A10

Always Secure. Always Available.

The Road to digital Resilliance

The Cybersecurity Landscape and Defense Strategies

Heiko Frank, Systems Engineer Manager, Core Europe

21st June 2023

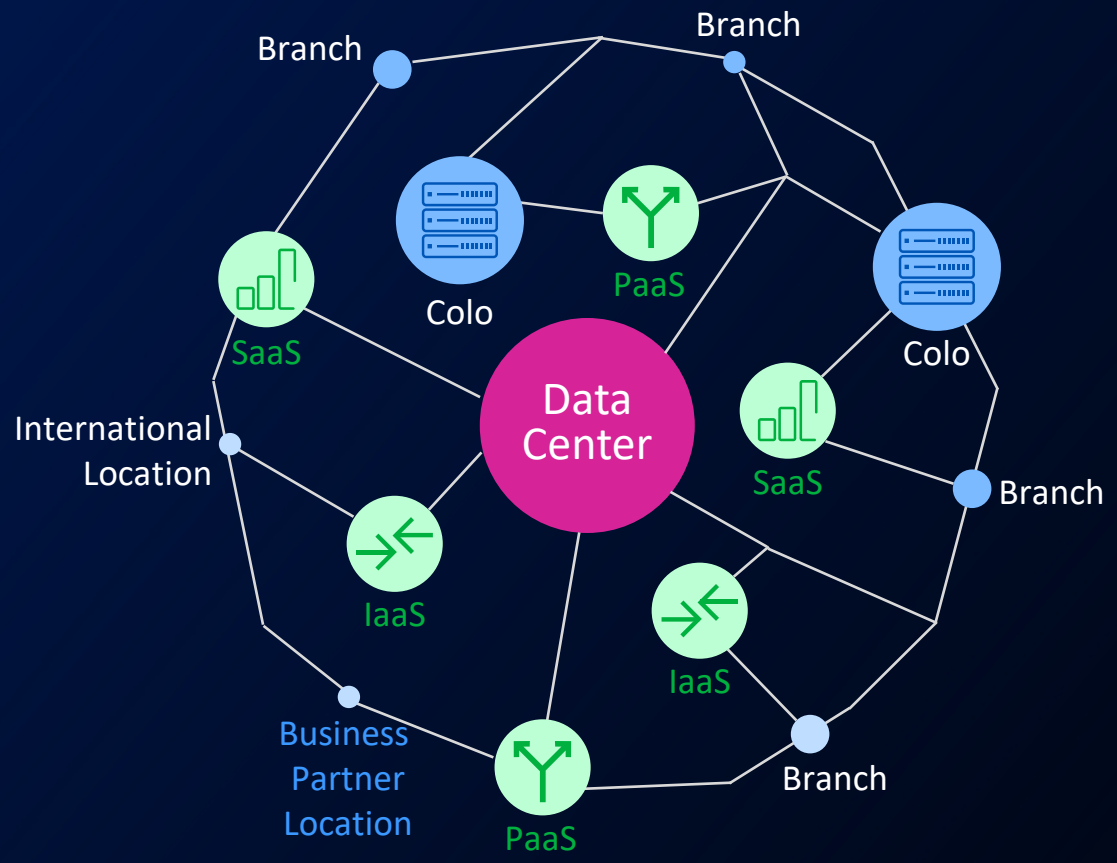
ACCELERATE

What is the biggest Enemy of Security?

Complexity

It’s Getting More Complicated

It’s Getting More Complicated



Cyber Threats and Security Landscape

informa

DARKReading | The Edge | DR Tech | Sections | Events

Attacks/Breaches | 5 MIN READ | NEWS

Attackers Are Already Exploiting ChatGPT to Write Malicious Code

The AI-ba
malware.

CYBER SECURITY HUB INCIDENT OF THE WEEK

IOTW: Russian hackers target NATO sites with DDoS attack

A Russian hacktivist group launched a series of DDoS attacl against NATO affecting the response of search and rescue teams in Turkey and Syria

Add bookmark

Tags: Hacktivist Hacktivism Hacker Cyber Attack Russia Turkey Syria Iran NATO DDo
Attack Distributed Denial Of Service Attack Killnet

Olivia Powell
02/17/2023

The North Atlantic Treaty Organization (NATO) has been the victi
series of **distributed denial of service (DDoS) attacks**, causing temporary disruption to some of its sites.

The DDoS attacks have been linked to the Russian **hacktivist** collective Killnet which had posted via an encrypted channel on social media platform Telegram that it was planning to launch attacks against NATO. The group also appeared to be asking for cryptocurrency donations to launch further attacks.

BLEEPINGCOMPUTER

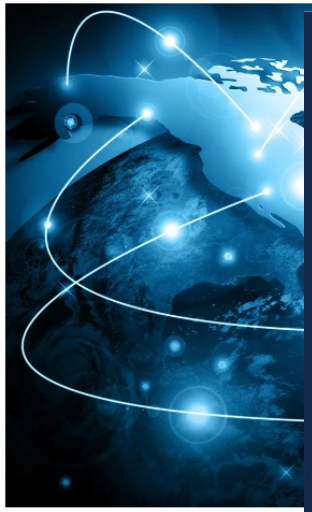
NEWS | DOWNLOADS | VIRUS REMOVAL GUIDES | TUTORIALS | DEALS

Home > News > Security > Russia's largest ISP says 2022 broke all DDoS attack records

Russia's largest ISP says 2022 broke all DDoS attack records

By Bill Toulas

January 23, 2023 03:18 PM 2



Russia's largest internet service pr
of service attacks (DDoS) targeting

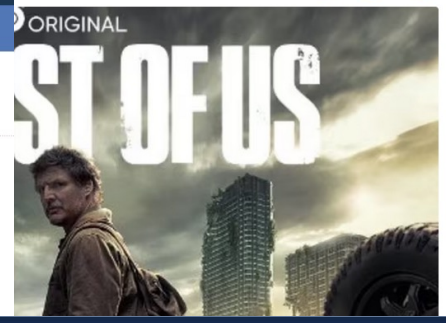
HT TECH
MAKE LIFE SIMPLE

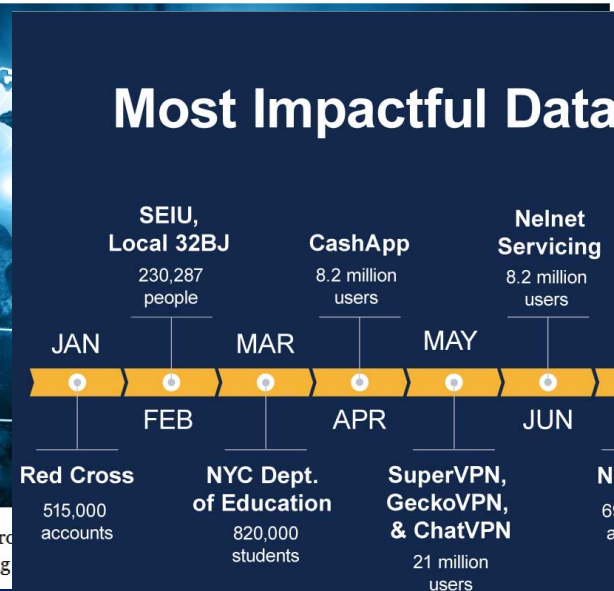
HOME | NEWS | MOBILE | LAPTOPS PC | HOW TO | GADGETS | RECOMMENDER | COMPARE | PHOTOS | VIDEOS | WEB STORIES

Home > Tech > News > Cyber scam alert! 'The Last Of Us' scam spreading fast, can cause money loss

