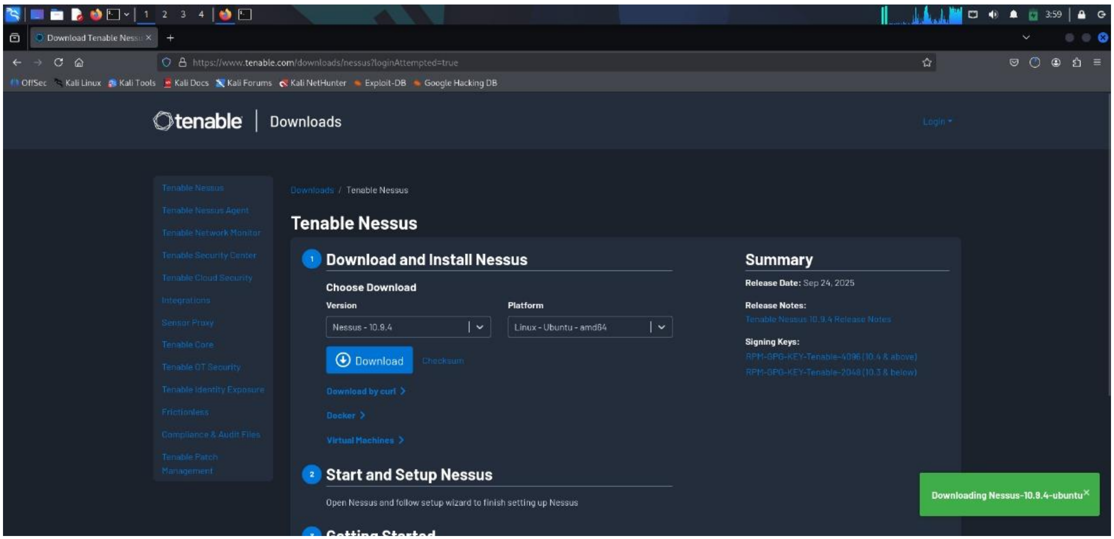


Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.9.4

Platform: Linux - Ubuntu - amd64

Download Checksum

Download by curl >

Docker >

Virtual Machines >

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

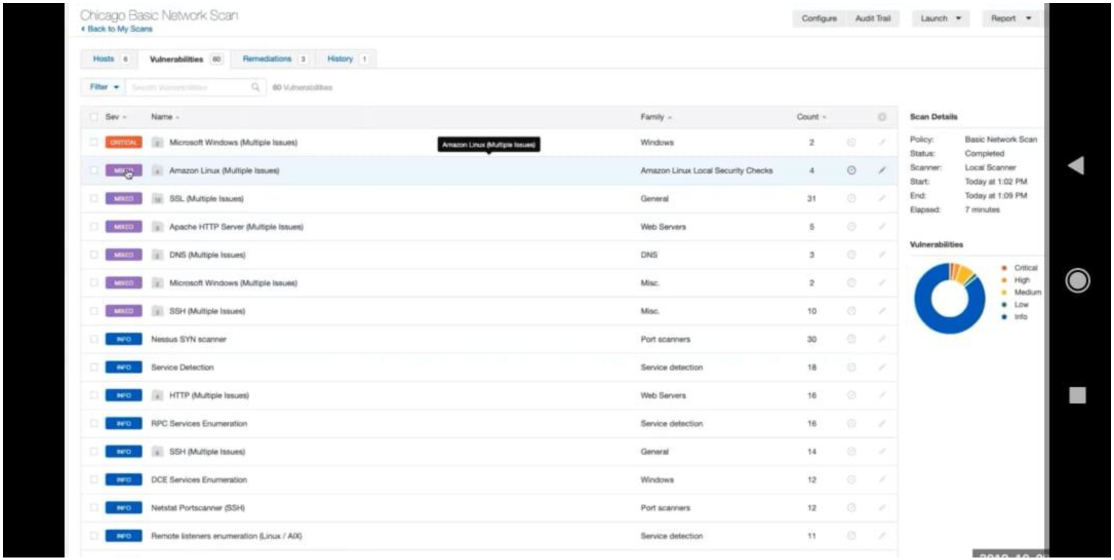
Summary

Release Date: Sep 24, 2025

Release Notes: Tenable Nessus 10.9.4 Release Notes

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

Downloading Nessus-10.9.4-ubuntu



Chicago Basic Network Scan

‹ Back to My Scans

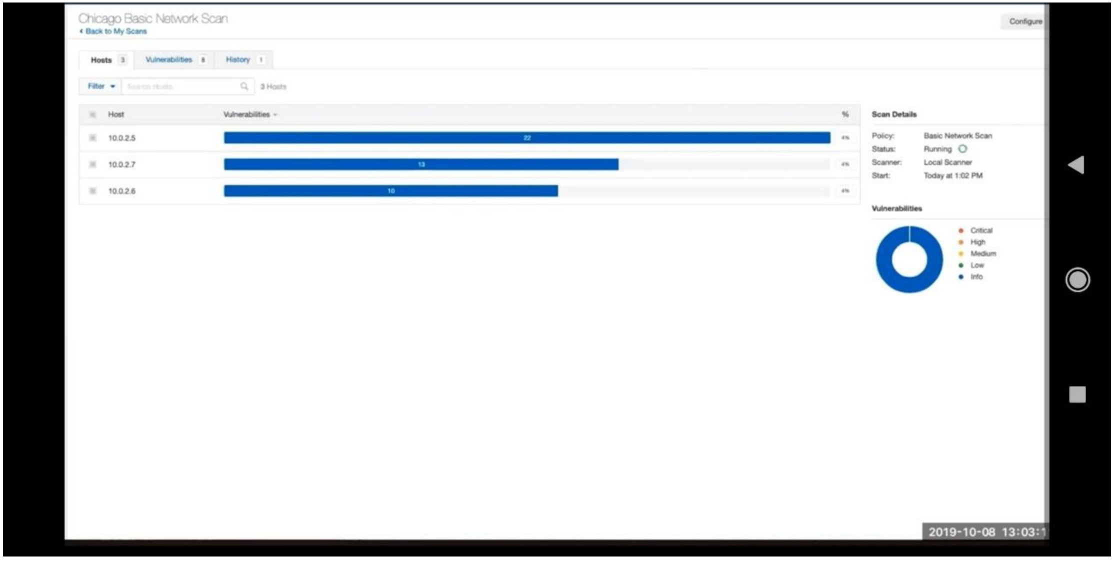
60 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Microsoft Windows (Multiple Issues)	Windows	2
MIXED	Amazon Linux (Multiple Issues)	Amazon Linux Local Security Checks	4
MIXED	SSL (Multiple Issues)	General	31
MIXED	Apache HTTP Server (Multiple Issues)	Web Servers	5
MIXED	DNS (Multiple Issues)	DNS	3
MIXED	Microsoft Windows (Multiple Issues)	Misc.	2
MIXED	SSH (Multiple Issues)	Misc.	10
INFO	Nessus SYN scanner	Port scanners	30
INFO	Service Detection	Service detection	18
INFO	HTTP (Multiple Issues)	Web Servers	16
INFO	RPC Services Enumeration	Service detection	16
INFO	SSH (Multiple Issues)	General	14
INFO	DCE Services Enumeration	Windows	12
INFO	Netstat Portscanner (SSH)	Port scanners	12
INFO	Remote listeners enumeration (Linux / AIX)	Service detection	11

