VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

Practical on Foot printing

By
Dr. Ravi Verma

Contents To Be Discuss

- Foot-Printing Concept
- Types of Foot-Printing
- Information collection through Foot-Printing
- DNS Foot-Printing
- WHOIS Foot-Printing
- Network Foot-Printing
- Email Foot- Printing
- Foot Printing Through Google Search Engine
- Google Hacking Database

Types OF Footprinting

- Passive Footprinting
- Active Footprinting

Information Collected Using Footprinting

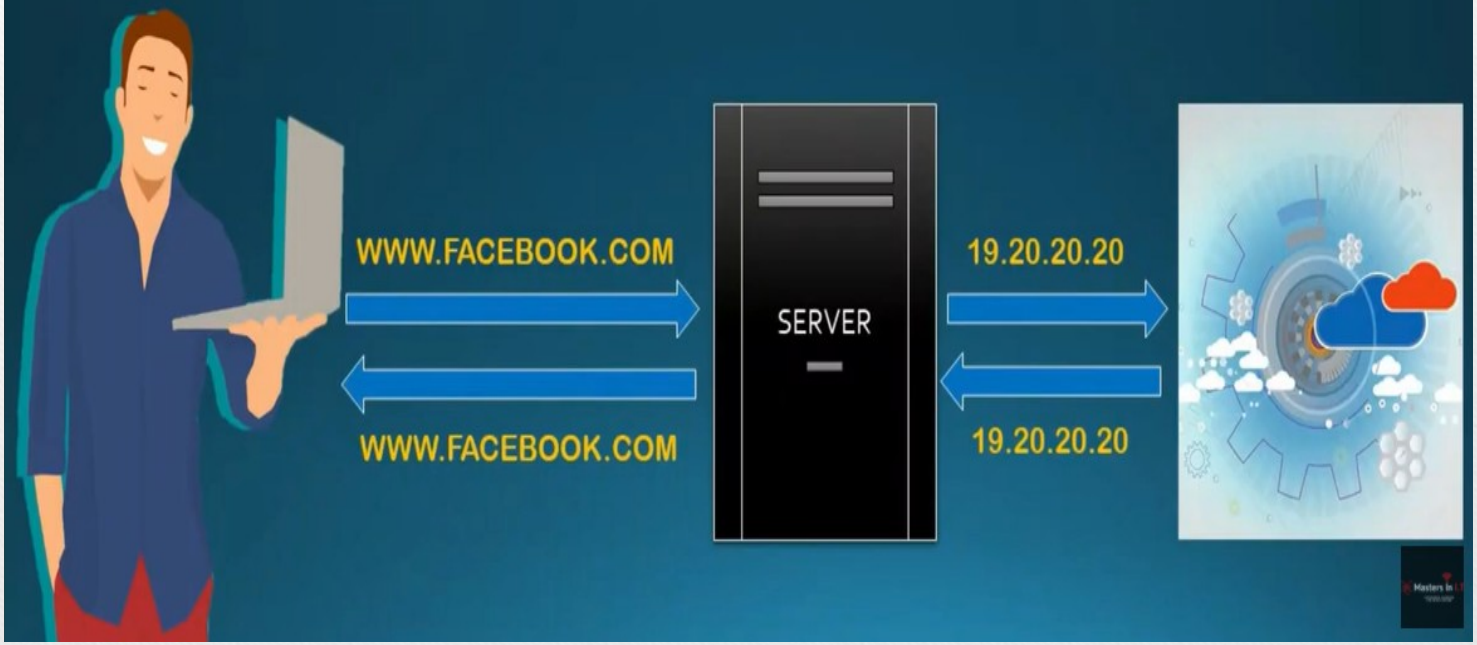
- IP Address
- Employee information
- E-mails
- Domain name
- Employee information
- Phone number
- Discover open ports
- Locate the network range
- Map the network

Types of Footprinting

- Footprinting through Search Engines
- Footprinting through Advance Google Hacking Techniques
- Footprinting through Social Networking Sites
- Footprinting through Websites
- Footprinting through Email
- Footprinting through Competitive Intelligence
- Footprinting through WHOIS
- Footprinting through DNS
- Footprinting through Network
- Footprinting through Social Engineering

DNS FOOTPRINTING

WHAT IS DNS ?


WWW.FACEBOOK.COM
WWW.FACEBOOK.COM
SERVER
19.20.20.20
19.20.20.20

DNS Footprinting

DNS lookup information is helpful to identify a host within a targeted network

RECORD TYPE	DESCRIPTION
A	The host's IP address
MX	Domain's Mail Server
NS	Host Name Server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for the domain
SRV	Service records
PTR	IP-Host Mapping
RP	Responsible Person
HINFO	Host Information
TXT	Unstructured Records

