

Objective of the Report

The objective of this report is to conduct an attack surface analysis targeting **Zoom Video Communications, Inc.** (zoom.com) from a Red Team perspective. The goal is to identify publicly exposed assets, potential attack vectors, and configurations that could be exploited by a malicious actor during the reconnaissance phase. This analysis is conducted for educational purposes and to practice offensive cybersecurity techniques, while strictly adhering to ethical and legal boundaries within a simulated environment.

Scope of this Report

The scope of this report is limited to passive analysis of assets associated with the zoom.com domain, including subdomains, public IP addresses, DNS records, technologies in use, SSL/TLS certificates, and potential leaks or exposures found through open-source intelligence (OSINT). No intrusive testing, vulnerability exploitation, or unauthorized access will be performed. All activities are intended to simulate the reconnaissance phase of a Red Team exercise without disrupting the availability or integrity of Zoom's legitimate services.

About Zoom

I have selected **Zoom Video Communications, Inc.** (zoom.com) as the target entity for this exercise. Zoom is a leading provider of video communications services, offering a robust platform for video conferencing, voice calls, webinars, online meetings, and team collaboration. Headquartered in San Jose, California, Zoom has become a critical tool for remote communication across various sectors including business, education, healthcare, and government.

The company was founded in 2011 by Eric Yuan, a former lead engineer at Cisco WebEx. Zoom quickly gained global recognition for its ease of use, reliability, and scalability, especially during the COVID-19 pandemic, when it became one of the most widely used platforms for remote work and

learning. As a technology company with a vast digital presence, Zoom operates numerous publicly accessible assets and infrastructures that may be of interest during a Red Team reconnaissance phase.

Beginning with the analysis of this entity:

```
osboxes@alain:~/planning-recon$ nslookup zoom.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   zoom.com
Address: 170.114.0.12
```

**HURRICANE ELECTRIC
INTERNET SERVICES**

Search

[zoom.com](#)

Quick Links

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
Exchange Report
Bogon Routes
World Report
Multi Origin Routes

DNS Info

Website Info

IP Info

Whois

RDAP

Start of Authority
mname: ns-968.awsdns-57.net mname: awsdns-hostmaster.amazon.com
serial: 1
refresh: 7200 retry: 900
expire: 1209600 minimum: 86400

Nameservers
[ns-1473.awsdns-56.org](#), [ns-1861.awsdns-40.co.uk](#), [ns-481.awsdns-60.com](#), [ns-968.awsdns-57.net](#)

Mail Exchangers
[mx-00569201.gslb.pphosted.com\(10\)](#), [mxb-00569201.gslb.pphosted.com\(10\)](#)

[zoom.com](#)

Quick Links

BGP Toolkit Home
BGP Prefix Report

DNS Info

Website Info

IP Info

Whois

RDAP

[170.114.0.12](#) > [170.114.0.0/20](#) > [AS14618](#) > Amazon.com, Inc.

[zoom.com](#)

Quick Links

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification

DNS Info

Website Info

IP Info

Whois

RDAP

Domain Name: ZOOM.COM
Registry Domain ID: 5534959_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-07-05T21:14:24Z
Creation Date: 1999-04-22T04:00:00Z
Registry Expiry Date: 2025-12-02T04:59:59Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>
Domain Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>
Domain Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>
Domain Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>
Name Server: NS-1473.AWSDNS-56.ORG
Name Server: NS-1861.AWSDNS-40.CO.UK
Name Server: NS-481.AWSDNS-60.COM
Name Server: NS-968.AWSDNS-57.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of whois database: 2025-01-18T06:39:04Z <<<

By analyzing the domain zoom.com using the Hurricane Electric Internet Services tool, it was determined that the associated IP address is 170.114.0.15, which belongs to the 170.114.0.0/20 block. This IP range is assigned to **Autonomous System AS14618**, which is owned by **Amazon.com, Inc.** This indicates that Zoom is using **Amazon Web Services (AWS)** infrastructure to host part of its services—a common practice among tech companies due to the scalability and security offered by Amazon's cloud platform.

It is not possible to obtain specific information about the zoom.com domain using the whois tool because it uses Amazon Web Services (AWS) servers. AWS hosts multiple services and companies under shared IP ranges, making it difficult to identify details about a single domain. In such cases, the whois information reflects the infrastructure provider (such as Amazon), not the individual service like Zoom.