Cyber scam alert! 'The Last Of Us' scam spreading fast, can cause money loss

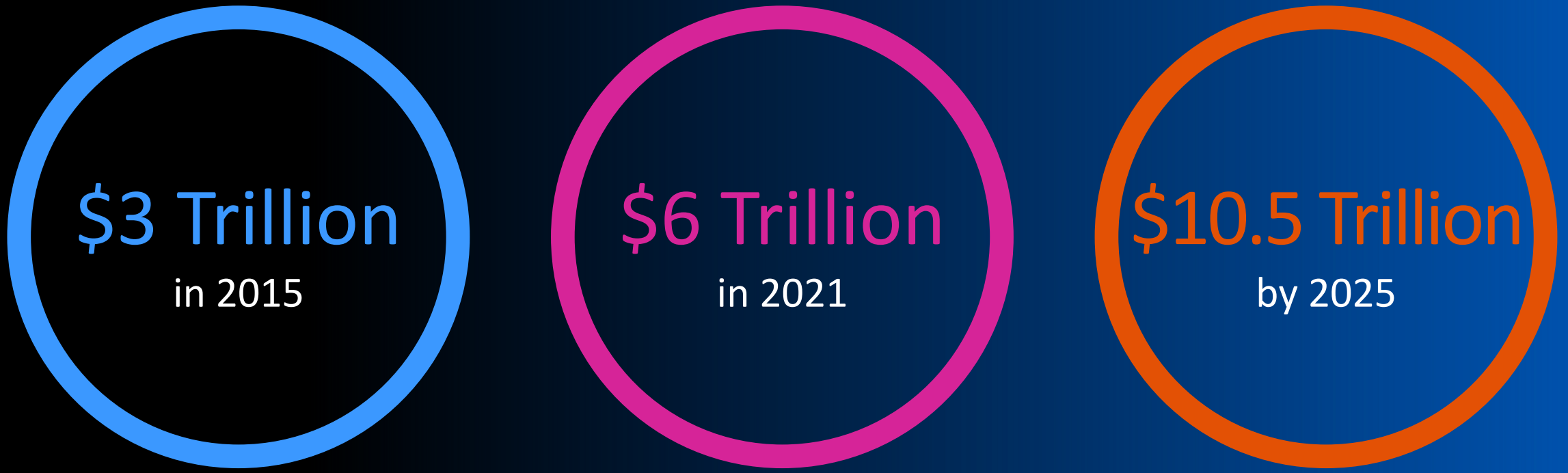
illiant adaptation? Beware as a new scam could steal your money.





ACCELERATE

The Cost of Cybercrime Annually



Source: https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

022

Report Introduction | The State of Cybercrime | Nation State Threats | Devices and Infrastructure | Cyber Influence Operations | Cyber Resilience | Contributing Teams

d

n has network oving to the cloud means enterprises must adopt cloud-native network security to protect digital assets.

Attack complexity, frequency, and volume continue to grow and are no longer limited to holiday seasons, indicating a shift toward year-round attacks. This highlights the importance of ongoing protection beyond traditional peak traffic seasons.

Distributed denial of service (DDoS) attacks

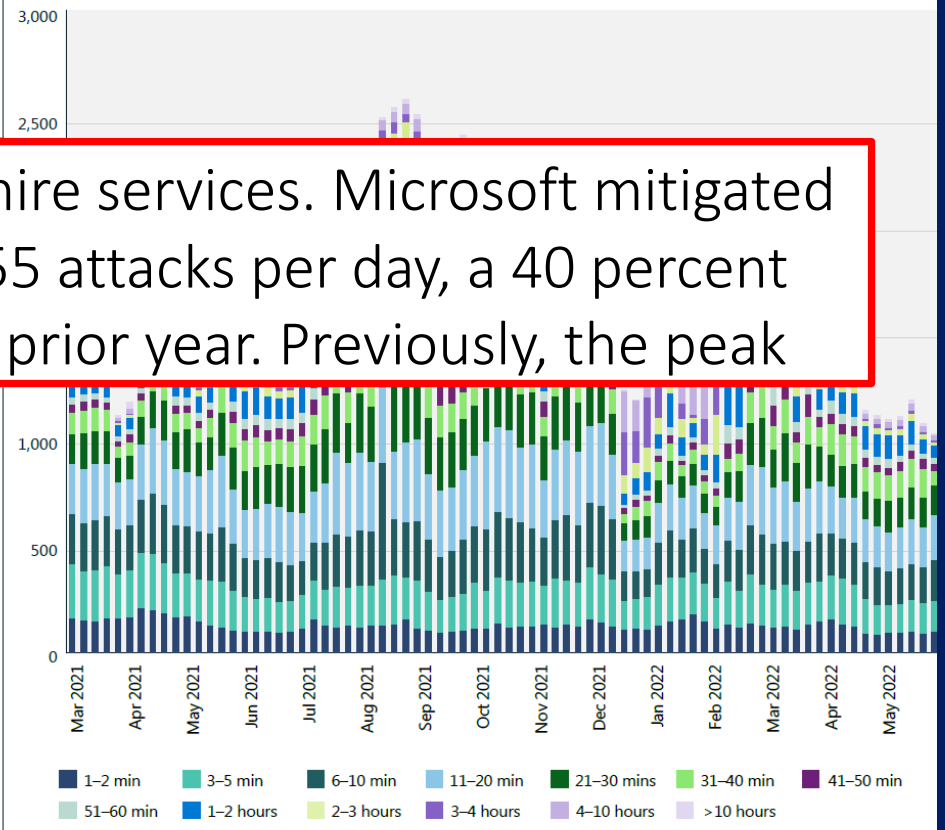
Over the past year, the world experienced DDoS activity that was unprecedented in volume, complexity, and frequency. This DDoS explosion was driven by a substantial increase in nation state attacks and continued proliferation of low-

In November 2021, Microsoft thwarted a volumetric DDoS attack with a throughput of 3.4 terabits per second (Tbps) from approximately 10,000 sources spanning multiple countries. Similar high volumetric attacks above 2+Tbps were mitigated in 2022 highlighting that it's not just the complexity, frequency of attacks that's increasing, but also the volume (bandwidth) of attack.

Attack duration

Most attacks observed over this past year were short-lived. Approximately 28 percent of the attacks lasted less than 10 minutes, 26 percent lasted 10–30 minutes and 14 percent lasted 31–60 minutes. Thirty-two percent of the attacks were more than an hour in duration.

Number of DDoS attacks and duration distribution
(March 2021–May 2022)



Most attacks in the last year were short-lived. Approximately 28 percent of the attacks lasted less than 10 minutes.

Cost of DDoS-for-hire services. Microsoft mitigated an average of 1,955 attacks per day, a 40 percent increase from the prior year. Previously, the peak

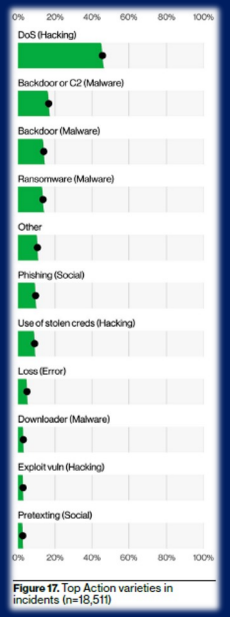


Figure 17. Top Action varieties in incidents (n=18,511)

