



Cybersecurity Landscape in Nepal: 2025

Santosh Sharma



Cybersecurity Practitioner and Academician for 15+ years



Currently Cybersecurity Consultant @WorldbankGroup



CISO/CEO @AbrikTech



Certified EC Council Instructor (CPENT, CEH, CSA,CCT,CSA)



Visiting Faculty (IOE, Pulchowk, The British College, Islington College)



Previously CTO/CISO @ Eminence Ways, Cybersecurity company (9 years)

About Me

Santosh Sharma





Companies

News

Sign Up

World Clocks
Los Angeles
08:45 PM -1d
New York
11:45 PM -1d
London
04:45 AM
Paris
05:45 AM
Moscow
06:45 AM
Beijing
11:45 AM
Tokyo
12:45 PM

Visitors
Last 24 hours
5,109
Last 7 days
32,859
Last month
87,851
Online
63

Companies

All 21 Stocks 2 US 11 Europe 4

Filter

Eastern Platinum Limited

Canada



Revenue \$104M Employees 1,800 Stocks TSE: ELR Disclosures 1/1

HealthCare

United States of America



Revenue Employees Disclosures 1/1

nson

United States of America



Revenue \$89M Employees 450 Disclosures 1/1

healthcare

United States of America



Revenue \$190M Employees 1,200 Disclosures 0/1

research

United States of America



Revenue \$5M Employees 25 Disclosures 1/1

Disclosures

Eastern Platinum LTD

Published
6d 05h 32m



Eastern Platinum Limited (Eastern Platinum) is a Platinum group metals) and chrome producer with operations and assets located in South Africa. They are a mining and exploration company based in Vancouver, Canada, with a primary listing on the Toronto Stock Exchange and a secondary listing on the Johannesburg Stock Exchange.

Screenshots 7



View 112.6 GB • 79,044 files • 118 views

Website
www.eastplats.com

Share on:

Key Insights



40,000 new vulnerabilities added in 2024 (33% increase from 2023)



331 zero-day vulnerabilities identified



55% with publicly available POC code



32% fully functional exploit code available



30% used in ransomware and APT campaigns

AI enabled Cyber crime



DeepfaceLab and Faceswap



FraudGPT and WormGPT



AI generated Phishing pages



Eleven Labs and Voicemy.ai

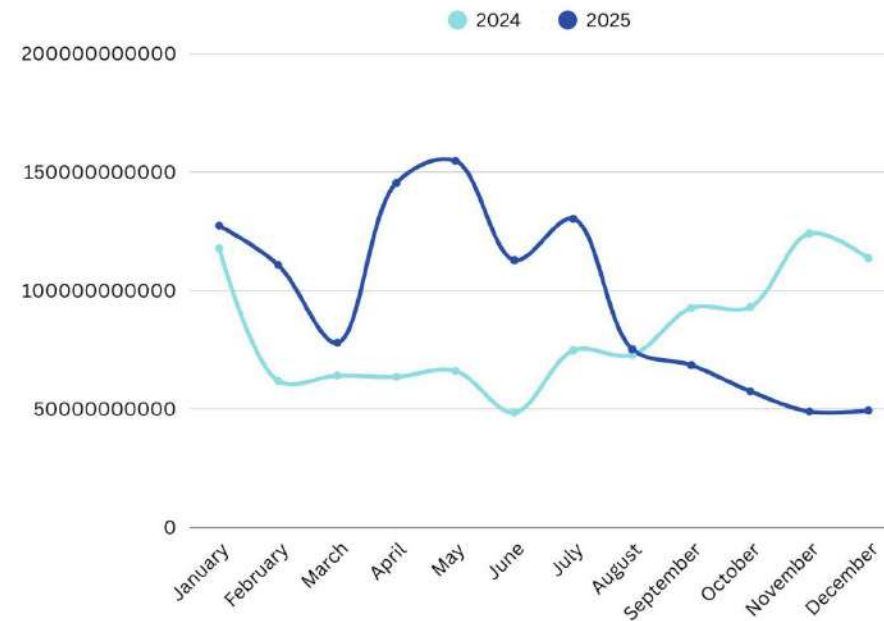


AI power social engineering bot

Rise of Automated Scanning

- Approx 36,000 scans per second (Rise of 16.7%)
- Targeted services include SIP, RDP, OT/IoT protocols

