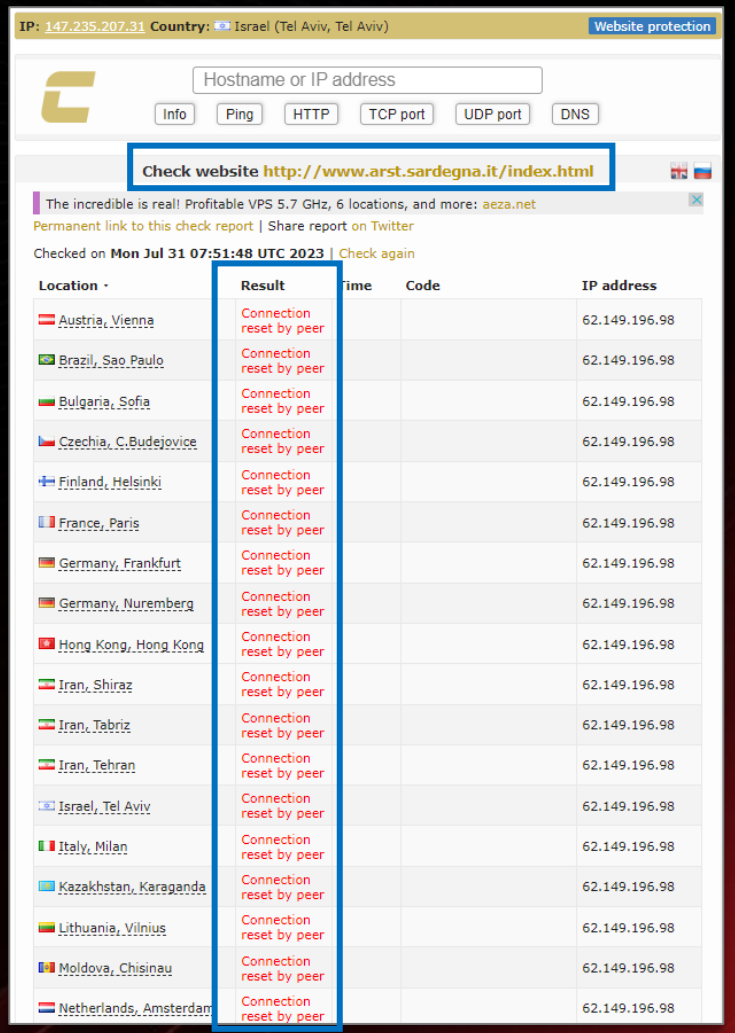
* 태국 증권 거래소 (Stock Exchange of Thailand)

- Web Site : www.set.or.th
- Country : 태국 (Thailand)
- Industry : 금융 서비스 (FSI)
- Telegram Message (Anonymous Cambodia) :

  https://t.me/anoncambodia/74

C사 고객사 피해 사례





* 사르디니아 교통공단

- Web Site : www.arst.sardegna.it
- Country : 이탈리아
- Industry : 정부 (Government)
- Telegram Message (Noname057) :

https://t.me/noname05716/4383

기존 솔루션 방어는 효과적인 방어가 불가

네트워크 기반 디도스 보호는 L7 공격을 탐지 및 완화 할 수 없음

기존 WAF 솔루션은 취약점 공격 대응이 주 목표

속도 제한 (Rate-limiting)은 정상적인 트래픽에도 영향

기존 방어 솔루션으로는 정상적인 웹 트래픽에 영향을 주거나 HTTP/S 공격을 탐지 및 완화 할 수 없음!

라드웨어 클라우드 디도스 솔루션

TREND MICRO

라드웨어 디도스 솔루션

클라우드 서비스

Always-On & On-Demand

하이브리드

Integrated Cloud & Appliance

어플라이언스

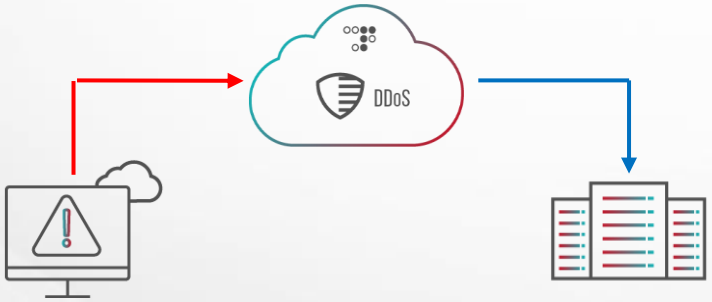
Physical / Virtual

라드웨어 클라우드 디도스 서비스

클라우드 서비스

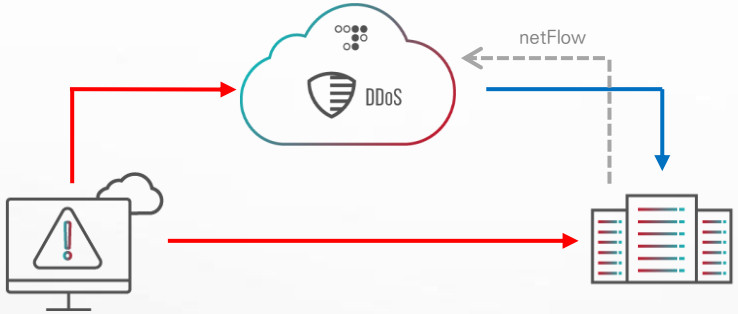
Always-On & On-Demand

Always-on



- 라드웨어 스크러빙 센터의 DDoS 완화 장비로 **항상 우회** 됨
- 클라우드 스크러빙 센터를 통한 **실시간 공격 탐지 및 완화**

On-Demand



- DDoS 공격 탐지 :
  - NetFlow 정보를 통한 탐지
  - Arbor TMS messages
  - AWS and Azure telemetry
- **공격 시** 만 트래픽 우회