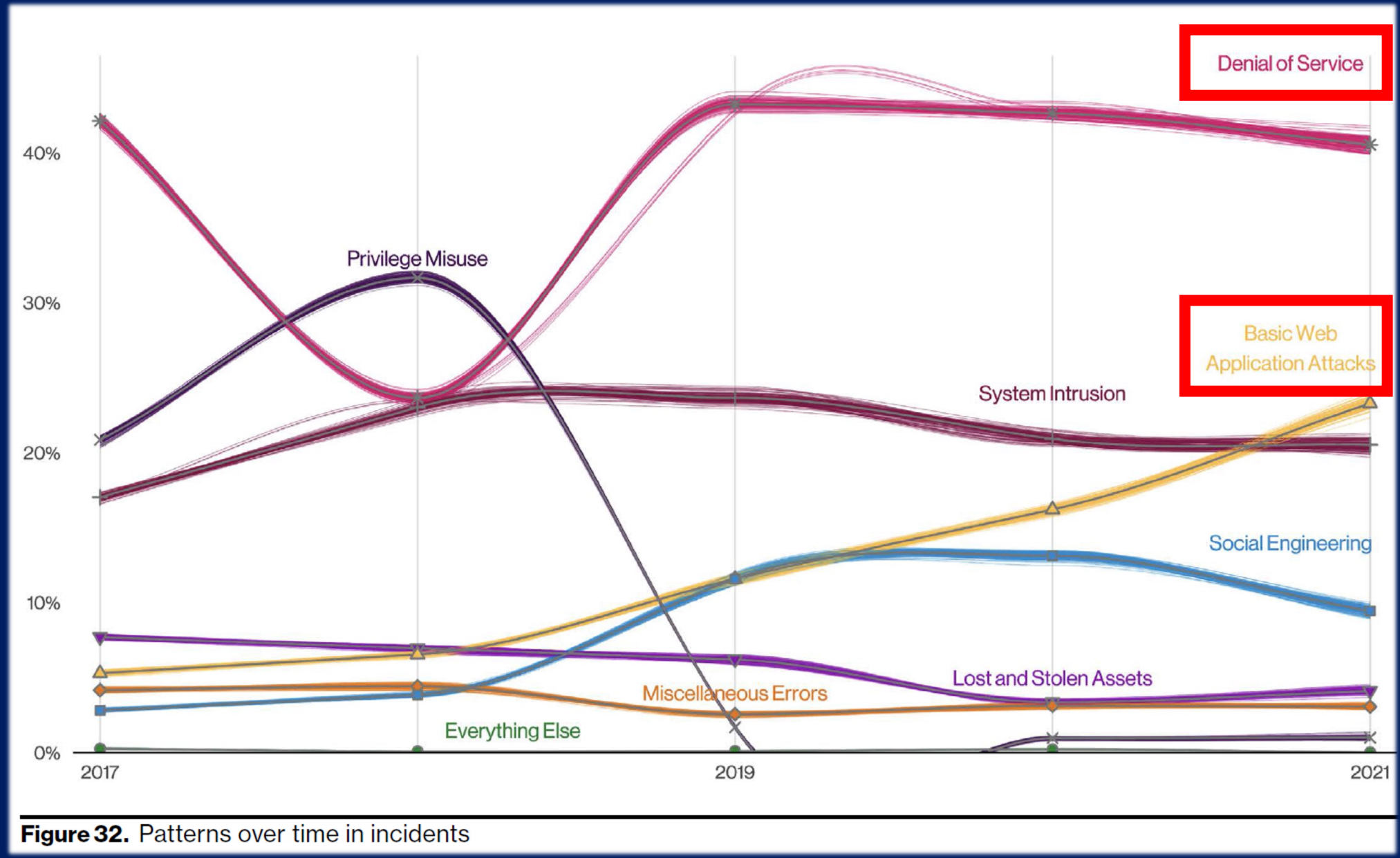


Figure 32. Patterns over time in incidents


The Scale of Cyber Operations is Immense

In a Week

Microsoft Will Block 13,685 Attacks

Leaseweb Will Block 2,087 Attacks

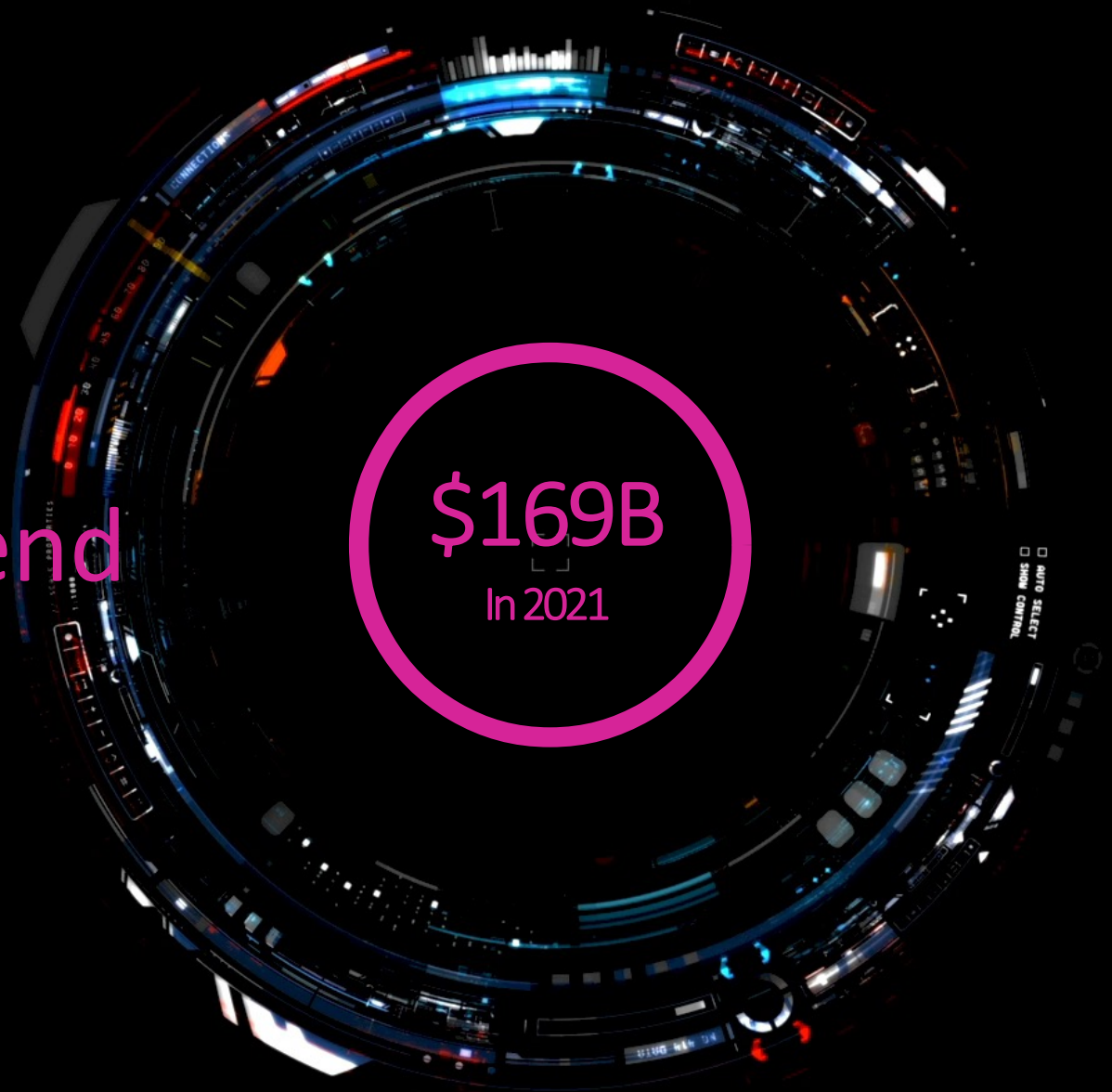
AWS Will Push Code 7 Million Times

Twitter Will Serve 3.5 Billion Tweets

Security Spend

Source: Statista, 2023

Security Spend

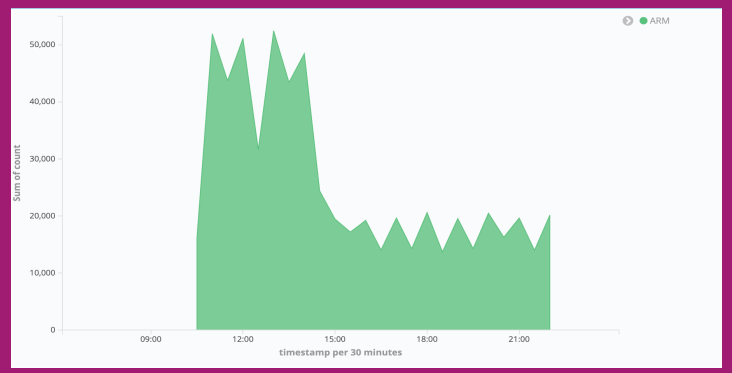


Source: Statista, 2023

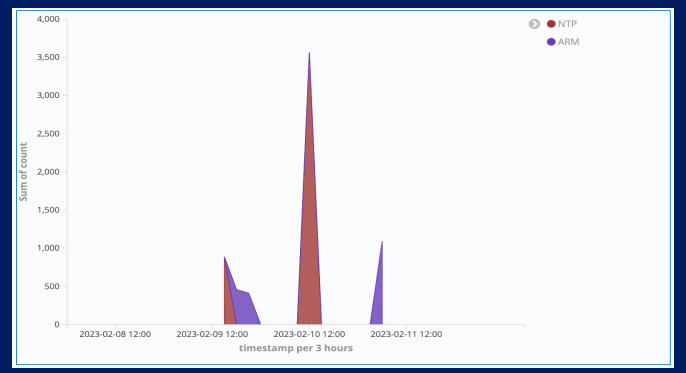
A10 Threat Research

Real World Events: DDoS Attacks in Every Vertical

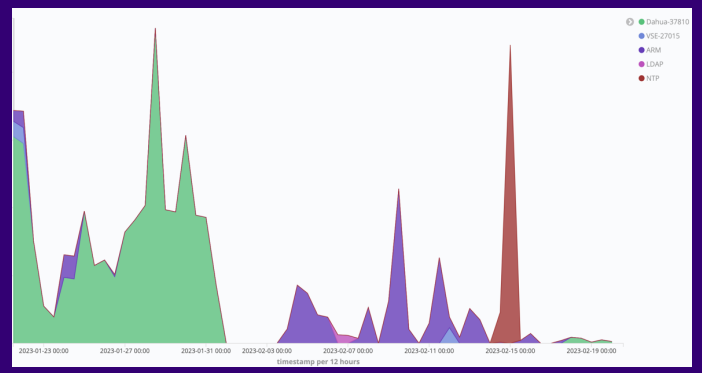
Coordinated Attacks: NATO



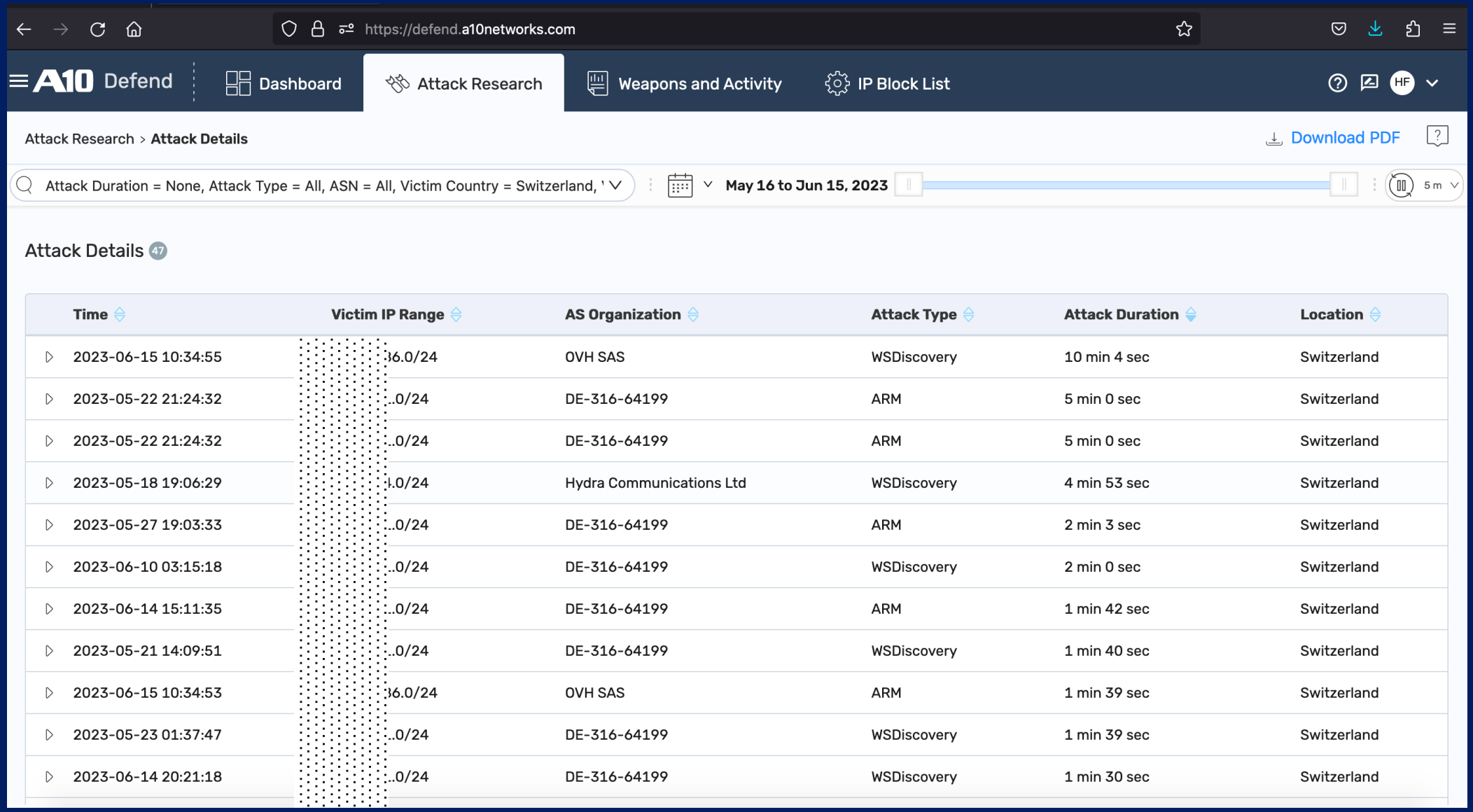
Large Enterprise Attack: BMW



Continuous Gaming Attack: Roblox



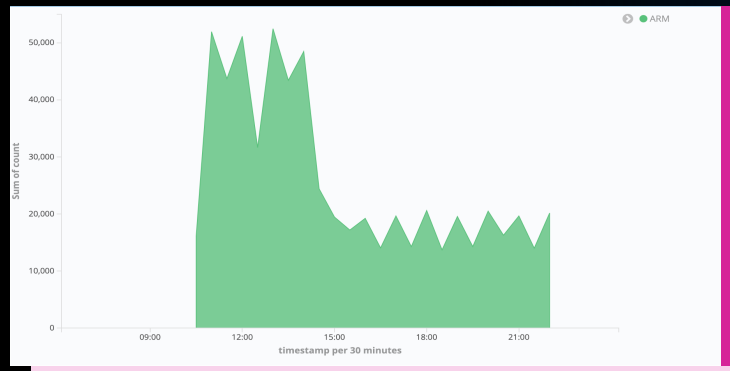
Real World Events: DDoS Attacks in CH



Time	Victim IP Range	AS Organization	Attack Type	Attack Duration	Location
2023-06-15 10:34:55	[redacted]6.0/24	OVH SAS	WSDiscovery	10 min 4 sec	Switzerland
2023-05-22 21:24:32	[redacted]..0/24	DE-316-64199	ARM	5 min 0 sec	Switzerland
