

OSINT Reconnaissance Report - Target: nmap.org

Author : Yeswanth Boddeda

Date : 09/08/2025

Executive Summary

This OSINT (Open-Source Intelligence) investigation was conducted on the public-facing infrastructure of **nmap.org**, the official website for the Nmap Security Scanner project. The goal was to gather publicly available technical and security-related information without engaging in intrusive activities, in order to demonstrate reconnaissance capabilities using open-source tools.

The assessment followed a structured workflow covering **domain intelligence**, **DNS mapping**, **IP and hosting analysis**, **service enumeration**, **geolocation**, and **breach history verification**.

Key tools included: **Whois**, **nslookup**, **dig**, **DNSDumpster**, **Shodan**, **IPinfo.io**, **Nmap**, and **HavelBeenPwned**.

Key findings include:

- **Domain Registration** – Registered with Dynadot Inc., privacy-protected via Super Privacy Service LTD, using Linode name servers.
- **DNS Infrastructure** – Mail services hosted by Google; multiple subdomains including www.nmap.org and ack.nmap.org.
- **Hosting & Network** – Infrastructure hosted on Linode (Akamai Connected Cloud) in Fremont, California, ASN AS63949.
- **Open Services** – SSH (22), SMTP (25), HTTP (80), HTTPS (443) detected; banners indicated Apache HTTPD and Postfix SMTPD.
- **Breach History** – Publicly documented project email (fyodor@nmap.org) found in four historical data breaches (2017–2020), with some breaches exposing passwords and personal identifiers.

The results show that nmap.org's public infrastructure is **well-maintained and secured against major misconfigurations**, but historical data exposure through third-party breaches poses potential social engineering and phishing risks.

1.WHOIS Lookup

Tools used: Whois command line tool/ whois.domaintools.com

Findings:

Registrar : Dynadot Inc

Registrant Organization : Super Privacy Service LTD % Dynadot

Registration Date: 1999-01-18T05:00:00

Expiry Date: 2029-01-18T05:00:00Z

Name Servers:

- ns1.linode.com
- ns2.linode.com
- ns3.linode.com
- ns4.linode.com
- ns5.linode.com

```
Creation Date: 1999-01-18T05:00:00Z
Registry Expiry Date: 2029-01-18T05:00:00Z
Registrar: Dynadot Inc
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.6502620100
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: Super Privacy Service LTD c/o Dynadot
```

```
Name Server: ns1.linode.com
Name Server: ns2.linode.com
Name Server: ns3.linode.com
Name Server: ns4.linode.com
```

2. DNS Enumeration

Tools Used: nslookup, dig, DNSDumpster

Findings :

nslookup and **dig** commands were executed for nmap.org to retrieve DNS records.

No additional DNS records were retrieved directly via these tools beyond those visible from DNSDumpster.

```
(yash@kali)-[~]
$ dig ANY nmap.org
;; Connection to 192.168.0.1#53(192.168.0.1) for nmap.org failed: timed out.
;; no servers could be reached
;; Connection to 192.168.0.1#53(192.168.0.1) for nmap.org failed: timed out.
;; no servers could be reached
;; Connection to 192.168.0.1#53(192.168.0.1) for nmap.org failed: timed out.
;; no servers could be reached
```

```
(yash@kali)-[~]
$ nslookup -type=ANY nmap.org
;; Connection to 192.168.0.1#53(192.168.0.1) for nmap.org failed: timed out.
;; no servers could be reached
;; Connection to 192.168.0.1#53(192.168.0.1) for nmap.org failed: timed out.
;; no servers could be reached
;; Connection to 192.168.0.1#53(192.168.0.1) for nmap.org failed: timed out.
;; no servers could be reached
```

DNSDumpster revealed the target's DNS infrastructure including:

- A records (IPv4 addresses)
- MX records (Mail servers)
- TXT records (SPF, DKIM, DMARC Policies)

MX Records

10 aspmx3.googlemail.com	173.194.76.27 ws-in-f27.1e100.net	ASN:15169 173.194.76.0/24	GOOGLE United States	:
5 alt2.aspmx.l.google.com	173.194.76.26 ws-in-f26.1e100.net	ASN:15169 173.194.76.0/24	GOOGLE United States	:
10 aspmx2.googlemail.com	172.253.116.26 dj-in-f26.1e100.net	ASN:15169 172.253.116.0/24	GOOGLE United States	:
1 aspmx.l.google.com	172.253.63.27 bi-in-f27.1e100.net	ASN:15169 172.253.63.0/24	GOOGLE United States	:
5 alt1.aspmx.l.google.com	172.253.116.26 dj-in-f26.1e100.net	ASN:15169 172.253.116.0/24	GOOGLE United States	:

