

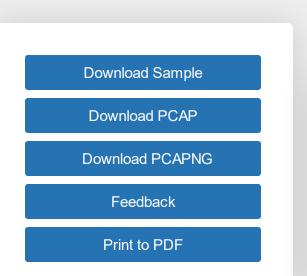
Submit

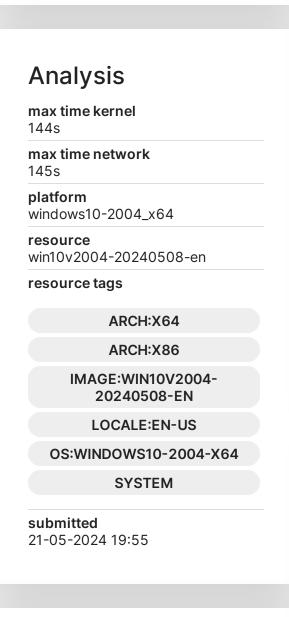
Reports

Overview

overview

sample.html windows10-2004-x64



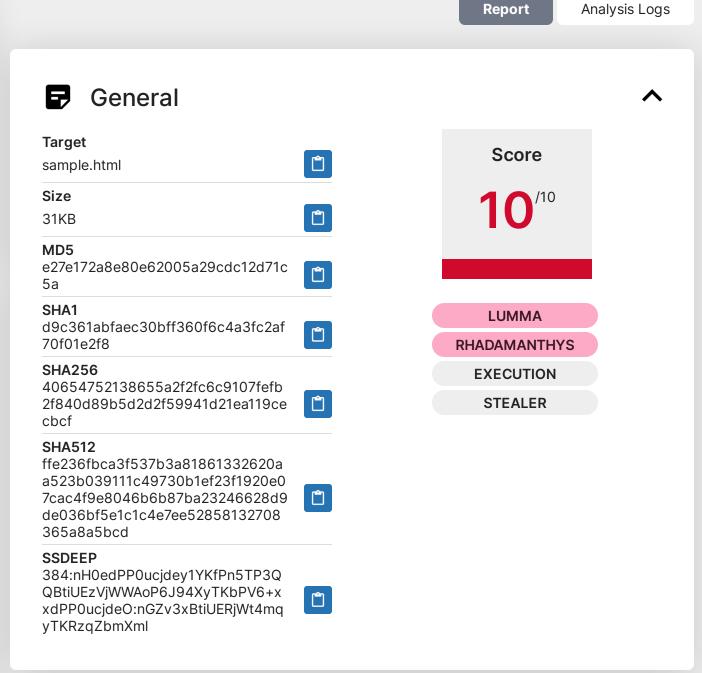


Copy URL

Twitter

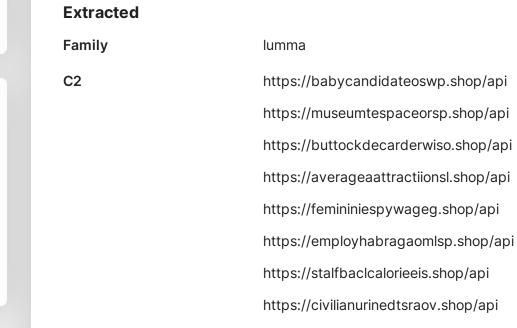
E-mail

Sharing



Static

static



Malware Config

about your privacy

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.

Accept

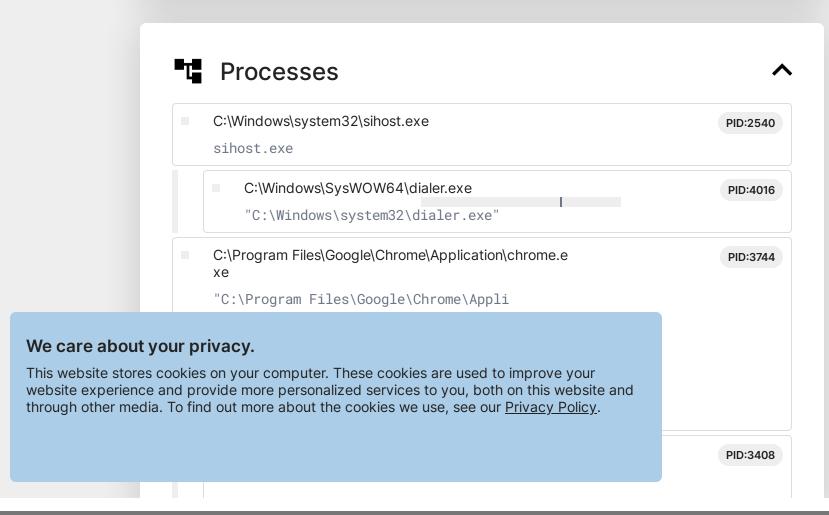
Copy all

Execution Discovery

Command and Control

https://roomabolishsnifftwk.shop/api





"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=crash pad-handler "--user-data-dir=C:\Us ers\Admin\AppData\Local\Google\Chr ome\User Data" /prefetch:7 --monit or-self-annotation=ptype=crashpadhandler "--database=C:\Users\Admin Data\Crashpad" "--metrics-dir=C:\U sers\Admin\AppData\Local\Google\Ch rome\User Data" --url=https://clie nts2.google.com/cr/report --annota tion=channel= --annotation=plat=Wi n64 --annotation=prod=Chrome --ann otation=ver=110.0.5481.104 --initi al-client-data=0xfc,0x100,0x104,0x d8, 0x108, 0x7fffadd2ab58, 0x7fffadd2 ab68,0x7fffadd2ab78

