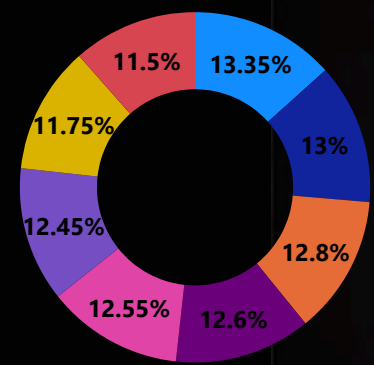


# CYBER ATTACK LIVE REPORT

Count of Attack ID by Attack Type



Attack Type ● XSS ● SQL Inj... ● Brute ... ● MITM ... ● DDoS ▶

Country of Origin

Brazil	Germany	Iran	Russia
China	India	North Korea	UK

20-08-2024

18-12-2024

Overview of Cyber attacks

Attack Trends and Analysis

Most Targeted Destinations

Malware Analysis

Financial Impact and Ransom Analysis

Remediation and Firewall

Total Attacks

2000

Max. Ransom Demand

\$986.60K

Success Rate

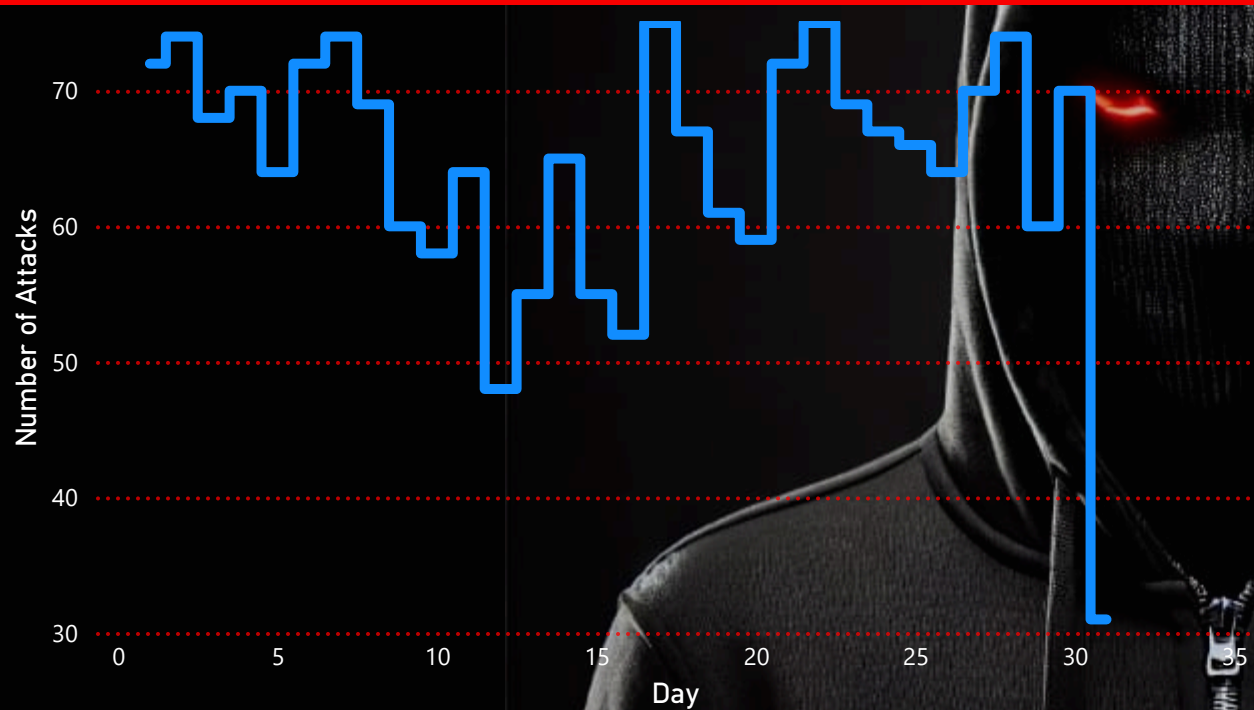
50.25

Top Affected Industry

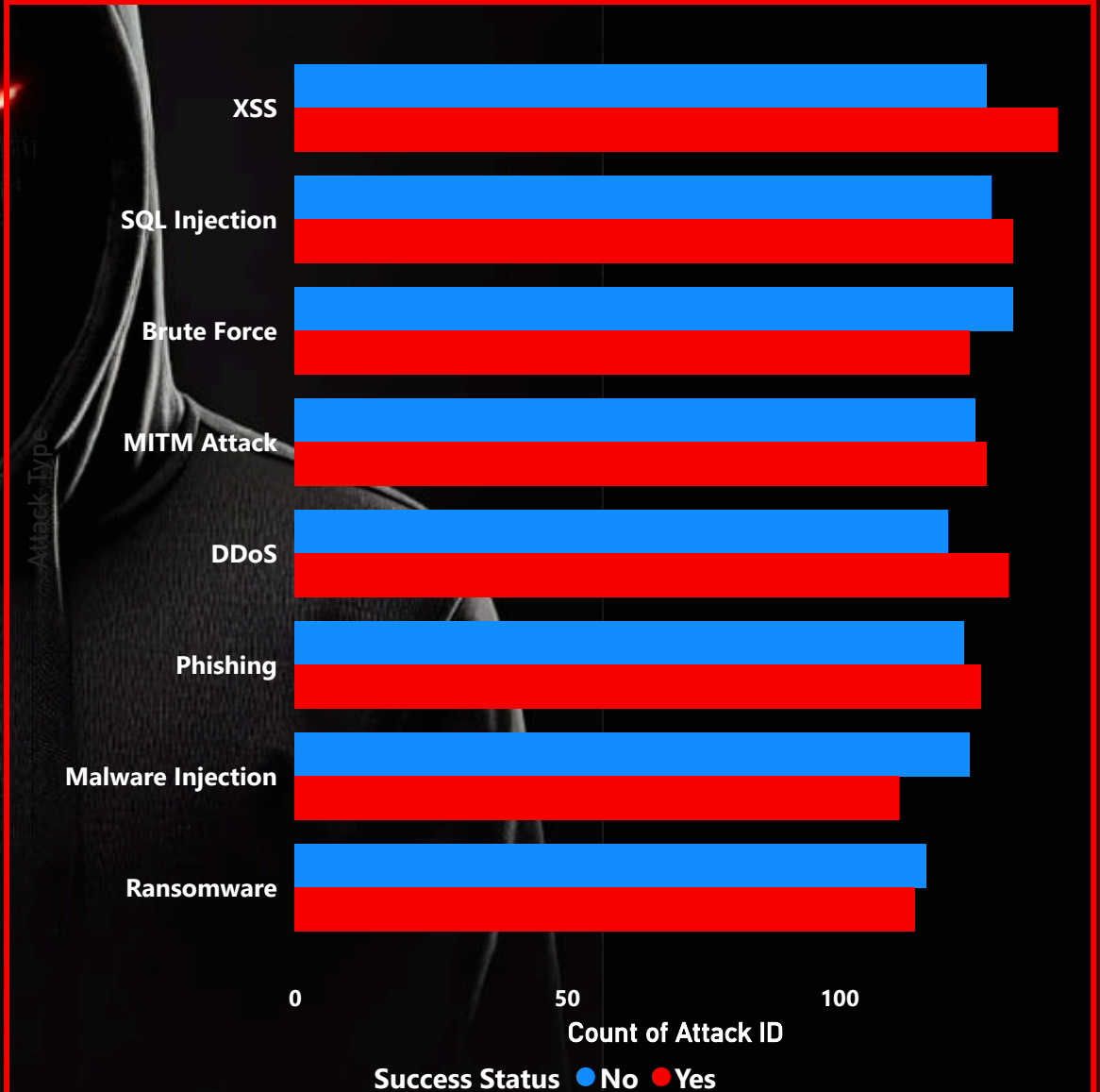
GovSecure

# ATTACK TRENDS AND ANALYSIS

## Number of Attacks by Day



## Count of Attack ID by Attack Type and Success Status



### Attack Type

- ☐ Brute Force
- ☐ DDoS
- ☐ Malware Injection
- ☐ MITM Attack
- ☐ Phishing
- ☐ Ransomware