NS Records

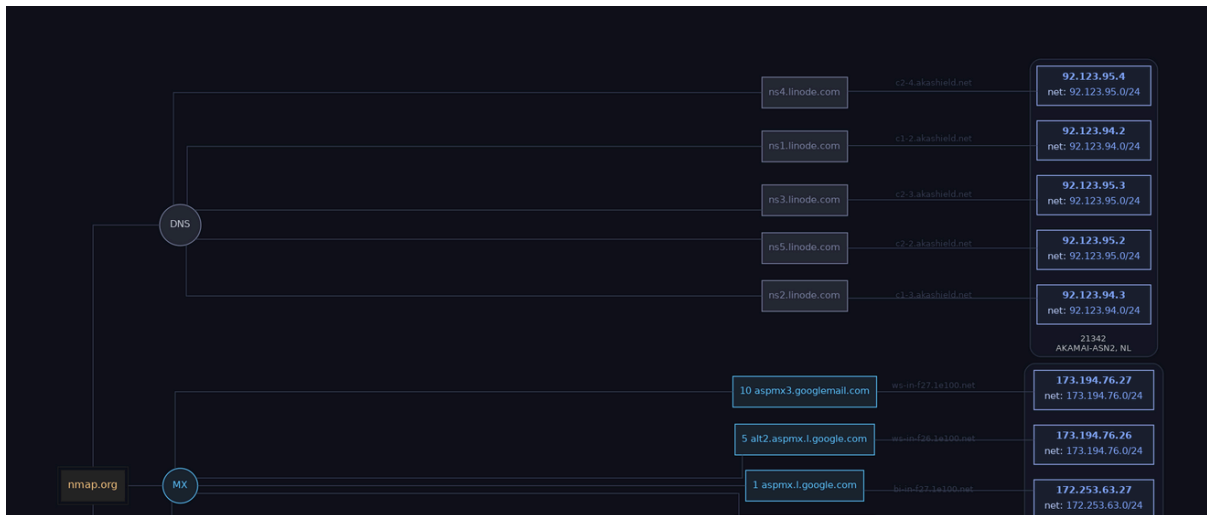
ns4.linode.com	92.123.95.4 c2-4.akashield.net	ASN:21342 92.123.95.0/24	AKAMAI-ASN2, NL The Netherlands	:
ns1.linode.com	92.123.94.2 c1-2.akashield.net	ASN:21342 92.123.94.0/24	AKAMAI-ASN2, NL The Netherlands	:
ns3.linode.com	92.123.95.3 c2-3.akashield.net	ASN:21342 92.123.95.0/24	AKAMAI-ASN2, NL The Netherlands	:
ns5.linode.com	92.123.95.2 c2-2.akashield.net	ASN:21342 92.123.95.0/24	AKAMAI-ASN2, NL The Netherlands	:
ns2.linode.com	92.123.94.3 c1-3.akashield.net	ASN:21342 92.123.94.0/24	AKAMAI-ASN2, NL The Netherlands	:

TXT Records

"google-site-verification=SrtYpJGxZzMTcczZG44XtLVK-sEPit9bputDjWc0lF4"

"v=spf1 a mx ptr ip4:50.116.1.184 ip6:2600:3c01::f03c:91ff:fe98:ff4e ip6:2600:3c01:e000:3e6::6d4e:7061 include:_spf.google.com ~all"

This diagram visualizes the DNS and mail server architecture for nmap.org. It shows the domain's name servers (managed by Linode), mail servers (hosted by Google), subdomains (such as www.nmap.org and ack.nmap.org), and their associated IP addresses. The flow illustrates how DNS queries are routed and displays the infrastructure behind nmap.org's web and email services.



These diagrams are useful for:

- Visualizing the registration and DNS configuration of nmap.org.
- Quickly identifying the providers responsible for core services (DNS, mail, hosting).
- Assessing the security posture by reviewing DNS organization, subdomain exposure, and network segmentation.

3. IP & Service Information


Tools used : [Shodan.io](https://shodan.io)

Findings :

The IP address 50.116.1.184 hosts the target infrastructure.