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:3772

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:932

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=network.mojo m.NetworkService --langen of service-sandbox-type=none --mojo-pla tform-channel-handle=2152 --field-trial-handle=1748,i,15457931719572 670153,4062602848324179866,131072 /prefetch:8

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:4760

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=storage.mojo m.StorageService --langer os service-sandbox-type=service --mojo-platform-channel-handle=2248 --fie ld-trial-handle=1748,i,15457931719 572670153,4062602848324179866,1310 72 /prefetch:8

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:3892

"C:\Program Files\Google\Chrome\Ap
plication\chrome.exe" --type=rende
rer --first-renderer-process --lan
g=en-US --device-scale-factor=1 -num-raster-threads=4 - Enable main
-frame-before-activation --rendere

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

PID:2744

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=rende rer --lang=en-US --device-scale-fa ctor=1 --num-raster-threads=4 --en able-main-frame-before-activation --renderer-client-id=5 --mojo-plat form-channel-handle=2908 --field-t rial-handle=1748,i,154579317195726 70153,4062602848324179866,131072 / prefetch:1

C:\Program Files\Google\Chrome\Application\chrom

PID:2836

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.ProcessorMetrics --lang=en-US -service-sandbox-type=none --mojo-p latform-channel-handle=4320 --fiel d-trial-handle=1748, i, 154579317195 72670153, 4062602848324179866, 13107 2 /prefetch:8

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:3816

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.UtilWin --lang=en-US --service-s andbox-type=none --mojo-platform-c hannel-handle=4500 --field-trial-h andle=1748, i, 15457931719572670153, 4062602848324179866,131072 /prefet

C:\Program Files\Google\Chrome\Application\chrom

PID:1688

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=rende rer --lang=en-US --device-scale-fa ctor=1 --num-raster-threads=4 --en able-main-frame-before-activation --renderer-client-id=9 --mojo-plat form-channel-handle=4792 --field-t rial-handle=1748, i, 154579317195726 70153,4062602848324179866,131072 / prefetch:1

C:\Program Files\Google\Chrome\Application\chrom

PID:4004

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=audio.mojom. AudioService --lang=en-Us service e-sandbox-type=audio --mojo-platfo rm-channel-handle=3192 --field-tri al-handle=1748, i, 15457931719572670 153,4062602848324179866,131072 /pr efetch:8

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:1988

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=rende rer --lang=en-US --device-scale-fa ctor=1 --num-raster-threads=4 --en

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

PID:4696

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chreme.mojo m.UtilWin --lang=en-US --service-s andbox-type=none --mojo-platform-c hannel-handle=4872 --field-trial-h andle=1748, i, 15457931719572670153, 4062602848324179866,131072 /prefet ch:8 "C:\Program Files\Google\Chrome\Ap

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:232

plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.UtilReadIcon --lang=en-US --serv ice-sandbox-type=icon_reader --moj o-platform-channel-handle=5148 --f ield-trial-handle=1748,i,154579317 19572670153, 4062602848324179866, 13 1072 /prefetch:8

C:\Program Files\Google\Chrome\Application\chrom

PID:224

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.UtilReadIcon --lang=en-US --serv ice-sandbox-type=icon_reader --moj o-platform-channel-handle=5176 --f ield-trial-handle=1748,i,154579317 19572670153, 4062602848324179866, 13 1072 /prefetch:8

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:5016

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=rende rer --lang=en-US --device-scale-fa ctor=1 --num-raster-threads=4 --en able-main-frame-before-activation --renderer-client-id=15 --mojo-pla tform-channel-handle=5540 --fieldtrial-handle=1748, i, 15457931719572 670153, 4062602848324179866, 131072 /prefetch:1

C:\Program Files\Google\Chrome\Application\chrom

PID:512

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=rende rer --lang=en-US --device-scale-fa ctor=1 --num-raster-threads=4 --en able-main-frame-before-activation --renderer-client-id=16 --mojo-pla tform-channel-handle=5564 --fieldtrial-handle=1748,i,15457931719572 670153,4062602848324179866,131072 /prefetch:1

