CORE

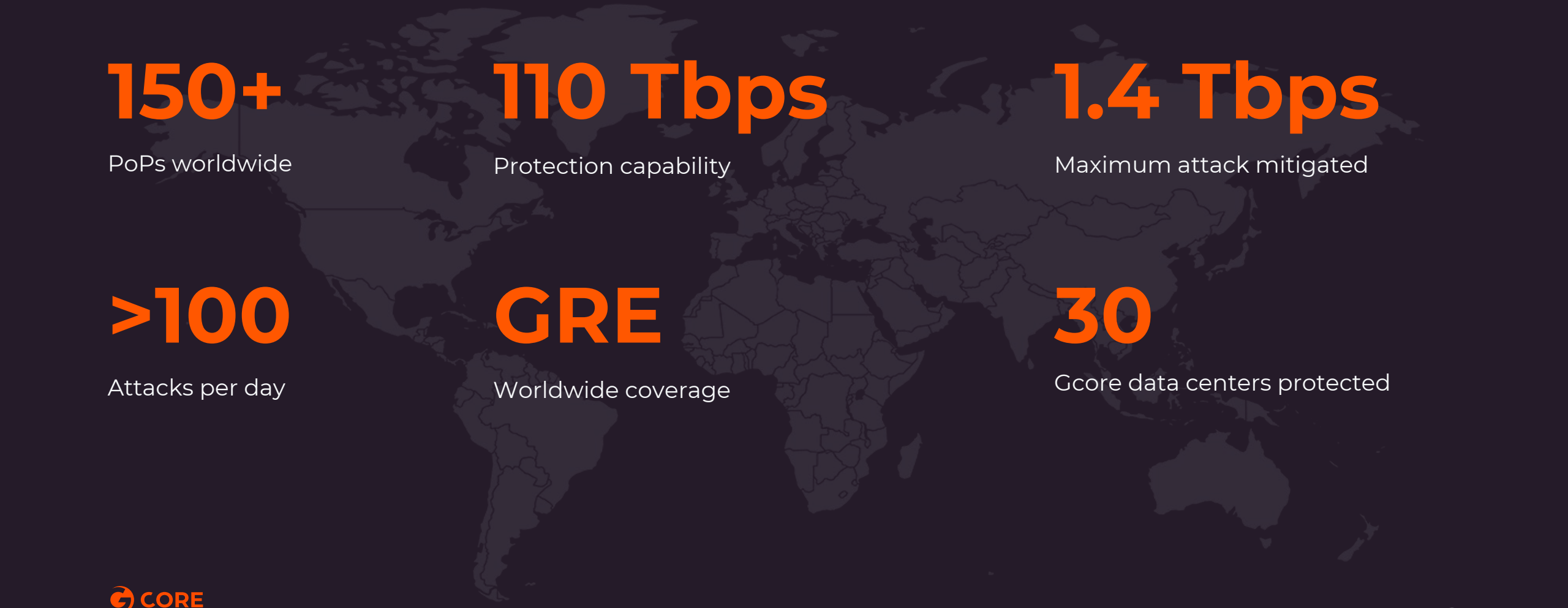
The Role of IoT and 5G Devices in DDoS Attacks: A Growing Threat Landscape

PCI DSS COMPLIANT

MADE IN LUXEMBOURG

GUINNESS WORLD RECORDS

DDoS Protection Solution



150+

PoPs worldwide

110 Tbps

Protection capability

1.4 Tbps

Maximum attack mitigated

>100

Attacks per day

GRE

Worldwide coverage

30

Gcore data centers protected

DDoS attack trends

DDoS Attacks

- Overwhelm servers and infrastructure with massive traffic
- Impact: Loss of revenue, reputation and customers