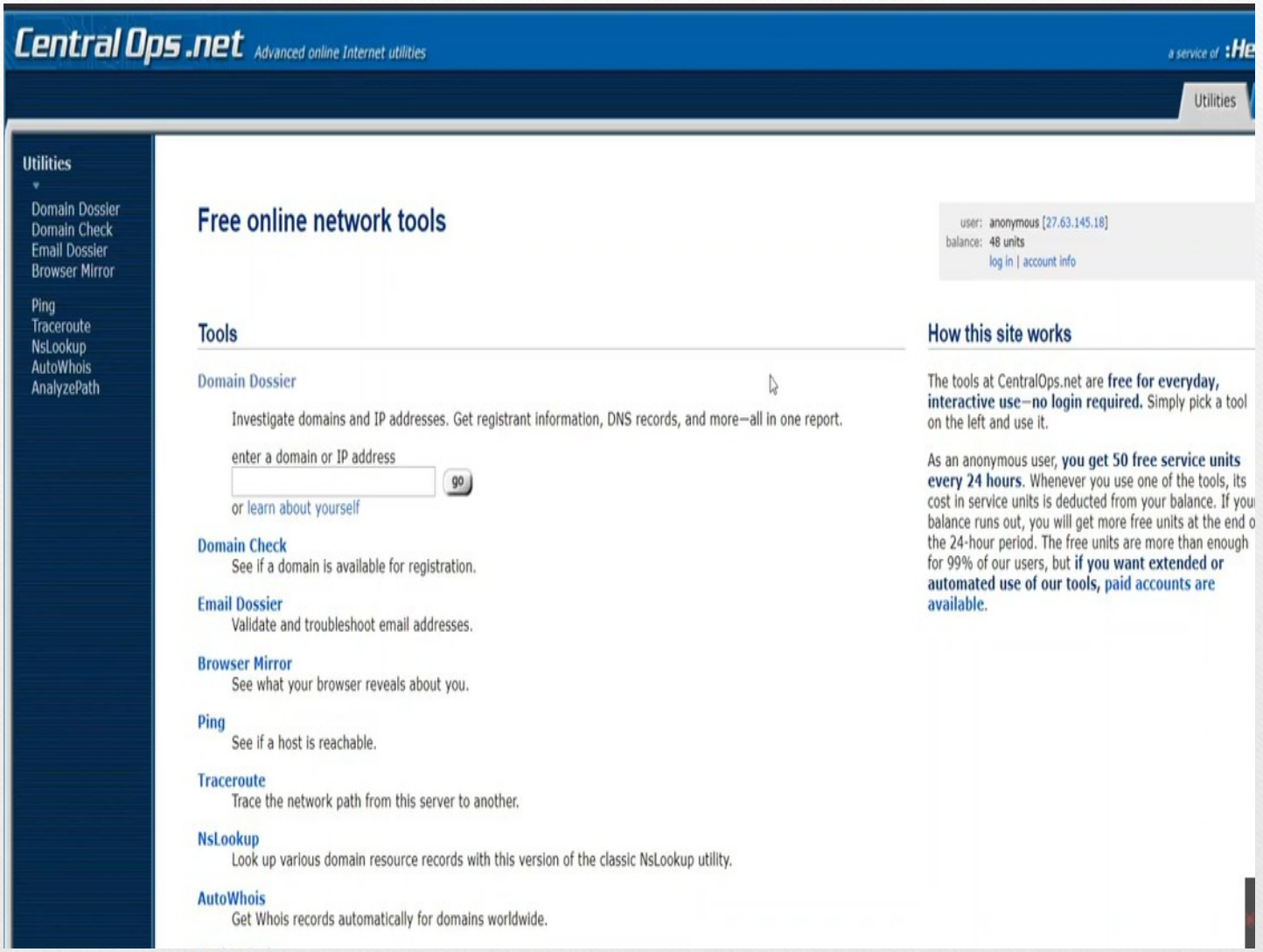
WHOIS Footprinting

"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

Network Footprinting

One of the important types of footprinting is network footprinting.

- Network address ranges
- Hostnames
- Exposed hosts
- OS and application version information
- Patch state of the host and the applications
- Structure of the applications and back-end servers


CentralOps.net
Advanced online Internet utilities
Utilities
Utilities
Domain Dossier
Domain Check
Email Dossier
Browser Mirror
Ping
Traceroute
NsLookup
AutoWhois
AnalyzePath
Free online network tools
user: anonymous [27.63.145.18]
balance: 48 units
log in | account info
Tools
Domain Dossier
Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.
enter a domain or IP address
go
or learn about yourself
Domain Check
See if a domain is available for registration.
Email Dossier
Validate and troubleshoot email addresses.
Browser Mirror
See what your browser reveals about you.
Ping
See if a host is reachable.
Traceroute
Trace the network path from this server to another.
NsLookup
Look up various domain resource records with this version of the classic NsLookup utility.
AutoWhois
Get Whois records automatically for domains worldwide.
How this site works
The tools at CentralOps.net are free for everyday, interactive use—no login required. Simply pick a tool on the left and use it.
As an anonymous user, you get 50 free service units every 24 hours. Whenever you use one of the tools, its cost in service units is deducted from your balance. If you
balance runs out, you will get more free units at the end o
the 24-hour period. The free units are more than enough
for 99% of our users, but if you want extended or automated use of our tools, paid accounts are available.

LookIP.net

IP address lookup and information tool

Home | IP Address Lookup | Website Lookup

IP Lookup Tool

LookIP.net is a free set of tools which use a self-learning automated system based on user input and cross-linked datasources and references. It provides the user with a detailed overview.

With LookIP.net you can find all publicly available information about any specific IP address or website. This enables you to find out the geolocation and owner of an IP address or website, which could be useful for many reasons like security issues and abuse reports.
We are constantly adding more resources to our database. If you have any suggestions, please let us know by filling out our contact form.