Static Analysis Tools Used for Reconnaissance

From this point onward, static analysis tools were used to perform passive reconnaissance on the target entity, aiming to map its publicly exposed digital footprint without engaging in any intrusive or active probing techniques.

To initiate the DNS analysis, the `dig` command with the `+short` option was used to resolve the domain www.zoom.com. The `dig` (Domain Information Groper) tool is commonly used to query DNS servers and obtain details such as IP addresses, CNAMEs, and other DNS records. The `+short` flag simplifies the output by returning only the relevant result in a compact format.

The command output showed that www.zoom.com resolves directly to the IP address 170.114.78.80. This suggests that Zoom is hosting this subdomain on its own infrastructure or through a specific service provider, rather than using a content delivery network (CDN) like Akamai for this entry point. This IP address becomes a valuable starting point for further

passive reconnaissance, such as reverse IP lookups or service fingerprinting.

```
osboxes@alain:~/planning-recon$ dig +short www.zoom.com
170.114.78.80
```

To perform subdomain enumeration, the tool **subfinder** was used with the target domain zoom.com, utilizing a custom list of trusted DNS resolvers (resolvers.txt) for improved accuracy and speed. The purpose of subfinder is to passively collect valid subdomains associated with a target domain by querying a variety of public sources and APIs. This method is non-intrusive and effective in mapping the external surface of an organization.

The execution of the command resulted in the discovery of 927 subdomains for zoom.com in approximately 25.4 seconds, indicating a large and diverse infrastructure behind the domain. This list of subdomains serves as a valuable foundation for further reconnaissance steps such as DNS resolution, port scanning, and vulnerability analysis.

```
osboxes@alain:~/planning-recon$ ~/go/bin/subfinder -d zoom.com -r ~/planning-recon/resolvers.txt -o sub_zoom.txt
```

```
[INF] Found 924 subdomains for zoom.com in 9 seconds 904 milliseconds
```

Brief Analysis of Selected Subdomains

Among the numerous subdomains identified for zoom.com, several stand out due to their potential operational significance or exposure to risks: backend.jenkins.ops.corp.zoom.com – This subdomain suggests the presence of a Jenkins CI/CD server used internally for development or deployment. If exposed or misconfigured, it could be a critical entry point for attackers.

vault.ops.corp.zoom.com and its variants

(e.g., prod.vault.ops.corp.zoom.com, [nonprod-](https://nonprod-04.vault.ops.corp.zoom.com)

04.vault.ops.corp.zoom.com)– These indicate the use of HashiCorp Vault,

likely for secrets and credential management. Improper access controls here could lead to severe data breaches.

artifactory-cache-prod-aws-us-west-2-green.artifacts.ops.corp.zoom.com

– Refers to a production-level Artifactory repository, probably caching software artifacts. Such endpoints could reveal internal development components or be abused in supply chain attacks.

nifi-nginx-waf.sml.corp.zoom.com – This subdomain indicates a NiFi deployment behind a NGINX Web Application Firewall. The presence of a WAF implies a layer of protection but also hints at sensitive data workflows worth protecting.

monitoring-smokescreen-us01-alert.ops.corp.zoom.com – This subdomain appears tied to internal monitoring and alerting infrastructure. Exposing such systems could provide attackers with insight into internal defenses or downtime windows.

community.zoom.com – A more public-facing subdomain, likely hosting forums or user interaction platforms. While less critical internally, vulnerabilities here can still impact brand trust and user privacy. These subdomains reflect a mixture of development, monitoring, infrastructure, and user-facing environments. Proper segmentation and access controls are essential to mitigate potential attack vectors exposed through subdomain enumeration.

