THREAT REPORT 2021 Q4

A sneak peak at the world of cyber-threats
powered by HONEYKUBE

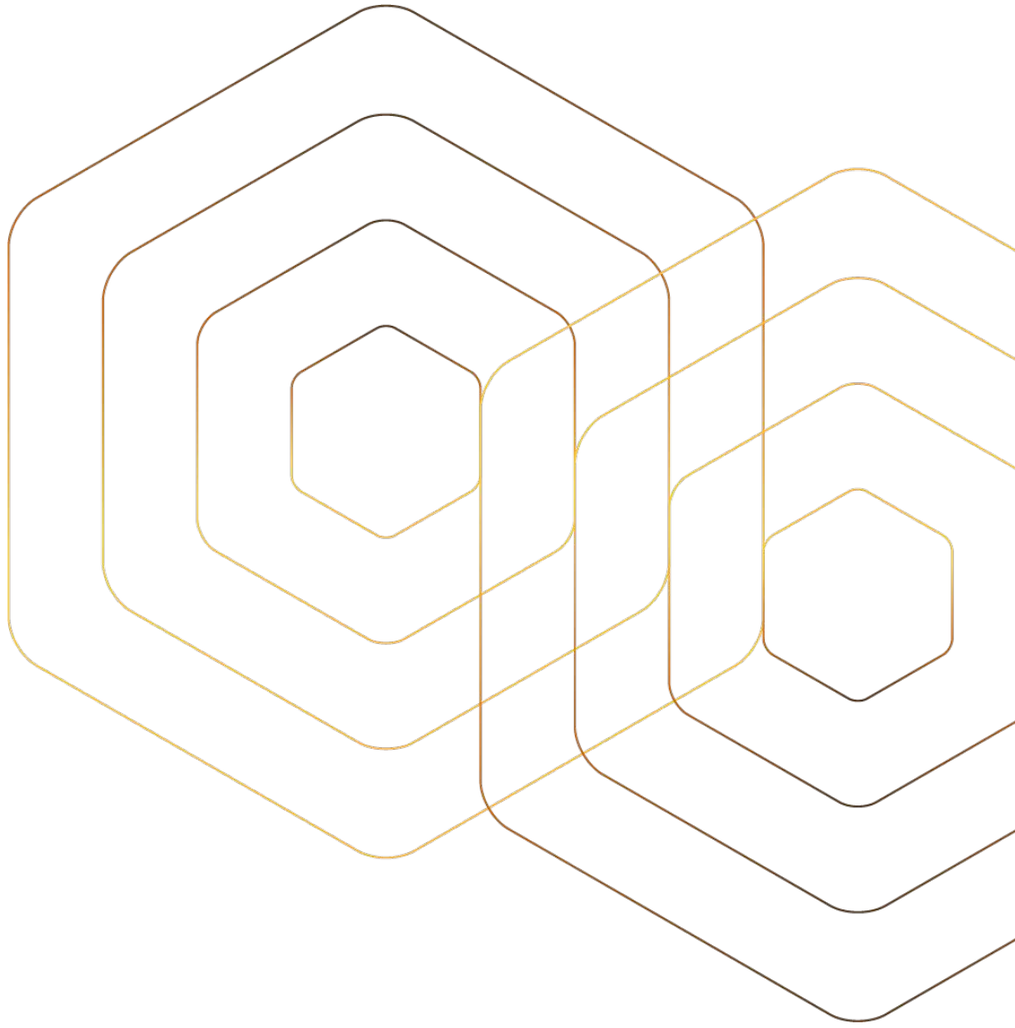
honeykube.ch

HONEYKUBE

OVERVIEW

In recent years, the quantity, diversity and complexity of malicious code has increased dramatically. This has been further fueled by the recent rise of teleworking, with attackers intensifying their focus on developing campaigns aimed at major corporate targets. There are millions of new malware samples arriving in analysis labs each day, with new tools constantly expanding the repertoire of methodologies used by attackers.

In this report, we seek to analyse the latest trends in cybersecurity attacks caught by our honeypots during the last quarter of 2021, providing a better understanding of the threat landscape that companies face every day.



HONEYKUBE

HONEYKUBE, A KUBERNETES-BASED SOLUTION TO CYBER-INTELLIGENCE

Honeykube uses **container isolation technology in Kubernetes** to create custom honeypots, which are then combined to seamlessly replicate complex infrastructures and attract a wide variety of threat actors.

ENDLESS CUSTOMISATION

As Honeykube's honeypots are highly customisable on a case-by-case basis, it is **impossible for an attacker to determine** whether they are on a real system or inside one of our honeypots.

REAL-TIME VISIBILITY

While attackers use different techniques to try to escalate permissions such as exploiting zero-days, executing malware, or making lateral moves to other services, Honeykube is able to record each of these activities as they occur.

ADVANCE DETECTION

Honeykube was designed to track, geo-locate and reveal the mechanisms used by malicious actors, enabling advanced profiling of adversaries with details on their preferred attacks, tools, tactics, techniques, and procedures.

