2023
A MSSPs Perspective

Ioan Constantin
Orange Romania

orange™

Contents

Rough seas

2023 was tough.

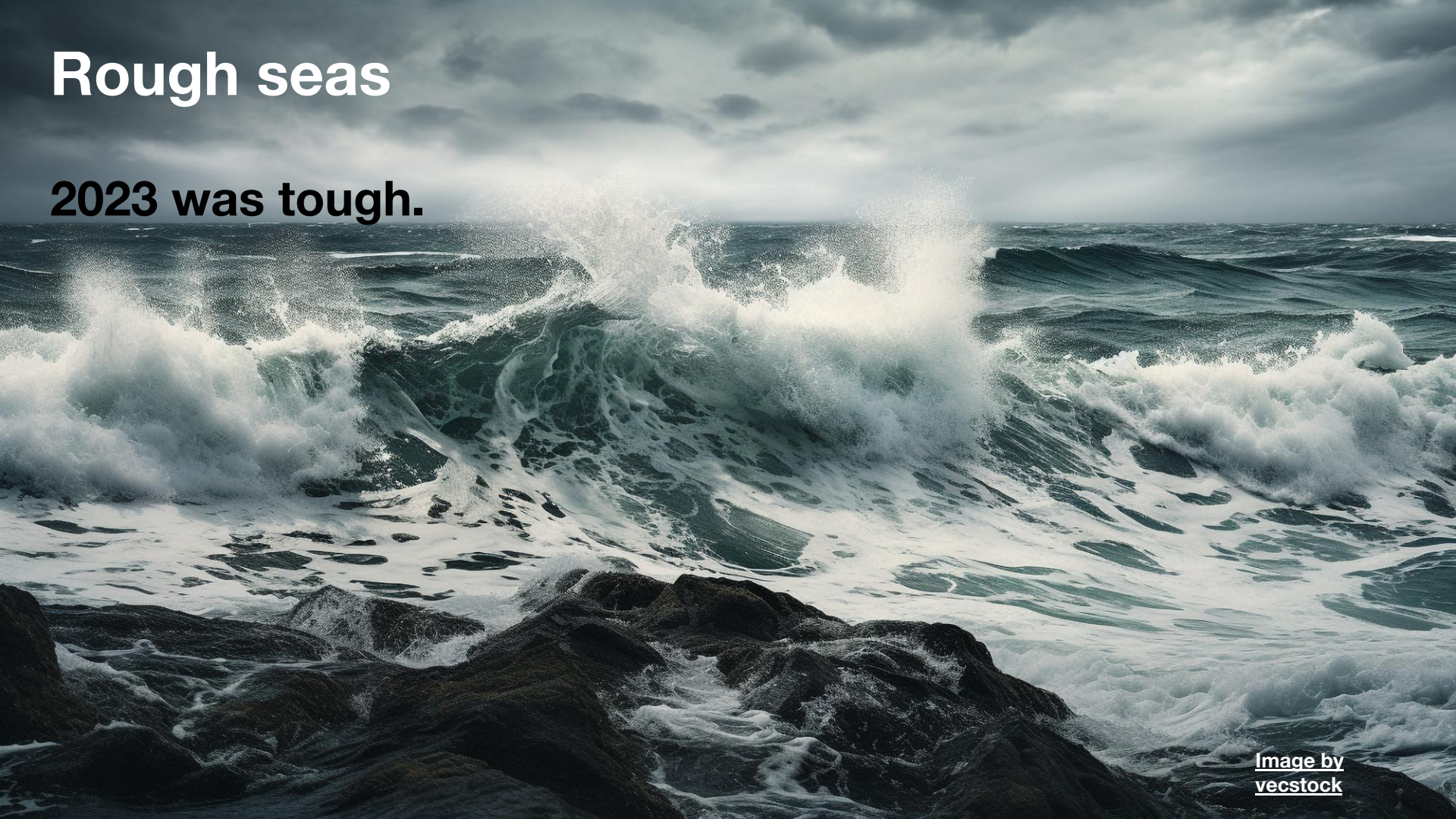


Image by vecstock

In numbers. Actually in Figures*

Attacks (Volume)

Cost (Impact)

Crypto malware

Leaks (Number)

New 0-Days (YoY)

Ransom Paid ($, YoY)

Dwell Times (D)

New APT Groups (YoY)

MTTD 8% down Y0Y

MTTM 1% down Y0Y

Image by vecstock

*Sources: Mandiant, CISCO, Sophos, Orange

Context

1

Everything off-prem

Accelerated migration to cloud & hybrid cloud means unsecured, internet-facing data & APIs.