The tool shuffledns is a valuable tool when the goal is comprehensive discovery or when dealing with targets that have a large attack surface like Zoom.

```
osboxes@alain:~/planning-recon$ shuffledns -mode bruteforce -d zoom.com -w /home/osboxes/nassdns/SecLists/Di
scovery/DNS/subdomains-top1million-110000.txt -r ~/planning-recon/resolvers.txt -silent -o ~/planning-recon/
shuffledns.txt
```

```
osboxes@alain:~/planning-recon$ ls
resolvers.txt  shuffledns.txt  sub_zoom.txt
osboxes@alain:~/planning-recon$ cat shuffledns.txt | wc
3977      3962      60368
```

Below are selected subdomains that may indicate interesting, sensitive, or unusual infrastructure:

Subdomain	Possible Purpose or Relevance
mail.zoom.com	Mail gateway or internal messaging system
smtp.zoom.com	Outbound email server — potential vector for spoofing or phishing
imap.zoom.com	Email retrieval — legacy mail service or internal use
support.zoom.com	Customer support platform — social engineering risk surface
trust.zoom.com	Public transparency or security trust portal
zabbix.zoom.com	Network monitoring via Zabbix — suggests internal IT infrastructure
snowflake.zoom.com	Integration with Snowflake (data analytics/storage platform)
nike.zoom.com, dell.zoom.com, walmart.zoom.com	Possibly used for partner access or corporate branding tests
bounce.zoom.com	Handles bounced emails — might expose marketing activity
girlscouts.zoom.com, remax.zoom.com	Unusual — possibly vanity or campaign-specific subdomains

I used the tool **cero** to discover domains and subdomains associated with [zoom.com](https://zoom.us). This tool queries various certificate transparency logs to find domains linked to SSL/TLS certificates issued for the target. In this case, the only result returned was the main domain [zoom.com](https://zoom.us), which suggests that no additional subdomains using distinct certificates were found through this method.

```
osboxes@alain:~/planning-recon$ cero -d zoom.com | grep "zoom.com" > cero.txt
osboxes@alain:~/planning-recon$ ls
analytics.txt  cero.txt  resolvers.txt  shuffledns.txt  sub_zoom.txt
osboxes@alain:~/planning-recon$ cat cero.txt
zoom.com
```

I used **Katana**, a web crawling and content discovery tool, to extract information from [zoom.com](https://zoom.us). By specifying the flags `-kf robotstxt`, `sitemapxml`, the tool was instructed to focus on parsing the


```
osboxes@alain:~/planning-recon$ echo zoom.com | katana -jc -o katana_output -kf robotstxt,sitemapxml
```

ATTENTION

```
osboxes@alain:~/planning-recon$ cat katana_output | wc
```

172	172	10470
-----	-----	-------

```
osboxes@alain:~/planning-recon$ cat katana_output | tail
```

- https://www.zoom.com/pt
- https://www.zoom.com/fr
- https://www.zoom.com/zh-tw
- https://www.zoom.com/zh-cn
- https://www.zoom.com/de
- https://www.zoom.com/es
- https://www.zoom.com/nl
- https://www.zoom.com/en/audiences/marketing-events/
- https://support.zoom.com/hc/en
- https://www.zoom.com/en/trust/

Among the results, I identified various paths that reveal Zoom's content organization by language, product-specific pages, developer assets such as JavaScript libraries, and internal resources like error pages and sitemaps. This enumeration helps outline potential attack surfaces and content of interest for reconnaissance in a security auditing context.

To further process the URLs discovered by Katana, I used the command `cat katana_output | unfurl --unique domains > katana.txt`. This command

extracted and listed all unique domain names found within the Katana output. As a result, I obtained the domains written below.

```
osboxes@alain:~/planning-recon$ cat katana_output | unfurl --unique domains > katana.txt
osboxes@alain:~/planning-recon$ cat katana.txt | wc
      5      5     73
osboxes@alain:~/planning-recon$ cat katana.txt
www.zoom.com
zoom.com
media.zoom.com
community.zoom.com
support.zoom.com
```

Domain Breakdown:

- [zoom.com](#)
This is the primary root domain of Zoom. It typically redirects users to the main corporate or regional landing pages or is used for redirection and DNS purposes.
- [www.zoom.com](#)
This is the main web interface for Zoom's public-facing site. It hosts information about products, services, pricing, company details, and acts as the primary entry point for most users.
- [media.zoom.com](#)
This subdomain is likely used to host media content such as videos, images, press materials, or downloadable assets. It may serve static content for marketing or documentation.
- [community.zoom.com](#)
This is probably the domain for Zoom's public forums or user community. It allows users to ask questions, share experiences, report issues, and get advice from other users and moderators.
- [support.zoom.com](#)
This subdomain is most likely dedicated to technical support and help resources. It often includes FAQs, troubleshooting guides, ticket submission forms, and product documentation.

```
osboxes@alain:~/planning-recon$ cat shuffledns.txt cero.txt katana.txt > subdomains.txt
osboxes@alain:~/planning-recon$ cat subdomains.txt | wc
 3983   3968  60450
osboxes@alain:~/planning-recon$ grep -E '\.zoom\.com$|\.zoom\.com/' clean_subdomains.txt > final_subdomains.txt
```