라드웨어 클라우드 디도스 서비스

DDoS 클라우드 스크러빙 센터

19 개
클라우드 디도스 센터 보유

12 Tbps
이상 글로벌 방어 성능

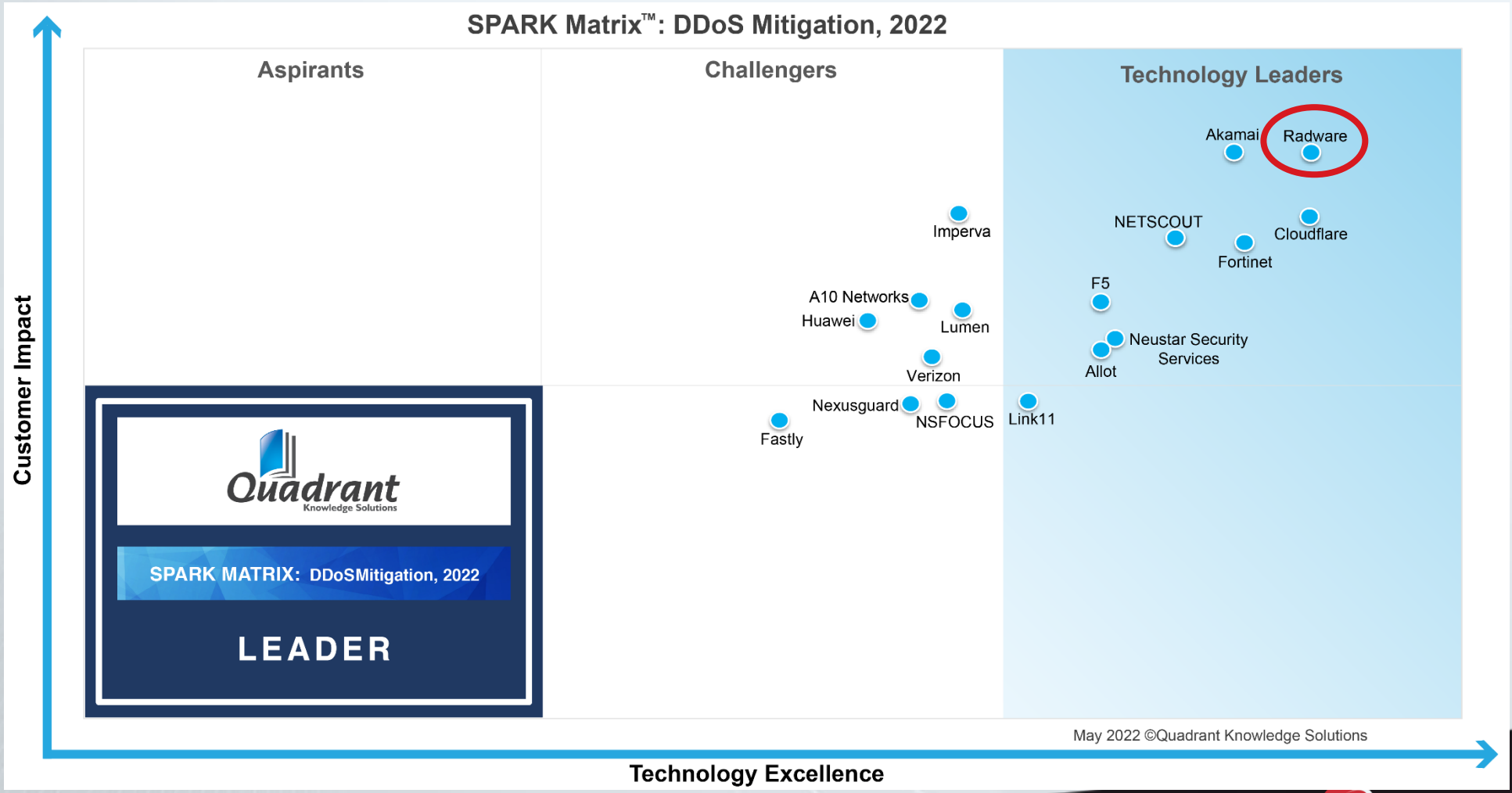
국내 SC센터
국내 디도스 클라우드 센터 보유

라드웨어 – 글로벌 DDoS 보호 시장의 마켓 리더

Quadrant Knowledge Solutions

SPARK Matrix: DDoS Mitigation, 2022

LEADER

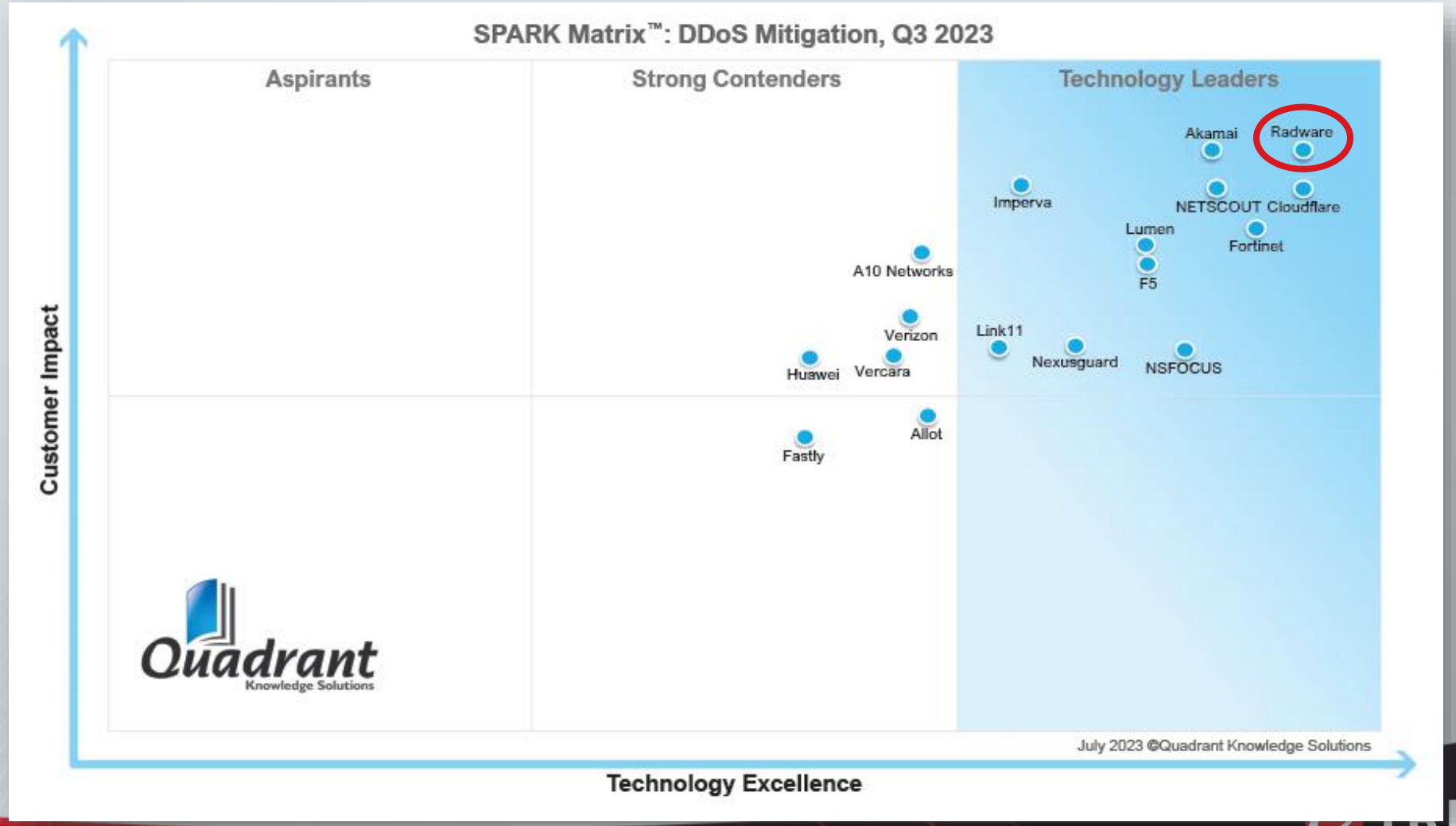


라드웨어 – 글로벌 DDoS 보호 시장의 마켓 리더

Quadrant Knowledge Solutions