Scan Details

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 1:02 PM
End: Today at 1:09 PM
Elapsed: 7 minutes

Vulnerabilities



Chicago Basic Network Scan

‹ Back to My Scans

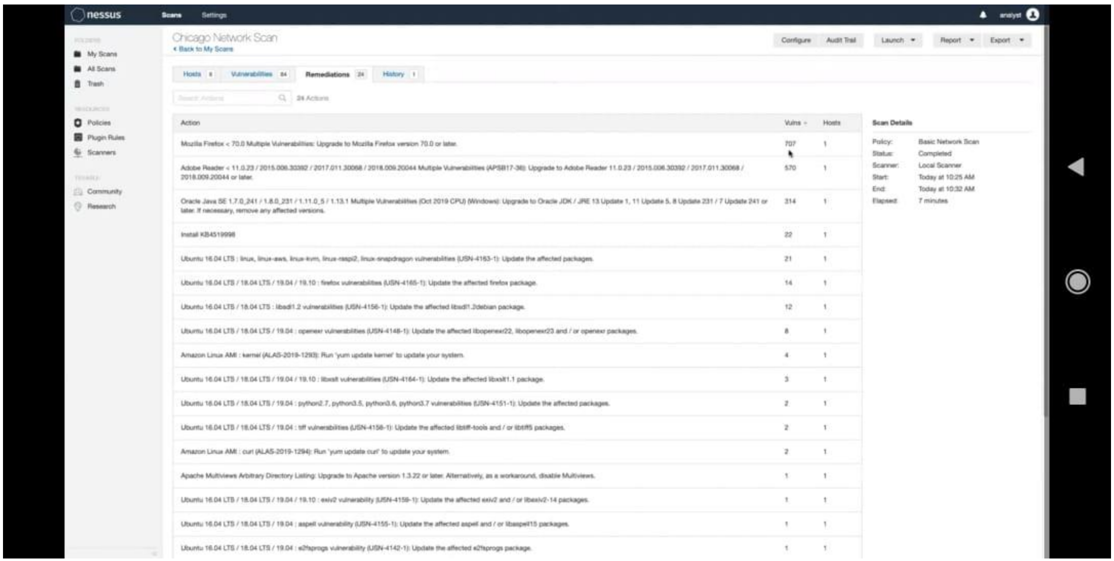
3 Hosts

Host	Vulnerabilities	%
10.0.2.5	22	4%
10.0.2.7	13	4%
10.0.2.6	10	4%

Scan Details

Policy: Basic Network Scan
Status: Running
Scanner: Local Scanner
Start: Today at 1:02 PM