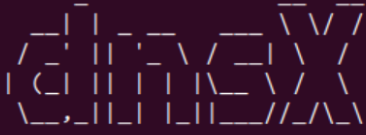


```
osboxes@alain:~/planning-recon$ cat final_subdomains.txt | wc
3904      3904      59647
osboxes@alain:~/planning-recon$ cat final_subdomains.txt | head
mail.zoom.com
preview.zoom.com
ade.zoom.com
trust.zoom.com
library.zoom.com
localhost.shop.zoom.com
avon.zoom.com
imap.zoom.com
zmail.zoom.com
smtp.zoom.com
```

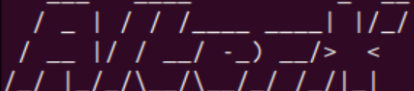
To enrich the list of discovered subdomains with additional context and validate their DNS resolution status, we use a chained command involving alterx and dnsx. The command `cat final_subdomains.txt | alterx | dnsx -o alterx.txt` first processes the subdomains through alterx, which generates altered or permutation-based variants (such as subdomain mutations, additions, or known patterns).

These variants are then passed directly into dnsx, a fast DNS resolution tool, which verifies which of these subdomains resolve to valid IP addresses. The results are saved in alterx.txt, providing a refined and actionable list of active subdomains for further reconnaissance or analysis.

```
osboxes@alain:~/planning-recon$ cat final_subdomains.txt | alterx | dnsx -o alterx.txt
```



projectdiscovery.io



```
Current dnsx version 1.2.2 (latest)
[INF] Current alterx version v0.0.6 (latest)
[INF] Generated 993088 permutations in 12.1219s
acc.zoom.com
aisinfo.zoom.com
allegro-test.zoom.com
api.zoom.com
aqa.zoom.com
atlas.zoom.com
auto1.zoom.com
bainlab.zoom.com
barracuda-staging.zoom.com
bbctest.zoom.com
beaconlive.zoom.com
beta.zoom.com
```


The execution of the alterx and dnsx pipeline yielded significant results. According to the output, alterx (v0.0.6) generated 993,088 subdomain permutations in approximately 12.12 seconds, demonstrating its efficiency and speed in expanding the attack surface through permutation-based discovery. Following this, dnsx (v1.2.2) validated a subset of those permutations, resolving them to live IP addresses. Among the verified subdomains were several interesting and potentially high-value assets such as [api.zoom.com](#), [atlas.zoom.com](#), [auto1.zoom.com](#), and [bloombergbeta.zoom.com](#).


These findings highlight the effectiveness of combining both tools for discovering both standard and obscure subdomains.


The **crt.sh** tool is a very useful resource for reconnaissance, as it allows searching for digital certificates issued for a specific domain—in this case, zoom.com. When querying this page, dozens of certificates were found related to subdomains, internal services, and other valuable technical details. However, the volume of results was so large that it made it difficult to quickly extract relevant information. This highlights both the usefulness and the challenge of interpreting large datasets during open-source intelligence (OSINT) exercises.