C:\Program Files\Google\Chrome\Application\chrom e.exe

PID:4168

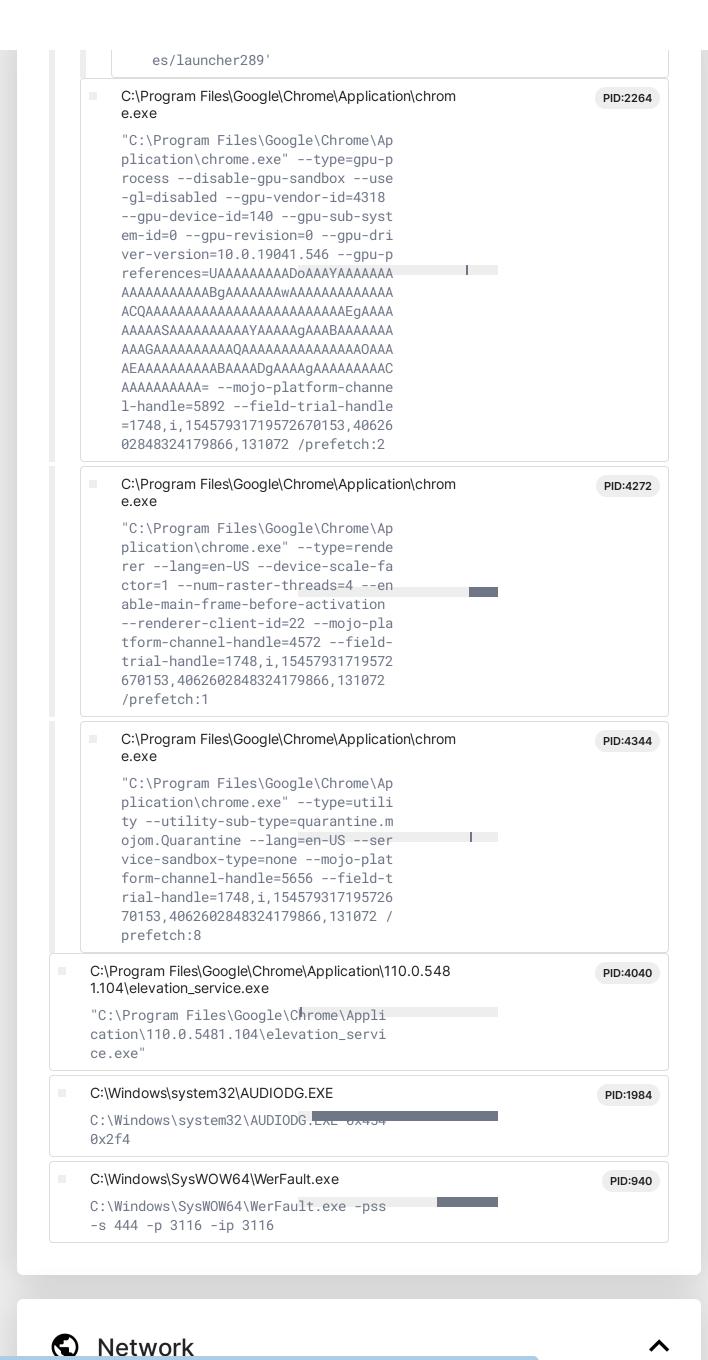
"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=quarantine.m ojom.Quarantine --lang=en-US --ser