Your IP address

27.63.145.18

IP address lookup

Enter an IP address in the box below to locate it and get more details.
Example: 8.8.8.8

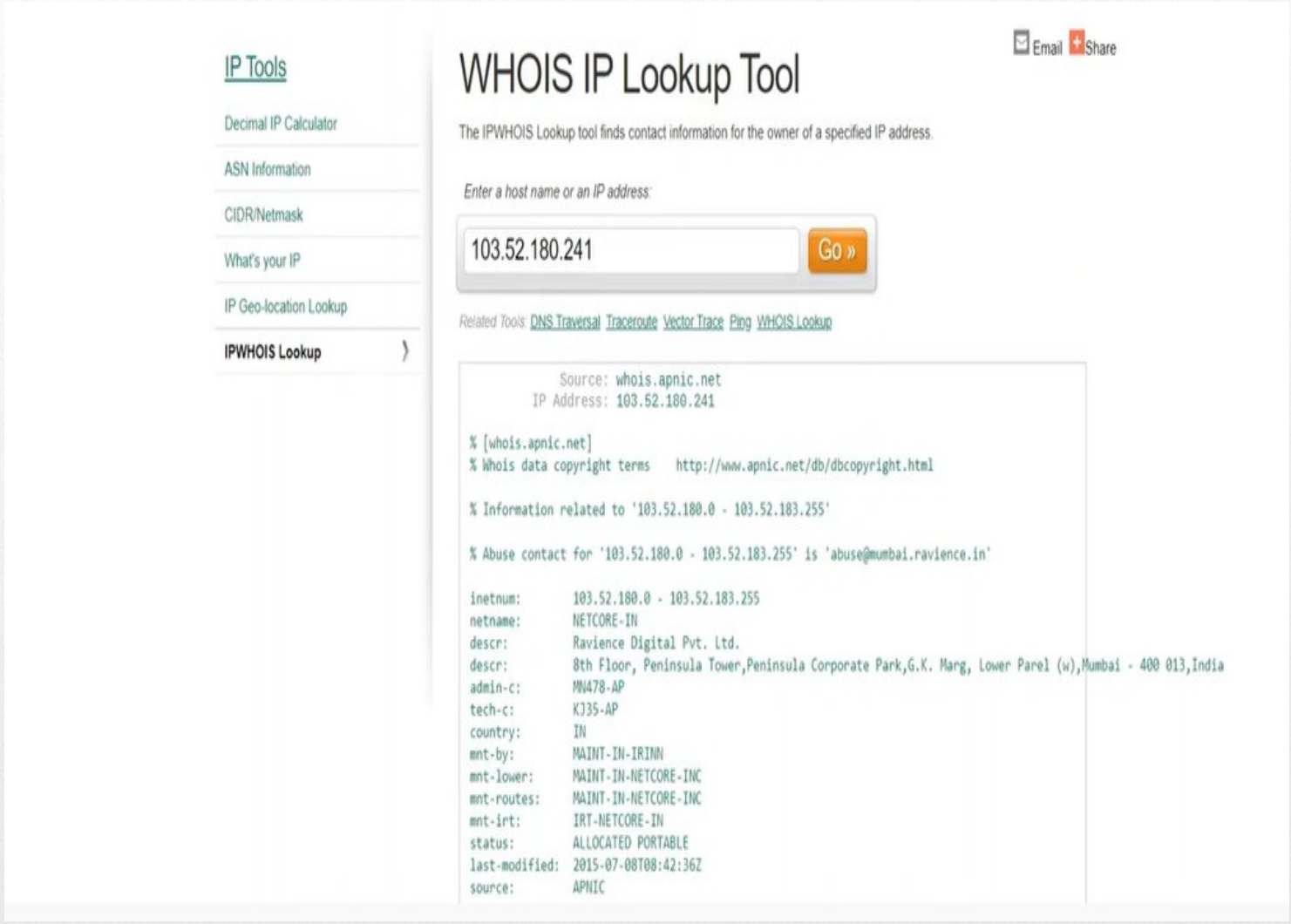
Email Footprinting

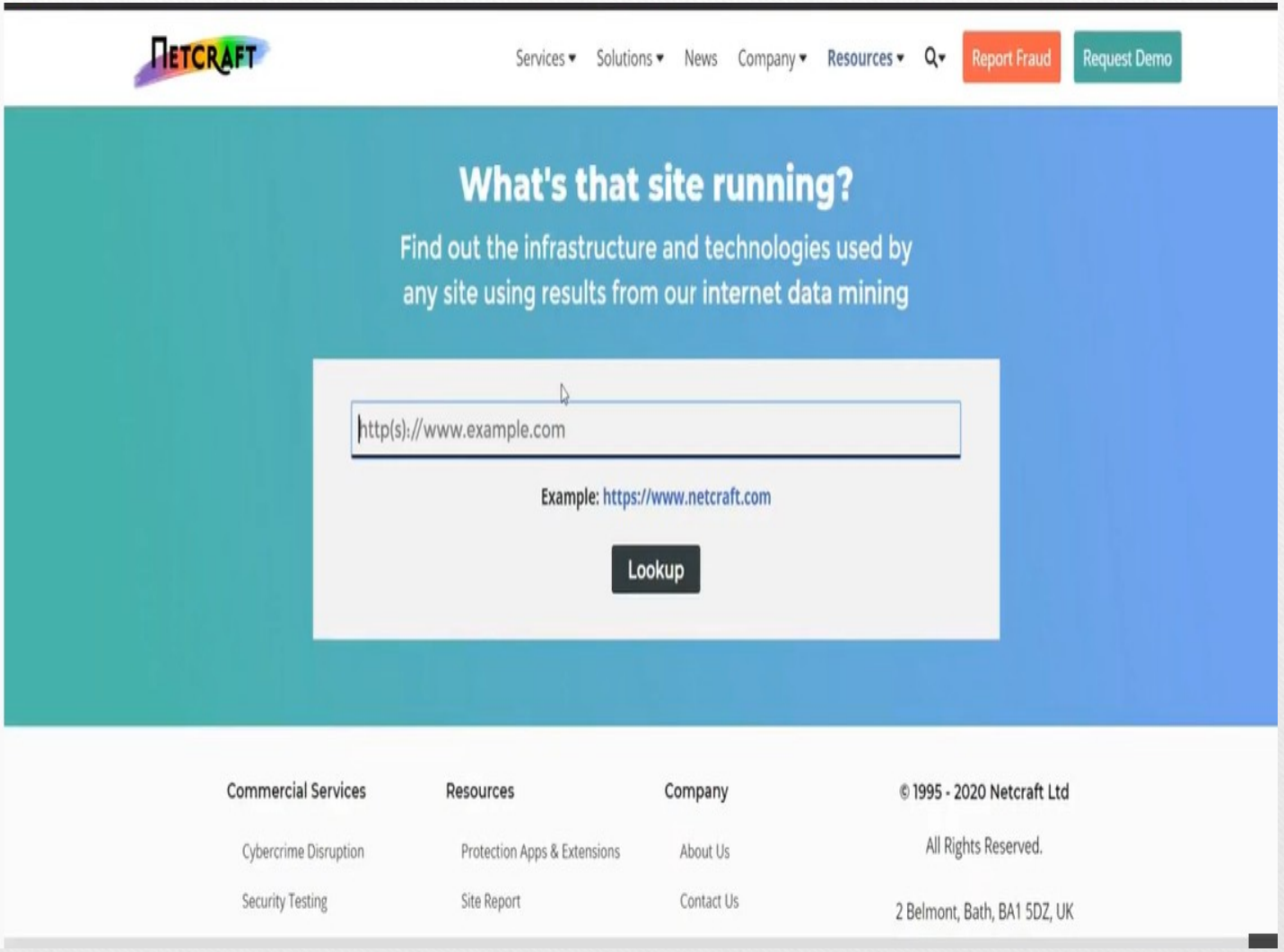
Email is one of the most popular, widely used professional ways of communication which is used by every organization.