HONEYKUBE

THE ENVIRONMENT

Honeykube has become a critical asset in the collection, distribution, and presentation of information. Combining the best features of traditional honeypots and the full potential of containers in Kubernetes, Honeykube allows the quick deployment of honeynets with different levels of interaction, capable of seamlessly representing a corporate infrastructure

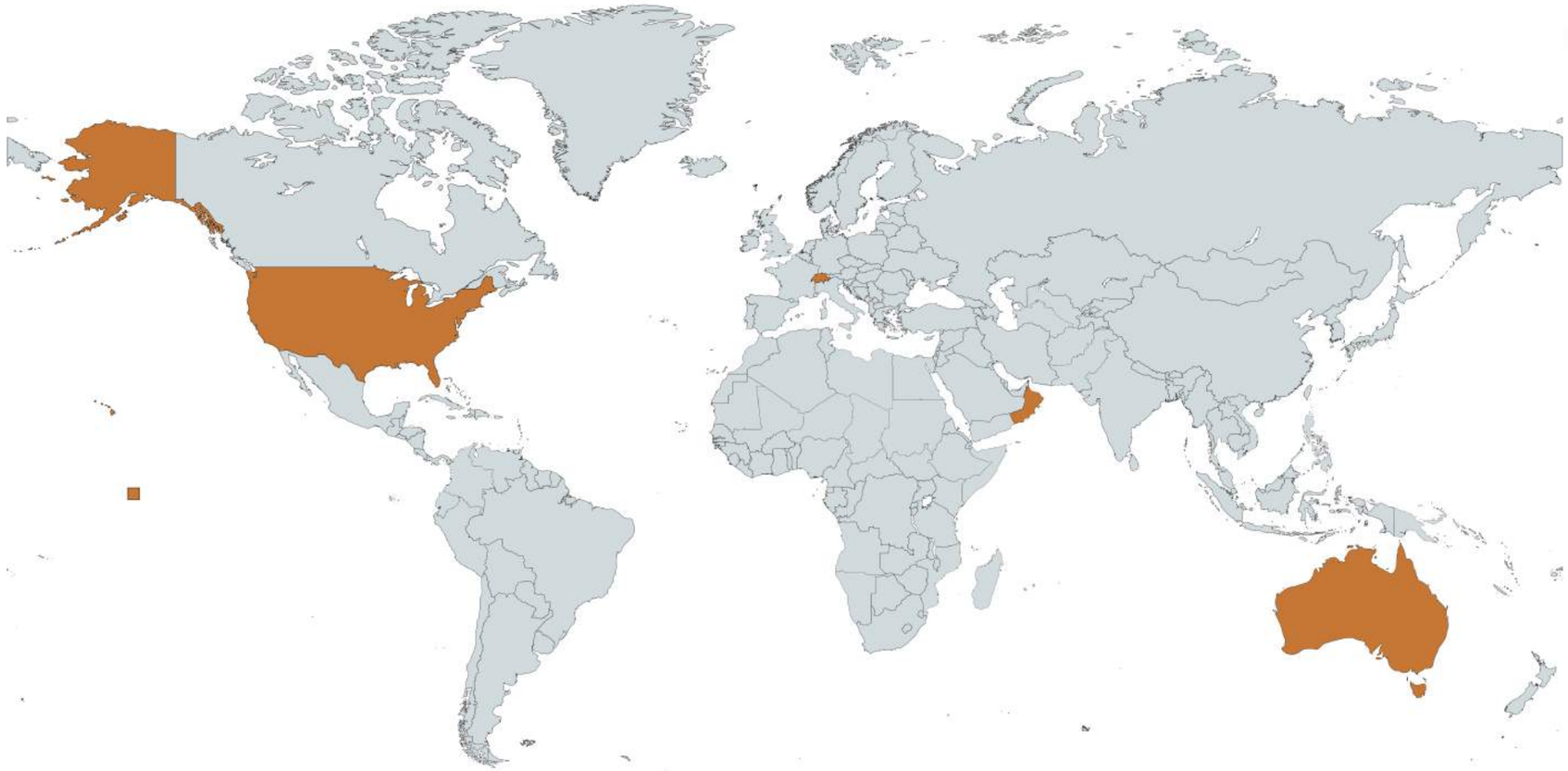
- Manage honeypots and honeynets deployed in different countries all around the world.
- Quickly identify the attackers showing real interest in the honeypots, separating them from simple exploratory scripts and providing a summary of their interactions with the different services deployed.
- Honeykube enables honeypots to be started, stopped, or restored with a single click, removing any trace of malicious activity in a compromised environment.

HONEYKUBE

HONEYKUBE CLUSTERS

Our honeypots are currently deployed in four clusters around the world. These clusters are located in strategic countries, including the **United States of America, Switzerland, Oman** and **Australia**.

Thanks to this diversity, we are able to capture incoming attacks from all sorts of threat actors located throughout the globe.



HONEYKUBE

OUR HONEYPOTS

The real flexibility of Honeykube lies in the fact that, **if it can be run in a container, it can become a honeypot.**

Web servers, file servers, database servers, network devices, industrial systems, medical and IoT equipment – the list is *endless*.

20 Deployed honeypots

13 High interaction

5 Medium interaction

SOME OF OUR DEPLOYED HONEYPOTS INCLUDE THE FOLLOWING SERVICES:

- ElasticSearch
- Samba
- MySQL
- CISCO ASA
- CITRIX
- SAP
- SMTP
- phpMyAdmin
- FTP
- SSH
- TELNET
- ADB
- OPENPLC
- NTP

HONEYKUBE

GENERAL STATISTICS

93 Days

21 Honeypots

73,903 Total attacks

For over three months, our honeypots have been gathering information on the threat landscape, **intercepting more than 70k attacks** from all over the world.