Surge in 5G and IoT Devices

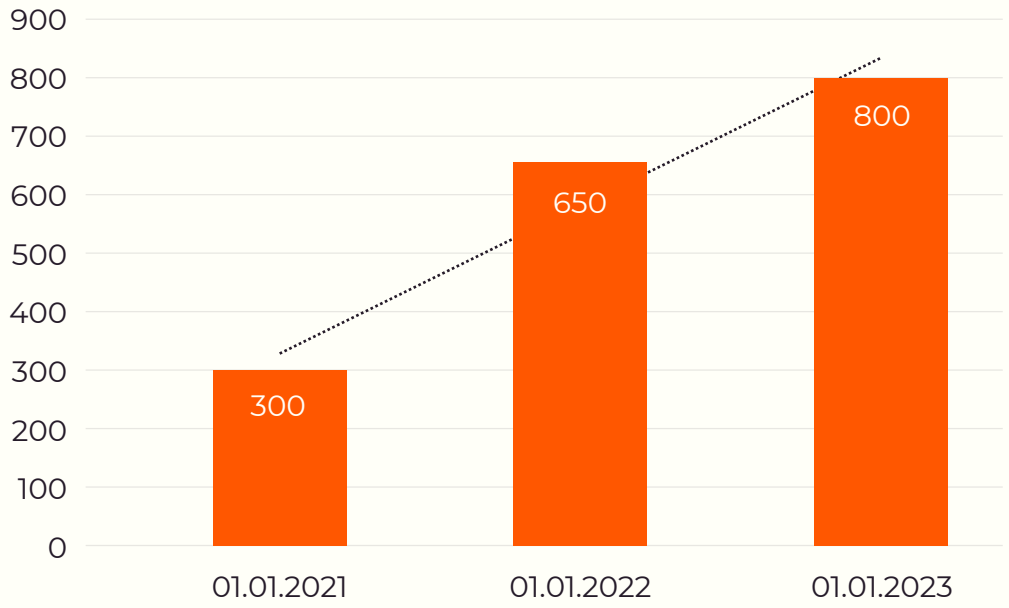
- Increases the arsenal for cybercriminals
- Expands attack capabilities
- IoT devices in botnets: From 200,000 to 1 million in a year
- Steep rise in botnet-driven DDoS attacks

Future Outlook

- Expect more powerful and frequent DDoS attacks
- Increasing number of vulnerable devices prone to botnet recruitment

CORE

Attack volume, GBPS



The danger of 5G and IoT

IoT Devices: Pros and Cons

- Benefits: Convenience and automation
- Risks: Low security, easily hackable

IoT as Botnet Recruits

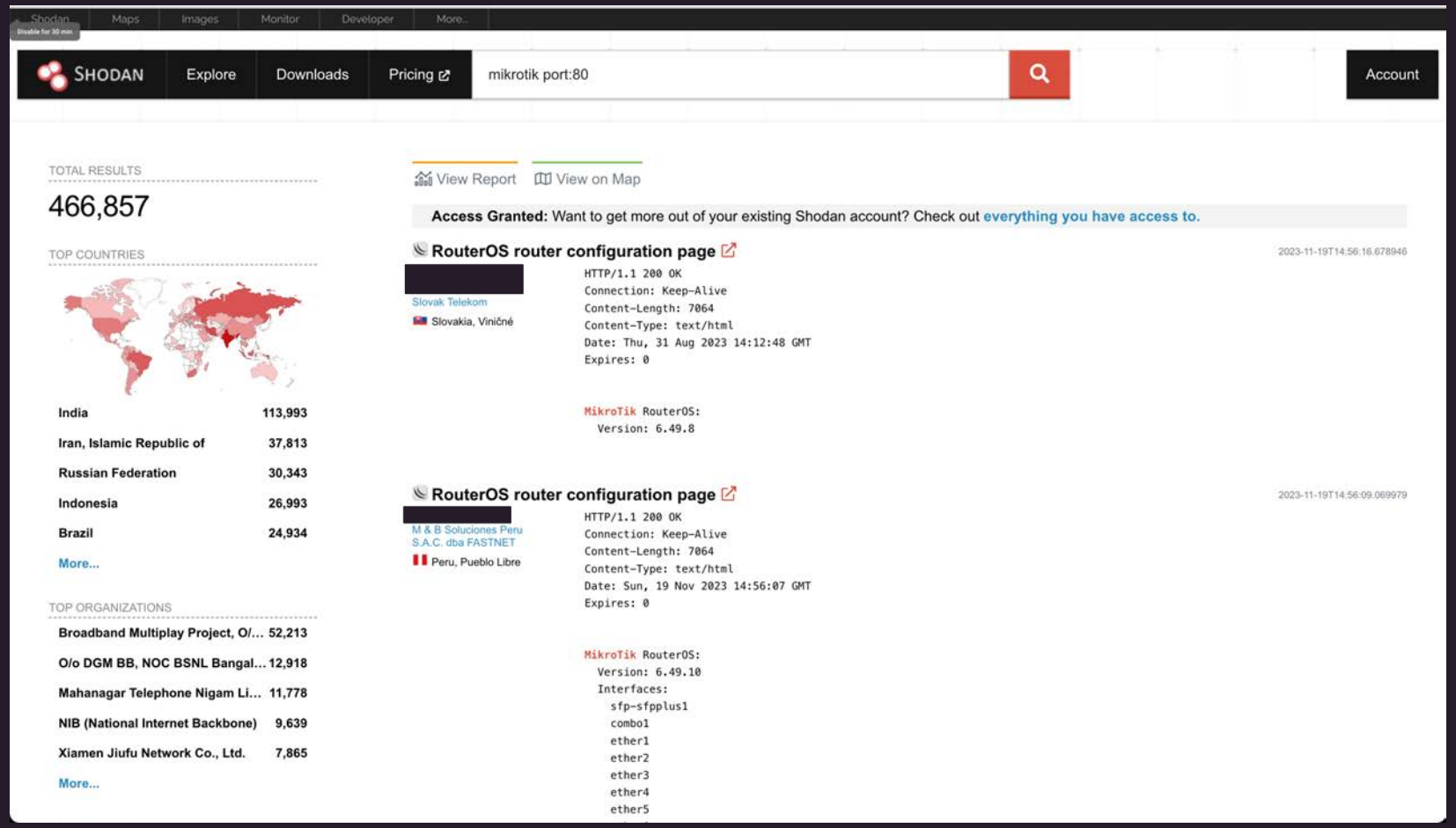
- Smart devices can be weaponized
- Strong passwords essential