Tracing an email using email header can reveal the following information:

- Destination address
- Sender's IP address
- Sender's Mail server
- Time & Date information
- Authentication system information of sender's mail server


REGISTERED USERS: 60,095
neustar // UltraTools
Free Domain, DNS, WHOIS and IP Tools
Email Address
Login
Remember me
Forgot your password?
Home
Domain Health Report
WHOIS+
Monitoring
UltraTools
Statistics
UltraTools Mobile
Create Free Account
Domain Health Report
UltraTools Health Report is your ultimate all-in-one resource for domain name and DNS server health.
• The most comprehensive domain test suite on the web
• Testing results show you details on Parent, Name Server, Start of Authority, MX Record, Mail Server, Web Server, Domain Records, DNSSEC, and IPv6
• Ability to save results and return at a later time
Report Summary
100% FREE
Enter your domain name...
Start »
Tracing Tools
Tracing Tools provide real-time routing information to test the connection to your servers to assist you with your day-to-day system administration tasks. Tools include:
• Ping
• Traceroute
• Vector Trace
• Completely FREE
Learn More »
Neustar DNS Advantage
Manage traffic by location and localize Web content, featuring:
• Origination-Based Routing
• Custom Responses
• Powerful Grouping Capabilities
• Cloud-Based, Hardware-Free
Learn More »
WHOIS Tools
Our WHOIS tools give you the ability to find domain and IP ownership information. Tools include:
• Full WHOIS
• IPWHOIS for IP Addresses
• RWHOIS for RWHOIS lookups
• Completely FREE
Learn More »


IP Tools
Decimal IP Calculator
ASN Information
CIDR/Netmask
What's your IP
IP Geo-location Lookup
IPWHOIS Lookup
Email
Share
WHOIS IP Lookup Tool
The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.
Enter a host name or an IP address:
103.52.180.241
Go »
Related Tools: DNS Traversal Traceroute Vector Trace Ping WHOIS Lookup
Source: whois.apnic.net
IP Address: 103.52.180.241
% [whois.apnic.net]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
% Information related to '103.52.180.0 - 103.52.183.255'
% Abuse contact for '103.52.180.0 - 103.52.183.255' is 'abuse@mumbai.ravience.in'
inetnum: 103.52.180.0 - 103.52.183.255
netname: NETCORE-IN
descr: Ravience Digital Pvt. Ltd.
descr: 8th Floor, Peninsula Tower,Peninsula Corporate Park,G.K. Marg, Lower Parel (w),Mumbai - 400 013,India
admin-c: MN478-AP
tech-c: KJ35-AP
country: IN
mnt-by: MAINT-IN-IRINN
mnt-lower: MAINT-IN-NETCORE-INC
mnt-routes: MAINT-IN-NETCORE-INC
mnt-irt: IRT-NETCORE-IN
status: ALLOCATED PORTABLE
last-modified: 2015-07-08T08:42:36Z
source: APNIC


NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Demo
What's that site running?
Find out the infrastructure and technologies used by any site using results from our internet data mining
http(s)://www.example.com
Example: https://www.netcraft.com
Lookup
Commercial Services
Cybercrime Disruption
Security Testing
Resources
Protection Apps & Extensions
Site Report
Company
About Us
Contact Us
© 1995 - 2020 Netcraft Ltd
All Rights Reserved.
2 Belmont, Bath, BA1 5DZ, UK

- **Footprinting through Search Engines**

  Attackers use search engines to extract information about the target such as technology platforms, employee details, login pages, intranet portals, etc.