Behavioral Trend Analysis by Month



Current
Detections

1.16
trillion

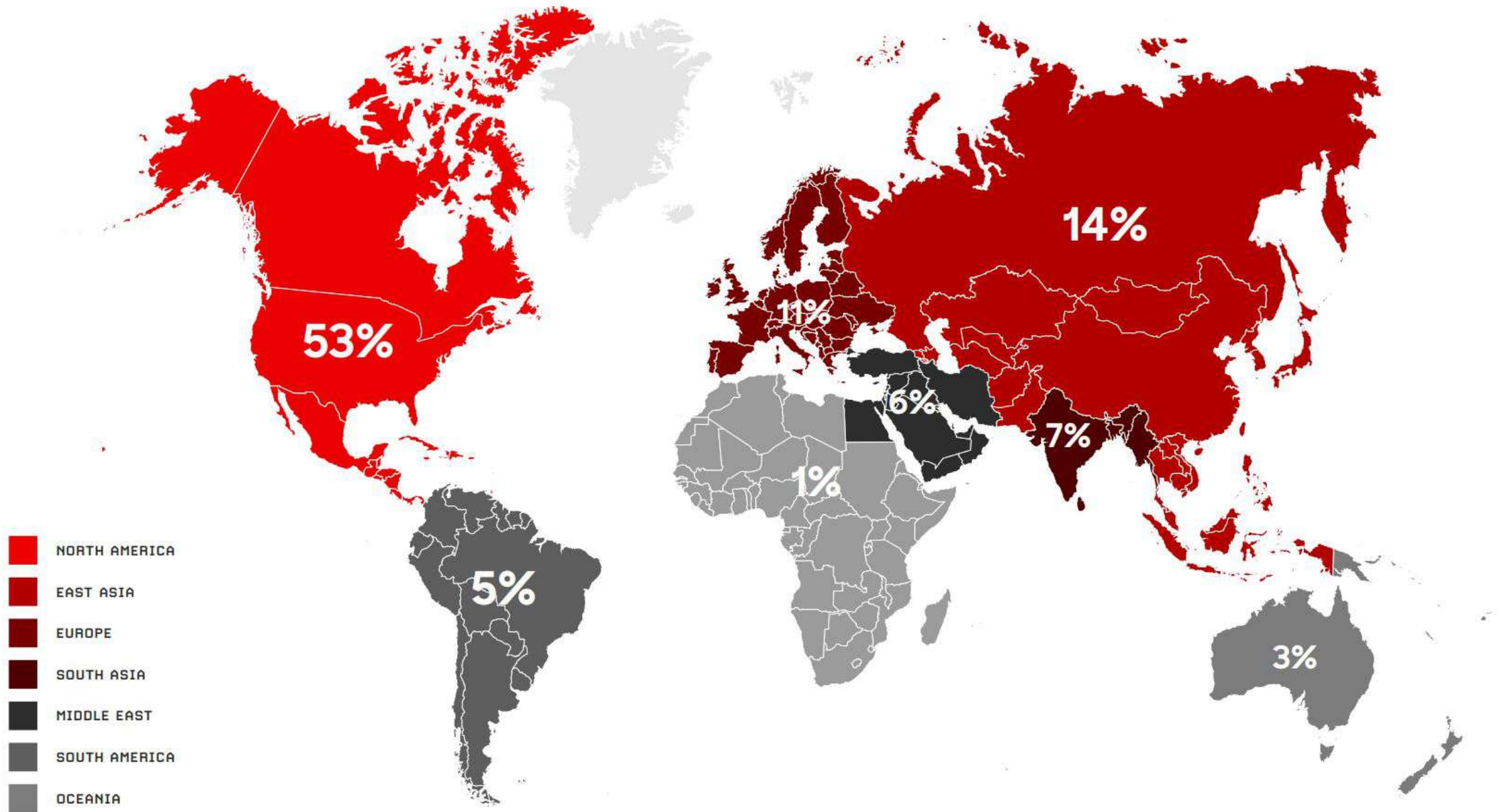
Detections
in 2024

993
billion

Growth year
over year

16.71%

Interactive Intrusions by Region



Top vulnerabilities

Windows SMB Info Disclosure vulnerability

Apache Log4j RCE

Hardcoded password in IoT devices

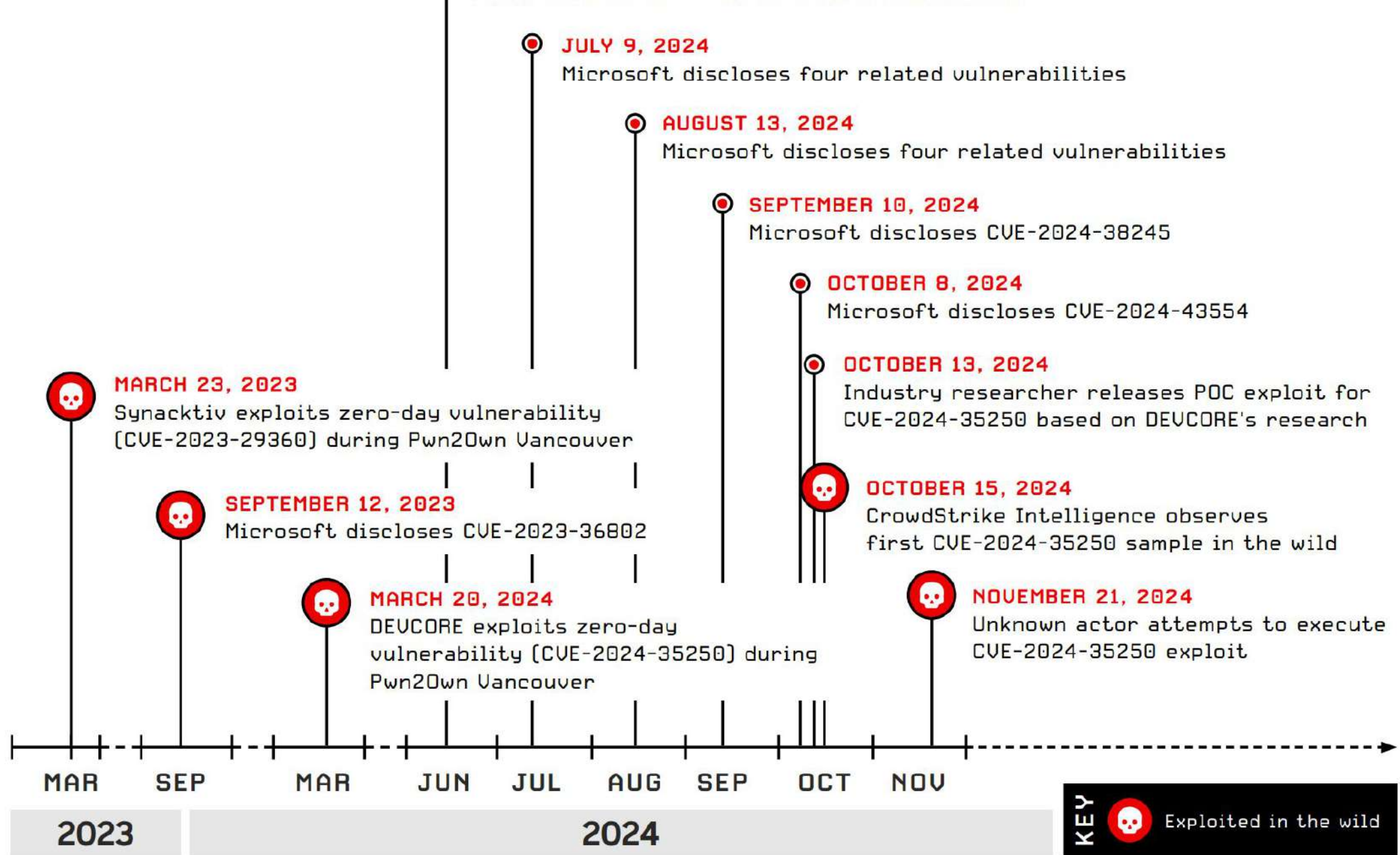
IOT device commonly exploited

- Netcore Netis Router
- Wifi P2P GoAhead Cameras
- Zyxel Firewalls and Routers
- TP-Link Archer Routers
- GPON Routers from multiple vendors

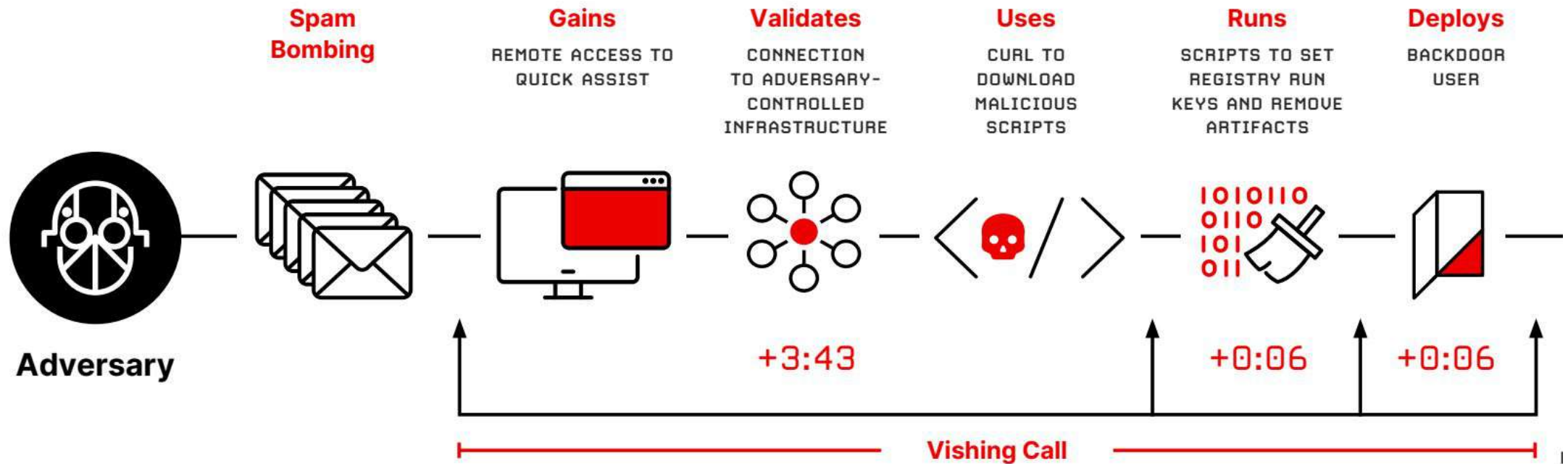
Google Chrome V8 Javascript engine

RCE vulnerability in Microsoft Outlook

Oracle Web logic vulnerabilities to deploy crypto mining malware



















Curly Spider Social Engineering Attacks



New Adversaries

NAMING CONVENTIONS

ADVERSARY	NATION-STATE OR CATEGORY
 BEAR	RUSSIA
 BUFFALO	VIETNAM
 CHOLLIMA	DPRK (NORTH KOREA)
 CRANE	ROK (REPUBLIC OF KOREA)
 HAWK	SYRIA
 JACKAL	HACKTIVIST
 KITTEN	IRAN
 LEOPARD	PAKISTAN
 LYNX	GEORGIA
 OCELOT	COLOMBIA
 PANDA	PEOPLE'S REPUBLIC OF CHINA
 SAIGA	KAZAKHSTAN
 SPHINX	EGYPT
 SPIDER	eCRIME
 TIGER	INDIA
 WOLF	TURKEY



Nepal: Cybersecurity Stats



The background of the slide features a complex digital aesthetic. It includes vertical columns of binary code (0s and 1s) in red and white. Overlaid on this are several bar charts: one with green bars on the left and another with red bars on the right. A white line graph with a downward trend is also visible. At the bottom, a blurred city skyline at night is shown. Various binary sequences like '0 10 1 0' and '10 1 0' are scattered throughout the image.