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

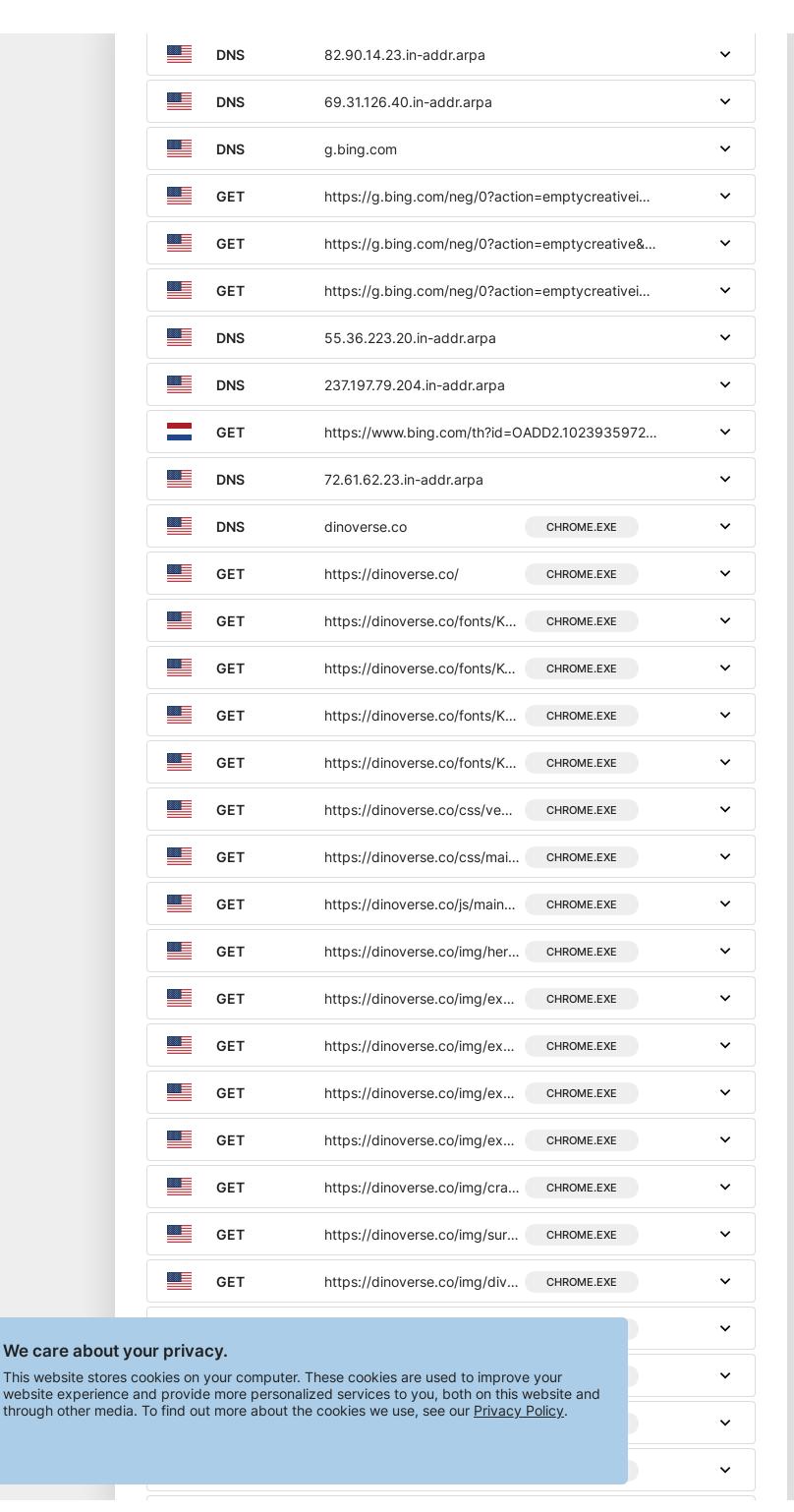
PID:752

"C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.UtilReadIcon --lang=en-US --serv ice-sandbox-type=icon_reader --moj o-platform-channel-handle=5908 --f ield-trial-handle=1748,i,154579317 19572670153, 4062602848324179866, 13 1072 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrom PID:4368 e.exe "C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.UtilReadIcon --lang=en-US -Lserv ice-sandbox-type=icon_reader --moj o-platform-channel-handle=5932 --f ield-trial-handle=1748,i,154579317 19572670153, 4062602848324179866, 13 1072 /prefetch:8 C:\Program Files\Google\Chrome\Application\chrom PID:4512 "C:\Program Files\Google\Chrome\Ap plication\chrome.exe" --type=utili ty --utility-sub-type=chrome.mojo m.UtilWin --lang=en-US --service-s andbox-type=none --mojo-platform-c hannel-handle=5800 --field-trial-h andle=1748, i, 15457931719572670153, 4062602848324179866,131072 /prefet ch:8 C:\Users\Admin\Downloads\Installer.exe PID:2864 "C:\Users\Admin\Downloads\Installe r.exe" C:\Windows\System32\WindowsPowerShell\v1.0 PID:1604 \powershell.exe "powershell.exe" Add-MpPreferenc e -ExclusionPath 'C:/Program Fil es/launcher289' C:\Program Files\launcher289\connection1404.ex PID:4880 "C:\Program Files\launcher289\co nnection1404.exe" C:\Windows\BitLockerDiscoveryVolumeConten PID:2440 ts\BitLockerToGo.exe C:\Windows\BitLockerDiscoveryV olumeContents\BitLockerToGo.ex C:\Windows\System32\WindowsPowerShell\v1.0 PID:396 \powershell.exe "powershell.exe" Add-MpPreferend e -ExclusionPath 'C:/Program Fil es/launcher289' C:\Program Files\launcher289\update1404.exe PID:3116 "C:\Program Files\launcher289\up date1404.exe" PID:2340 We care about your privacy. This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy. PID:2240