5G's Cybersecurity Impact

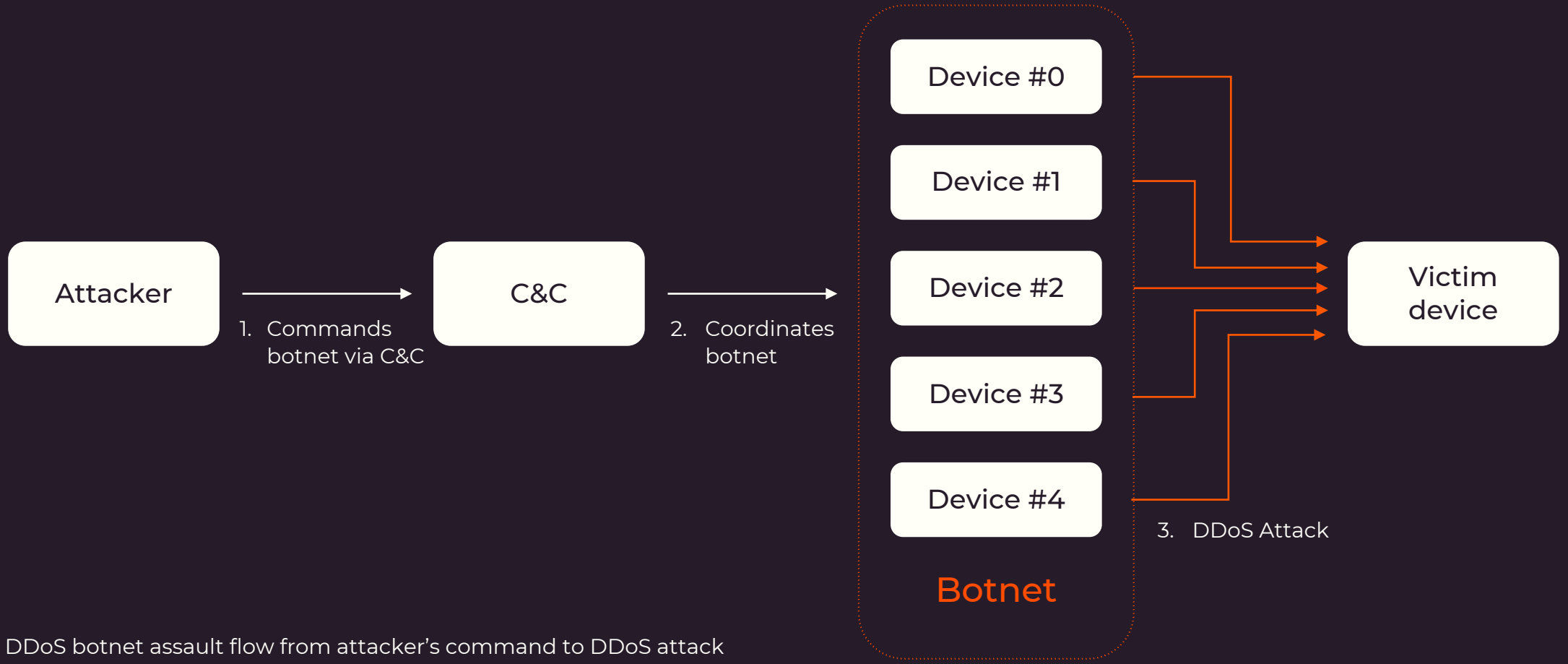
- Increases network bandwidth
- Amplifies attack potency

CORE

The danger of 5G and IoT



Anatomy of IoT-Driven botnet DDoS Attacks



DDoS botnet assault flow from attacker's command to DDoS attack

CORE

Algorithm of IoT-Driven botnet DDoS Attacks

1. The attacker targets the botnet to a victim

The botnet operator identifies the target—usually a device, website, or online service—that they want to take down.