### Success Status

No

Yes

# MOST TARGETED DESTINATIONS

Protocol Used

FTP

ICMP

TCP

HTTP

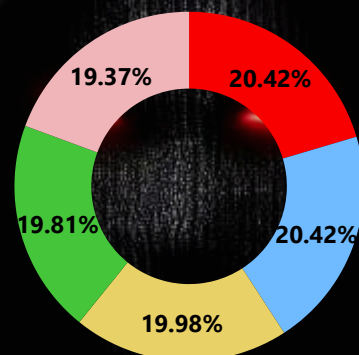
SMTP

UDP

HTTPS

SSH

## TOP FIVE TARGETED COUNTRIES



Country ● Germany ● India ● UK ● Brazil ● Russia

Country of Origin

Brazil

India

Russia

China

Iran

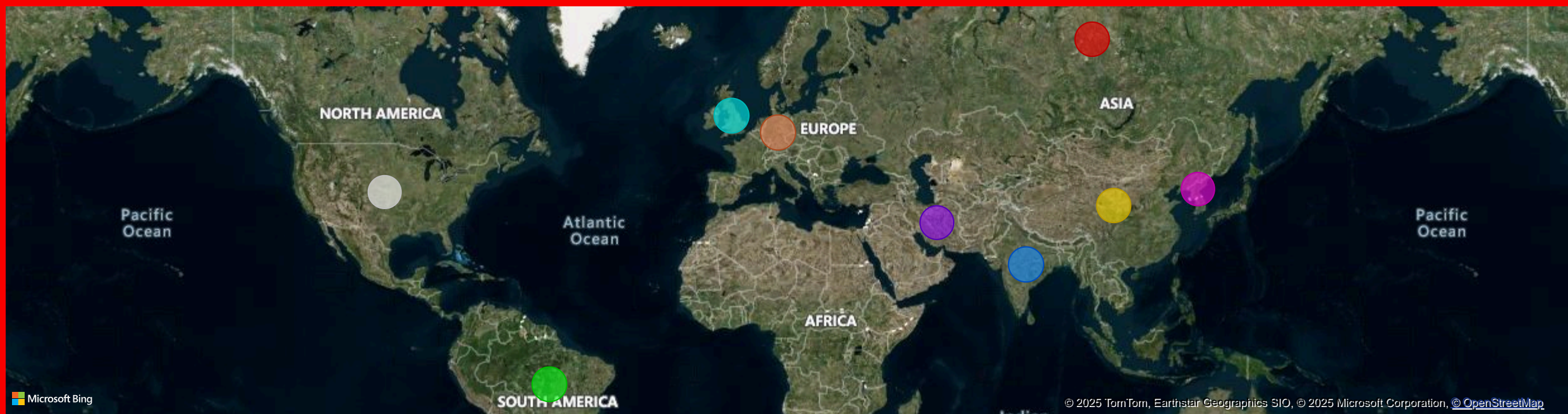
UK

Germany

North Korea

USA

## NUMBER OF ATTACKS BY COUNTRY





# MALWARE ANALYSIS

## Malware Used

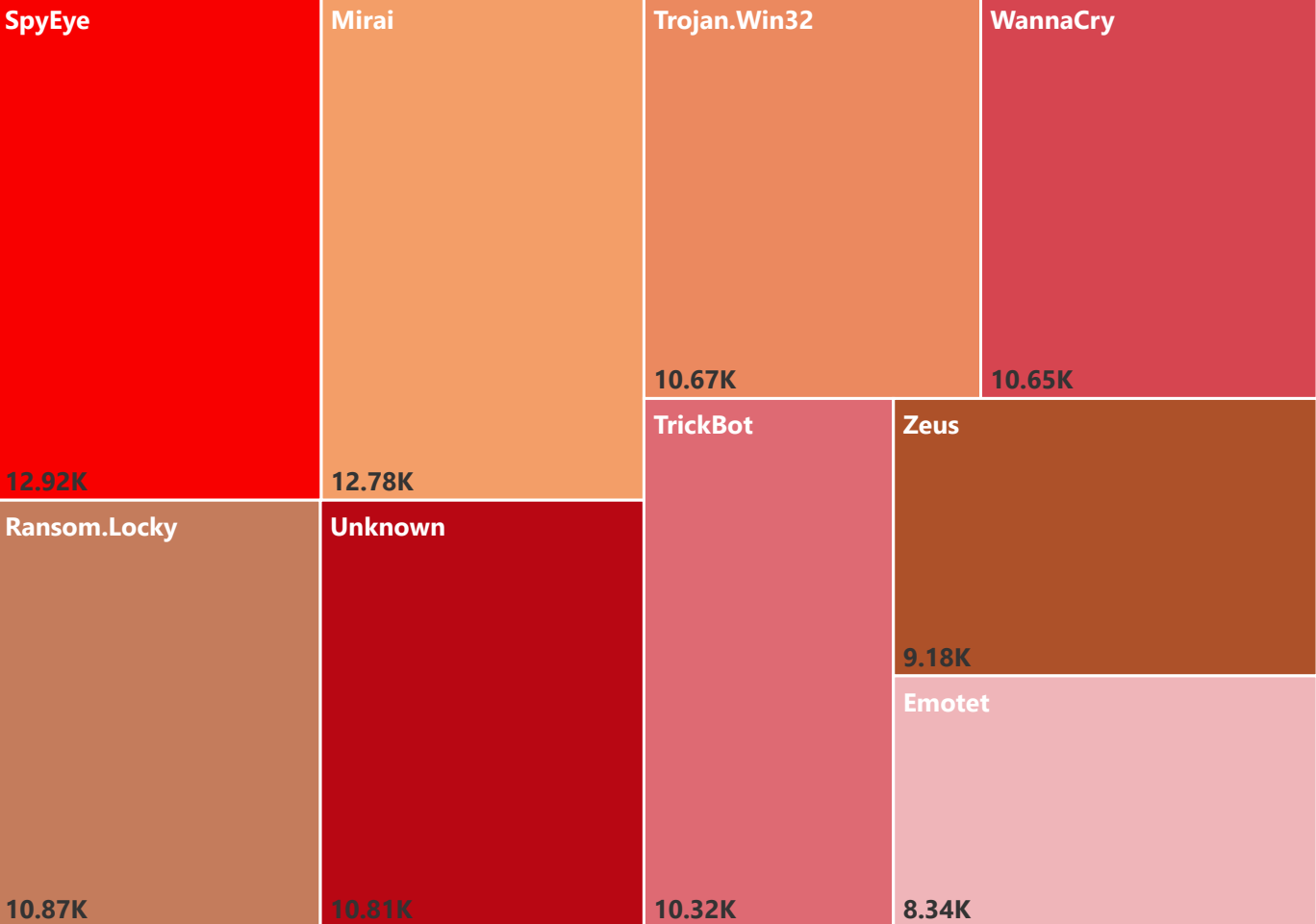
- ☐ Emotet
- ☐ Mirai