2

Improved Tools

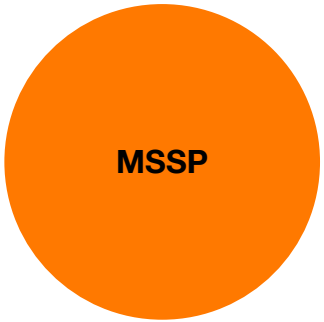
Malware distribution platforms, C2C for hire, Ransomware as a Service.

3

Geopolitics

Still plays a major role. State-nexus groups are advancing cyber warfare methods.

Orange Business Services



Managed Services

Prevention

Detection

Monitoring

Response

400+ Companies

SMEs to Large Enterprises and Public Sector

Tens of thousand of protected assets

Managed

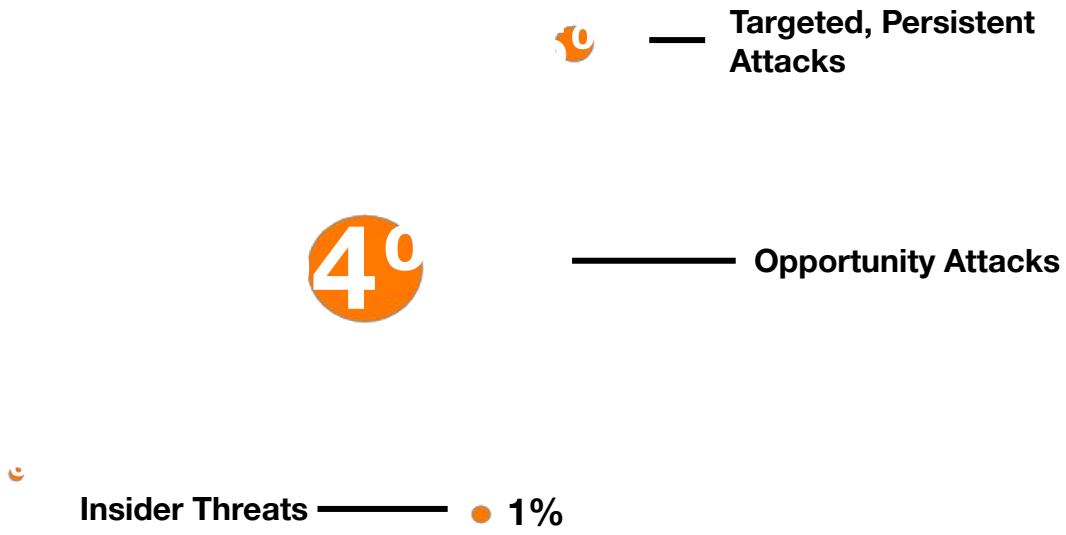
Firewalls; IPS/IDS; EDR/XDR; SIEM; MDM; Anti-DDoS; WAF; Vulnerability Management; SOC

Attacks

2023: Ransomware

We've seen large Year-Over-Year increase in activity:

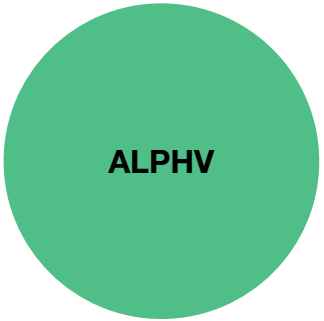
- **Ransomware up to 34% over 2022 in all counted detection**
- **DDoS attacks up to 18% over 2022 in all blocked attempts, across our customers base**



Attacks

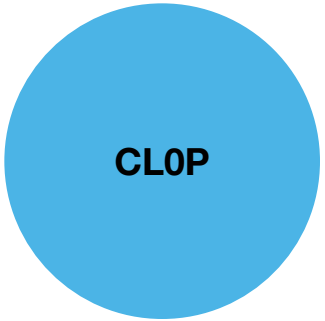
Insights – Ransomware observed through BIS

Observed through the entire 2023 timeframe. Most active & prolific ransomware variant. Present in most detections, makes up some 30% of all recorded incidents. Some RO data present on leaksites.