SPARK Matrix: DDoS Mitigation, 2023

LEADER



라드웨어 클라우드 디도스 서비스

최고의 클라우드 디도스 방어 서비스

- 클라우드 디도스 완화 시장의 리더
- 행동 기반의 탐지 – 악성 트래픽만 차단
- 실시간 시그니처 생성을 통한 완화

완전 자동화된 방어 서비스

- 보안 전문가(ERT)의 완전 관리형 보안 서비스
- 담당자의 운영 부하 감소

포괄적인 보호 서비스

- 전용 디도스 포털에서 분산된 대규모 네트워크 자산 운영 및 관리
- 유연한 서비스 구성 – 상시 우회 서비스, 온디맨드, 하이브리드

IDC Analyze the Future — DDoS MarketScape **#1 Leader**

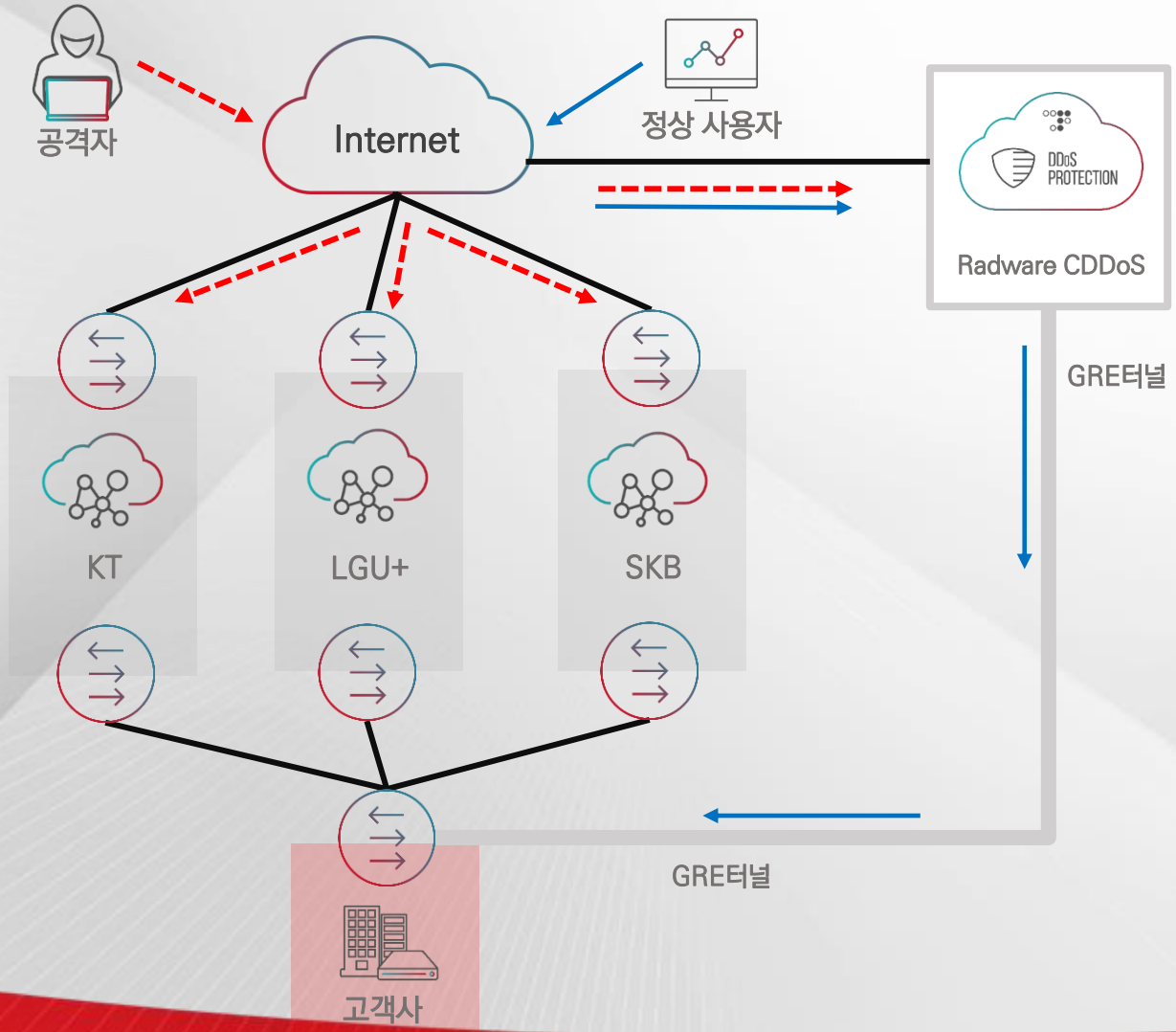
FORRESTER® WAVE LEADER 2021 DDoS Mitigation Solutions — DDoS Wave **Leader**

Quadrant Knowledge Solutions — SPARK Matrix:
DDoS Mitigation, 2022 **Leader**
DDoS Mitigation, 2023 **Leader**

AT&T verizon Deutsche Telekom U.S.Cellular Telefónica vodafone Singtel Bell TELSTRA