Vulnerabilities



Chicago Network Scan

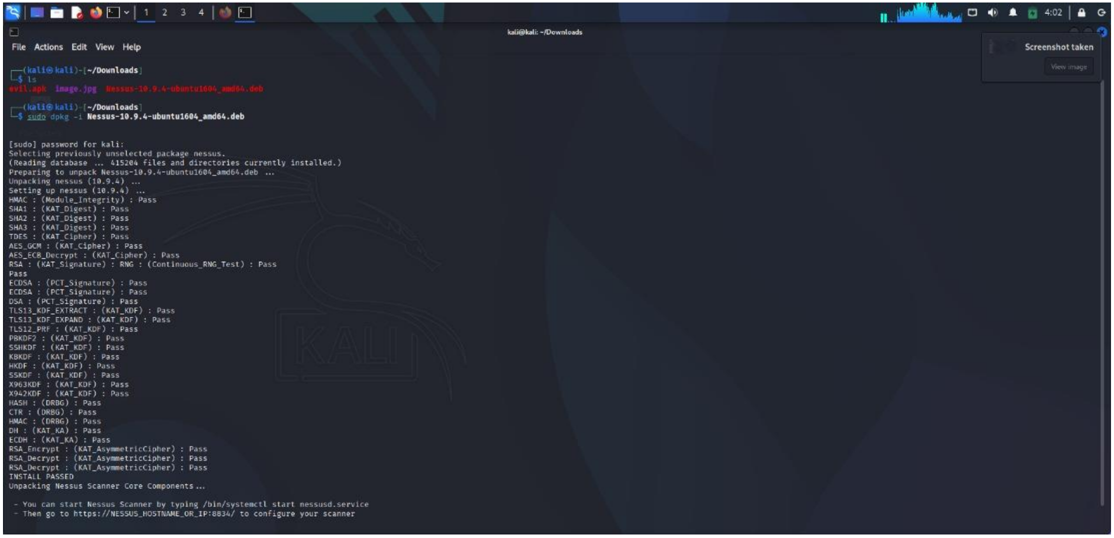
‹ Back to My Scans

24 Actions

Action	Vulns	Hosts
Mozilla Firefox < 70.0 Multiple Vulnerabilities: Upgrade to Mozilla Firefox version 70.0 or later.	707	1
Adobe Reader < 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 Multiple Vulnerabilities (APSB17-36): Upgrade to Adobe Reader 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 or later.	570	1
Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows): Upgrade to Oracle JDK / JRE 13 Update 1, 11 Update 5, 8 Update 231 / 7 Update 241 or later. If necessary, remove any affected versions.	314	1
Install KB4519998	22	1
Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4163-1): Update the affected packages.	21	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : firefox vulnerabilities (USN-4165-1): Update the affected firefox package.	14	1
Ubuntu 16.04 LTS / 18.04 LTS : libsdl1.2 vulnerabilities (USN-4156-1): Update the affected libsdl1.2debian package.	12	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : openexr vulnerabilities (USN-4148-1): Update the affected libopenexr22, libopenexr23 and / or openexr packages.	8	1
Amazon Linux AMI : kernel (ALAS-2019-1293): Run 'yum update kernel' to update your system.	4	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : libxslt vulnerabilities (USN-4164-1): Update the affected libxslt1.1 package.	3	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : python2.7, python3.5, python3.6, python3.7 vulnerabilities (USN-4151-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : tiff vulnerabilities (USN-4158-1): Update the affected libtiff-tools and / or libtiff5 packages.	2	1
Amazon Linux AMI : curl (ALAS-2019-1294): Run 'yum update curl' to update your system.	2	1
Apache Multiviews Arbitrary Directory Listing: Upgrade to Apache version 1.3.22 or later. Alternatively, as a workaround, disable Multiviews.	1	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : exiv2 vulnerability (USN-4159-1): Update the affected exiv2 and / or libexiv2-14 packages.	1	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : aspell vulnerability (USN-4155-1): Update the affected aspell and / or libaspell15 packages.	1	1
Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : e2fsprogs vulnerability (USN-4142-1): Update the affected e2fsprogs package.	1	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 10:25 AM
End:	Today at 10:32 AM
Elapsed:	7 minutes

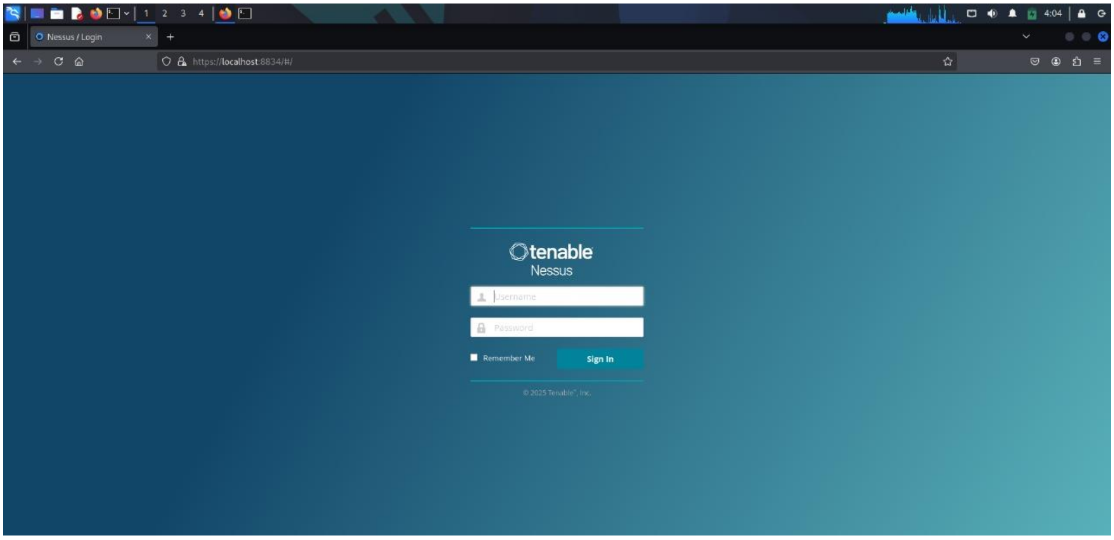


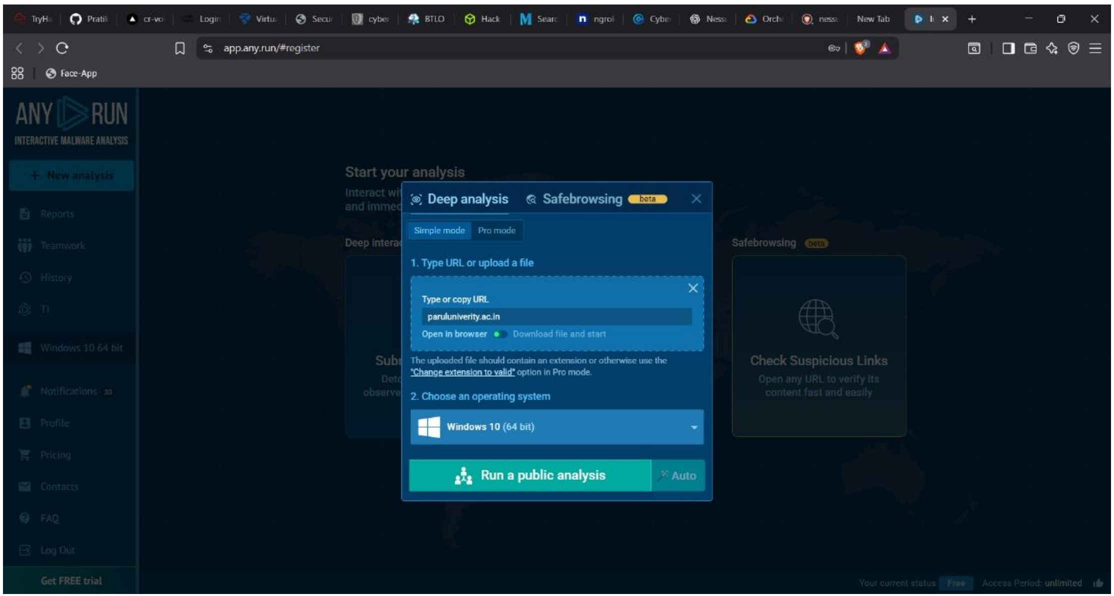
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
evil.apk  image.jpg  Nessus-10.9.4-ubuntu1604_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.9.4-ubuntu1604_amd64.deb