- **Finding Company's Public and Restricted Websites**

- **Collect Location Information**

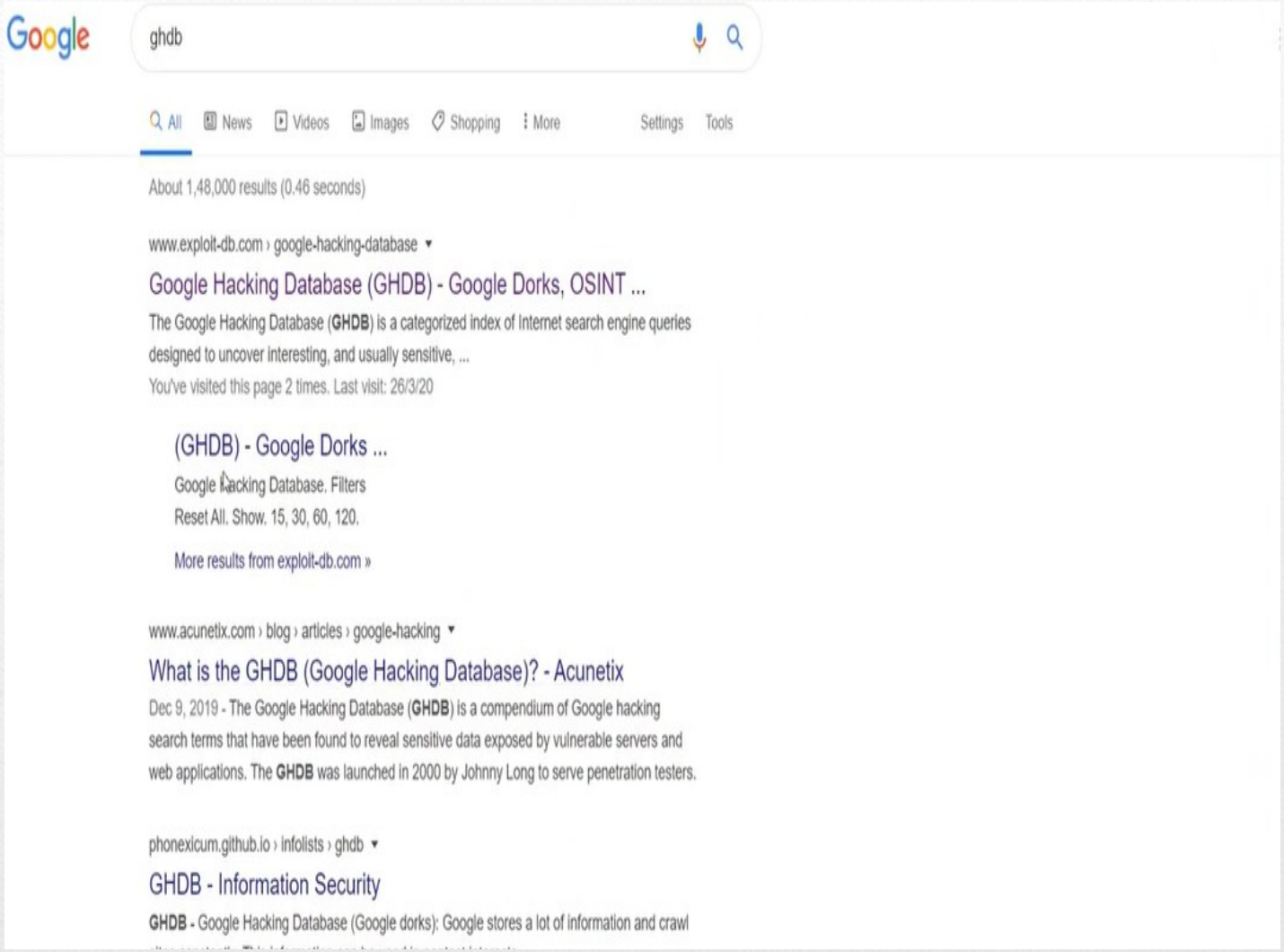
Footprinting using Advanced Google Hacking Techniques