Shodan identified open ports such as : port 22, 25, 80, 443

Detected Service : OpenSSH, Postfix smtpd, Apache httpd

 Open Ports

22

25

80

443

// 22 / TCP1900237220 | 2025-07-31T23:08:45.007673

OpenSSH 7.4

SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQD0rn6FGID6Z9f1FRcBJyAD7twguPmDpnIQkK6R5zczrHPK7vyIx55zS9Gn//KfefecFkcu3AI8x/YTIMPb36UFyS/cJN/j1VY86eS6xJX/7VTzgZzcbAoBL8715EQgWoEz60mV698i8kXRqvWJ1HDdwqWT+NtHIU3nEyHgWFCwQCC5Y6dGe3JXvbw3BEXiMDaRRb a+apTNOG+Gii92VjMlbo+UiiSo+scZCmZrTmZD+LDQbDhvmgPoWZ7FmUKLJ0fZY44dyrgsLQuYVG uNlwa6xNF12BCr0+E6Vb4C8vQK0KYK0uNygL9atv+eptVz4XGtDVxBZoBr0NL574qVCX5
Fingerprint: 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1

Server Host Key Algorithms:
ssh-rsa
rsa-sha2-512
rsa-sha2-256
ecdsa-sha2-nistp256
ssh-ed25519

// 80 / TCP1526930258 | 2025-08-06T04:38:09.466531

Apache httpd 2.4.6

403 Forbidden

HTTP/1.1 403 Forbidden
Date: Wed, 06 Aug 2025 04:38:09 GMT
Server: Apache/2.4.6 (CentOS)
Content-Length: 398
Content-Type: text/html; charset=iso-8859-1

Vulnerabilities

18

33

42

3

0

// 25 / TCP868566298 | 2025-08-05T02:57:09.442403

Postfix smtpd

220 ack.nmap.org ESMTP Postfix
250-ack.nmap.org
250-PIPELINING
250-SIZE 102400000
250-VERFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN

SSL Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
06:ff:b7:c0:d0:cd:5c:32:f2:02:d9:05:c8:ed:29:3a:87:21
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Let's Encrypt, CN=R11
Validity
Not Before: Jul 22 09:04:19 2025 GMT
Not After : Oct 20 09:04:18 2025 GMT
Subject: CN=insecure.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)

```
// 443 / TCP 1614115339 | 2025-08-09T06:05:36.337708


Apache httpd 2.4.6

301 Moved Permanently

HTTP/1.1 301 Moved Permanently
Date: Sat, 09 Aug 2025 06:05:36 GMT
Server: Apache/2.4.6 (CentOS)
Location: https://github.com/nmap/nmap/issues/
Content-Length: 322
Content-Type: text/html; charset=iso-8859-1


SSL Certificate

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    06:ff:b7:c0:d0:cd:5c:32:f2:02:d9:05:c8:ed:29:3a:87:21
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=US, O=Let's Encrypt, CN=R11
  Validity
    Not Before: Jul 22 09:04:19 2025 GMT
    Not After : Oct 20 09:04:18 2025 GMT
  Subject: CN=insecure.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
```

 **Vulnerabilities**

All ports ▾ Latest ▾

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

 **2025** (3)

CVE-2025-49812

7.4 In some mod_ssl configurations on Apache HTTP Server versions through to 2.4.63, an HTTP desynchronisation attack allows a man-in-the-middle attacker to hijack an HTTP session via a TLS upgrade. Only configurations using 'SSLEngine optional' to enable TLS upgrades are affected. Users are recommended to upgrade to version 2.4.64, which removes support for TLS upgrade.

CVE-2025-32728

4.3 In sshd in OpenSSH before 10.0, the DisableForwarding directive does not adhere to the documentation stating that it disables X11 and agent forwarding.

CVE-2025-26465

6.8 A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

These images display network security scan results for a server, highlighting detected vulnerabilities from 2025 and the server's open ports and SSH configuration details.