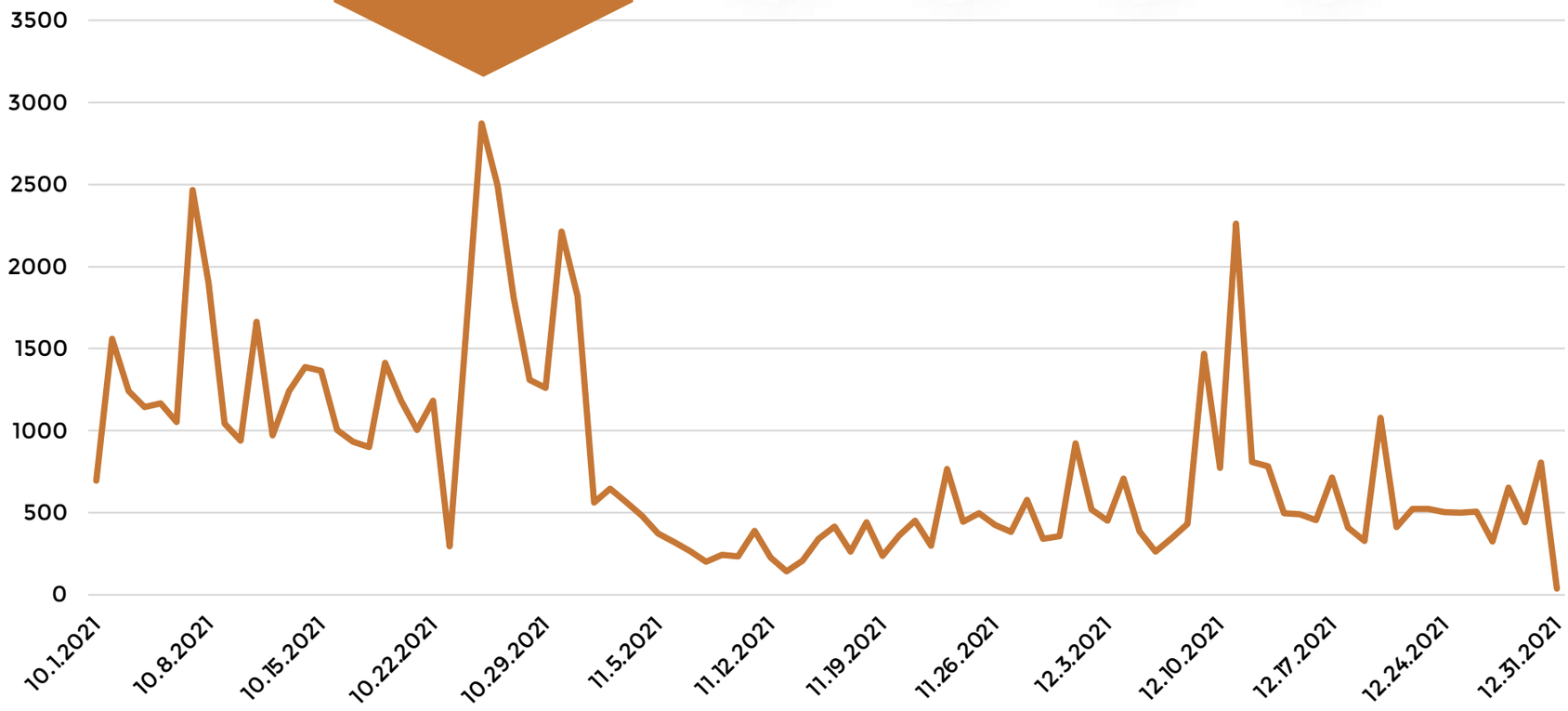
HONEYKUBE

ATTACKS PER DAY

The beginning and end of the year tend to be periods of high activity when it comes to security threats, specially when new vulnerabilities are revealed to the world.

We can see this clearly in the correlation between the log4j-related vulnerabilities and the increase of attacks happening mid December.