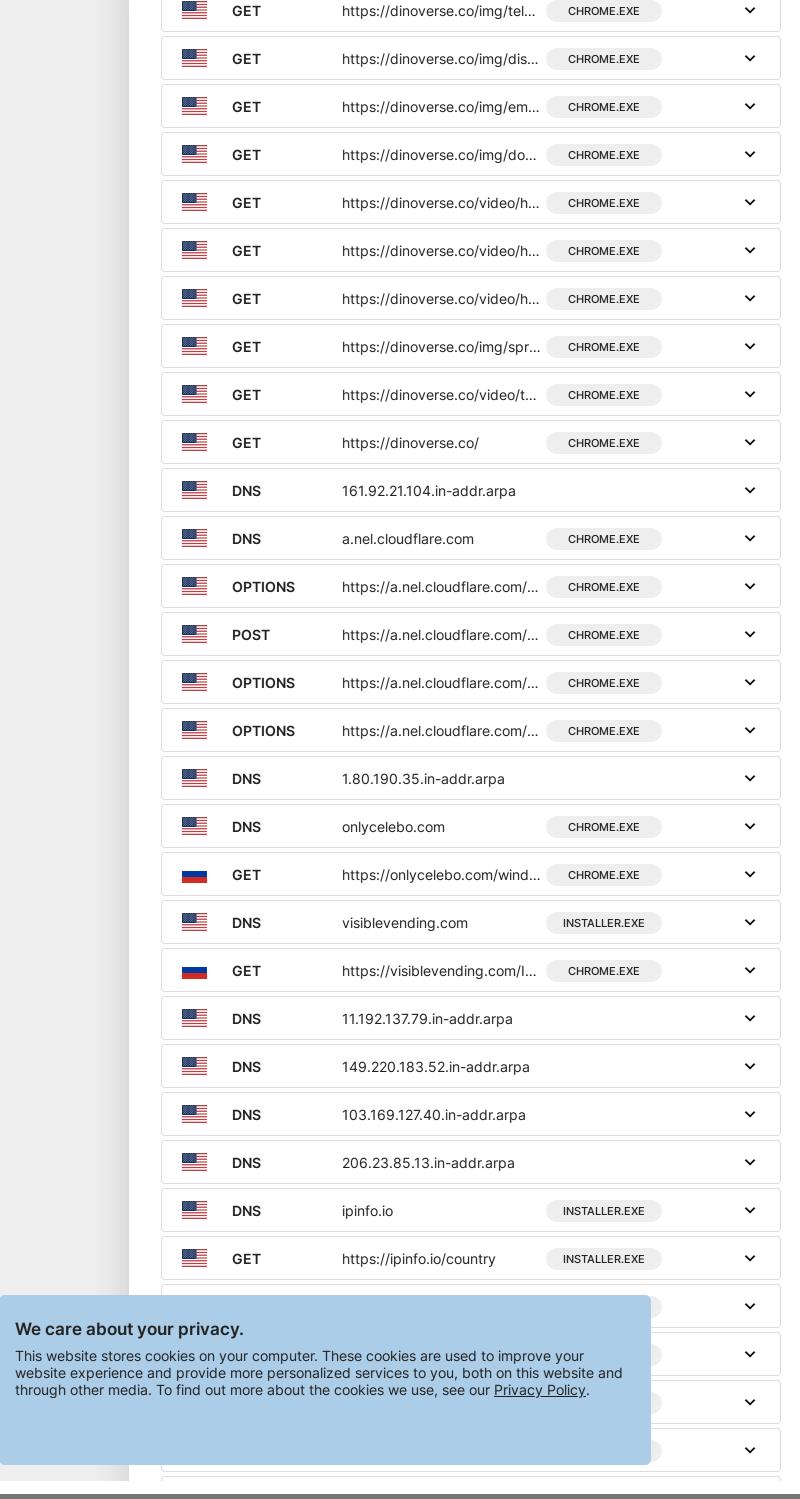


We care about your privacy.

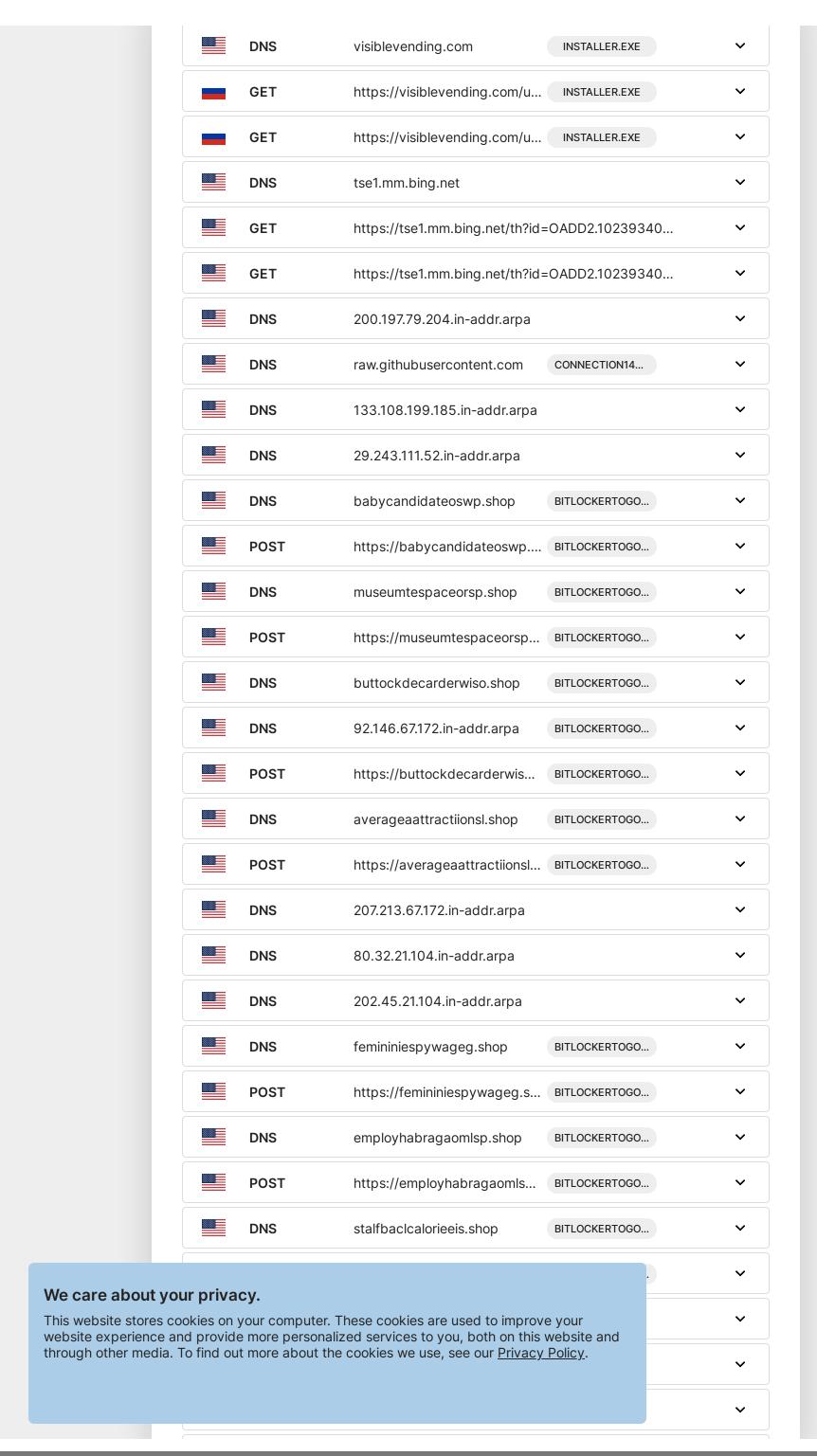
This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.