4. IP Geolocation

Tools Used : [IPinfo.io](https://ipinfo.io)

Findings :

ASN : AS63949 – Akamai Connected Cloud


Hosting Provider: Linode

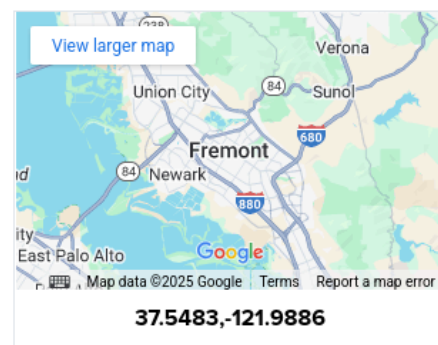
Location : Fremont, California, United States

Summary

ASN	AS63949 - Akamai Connected Cloud
Hostname	ack.nmap.org
Range	50.116.0.0/20
Company	Linode
Hosted domains	287
Privacy	✓ True
Anycast	✗ False
ASN type	Hosting
Abuse contact	abuse@linode.com

IP Geolocation

City	Fremont
State	California
Country	 United States
Postal	94536
Local time	12:24 AM, Saturday, August 09, 2025
Timezone	America/Los_Angeles
Coordinates	37.5483,-121.9886



ASN

AS63949 - Akamai Connected Cloud



DOMAIN
linode.com



ASN TYPE
Hosting



ROUTE
50.116.0.0/20

Company

Linode

Company API

Provides the company behind the IP address. This includes the company's name, domain name, and what type of company it is: ISP, business, or hosting.).

[Read more >](#)

Useful for [Account Based Marketing](#)

Abuse Details



US, PA, Philadelphia, 249 Arch St, 19106



+1-609-380-7100



abuse@linode.com

NAME	NETWORK
Linode Abuse Support	50.116.0.0/18

These images provide an overview of the hosting and network details for the observed IP range. The ASN (AS63949 – Akamai Connected Cloud) is associated with Linode, the hosting provider for the infrastructure. The geolocation indicates the servers are based in Fremont, California, USA, ensuring clarity on both network ownership and physical server location for documentation purposes.

5. Port Scanning

Tools used : Nmap

Open Ports Detected :

- 22/tcp
- 25/tcp
- 80/tcp
- 443/tcp

Services Running :

- 22/tcp: ssh
- 25/tcp: smtp
- 80/tcp: http
- 443/tcp: https

```
└─$ nmap -T4 --top-ports 100 nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 03:31 EDT
Nmap scan report for nmap.org (50.116.1.184)
Host is up (0.30s latency).
Other addresses for nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 50.116.1.184: ack.nmap.org
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
```

This screenshot displays the results of a network scan on nmap.org, revealing four open ports—22 (SSH), 25 (SMTP), 80 (HTTP), and 443 (HTTPS). Each open port is associated with a standard internet service, indicating that the server is configured to allow secure shell access, email transfer, and web services over both HTTP and HTTPS protocols.

6. Breach Search

Tools used : HavelBeenPwned

Findings :

The publicly available email address fyodor@nmap.org was identified through the Nmap project's official documentation.

A HavelBeenPwned search revealed that this email address was found in 4 separate data breaches.

Breaches Identified:

1. **Gravatar (October 2020)** – A scraping technique exposed 167M names, usernames, and MD5 hashes of email addresses. 114M hashes were cracked, revealing the original emails and associated details.

Compromised data: Email addresses, names, usernames.

2. **Covve / db8151dd (February 2020)** – An exposed Elasticsearch server linked to the Covve contacts app revealed extensive personal and contact interaction data.