TREND MICRO

통신사 클린존 서비스와 비교



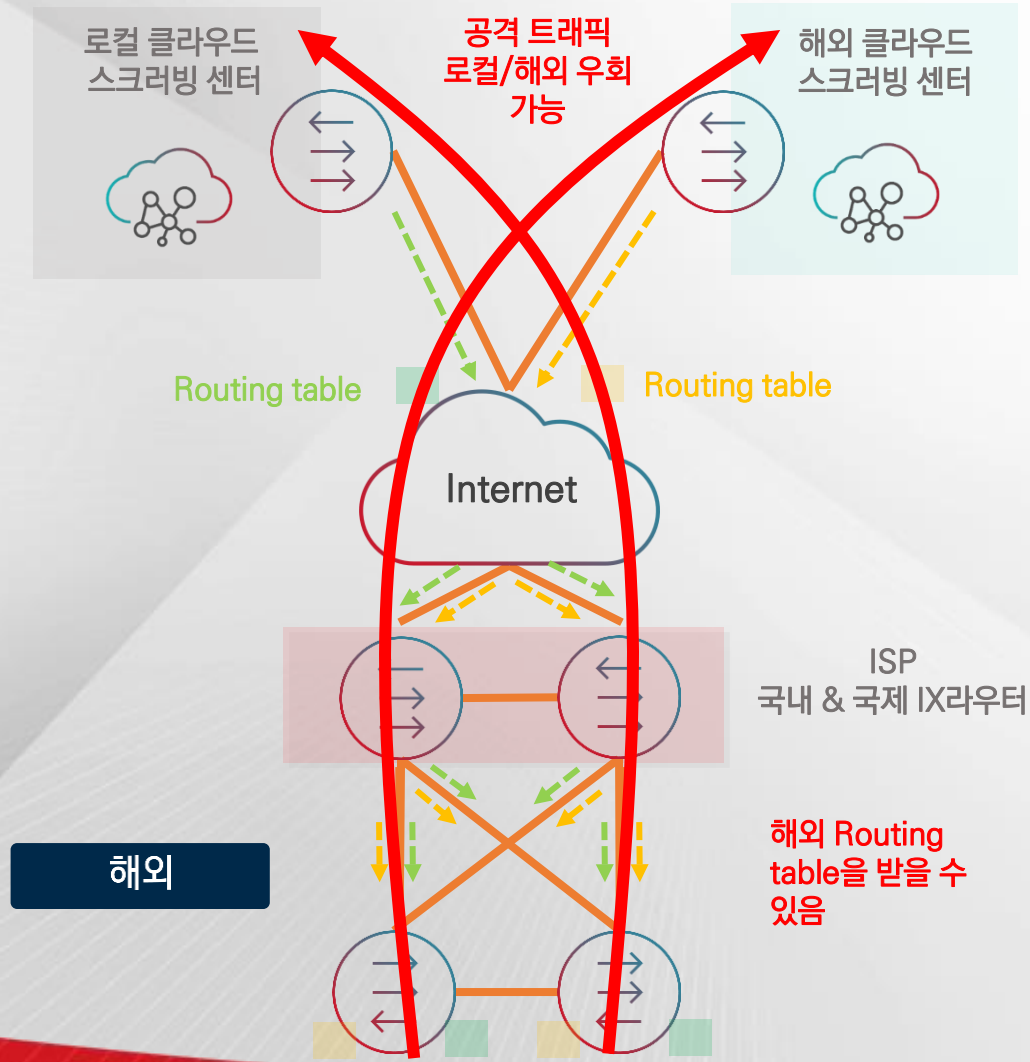
통신사 클린존 서비스

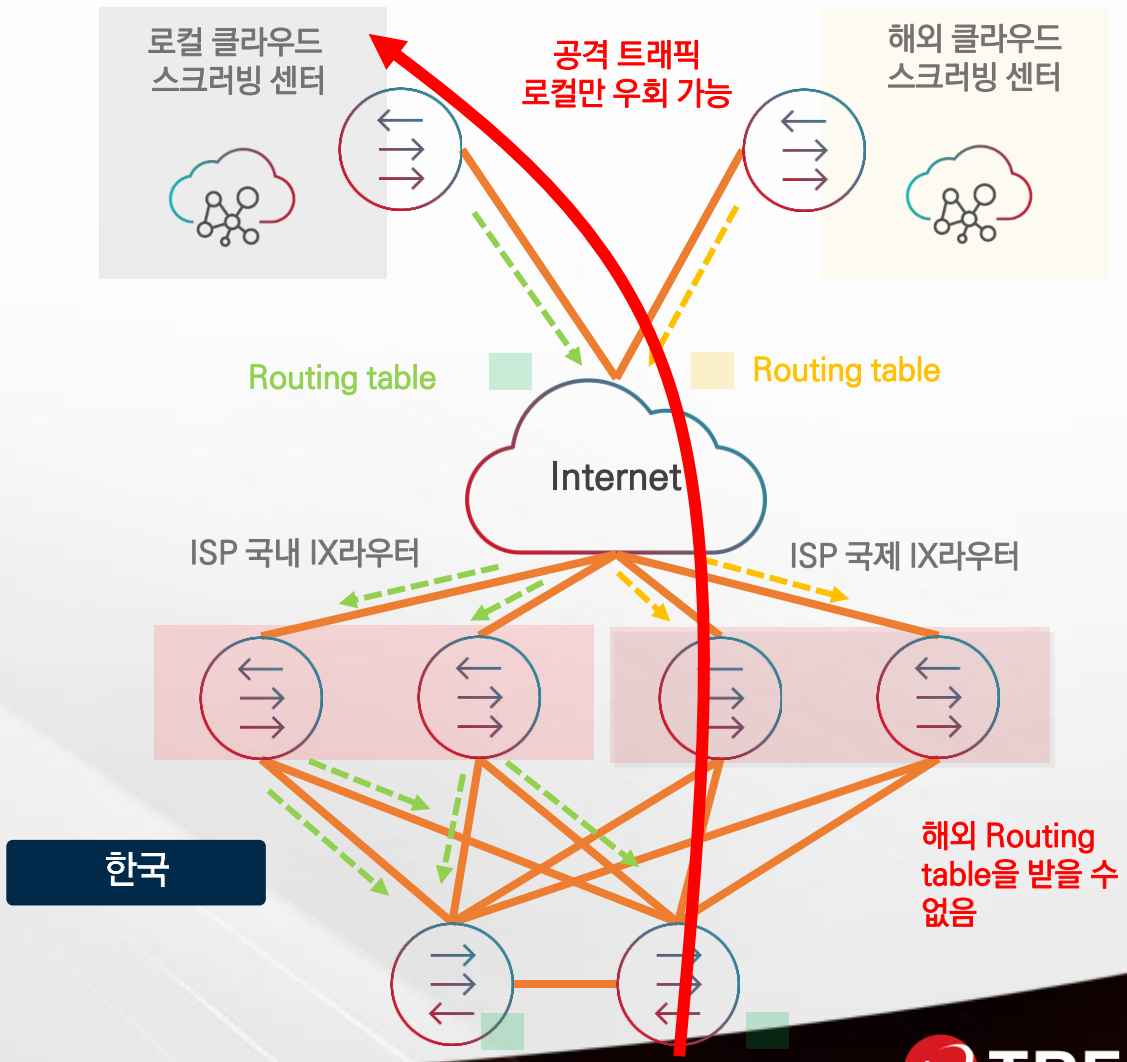
- ✓ 해당 회선의 공격만 차단
- ✓ 제한적인 해외 공격 차단
- ✓ 3개사 회선 사용시 회선별 클린존 필요 – 고비용
- ✓ 전용 포털 미제공