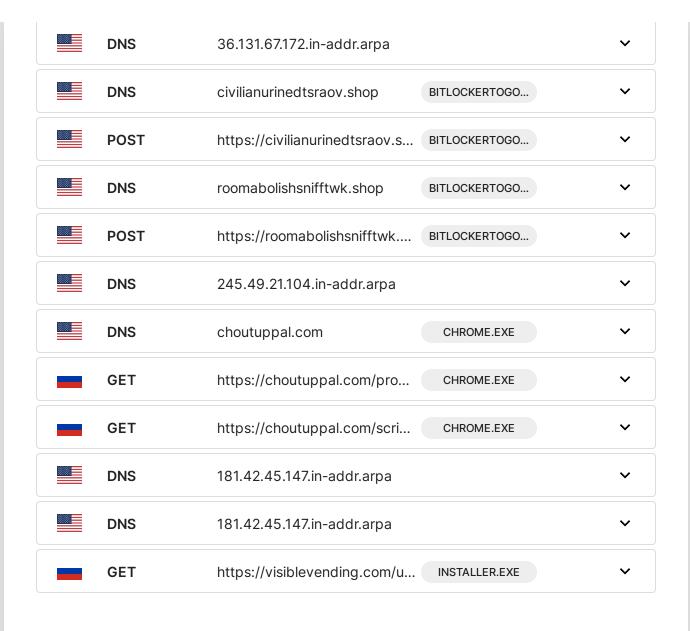


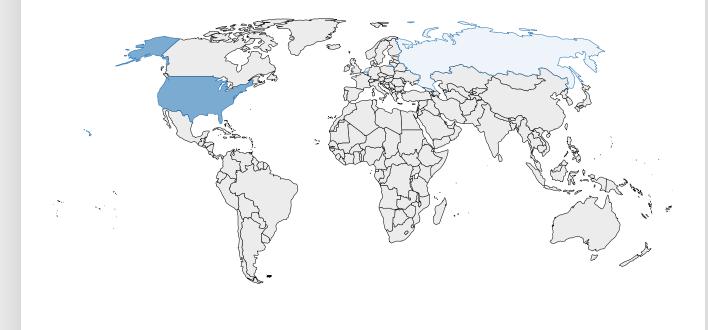
Page 8 of 16



		GET	https://ipinfo.io/ip	INSTALLER.EXE	~	
		GET	https://ipinfo.io/country	INSTALLER.EXE	~	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	~	
		GET	https://ipinfo.io/country	INSTALLER.EXE	~	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	~	
		GET	https://ipinfo.io/country	INSTALLER.EXE	·	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	·	
		GET	https://ipinfo.io/country	INSTALLER.EXE	·	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	·	
		GET	https://ipinfo.io/country	INSTALLER.EXE	~	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	~	
		GET	https://ipinfo.io/country	INSTALLER.EXE	~	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	~	
		GET	https://ipinfo.io/country	INSTALLER.EXE	~	
		GET	https://ipinfo.io/ip	INSTALLER.EXE	~	
		GET	https://ipinfo.io/country	INSTALLER.EXE	~	
		DNS	192.186.117.34.in-addr.arpa		~	
		DNS	api.telegram.org	INSTALLER.EXE	~	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	~	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	~	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	~	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	·	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	·	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	·	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	·	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	~	
		GET	https://api.telegram.org/bot	INSTALLER.EXE	~	
	_				~	
We care about your privacy. This website stores cookies on your computer. These cookies are used to improve your						
website experience an	website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy .					