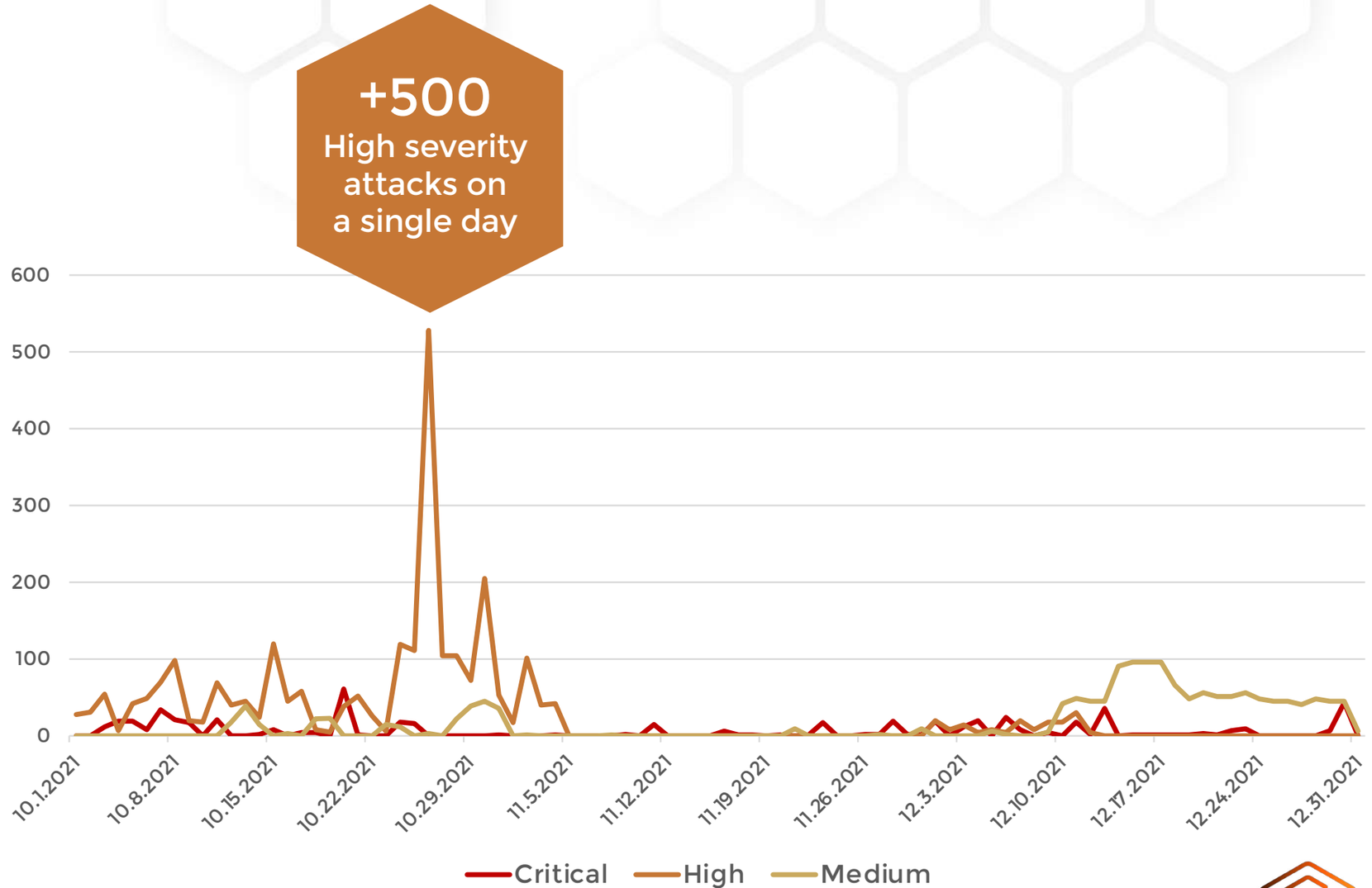
+2800
Attacks on a single day



HONEYKUBE

HIGH SEVERITY ATTACKS

While high severity and critical attacks are not as common, having a cyber-intelligence tool among your assets can help your organisation understand when this high priority attacks are occurring, who is behind these peaks of activity and what might be causing them.



HONEYKUBE

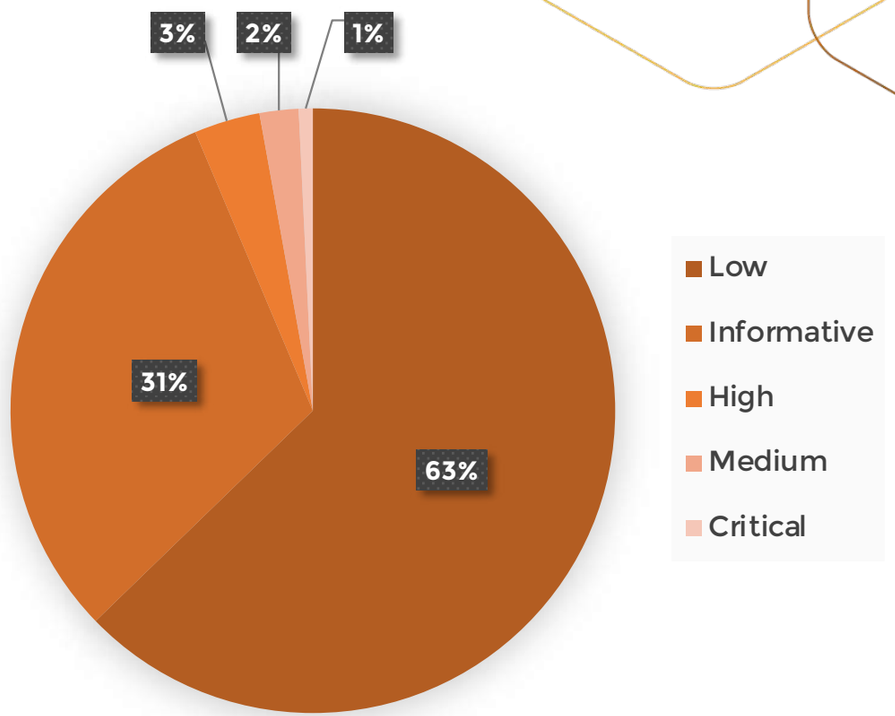
ATTACKS BY TYPE

As expected, most interactions were low severity attacks, such as connection attempts (25,185; 34%) and login attempts (24,697; 33%). Command execution was another popular category (23,106; 31%) for incoming activity. Finally, arbitrary file uploads (434; 0.6%), exploits (288; 0.4%), enumeration attacks (174; 0.2% and ransomware (19; 0,03%) were the categories with the least percentage of detection.

EXPLOITS

Less popular than brute forcing attempts **but far more dangerous**, these were **the CVEs with most attack detections**:

- CVE-2021-44228 RCE on ElasticSearch and phpMyAdmin
- CVE-2015-1427 RCE on ElasticSearch
- CVE-2014-3120 RCE on ElasticSearch
- CVE-2019-19781 Directory traversal on Citrix
- CVE-2020-3452 Directory traversal on Cisco ASA