crt.sh

Identity Search







Groups by Issuer

Criteria

Type: Identity

Match: ILIKE

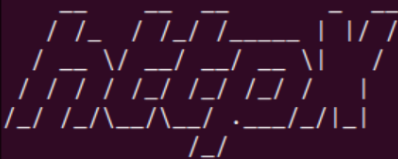
Search: 'zoom.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	18605064569	2025-05-25	2025-05-25	2026-05-26	ngxpls-acprod.asynccommu02.zoom.us	ngxpls-ac740-internal.asynccommu02.corp.zoom.com ngxpls-acprod-internal.asynccommu02.corp.zoom.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
	18605045595	2025-05-25	2025-05-25	2026-05-26	ngxpls-acprod.asynccommca.zoom.us	ngxpls-ac710-internal.asynccommca.corp.zoom.com ngxpls-acprod-internal.asynccommca.corp.zoom.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
	18605030477	2025-05-25	2025-05-25	2026-05-26	ngxpls-acprod.asynccommmsg.zoom.us	ngxpls-ac730-internal.asynccommmsg.corp.zoom.com ngxpls-acprod-internal.asynccommmsg.corp.zoom.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
	18605030465	2025-05-25	2025-05-25	2026-05-26	ngxpls-acprod.asynccommu.zoom.us	imap.zoom.com imap.zoom.com ngxpls-ac700-internal.asynccommu.corp.zoom.com ngxpls-acprod-internal.asynccommu.corp.zoom.com smtpex.zoom.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
	18605029495	2025-05-25	2025-05-25	2026-05-26	ngxpls-acprod.asynccommuau.zoom.us	smtp.zoom.com ngxpls-ac500-internal.asynccommuau.corp.zoom.com	C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA

httpx is a powerful and efficient command-line tool designed to identify which subdomains or URLs are actively responding over HTTP or HTTPS. It plays a critical role during the reconnaissance phase of security assessments or penetration testing, helping analysts quickly filter out inactive endpoints and focus their efforts on those that are reachable. The tool supports large input files and can check thousands of targets concurrently, making it ideal for automated scans in modern reconnaissance workflows.

In this case, httpx was run against a cleaned list of Zoom subdomains using the command `httpx -l final_subdomains_copy.txt > subdomains_live.txt`. Out of 3,983 initial subdomains, 1,356 were found to be live. Sample results include live hosts like <https://amiad.zoom.com>, <http://accenture.zoom.com>, <https://alibaba.zoom.com>, and <http://airtel.zoom.com>, which indicate the presence of potentially active services or portals for organizations or internal projects hosted under Zoom's domain. These findings are valuable for narrowing down the attack surface and focusing follow-up testing efforts such as content discovery, login portals, or vulnerability scans.

```
osboxes@alain:~/planning-recon$ httpx -l final_subdomains_copy.txt > subdomains_live.txt
```



```
osboxes@alain:~/planning-recon$ cat subdomains_live.txt | wc
1356      1356      31181
```

The following command iterates through each subdomain listed in subd_live_final.txt, performs a DNS lookup using dig to retrieve its corresponding IP address, filters the result to extract valid IPv4 addresses using a regular expression with grep, and saves the output into subd_final_ips.txt.

```
osboxes@alain:~/planning-recon$ for subdomain in $(cat subd_live_final.txt); do dig +short $subdomain | grep -Eo '([0-9]{1,3}.){3}[0-9]{1,3}'; done > subd_final_ips.txt
```

Controlled Masscan Execution for Sample Analysis

The following command was executed for a short and controlled duration to analyze a representative sample of open ports across the previously identified IP addresses. The scan was limited in scope and time to avoid overloading the network or triggering security alerts.

```
osboxes@alain:~/planning-recon$ sudo masscan -p0- -iL subd_final_ips.txt > masscan_final_ips.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-05-25 18:38:26 GMT
Initiating SYN Stealth Scan
Scanning 25 hosts [65536 ports/host]
```

```
osboxes@alain:~/planning-recon$ cat subd_final_ips.txt | wc
1567      1567      19844
```

```
osboxes@alain:~/planning-recon$ sudo masscan -p0- -iL subd_final_ips.txt > masscan_final_ips.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-05-25 18:38:26 GMT
Initiating SYN Stealth Scan
Scanning 25 hosts [65536 ports/host]
```

```
osboxes@alain:~/planning-recon$ cat masscan_final_ips.txt
Discovered open port 443/tcp on 52.84.66.112
Discovered open port 80/tcp on 170.114.11.147
Discovered open port 80/tcp on 52.84.66.112
```

Gowitness is a reconnaissance tool used to capture screenshots of websites and web applications. It automates the process of visually inspecting large sets of URLs by rendering their pages and saving images, which helps security professionals quickly identify interesting targets, check for defacements, or analyze web assets without manually visiting each URL.

```
osboxes@alain:~/planning-recon$ gowitness scan file -f subdomains.txt
```

The partial output shows a list of URLs from the scan, indicating various subdomains of the target domain that have been successfully captured by