2. The C&C server orchestrates the DDoS attack

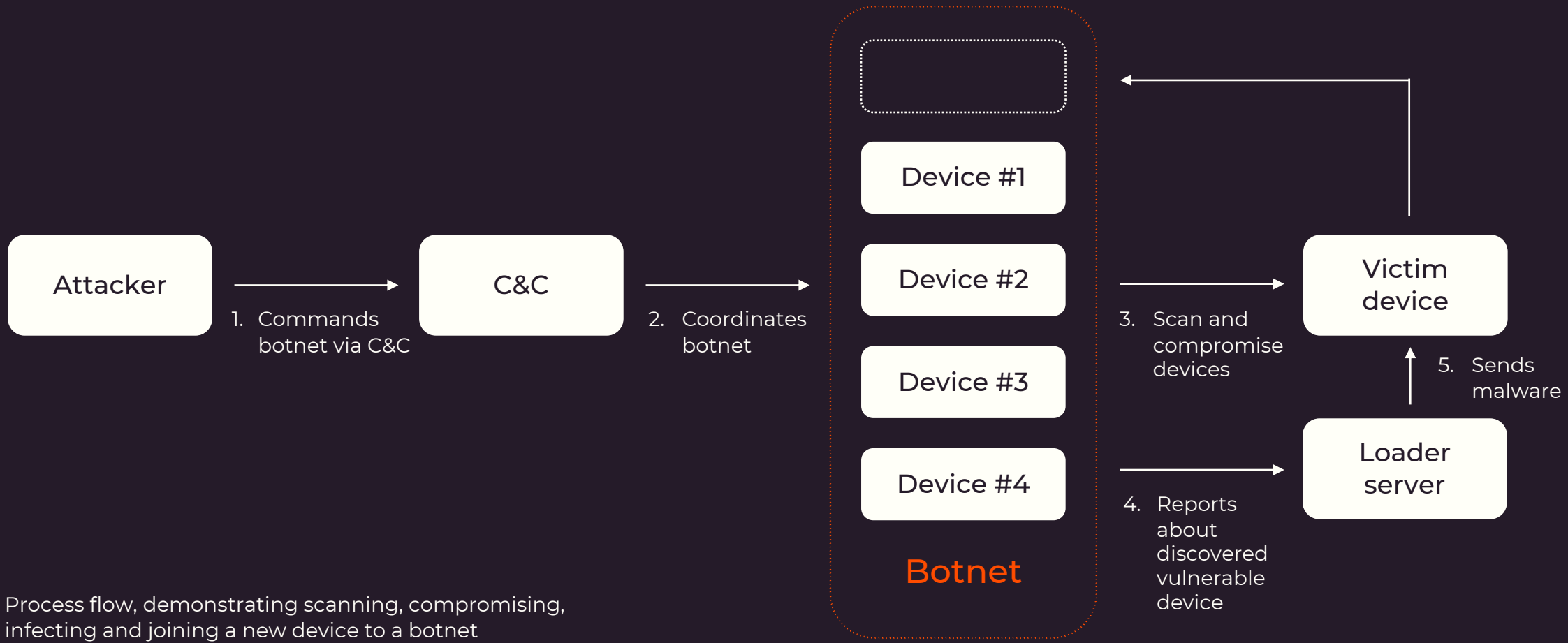
The C&C server sends the attacker's instructions to all the bots in the network to start sending requests to the target. It also coordinates the botnet's behavior.

3. A flood of traffic occurs

All the bots in the network start sending a large number of requests to the target website or server.

CORE

Stages of infecting IoT devices



Process flow, demonstrating scanning, compromising, infecting and joining a new device to a botnet

Stages of infecting IoT devices

Here are the stages of infecting IoT devices and connecting them to a botnet based the Mirai case:

1. Initial command: The attacker uses the C&C server to send a command to the botnet for attacking and incorporating new devices.