2023-05-22 21:24:32	[redacted]..0/24	DE-316-64199	ARM	5 min 0 sec	Switzerland
2023-05-18 19:06:29	[redacted]1.0/24	Hydra Communications Ltd	WSDiscovery	4 min 53 sec	Switzerland
2023-05-27 19:03:33	[redacted]..0/24	DE-316-64199	ARM	2 min 3 sec	Switzerland
2023-06-10 03:15:18	[redacted]..0/24	DE-316-64199	WSDiscovery	2 min 0 sec	Switzerland
2023-06-14 15:11:35	[redacted]..0/24	DE-316-64199	ARM	1 min 42 sec	Switzerland
2023-05-21 14:09:51	[redacted]..0/24	DE-316-64199	WSDiscovery	1 min 40 sec	Switzerland
2023-06-15 10:34:53	[redacted]6.0/24	OVH SAS	ARM	1 min 39 sec	Switzerland
2023-05-23 01:37:47	[redacted]..0/24	DE-316-64199	WSDiscovery	1 min 39 sec	Switzerland
2023-06-14 20:21:18	[redacted]..0/24	DE-316-64199	WSDiscovery	1 min 30 sec	Switzerland

Observed Attacks

BY A10 NETWORKS



February 13th, 13:00 GMT to 22:30 GMT Reported February 17th

CYBER SECURITY HUB INCIDENT OF THE WEEK

IOTW: Russian hackers target NATO sites with DDoS attack

A Russian hacktivist group launched a series of DDoS attacks against NATO affecting the response of search and rescue teams in Turkey and Syria

