

1) Perform Foot printing on Microsoft Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots

Domain Name: microsoft.com

Registry Domain ID: 2724960_DOMAIN_COM-VRSN

Registrar URL: <http://www.markmonitor.com>

Hosting company: Akamai Technologies

Hosting country: Netherland

IPv4 address 23.212.229.47

IPv4 autonomous systems: [AS20940](#)

IPv6 address: 2a02:26f0:71:49a:0:0:0:356e

IPv6 autonomous systems : [AS20940](#)

Reverse DNS: a23-212-229-47.deploy.static.akamaitechnologies.com

DNS admin : azuredns-hostmaster@microsoft.com

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Email: **abusecomplaints**@markmonitor.com

Subject Alternative Name:

wwwqa.microsoft.com

www.microsoft.com

Staticview.microsoft.com

i.s-microsoft.com

microsoft.com

c.s-microsoft.com

privacy.microsoft.com

Date :

Creation Date: 1991-05-01T21:00:00-0700

Expiration Date: 2022-05-02T00:00:00-0700

Updated Date: 2021-04-07T12:58:15-0700

Domain Status:

clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)

ClientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)

clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)

serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)

serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)

serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)

Registry Registrant ID:

Tech Name: MSN Hostmaster

Registrant Name: Domain Administrator

Organization: Microsoft Corporation

Street: One Microsoft Way

City: Redmond

State/Province: WA

Postal Code: 98052

Country: US

Phone: +1.4258828080

Fax: +1.4259367329

Email: **adnin**@domains.microsoft

Tech Email: **nsnhst**@microsoft.com

Servers:

Name Server: ns2-205.azure-dns.net

Name Server: ns3-205.azure-dns.org

Name Server: ns4-205.azure-dns.info

Name Server: ns1-205.azure-dns.com

DNSSEC: unsigned

IP delegation:

IPv4 address (23.212.229.47)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 23.0.0.0-23.255.255.255	United States	NET23	American Registry for Internet Numbers
↳ 23.192.0.0-23.223.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 23.212.228.0-23.212.231.255	Netherlands	AIBV	Akamai International, BV
↳ 23.212.229.47	Netherlands	AIBV	Akamai International, BV

IPv6 address (2a02:26f0:71:49a:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
↳ 2a02:26f0:71:49a:0:0:0:356e	European Union	EU-AKAMAI-20101022	Akamai International B.V.

SSL/TLS:

Public key algorithm : rsaEncryption

Serial number : 0x6b000003f4e3a67a2348550c330000000003f4

Certificate Revocation Lists:

<http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl>

<http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl>

Certificate Hash: eA9INc7iN2GD2kDDp1axPmscNsA

Public Key Hash: e01f082db576faf2c5b3426c66e79e53140ec299c645f26aa6342e7cb073ad4a

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2021 9lyUL9F3MCIUVBgl MJRWjuNNEzkzv98 MLyALzE7xZOM=	2020-08-28 22:27:05	Success
Certificate	Cloudflare Nimbus 2021 RJRIrDuzq/EQAfYq P4owNrmgr7YyzG1 P9MzlrW2gag=	2020-08-28 22:27:05	Success



Domain Information

Domain: microsoft.com

Registrar: MarkMonitor Inc.

Registered On: 1991-05-02

Expires On: 2022-05-02

Updated On: 2021-03-12

Status: clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited
serverDeleteProhibited
serverTransferProhibited
serverUpdateProhibited

Name Servers: ns1-205.azure-dns.com
ns2-205.azure-dns.net
ns3-205.azure-dns.org
ns4-205.azure-dns.info



Registrant Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin @domains.microsoft



Technical Contact

Name:	MSN Hostmaster
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	msnhst @microsoft.com




Administrative Contact









Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin @domains.microsoft

IP delegation

IPv4 address (23.212.229.47)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
 23.0.0.0-23.255.255.255	 United States	NET23	American Registry for Internet Numbers
 23.192.0.0-23.223.255.255	 United States	AKAMAI	Akamai Technologies, Inc.
 23.212.228.0-23.212.231.255	 Netherlands	AIBV	Akamai International, BV
 23.212.229.47	 Netherlands	AIBV	Akamai International, BV

IPv6 address (2a02:26f0:71:49a:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
 2a00::/11	 European Union	EU-ZZ-2A00	RIPE NCC
 2a00::/12	 Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
 2a02:26f0::/29	 European Union	EU-AKAMAI-20101022	Akamai International B.V.
 2a02:26f0:71:49a:0:0:0:356e	 European Union	EU-AKAMAI-20101022	Akamai International B.V.

Signature algorithm	sha256WithRSAEncryption
Serial number	0x6b000003f4e3a67a2348550c330000000003f4
Certificate Revocation Lists	http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl
Certificate Hash	eA9INc7IN2GD2kDDp1axPmscNsA
Public Key Hash	e01f082db576faf2c5b3426c66e79e53140ec299c645f26aa6342e7cb073ad4a

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2021 91yUL9F3MCIUVBgIMJRWjuNNExkz v98MLyALzE7xZOM=	2020-08-28 22:27:05	Success
Certificate	Cloudflare Nimbus 2021 RJRLrDuzq/EQAfYqP4owNrnmgr 7Y yzG1P9Mz1rW2gag=	2020-08-28 22:27:05	Success

Countermeasures for Footprinting:

- Restrict the employees to access social networking sites from organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogues, etc.
- Limit the amount of information that you are publishing on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available