Aka BlackCat, Noberus. Seen using software such as Impacket tool and RemCom for deployment. Recorded using CVE-2020-1472 (Zerologon) and newer high-severity flaws.

Distributed mainly out of Russia, armed to delete VSSes, able to exfiltrate regardless of payment of ransomware. Easily becoming mainstay.



Observed in February – July 2023 timeframe, attributed to their GoAnywhere MFT 0-day campaign. Pivoted to use CVE-2023-34362 in MOVEit file transfer service

Attacks

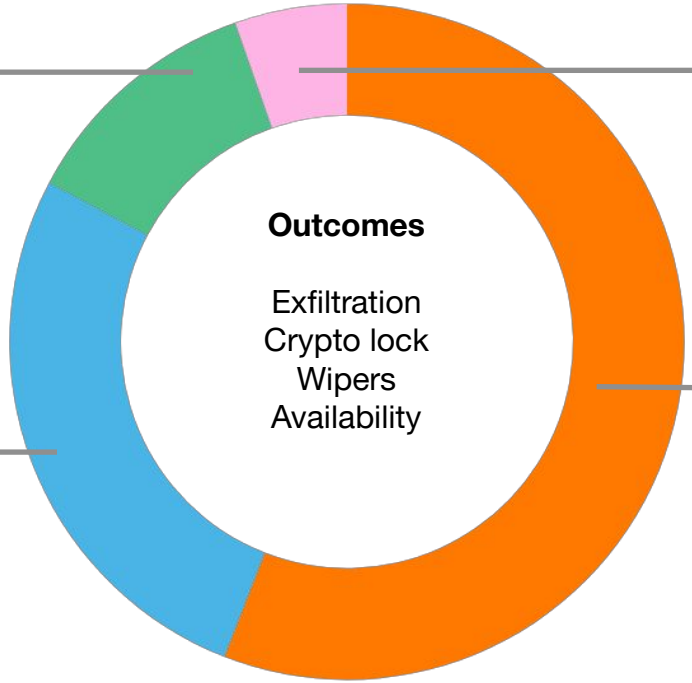
Insights - Vectors and Outcomes of Targeted Attacks

Spear Phishing

Some 10 percent
Attacks are relevantly targeted, mostly against business and specific verticals, less common against individuals

Brute Force

All over the place
DDoS mostly, targeting low hanging fruits



Exploits

Less than 1 out of 10
Attacks are actively trying to exploit unpatched & known vulnerabilities

Phishing

6 out of every 10
Attacks are vectored through phishing. Most by e-mail, seconded by social media and SMS in third place

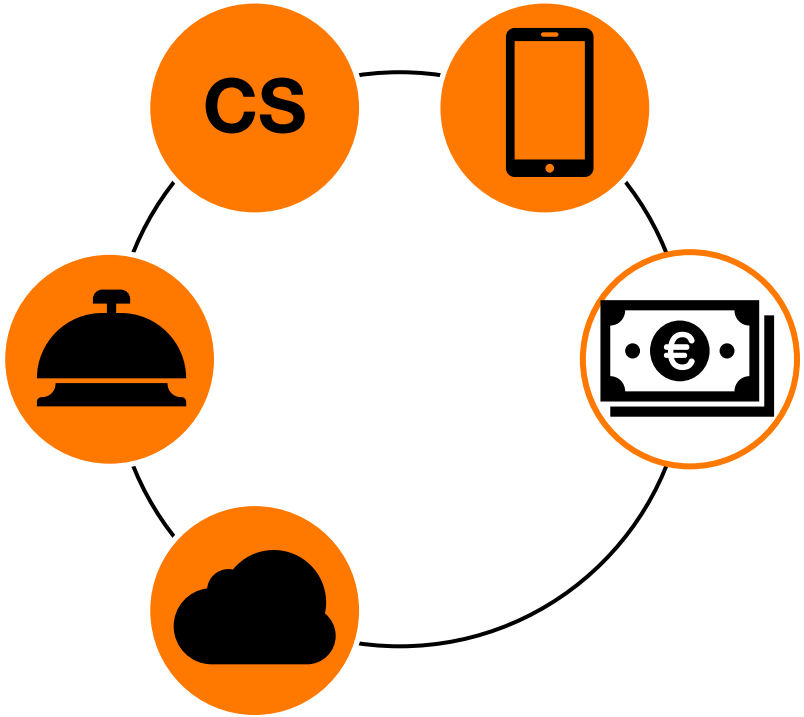
Attacks

Insights – Trends in Attack Orchestration

CobaltStrike
Still in operation, doing fairly well in the RO landscape, uptick in activity during the March ’23

R-a-a-S
Ransomware C2C Platforms observed, most notable REvil.