Add bookmark

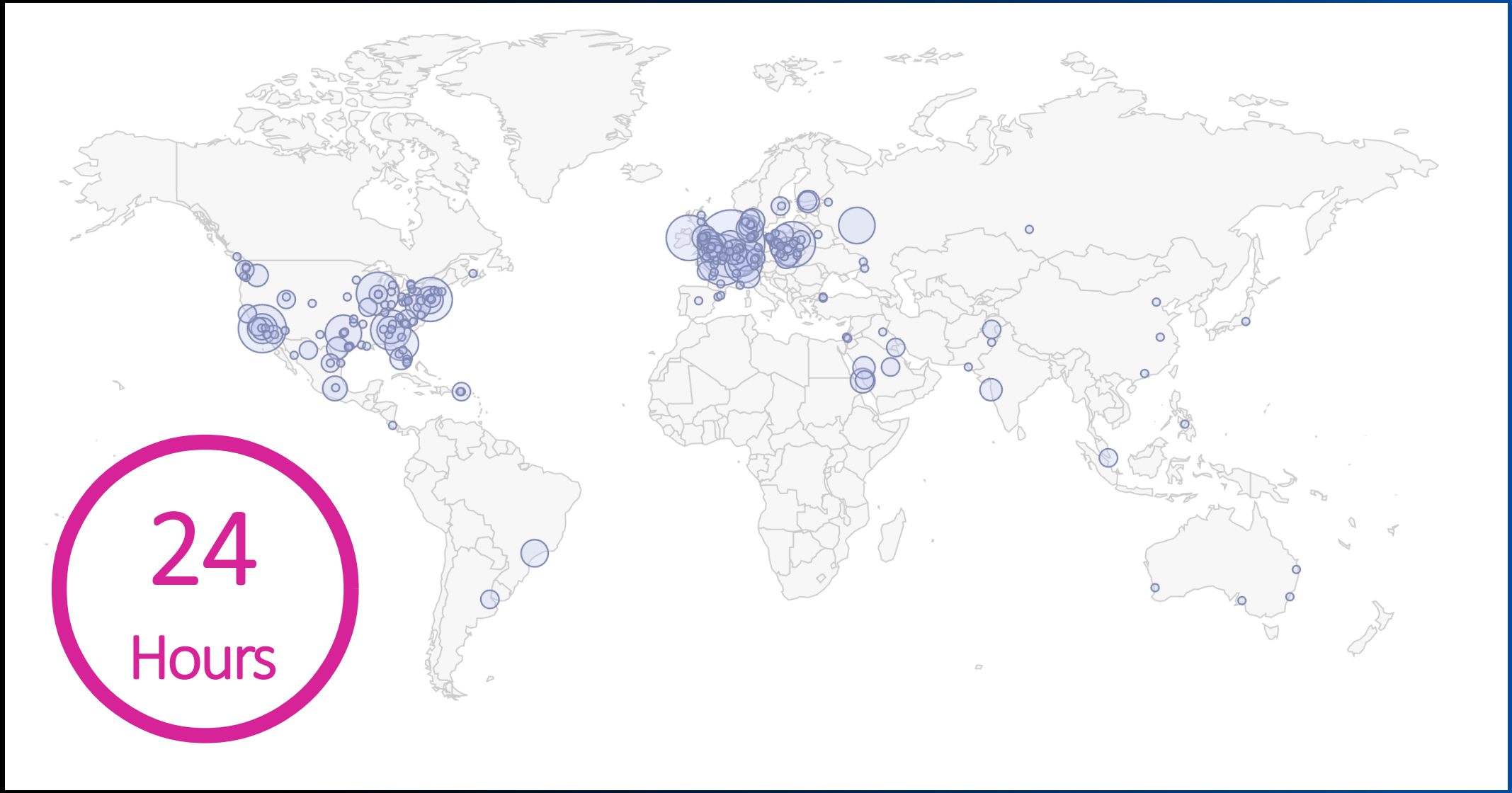
Tags: Hacktivist Hacktivism Hacker Cyber Attack Russia Turkey Syria Iran NATO DDoS Attack Distributed Denial Of Service Attack Killnet

Olivia Powell
02/17/2023

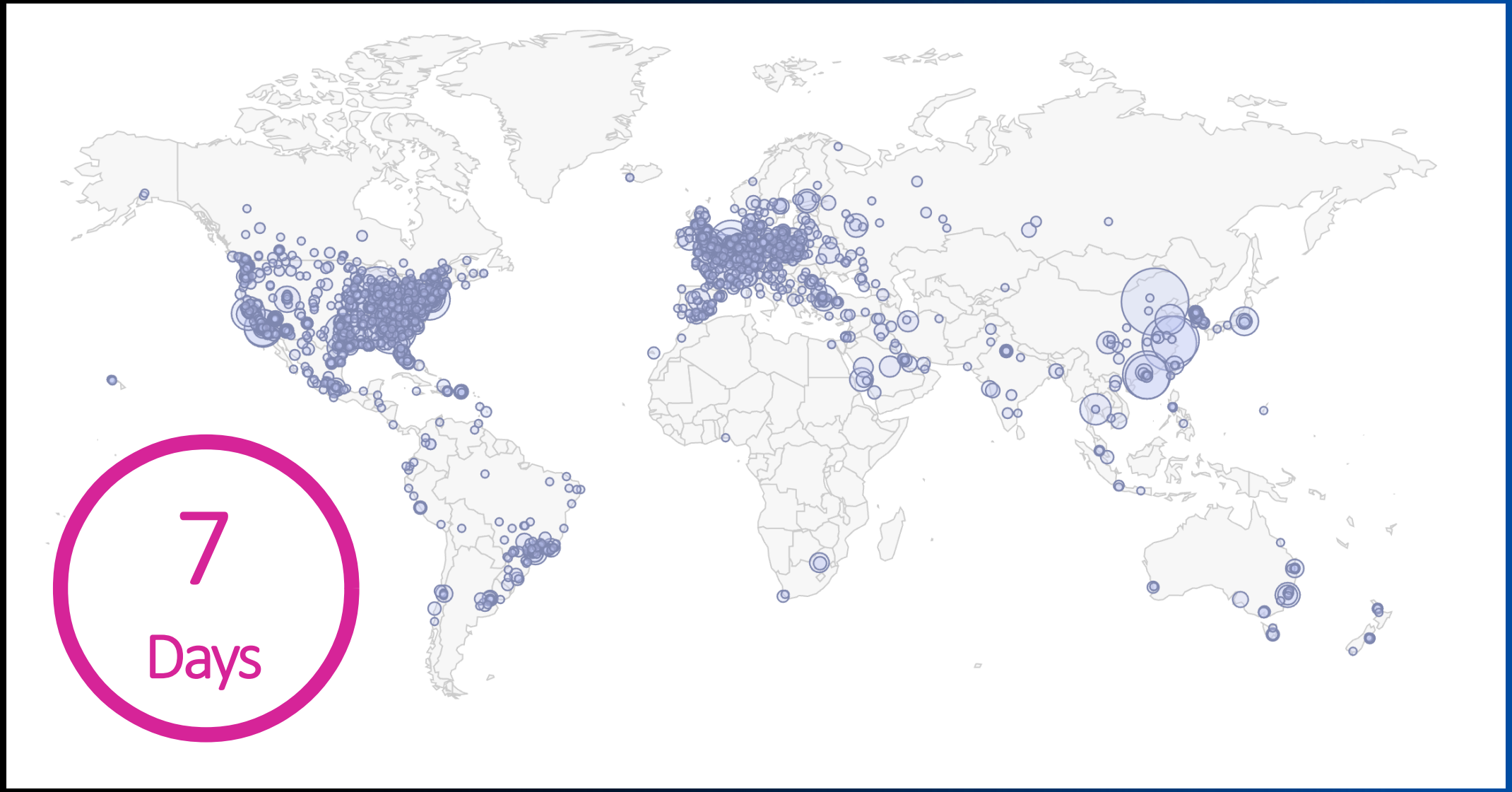
The North Atlantic Treaty Organization (NATO) has been the victim of a series of **distributed denial of service (DDoS) attacks**, causing temporary disruption to some of its sites.

The DDoS attacks have been linked to the Russian **hacktivist** collective Killnet which had posted via an encrypted channel on social media platform Telegram that it was planning to launch attacks against NATO. The group also appeared to be asking for cryptocurrency donations to launch further attacks.