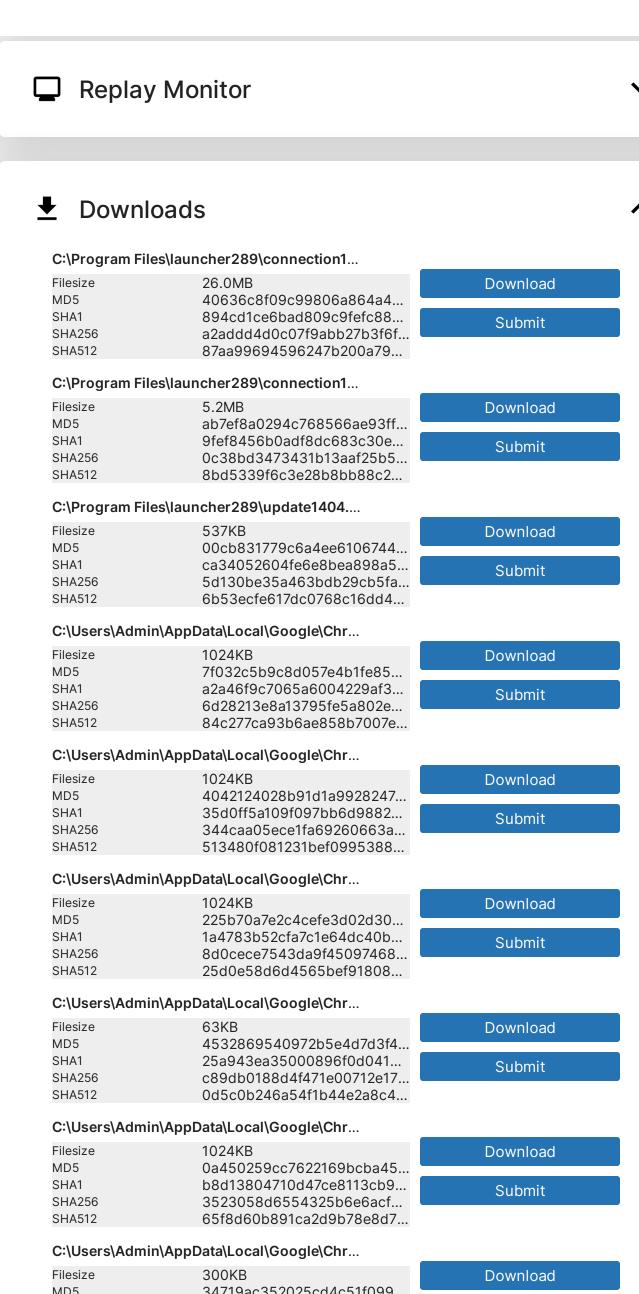






We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.



MD5 34719ac352025cd4c51f099...
SHA1 8d0778a93035733be0bda8...
SHA256 2b906ef3dbfaf48616d1bc0f...

Submit

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.

nload

mit

Filesize 72B

MD5 969401e9fdd0b6241a02cc8... SHA1 9de88b7e388fe51469d9c3b... SHA256 cf6d54fef643fbe85b773596... SHA512

f0024c4441fb6cfbd4a8c6e5...

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize 72B

MD5 28862ab369a56c5511c18eb... SHA1 05c2cdb18490f48256f381b... SHA256 7dedfd3e6ec5cfe889d7c373... **SHA512** b5513ba2776f3f0b1c4b3a7...

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize 2KB

MD5 a9595cb3c5a4db3f7e328d7... SHA1 8bb997522fdbba45f1e24ba... SHA256 0b108144c9c9afd59d75c81... **SHA512** 8aefb4394e20a7ca75dd326...

Submit

Download

Submit

Download

Submit

Download

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize 2B

MD5 d751713988987e933198036... SHA1 97d170e1550eee4afc0af065... SHA256 4f53cda18c2baa0c0354bb5... **SHA512** b25b294cb4deb69ea00a4c...

Download

Submit

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize 7KB MD5 6e290151d441ed9cfcf9f2af8...

SHA1 8561cbecdf2b2bd8144e15e... 087e7fdb0daee157b225840... SHA256 SHA512 d5a940a6a9ccc3ee24b2b2f... Download

Submit

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize **10KB**

MD5 a0c36ee98ffbbbaa9cc09f98... SHA1 a5e1a56b4876b71aa17c760... SHA256 ce9f5901407d094841af5df0... SHA512 94581623a05239c8e1ab410...

Download Submit

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize **10KB**

MD5 2d4e8526dd3495ad58dbd8... SHA1 ae56cf3b08aad326cdda318... SHA256 0b31a6631741a8aa7c6b3bef... SHA512 583e219cf8992c4348cc5e0...

Download Submit

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize **10KB**

MD5 5c94edcbc22ebd88155dfe3... SHA1 fae518dae088b82742c8190... SHA256 b65c6ae351217a0d6fa756d... **SHA512** d74e17ed640cda72d0ccac1...