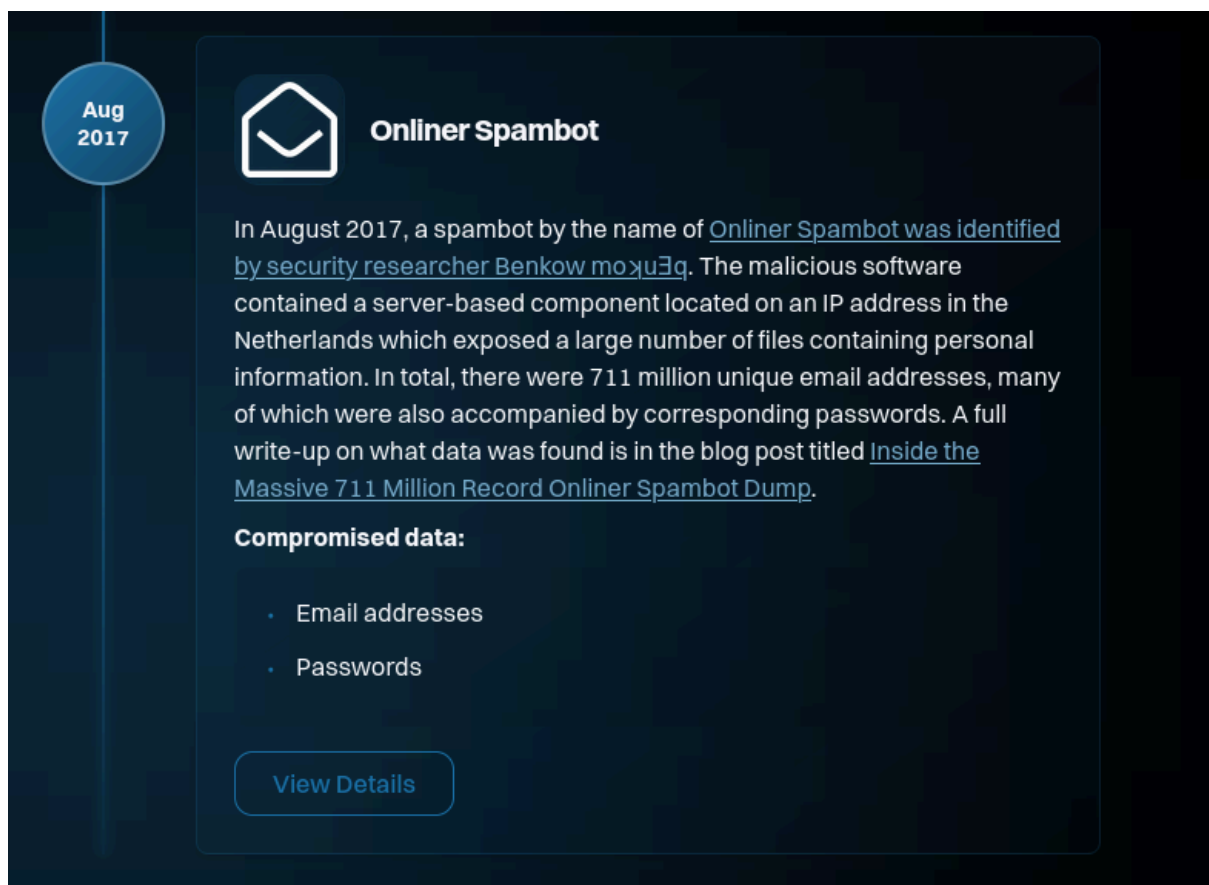
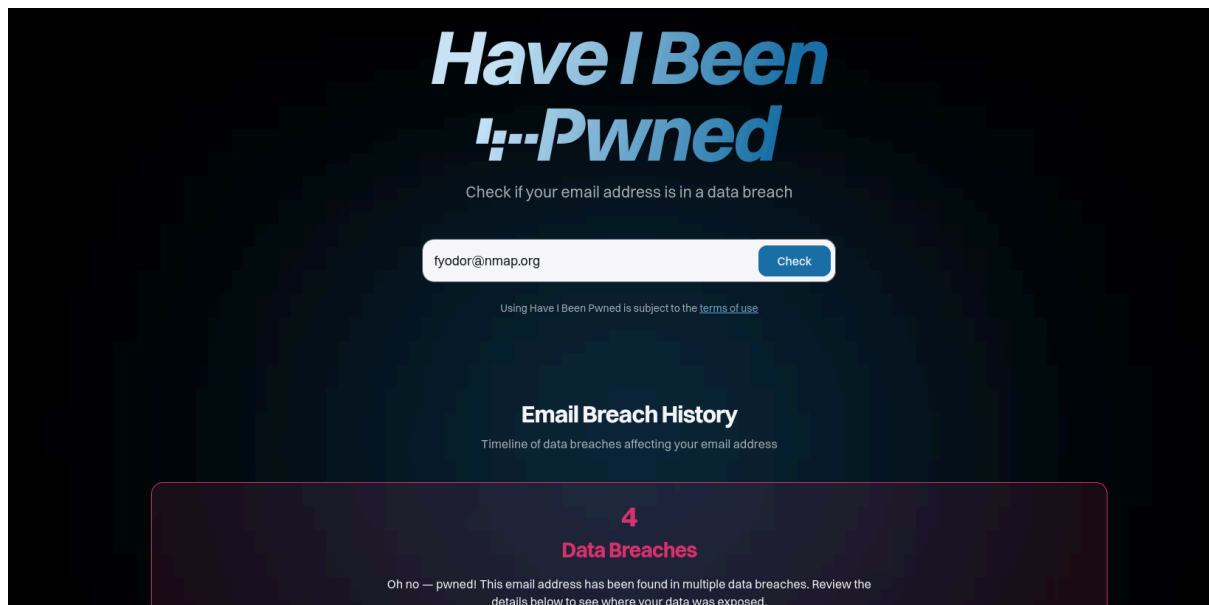
Compromised data: Email addresses, job titles, names, phone numbers, physical addresses, social media profiles.