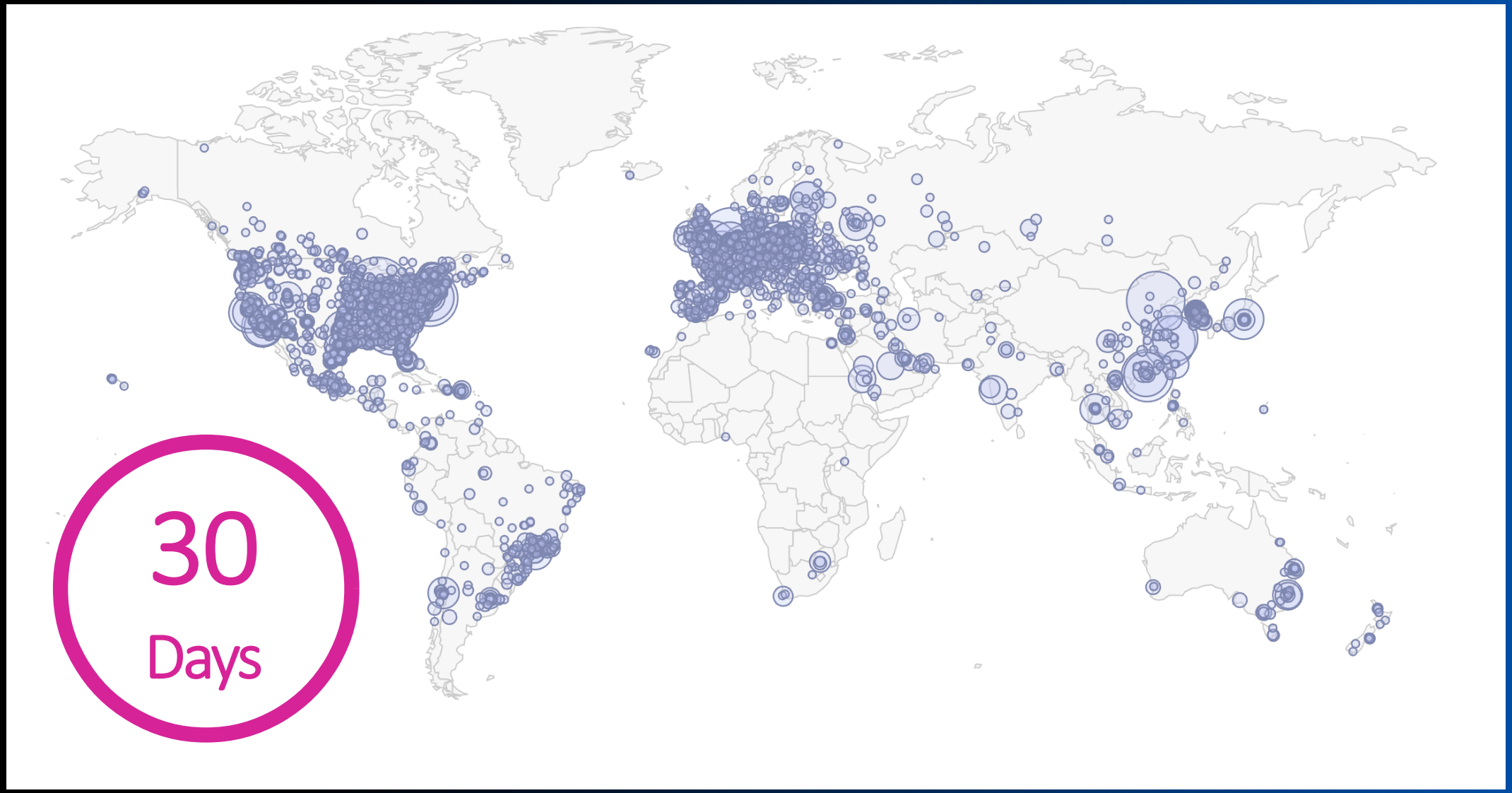
Observed Attacks



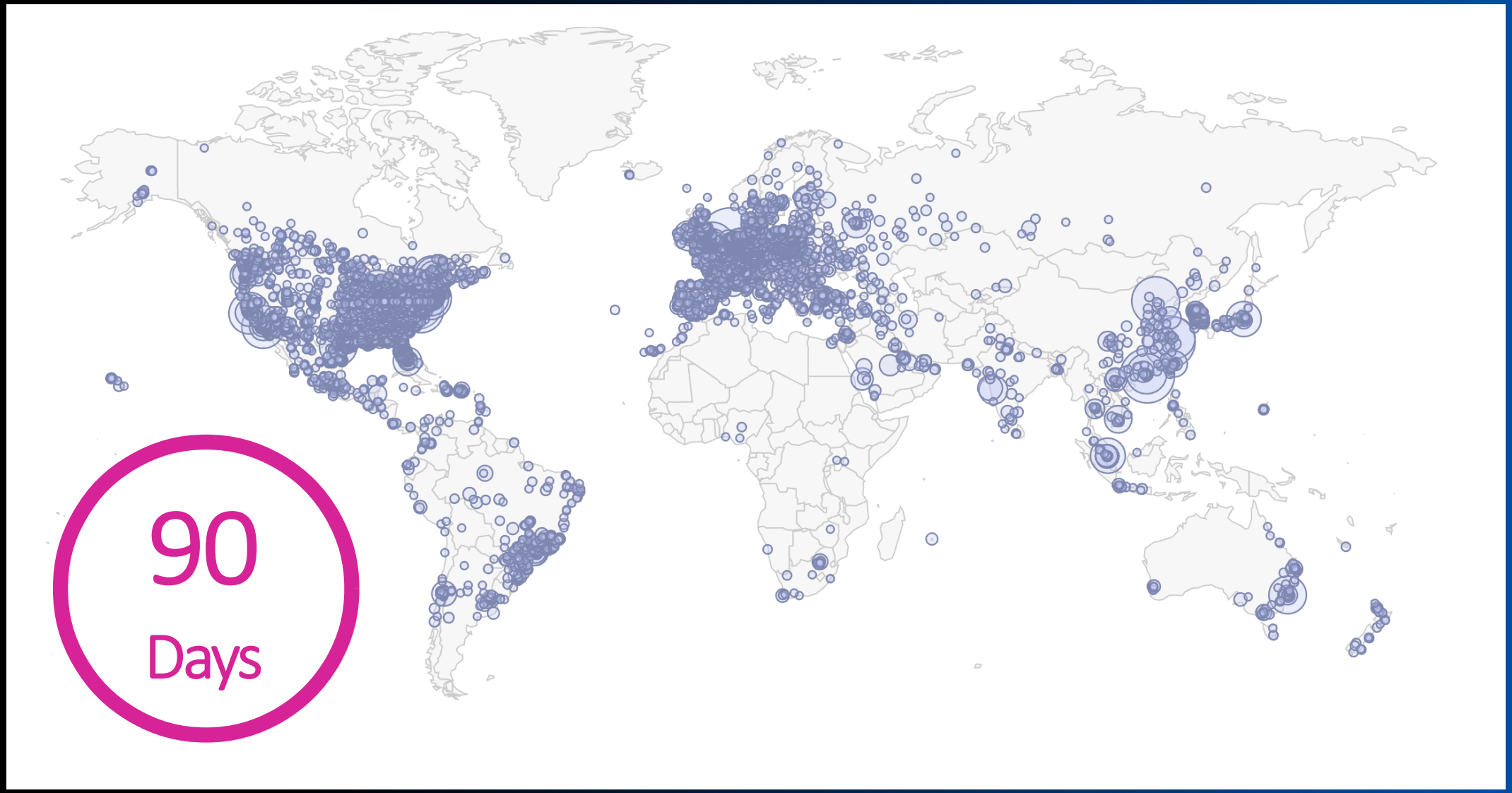
Observed Attacks



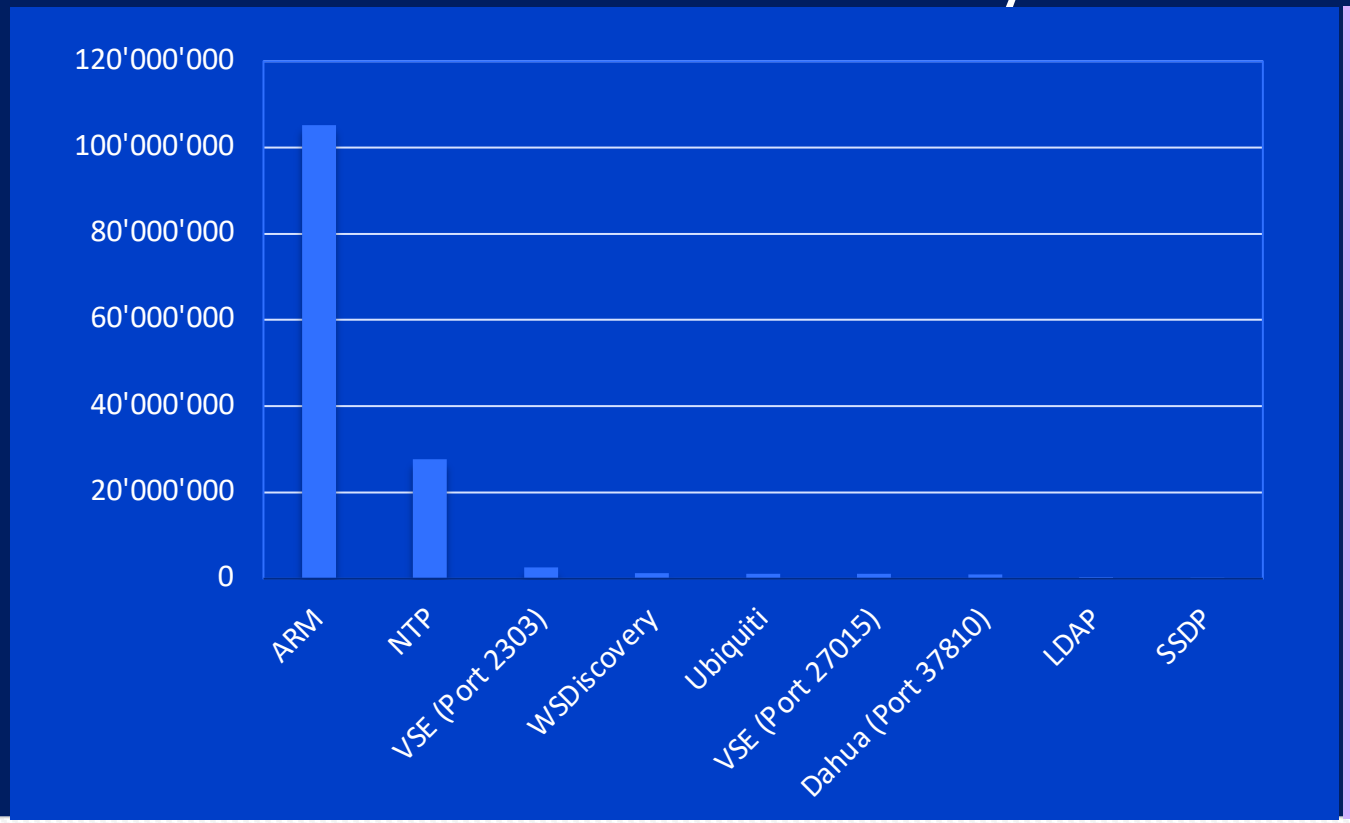
Observed Attacks

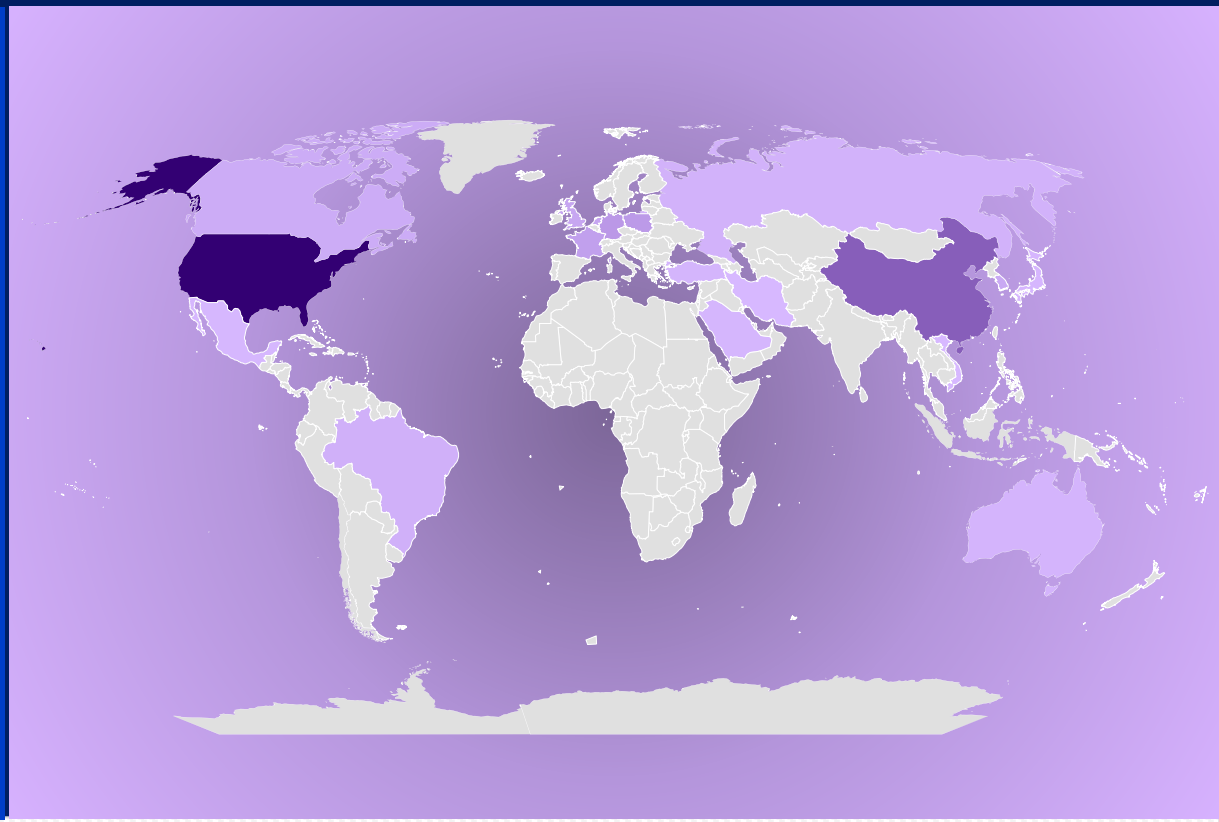


Observed Attacks



30 Days of DDoS Attacks





DDoS Attack Weapons Update

Total Weapons

- 15 million combined reflectors and bots
- SSDP is the largest by number of hosts at nearly 3 million
- SNMPv2 systems come in at 1.7 million
- China has the largest number of weapons with 1.7 million