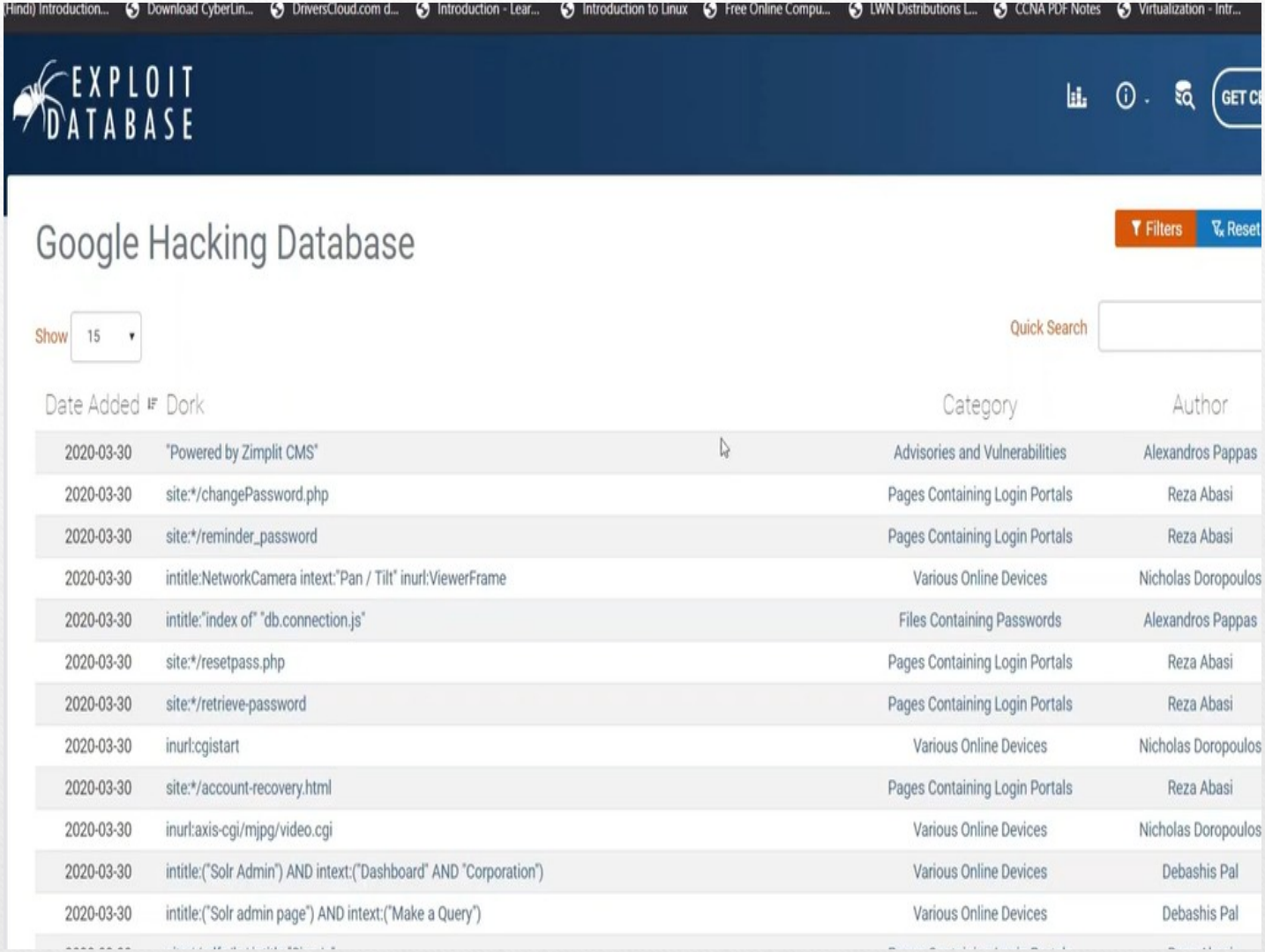
Advanced Search Operator

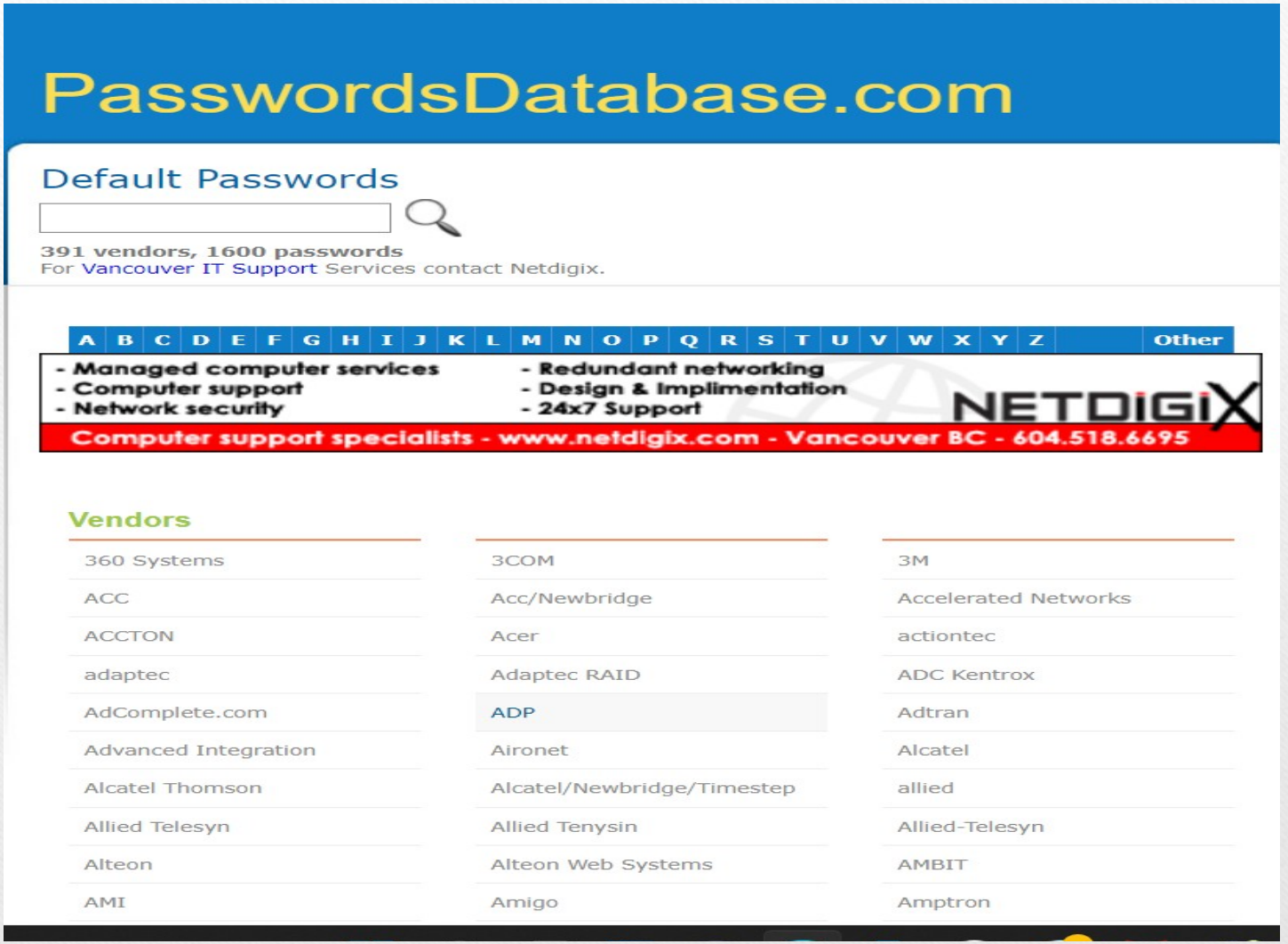
site :	Search for the result in the given domain
related :	Search for Similar web pages
link :	List the websites having a link to a specific web page
allintext :	Search for websites containing a specific keyword
intext :	Search for documents containing a specific keyword
allintitle :	Search for websites containing a specific keyword in the title
intitle :	Search for documents containing a specific keyword in the title

Google Hacking Database (GHDB)

Google hacking database provide the updated information that is useful for exploitation such as footholds, sensitive directories, vulnerable files, error messages and much more.