- ☐ Ransom.Locky

## Firewall Status

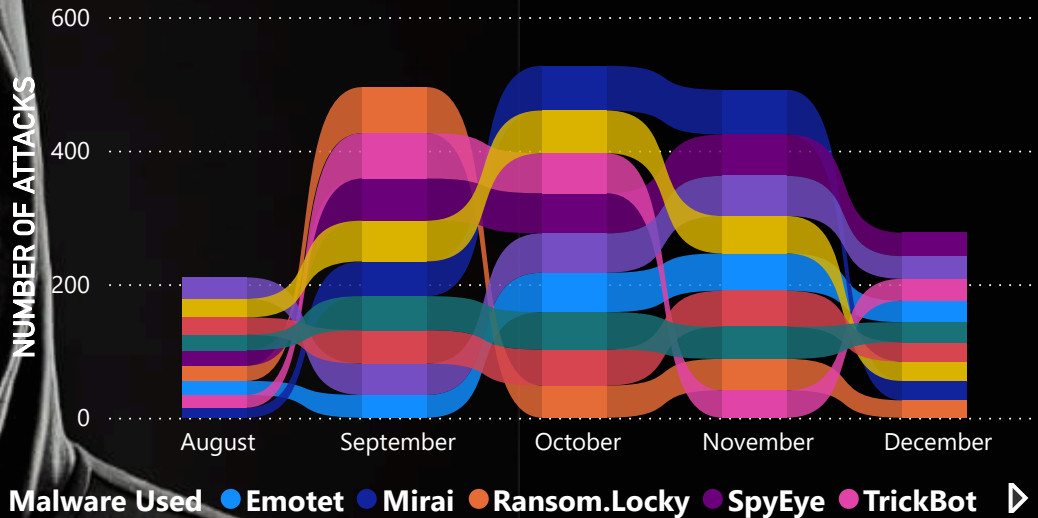
No

Yes

## DISTRIBUTION OF MALWARE TYPES BY TOTAL DATA COMPROMISED



## Malware Dominance Over Time - A comparative view



## Malware Used

## Count of Unique Organizations

SpyEye	243
Unknown	238
Trojan.Win32	232
Mirai	230
TrickBot	221
Ransom.Locky	213
WannaCry	213
Zeus	208
Total	2000

# FINANCIAL IMPACT & RANSOM ANALYSIS

Ransom Range

- ☐ High Ransom
- ☐ Low Ransom
- ☐ Medium Ransom Amount
- ☐ No Ransom
- ☐ Very High Ransom