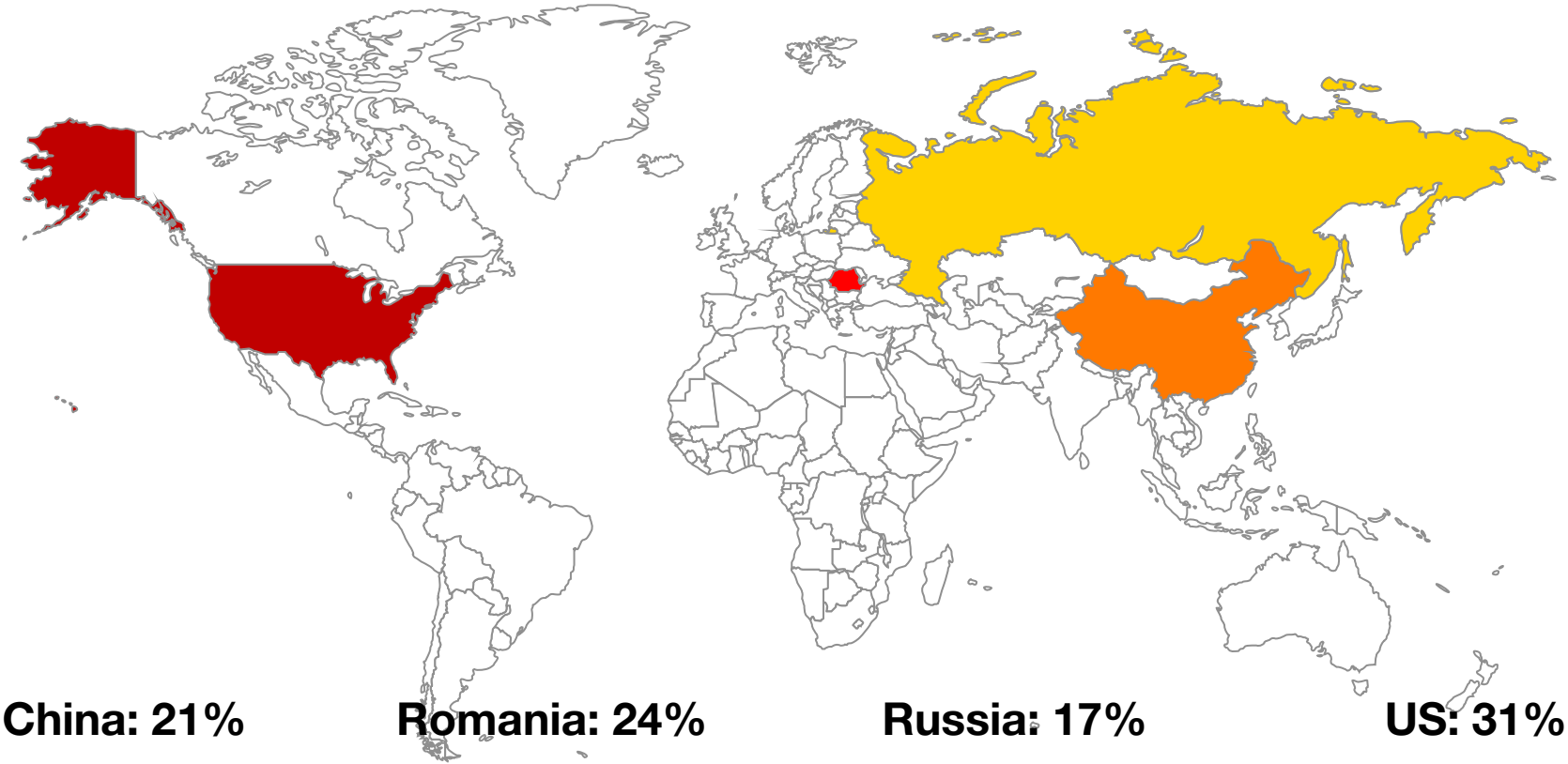
DDoS
Mostly uneffective, heavily reliant on (very) old existing botnets. Most notable operator: Kill.net (2023)



Mobile Attacks
Text-based attacks prevalent. Attackers using SMS, RCS, and Whatsapp vectors

Ransomware
Large increase in volumes YoY but high profile victims are hit and miss, opportunity attacks yield low to zero $$$

Attackers



China: 21% **Romania: 24%** **Russia: 17%** **US: 31%**

Attackers

We're tracking the activity of some 13 APT groups across the Globe, with relevant Ops in Romania

TA505 – Operators of CL0P. Probably based in one of the CIS states.