Digital Transformation



39M cellular mobile connection (132% of total population)



80.5% of mobile connection as broadband (3G, 4G)



15.5M millions individuals using internet



14.3 Million Social media users (48% of total population)



Online penetration above 55%



Median fixed internet download speed: 70.94 Mbps



Rapid adoption of digital services (Digital payments, eCommerce)



Business as well as government embracing digital. (Nagarik App, Online Password, Tax systems and more)

Policy and Regulations

ETA 2063/ The Privacy Act 2075

National Cyber security Policy 2080

National Cyber security Center Established

IT/Cybersecurity Bill in draft

Regulatory bodies

- NTA (Cyber security Byelaw 2077)
- NIA
- NRB

Key Cybersecurity Threats (Nepal)



SURGE IN
PHISHING
CAMPAIGNS



MALWARE
ATTACKS
(RANSOMWARE)



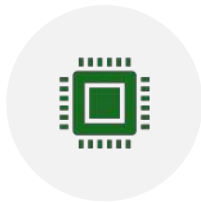
WEBSITE
DEFACEMENT



DATA BREACH



FINANCIAL FRAUD



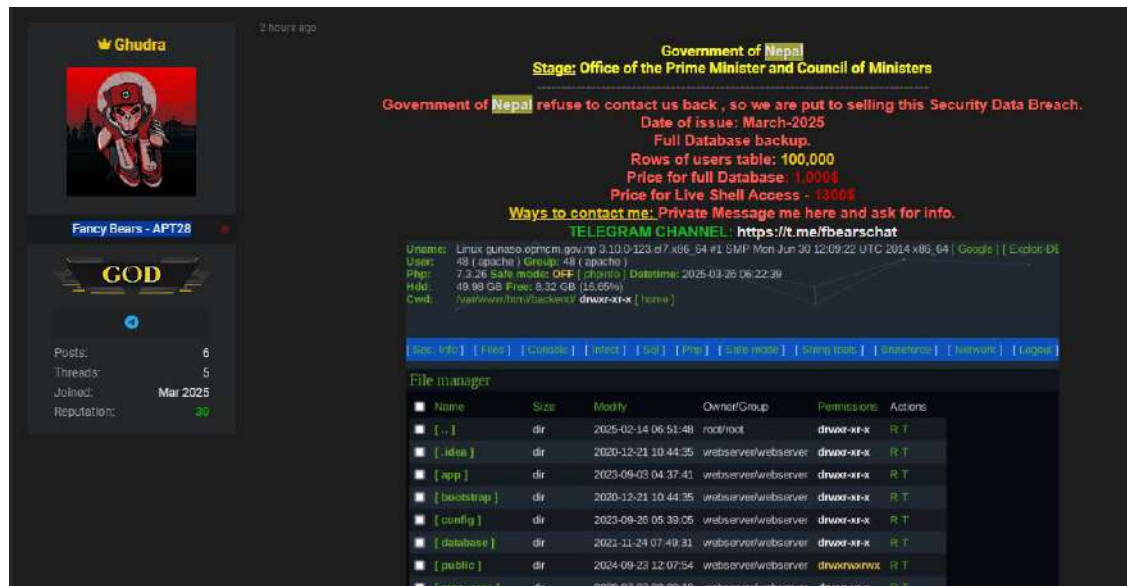
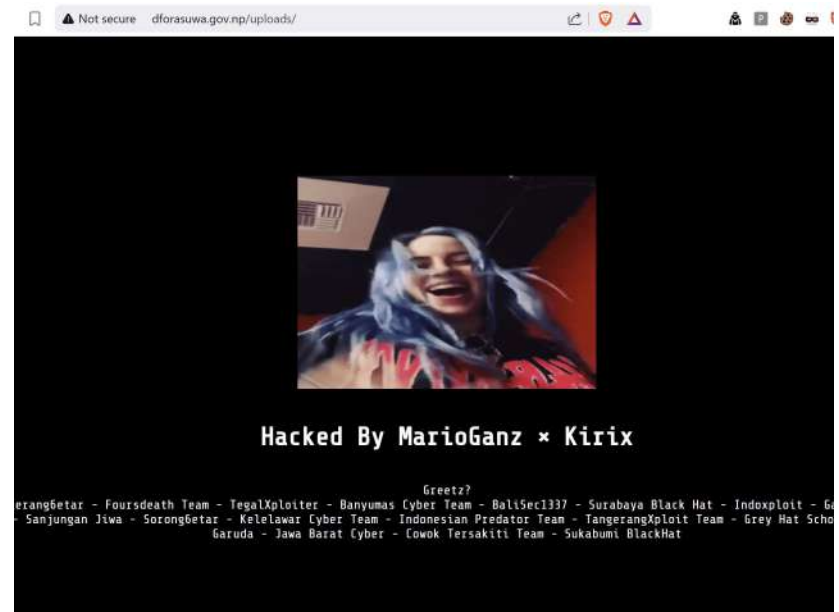
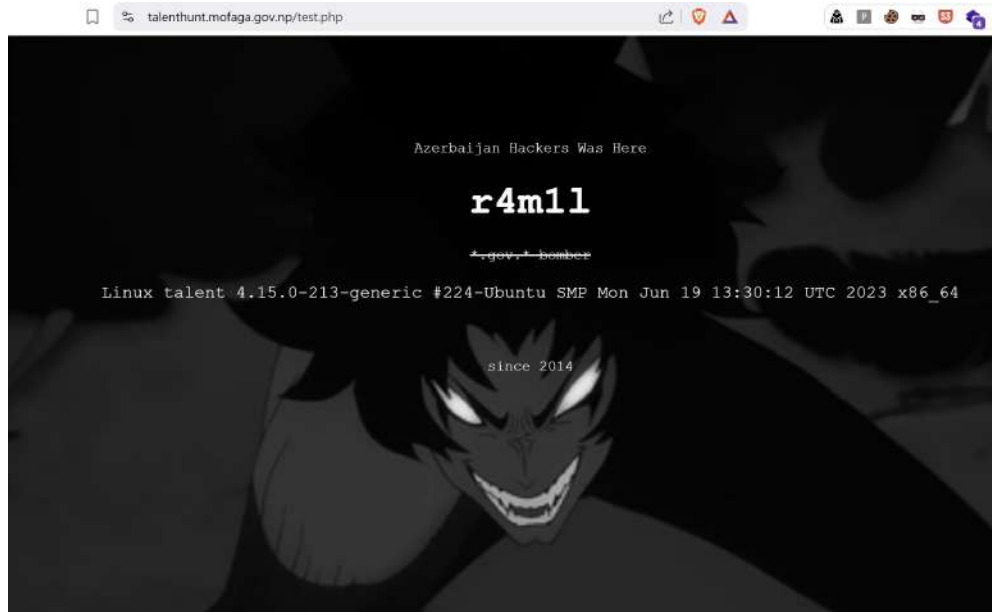
SOCIAL
ENGINEERING (VIA
SOCIAL MEDIA)