2. Orchestration: The C&C server coordinates the botnet's actions.

3. Scanning and compromise: The botnet scans and compromises victim devices to gain privileged access by brute-forcing weak passwords or exploiting outdated firmware or insecure configurations.

4. Data reporting: The botnet relays the victim's IP address and access credentials to the loader server once the device is hacked.

5. Malware delivery and infection: The loader server sends malware or malicious instructions, which are then executed by a compromised device, turning it into a bot.

6. Joining the botnet: The newly infected device becomes part of the botnet and awaits further commands, often operating undetected.

IoT Attacks on the Rise

IoT-driven DDoS attacks increased by

300%

in the first half of 2023, causing $2.5 billion financial loss.

90%

of complex, multi-vector DDoS attacks are based on botnets.

Number of IoT devices engaged in botnet-driven DDoS attacks rose from 200,000 a year ago to

1M

devices.

Threats of losses when DDoS attacks happen

DDoS attacks can harm any company, from small businesses to global giants. Without protection, anyone may experience the disastrous consequences of an attack, including:

Loss of profit

It is easy to calculate the losses from a DDoS attack: they total your income per hour. Imagine that your online store earns $50,000 per hour. That means that every hour of inaccessibility owing to DDoS attack will cost you $50,000.

Loss of clients

In competitive industries, your customers might go to your competitors who have taken care to protect their business from cybercriminals.

Loss due to compensation

For example, if your project is a SaaS, be prepared to compensate your customers if your service is unavailable.

Loss of customers' data

Often, a DDoS attack is one part of a larger attack designed to steal users' personal data.

Theft of intellectual property

For example, if a server is attacked, all information about an upcoming release could be published too early.

Destruction of valuable resources

Hackers might attack the server and disrupt the infrastructure.

Negative impact on the brand

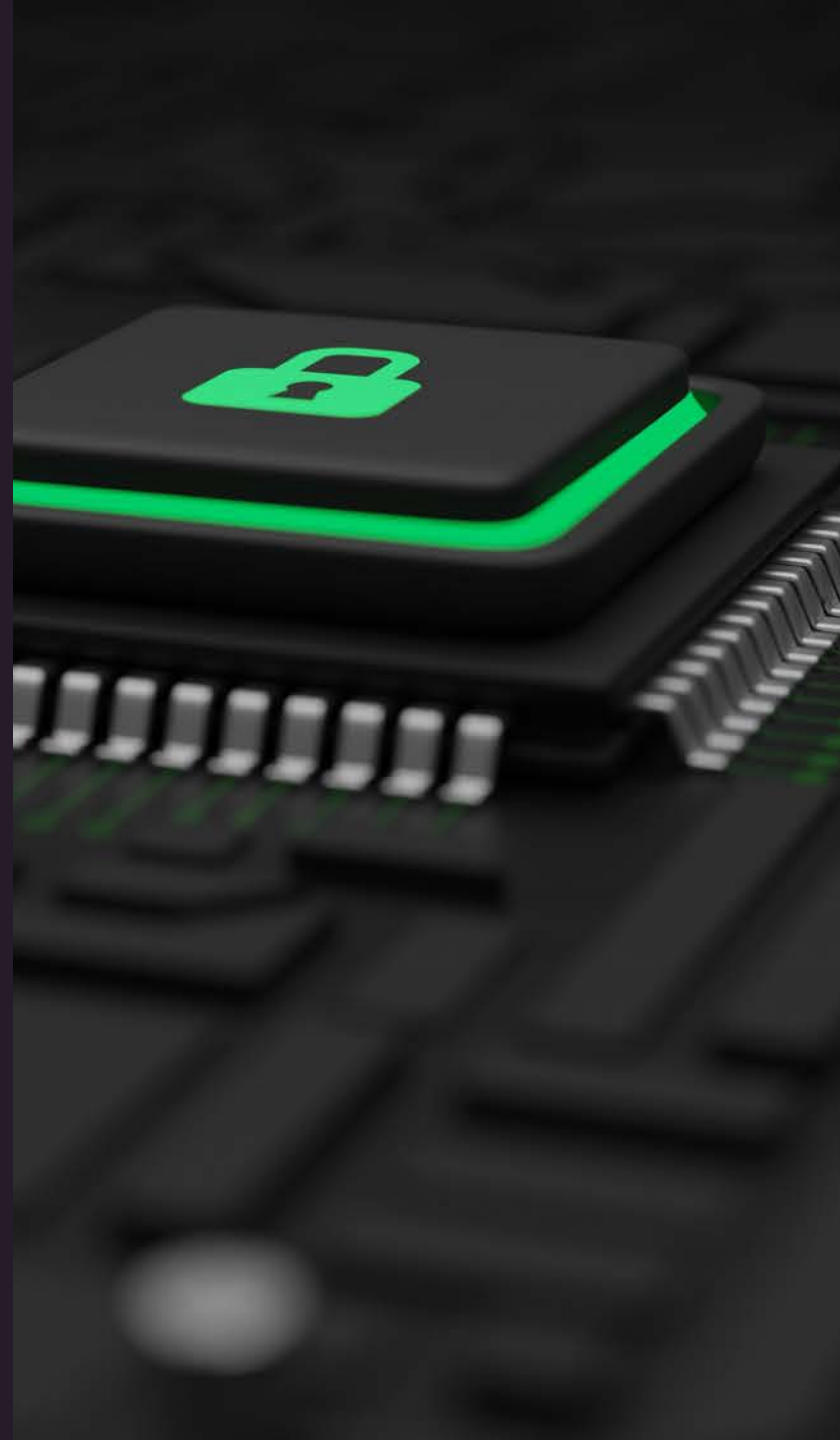
Customer dissatisfaction in our digital world spreads in minutes and impacts negatively on company's reputation.