라드웨어 클라우드 DDoS

- ✓ 국내/국제회선 상관없이 공격 차단 제공
- ✓ 각 회선별 클린존 서비스 비용 대비 저렴
- ✓ 전용 포털 화면 제공 (수동/자동 우회)

왜 국내의 로컬 클라우드 스크러빙 센터가 필요한가?

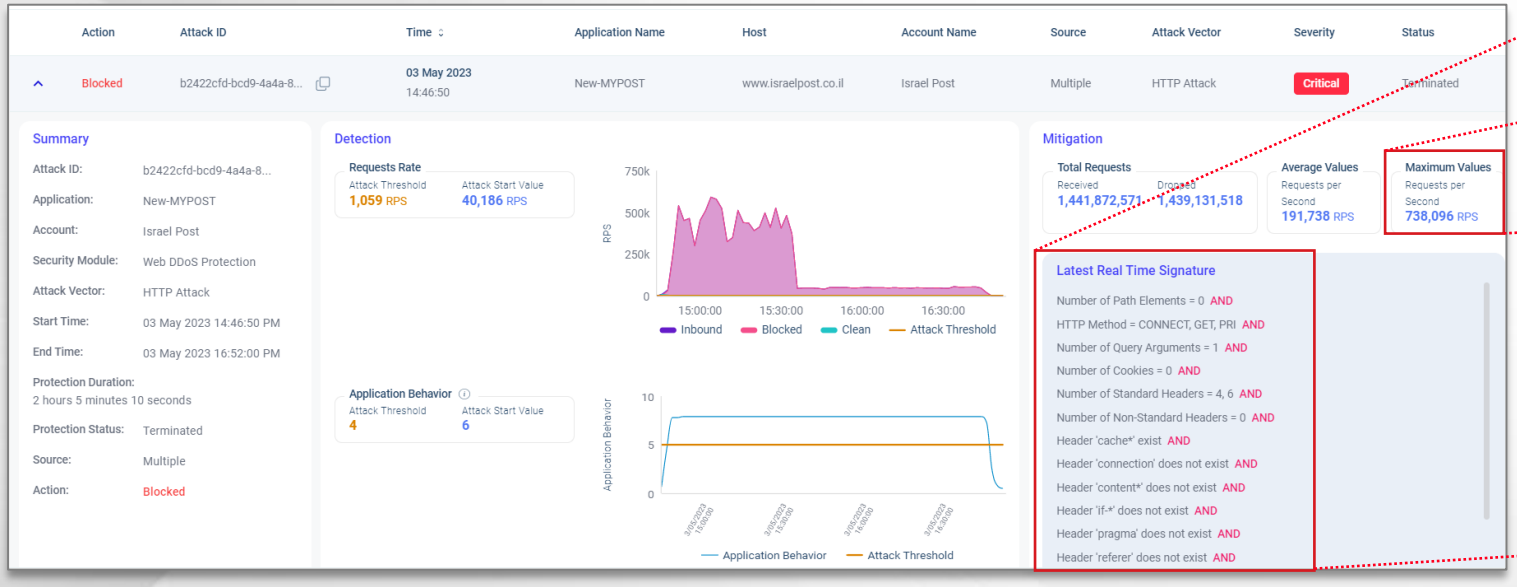




라드웨어 웹 디도스 솔루션

Web DDoS

Web DDoS 공격으로부터 정부 서비스를 보호 (2023년5월)



Latest Real Time Signature
Number of Path Elements = 0 AND
HTTP Method = CONNECT, GET, PRI AND
Number of Query Arguments = 1 AND
Number of Cookies = 0 AND
Number of Standard Headers = 4, 6 AND
Number of Non-Standard Headers = 0 AND
Header 'cache*' exist AND
Header 'connection' does not exist AND
Header 'content*' does not exist AND
Header 'if-*' does not exist AND
Header 'pragma' does not exist AND
Header 'referer' does not exist AND