Google
ghdb
All
News
Videos
Images
Shopping
More
Settings
Tools
About 1,48,000 results (0.46 seconds)
www.exploit-db.com › google-hacking-database
Google Hacking Database (GHDB) - Google Dorks, OSINT ...
The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, ...
You've visited this page 2 times. Last visit: 26/3/20
(GHDB) - Google Dorks ...
Google Hacking Database. Filters
Reset All. Show. 15, 30, 60, 120.
More results from exploit-db.com »
www.acunetix.com › blog › articles › google-hacking
What is the GHDB (Google Hacking Database)? - Acunetix
Dec 9, 2019 - The Google Hacking Database (GHDB) is a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications. The GHDB was launched in 2000 by Johnny Long to serve penetration testers.
phonexicum.github.io › infolists › ghdb
GHDB - Information Security
GHDB - Google Hacking Database (Google dorks): Google stores a lot of information and crawl


(Hindi) Introduction...
Download CyberLin...
DriversCloud.com d...
Introduction - Lear...
Introduction to Linux
Free Online Compu...
LWN Distributions L...
CCNA PDF Notes
Virtualization - Intr...
EXPLOIT DATABASE
GET C
Google Hacking Database
Filters
Reset
Show 15
Quick Search
Date Added
Dork
Category
Author
2020-03-30 "Powered by Zimplit CMS" Advisories and Vulnerabilities Alexandros Pappas
2020-03-30 site:*/changePassword.php Pages Containing Login Portals Reza Abasi
2020-03-30 site:*/reminder_password Pages Containing Login Portals Reza Abasi
2020-03-30 intitle:NetworkCamera intext:"Pan / Tilt" inurl:ViewerFrame Various Online Devices Nicholas Doropoulos
2020-03-30 intitle:"index of" "db.connection.js" Files Containing Passwords Alexandros Pappas
2020-03-30 site:*/resetpass.php Pages Containing Login Portals Reza Abasi
2020-03-30 site:*/retrieve-password Pages Containing Login Portals Reza Abasi
2020-03-30 inurl:cgistart Various Online Devices Nicholas Doropoulos
2020-03-30 site:*/account-recovery.html Pages Containing Login Portals Reza Abasi
2020-03-30 inurl:axis-cgi/mjpg/video.cgi Various Online Devices Nicholas Doropoulos
2020-03-30 intitle:("Solr Admin") AND intext:("Dashboard" AND "Corporation") Various Online Devices Debashis Pal
2020-03-30 intitle:("Solr admin page") AND intext:("Make a Query") Various Online Devices Debashis Pal



PasswordsDatabase.com

Default Passwords

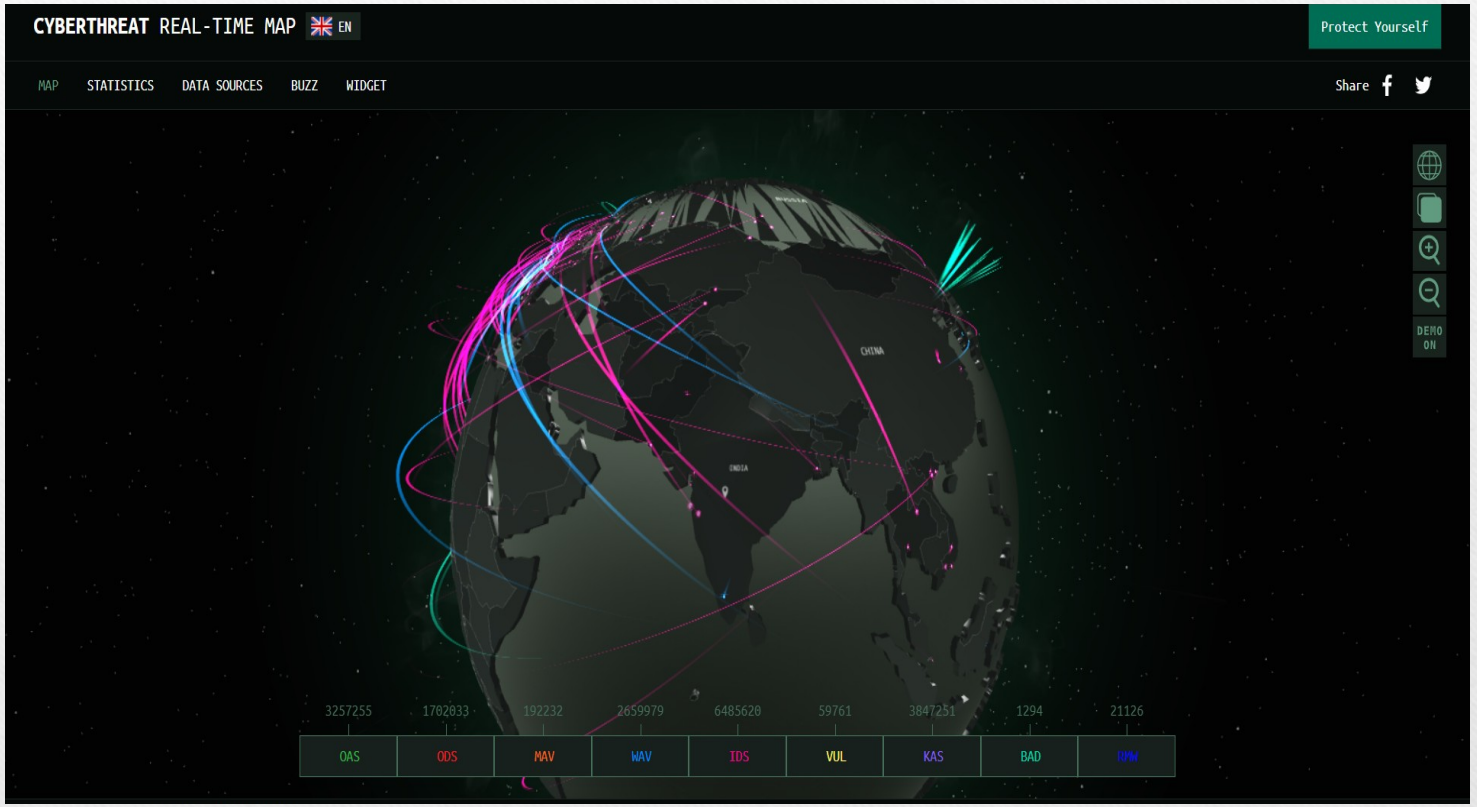
391 vendors, 1600 passwords
For Vancouver IT Support Services contact Netdigix.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other