DDOS ATTACKS

Key Incidents (Nepal)

Date	Target	Attack Type	Impact Summary
2017	Multiple government websites defacement	Website defacement/data leak	Threatened data exposure
2017	Class A Bank SWIFT Transfer	User compromise	Fund transfer to foreign account
2020	Food Delivery & ISP Data breach	Data breach/domain intrusion	~50k user records leaked; threatened additional bodies
2023	Government Servers	DDoS attack	~1,500 gov. sites offline; airport disruption
2024	Government servers	DDoS reattack	Hundreds of websites down
2025	Hello Sarkar (PMO)	Data breach	PII leaked/sold on darkweb
2020-		Rise in data breach	Multiple org on Darkweb



Website Defacement: stats

NOTIFIER DOMAIN

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date :

Total notifications: **5,012** of which **851** single ip and **4,161** mass defacements

Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

L - IP address location

★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2025/05/22	IOxtOx			M		www.jayakishan.com.np/ioxtox.php	Linux	mirror
2025/05/22	IOxtOx	H	M			www.lalupatetravels.com.np	Linux	mirror
2025/05/19	DimasHxR			M		himalayanrangetreks.com.np/a.html	FreeBSD	mirror
2025/05/19	DimasHxR					hrworldservice.com.np/a.html	FreeBSD	mirror
2025/05/19	DimasHxR			M		karmavahandicraft.com.np/a.html	Linux	mirror
2025/05/19	Mr. BDKR28			M		titankitchen1.pramsoft.com.np/...	Linux	mirror
2025/05/19	Mr. BDKR28			M		ugc.com.np/BDKR28.txt	Linux	mirror
2025/05/19	Mr. BDKR28			M		cafe.pramsoft.com.np/BDKR28.txt	Linux	mirror
2025/05/13	Mr. BDKR28					mountech.com.np/a.htm	Linux	mirror
2025/05/09	CaptainSmok3r	H	M	R		nepalgas.com.np	FreeBSD	mirror
2025/04/29	ynR !					affiliate.bizbazar.com.np/ynr...	Linux	mirror
2025/04/29	ynR !			M		chatbot.bizbazar.com.np/ynr.html	Linux	mirror
2025/04/29	ynR !			M		survey.bizbazar.com.np/ynr.html	Linux	mirror
2025/04/17	Simsimi				R 	www.dryadavbhatta.com.np/image...	Linux	mirror
2025/04/14	AnonSec Team			M		www.nap.com.np/ez.php	Linux	mirror
2025/04/14	F4st~03			M		hariyaliabhan.com.np/y.txt	Linux	mirror
2025/04/14	F4st~03			M		sarbodaya.com.np/y.txt	Linux	mirror
2025/04/14	F4st~03			M		sbc.com.np/y.txt	Linux	mirror
2025/04/14	ReflinP			M		ankitrawal.com.np/index2.html	Linux	mirror
2025/04/14	SMoker666	H				medcare.com.np	Linux	mirror
2025/04/09	VenoRyan			M		politics.manirajkatuwal.com.np...	Linux	mirror
2025/04/09	VenoRyan			M		ribeshbasnet.com.np/veno.htm	Linux	mirror
2025/04/09	KAKEGURAI			M		aaviss.com.np/ind.html	Linux	mirror
2025/04/07	/Rayzky_					admaxconsultancy.com.np/yea.html	Linux	mirror
2025/04/07	/Ravzkyv			M		www.nnlb.com.np/lovv.html	Linux	mirror

NOTIFIER DOMAIN

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date :

Total notifications: **2,370** of which **512** single ip and **1,858** mass defacements

Legend:




H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

L - IP address location

★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2025/04/23	CaptainSmok3r	H		R		★ www.dhm.gov.np	Linux	mirror
2025/04/16	Error People Squad					★ brhospital.bagamati.gov.np/aer...	Linux	mirror
2025/04/11	CaptainSmok3r	H				★ naflqml.gov.np	Unknown	mirror
2025/04/07	/Rayzky_	H	M			★ phd.p2.gov.np	Linux	mirror
2025/02/20	CaptainSmok3r	H		R		★ dls.gov.np	Unknown	mirror
2025/02/19	Cyb3r_Drag0nz_Team	H	M			★ cdcpalpa.gov.np	Linux	mirror
2025/02/19	Cyb3r_Drag0nz_Team	H	M			★ idokanchanpur.sudurpashchim.go...	Linux	mirror
2025/02/18	rizky07			M		★ akcpalpa.gov.np/rizky.htm	FreeBSD	mirror
2025/02/18	rizky07			M		★ tanahun.akc.gov.np/rizky.htm	Linux	mirror
2025/02/18	rizky07			M		★ bhajpur.akc.gov.np/rizky.htm	FreeBSD	mirror
2025/02/18	rizky07			M		★ dolpa.akc.gov.np/rizky.htm	FreeBSD	mirror
2025/02/18	rizky07			M		★ palpa.akc.gov.np/rizky.htm	FreeBSD	mirror
2025/02/18	rizky07			M		★ salyan.akc.gov.np/rizky.htm	FreeBSD	mirror
2025/02/18	Mr.Kro0oz.305	H	M			★ khaptadnationalpark.gov.np	Linux	mirror
2025/02/13	ynR !					★ dfobhojpur.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfodhankuta.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfogaighat.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfokhotang.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfomorang.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfojhapa.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfookhaldhunga.koshi.gov.np/yn...	Unknown	mirror
2025/02/13	ynR !			M		★ dfosankhuwasabha.koshi.gov.np/...	Unknown	mirror
2025/02/13	ynR !			M		★ dfoilam.koshi.gov.np/ynr.html	Unknown	mirror
2025/02/13	ynR !			M		★ dfosolukhumbu.koshi.gov.np/ynr...	Unknown	mirror
2025/02/13	ynR !			M		★ dfosunsari.koshi.gov.np/ynr.html	Unknown	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30




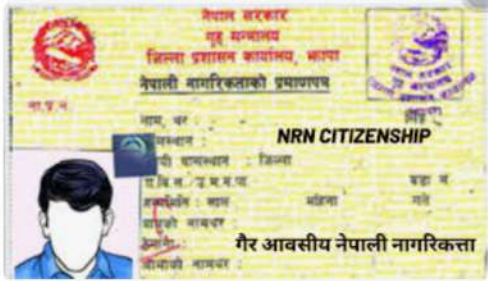
DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some






Data on Internet

Google real nepali citizenship

All Images News Videos Books Maps Finance More Tools Saved

Nrn card Citizenship status National identity card Lost citizenship certificate Non resident nepali Bara

The Record Nepal
Discriminatory citizenship laws ...