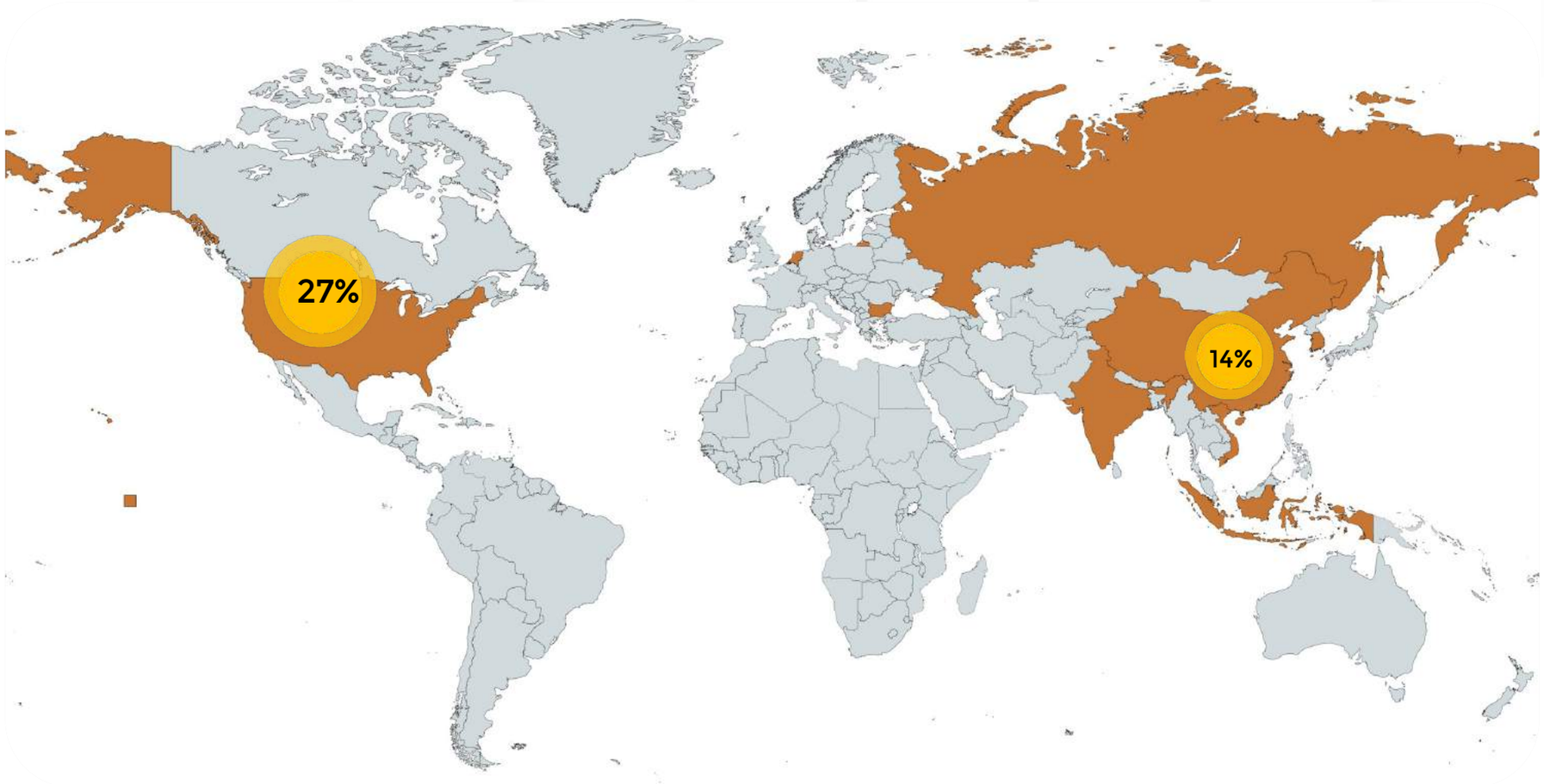
ATTACKS BY SEVERITY

HONEYKUBE

ORIGIN OF ATTACKS

Most attacks were originated in the United States of America (27%), China (14%) and Vietnam (7%).

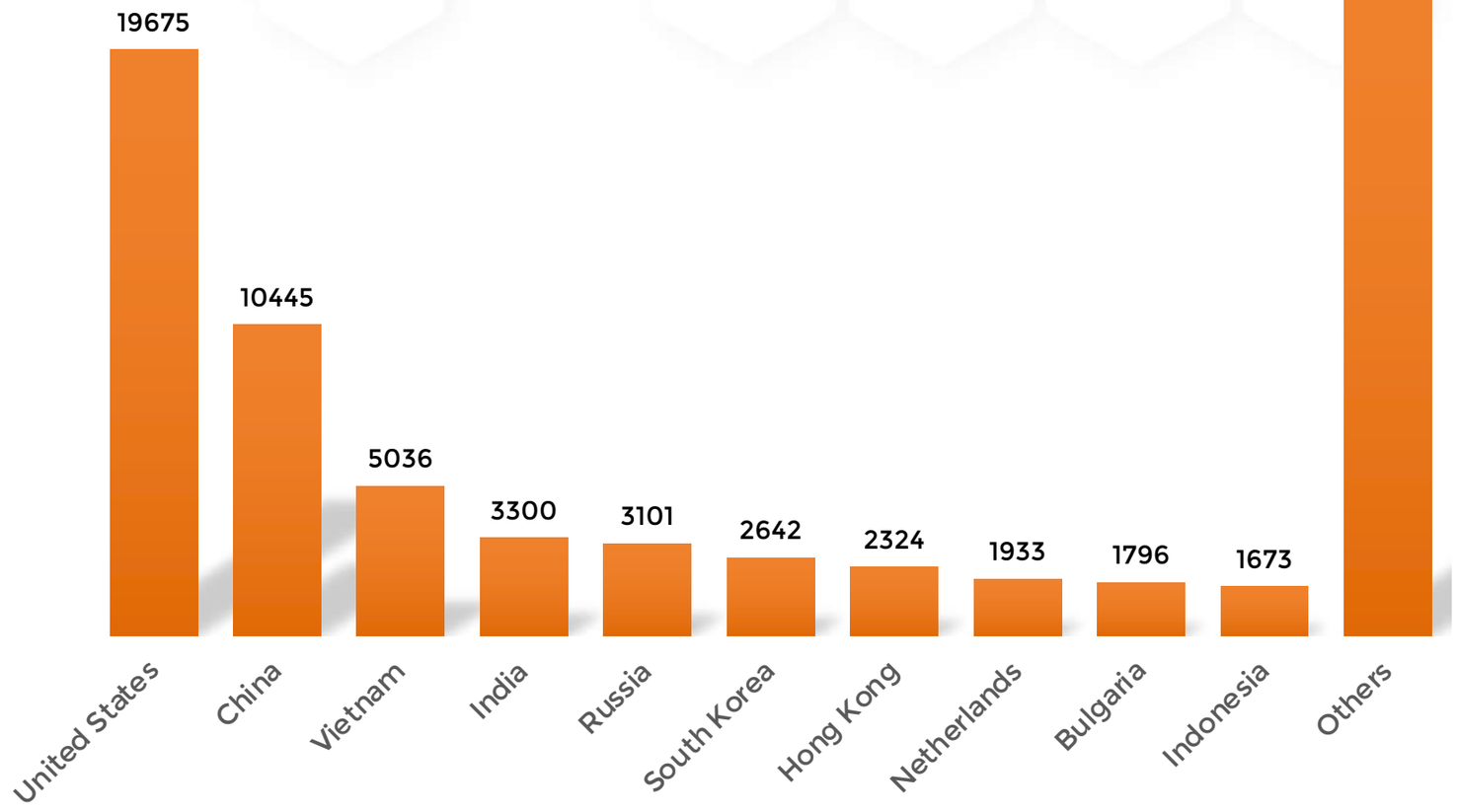
Other two countries that made it to the top five were India (5%) and Russia (4%).