[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 415204 files and directories currently installed.)
Preparing to unpack Nessus-10.9.4-ubuntu1604_amd64.deb ...
Unpacking nessus (10.9.4) ...
Setting up nessus (10.9.4) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner
```





app.any.run/#register

Deep analysis | Safebrowsing beta

Simple mode | Pro mode

1. Type URL or upload a file

Type or copy URL

paruluniverity.ac.in

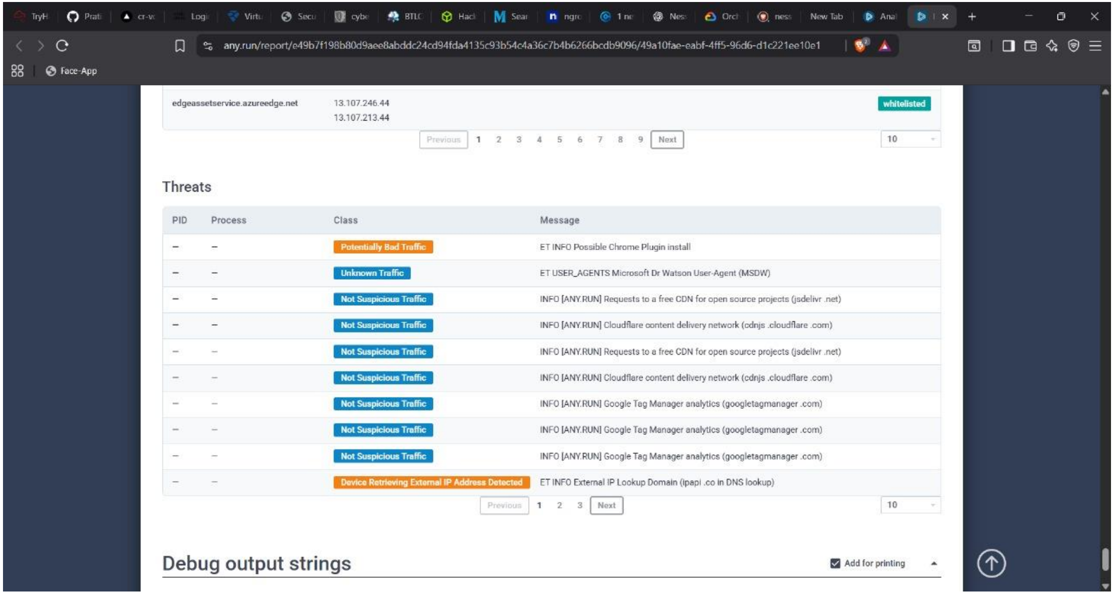
Open in browser ● Download file and start

The uploaded file should contain an extension or otherwise use the "Change extension to valid" option in Pro mode.

2. Choose an operating system

Windows 10 (64 bit)

Run a public analysis | Auto



any.run/report/e49b7f198b80d9aee8abddc24cd94fda4135c93b54c4a36c7b4b6266bcdb9096/49a10fae-eabf-4ff5-96d6-d1c221ee10e1

edgeassetservice.azureedge.net	13.107.246.44 13.107.213.44	whitelisted

Previous 1 2 3 4 5 6 7 8 9 Next

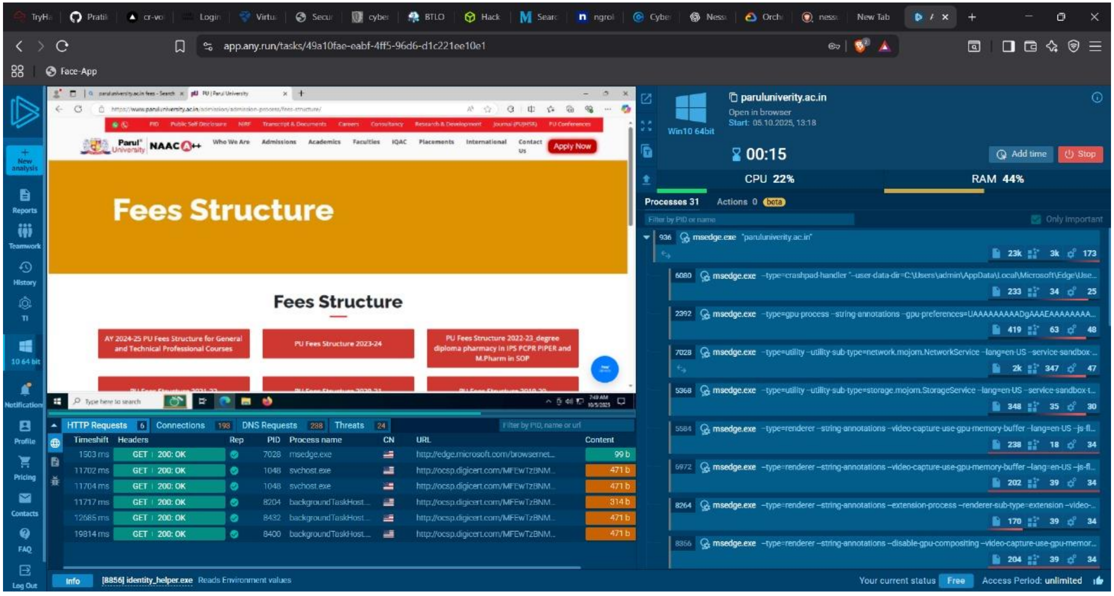
Threats

PID	Process	Class	Message
–	–	Potentially Bad Traffic	ET INFO Possible Chrome Plugin install
–	–	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Requests to a free CDN for open source projects (jsdelivr .net)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare content delivery network (cdnjs .cloudflare .com)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Requests to a free CDN for open source projects (jsdelivr .net)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Cloudflare content delivery network (cdnjs .cloudflare .com)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Google Tag Manager analytics (googletagmanager .com)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Google Tag Manager analytics (googletagmanager .com)
–	–	Not Suspicious Traffic	INFO [ANY.RUN] Google Tag Manager analytics (googletagmanager .com)
–	–	Device Retrieving External IP Address Detected	ET INFO External IP Lookup Domain (ipapi .co in DNS lookup)

Previous 1 2 3 Next

Debug output strings

☑ Add for printing



app.any.run/tasks/49a10fae-eabf-4ff5-96d6-d1c221ee10e1

Parul University
NAAC A++
Apply Now
Fees Structure
Fees Structure