APT29 – Phishing with data exfiltration as a goal

KillNet – High Noise, Low Yield type of Op, mostly DDoS against visible targets. In the media and on SoMe, they've spun off to smaller groups – Noname057

UNC4841 – Minimal footprint, mostly poking around for CVE-2023-2868 / Barracuda ESG 0-day

APT41 – Uses spear phishing to gain access, deals in a variety of malware mostly for data exfiltration and the occasional ransomware

APT35/Charming Kitten – Complex Social Engineering Ops, Spear Phishing, Drubot, Houseblend then Data Exfil.

TL;DR

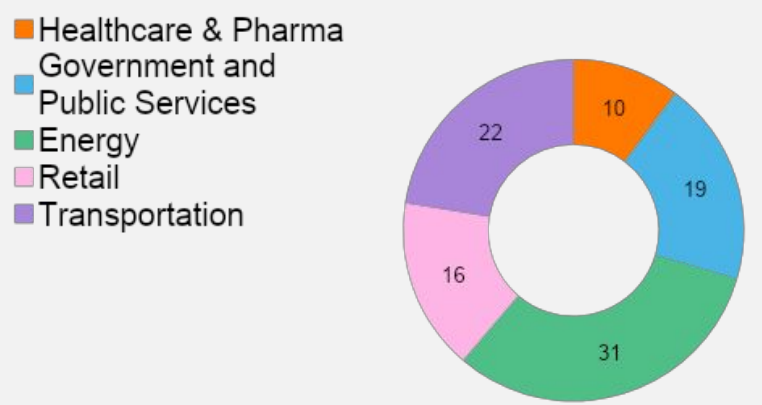
There is minimal APT activity across our monitoring surface with here-and-there attempts to exploitation of infrastructure.

There's been an uptick in interest in CVE-2023-20198 / Cisco IOS XE, we've recorded some activity (mostly scanning) in our perimeters, starting late-October. Little to none exploitation attempts.

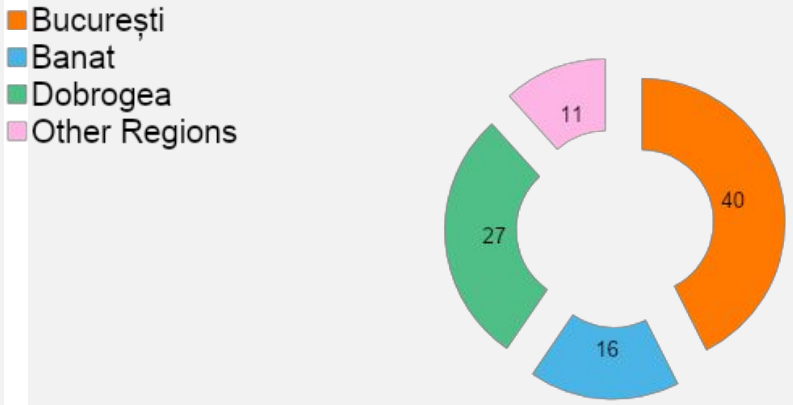
Most observables are phishing artefacts.

Targets

By business vertical



By region



BIS Report 2023

Business Internet Security Report

6th edition, 2023

Business

Predictions

2024 is going to be rough.

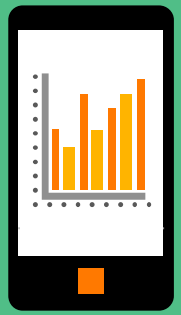
Cyberwarfare

Large, state-sponsored actors

Huge BoM for their TTPs

Lack of normalization of response

Mobile Malware on the rise



ICS/IoT

Increase of ICS targeting, Attacks through the “red line”

IoT is becoming ubiquitous, this means ripe & low hanging

Adversarial A.I.

Not a buzzword.

Noise Generation / Obfuscation

Evasive techniques

TTPs diversification