HONEYKUBE

ORIGIN OF ATTACKS (CONT.)

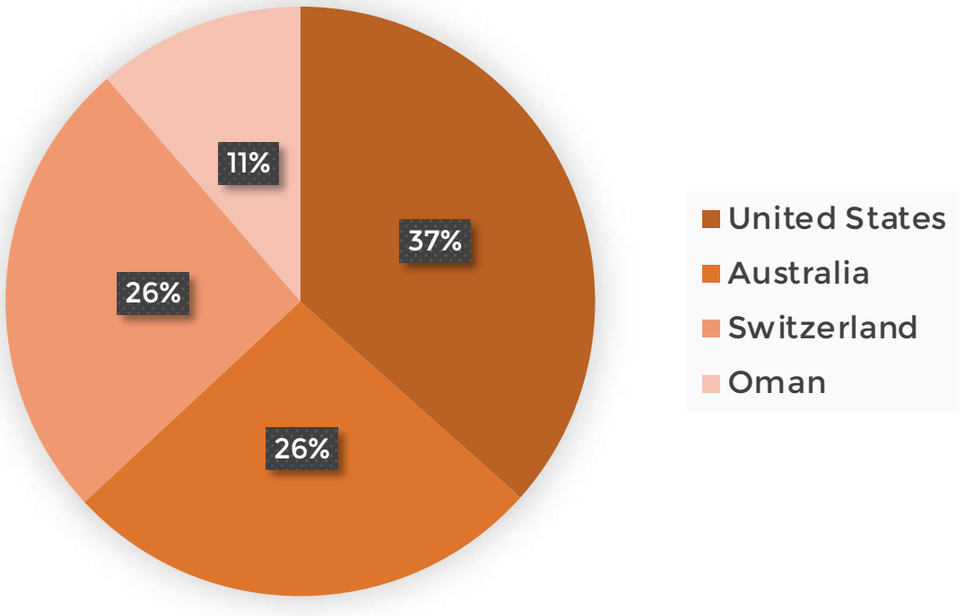
South Korea (3.6%), Hong Kong (3.1%), the Netherlands (2.6%), Bulgaria (2.4%) and Indonesia (2.3%) were also included among the top ten countries that initiated the most attacks during the last quarter of 2021.



DISTRIBUTION OF ATTACKS

The vast majority of attacks (37%) targeted services hosted in the USA.
Out of all the American honeypots; the ADB honeypot was attacked the most, with the majority of attempts trying to install cryptominers in our rogue mobile devices.

The second region with most attacks was Australia (26%), mostly due to high levels of activity (login attempts) targeting the Samba service.