AY 2024-25 PU Fees Structure for General and Technical Professional Courses
PU Fees Structure 2023-24
PU Fees Structure 2022-23_degree diploma pharmacy in IPS PCPR PIPER and M.Pharm in SOP
Type here to search
7:49 AM
10/5/2025

paruluniverity.ac.in

Open in browser

Start: 05.10.2025, 13:18

Win10 64bit

00:15 | Add time | Stop

CPU 22% RAM 44%

Processes 31 Actions 0 beta

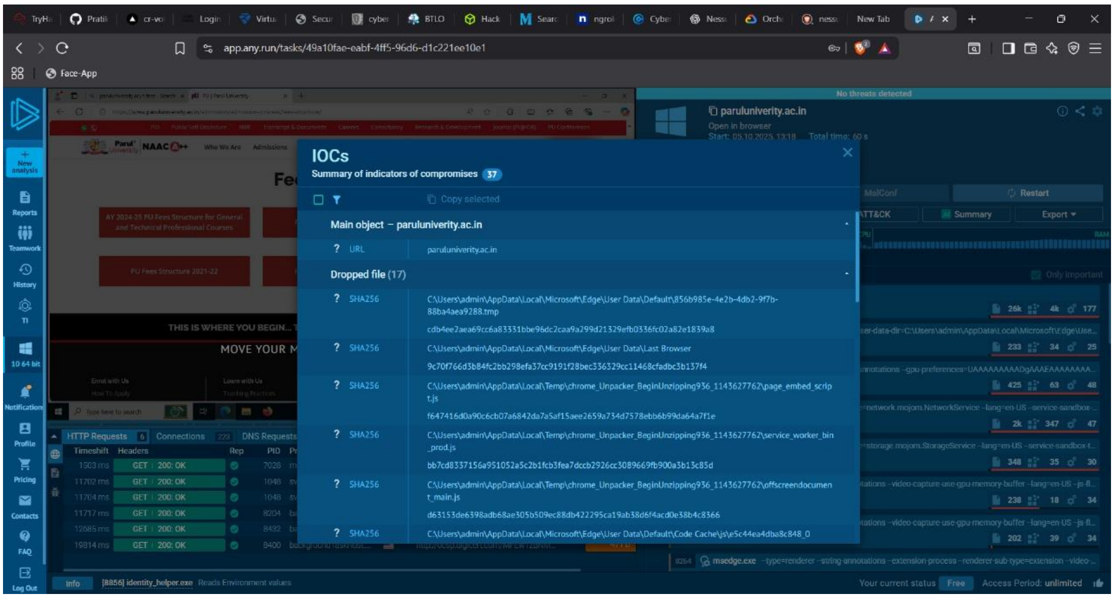
```
936  msedge.exe "paruluniverity.ac.in"                                                                23k  3k  173
  6080  msedge.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Microsoft\Edge\Use...   233  34  25
  2392  msedge.exe --type=gpu-process --string-annotations --gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAA...        419  63  48
  7028  msedge.exe --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-...  2k  347  47
  5368  msedge.exe --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-t...  348  35  30
  5584  msedge.exe --type=renderer --string-annotations --video-capture-use-gpu-memory-buffer --lang=en-US --js-fl...  238  18  34
  6972  msedge.exe --type=renderer --string-annotations --video-capture-use-gpu-memory-buffer --lang=en-US --js-fl...  202  39  34
  8264  msedge.exe --type=renderer --string-annotations --extension-process --renderer-sub-type=extension --video-...  170  39  34
  8356  msedge.exe --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memor...  204  39  34
```

HTTP Requests 6 | Connections 193 | DNS Requests 288 | Threats 24

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
1503 ms	GET 200: OK	✓	7028	msedge.exe	🇺🇸	http://edge.microsoft.com/browsernet...	99 b
11702 ms	GET 200: OK	✓	1048	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNM...	471 b
11704 ms	GET 200: OK	✓	1048	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNM...	471 b
11717 ms	GET 200: OK	✓	8204	backgroundTaskHost...	🇺🇸	http://ocsp.digicert.com/MFEwTzBNM...	314 b
12685 ms	GET 200: OK	✓	8432	backgroundTaskHost...	🇺🇸	http://ocsp.digicert.com/MFEwTzBNM...	471 b
19814 ms	GET 200: OK	✓	8400	backgroundTaskHost...	🇺🇸	http://ocsp.digicert.com/MFEwTzBNM...	471 b

Info [8856] identity_helper.exe Reads Environment values