Maximum Values
Requests per Second
738,096 RPS

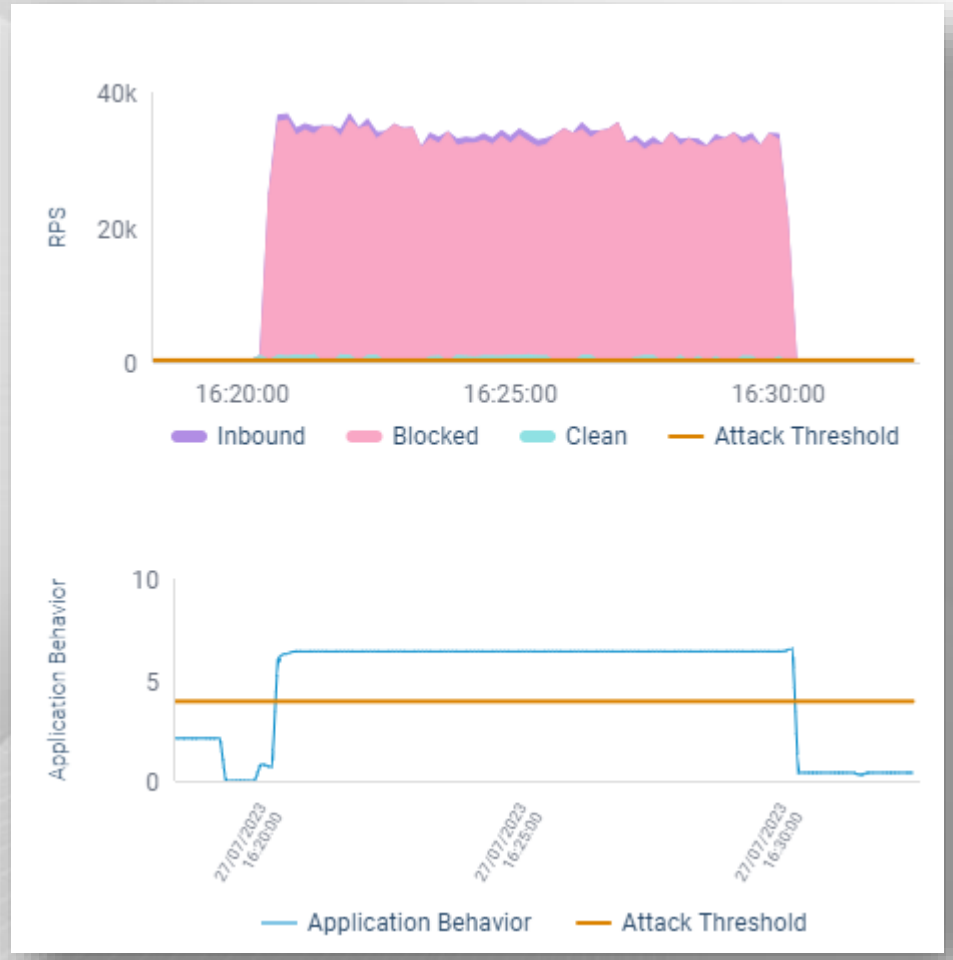
공격 피크
Up to
738K
RPS

공격 시간
Almost
2 Hours

공격 레이어
HTTP 플러드
+
네트워크 플러드

공격 차단 엔진
Web DDoS
+
L3 차단

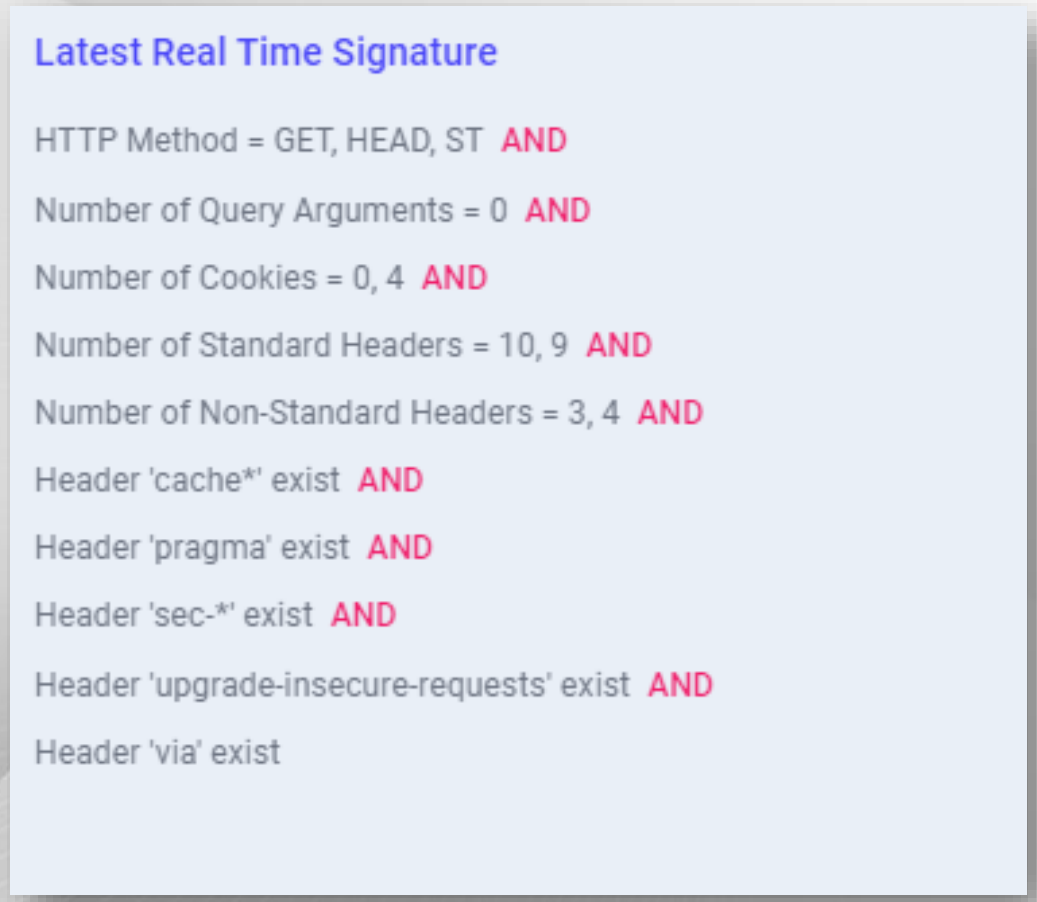
업계 최고의 행동 기반 L7 DDoS 공격 탐지



- 속도기반 (volume) 및 행동기반 (risk) 파라메터를 결합
- 각 파라메터 유형에 대한 별도의 독립적인 임계값
- 볼륨 임계값을 초과하지 않는 저용량 공격도 식별 가능
- 정상 트래픽 증가 와 실제 공격을 구별하여 오탐 최소화