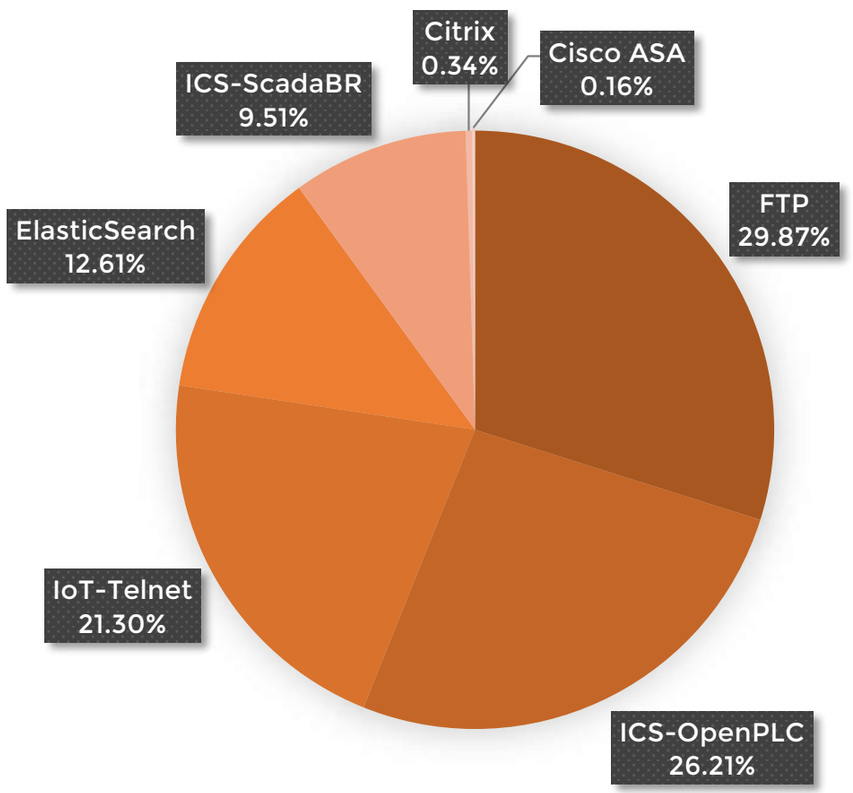


ATTACKERS WERE HIGHLY INTERESTED IN HIGH INTERACTION HONEYPOTS

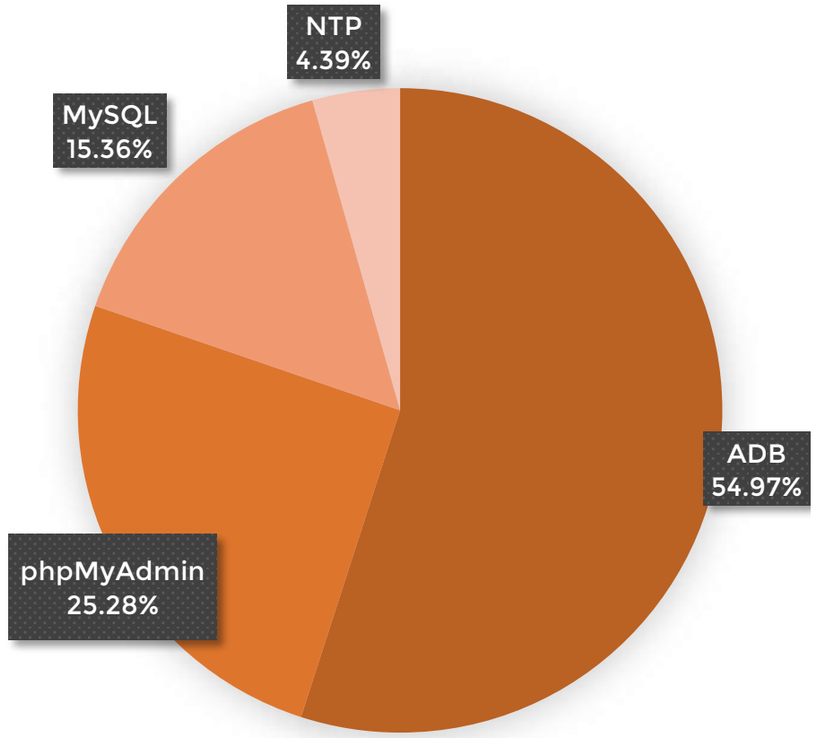
74% of attacks were directed towards our high interaction honeypots (e.g. ElasticSearch, MySQL, Samba, FTP, SMTP, etcetera), 20% towards low interaction honeypots (i.e. Cisco ASA, SAP, Citrix, ADB) and only 6% of attacks affected medium interaction honeypots (e.g. SSH, Telnet).