Your current status Free Access Period: unlimited



IOCs

Summary of indicators of compromises 37

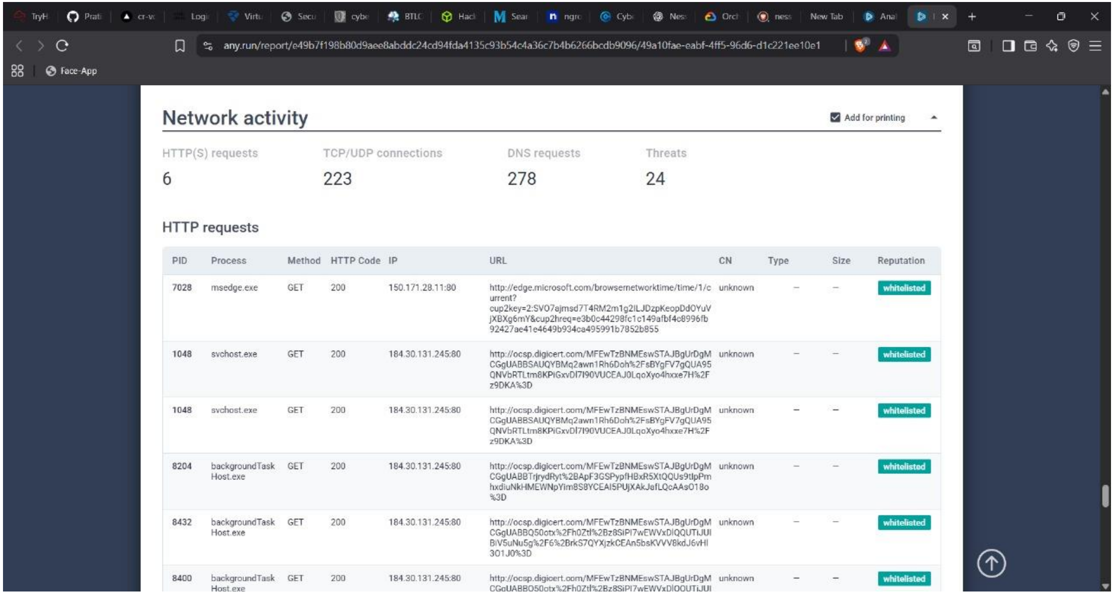
□ Copy selected

Main object – paruluniverity.ac.in

?	URL	paruluniverity.ac.in

Dropped file (17)

?	SHA256	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\856b985e-4e2b-4db2-9f7b-88ba4aea9288.tmp cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
?	SHA256	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Browser 9c70f766d3b84fc2bb298efa37cc9191f28bec336329cc11468cfadbc3b137f4
?	SHA256	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping936_1143627762\page_embed_script.js f647416d0a90c6cb07a6842da7a5af15aee2659a734d7578ebb6b99da64a7f1e
?	SHA256	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping936_1143627762\service_worker_bin_prod.js bb7cd8337156a951052a5c2b1fcb3fea7dccb2926cc3089669fb900a3b13c85d
?	SHA256	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping936_1143627762\offscreendocument_main.js d63153de6398adb68ae305b509ec88db422295ca19ab38d6f4acd0e38b4c8366
?	SHA256	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\e5c44ea4dba8c848_0

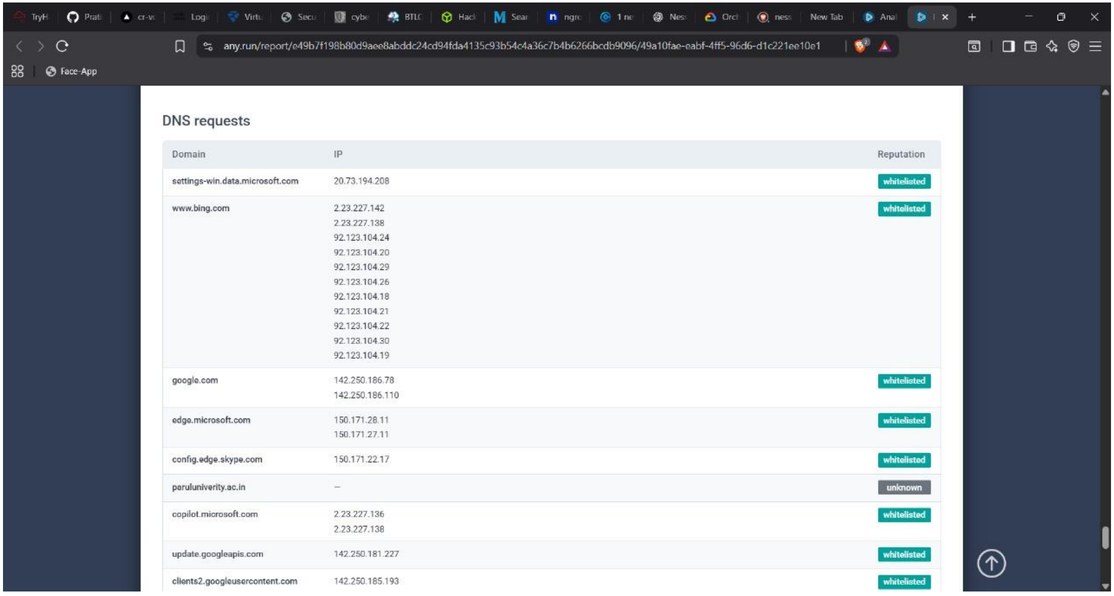

any.run/report/e49b7f198b80d9aee8abddc24cd94fda4135c93b54c4a36c7b4b6266bcdb9096/49a10fae-eabf-4ff5-96d6-d1c221ee10e1
☑ Add for printing

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
6	223	278	24

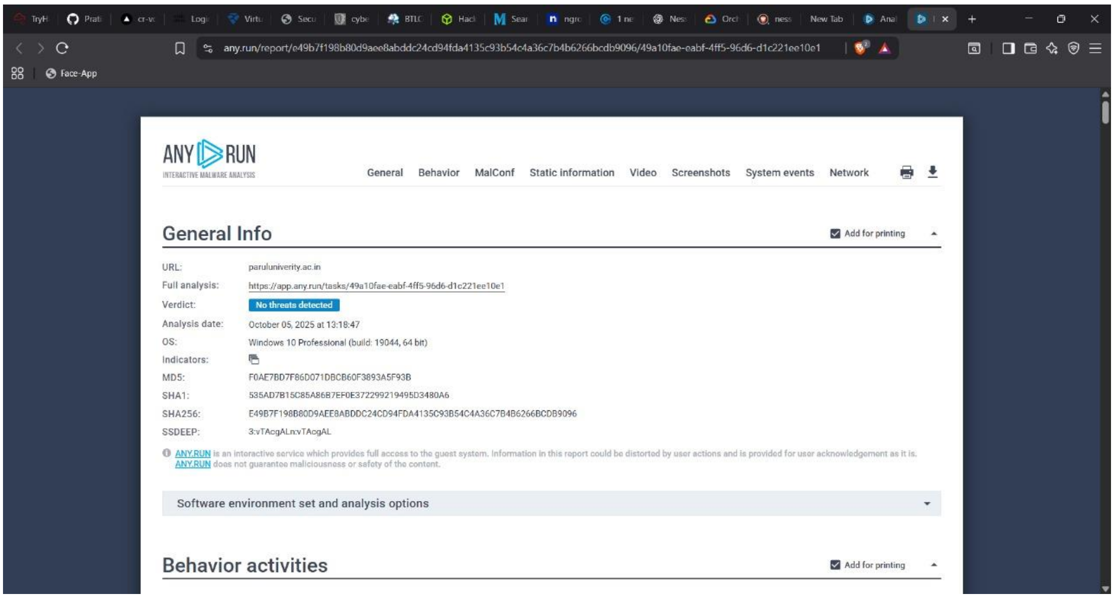
HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
7028	msedge.exe	GET	200	150.171.28.11:80	http://edge.microsoft.com/browsernetworktime/time/1/current?cup2key=2:SVO7ajmsd7T4RM2m1g2ILJDzpKeopDdOYuVjXBXg6mY&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	unknown	–	–	whitelisted
1048	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
1048	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
8204	backgroundTaskHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tlpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	–	–	whitelisted
8432	backgroundTaskHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPl7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	–	–	whitelisted
8400	backgroundTaskHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPl7wEWVxDlQQUTiJUI	unknown	–	–	whitelisted