The Record Nepal
Unequal citizens - The Record

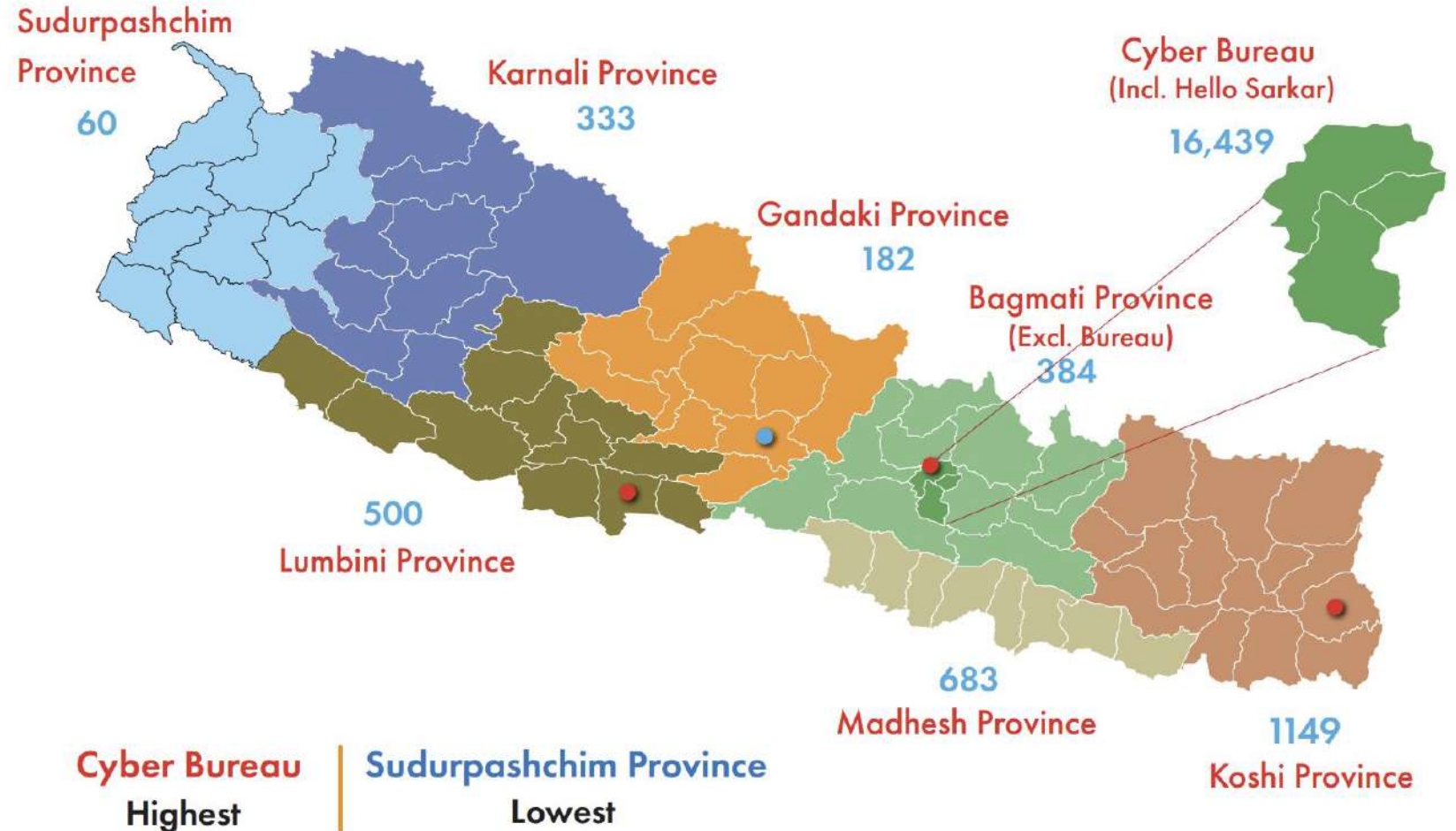
The Kathmandu Post
Bhumika receives citizenship under 'O ...

Corporate Lawyer Nepal
How to obtain NRN citizenship in Nepal ...

Nepal Police Cyber crime stats FY80/81

No. of Cases Registered by Provinces

Total Application: **19,730**



119% Rise from last FY

Victim

Total Victim: 19,730



253
Boys



382
Girls



8,745
Women



9,583
Men



767
LGBTQI+

Medium of Cyber Crime



16,096
Facebook
(Incl. Messenger)



1114
Instagram



981
WhatsApp



690
TikTok



376
Esewa



117
Email



69
Youtube



21
Viber



15
IMO



14
Twitter



13
Website Hacking



224
Other

FY 2081/82 Stats



Around 15k cases till now



Telegram related Complain in
rise



Rise in Whatsapp related
complaints

Challenges Faced by Nepal

- Limited cybersecurity Awareness
- Skilled Professional Shortage
- Budget Constraints
- No proper centralized National level CERT
- No mandatory incident reporting
- Fragmented policies
- Insufficient public-private-academic coordination





Few Insights

Exposed devices,
services and port

Vulnerable devices



IP observed in
Malicious Activities



Sensitive information
leaking online

Top Vulnerabilities:



Exposed services

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | country:NP port:161 | Account

TOTAL RESULTS: 8,171

TOP CITIES

Kathmandu	6,822
Pokhara	247
Bharatpur	216
Pātan	157
Butwāl	101
More...	

TOP ORGANIZATIONS

Nepal Telecommunications Corporation	3,196
Internet Service Provider	493
Mercantile Communications Pvt. Ltd	376
Mercantile Communications Pvt Ltd	313
VIA NET COMMUNICATION LTD	298
...	

View Report | Download Results | Historical Trend | View on Map | Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

11[REDACTED].189
Internet Service Provider
Nepal, Kathmandu
2025-06-11T13:52:18.985101

SAOP:
Versions:
3
Engine Boots: 83
EngineID Data: 0000000030070ea1a9da904
Enterprise: 9
Engine Time: 370 days, 3:27:42

1[REDACTED].26
Nepal Telecommunications Corporation
Nepal, Pātan
2025-06-11T13:52:08.977879

SAOP:
Versions:
3
Engine Boots: 6
EngineID Data: 000000003006c310e265e0
Enterprise: 9
Engine Time: 1072 days, 6:29:28

16[REDACTED].203
SUBISU_Corporate_Food
Nepal, Kathmandu
2025-06-11T13:47:36.140108

SAOP:
Versions:
3
EngineID Format: text
Engine Boots: 0
EngineID Data: 00003a8c04
Enterprise: 10658



Set-Cookie: 55-ST-262-f1-f1665754014=1; path=/

222

More...

More...

Q Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access](#)

database	eol-product
----------	-------------

```
MySQL:
Protocol Version: 10
Version: 5.7.44
Capabilities: 65535
Server Language: 8
Server Status: 2
Extended Server Capabilities: 49663
Authentication Plugin: mysql_native_password
```

2025-06-11T14:02:3

2025-06-11T11:33:2

database	eol-product
----------	-------------

```
MySQL:
Protocol Version: 10
Version: 5.7.36
Capabilities: 65535
Server Language: 8
Server Status: 2
Extended Server Capabilities: 49663
Authentication Plugin: mysql_native_password
```

level2-oplocks, lock-and-read

2025-06-11T10:34:5

database

```
MySQL:
  Protocol Version: 10
  Version: 8.0.33
  Capabilities: 65535
  Server Language: 255
  Server Status: 2
```

TOTAL RESULTS

622

TOP CITIES

Siddharthanagar	462
Kathmandu	128
Pātan	6
Bharatpur	5
Butwāl	5

[More...](#)

TOP PORTS

80	82
81	18
443	12
82	10
8080	7

[More...](#)

TOP ORGANIZATIONS

[View Report](#)[Download Results](#)[Historical Trend](#)[View on Map](#)[Advance](#)**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)**124.41.213.170** [↗](#)170.213.41.124.dynamic.wlink.co
m.np[Static subnet for enterprise at BTW-
BHW](#)

Nepal, Siddharthanagar

HTTP/1.1 200 OK

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

Content-Type: text/html

X-Content-Type-Options: nosniff

Date: Wed, 11 Jun 2025 21:21:44 GMT

ETag: 1725461428

Content-Length: 481

X-XSS-Protection: 1; mode=block

Last-Modified: Wed, 09 Dec 2020 06:45:20 GMT

Connection: Kee...