MOST TARGETED SERVICES PER COUNTRY

SWITZERLAND



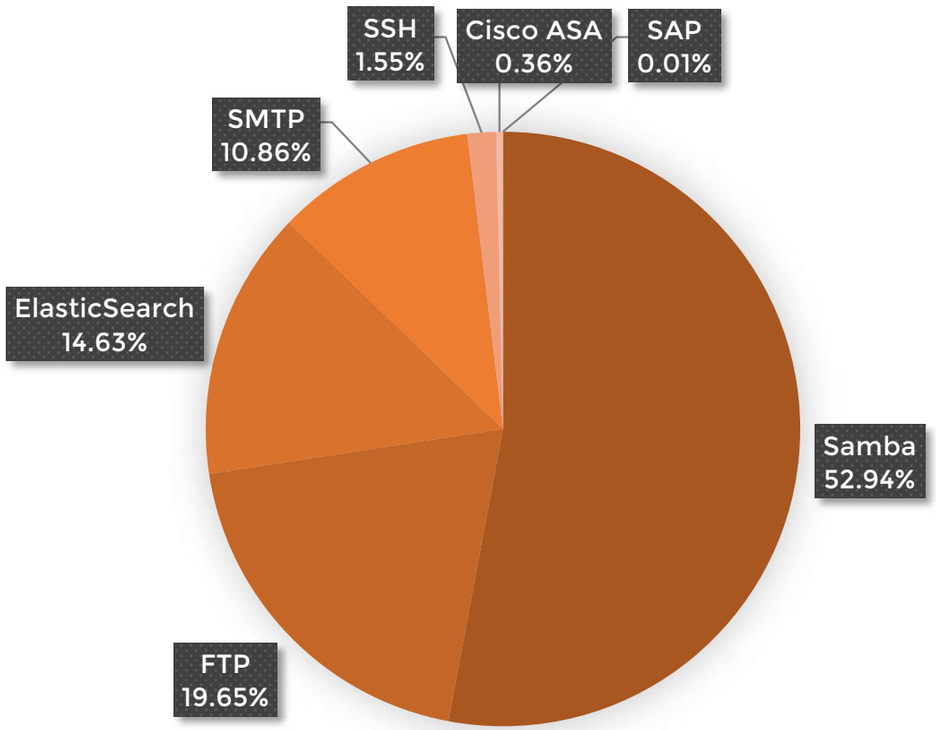
UNITED STATES



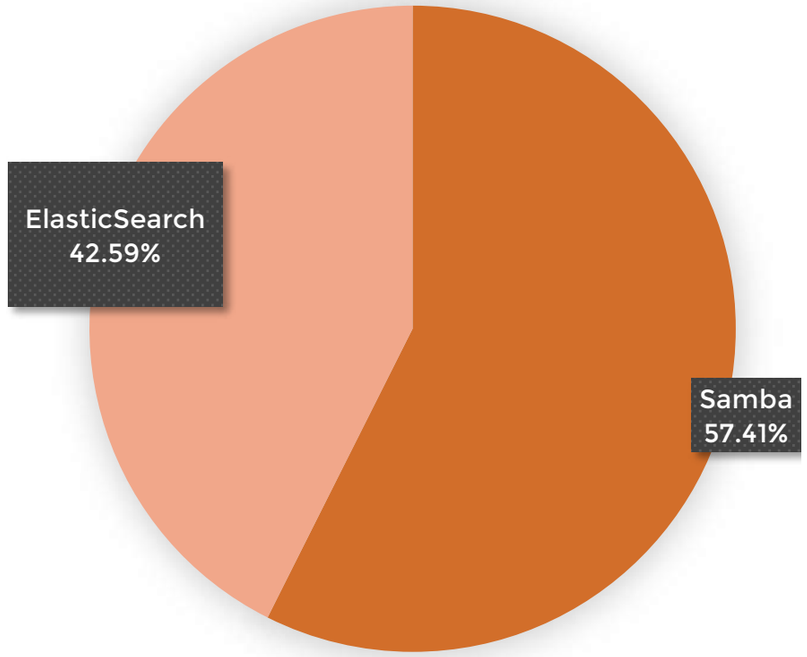
HONEYKUBE

MOST TARGETED SERVICES PER COUNTRY

AUSTRALIA



OMAN



HONEYKUBE

FTP UPLOADS

Honeykube's FTP honeypots were often attacked by cryptominers that copied themselves to FTP folders in the hope of being executed on other machines.

- The most common file names for these malicious uploads were Photo.scr, AV.lnk and AV.scr.
- Most used FTP password was blank.
- Most used username was "www".

SSH LOGIN ATTEMPTS

We recorded more than 300 attempts to bypass our SSH honeypot.

- The most common username was "pi"
- The most used password was "raspberryraspberry993311", followed by "raspberry" and "nicole".

TELNET LOGIN ATTEMPTS

In comparison with the SSH honeypot, our Telnet honeypot posing as a rogue IoT device –a DVR IP camera– was highly targeted, with more than 4000 hits in total and an average of 45 login attempts per day.

- The username "abc123" and password "enable" were the most common combination in these login attempts.

HONEYKUBE

LOG4J-RELATED EXPLOITS

The services ElasticSearch and phpMyAdmin were the most targeted with the log4j exploits, immediately after the vulnerability became public.

With more than 200 exploiting attempts, we were able to log, collect and analyze a wide **variety of obfuscated payloads** to better understand the way in which attackers were trying to take advantage of our exposed infrastructure.

These attacks came from IPs geo-located in Russia, United States, China, Germany, Portugal, Mexico, Oman and the Netherlands, among others.

SAMBA LOGIN ATTEMTPS

One of the most targeted services on our clusters were the Samba honeypots. With **more than 15,000 attacks in total**, these honeypots logged a wide variety of attacks, including exploratory scans, malware uploads and login attempts.

“Administrator” and “admin” were the most common usernames used by attacks when trying to log in.

KNOWLEDGE IS THE KEY

Threat intelligence is critical in dealing with threat actors, and primarily involves the collection, collation, and distribution of information regarding threats that compromise the integrity and confidentiality of different institutional departments. To ensure that the outcome of any cyber intelligence process will yield data of value to all stakeholders, these threats must be identified and prioritised.

Honeykube allows researchers and organisations to visualise attacks being carried out against the different honeypot clusters in real time. Quickly identify the most frequent attack type, their severity, country of origin and the most attracting services for adversaries.

Keeping up with and applying the latest threat intelligence is critical to evolve your security program to combat new attacker techniques. Our new Threat Landscape Quarterly Reports will define shifts in attacker trends and provide a glimpse into the incredible potential of our honeypot solution for a better understanding of the threat landscape, and thus providing the necessary intelligence insights for combatting increasing threats and improving situational awareness.

HONEYKUBE

HONEYKUBE

www.honeykube.ch

Dreamlab Switzerland - HQ
Monbijoustrasse 36, Bern
Suiza – 3011

Dreamlab Chile
Villavicencio 361, Of.104
Santiago Chile – 8320154

Dreamlab Spain
Calle Hermosilla 48
1. Dcha 28001 Madrid

Dreamlab Colombia
Calle 93a # 13-24
Piso 5
Bogotá, Colombia

Dreamlab Peru
Av. Salaverry 3240
Piso 4 San Isidro Lima
Peru – 15076

Dreamlab Bolivia
Edificio De Luna Oficina 3-A
Lisimaco Gutierrez 490 - 2
La Paz, Bolivia

Dreamlab Malaysia
Vertical Business Suite, Tower A, Level 29-0
Bangar South Kuala Lumpur Malaysia – 59200

Dreamlab Oman
P.O. Box 55
Minarit Al Qurum Building Office No. 233
Al Khuwair, Sultanate of Oman – 133

Dreamlab Australia & New Zeland
2/23 Foster Street
Surry Hills, NSW 2010

HONEYKUBE

HONEYKUBE

A solution by

DREAMLAB TECHNOLOGIES