Loss of loyalty

The internet has empowered users to leave negative reviews on the web, and those reviews will take away potential new customers.

Protection Measures: Best Practices

1. **Protect your IoT from being infected:**
   - Change default passwords
   - Regularly update firmware
   - Implement strong authentication
   - Consider IoT security frameworks
2. **Protect against IoT-driven botnets with specialized DDoS Protection solutions**



CORE

Example of IoT Botnet Attack from GCORE

Client DDoS Attack: Case Study

- Highly Distributed: Involved numerous devices
- Attack Method: "Carpet Bombing" with UDP traffic

Challenges

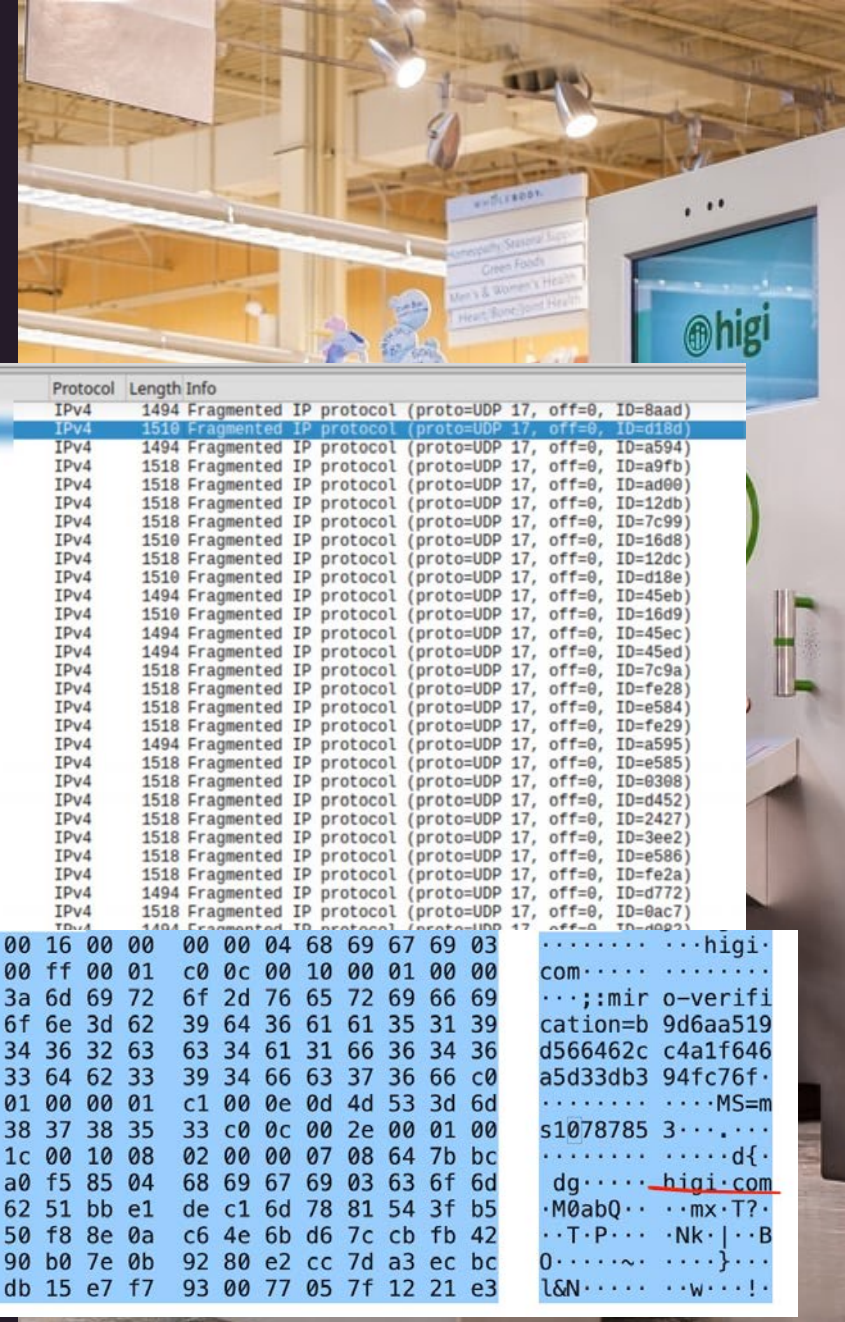
- Multiple client addresses targeted
- Uplinks overloaded due to cumulative traffic