**103.41.173.18** [↗](#)[VIA NET COMMUNICATION LTD](#)

Nepal, Kathmandu

HTTP/1.1 200 OK

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

Content-Type: text/html

X-Content-Type-Options: nosniff

Date: Wed, 11 Jun 2025 20:23:05 GMT

ETag: 1739961773

Content-Length: 481

X-XSS-Protection: 1; mode=block

Last-Modified: Mon, 19 Jun 2023 06:07:25 GMT

Connection: Kee...



Facet Analysis

country:NP org:"WorldLink Communicatio

vuln.verified



// TOTAL: 9,011

**cve-2020-0796**

12

cve-2015-1635

3

cve-2021-31206

3

cve-2021-31207

3

cve-2021-34473

3

cve-2021-34523

3

ms15-034

3

cve-2019-0708

2

cve-2024-23897

2

cve-2021-26855

1

cve-2021-26857

1

cve-2021-26858

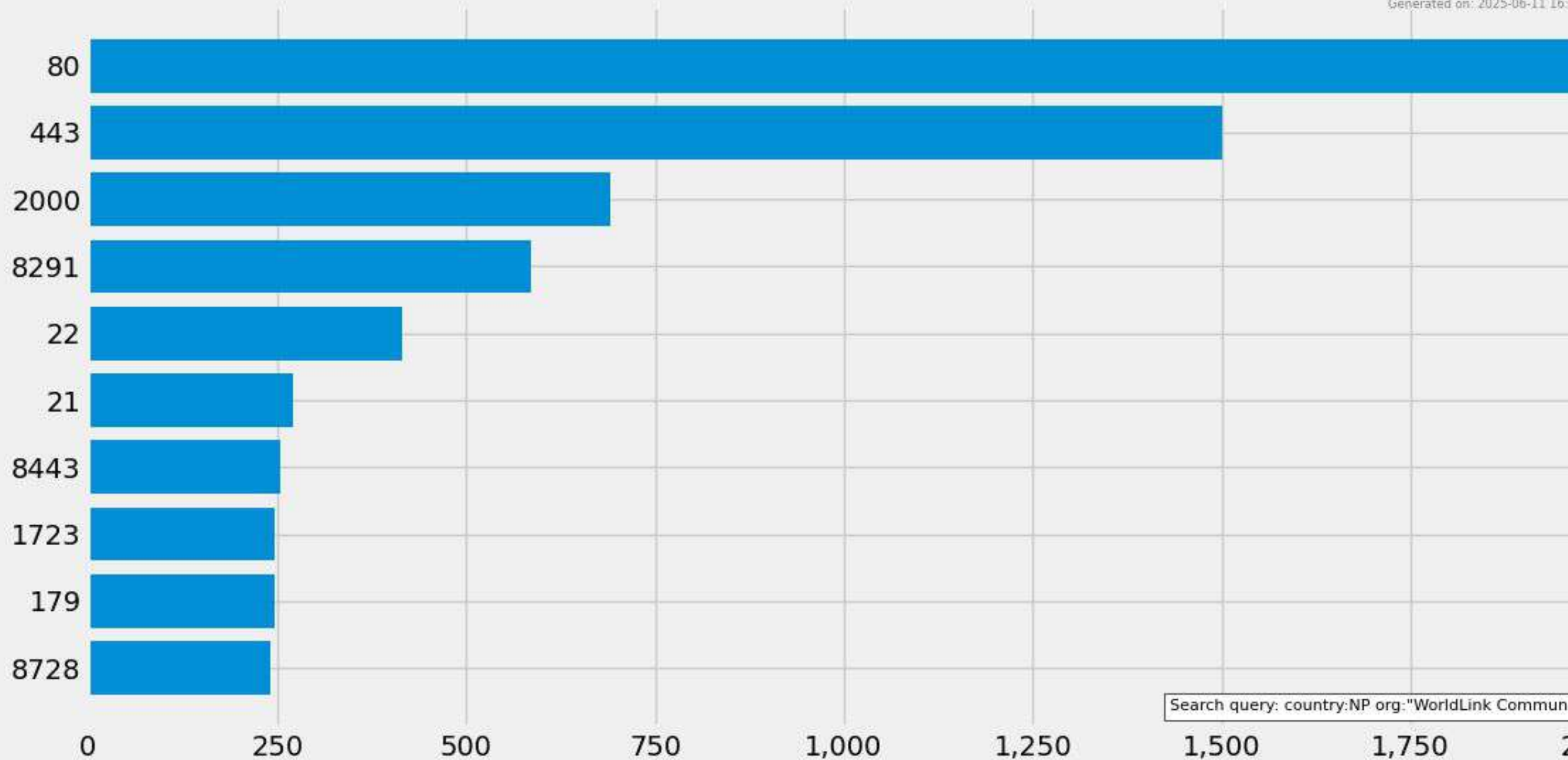
1

cve-2021-27065

1

Top 10 Values for: port

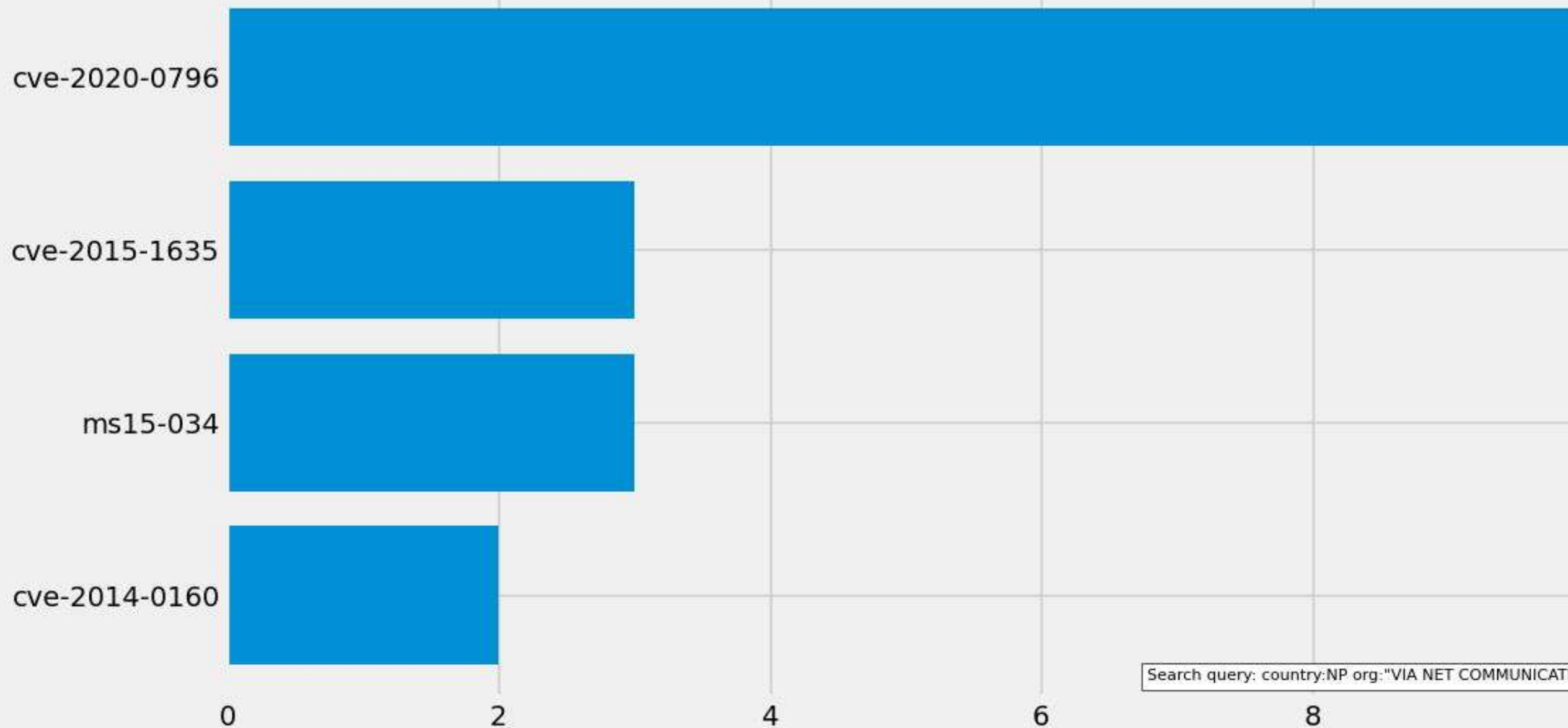
Generated on: 2025-06-11 16:30



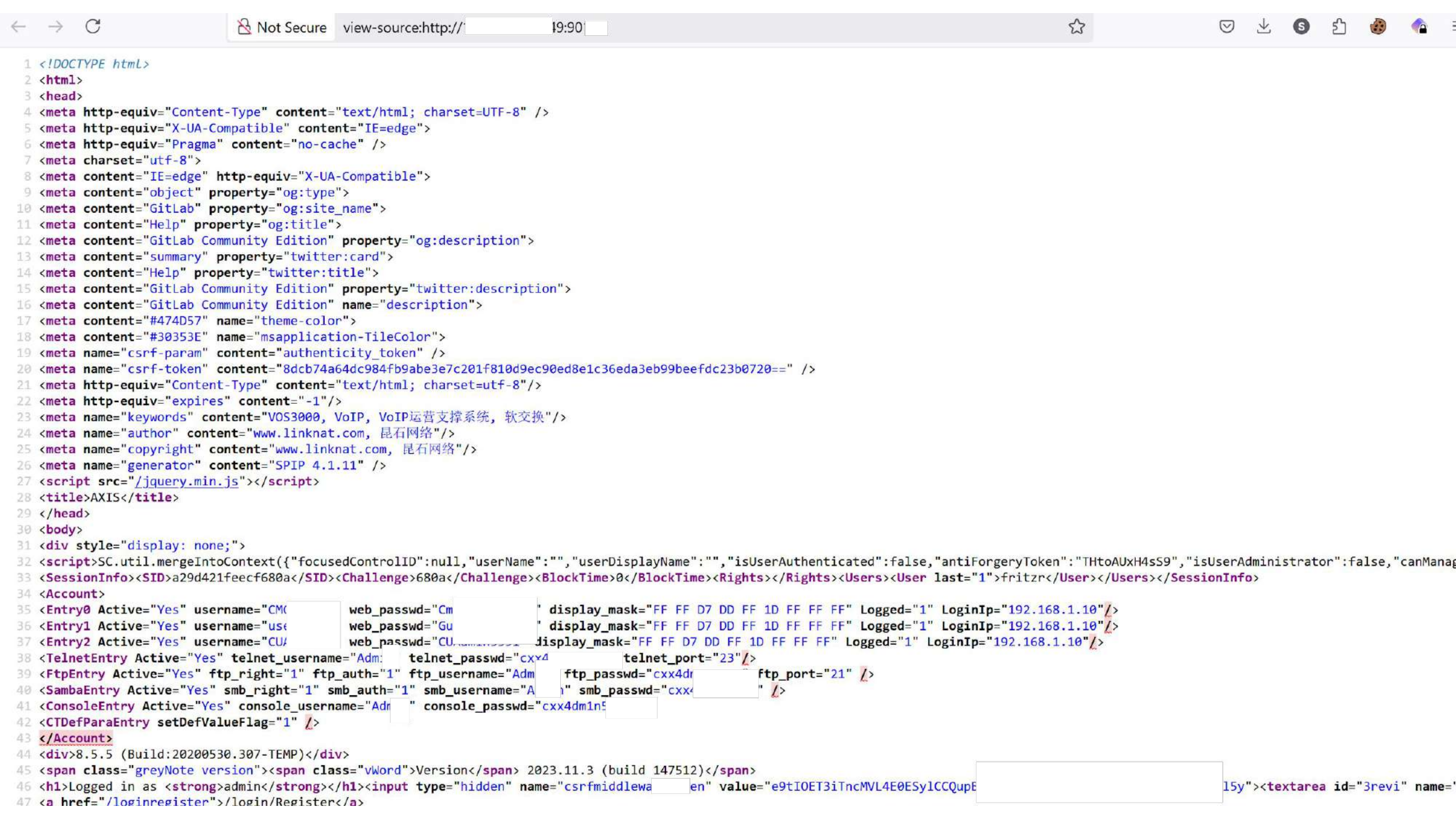
Search query: country:NP org:"WorldLink Commun

Top 10 Values for: vuln.verified

Generated on: 2025-06-11 16:30



Search query: country:NP org:"VIA NET COMMUNICAT






LIVE CYBER THREAT MAP



2,316,513 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS



ATTACKS  Current rate **4**  

-  Cross-Site Scripting Over HTTP
09:36:28 Canada → Canada