Gowitness. Each URL corresponds to a distinct web interface or service, reflecting a broad range of potential attack surfaces or assets that may require further analysis.

```
osboxes@alain:~/planning-recon/screenshots$ ls
http---ade.zoom.com-443.jpeg      https---library.zoom.com-443.jpeg
http---library.zoom.com-443.jpeg  https---mail.zoom.com-443.jpeg
http---library.zoom.com-80.jpeg   https---preview.zoom.com-443.jpeg
http---mail.zoom.com-443.jpeg     https---trust.zoom.com-443.jpeg
http---mail.zoom.com-80.jpeg      http---trust.zoom.com-443.jpeg
http---preview.zoom.com-443.jpeg  http---trust.zoom.com-80.jpeg
http---preview.zoom.com-80.jpeg
```

Wafw00f is a web application firewall (WAF) detection tool designed to identify whether a target web application is protected by a WAF and, if so, to determine which WAF is in place. This can help penetration testers and security professionals understand the level of protection present before conducting further testing. By analyzing HTTP responses and known WAF signatures, Wafw00f provides insights into the defensive technologies deployed on a given domain or subdomain.

```
osboxes@alain:~/planning-recon$ wafw00f -i final_urls.txt > waf00f.txt
```

In the scan performed against various Zoom subdomains, Wafw00f attempted to connect to over a thousand URLs. A portion of the results indicated that some domains were unreachable or returned errors such as DNS resolution failures, connection refusals, or timeouts—for example, localhost.shop.zoom.com failed due to a name resolution error, both imap.zoom.com and smtp.zoom.com refused connections.

These errors suggest that either the services are not publicly accessible or that active protections or network restrictions are in place, potentially including firewalls or closed ports.


WhatWeb is a web scanner used to identify technologies used by websites, such as web servers, frameworks, content management systems (CMS), analytics tools, and more. It works by inspecting HTTP headers, HTML content, JavaScript, and other response elements. WhatWeb is useful for reconnaissance during penetration testing, helping analysts understand the target's tech stack and potential attack surfaces.


```
osboxes@alain:~/planning-recon$ whatweb zoom.com
http://zoom.com [302 Found] Country[UNITED STATES][US], HTTPServer[zoom], IP[170.114.0.12], RedirectLocation[https://www.zoom.com], Title[302 Found]
https://www.zoom.com [200 OK] Cookies[__cf_bm], Country[UNITED STATES][US], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[170.114.78.80], Open-Graph-Protocol, Script[application/json,application/ld+json,module], Strict-Transport-Security[max-age=15552000; includeSubDomains], Title[One platform to connect | Zoom], UncommonHeaders[cf-cache-status,access-control-allow-origin,access-control-request-method,cross-origin-resource-policy,x-amz-server-side-encryption,x-amz-storage-class,alt-svc,cf-ray]
```

In this scan of zoom.com, WhatWeb successfully identified a redirect from, <http://zoom.com> to <https://www.zoom.com>, indicating the use of HTTPS. The site is hosted in the United States and uses Cloudflare as the HTTP server. The response includes headers related to security (Strict-Transport-Security) and session protection (HttpOnly cookies like __cf_bm). The presence of modern elements like HTML5, Open Graph protocol, and structured data scripts (application/ld+json) suggests that the site follows current web development practices. The results confirm that WhatWeb was executed correctly and provided valuable insights into the security and structure of the Zoom homepage.

Nuclei is a fast, flexible vulnerability scanner designed to identify security issues across a wide range of targets using customizable templates. It is widely used in bug bounty hunting, penetration testing, and attack surface mapping. Nuclei excels at detecting known vulnerabilities (CVEs), misconfigurations, exposed panels, default credentials, and other security flaws by leveraging a vast and continuously updated community-driven template repository. Its speed and ability to run thousands of checks in parallel make it highly effective during the reconnaissance and assessment phases of a security engagement.

```
osboxes@alain:~/planning-recon$ nuclei -u zoom.com > nuclei_zoom.txt
```




```
[INF] Scan completed in 2m. 10 matches found.  
osboxes@alain:~/planning-recon$ cat nuclei_zoom.txt | wc  
10      55     1625
```