Our Response

- Quick defense system activation
- Identified common attack pattern
- Successfully blocked the attack

Post-Investigation Findings

- Attacker: Botnet exploiting health check kiosks
- Constructed botnet network based on these kiosks



Destination	Protocol	Length	Info
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=8aad)
	IPv4	1510	Fragmented IP protocol (proto=UDP 17, off=0, ID=d18d)
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=a594)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=a9fb)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=ad00)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=12db)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=7c99)
	IPv4	1510	Fragmented IP protocol (proto=UDP 17, off=0, ID=16d8)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=12dc)
	IPv4	1510	Fragmented IP protocol (proto=UDP 17, off=0, ID=d18e)
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=45eb)
	IPv4	1510	Fragmented IP protocol (proto=UDP 17, off=0, ID=16d9)
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=45ec)
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=45ed)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=7c9a)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=fe28)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=e584)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=fe29)
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=a595)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=e585)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0308)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=d452)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=2427)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=3ee2)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=e586)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=fe2a)
	IPv4	1494	Fragmented IP protocol (proto=UDP 17, off=0, ID=d772)
	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=0ac7)

```
0030  83 80 00 01 00 16 00 00  00 00 04 68 69 67 69 03   ........ ...higi.
0040  63 6f 6d 00 00 ff 00 01  c0 0c 00 10 00 01 00 00   com..... ........
0050  01 c1 00 3b 3a 6d 69 72  6f 2d 76 65 72 69 66 69   ...;:mir o-verifi
0060  63 61 74 69 6f 6e 3d 62  39 64 36 61 61 35 31 39   cation=b 9d6aa519
0070  64 35 36 36 34 36 32 63  63 34 61 31 66 36 34 36   d566462c c4a1f646
0080  61 35 64 33 33 64 62 33  39 34 66 63 37 36 66 c0   a5d33db3 94fc76f.
0090  0c 00 10 00 01 00 00 01  c1 00 0e 0d 4d 53 3d 6d   ........ ....MS=m
00a0  73 31 30 37 38 37 38 35  33 c0 0c 00 2e 00 01 00   s1078785 3...,...
00b0  00 01 c1 01 1c 00 10 08  02 00 00 07 08 64 7b bc   ........ .....d{.
00c0  20 64 67 f5 a0 f5 85 04  68 69 67 69 03 63 6f 6d    dg..... higi.com
00d0  00 4d 30 61 62 51 bb e1  de c1 6d 78 81 54 3f b5   .M0abQ.. ..mx.T?.
00e0  95 c9 54 8f 50 f8 8e 0a  c6 4e 6b d6 7c cb fb 42   ..T.P... .Nk.|..B
00f0  4f 96 bd d5 90 b0 7e 0b  92 80 e2 cc 7d a3 ec bc   O.....~. ....}...
0100  6c 26 4e a4 db 15 e7 f7  93 00 77 05 7f 12 21 e3   l&N..... ..w...!.
```

What help us to sustain such kind of attacks?