3. **Verifications.io (February 2019)** – An unsecured MongoDB database exposed 763M email addresses and personal information. No passwords were included, but the dataset contained multiple identifying attributes.

Compromised data: Dates of birth, email addresses, employers, genders, geographic locations, IP addresses, job titles, names, phone numbers, physical addresses.

4. **Onliner Spambot (August 2017)** – A spambot campaign exposed 711M email addresses, many with associated passwords, through a server-based component hosted in the Netherlands.

Compromised data: Email addresses, passwords.



This image summarizes the 2017 Onliner Spambot breach, which exposed 711 million unique email addresses and passwords. It provides details about the compromise, its discovery, and the type of data affected.



Verifications.io

Feb
2019

In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by [Bob Diachenko](#) and [Vinny Troia](#), the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although [an archived copy remains viewable](#).

Compromised data:

- Dates of birth
- Email addresses
- Employers
- Genders
- Geographic locations
- IP addresses
- Job titles
- Names
- Phone numbers
- Physical addresses

This image details the February 2019 data breach of Verifications.io, an email validation service, where an unsecured database exposed 763 million unique email addresses. Security researchers Bob Diachenko and Vinny Troia discovered the breach. The exposed data included personal information such as names, phone numbers, email addresses, dates of birth, employers, and IP addresses. No passwords were leaked, but the sheer volume and sensitivity of the data posed substantial privacy risks. Following the breach, the Verifications.io website was taken offline as details were disclosed to the public.

Feb
2020



Covve

In February 2020, [a massive trove of personal information referred to as "db8151dd"](#) was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by [dehashed.com](#).

Compromised data:

- Email addresses
- Job titles
- Names
- Phone numbers
- Physical addresses
- Social media profiles

[View Details](#)

This image describes the Covve data breach that occurred in February 2020, where a massive collection of personal information from the Covve contacts app was left exposed online due to an unsecured Elasticsearch server. The leaked data included email addresses, job titles, names, phone numbers, physical addresses, and social media profiles—affecting both Covve users and their contacts. Security researchers discovered the breach and provided the data to Have I Been Pwned via dehashed.com. The breach highlighted significant risks to personal privacy, as comprehensive contact and interaction details were inadvertently made public. This incident is an example of how the misconfiguration of cloud services can lead to large-scale data exposures. It serves as a reminder of the need for robust data security practices around sensitive personal information.



Gravatar

Oct
2020

In October 2020, [a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars](#). 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, [Gravatar release an FAQ detailing the incident](#).

Compromised data:

- Email addresses
- Names
- Usernames

[View Details](#)

This image summarizes the October 2020 Gravatar data breach, where a security researcher scraped 167 million names, usernames, and MD5-hashed email addresses from Gravatar profiles. Of these, 114 million MD5 hashes were cracked, revealing the original email addresses and associated usernames to the hacking community. The breach exposed sensitive identifying information, raising significant privacy concerns for affected users.

Conclusion

The OSINT investigation of **nmap.org** successfully demonstrated the ability to gather actionable intelligence using open-source tools. The findings confirm:

- The infrastructure is hosted on **Linode (Akamai Connected Cloud)** in Fremont, California.
- Open services include **SSH, SMTP, HTTP, and HTTPS**.
- No additional DNS records were found beyond those revealed by DNSDumpster.
- The public email address fyodor@nmap.org is linked to four historical breaches, some exposing personal data and passwords.

Overall, the target demonstrates a relatively secure network configuration, but the exposure of historical credentials linked to an official project email address may pose ongoing risks.

Recommendations

1. **Breach Monitoring** – Continuously monitor for new breaches involving official project email addresses to detect possible compromises early.
2. **Credential Hygiene** – Ensure any exposed passwords from historical breaches are no longer in use and have been changed.
3. **Limit Service Exposure** – Restrict SSH and SMTP access to trusted IP ranges to minimize attack surface.
4. **Regular DNS Audits** – Conduct periodic reviews of DNS records to detect and remove any unused or vulnerable subdomains.
5. **Employee Security Awareness** – Train staff on phishing risks, especially when emails are publicly accessible.