Rate-variant와 Rate-invariant 파라미터를 이용한 행동기반 탐지

자동 실시간 시그니처 생성



변화하는 공격 패턴에 자동으로 실시간 시그니처 생성

- 공격 특성에 맞춰진 **자동화된 실시간 시그니처**
- 최대 **40개의 HTTP/S 매개변수**로 L7 로직에 적용
- 변화하는 트래픽 패턴에 **동적으로 대응**
- 사람의 개입 없이 **자동으로 시그니처를 생성**하고, **공격을 완화**

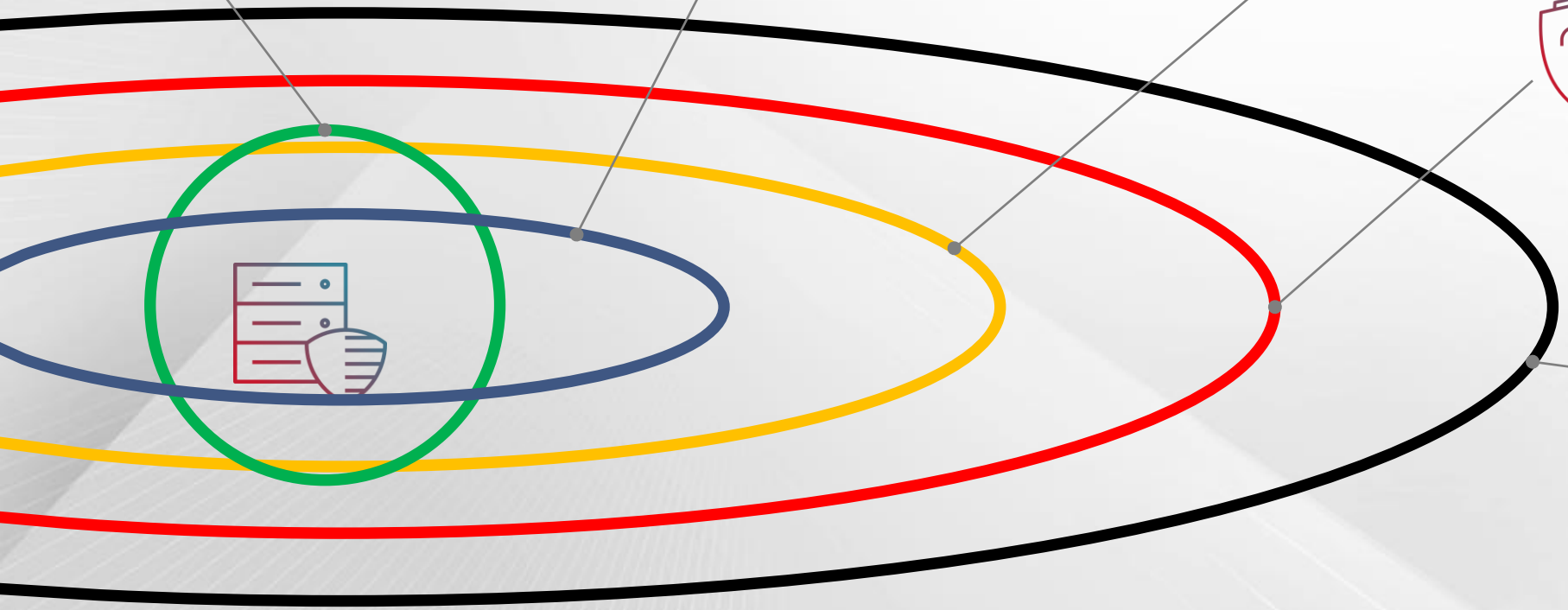
라드웨어 L7 디도스 방어

평상 시 학습
학습 및 베이스라인 및
애플리케이션 동작

L7 행동 탐지
- 사전 공격 탐지
- 일시적인 접속 (Flash Crowd) 증가 식별

향상된 HTTPS – L7 방어
- L7 시그니처 기반 완화

L3-L4 행동기반 탐지 및 완화
- DDoS
- Defense SSL – 인증 (Challenge) 기반의 완화



EAAF & Bad Actors
공격 IP를 식별하고 ACL에
추가하여 즉시 차단

요약

대규모 애플리케이션 디도스 공격으로 빠르게 증가

L3~L7 디도스 공격 방어 체계 구축 필요

정확한 탐지/완화를 위해서는 자동화 된 행동 기반의 탐지/차단 방식 필요

라드웨어의 Cloud DDOS / Web DDoS 방어 솔루션 제공

TREND MICRO™ | Global Leader in Cybersecurity

Radware Korea AMS Team

Security_kr@radware.com

Thank you