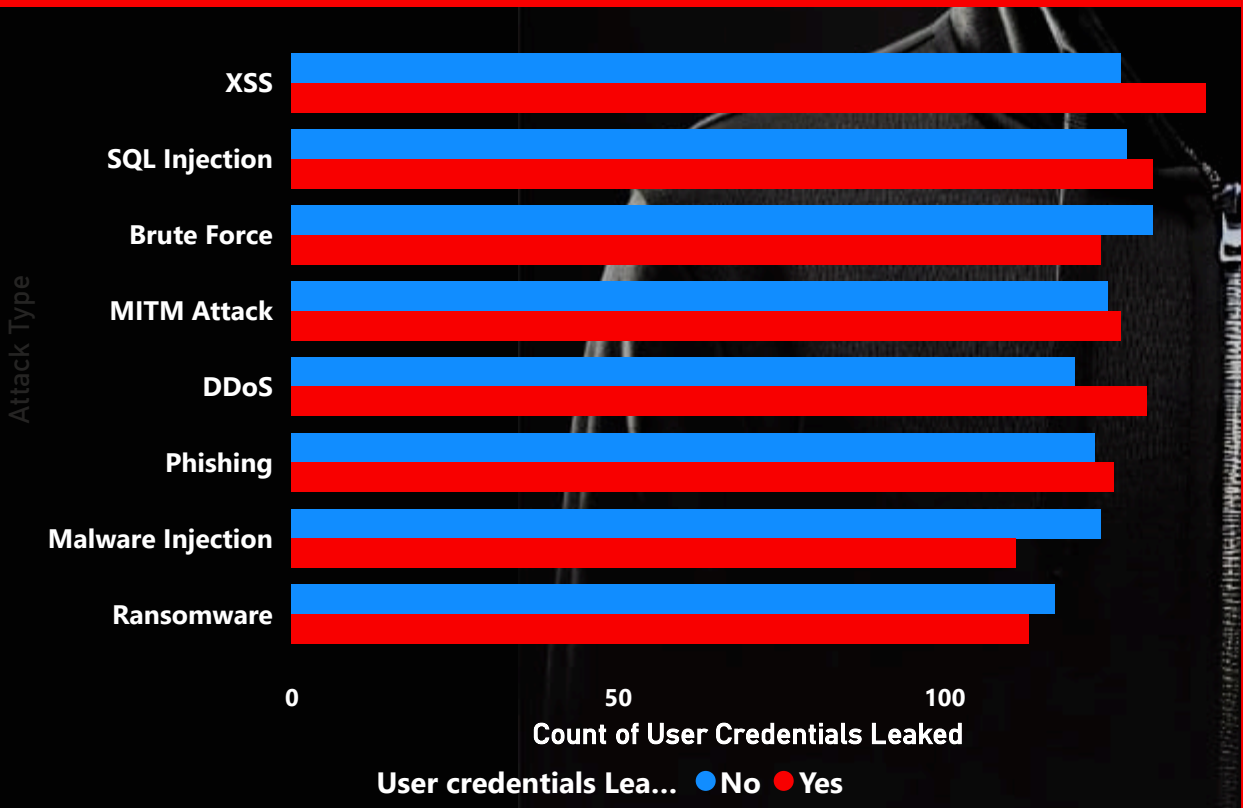
Success Status

- ☐ No
- ☐ Yes

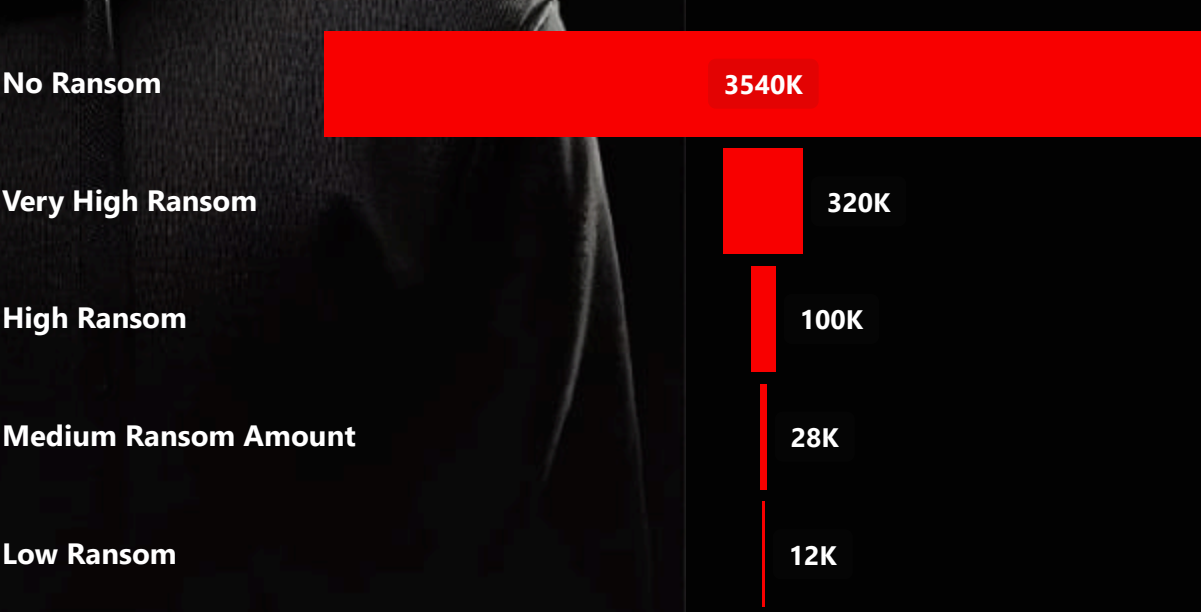
Average of Ransom Demand



Credentials Leaked by Attack Type



Distribution of Attacks based on Ransome Demand Levels



# REMEDIATION & FIREWALL EFFECTIVENESS

Daily Cyber Attacks: Firewall & Remediation Effectiveness



Attack Severity

Critical

Low

High

Medium

Firewall Status

All

Firewall Status

Yes

Attack Type

MITM Attack

Attack Severity

High

Remediation App...

Count of Success S...  
2000

Yes  
1011

No  
989

Brute Force  
127

MITM Attack  
117

Ransomware  
115

Critical  
31

Low  
27

High  
22

IP Ban  
7

Data Recovery  
6

Patch Update  
4