any.run/report/e49b7f198b80d9aee8abddc24cd94fda4135c93b54c4a36c7b4b6266bcdb9096/49a10fae-eabf-4ff5-96d6-d1c221ee10e1

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	20.73.194.208	whitelisted
www.bing.com	2.23.227.142 2.23.227.138 92.123.104.24 92.123.104.20 92.123.104.29 92.123.104.26 92.123.104.18 92.123.104.21 92.123.104.22 92.123.104.30 92.123.104.19	whitelisted
google.com	142.250.186.78 142.250.186.110	whitelisted
edge.microsoft.com	150.171.28.11 150.171.27.11	whitelisted
config.edge.skype.com	150.171.22.17	whitelisted
paruluniverity.ac.in	–	unknown
copilot.microsoft.com	2.23.227.136 2.23.227.138	whitelisted
update.googleapis.com	142.250.181.227	whitelisted
clients2.googleusercontent.com	142.250.185.193	whitelisted



any.run/report/e49b7f198b80d9aee8abddc24cd94fda4135c93b54c4a36c7b4b6266bcdb9096/49a10fae-eabf-4ff5-96d6-d1c221ee10e1

General Info

☑ Add for printing

URL: paruluniverity.ac.in

Full analysis: https://app.any.run/tasks/49a10fae-eabf-4ff5-96d6-d1c221ee10e1

Verdict: No threats detected

Analysis date: October 05, 2025 at 13:18:47

OS: Windows 10 Professional (build: 19044, 64 bit)

Indicators:

MD5: F0AE7BD7F86D071DBCB60F3893A5F93B

SHA1: 535AD7B15C85A86B7EF0E372299219495D3480A6

SHA256: E49B7F198B80D9AEE8ABDDC24CD94FDA4135C93B54C4A36C7B4B6266BCDB9096

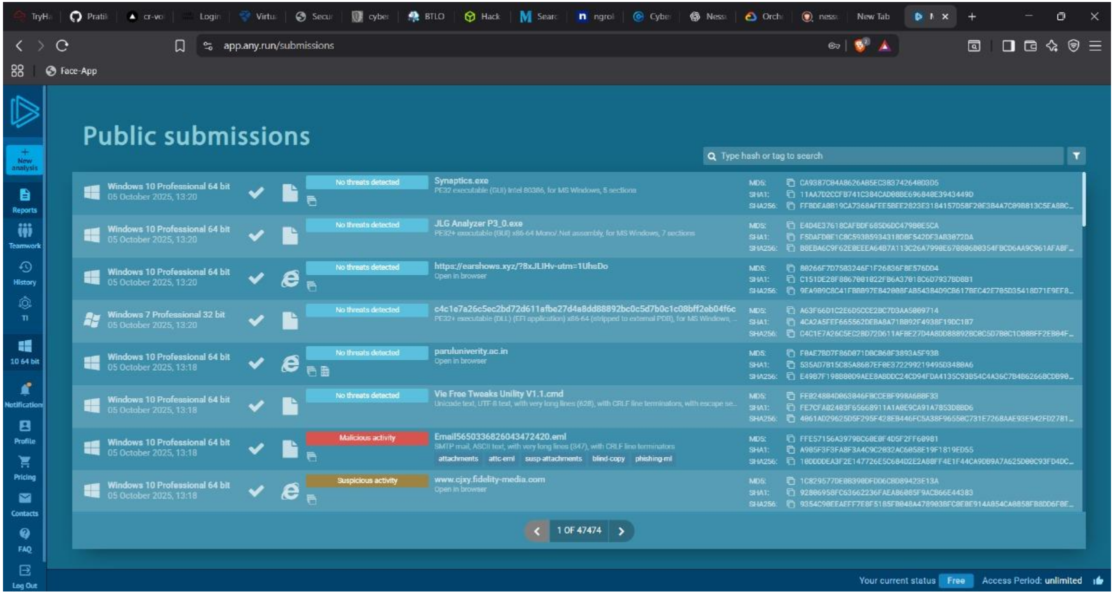
SSDEEP: 3:vTAcgALn:vTAcgAL

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

☑ Add for printing



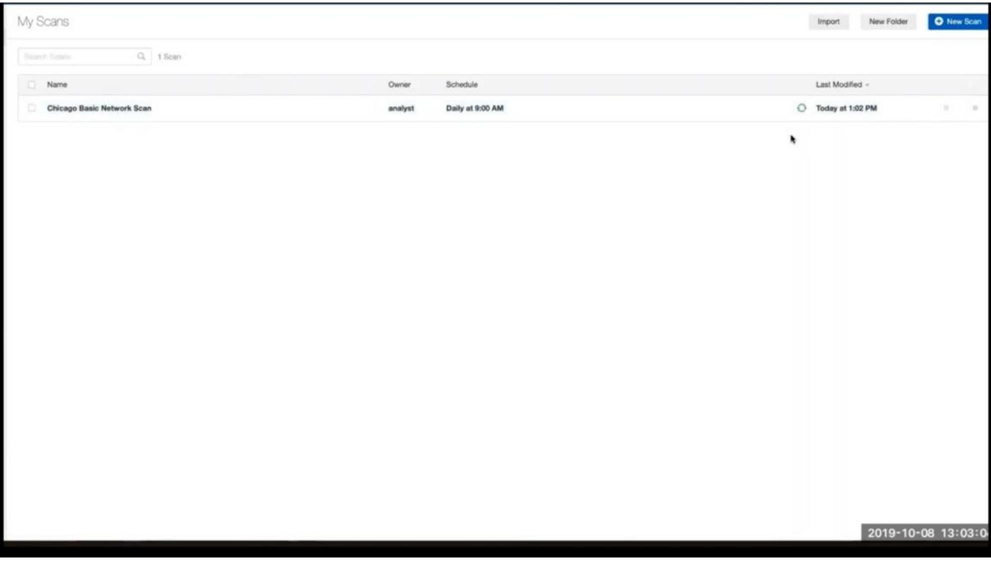
app.any.run/submissions

Public submissions

Windows 10 Professional 64 bit 05 October 2025, 13:20	No threats detected	Synaptics.exe PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections	MD5: CA9387C84A8626A85EC3837426480305 SHA1: 11AA7D2CCFB741C384CAD088E696848E3943449D SHA256: FFBDEA8B19CA7368AFEE58EE2823E3184157D58F28E384A7C89B813C5EA8BC…
Windows 10 Professional 64 bit 05 October 2025, 13:20	No threats detected	JLG Analyzer P3_0.exe PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows, 7 sections	MD5: E4D4E37618CAFBDF685D6DC47980E5CA SHA1: F5DAFD0E1C8C593B5934318D8F542DF3AB3072DA SHA256: B8EBA6C9F62E8EEEA64B7A113C26A7990E67080680354FBCD6AA9C961AFABF…