- USA coming in at nearly 1.6 million
- Both Korea Telecom and Chinanet top the largest networks with approximately 800k per

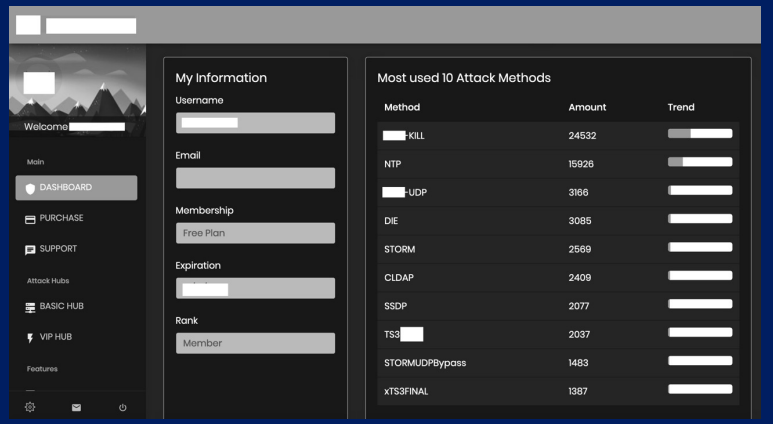
Total Bot Activity Over 400 Thousand Hosts

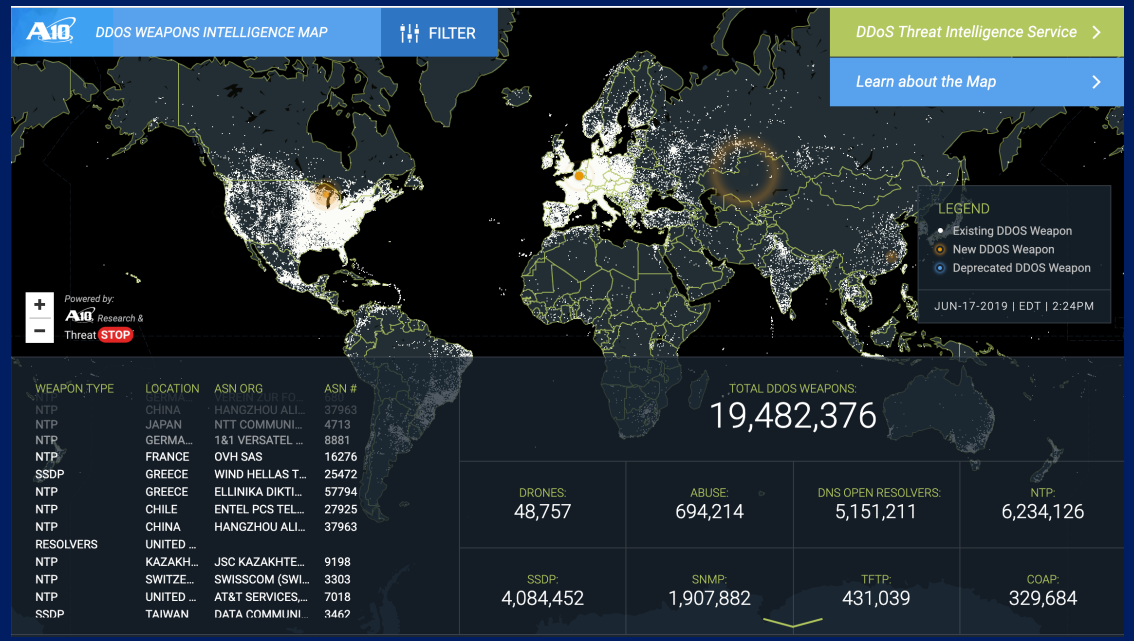
- China and India are the top-two sources of bot activity
- Chinanet and BSNL in India are the largest networks
- Most bots are infecting others using open telnet ports and default credentials
- Most frequently attempted CVE for infection is CVE-2017-17215 for Huawei HG532