-  Cross-Site Scripting Over HTTP
09:36:28 Canada → Canada
-  Cross-Site Scripting Over HTTP
09:36:27 Canada → Canada
-  PDF Containing Obfuscated Name O...
09:36:27 Canada → Canada

-  PDF Containing Obfuscated Name O...
09:36:27 Canada → Canada
-  Cross-Site Scripting Over HTTP
09:36:27 Canada → Canada



DON'T WAIT TO
PREVENTION ST.

TOP TARGETED CO

Highest rate of attack
in the last day.

-  Ethiopia
-  Nepal
-  Indonesia
-  Mongolia
-  Vietnam




TOP TARGETED IND

Highest rate of attack
in the last day.

-  Education
-  Government
-  Healthcare

TOP MALWARE TYPE

Malware types with the
highest impact in the last day.

-  Mobile
-  Phishing
-  Adware

Attack Trends: Nepal



LIVE CYBER THREAT MAP

TOTAL ATTACKS DETECTED

10,155,519

ATTACK STATISTICS



RECENT DAILY ATTACKS

- Phishing Campaign - Toronto**
🇨🇦 CA • Jan 01, 2025
- Banking System Exploitation - Sao Paulo**
🇧🇷 BR • Jan 01, 2025
Exploit Kit
- Malware Distribution - Seoul**
🇰🇷 KR • Jan 01, 2025
- Financial Services Attack - Dubai Bank**
🇦🇪 AE • Jan 01, 2025
Malware
- Tech Company Data Theft - Paris**
🇫🇷 FR • Jan 01, 2025
Dataexfil



HIGHEST RATE OF ATTACK ORIGINS

United States	60.48%
China	14.15%
India	10.78%
Germany	9.19%
United Kingdom	5.39%