Download

Submit

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize

MD5 fe5354ecacecefbd691285cb... SHA1 af9ec7156f92a025f7eb4efa6... SHA256 b52c8d8f296ca9cd38cf709... SHA512 6891e07723f6bf44e820c06...

Download

Submit

C:\Users\Admin\AppData\Local\Google\Chr...

C:\Users\Admin\AppData\Local\Google\Chr...

Filesize 9KB

MD5 c82a033f819017f3107087b1... SHA1 85143829e0780857eecbd9... e96482f1c612f1dc477bea26... SHA256 SHA512 3f9287c067f04308b241550... Download

Submit

255KB

MD5 1c12ee90a54eaef8d681d84... SHA1 f8b2e8aa8b68bfbf770ca653... SHA256 de2abce4dfdbab0f922a2d5...

Download

Submit

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our Privacy Policy.

nload

mit

Filesize 101KB Download MD5 ef93373f93537c140269c36... SHA1 c96cd85d34ecb291e76389... Submit SHA256 c4ab95811d5fbe4563ea731... SHA512 0773d98b78d648cae51fbcc... C:\Users\Admin\AppData\Local\Google\Chr... Filesize **88KB** Download MD5 397327d8185a11922743ee0... SHA1 2b29a6f596574e946c6b20a... Submit 31bafae5171d06419fc33ced... SHA256 4322a826c5861f472a5db94... **SHA512** C:\Users\Admin\AppData\Local\Microsoft\... Filesize 2KB Download MD5 d85ba6ff808d9e5444a4b36... SHA1 31aa9d96590fff6981b315e0... Submit SHA256 84739c608a73509419748e... **SHA512** 8c414eb55b45212af385acc... C:\Users\Admin\AppData\Local\Microsoft\... Filesize 944B Download MD5 6d42b6da621e8df5674e26b... SHA1 ab3ce1327ea1eeedb987ec82... Submit SHA256 5ab6a1726f425c6d0158f55e... 53faffbda8a835bc1143e894... **SHA512** C:\Users\Admin\AppData\Local\Microsoft\... Filesize 944B Download MD5 15dde0683cd1ca19785d726... SHA1 d039c577e438546d10ac64... Submit SHA256 d6fa39eab7ee36f44dc3f9f2... 57c0e1b87bc1c136f0d39f3c... SHA512 C:\Users\Admin\AppData\Local\Temp\.net\I... Filesize 4.7MB Download MD5 a7b7470c347f84365ffe1b20... SHA1 57a96f6fb326ba65b7f70162... Submit SHA256 af7b99be1b8770c0e4d18e4... SHA512 83391a219631f750499fd96... C:\Users\Admin\AppData\Local\Temp\.net\I... Filesize 1.2MB Download MD5 0c147149b444748dae0a04e... SHA1 f7edbcd6d1d6b199b6c997d... Submit SHA256 e284235a4d6e5d90569235... SHA512 ec057829c03623cabc5a42d... C:\Users\Admin\AppData\Local\Temp\.net\I... Filesize 1.9MB Download MD5 425573cd9eea68d2dc78bd7... SHA1 156ba2df6d5f9ac9b72bb1f9... Submit SHA256 9c3fdfb42c920bf26f0fbeaee... **SHA512** 91c2c7279bd4cf9aac6fb699... C:\Users\Admin\AppData\Local\Temp__PS... Download Filesize MD5 d17fe0a3f47be24a6453e9ef... SHA1 6ab83620379fc69f80c0242... Submit 96ad1146eb96877eab5942a... SHA256 SHA512 5b592e58f26c264604f98f6... \??\pipe\crashpad_3744_NWUOASVMYNYB... Download MD5 d41d8cd98f00b204e98009... SHA1 da39a3ee5e6b4b0d3255bfe... Submit e3b0c44298fc1c149afbf4c8... SHA256 SHA512 cf83e1357eefb8bdf1542850... memory/1604-286-0×000001E3E9260000... Download Filesize 136KB memory/2440-339-0×000000001210000... Download Filesize 328KB We care about your privacy. nload This website stores cookies on your computer. These cookies are used to improve your

website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.

nload

mamaru/4000_242_0~00007EE701140000

memory/3116	-353-0×0000000033C0000	Download
Filesize	4.0MB	Download
memory/3116	-354-0×0000000033C0000	Download
Filesize	4.0MB	
memory/3116	-355-0×00007FFFBC790000	Download
Filesize	2.0MB	
memory/3116	-357-0×000000077280000	Download
Filesize	2.1MB	
memory/4016	-360-0×000000002AE000	Download
Filesize	4.0MB	
memory/4016	-361-0×00007FFFBC790000	Download
Filesize	2.0MB	
memory/4016	-363-0×0000000077280000	Download
Filesize	2.1MB	Download
memory/4016	-358-0×000000000DC000	
Filesize	36KB	Download
	© 2018-2024	Terms Priva

·I¦I·Recorded Future®

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.