1

Distributed architecture integrated with CDN network

2

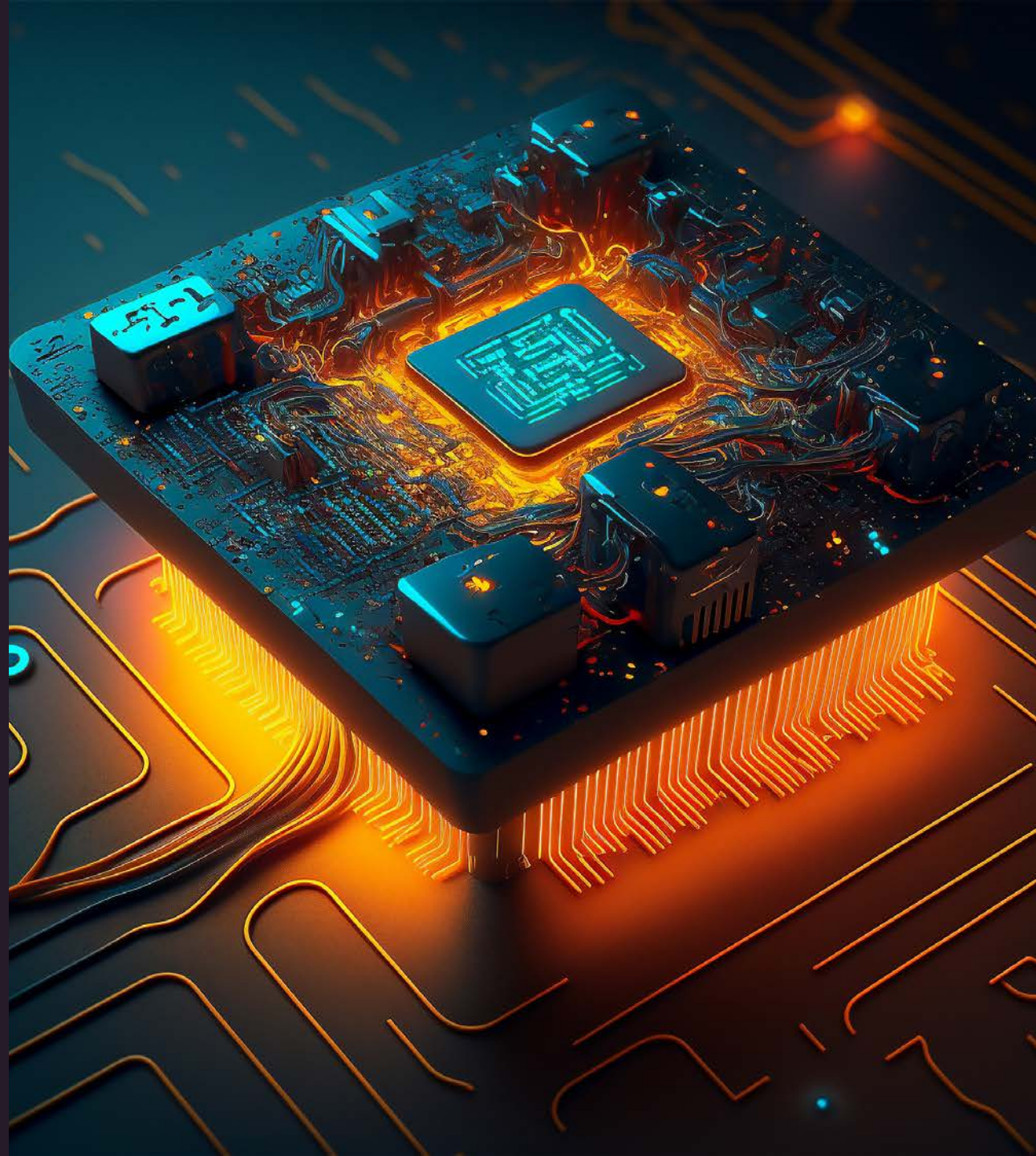
AI-driven analytic system

3

Deep packet inspection

Conclusion

- **Advancements vs. Risks**: 5G and IoT enhance connectivity but escalate cybersecurity threats, including DDoS attacks.
- **5G Impact:** Enhanced speed and connectivity of 5G increase the potential severity of cyber attacks.
- **IoT Vulnerability: IoT** devices often lack robust security, presenting easy targets for attacks.
- **Collective Effort:** Emphasizes the need for widespread awareness and standard security protocols in IoT and 5G devices.
- **Proactive Measures:** Highlights the importance of regular updates, strong authentication, and advanced cybersecurity solutions.
- **DDoS Protection Services:** Use of specialized third-party DDoS services with the capacity to handle large-scale attacks in 5G and IoT contexts.



CORE

Thank you!

Stay safe with Gcore

gcore.com