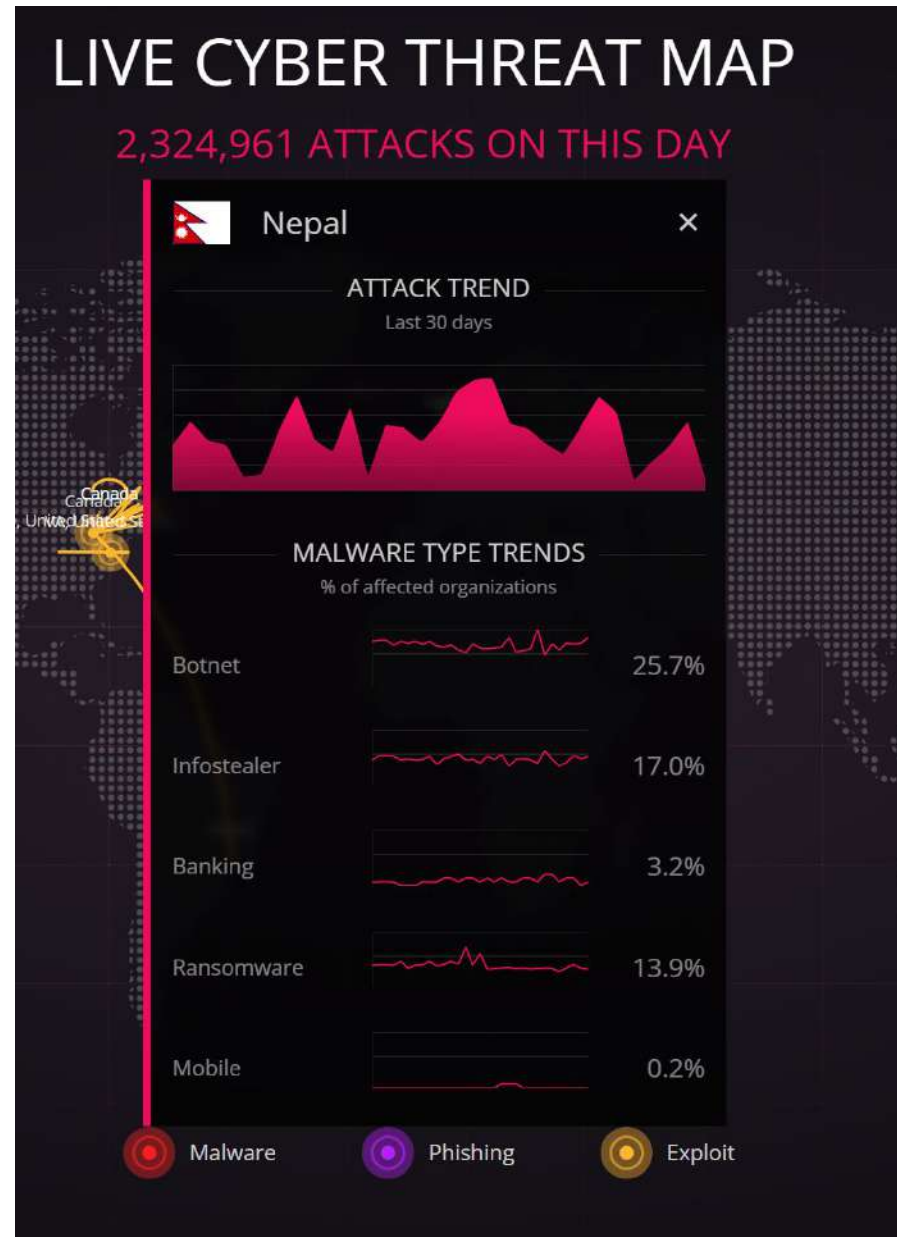
HIGHEST RATE OF ATTACK TARGETS

United States	42.5%
China	28.7%
United Kingdom	14.6%
Morocco	14.2%

TOP ATTACK CATEGORIES

Bruteforce	47.88%
Scanning Host	15.15%
Malware	15.01%
Phishing	12.85%
Malvertising	3.69%
Trojan	3.09%
Denial of Service	2.46%

Attack Types



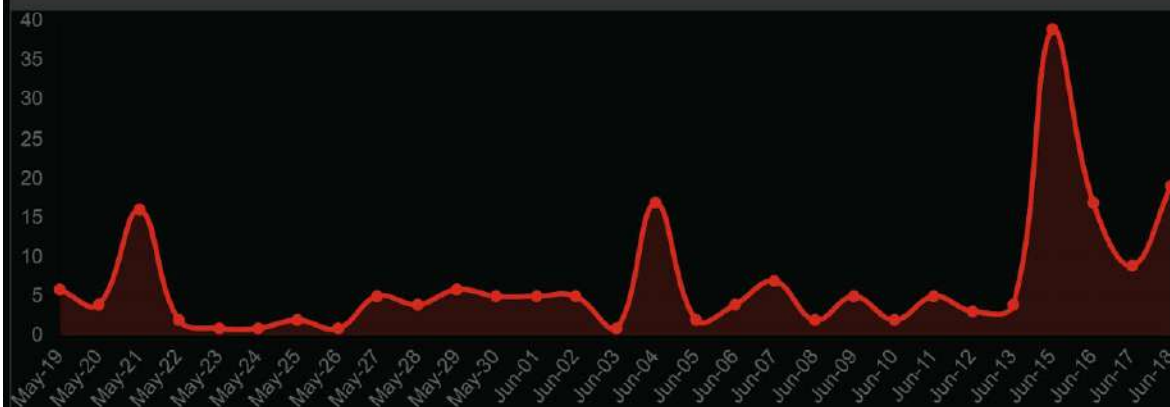
Nepal



Ransomware

TIME PERIOD: ☐ Last week ☒ Last month

Top - Ransomware IN THE LAST MONTH



Top - Ransomware IN THE LAST MONTH

1	Trojan-Ransom.WIN32.Phny.a	31.16%
2	Trojan-Ransom.Win32.Gen.abxr	11.06%
3	Trojan-Ransom.Win32.Blocker.jaic	9.05%
4	Trojan-Ransom.Win32.PornoBlocker.vho	7.04%
5	Trojan-Ransom.Win32.PornoBlocker.pef	6.53%
6	Trojan-Ransom.MSIL.Blocker.gen	5.53%
7	Trojan-Ransom.Win32.Foreign.vho	5.03%
8	Trojan-Ransom.Win32.Convagent.gen	4.52%
9	Trojan-Ransom.Win32.Encoder.adlb	2.51%
10	Trojan-Ransom.Win32.Blocker.gfeq	2.51%

Nepal



Vulnerability Scan

TIME PERIOD: ☐ Last week ☒ Last month

Top - Vulnerability Scan IN THE LAST MONTH



Top - Vulnerability Scan IN THE LAST MONTH

1	Exploit.Win32.Convagent.gen	51.39%
2	Exploit.MSIL.ChecksumController.gen	6.94%
3	Exploit.MSOffice.CVE-2017-11882.gen	6.94%
4	Exploit.RTF.CVE-2018-0802.gen	2.78%
5	Exploit.MSWord.Agent.gen	2.78%
6	Exploit.RTF.CVE-2017-11882.gen	2.78%
7	Exploit.AndroidOS.Lotoor.cc	2.78%
8	Exploit.Script.Petitpotam.a	2.78%
9	Exploit.Multi.CVE-2020-1472.gen	2.78%
10	Exploit.Win32.CVE-2012-0158.j	2.78%

Recommendations for Strengthening Cybersecurity



MFA Implementation / Identify and Access Management



Regular updates/patches



Periodic Audit / Penetration testing / Risk Assessment



Cyber security awareness and training



Reduce Attack surface exposure / Secure by design principle



Develop a robust vendor management program



Leverage Dark web and threat intelligence



Thank you

References

- https://www.nepalpolice.gov.np/media/filer_public/fd/3e/fd3e1c95-aaa1-41bd-815e-0221254141d4/fy_2080-81_suicide_cyber_crime_-_en.pdf
- <https://datareportal.com/reports/digital-2025-nepal>
- <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf>
- <https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report--cyber-security-report-2025>
- <https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0>
- <https://www.shodan.io/>
- <http://www.zone-h.org/archive>