Be Aware of Your Opponents' Weapons

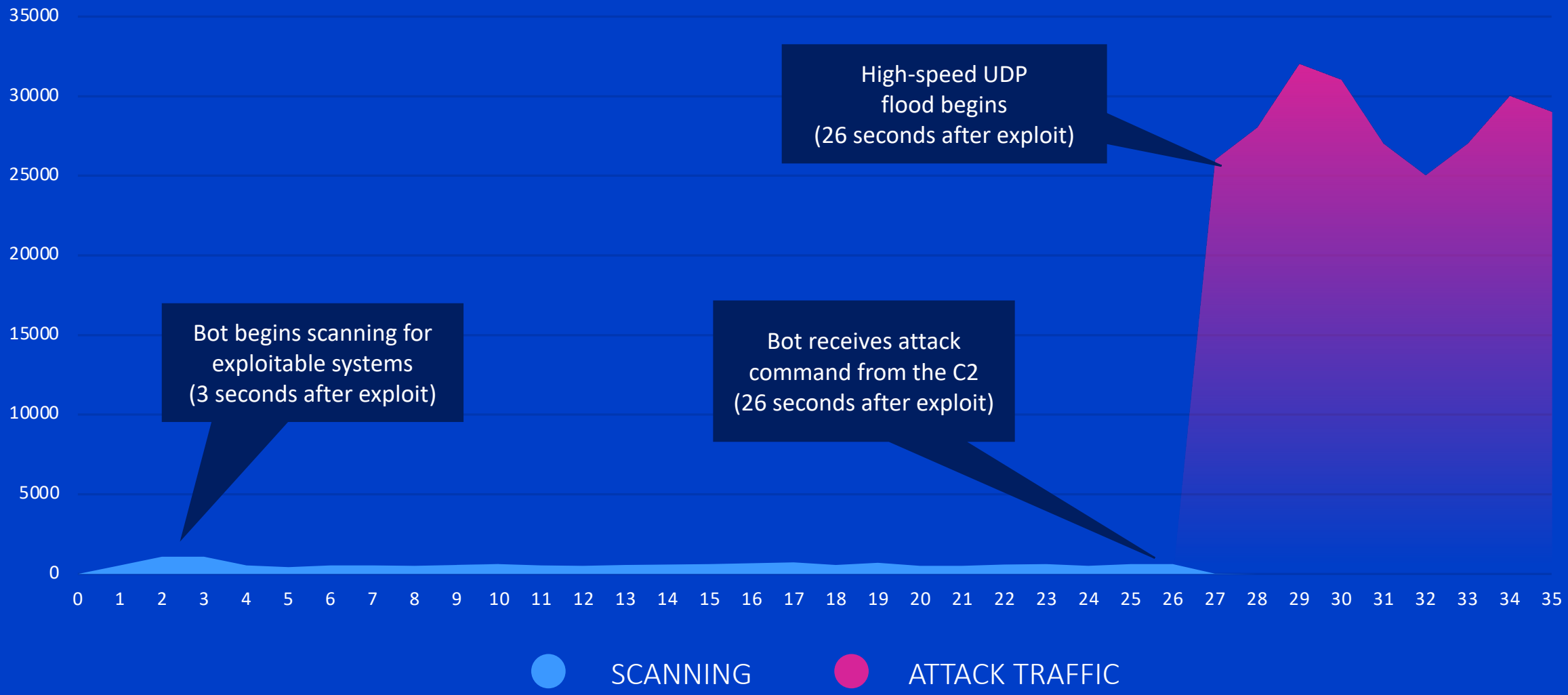
- Knowing where your opponents' weapons are is important in any combat
- DDoS protection is no different

New photographic evidence has emerged of "significant" Chinese military defences on artificial islands in the South China Sea, a think tank reports.

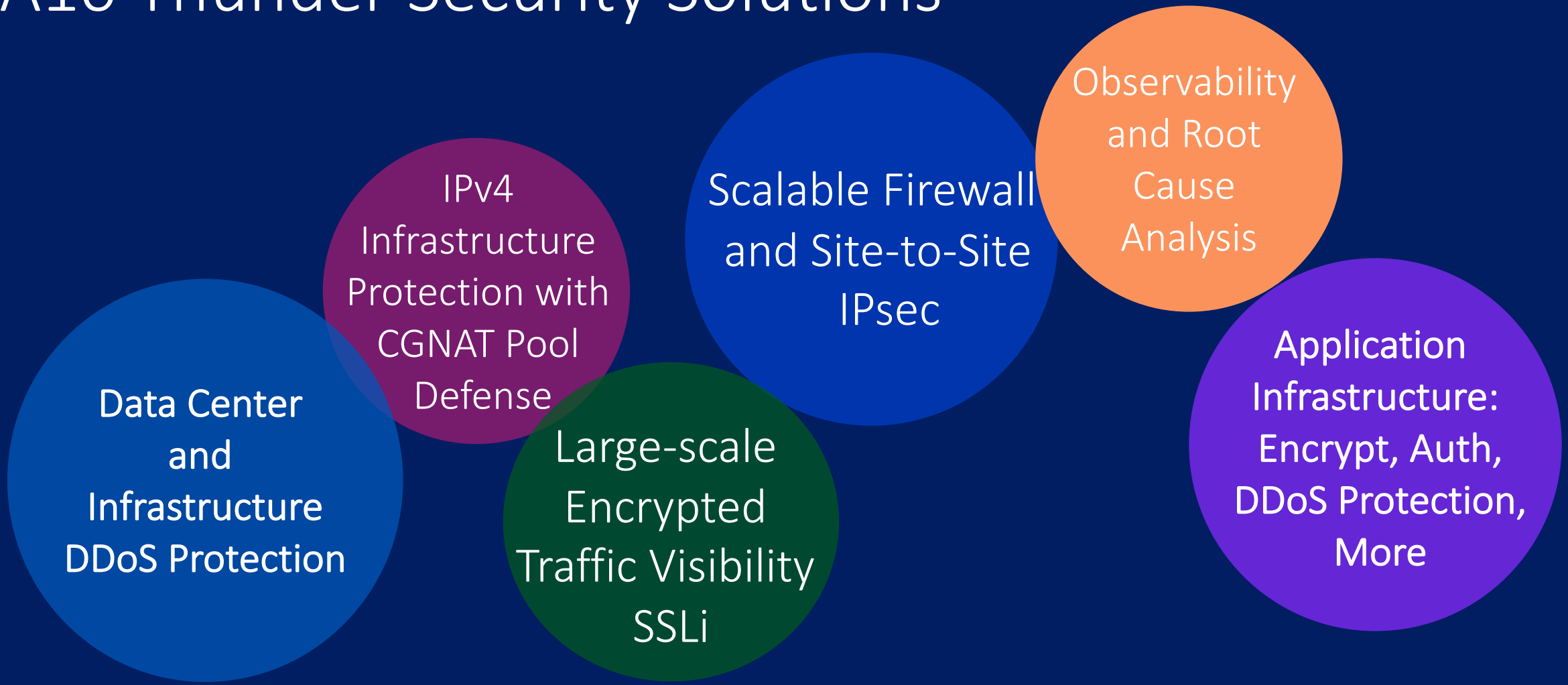




Bot Behavior Explained



A10 Thunder Security Solutions



A10

Always Secure. Always Available.

Thank You