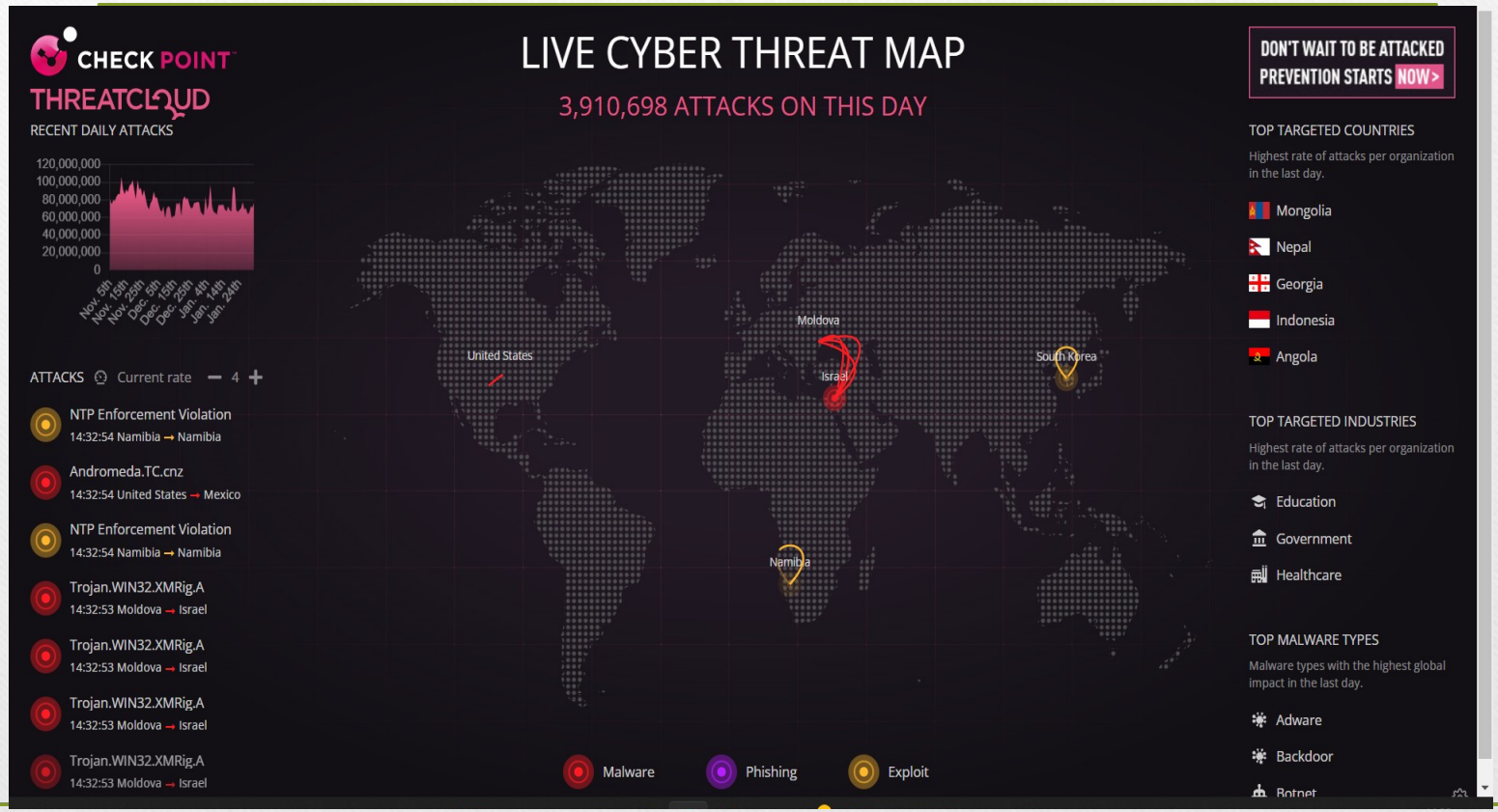
Vendors

360 Systems	3COM	3M
ACC	Acc/Newbridge	Accelerated Networks
ACCTON	Acer	actiontec
adaptec	Adaptec RAID	ADC Kentrox
AdComplete.com	ADP	Adtran
Advanced Integration	Aironet	Alcatel
Alcatel Thomson	Alcatel/Newbridge/Timestep	allied
Allied Telesyn	Allied Tenysin	Allied-Telesyn
Alteon	Alteon Web Systems	AMBIT
AMI	Amigo	Amptron

cybermap.kaspersky.com



threatmap.checkpoint.com



Question Please?

THANK YOU