In the scan results for zoom.com, Nuclei identified several interesting findings. These include missing Subresource Integrity (SRI) attributes on loaded JavaScript and CSS files, which could pose a risk if content is tampered with. The domain is integrated with Azure Active Directory (AAD), as indicated by the azure-domain-tenant detection. TLS configuration appears solid, using TLS 1.2 and a wildcard certificate issued by DigiCert. The DNS results show configured mail exchange servers, name servers hosted by AWS, and a strict DMARC policy enforcing email authentication. Overall, the results reflect a mature security posture with some room for improvement in frontend integrity controls.

```
osboxes@alain:~/planning-recon$ cat nuclei_zoom.txt  
[missing-sri] [http] [info] https://www.zoom.com ["https://st1.zoom.us/homepage/publish/_nuxt/DWGTfSef.js","https://st1.zoom.us/homepage/publish/_nuxt/entry.Da4ose4m.css","https://st1.zoom.us/homepage/publish/_nuxt/index.CKSe7gns.css"]  
[azure-domain-tenant] [http] [info] https://login.microsoftonline.com:443/zoom.com/v2.0/.well-known/openid-configuration ["e31a6123-4833-4fde-975b-9391bde7a2e"]  
[tls-version] [ssl] [info] zoom.com:443 ["tls12"]  
[ssl-issuer] [ssl] [info] zoom.com:443 ["DigiCert Inc"]  
[ssl-dns-names] [ssl] [info] zoom.com:443 ["*.zoom.com","zoom.com"]  
[wildcard-tls] [ssl] [info] zoom.com:443 ["CN: *.zoom.com","SAN: [*.zoom.com zoom.com]"]  
[mx-fingerprint] [dns] [info] zoom.com ["10 mxa-00569201.gslb.pphosted.com","10 mxb-00569201.gslb.pphosted.com"]  
[nameserver-fingerprint] [dns] [info] zoom.com ["ns-1861.awsdns-40.co.uk","ns-481.awsdns-60.com","ns-968.awsdns-57.net","ns-1473.awsdns-56.org"]  
[caa-fingerprint] [dns] [info] zoom.com  
[dmARC-detect] [dns] [info] _dmarc.zoom.com ["v=DMARC1;p=reject;ri=3600;fo=1;pct=1;rua=mailto:sesbounce@zoom.com,mailto:dmarc_rua@emaildefense.proofpoint.com;ruf=mailto:sesbounce@zoom.com,mailto:dmarc_ruf@emaildefense.proofpoint.com"]
```

As part of the passive reconnaissance and security evaluation of Zoom's exposed services, the **Qualys SSL Labs** tool was used to analyze the SSL/TLS certificate configuration of the main domain. This tool helps identify weak configurations, expired certificates, use of deprecated protocols, and other critical aspects that may pose a risk. The information provided by Qualys SSL is valuable for assessing the cryptographic security posture of the target organization.

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > zoom.com

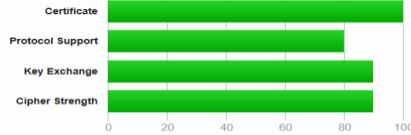
SSL Report: zoom.com (170.114.0.15)

Assessed on: Sun, 25 May 2025 20:09:17 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server does not support TLS 1.3. [MORE INFO](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