Windows 10 Professional 64 bit 05 October 2025, 13:20	No threats detected	https://earshows.xyz/?8xJLIHv-utm=1UhsDo Open in browser	MD5: 80266F7D7503246F1F26836F8E576DD4 SHA1: C151DE28F8867001822FB6A37018C6D7937BD8B1 SHA256: 9EA9B9C8C41FB8897E842008FAB5438409CB617BEC42E785D35418D71E9EF8…
Windows 7 Professional 32 bit 05 October 2025, 13:20	No threats detected	c4c1e7a26c5ec2bd72d611afbe27d4a8dd88892bc0c5d7b0c1c08bff2eb04f6c PE32+ executable (DLL) (EFI application) x86-64 (stripped to external PDB), for MS Windows, …	MD5: A63F66D1C2E6D5CCE2BC7D3AA5009714 SHA1: 4CA2A5FEF665562DEBA8A71B892F4938F19DC187 SHA256: C4C1E7A26C5EC2BD72D611AFBE27D4A8DD88892BC0C5D7B0C1C088FF2EB04F…
Windows 10 Professional 64 bit 05 October 2025, 13:18	No threats detected	paruluniverity.ac.in Open in browser	MD5: F0AE7BD7F86D071DBCB60F3893A5F93B SHA1: 535AD7B15C85A86B7EF0E372299219495D3480A6 SHA256: E49B7F198B80D9AEE8ABDDC24CD94FDA4135C93B54C4A36C7B4B6266BCDB90…
Windows 10 Professional 64 bit 05 October 2025, 13:18	No threats detected	Vie Free Tweaks Unility V1.1.cmd Unicode text, UTF-8 text, with very long lines (628), with CRLF line terminators, with escape se…	MD5: FE824884D063046F8CCE8F998A688F33 SHA1: FE7CFA82403F65668911A1A0E9CA91A7853D88D6 SHA256: 4061AD29625D5F295F428EB446FC5A38F96558C731E7268AAE93E942FD2781…
Windows 10 Professional 64 bit 05 October 2025, 13:18	Malicious activity	Email5650336826043472420.eml SMTP mail, ASCII text, with very long lines (347), with CRLF line terminators attachments attc-eml susp-attachments blind-copy phishing-ml	MD5: FFE57156A3979BC60E8F4D5F2FF60981 SHA1: A985F3F3FA8F3A4C9C2832AC6058E19F1819ED55 SHA256: 160DDDEA3F2E147726E5C684D2E2A88FF4E1F44CA9DB9A7A625D00C93FD4DC…
Windows 10 Professional 64 bit 05 October 2025, 13:18	Suspicious activity	www.cjxy.fidelity-media.com Open in browser	MD5: 1C829577DE88398DFDD6C8D89423E13A SHA1: 92806958FC63662236FAEA86085F9ACB66E44383 SHA256: 9354C98EEAFFF7E8F5185FB848A478903BFC8E8E914A854CA8858FB8DD6F8E…

1 OF 47474

Your current status Free Access Period: unlimited



My Scans

Name	Owner	Schedule	Last Modified
Chicago Basic Network Scan	analyst	Daily at 9:00 AM	Today at 1:02 PM

2019-10-08 13:03:0