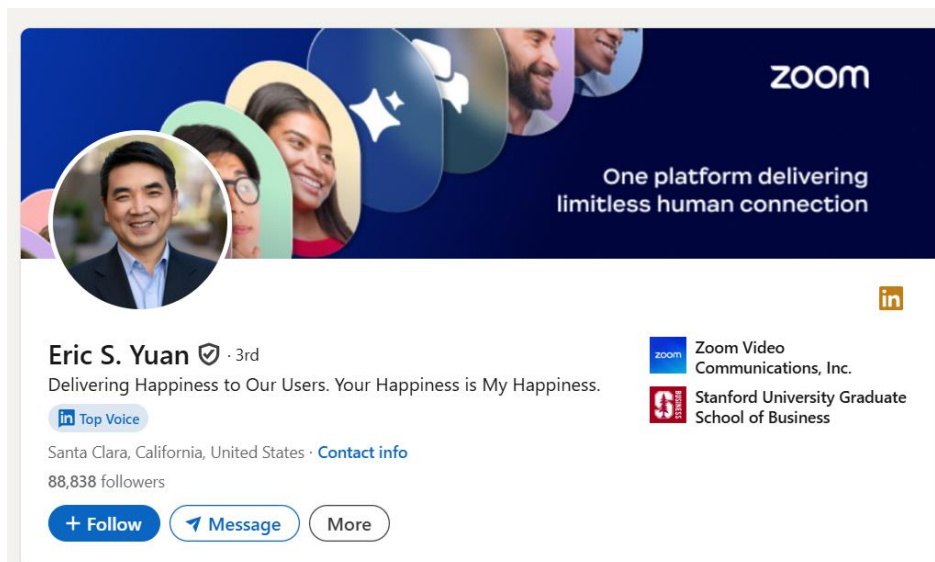
Subject	*.zoom.com Fingerprint SHA256: 7f57205804d062a93fcd296e17f0727e3a5e4ca545cfabd4c9e0c4f9d8650525 Pin SHA256: C7CPzP41ZISf5vSFAMF9cU7S9XwIG2o7yHm1T+YIGBY=
Common names	*.zoom.com
Alternative names	*.zoom.com zoom.com
Serial Number	0bb3c3045b897cae6212d8cfa5e05f3c
Valid from	Mon, 13 Jan 2025 00:00:00 UTC
Valid until	Sun, 17 Aug 2025 23:59:59 UTC (expires in 2 months and 23 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert Global G2 TLS RSA SHA256 2020 CA1 AIA: http://cacerts.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-1.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

During the analysis of Zoom's domain using Qualys SSL Labs, only two screenshots were captured to illustrate the relevance and depth of information provided by this tool. The page includes a detailed summary of the SSL/TLS configuration and the certificate in use — in this case, Certificate #1: RSA 2048 bits (SHA256withRSA). The Qualys SSL platform offers extensive data that can be thoroughly analyzed, including protocol support, key strength, cipher suites, and potential vulnerabilities. Although only a portion of the output is shown, the full report contains significantly more valuable security insights.

OSINT. (LinkedIn)

By leveraging LinkedIn, it is possible to gather valuable information about key members of Zoom's management team, including the CEO, CFO, CTO, and other executives. Their public profiles often reveal professional backgrounds, career trajectories, affiliations, skills, and sometimes even personal interests or connections. This data can be used for competitive analysis, social engineering, or to gain insight into the company's leadership structure and decision-making approach.

Eric Yuan, **Zoom CEO**



Michelle Chang, **Zoom CFO**



Michelle Chang  · 3rd

CFO Zoom

United States · [Contact info](#)


500+ connections



[Connect](#) [Message](#) [More](#)

 Zoom

 University of Washington

Xuedong Huang, Zoom CTO




Xuedong D. Huang   · 3rd


Chief Technology Officer

United States · [Contact info](#)

23,169 followers · 500+ connections

[+ Follow](#) [Message](#) [More](#)

 Zoom

 The University of Edinburgh

About

As the Chief Technology Officer (CTO) at Zoom, Xuedong (XD) Huang leads the company's AI efforts to enhance the user experience and productivity of millions of customers worldwide. With over 30 years of experience in the AI space, XD is a recognized leader and innovator, having achieved several industry-first human parity AI milestones with his Microsoft colleagues and holding over 170 US patents....[see more](#)

Other members of Zoom's Management Team

Management Team

**Eric S. Yuan**

Founder & Chief Executive Officer

[Read bio](#) ▾**Velchamy Sankarlingam**

President of Product and Engineering

[Read bio](#) ▾**Abhisht Arora**

Chief Strategy Officer

[Read bio](#) ▾**Aparna Bawa**

Chief Operating Officer

[Read bio](#) ▾**Vi Chau**

General Manager of Online Business

[Read bio](#) ▾**Michelle Chang**

Chief Financial Officer

[Read bio](#) ▾**Graeme Geddes**

Chief Sales and Growth Officer

[Read bio](#) ▾**Xuedong Huang**

Chief Technology Officer

[Read bio](#) ▾**Kimberly Storin**

Chief Marketing Officer

[Read bio](#) ▾**Gary J. Sorrentino**

Global Chief Information Officer

[Read bio](#) ▾**Sandra McLeod**

Chief Information Security Officer

[Read bio](#) ▾**Mu Han**

Chief Development Officer

[Read bio](#) ▾